

20212944627

СОБРАНИЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на членот 75, ставови 1 и 2 од Уставот на Република Северна Македонија, претседателот на Република Северна Македонија и претседателот на Собранието на Република Северна Македонија издаваат

У К А З

ЗА ПРОГЛАСУВАЊЕ НА ЗАКОНОТ ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Се прогласува Законот за изменување и дополнување на Законот за заштита на личните податоци,

што Собранието на Република Северна Македонија го донесе на седницата одржана на 23 декември 2021 година.

Бр. 08-5469/1
23 декември 2021 година
Скопје

Претседател на Република
Северна Македонија,
Стево Пендаровски, с.р.

Претседател
на Собранието на Република
Северна Македонија,
м-р **Talat Xhaferi, с.р.**

ЗАКОН ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 1

Во Законот за заштита на личните податоци (*) („Службен весник на Република Северна Македонија“ број 42/20), насловот на членот 14 се менува и гласи: „Обработка на лични податоци поврзани со казнени осуди и казнени дела“.

Член 2

Во член 14 во првата и втората реченица зборовите: „осуди за кривични дела“ се заменуваат со зборовите: „казнени осуди и казнени дела“.

Член 3

Во членот 39 став (9) по зборот „Контролорот“ се додаваат зборовите: „е должен да“.

Член 4

Во членот 64 став (1) зборовите: „со овој“ се бришат.

Член 5

Во член 122 зборот „до“ се заменува со зборот „со“.

Член 6

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

20242664621

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр.42/20 и 294/21), директорот на Агенцијата за заштита на личните податоци донесе

ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Предмет

Член 1

Со овој правилник се пропишуваат насоки за активностите кои контролорите треба да ги преземаат при планирање, воспоставување, применување, преиспитување и ажурирање на техничките и на организациските мерки за да се обезбеди безбедност на обработката на личните податоци.

Поимник

Член 2

Одделните изрази употребени во овој правилник и во неговите прилози го имаат следново значење:

1. **Цел на заштита** е обезбедување на правно усогласена обработка на личните податоци преку соодветни технички и организациски мерки, со цел да се ублажат ризиците и да се избегнат негативните влијанија врз правата и слободите на физичките лица;

2. **Минимизирање на личните податоци** е цел на заштита преку ограничување на обработката на личните податоци на она што е соодветно, релевантно и неопходно за конкретната цел. Минимизирањето се однесува на дизајнот на системите за обработка на личните податоци, количината на обработени лични податоци, обемот на обработка, достапноста и периодот на чување;

3. **Доверливост** е цел на заштита преку која треба да се обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци;

4. **Интегритет** е цел на заштита преку која се гарантира дека личните податоци што се обработуваат се целосни, точни и ажурирани. Интегритетот се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции;

5. **Достапност** е цел на заштита преку која треба да се обезбеди непречен пристап и контитуирана расположливост на личните податоци, односно пристапот до личните податоци и нивната обработка се можни без одложување, како и дека личните податоци може да се користат правилно во предвидениот процес;

6. **Неповрзливост** е цел на заштита преку која треба да се обезбеди дека личните податоци се обработуваат строго ограничувајќи се на целта за која првично биле собрани, како и дека нема да се спојуваат или да се поврзуваат со други лични податоци што се собрани за други цели.

7. **Транспарентност** е цел на заштита преку која треба да се обезбедат информации за обработката на личните податоци, односно можност да се идентификува на различно ниво кои податоци се собираат и се обработуваат, кога и за кои цели на обработка, кои системи и процеси се користат за да се утврди дали личните податоци се обработуваат според определената цел, како и кој има одговорност во различните процеси на нивната обработка;

8. **Интервенирање** е цел на заштита преку која треба да се обезбеди ефективно остварување на правата на субјектите на лични податоци, како и применување на мерки за идентификување и автентикација на субјектите на лични податоци кои сакаат да ги остварат своите права;

9. **Ризик** е постоење можност за појава на настан што сам по себе претставува штета (вклучително и неоправдано вмешување во правата и слободите на физичките лица) или може да доведе до дополнителна штета за едно или за повеќе физички лица. Сериозноста на ризикот е комбинација од влијанието на штетата и веројатноста дека настанот и последователната штета ќе се случат. Ризикот во контекст на заштита на личните податоци секогаш се оценува во однос на негативните влијанија врз правата и слободите на физичките лица;

10. **Процес на управување со ризик** е систематска примена на политики, процедури и практики за управување со активностите кои се однесуваат на: комуницирање, консултирање, утврдување на контекстот, идентификување, анализирање, евалуирање, третирање, следење и проверување на ризикот;

11. **Систем за заштита на лични податоци** е збир од документирани политики, кодекси на однесување, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на технички и организациски мерки за постигнување на целта на заштита согласно прописите за заштита на личните податоци;

12. **Информациски систем** е целина од компоненти преку кои се обработуваат личните податоци при активностите за нивна обработка. Ова ги опфаќа вклучените системи (на пример, работни станици, сервери, мрежни или безбедносни уреди), услуги (на пример, процедура, единствена функција или збир од функции што служат за одредена цел) и податоци (на пример, специфични полиња од лични податоци што се користат за обработка);

13. **Инцидент** или таканаречен настан е појава или промена на одредени околности кои што влијаат врз правата и слободите на физичките лица.

Примена

Член 3

Одредбите од овој правилник кои се однесуваат на воспоставување на информациски систем се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци и
- друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Воспоставување на информациски систем

Член 4

(1) Контролорот е одговорен за воспоставување на функционален и одржлив информациски систем според прописите за заштита на личните податоци.

(2) За воспоставување на информациски систем, контролорот треба да подготви соодветна документација за системот, која особено опфаќа:

- прикажување на определената цел за обработка на личните податоци;
- прикажување на редоследот на активности за обработка на личните податоци;
- прикажување на сите употребени и генерирани лични податоци;
- опишување на техничките компоненти што се користат (хардвер, софтвер и инфраструктура);
- евиденција на активностите за обработка;
- разграничување со други активности кои што не се однесуваат на обработка на лични податоци;
- прикажување на релации со други системи за контрола и верификација на движењето на личните податоци.

(3) Пред воспоставување на информациски систем, контролорот треба да ја процени подготвената документација од ставот (2) на овој член според:

- начелата поврзани со обработката на личните податоци;
- законитост на обработката на личните податоци;
- правата на субјектите на личните податоци;
- неопходноста од вршење на проценка на влијанието на заштитата на личните податоци;
- примената на соодветни технички и организациски мерки од страна на обработувачите;
- условите за пренос на лични податоци.

(4) Доколку се исполнети околностите од ставот (3) на овој член, контролорот треба да изврши проценка на ризикот според Методологијата за проценка на ризик (Прилог бр.1), која е составен дел на овој правилник, а за да се избегнат негативните влијанија врз правата и слободите на физичките лица.

(5) Според процената на ризикот од ставот (4) на овој член, контролорот треба идентификуваните ризици да ги ублажи до соодветно ниво на прифатливост на ризикот преку избор и примена на соодветни технички и организациски мерки за да се обезбеди ниво на безбедност соодветно на ризикот, а според Прилог бр. 2 - Цели на заштита, закани и мерки, кој е составен дел на овој правилник.

(6) За воспоставување на информациски систем, контролорот треба да преземе активности за усогласување на околностите од ставот (3) на овој член со соодветното ниво на прифатливост на ризикот од процената на ризикот од ставот (4) на овој член.

(7) Документираниот процес од овој член во однос на воспоставување на информациски систем ќе се смета за систем за заштита на личните податоци според прописите за заштита на личните податоци.

Одржување на информацискиот систем

Член 5

(1) Контролорот е одговорен за преиспитување и ажурирање на информацискиот систем, а особено во однос на техничките и организациските мерки кои ги применува за да обезбеди безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци.

(2) Физичките или правните лица кои вршат одржување на информацискиот систем во име на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

Пренос на лични податоци во трети земји

Член 6

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во трети земји само согласно условите утврдени во прописите за заштита на лични податоци.

Систем за заштита на лични податоци

Член 7

(1) Според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различно ниво на сериозност во однос на нивното влијание врз правата и слободите на физичките лица, контролорот воспоставува систем за заштита на личните податоци преку примена на технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот.

(2) Техничките и организациските мерки од ставот (1) на овој член треба да ги вклучуваат сите неопходни мерки за гарантирање на целите на заштитата и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање (Прилози бр.1 и бр.2).

(3) Контролорот задолжително ги преиспитува и ги ажурира техничките и организациските мерки, при што секогаш ги применува оние мерки кои се соодветни за гарантирање на целите на заштита пропишани со одредбите на овој правилник.

(4) Процесот за управување со системот за заштита на личните податоци од ставот (1) на овој член се дефинира како дел од политиката на контролорот за системот за заштита на личните податоци кој треба да е соодветен на природата, обемот и сложеноста на активностите коишто контролорот ги врши при обработката на личните податоци и ризиците на коишто е изложен системот.

(5) Контролорот задолжително ја ревидира и ажурира документацијата во врска со системот за заштита на личните податоци според направените промени во неговите операции на обработка на личните податоци.

Управување со ризик

Член 8

(1) При идентификување и проценка на ризиците (управување со ризик), контролорот задолжително ги зема предвид ризиците кои се поврзани со обработката на личните податоци за да ги обезбеди целите на заштитата и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање (Прилози бр.1 и бр.2).

(2) Управувањето со ризикот од ставот (1) на овој член опфаќа неколку фази и тоа:

а) список (преглед) на информацискиот систем во целина со сите системи, услуги и податоци што се користат за обработка на личните податоци;

б) проценка на ризиците за секој процес на обработка на личните податоци;

в) спроведување и проверка на планираните мерки и

г) спроведување на периодични безбедносни проверки.

(3) Списокот на системи, услуги и податоци што се користат за обработка на личните податоци од ставот (2) точка а) на овој член треба да биде опфатен со описот на техничките и организациските мерки кои се применуваат за обезбедување безбедност на обработката на личните податоци.

(4) Процената на ризиците од ставот (2) точка б) на овој член, за секој ризик, го вклучува најмалку следното:

(а) идентификување на потенцијалните влијанија и ефекти врз правата и слободите на засегнатите физички лица во однос на можните закани за целите на заштитата како што следува:

- минимизирање на личните податоците (на пример, имплементација на периоди за чување, криптирање или анонимизација),
- достапност (на пример, привремена или целосна недостапност на личните податоци),
- интегритет (на пример, несакани промени на личните податоци),
- доверливост (на пример, неовластен пристап до личните податоци),
- неповрзливост (на пример, ограничување на овластувањата за обработка, користење и пренос),

- транспарентност (на пример, записи за пристап до личните податоци) и
- интервенирање (на пример, имплементација на стандардизирани процедури за обезбедување на правото на пристап на субјектите на личните податоци);

(б) идентификување на изворите на ризик кои што би можеле да бидат причина за секој непосакуван настан, со соодветно разгледување на внатрешните и на надворешните човечки ресурси (на пример, администратор на информациски систем, овластено лице, надворешен напаѓач, конкурент), како и други внатрешни и надворешни извори (на пример, вода, опасни материјали, пожар, вирус);

(в) идентификување на лице или субјект со одговорност и овластување да управува со конкретниот ризик (сопственик на ризик);

(г) идентификување на можните закани кои би можеле да се случат преку медиуми на кои се обработуваат личните податоци (на пример, хардвер, софтвер, комуникациски канали, документи во хартиена форма, итн.), кои би можеле да се:

- користат на несоодветен начин (на пример, злоупотреба на овластувањата, грешка при ракување);

- изменат (на пример, „заразен“ софтвер или хардвер со снимач на записите на тастатурата, инсталирање на злонамерен односно малициозен софтвер итн.);

- изгубат (на пример, кражба на лаптоп или губење мемориски уреди);

- надгледуваат (на пример, геолокација на опремата);

- оштетат (на пример, вандализам, деградација поради природно абење);

- преоптоварат (на пример, медиумот за чување на лични податоци е целосно пополнет, напад на одбивање услуга итн.);

(д) процена на веројатноста за појава (веројатност) во однос на претходните елементи предвидени во овој став на скала за процена: ретко, повремено и често;

(ѓ) процена на нивото на влијание во однос на претходните елементи предвидени во овој став на скала за процена: ниско, средно и високо;

(е) процена на сериозноста на ризикот во однос на претходните елементи предвидени во овој став на скала за процена: незначителен ризик, ризик и висок ризик.

(5) Контролорот задолжително врши спроведување и проверка на планираните мерки од ставот (2) точка в) на овој член за да обезбеди дека тие се применуваат и тековно се тестираат.

(6) Контролорот задолжително спроведува периодични безбедносни проверки од ставот (2) точка г) на овој член, за што се изготвува акционен план чија имплементација се следи од страна на раководството на контролорот.

Период на прилагодување

Член 9

Во смисла на член 28 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр.42/20 и 294/21), контролорот задолжително го прилагодува своето работење со одредбите на овој правилник во рамките на предвидениот период на преиспитување и ажурирање на техничките и организациските мерки кои се применуваат за обезбедување безбедност на обработката на личните податоци.

Престанување на важење

Член 10

Со денот на применувањето на овој правилник престанува да важи Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр.122/20).

Влегување во сила и примена

Член 11

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“, а ќе започне да се применува од 1 јули 2025 година.

Бр. 01-1320/1
23 декември 2024 година
Скопје

Директор,
Имер Алиу, с.р.

Прилог бр.1

Методологија за процена на ризик

1. Подготовка на анализа на ризик

Идентификување на процесот што треба да се евалуира и предвидената цел

Процес на обработка на лични податоци	
Цел	

Пример:

Процес на обработка на лични податоци	<i>Педагошка документација и педагошка евиденција вклучително и досие на детето</i>
Цел	<i>Детската градинка/центарот за ран детски развој води педагошка документација и педагошка евиденција за воспитно-образовните активности согласно Законот за заштита на децата</i>

Информациите за процесот којшто треба да се евалуира и предвидената цел може да се преземат од евиденцијата на активности за обработка која контролорот ја води според одредбите на членот 34 од Законот за заштита на личните податоци.

Анализата на ризик ги опфаќа постапките (специфичен начин за извршување на активноста) кои што треба да се проценат, вклучувајќи ги сите технички и организациски мерки кои се користат од страна на контролорот.

Доколку се планирани други технички и организациски мерки, но истите сè уште не се интегрирани во постапките, тогаш контролорот тие мерки не ги зема предвид при оваа анализа на ризик.

Првиот чекор е да се идентификуваат субјектите на лични податоци односно категориите на субјекти на лични податоци (физички лица) за кои се обработуваат лични податоци во текот на процесот (збир на активности кои меѓусебно се поврзани или се во меѓусебна зависност).

Субјекти на лични податоци (категории на субјекти на лични податоци)	
---	--

Пример:

Субјекти на лични податоци (категории на субјекти на лични податоци)	Деца, воспитувачи
--	-------------------

Потоа се идентификуваат личните податоци односно категориите на лични податоци што се обработуваат во текот на процесот.

Категории на лични податоци	
-----------------------------	--

Пример:

Категории на лични податоци	Деца: име и презиме на детето, датум и место на раѓање, државјанство, адреса на живеење Воспитувачи: име, презиме, степен на образование, лиценца
-----------------------------	--

Понатаму, следува идентификување на другите компоненти што се вклучени во процесот на обработка (системи, услуги и процеси).

Системи	
Услуги	
Процеси	

Пример:

Системи	Лаптоп, софтвер за обработка на документи или друг специјализиран софтвер, локална мрежа, сервери
Услуги	Регистрирање
Процеси	Методи на внесување, ажурирање и бришење

2. Скала на влијание

Контролорот потребата за заштита ја идентификува преку личните податоци коишто се обработуваат, нивната природа, обем, контекст и цел на обработка и истата треба да одговара на максималното ниво на влијание на кои можат да бидат изложени правата и слободите на засегнатите физички лица во однос на можните закани на целите на заштитата.

Целите на заштита се следните:

- Минимизирање на личните податоци
- Доверливост
- Интегритет
- Достапност
- Неповрзливост
- Транспарентност
- Интервенирање

На потребата за заштита не влијаат техничките и организациските мерки кои ги користи контролорот и истата е предвидена на скала од три нивоа како што следува:

Влијание	Дефиниција	Примери
Ниско [Вредност = 1]	Тоа се лични податоци чија обработка не предизвикува сериозни влијанија за засегнатите субјекти на лични податоци.	Име и презиме без известување за ограничување, назив/звање на работно место
Средно [Вредност = 2]	Тоа се лични податоци чија обработка може негативно да влијае врз засегнатите субјекти на лични податоци во однос на нивната социјална или економска положба.	Година на раѓање, датум на раѓање, податоци за висина на плата, податоци за други лични приходи
Високо [Вредност = 3]	Тоа се лични податоци чија обработка може значително да влијае врз засегнатите субјекти на лични податоци во однос на нивната социјална или економска положба, како и за нивната лична слобода.	Генетски податоци, биометриски податоци, здравствени податоци или податоци што се однесуваат на сексуалниот живот или на сексуалната ориентација, податоци поврзани со казни осуди и казни дела, единствен број на граѓанинот.

Во случај на ниско или средно ниво на влијание, има потреба за заштита на најмалку на „основно ниво“ од страна на контролорот, а при високо ниво на влијание се јавува потреба за заштита од „високо ниво“.

Притоа, важен индикатор за активностите за обработка се категориите на лични податоци, особено кога станува збор за посебни категории на лични податоци (генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето и други податоци), па врз основа на овие категории на лични податоци, би можело да се предвиди соодветна потреба за заштита („високо ниво“) без дополнителна анализа, а според претходно наведената скала на влијание.

Пример: за обработка на лични податоци на деца секогаш постои најмалку „високо ниво“ на потреба од заштита, а за обработка на податоци на воспитувачите вообичаено постои потреба за заштита на „основно ниво“.

Потребите за заштита што се предвидени во овој дел, имаат влијание и врз системите, услугите и процесите што се вклучени во обработката на личните податоци. По правило, потребата за заштита се однесува и на компонентите со кои се врши обработка на личните податоци. Во одредени случаи, како на пример во однос на централните компоненти како што се серверите, истите може да се класифицираат и поинаку доколку компонентата се користи и за други постапки или доколку е редундантна.

☐ Ниско	☐ Средно	☐ Високо
--------------------------------	---------------------------------	---------------------------------

3. Идентификување (релевантни) закани за компонентите на постапката

Секоја обработка на лични податоци сама по себе претставува настан што може негативно да влијае врз правата и слободите на физичките лица. Затоа, од една страна, закани на тие права и слободи може да произлегуваат од дизајнот на самата активност за обработка, односно од дизајнот на поврзаните системи и услуги и пот процеси.

Примери за ова би биле: правата за пристап според правилото „потребно е да знае“ или ограничување на правата на субјектите на лични податоци.

Од друга страна, закани на правата и слободите на физичките лица може да произлегуваат од безбедноста на информатичката технологија која се користи за обработка на личните податоци, како и од организациското опкружување на обработката, а тоа може да има индиректно влијание врз активноста на обработка и на личните податоци што се обработуваат, особено поради недоволните заштитни мерки кои се користат од страна на контролорот.

Пример за ова би било: напад со злонамерен софтвер што може да ја загрози доверливоста на личните податоци.

Закани	
---------------	--

Пример:

Закани	Ненамерно менување на податоците поради неправилна работа на софтверската апликација Неовластен пристап до (и откривање на) податоците на децата поради кражба на лаптоп
---------------	--

4. Скала на веројатност за појава

За секоја идентификувана закана, веројатноста за појава се одредува на скала од три нивоа како што следува:

Веројатност за појава	Дефиниција
Ретко [Вредност = 1]	- Може да настане штета, но конкретните околности спречуваат таков настан и не треба да се очекува дека тој ќе се појави. - Можно е да настане штета, но зависи од однесувањето на трети лица, а конкретните околности укажуваат на тоа дека третите лица преземаат активности против настанување на штета и не се очекува тоа да се промени.
Повремено [Вредност = 2]	- Може да настане штета, која зависи од несигурностите што не можат да се предвидат. - Може да настане штета, која зависи од однесувањето на трети лица кое не може да се предвиди.
Често [Вредност = 3]	- Може да се очекува да настане штета. - Може да настане штета и треба да се очекува дека ќе настанат околности што ќе ја предизвикаат истата. - Може да настане штета, која зависи од однесувањето на трети лица, кое веќе произлегува/се појавува за што постои ефективна ситуација за предизвикување

Пример:

Веројатност за појава	Ненамерно менување на податоците поради неправилна работа на софтверската апликација <u>Ретко</u> Неовластен пристап до (и откривање на) податоците на децата поради кражба на лаптоп <u>Често</u>
------------------------------	--

При процена на веројатноста за појава во однос за настан што произлегува од самиот дизајн на активност на обработката, начелно мора да се претпостави најголемата веројатност за појава („често“), а во однос на закани што потекнуваат надвор од планирањето на активност за обработка може да биде на пониско ниво.

☐ Ретко	☐ Повремено	☐ Често
--------------------------------	------------------------------------	--------------------------------

Оттука, описот на поединечните ризици е целосен кога се состои од: прецизирање на ризична ситуација во компонентата што е вклучена во процесот на обработка (настан на штета), потребата за заштита на соодветните лични податоци, како и веројатноста за појава на штетниот настан.

5. Матрица за процена

Ризиците што се идентификувани и рангирани во однос на влијанието и веројатноста за појава, може да се прикажат на дводимензионален дијаграм за илустрирање и одредување на сериозноста на конкретниот ризик.

Добиената вредност на ризик може да се пресмета како: Ризик = Влијание x Веројатност за појава.

Обработката со проценето *средно влијание* (вредност 2) и процена *често* (вредност 3) за веројатноста за појава ќе доведе до резултат од *висок ризик* ($2 \times 3 = 6$).

Резултат на матрицата на ризик :

Влијание			
Високо	3	6	9
Средно	2	4	6
Ниско	1	2	3
Веројатност за појава (Веројатност)	Ретко	Повремено	Често

- ☐ **Зелена:** Незначителен 1-2
☐ **Жолта:** Ризик 3-4
☐ **Црвена:** Висок ризик ≥ 6

6. Евалуација/толкување

За секој идентификуван ризик, се врши процена земајќи ги предвид нивото на влијание и веројатноста за појава.

Во случај на резултат во **зелените** полиња (*незначителен ризик*), обработката може да се реализира.

Во случај на резултат во **жолтите** полиња (*ризик*), контролорот треба да има предвид дали обработката може да се реализира во предвидената форма.

Во случај на резултат во **црвените** полиња (*висок ризик*), обработката на личните податоци не е дозволена без примена на дополнителни мерки за заштита.

7. Постапување со ризик

Контролорот за да може да управува со идентификуваните ризици, мора за секој ризик да добие резултат во жолта или зелено поле со примена на соодветни мерки за заштита за да може обработката да се реализира во предвидената форма. Доколку со предвидените мерки, контролорот не може да го ублажи ризикот со резултат во жолто или зелено поле, во тој случај контролорот треба да се консултира со Агенцијата за да се оцени дали и под кои услови предвидената обработка би можела да се реализира според одредбите од членот 40 од Законот за заштита на личните податоци.

Предвидените мерки за заштита може да влијаат како на нивото на влијание, така и на нивото на веројатноста за појава или на двете нивоа заедно.

Доколку се предвидат мерки за заштита, како, на пример, исклучување на одредени категории на лични податоци од процесот на обработка или спроведување други форми на минимизирање на личните податоци, тогаш тоа претставува значајна промена во активностите за обработка на личните податоци и во тој случај, контролорот мора да ја повтори анализата на ризик и постапувањето со активностите за обработка. При настанатите промени во активностите за обработка на овој начин, контролорот може да идентификува потреба од промена на мерките за заштита. Ако контролорот не идентификува потреба од промена на мерките за заштита, тогаш треба да ја повтори само

процената на веројатноста за појава.

За проверка на предвидените мерки за заштита, контролорот може проверката да ја изврши преку прашалникот во кој се структурирани мерките во однос на целите за заштита, даден во оваа методологија.

Прашалник за проверка

Минимизирање на личните податоци	
Заштитната цел на минимизирање на личните податоци се однесува на основното барање од Законот за заштита на личните податоци за ограничување на обработката на лични податоци само на тоа што е соодветно, релевантно и неопходно за целите на обработката. Барањето за минимизирање не се применува само на количината на лични податоци што се обработуваат, туку и на опфатот на самата обработка, периодот на чување и достапноста на податоците. Поконкретно, треба да се обезбеди дека личните податоци се чуваат во форма која дозволува само идентификација на субјектите на лични податоци сè додека тоа е неопходно за целите на обработката.	
☐	Намалување на евидентираниите категории на лични податоци;
☐	Намалување на операциите за обработка во секој процес;
☐	Намалување на можностите за давање на информации за личните податоци;
☐	Воспоставување на стандардни поставки за субјектите на лични податоци што ја ограничуваат обработката на нивните лични податоци на она што е неопходно за целта на обработката
☐	Воведување на мерки за автоматско блокирање и бришење;
☐	Маскирање на податоците за прикривање на полињата со личните податоци и воведување на процедури за автоматско блокирање и бришење и мерки за псевдонимизација и анонимизација;
☐	Редовно ажурирање на воспоставените процедури врз основа на спроведени контроли.

Достапност
Заштитната цел на достапноста се однесува на непречен пристап и континуирана расположливост на обработката на личните податоци. За таа цел, овластените лица треба да имаат пристап до личните податоци и при нивната обработка да ги применуваат предвидените процедури/политики. Достапноста вклучува конкретна можност за враќање на личните податоци, на пример преку системи за управување со податоци, структурирани бази на податоци и функции за пребарување, како и способност на техничките системи да ги презентираат податоците.

☐	Правење на сигурносни копии, соодветно планирање на состојбите на (во) процесот, конфигурирање, структурирање на податоците, историја на трансакции, според тестиран концепт;
☐	Заштита од надворешни влијанија (злонамерен софтвер, саботажа, виша сила);
☐	Документирање на синтаксата на податоците;
☐	Редундантност на хардвер, софтвер и инфраструктура;
☐	Спроведување на мерки за навремено повторно воспоставување на достапноста до личните податоци и пристапот во случај на инцидент, како и за правење на сигурносна копија;
☐	Подготвување на План за итни состојби кој ги предвидува мерките за обновување на активностите за обработка на личните податоци;
☐	Воведување на мерки за обезбедување на замена на овластените лица кои имаат пристап до личните податоци.

Интегритет	
Заштитната цел на интегритет од една страна се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции, а од друга страна интегритетот гарантира дека личните податоци кои се обработуваат континуирано се точни, целосни и ажурирани.	
☐	Ограничување на привилегиите за внес и промени;
☐	Користење на алгоритми за криптирање при обработката на личните податоци (контролни суми, електронски печат и потпис);
☐	Документирање на постапките за идентификација и проверка на пристапот на овластените лица и доделените улоги;
☐	Бришење и ажурирање на неточни лични податоци;
☐	Зајакнување на информациските системи преку склучување и минимизирање на секундарни функционалности;
☐	Идентификација и автентикација на овластените лица и опремата која се користи;
☐	Континуирано оценување, евалуација и ажурирање на документацијата за технички и организациски мерки;
☐	Дефинирање на процесите и редовно тестирање на функционалноста, ризиците, безбедносните празнини и несаканите ефекти на процесите;

☐	Определување на процесите и нивно редовно тестирање;
☐	Заштита од надворешни влијанија (шпионажа, хакирање).

Доверливост	
Заштитната цел на доверливоста треба да обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци. Неовластени лица не се само трети лица надвор од контролорот, туку и вработени кај обработувачи за кои не е потребен пристап до личните податоци за да ја извршат услугата или лица во организациски единици кај контролорот што немаат никаква поврзаност со обработката на личните податоци.	
☐	Сегрегација на должности и одговорности на овластените лица според правилото „потребно е да знае“, при што да се има предвид судирот на интереси при извршувањето на нивните работни задачи;
☐	Воведување мерки за автентикација на овластените лица;
☐	Спецификација и мониторинг на користењето на авторизирани ресурси, а особено комуникациските канали;
☐	Определување на опкружувањето (згради, простории) кои се опремени за обработка на лични податоци;
☐	Воведување мерки за вршење контрола на примената на организациските мерки, интерните процедури и договорните аранжмани со обработувачите;
☐	Користење на алгоритми за криптирање на личните податоци кои што се чуваат или се пренесуваат, како и воспоставување процеси за управување и заштита на криптираните информации;
☐	Заштита од надворешни влијанија (шпионажа, хакирање).

Неповрзливост	
Заштитната цел на неповрзувањето е да се обезбеди дека личните податоци нема да се обработуваат за друга цел различна од целта за која првично биле собрани при што натамошната нивна обработка би можела да биде дозволена само во строго дефинирани околности. Неповрзливоста треба да се обезбеди со технички и организациски мерки.	
☐	Воведување на мерки за ограничување на пристапот за обработка, користење и пренос на податоци од страна на овластените лица;
☐	Програмски пропуст или деактивирање на интерфејси во методите и компонентите при обработка на личните податоци;

☐	Воведување на мерки за забрана на заден влез (backdoors), како и воспоставување механизми за обезбедување на контрола на квалитетот при развивање софтверски решенија за обработка на личните податоци;
☐	Воспоставување на постапки за начинот на доделување на пристап според организациската поставеност и воведување на права на пристап според извршувањето на работните задачи;
☐	Употреба на псевдоними за одредена цел, потврда на идентитетот преку анонимизација, односно примена на протоколи за потврда на идентитетот на корисниците без да се загрози нивната приватност и обработување на псевдонимизирани или анонимизирани податоци;
☐	Регулирање и документирање на процесите за промена на целите за обработка.

Транспарентност	
Заштитната цел на транспарентност е да обезбеди информации за обработката на личните податоци, односно можност да се идентификува на различно ниво, кои податоци се собираат и се обработуваат, кога и за кои цели на обработка, кои системи и процеси се користат за да се утврди дали податоците се обработуваат според предвидената цел, како и кој има одговорност за нивната обработка.	
☐	Документирање на активностите за обработка на личните податоци според членот 34 од Законот за заштита на личните податоци;
☐	Документирање на компонентите на активностите за обработка на личните податоци, особено деловните процеси, базите на податоци, движењето на податоците и плановите за мрежите, ИТ системите кои се користат за оваа цел, оперативните процедури, описи на активностите за обработка на личните податоци, интеракција со други активности за обработка на личните податоци.
☐	Документирање на тестирањето на информацискиот систем пред неговото имплементирање или по извршените промени, како и на проценката на влијанието на заштитата на личните податоци при користење на нови технологии или нивна промена;
☐	Документирање на факторите кои се користат при автоматско донесување на поединечни одлуки, вклучувајќи и профилирање;
☐	Документирање и регулирање на обврските и одговорностите за заштита на личните податоци при вработување или ангажирање на лицата, како и ангажирањето и контролата на надворешните субјекти (обработувачи) и други трети страни;
☐	Документирање на начинот на обезбедување на согласност, правото на повлекување на согласноста и правото на приговор;

☐	Воспоставување на евиденција за секој пристап до информацискиот систем (логови за пристап и промени);
☐	Документирање на секоја промена (верзија) на софтверот/информацискиот систем;
☐	Документирање на процесите на обработка на личните податоци по пат на протоколи засновани на концептот на евидентирање и евалуација;
☐	Проверка на изворот на податоци на пр. имплементирање на обврската за информирање на субјектите на личните податоци и справување со нарушувањата на безбедноста на личните податоците;
☐	Известување на субјектите на лични податоци во случај на нарушување на безбедноста на личните податоци или во случај на понатамошна обработка за друга цел различна од целта за кој што првично биле собрани;
☐	Видливост и следливост на активностите на организацијата за обезбедување на правата на субјектите на личните податоци;
☐	Инкорпорирање (или гарантирање) на правото на информираност на субјектите на личните податоци во концептот за евидентирање и евалуација;
☐	Обезбедување на информации и пристап на субјектите на личните податоци до нивните лични податоци.

Интервенирање	
Заштитната цел на интервенирањето е да обезбеди ефективно остварување на правата на субјектите на лични податоци и применување на мерки за идентификување и автентикација на субјектите на лични податоци кои сакаат да ги остварат своите права.	
☐	Воведување на мерки за обезбедување на диференцијална согласност, повлекување на согласноста и приговор;
☐	Овозможување на примена на мерки за блокирање на одредени индикатори, известувања, согласности, приговори, право на одговор;
☐	Документирање на начинот на пријавување, реакција и санирање со грешки, начинот на решавање на проблеми и промени на активностите за обработка, како и на техничките и организациските мерки;
☐	Воведување на можност за деактивирање на определени функции за пристап без влијание на работата на информацискиот систем;
☐	Имплементација на стандардизиран интерфејс за пребарување и дијалог со цел субјектите на личните податоци да можат да го поднесат и/или да го спроведат своето барања

☐	Воспоставување на функционален интерфејс за автоматско вчитување на податоците кои ќе можат да ги преземаат субјектите на личните податоци;
☐	Воведување на алатки за идентификација и автентикација на субјектите на лични податоци при остварување на нивните права, земајќи ја предвид расположливата технологија;
☐	Воспоставување единствена точка за контакт со субјектите на лични податоци;
☐	Воведување на алатки што овозможуваат собирање, исправка, блокирање и бришење на сите податоци за субјектите на личните податоци.
☐	Овозможување на субјектите на лични податоци да направат прилагодувања на програмата (софтверот) согласно барањата за заштита на личните податоци;

Заклучок

☐	Техничките и организациските мерки ги намалија ризиците што произлегуваат од обработката на личните податоци до соодветно ниво.
☐	Техничките и организациските мерки НЕ ги намалија ризиците што произлегуваат од обработката на личните податоци до соодветно ниво. Потребни се дополнителни мерки.

Забелешка: Мерките предвидени во овој прашалник во однос на целите на заштита не можат да бидат применливи при секоја обработка на личните податоци, па поради тоа може да се користат други мерки за заштита во зависност од природата, обемот, контекстот и целите на обработката на личните податоци и за нивно внесување, контролорот може да го користи празното поле на крајот на секоја цел на заштита.

8. Следење и преглед

Контролорот освен што мора да ги спроведува мерките за заштита, истите треба и да ги проверува за да се увери дека тие континуирано се применуваат, редовно се тестираат и сè уште се соодветни, а во случај кога настануваат промени во операциите за обработка или други околности кои може да доведат до поинакви резултати од процената на ризик во однос на нивото на влијание или веројатноста за појава на штета.

Контролорот задолжително треба да спроведува периодични безбедносни проверки, со цел да констатира дали мерките за заштита кои ги применува сè уште се соодветни во однос на обезбедување безбедност на обработката на личните податоци според прописите за заштита на личните податоци.

Во случај, мерките за заштита да не обезбедуваат соодветно ниво на безбедност на обработката на личните податоци, тогаш контролорот задолжително предвидува и применува дополнителни мерки за заштита.

Прилог бр.2

Цели на заштита, закани и мерки

Содржина

1. ВОВЕД	
2. ЦЕЛИ НА ЗАШТИТА	
2.1. Минимизирање на личните податоци (МЛП)	
2.2. Достапност (Д)	
2.3. Интегритет (И)	
2.4. Доверливост (Дов)	
2.5. Неповрзливост (Н)	
2.6. Транспарентност (Т)	
2.7. Интервенирање (ИВ)	
3. ЗАКАНИ	
Објаснување на ЗАКАНИТЕ	
4. ЗАКАНИ И МЕРКИ	
4.1. Организација	
4.2. Кадар	
4.3. Свесност и обука за безбедност на информациите	
4.4. Откривање настани што се важни за безбедноста	
4.5. Постапување со безбедносен инцидент	
4.6. Правилно администрирање на информатичката технологија	
4.7. Генерички објект	
4.8. Центар за податоци и серверска просторија	
4.9. Архиви за медиуми за чување податоци	
4.10. Работа на далечина	
4.11. Безбедност на информации при патувања во странство	
4.12. Мрежна архитектура и дизајн	
4.13. Рутери и преклопници (SWITCHES)	
4.13.5 Напредни мерки	
4.14. Заштитен ѕид	
4.15. Работа на безжична локална мрежа (WLAN)	
4.16. Виртуелна приватна мрежа (VPN)	
4.17. Далечинско одржување	
4.18. Управување со идентитет и пристап	
4.19. Криптографија	
4.19.4 Мерки	
4.20. Сигурносна копија	
4.21. Управување со софтверски поправки и промени	
4.22. Заштита од злонамерен софтвер	
4.23. Бришње и уништување податоци и уреди	
4.23.4 Мерки	
4.24. Размена на информации	
4.25. Евиденција на пристап (LOGGING)	
4.26. Сервери за датотеки	
4.27. Општ клиент	
4.28. Клиенти на Windows 10	
4.29. Активен директориум	
4.30. Општи клиенти и сервери за е-пошта	
4.31. Microsoft Exchange и Outlook	
4.32. Виртуелизација	
4.33. Лаптопи	
4.34. Преносливи медиуми	
4.35. Паметни телефони и таблети	
4.36. Управување со мобилни уреди	
4.37. Веб прелистувачи	
4.38. Веб сервери	
4.39. Печатачи, апарати за копирање и уреди сè-во-едно	
5. ТЕРМИНОЛОГИЈА	

1. Вовед

Не постои единствен пристап кој што води до безбедност, особено не во областа на безбедноста на личните податоци. Сите изрази, како што се „цел на заштита“, „закана“ или „мерка“, се приближни и служат за усогласување на обработката на личните податоци во една организација со прописите за заштита на личните податоци. Овие изрази потекнуваат од полето на безбедноста на информациите кои со години се развиваат. Оттука, безбедноста на информациите е насочена кон средствата т.е кон материјалните или нематеријалните вредности на организацијата, а заштитата на личните податоци е фокусирана кон субјектот на личните податоци, односно на какво влијание може да биде истиот изложен поради одредена закана која може негативно да се одрази на неговите права и слободи.

Во овој прилог најпрво се дава преглед на целите на заштита во однос на заштитата на личните податоци, по што следува преглед на законите и нивната класификација во една организација.

2. Цели на заштита

2.1. Минимизирање на личните податоци (МЛП)

Заштитната цел на минимизирање на личните податоци се однесува на основното барање од Законот за заштита на личните податоци за ограничување на обработката на лични податоци само на тоа што е соодветно, релевантно и неопходно за целите на обработката. Барањето за минимизирање не се применува само на количината на лични податоци што се обработуваат, туку и на опфатот на самата обработка, периодот на чување и достапноста на податоците. Поконкретно, треба да се обезбеди дека личните податоци се чуваат во форма која овозможува само идентификација на субјектите на лични податоци сè додека тоа е неопходно за целите на обработката. Минимизирањето на личните податоци започнува при дизајнирањето на информатичката технологија од страна на производителот преку нејзино конфигурирање и приспособување на планираните операции на обработка со примена на техничка и интегрирана заштита на личните податоци, а продолжува преку нејзина употреба при процесите на обработка, како и при одржување на системот којшто се користи.

Најчести мерки за да се постигне минимизирање на личните податоци:

- Намалување на евидентираниите категории на лични податоци;
- Намалување на операциите за обработка во секој процес;
- Намалување на можностите за давање на информации за личните податоци;
- Воспоставување на стандардни поставки за субјектите на лични податоци што ја ограничуваат обработката на нивните лични податоци на она што е неопходно за целта на обработката;

- Воведување на мерки за автоматско блокирање и бришење;
- Маскирање на податоците за прикривање на полињата со личните податоци и воведување на процедури за автоматско блокирање и бришење и мерки за псевдонимизација и анонимизација;
- Редовно ажурирање на воспоставените процедури врз основа на спроведени контроли.

2.2.Достапност (Д)

Заштитната цел на достапноста се однесува на непречен пристап и континуирана расположливост на обработката на личните податоци. За таа цел, овластените лица треба да имаат пристап до личните податоци и при нивната обработка да ги применуваат предвидените методи за таа обработка. Достапноста вклучува конкретна можност за враќање на личните податоци, на пример преку системи за управување со податоци, структурирани бази на податоци и функции за пребарување, како и способност на техничките системи да ги презентираат податоците. Оттука, треба да се преземат мерки за гарантирање на достапноста за да се обезбеди дека личните податоци и пристапот до нив може брзо да се обноват во случај на физички или технички инцидент (можност за враќање на податоците). Притоа, треба да се спроведат мерки за да се гарантира достапноста на личните податоци и на системите и услугите што ги обработуваат, кога се изложени на оптоварување кое реално може да се очекува, како и да се обезбеди дека заштитата на личните податоци не е загрозена во случај на неочекувано големо оптоварување (отпорност). Доколку, во исклучителни случаи, сепак настане нарушување на безбедноста на личните податоци во однос на достапноста, треба да се применат мерки за отстранување и за ублажување на негативните ефекти.

Најчести мерки за да се гарантира достапноста:

- Правење на сигурносни копии, соодветно планирање на состојбите на (во) процесот, конфигурирање, структурирање на податоците, историја на трансакции, според тестиран концепт;
- Заштита од надворешни влијанија (злонамерен софтвер, саботажа, виша сила);
- Документирање на синтаксата на податоците;
- Редундантност на хардвери, софтвери и инфраструктура;
- Спроведување на мерки за навремено повторно воспоставување на достапноста до личните податоци и пристапот во случај на инцидент, како и за правење на сигурносна копија;
- Подготвување на план за итни состојби кој ги предвидува мерките за обновување на активностите за обработка на личните податоци;
- Воведување на мерки за обезбедување на замена на овластените лица кои имаат пристап до личните податоци.

2.3.Интегритет (И)

Заштитната цел на интегритетот од една страна се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции, а од друга страна интегритетот гарантира дека личните податоци кои се обработуваат континуирано се точни, целосни и ажурирани. Отстапувањата од овие барања мора да се исклучат или најмалку барем да може да се откријат преку следење на обработката за да може истите да се детектираат и коригираат (на пример мерки за отстранување и за ублажување на негативните ефекти во случај на нарушување на безбедноста на личните податоци). Ова, исто така се однесува и на основните системи и услуги ако истите се неочекувано преоптоварени. Покрај аспектот за немање грешки, треба да се има предвид и аспектот на недискриминација, особено при автоматско донесување на поединечни одлуки, вклучувајќи и профилирање.

Најчести мерки за заштита на интегритетот:

- Ограничување на привилегиите за внес и промени;
- Користење на алгоритми за криптирање при обработката на личните податоци (контролни суми, електронски печат и потпис);
- Документирање на постапките за идентификација и проверка на пристапот на овластените лица и доделените улоги;
- Бришење и ажурирање на неточни лични податоци;
- Зајакнување на информациските системи преку склучување и минимизирање на секундарни функционалности;
- Воспоставување на процеси за одржување на навременост на податоците;
- Идентификација и автентикација на овластените лица и опремата која се користи;
- Дефинирање на процесите и редовно тестирање за утврдување и документирање на функционалноста, ризиците, безбедносните празнини и несаканите ефекти на процесите;
- Определување на целното однесување на процесите и процедурите и нивно редовно тестирање за да се провери и утврди нивната сегашна состојба;
- Заштита од надворешни влијанија (шпионажа, хакирање).

2.4.Доверливост (Дов)

Заштитната цел на доверливоста треба да обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци. Неовластени лица не се само трети лица надвор од организацијата, туку и вработени кај даватели на услуги за кои не е потребен пристап до личните податоци за да ја извршат услугата или лица во организациски единици кај организацијата што немаат никаква поврзаност со обработката на личните податоци. Доверливоста на личните податоци мора да се обезбеди и кога основните системи и услуги се неочекувано преоптоварени. Доколку, во исклучителни случаи, сепак настане нарушување на безбедноста на личните податоци во однос на доверливоста, треба да се применат мерки за отстранување и за ублажување на негативните ефекти.

Најчести мерки за гарантирање на доверливоста:

- Сегрегација на должности и одговорности на овластените лица според правилото „потребно е да знае“, при што да се има предвид судирот на интереси при извршувањето на нивните работни задачи;
- Воведување мерки за автентикација на овластените лица;
- Спецификација и мониторинг на користењето на авторизирани ресурси, а особено комуникациските канали;
- Дефинирање на условите на просториите и опремата за обработка на лични податоци;
- Воведување мерки за вршење контрола на примената на организациските мерки, интерните процедури и договорните аранжмани со давателите на услуги;
- Користење на алгоритми за криптирање на личните податоци кои што се чуваат или се пренесуваат, како и воспоставување процеси за управување и заштита на криптираните информации;
- Заштита од надворешни влијанија (шпионажа, хакирање).

2.5.Неповрзливост (Н)

Заштитната цел на неповрзувањето е да се обезбеди дека личните податоци нема да се обработуваат за друга цел различна од целта за која првично биле собрани при што натамошната нивна обработка би можела да биде дозволена само во строго дефинирани околности. Неповрзливоста треба да се обезбеди со технички и организациски мерки. Покрај мерките за псевдонимизација, соодветни се и други мерки што овозможуваат понатамошна обработка одделно од првичната обработка, како на организациската страна, така и на страната на системот. Базата на податоци може да се приспособи, на пример, со системи за авторизација и намалување до степенот што е неопходен за новата цел.

Најчести мерки за гарантирање на неповрзливоста:

- Воведување на мерки за ограничување на пристапот за обработка, користење и пренос на податоци од страна на овластените лица;
- Програмски пропуст или деактивирање на интерфејси во методите и компонентите при обработка на личните податоци;
- Воведување на мерки за забрана на заден влез (backdoors), како и воспоставување механизми за обезбедување на контрола на квалитетот при развивање софтверски решенија за обработка на личните податоци;

- Воспоставување на постапки за начинот на доделување на пристап според организациската поставеност и воведување на права на пристап според извршувањето на работните задачи;
- Употреба на псевдоними за одредена цел, потврда на идентитетот преку анонимизација, односно примена на протоколи за потврда на идентитетот на корисниците без да се загрози нивната приватност и обработување на псевдонимизирани или анонимизирани податоци;
- Регулiranje и документирање на процесите за промена на целите за обработка.

2.6.Транспарентност (Т)

Заштитната цел на транспарентност е да обезбеди информации за обработката на личните податоци, односно можност да се идентификува на различно ниво, кои податоци се собираат и се обработуваат, кога и за кои цели на обработка, кои системи и процеси се користат за да се утврди дали податоците се обработуваат според предвидената цел, како и кој има одговорност во различните фази за нивната обработка. Транспарентноста е неопходна за следење и контрола на податоците, процесите и системите од нивното создавање до нивното бришење и претставува предуслов за законита обработка на личните податоци за која, каде што е потребно, субјектите на личните податоци можат да дадат конкретна, информирана и недвосмислена согласност (управување со согласност). Транспарентноста на целиот процес на обработката на личните податоци овозможува субјектите на личните податоци и Агенцијата за заштита на личните податоци да можат да идентификуваат одредени недостатоци и доколку е потребно да побараат и соодветни промени во обработката на личните податоци.

Најчести мерки за гарантирање на транспарентноста:

- Документирање на активностите за обработка на личните податоци според одредбите на членот 34 од Законот за заштита на личните податоци;
- Документирање на компонентите на активностите за обработка на личните податоци, особено деловните процеси, базите на податоци, движењето на податоците и плановите за мрежите, ИТ системите кои се користат за оваа цел, оперативните процедури, описи на активностите за обработка на личните податоци, интеракција со други активности за обработка на личните податоци.
- Документирање на тестирањето на информацискиот систем пред неговото имплементирање или по извршените промени, како и на проценката на влијанието на заштитата на личните податоци при користење на нови технологии или нивна промена;
- Документирање на факторите кои се користат при автоматско донесување на поединечни одлуки, вклучувајќи и профилирање;
- Документирање и регулирање на обврските и одговорностите за заштита на личните податоци при вработување или ангажирање на лицата, како и ангажирањето и контролата на надворешните субјекти (даватели на услуги) и други трети страни;

- Документирање на начинот на обезбедување на согласност, правото на повлекување на согласноста и правото на приговор;
- Воспоставување на евиденција за секој пристап до информацискиот систем (логови за пристап и промени);
- Документирање на секоја промена (верзија) на софтверот/информацискиот систем;
- Документирање на процесите на обработка на личните податоци по пат на протоколи засновани на концептот на евидентирање и евалуација;
- Проверка на изворот на податоци на пр. имплементирање на обврската за информирање на субјектите на личните податоци и справување со нарушувањата на безбедноста на личните податоците;
- Известување на субјектите на лични податоци во случај на нарушување на безбедноста на личните податоци или во случај на понатамошна обработка за друга цел различна од целта за којашто првично биле собрани;
- Видливост и следливост на активностите на организацијата за обезбедување на правата на субјектите на личните податоци;
- Инкорпорирање (или гарантирање) на правото на информираност на субјектите на личните податоци во концептот за евидентирање и евалуација;
- Обезбедување на информации и пристап на субјектите на личните податоци до нивните лични податоци.

2.7.Интервенирање (ИВ)

Заштитната цел на интервенирањето е да обезбеди ефективно остварување на правата на субјектите на лични податоци и применување на мерки за идентификување и автентикација на субјектите на лични податоци кои сакаат да ги остварат своите права. За да се остварат правата на субјектите на личните податоци како и да може да се отстранат и ублажат негативните ефекти од нарушувањето на безбедноста на личните податоци, организацијата треба постојано да биде во можност да презема активности во однос на обработката на личните податоци и тоа од моментот на нивното собирање се до нивното бришење. Кога обработката на личните податоци се врши врз основа на согласност на субјектот на личните податоци, треба да се преземат мерки за да се обезбеди дека личните податоци се обработуваат само кога субјектот на личните податоци дал конкретна, информирана и недвосмислена согласност за таквата обработка и притоа истата не е повлечена (управување со согласност). При користење на информатичката технологија од страна на субјектите на личните податоци (на пример, апликации на паметниот телефон), а за која се предвидени различни поставки за заштита на личните податоци, организацијата треба да дефинира и определи покрај стандардните поставки за обезбедување на интегрирана заштита на личните податоци и дополнителни поставки кои ќе им овозможат на субјектите на личните податоци да направат свои прилагодувања според целите и операциите за обработка (стандардни поставки за обезбедување интегрирана заштита на личните податоци).

Најчести мерки за гарантирање на интервенирањето:

- Воведување на мерки за обезбедување на диференцирана согласност, повлекување на согласноста и приговор;
- Овозможување на примена на мерки за блокирање на одредени индикатори, известувања, согласности, приговори, право на одговор;
- Документирање на начинот на пријавување, реакција и санирање со грешки, начинот на решавање на проблеми и промени на активностите за обработка, како и на техничките и организациските мерки;
- Воведување на можност за деактивирање на определени функции за пристап без влијание на работата на информацискиот систем;
- Имплементација на стандардизиран интерфејс за пребарување и дијалог со цел субјектите на личните податоци да можат да го поднесат и/или да го спроведат своето барања;
- Воспоставување на функционален интерфејс за автоматско вчитување на податоците кои ќе можат да ги преземаат субјектите на личните податоци;
- Воведување на алатки за идентификација и автентикација на субјектите на лични податоци при остварување на нивните права, земајќи ја предвид расположливата технологија;
- Воспоставување единствена точка за контакт со субјектите на лични податоци;
- Воведување на алатки што овозможуваат собирање, исправка, блокирање и бришење на сите податоци за субјектот на личните податоци;
- Овозможување на субјектите на лични податоци да направат прилагодувања на програмата (софтверот) согласно барањата за заштита на личните податоци.

3.Закани

Табеларен преглед на закани

Број	Закана	Цел на заштита
3_0.1	Пожар	Д
3_0.2	Неповолни услови во околината	И, Д
3_0.3	Вода	И, Д
3_0.4	Акумулирање нечистотии, прашина, корозија	И, Д
3_0.5	Природни катастрофи	Д
3_0.6	Катастрофи во животната средина	Д
3_0.7	Поголеми настани во околината	Дов, И, Д
3_0.8	Прекин или неисправност на напојувањето	И, Д
3_0.9	Дефект или неисправност на комуникациските мрежи	И, Д
3_0.10	Дефект или неисправност на мрежите за снабдување	Д
3_0.11	Дефект или неисправност на давателите на услуги	Дов, И, Д
3_0.12	Електромагнетни пречки	И, Д
3_0.13	Пресретнување компромитирачко зрачење	Дов
3_0.14	Шпионажа	Дов

3_0.15	Прислушување	Дов
3_0.16	Кражба на уреди, медиуми за чување податоци и документи	Дов, Д
3_0.17	Губење уреди, медиуми за чување податоци и документи	Дов, Д
3_0.18	Лошо планирање или недостаток на приспособување	Дов, И, Д
3_0.19	Откривање на информации што треба да бидат заштитени	Дов
3_0.20	Информации од несигурни извори	Дов, И, Д
3_0.21	Манипулација со хардвер или софтвер	Дов, И, Д
3_0.22	Манипулација со информации	И
3_0.23	Неовластено влегување во системи за информатичка технологија	Дов, И
3_0.24	Уништување на уреди или медиуми за чување податоци	Д
3_0.25	Дефект на уреди или на системи	Д
3_0.26	Неисправност на уреди или на системи	Дов, И, Д
3_0.27	Недостаток на ресурси	Д
3_0.28	Софтверски недостатоци или грешки	Дов, И, Д
3_0.29	Повреда на закони или на договори	Дов, И, Д
3_0.30	Неовластено користење или администрирање уреди и системи	Дов, И, Д
3_0.31	Неправилно користење или администрирање уреди и системи	Дов, И, Д
3_0.32	Злоупотреба на овластувања	Дов, И, Д
3_0.33	Недостиг на кадар	Д
3_0.34	Напад	Дов, И, Д
3_0.35	Принуда, изнуда или корупција	Дов, И, Д
3_0.36	Кражба на идентитет	Дов, И, Д
3_0.37	Одредување на дејствија	Дов, И
3_0.38	Злоупотреба на лични податоци	Дов
3_0.39	Злонамерен софтвер	Дов, И, Д
3_0.40	Одбивање на услуга	Д
3_0.41	Саботажа	Д
3_0.42	Социјален инженеринг	Дов, И
3_0.43	Вметнување пораки	Дов, И
3_0.44	Неовластен влез во простории	Дов, И, Д
3_0.45	Губење податоци	Д
3_0.46	Губење на интегритетот на информациите што треба да се заштитат	И
3_0.47	Штетни несакани ефекти	Дов, И, Д

Објаснување на законите

Пожар

З_0.1	Пожар	Д
Објаснување	Пожарите може да предизвикаат сериозни оштетувања на луѓето, на објектите и на нивната опрема. Покрај директната штета предизвикана од пожар, може да се утврди последователна штета чие штетно влијание може да достигне катастрофални размери, особено кај информатичката технологија. На пример, оштетувањето со вода за гаснење, не се случува само на местото на пожарот. Може да се случи и во други делови од објектот. При согорување на пластика, се создаваат гасови на хлор, кои заедно со влажноста во воздухот и со водата за гаснење формираат хлороводородна киселина. Доколку испарувањата на хлороводородната киселина се распространат низ системот за климатизација, на овој начин може да се предизвика штета на сензитивната електронска опрема што се наоѓа во дел од објектот далеку од местото на пожарот. Но, притоа „нормалниот“ чад од оган може да има штетно влијание и врз опремата за информатичка технологија. Пожар се предизвикува не само поради несовесно ракување со оган (на пример, оган на отворено без надзор, работа за заварување и лемење), туку и поради неправилна употреба на електрична опрема (на пример, кафемат без надзор, преоптоварување на повеќе приклучоци). Техничките дефекти на електричната опрема исто така може да доведат до пожар. Ширењето на пожарот може да се олесни, меѓу другото, со следното: - затворање на вратите за противпожарна заштита со клинови, - несоодветно складирање запаливи материјали (на пример, отпадна хартија), - непочитување на соодветните стандарди и прописи од областа за заштита од пожари, - недостаток на опрема за откривање пожар (на пример, детектори за чад), - исчезнати или нефункционални рачни противпожарни апарати или уреди за автоматско гаснење (на пример, системи за гаснење гас), - несоодветна превентивна заштита од пожари (на пример, недостаток на противпожарни бариери на кабелските траси или употреба на несоодветни изолациски материјали за топлинска и за звучна изолација).	
Пример(и)	- Голем центар за податоци претрпел катастрофална штета од пожар што довело до целосен прекин на електричната енергија. - Многу често малите електрични уреди, какви што се апарати за кафе или столни ламби, се неправилно инсталирани или поставени и како последица на тоа предизвикуваат пожари.	

Неповолни услови во околината

З_0.2	Неповолни услови во околината	И, Д
Објаснување	Неповолните климатски услови какви што се топлина, мраз или високо ниво на влажност може да доведат до оштетување од различен вид, на пример, дефекти во техничките компоненти или оштетување на медиумот за чување на податоците. Честите флукутации на климатските услови го интензивираат ова влијание. И неповолните климатски услови може да предизвикаат неспособност за работа на некое лице или дури и повреда или смрт. Секој човек и секој технички уред имаат опсег на температура во чии рамки е загарантирана неговата нормална работа или правилна функција. Доколку температурата на околината ги надмине границите над или под овој опсег, може да дојде до прекин на работата, оперативни неисправности или дефекти на опремата. Прозорците на серверските простории честопати се отвораат без дозвола заради вентилација. Во преодниот период (пролет, есен) тоа може да доведе до надминување на дозволената влажност поради силно ладење доколку има големи промени на температурата.	
Пример(и)	- При летни температури и недоволно ладење, може да настанат дефекти на опремата за информатичка технологија како резултат на температурата. - Премногу прашина во системите за информатичка технологија може да доведе до прегревање (акумулирање топлина). - Прекумерните температури може да ги демагнетизираат магнетните носачи на податоци.	

Вода

З_0.3	Вода	И, Д
Објаснување	Водата може да влијае врз интегритетот и достапноста на информациите што се чуваат на аналогни и на дигитални носачи на податоци. И информациите во работната меморија на системите за информатичка технологија се изложени на ризик. Примери за причини за неконтролирано влегување вода во објектите или во просториите се следните: - дефекти во водоснабдувањето или во отстранувањето отпадна вода, - дефекти во системот за греење, - дефекти во системите за климатизација со водоснабдувањето, - дефекти во системите со прскалки, - вода за гаснење при гаснење пожар и - саботажа со вода, на пример, со отворање славини и затнување на одводите. Без оглед на начинот на кој водата навлегува во објектите или во просториите, постои ризик од оштетување или прекин на работата на снабдувањето со комунални услуги или компонентите на информатичката технологија (краток спој, механичко оштетување, рѓа итн.). Особено доколку централните капацитети за снабдување на објектот (главни разводни табли за електрична енергија, телефон, податоци) се наоѓаат во подрумски простории без автоматско одводнување, водата што навлегува може да предизвика значителна штета.	

	И мразот може да предизвика проблеми. На пример, цевките во деловите што се склони да замрзнуваат може да протечат доколку водата остане во нив подолго време и кога се замрзнати подолг период. Со текот на времето мразот ја пробива и постојната топлинска изолација.
Пример(и)	- Во серверската просторија под таванот поминувала водоводна цевка, која била покриена со елементи од гипскартон. Кога почнало протекување од поврзувањето на водоводната цевка, тоа не било откриено навреме. Водата што истекувала првично се собирала на најниската точка на заштитната сидна облога (топлинска изолација) пред да се разлее и да предизвика краток спој во продолжениот кабел поставен долу. Поради тоа, морало целосно да се исклучат и водата и напојувањето со електрична енергија на погодениот дел од објектот додека да се направат завршните поправки.

Акумулирање нечистотии, прашина, корозија

З 0.4	Акумулирање нечистотии, прашина, корозија	И, Д
Објаснување	Покрај електрониката, многу уреди за информатичка технологија содржат и механички оперативни компоненти, како во случајот со хард-дискови и преносливи дискови, ДВД-читачи, печатачи, скенери итн., но и вентилатори на процесори и напојувања. Со зголемените барања за квалитет и брзина, овие уреди мора да работат со уште поголема прецизност. Дури и помала контаминација може да предизвика дефект на уредот. Прашината и контаминацијата може да бидат предизвикани, во поголема мера, од следниве активности, на пример: - работа на сидови, подигнати подови или други делови од објектот, - додавање нова технологија на хардвер или - активности за отпакување уреди (на пример, вртење на стиропор). Постојните безбедносни кола во опремата обично предизвикуваат нејзино навремено исклучување. Иако со ова се одржува ниско ниво на директното оштетување на опремата, трошоците за поправка и времето на застој, сепак последицата е достапност на погодената опрема. И опремата и инфраструктурата може да бидат изложени на корозија. Ова може да има негативно влијание не само врз информатичките технологии, туку и врз безбедноста на објектот. Корозијата може индиректно да создаде и други опасности. На пример, водата може да се разлее од кородирани делови. Општо, контаминацијата, прашината или корозијата може да доведат до дефекти или до оштетување на компонентите на информатичката технологија и опремата за снабдување. Како резултат на тоа, може да се наруши правилната обработка на информациите.	
Пример(и)	- Кога во просторијата за медиуми бил поставен сервер, заедно со апаратот за копирање и факс апаратот, вентилаторот на процесорот и вентилаторот за напојување се закочиле еден по друг поради големото оптоварување од прашина во просторијата. Дефектот на вентилаторот на процесорот предизвикал одредени откажувања на серверот. Дефектот на вентилаторот за напојување на крајот предизвикал прегревање на напојувањето, што резултирало со краток спој, кој на крајот предизвикал целосен дефект на серверот. - За да закачат сиден панел во една канцеларија, вработените издупчиле дупки во сидот. Затоа, вработениот накратко ја напуштил својата канцеларија. Откако се вратил на своето работно место, увидел дека неговиот персонален компјутер повеќе не работи. Причината за ова била прашината од дупчењето, која навлегла во напојувањето на компјутерот преку отворите за вентилација.	

Природни катастрофи

3_0.5	Природни катастрофи	Д
Објаснување	Природните катастрофи се природни промени што имаат разорни последици врз луѓето и врз инфраструктурата. Причините за природна катастрофа можат да бидат сеизмички, климатски или вулкански појави, какви што се земјотреси, поплави, лизгање на земјиштето, цунами, лавини и вулкански ерупции. Примери за екстремни метеоролошки феномени вклучуваат тешки временски услови, урагани или циклони. Во зависност од локацијата на организацијата, нејзината изложеност на ризици од различни видови природни катастрофи е различна. Примери: - За центрите за податоци што се наоѓаат во подрачја што се подложни на поплави, често постои особен ризик од неконтролирано навлегување вода во објектот (поплава или растење на нивото на водата). - Зачестеноста на земјотресите, а со тоа и придружниот ризик, значително зависат од географската локација. Без оглед на видот на природната катастрофа, дури и во областите што не се директно засегнати, постои ризик од оштетување или прекин на комуналните услуги, врските за комуникација или компонентите за информатичка технологија. Конкретно, дефектот на капацитетите за снабдување на централниот објект (главни разводни табли за електрична енергија, телефон, податоци) може да резултира со многу високи загуби. На оперативниот и на сервисниот кадар може да му биде забранет пристапот до инфраструктурата поради големи ограничени области.	
Пример(и)	- Многу комерцијални операции, што ги вклучува и големите организации, не се справуваат соодветно со опасностите од поплави. Една организација, на пример, веќе неколкупати била „изненадена“ од штетите од поплавите на нејзиниот центар за податоци. Центарот за податоци буквално испливал по вторпат во рок од 14 месеци. Настаната штета изнесувала неколку стотици илјади евра и не е покриена со никакво осигурување. - Системот за информатичка технологија е поставен на место чија географска локација е позната по вулканска активност (наизменична појава во која фазите на емисија се менуваат со понекогаш долги периоди на неактивност).	

Катастрофи во животната средина

3_0.6	Катастрофи во животната средина	Д
Објаснување	Некои организации може да претрпат штета ако се случи сериозна несреќа во близина, на пример, пожар, експлозија, ослободување токсични материи или протекување на опасно зрачење. Опасноста не произлегува само од самиот настан, туку и од активностите што често се јавуваат како последица на настанот, какви што се затворања (ограничувања на движењето) или спасувачки операции. Имотот на организацијата може да биде изложен на различни опасности од околината, вклучително сообраќајот (пат, железница, воздух, вода), соседните деловни или станбени области. Превентивните мерки или мерките за спасување може директно да влијаат врз имотот. Воедно, како резултат на ваквите мерки, вработените може да бидат спречени да стигнат до своите работни места или, пак, ќе мора да се евакуираат. Сепак, сложеноста на градежните услуги и капацитети за информатичка технологија исто така може да доведе до индиректни проблеми.	
Пример(и)	- Пожар во хемиска постројка во непосредна близина на центар за податоци (на воздушно растојание од приближно 1.000 метри) создал моќен облак од чад. Центарот за податоци имал систем за климатизација и вентилација што немал опција за надворешно следење на воздухот. Само со вниманието на вработениот (несреќата се случила во работно време), кој го следел формирањето и ширењето, можело навреме рачно да се исклучи доводот на надворешен воздух.	

Поголеми настани во околината

3_0.7	Поголеми настани во околината	Дов, И, Д
Објаснување	Поголемите настани од секаков вид може да доведат до пречки за правилното функционирање на организацијата. Таквите настани вклучуваат улични фестивали, концерти, спортски настани, работни спорови или демонстрации. Немирите поврзани со такви настани може да доведат до дополнителни влијанија, како што е заплашување на вработените до степен на насилство врз нив или врз објектот.	
Пример(и)	- За време на жешките летни месеци, се одржала демонстрација во близина на центар за податоци. Ситуацијата ескалирала и дошло до насилство. Во една споредна улица, прозорецот од областа на центарот за податоци сè уште бил отворен, низ него влегол демонстрант и ја искористил можноста да украде хардвер што содржи важни податоци. - При изградбата на голем саем, случајно бил пресечен далновод. Ова довело до прекин во центарот за податоци снабдуван од овој вод, кој сепак бил пресретнат и попречен од достапниот заштитен (резервен) систем за напојување.	

Прекин или неисправност на напојувањето

З 0.8	Прекин или неисправност на напојувањето	И, Д
Објаснување	И покрај високото ниво на безбедност на снабдувањето, често се случуваат прекини во снабдувањето со електрична енергија од операторите на дистрибутивната мрежа или од компаниите за снабдување со енергија. Поголемиот дел од овие прекини, со времиња помали од една секунда, се толку кратки што луѓето не ги забележуваат, а кои можат да го нарушат работењето на информатичките технологии. Меѓутоа, покрај пречки во мрежата за напојување, исклучувањата при ненајавена работа или оштетување кабел за време на градежни работи, исто така може да предизвикаат дефект на напојувањето. Од напојувањето не зависат само очигледните, директни потрошувачи на енергија (персонални компјутери, осветлување, итн.). Многу инфраструктурни објекти денес зависат од електрична енергија, на пример, лифтови, технологија за климатизација, системи за аларм за опасност, безбедносни врати, системи за автоматско заклучување на вратите и системи со прскалки. Во случај на долги прекини на електричната енергија, дефектот на инфраструктурните објекти може да значи дека не може да се вршат никакви активности во погодените простории. Покрај прекините, други дефекти на напојувањето исто така може да влијаат врз работењето. Пренапонот, на пример, може да доведе до дефекти или дури и оштетување на електричната опрема. Воедно, треба да се забележи дека дефектите или прекините на напојувањето во соседството исто така може да влијаат врз деловните процеси на организацијата, на пример, ако пристапните патишта се блокирани.	
Пример(и)	- Поради дефект во уредот за непрекинато напојување (UPS) на центарот за податоци, тој не се вратил во нормален режим на работа по краток прекин на напојувањето. Откако биле испразнети батериите (по околу 40 минути), сите персонални компјутери во погодената серверска соба откажале. - По обилни снежни врнежи, многу населби биле без струја со денови бидејќи многу високонапонски далноводи паднале поради оптоварувањето од снег и мраз, поради што биле потребни неколку денови да се врати напојувањето.	

Дефект или неисправност на комуникациските мрежи

З 0.9	Дефект или неисправност на комуникациските мрежи	И, Д
Објаснување	За многу деловни процеси денес се потребни непроменети комуникациски врски барем дел од времето, независно дали тоа е преку телефон, факс, е-пошта или други услуги преку локална или регионална мрежа. Ако дојде до дефект кај една или кај повеќе од овие комуникациски врски во текот на подолг временски период, тоа може да доведе, на пример, до ситуација каде што: - деловните процеси повеќе не можат да продолжат бидејќи не може да се вратат потребните информации, - клиентите повеќе не можат да стигнат до организацијата за прашања, - нарачките не можат да се доставуваат или да се комплетираат. Ако апликациите каде што времето е пресудно се користат на системи за информатичка технологија поврзани преку регионални мрежи, потенцијалната штета и последователната штета предизвикана од дефект на мрежата е соодветно висока ако нема алтернативни опции (на пример, поврзување со втора комуникациска мрежа). Слични проблеми може да се јават ако бараните комуникациски мрежи се прекинати, но не откажат во целост. Комуникациските врски може, на пример, да имаат зголемена стапка на грешки или други недостатоци на квалитетот. Неправилните работни параметри исто така може да предизвикаат нарушувања.	
Пример(и)	- Интернетот стана неопходен комуникациски медиум за многу организации, вклучително и за наоѓање важни информации, за надворешно презентирање и за комуникација со клиенти и со партнери. Организациите што се специјализирани за услуги засновани на интернет секако се особено зависни од функционална интернет врска. - Во текот на мрежната конвергенција, говорните и податочните услуги често се транспортираат преку истите технички компоненти (на пример, VoIP). Сепак, ова го зголемува ризикот за истовремено откажување на говорните услуги и на податочните услуги во случај на прекин во комуникациската технологија.	

Дефект или неисправност на мрежите за снабдување

З 0.10	Дефект или неисправност на мрежите за снабдување	Д
Објаснување	Постојат голем број мрежи во еден објект, кои служат за основно снабдување и располагање и затоа претставуваат основа за сите процеси на организацијата, вклучително и информатичките технологии. Примери за такви мрежи за снабдување се следните: - електрична енергија, - телефон, - ладење, - греење или вентилација, - вода и отпадни води, - водоснабдување за гаснење пожари,	

	- гас, - алармни и контролни системи (на пример, за кражба, пожар, системи за управување со згради) и - системи за домофон. Дефектот или прекилот на мрежата за снабдување, меѓу другото, може да значи дека луѓето повеќе не можат да работат во објектот или дека операциите на информатичките технологии, а со тоа и обработката на информациите, се нарушени. Мрежите се меѓусебно зависни во различна мера, така што прекините во работењето во некоја мрежа може да влијаат врз другите мрежи.
Пример(и)	- Дефект на греењето или на вентилацијата може да доведе до тоа сите вработени да мора да ги напуштат погодените објекти. Во одредени околности, ова може да резултира со големи штети. - Дефектот на напојувањето не само што директно влијае врз информатичките технологии, туку влијае и врз сите други мрежи што се опремени со електрична технологија за контрола и регулација. Дури и одводните линии може да имаат електрични пумпи за подигнување. - Дефектот на водоснабдувањето може да влијае врз функцијата на системите за климатизација.

Дефект или неисправност на давателите на услуги

З_0.11	Дефект или неисправност на давателите на услуги Дов, И, Д
Објаснување	Ретко која организација денес работи без даватели на услуги какви што се снабдувачи или надворешни добавувачи (надворешни даватели на услуги). Кога организациските единици се зависни од давателите на услуги, дефектите на надворешните услуги може да го нарушат извршувањето на задачата. Делумниот или целосниот дефект на надворешниот давател на услуги или на снабдувачот може да има значително влијание врз деловниот континуитет, особено во суштинските деловни процеси. Постојат различни причини за таквите дефекти, на пример, неликвидност, еднострано раскинување договор од страна на давателот на услугата или снабдувачот, оперативни проблеми поради природни сили или отсуства на кадарот. Може да настанат проблеми и ако услугите што ги обезбедува давателот на услугата не ги задоволуваат барањата за квалитет на организацијата. Треба да се истакне и дека давателите на услуги често користат подизведувачи за да ги обезбедат своите услуги на организацијата. Нарушувањата, дефектите во однос на квалитетот и дефектите од страна на подизведувачите на тој начин индиректно може да доведат до нарушувања за организацијата. Процесите кај организацијата исто така може да бидат нарушени од дефекти на системите за информатичка технологија кај давателот на услуги или на комуникациските врски со давателот на услуги. Секое неопходно пребарување на податоци преку надворешно обезбедени процеси може да биде сериозно попречено, на пример затоа што надворешно обезбедените процеси не се доволно документирани или затоа што претходниот давател на услуги не поддржува пребарување.

Пример(и)	- Една организација ги инсталирала своите сервери во центар за податоци управуван од надворешен давател на услуги. По пожарот во овој центар за податоци, организацијата повеќе не можела да функционира и претрпела значителни финансиски загуби. - Навременото производство на една организација било зависно од снабдувањето со оперативни ресурси од надворешни даватели на услуги. Откако камион се расипал поради дефект кај давателот на услугата, испораката на итно потребните делови драстично доцнела. Како резултат на тоа, одреден број клиенти не можеле да се снабдат навреме. - Организацијата ги извршувала сите транспорти на готовина со давател на услуги за транспорт на готовина. Давателот на услуги неочекувано поднел барање за стечај. Договорането и планирањето на маршрутата со нов давател на услуги за транспорт на готовина траело неколку денови. Како резултат на тоа, имало значителни проблеми и временски доцнења во снабдувањето и располагањето со готовина во организацијата.
-----------	---

Електромагнетни пречки

3_0.12	Електромагнетни пречки	И, Д
Објаснување	Денес, информатичката технологија во голем дел се состои од електронски компоненти. Иако сè повеќе се користи технологија за оптички пренос, на пример, компјутерите, елементите на мрежниот интерфејс и системите за чување на податоци главно содржат голем број електронски компоненти. Електромагнетните пречки што дејствуваат на таквите компоненти може да ја нарушат функцијата на електронските уреди или дури и да ги оштетат. Како резултат на тоа, меѓу другото, може да дојде до појава на дефекти, пречки, неточни резултати од обработката или комуникациски грешки. Безжичната комуникација може да биде нарушена и од зрачењето на електромагнетните пречки. Во одредени околности, силното нарушување на користените фреквенциски опсези е доволно за ова. Понатаму, информациите што се зачувани на одредени видови носачи на податоци може да се избришат или да се фалсификуваат со зрачење на електромагнетни пречки. Ова особено се однесува на носачите на податоци што можат да се магнетизираат (хард-дискови, магнетни ленти итн.) и на полупроводнички мемории. Можно е и оштетување на таквите носачи на податоци од зрачењето на електромагнетните пречки.	
Пример(и)	Постојат многу различни извори на електромагнетни полиња или на зрачење, на пример радиомрежи какви што се WLAN, Bluetooth, GSM, UMTS итн., постојани магнети и космичко зрачење. Покрај тоа, секој електричен уред емитува електромагнетни бранови со поголема или со помала јачина, кои меѓу другото може да се шират низ воздухот и по металните проводници (на пример, кабли, канали за климатизација, цевки за греење итн.).	

Пресретнување компромитирачко зрачење

З 0.13	Пресретнување компромитирачко зрачење	Дов
Објаснување	Електричните уреди испуштаат електромагнетни бранови. Во случај на уреди што обработуваат информации (на пример, компјутери, монитори, елементи на мрежен интерфејс, печатачи), ова зрачење може да ги носи и информациите што моментално се обработуваат. Таквото зрачење што носи информации се нарекува зрачење на изложеност или компромитирачко зрачење. На пример, напаѓачот што е во куќата на соседот или во возило паркирано во близина, може да се обиде да го прими ова зрачење и да го искористи за реконструкција на обработените информации. Со тоа се доведува во прашање доверливоста на информациите. Една можна цел на таков напад е индустриска шпионажа. Ограничувањата во прописите од областа за електромагнетна компатибилност на опремата најчесто не се доволни за да се спречи пресретнувањето на изложеното зрачење. Доколку овој ризик не може да се прифати, начелно мора да се преземат дополнителни заштитни мерки. Воедно, треба да се забележи дека во одредени случаи, изложувањето на зрачење може да биде предизвикано или засилено со надворешна манипулација со уредите. На пример, ако уредот е озрачен со електромагнетни бранови, рефлектираните бранови може да носат доверливи информации.	
Пример(и)	Изложувањето на зрачењето не е ограничено на електромагнетни бранови. Во одредени околности, корисни информации може да се добијат и од звучни бранови, на пример од печатачи или од тастатури.	

Шпионажа

З 0.14	Шпионажа	Дов
Објаснување	Шпионажата се однесува на напади чија цел е прибирање, евалуација и обработка на информации за организации, луѓе, производи или други целни објекти. Потоа обработените информации може да се користат, на пример, за да се дадат на друга организација одредени конкурентни предности, да се уценуваат луѓе или да се копира производ. Покрај разните технички сложени напади, често има многу поедноставни методи за добивање вредни информации, на пример со комбинирање информации од неколку јавно достапни извори што може да изгледаат безопасно поединечно, но можат да бидат компромитирачки во друг контекст. Бидејќи доверливите податоци честопати не се соодветно заштитени, тие често може да се шпионираат со визуелни средства, аудио средства или со електронски средства.	
Пример(и)	- Многу системи за информатичка технологија се заштитени од неовластено користење со механизми за идентификација и автентикација, на пример, во форма на проверки на корисничка идентификација и лозинка. Меѓутоа, доколку лозинката е испратена во нешифрирана форма преку линијата, можеби напаѓачот ќе може да ја прочита. - За подигање пари од банкомат, мора да се внесе точниот PIN код за користената електронска картичка или кредитна картичка. За жал, визуелната заштита на овие уреди честопати е недоволна, така што напаѓачот лесно може да погледне преку рамото на клиентот при внесување на PIN кодот. Ако напаѓачот потоа ја украде картичката, може да ја искористи за да повлече средства од сметката.	

	- За да стекне права за пристап до компјутер или на друг начин да манипулира со него, напаѓачот може да му прати на корисникот „тројански коњ“ прикачен на е-пошта како наводна корисна програма. Покрај непосредното оштетување, „тројанските коњи“ може да се користат за шпионирање голем број различни информации, не само за индивидуалниот компјутер, туку и за локалната мрежа. Многу „тројански коњи“ имаат конкретна цел да шпионираат лозинки или други податоци за пристап. - Во многу канцеларии нема добра акустична заштита меѓу работните станици. Како резултат на тоа, колегите и посетителите можеби ќе можат да слушаат разговори и да дознаваат информации што не се наменети за нив или дури се и доверливи.
--	--

Прислушување

3_0.15	Прислушување	Дов
Објаснување	Прислушувањето се однесува на насочени напади врз комуникациски врски, разговори, извори на бучава од секаков вид или системи за информатичка технологија за прибирање информации. Ова започнува со незабележано, тајно прислушување разговор, па сè до добро осмислени сложени напади за пресретнување сигнали испратени преку радио или линии, на пример, со помош на антени или сензори. Не само поради малиот ризик за откривање, прислушувањето линии или радиоврски е закана за безбедноста на информациите што не треба да се занемари. Начелно, нема кабли што се отпорни на прислушување. Единствената разлика помеѓу каблите е напорот што е потребен за да се прислушуваат. Дали линијата навистина се прислушува, може да се утврди само со голем метролошки напор. Незаштитениот пренос на податоци за автентикација има особено суштинско значење во случај на протоколи со обичен текст какви што се HTTP, FTP или Telnet, бидејќи јасната структура на податоците го олеснува автоматското анализирање. Одлуката да се прислушуваат информации некаде, во суштина е одредена од прашањето дали информациите вредат за техничкиот или за финансискиот напор и ризикот од откривање. Одговорот на ова прашање многу зависи од индивидуалните способности и интереси на напаѓачот.	
Пример(и)	- Во случај на телефонски повици, прислушувањето не е единственото што може да биде од интерес за напаѓачот. Информациите што се пренесуваат за време на сигнализацијата исто така може да бидат злоупотребени од напаѓачот, на пример, ако неправилно поставување во терминалниот уред предизвика пренос на лозинката во јасен текст за време на најавата. - Во случај на незаштитен или недоволно заштитен радиопренос (на пример, ако безжичната локална мрежа – WLAN е обезбедена само со алгоритам за безбедносна комуникација кај безжичните мрежи – WEP), напаѓачот може лесно да ја прислушува целата комуникација. - Е-поштата може да се чита додека патува низ мрежата доколку не е криптирана. Затоа, некриптираната е-пошта не треба да се споредува со класични писма, туку со честитки.	

Кражба на уреди, медиуми за чување податоци и документи

3_0.16	Кражба на уреди, медиуми за чување податоци и документи Дов, Д
Објаснување	Како резултат на кражбата на носачи на податоци, системи за информатичка технологија, додатоци, софтвер или податоци од една страна се создаваат трошоци за замена, како и за враќање на работната состојба, а од друга страна се јавуваат загуби поради недостапност. Доколку се откријат доверливи информации како резултат на кражбата, тоа може да доведе до дополнителна штета. Покрај серверите и другите скапи системи за информатичка технологија, често се крадат и мобилни системи за информатичка технологија, кои се незабележливи и лесни за пренос. Сепак, има и случаи кога носачи на податоци, какви што се документи или USB медиуми, се украдени со умисла, со цел да се добијат доверливите информации што се зачувани на нив.
Пример(и)	- Исчезнал лаптоп од организацијата. Во официјално соопштение, не била исклучена можноста уредот да содржи доверливи информации. Ниту, пак, било познато дали уредот е криптографски или на друг начин заштитен од неовластен пристап. - Во организацијата неколкупати била извршена кражба преку истите необезбедени прозорци. Покрај другите вредни предмети, исчезнале и мобилните системи за информатичка технологија. Не можело да се исклучи без сомнение дали датотеките биле копирани или биле подложни на некаква манипулација. - Вработен во центар за повици направил копии од голема количина доверливи податоци за клиентите непосредно пред да биде принуден да ја напушти организацијата. Откако ја напуштил организацијата, тој потоа им ги продал овие податоци на конкурентите. Бидејќи деталите за инцидентот подоцна протекле во медиумите, центарот за повици изгубил многу важни клиенти.

Губење уреди, медиуми за чување податоци и документи

3_0.17	Губење уреди, медиуми за чување податоци и документи Дов, И
Објаснување	Постојат различни причини што можат да доведат до губење уреди, носачи на податоци и документи. Ова директно влијае врз достапноста, но доверливите информации може да се најдат и во неовластени раце доколку носачите на податоци не се целосно криптирани. Се создаваат трошоци за замена на уреди или носачи на податоци, а кога тие повторно ќе се појават или ќе бидат пронајдени, информациите можеби веќе биле откриени или биле инсталирани несакани програми. Мобилните уреди и мобилните носачи на податоци особено лесно може да се изгубат. Денес, огромни количини податоци можат да се чуваат на мали мемориски картички. Сепак, често се случува документите во хартиена форма случајно да се забораваат некаде, на пример во ресторани или во превозни средства.
Пример(и)	- Вработена патува со автобус до своето работно место за да разгледа некои документи. Кога избезумено се симнува на постојката на одредиштето, случајно ги остава документите на седиштето до неа. Иако документите не се доверливи, потоа повторно треба да се добијат неколку потписи од високи раководители.

	- На голем настан, на вработен случајно и незабележано му паѓа мемориска картичка со доверливи пресметки на подот додека пребарува во својата актовка. Пронаоѓачот ја гледа содржината на својот лаптоп и ѝ ги продава информациите на конкуренцијата. - Производител испраќа со софтверски ажурирања за решавање проблеми на своите клиенти по пошта. Некои од овие CD-а се губат при пренесување без да бидат известени испраќачот или примачот за тоа. Како резултат на тоа, засегнатите клиенти се соочуваат со софтверски дефекти.
--	--

Лошо планирање или недостаток на приспособување

З_0.18	Лошо планирање или недостаток на приспособување	Дов, И, Д
Објаснување	Доколку организациските процеси што директно или индиректно служат за обработка на информации не се правилно дизајнирани, тоа може да доведе до безбедносни проблеми. Иако секој поединечен чекор на процесот се врши правилно, често настанува оштетување бидејќи процесите како целина се погрешно дефинирани. Друга можна причина за безбедносни проблеми се зависностите од други процеси, кои самите немаат очигледна врска со обработката на информациите. Таквите зависности може лесно да се занемарат при планирањето и на тој начин може да предизвикаат оштетувања за време на работата. Безбедносните проблеми може да произлезат и од фактот дека задачите, улогите или одговорностите не се јасно доделени. Меѓу другото, ова може да предизвика одложување на процесите, занемарување на безбедносните мерки или непочитување на прописите. Опасност постои и кога опремата, производите, процесите или другите средства за спроведување обработка на информации не се користат соодветно. На пример, изборот на несоодветен производ или пропусти во архитектурата на апликациите или во мрежниот дизајн може да доведе до безбедносни проблеми. Информатичката технологија и целокупното опкружување на една организација постојано се менуваат. Вработените ја напуштаат организацијата или нови вработени ѝ се приклучуваат на организацијата, се набавува нов хардвер или софтвер или некој давател на услуги банкротира. Доколку организациските и техничките приспособувања како резултат на ваквите настани не се земат предвид или се недоволно земени предвид, може да произлезат одредени опасности.	
Пример(и)	- Доколку процесите на одржување или поправка не се усогласени со деловните барања, тоа може да резултира со неприфатливо време на застој. - Може да има зголемен ризик од напади врз сопствените системи за информатичка технологија на организацијата доколку не се земат предвид безбедносните барања при набавка на информатичка технологија. - Доколку потребните потрошни материјали не се навремено достапни, процесите за информатичка технологија што зависат од нив може да попуштат.	

	- Може да се појават тешкотии доколку се избераат несоодветни протоколи за пренос при планирање процедура за информатичка технологија. - Структурните промени во објектот ги менуваат постојните маршрути за бегство. Бидејќи вработените не се соодветно известени, објектот не може да се евакуира во потребното време. - Кога се пренесуваат електронски документи, не се води сметка да се користи формат на податоци што примачот може да го прочита.
--	--

Откривање на информации што треба да се заштитат

З_0.19	Откривање на информации што треба да се заштитат	Дов
Објаснување	Доверливите податоци и информации мора да бидат достапни само за лица што се овластени да ги забележат. Покрај интегритетот и достапноста, доверливоста е една од основните вредности на безбедноста на информациите. Доверливите информации (какви што се лозинки, лични податоци, деловни тајни, податоци за развој) подложат на својствен ризик да бидат откриени како резултат на технички дефект, невнимание или дури и намерни дејства. До овие доверливи информации може да се пристапи на различни точки, на пример: - на медиуми за чување податоци во компјутери (хард-дискови), - на пренослив медиум за чување податоци (USB, CD-а или ДВД дискови), - во печатена форма на хартија (печатени материјали, датотеки) и - на патеките за пренос за време на пренос на податоци. Начините на кои се откриваат информациите исто така може значително да се разликуваат, на пример: - неовластено читање датотеки, - невнимателно откривање, на пример во текот на налози за поправка, - несоодветно бришење или уништување на медиумот за податоци, - кражба на медиуми за чување податоци и последователна експлоатација, - прислушување преносни линии, - заразени системи за информатичка технологија со злонамерен софтвер, - читање на екранот или прислушување разговори. Доколку се откријат информации што се вредни за заштита, тоа може да има сериозни последици за организацијата. Меѓу другото, губењето на доверливоста може да доведе до следните негативни последици за организацијата: - прекршување на законите, на пример, заштита на личните податоци, банкарска тајна, - негативно внатрешно влијание, на пример, деморализација на вработените, - негативно надворешно влијание, на пример, нарушување на односите со деловните партнери, изгубена доверба кај клиентите,	

	- финансиско влијание, на пример, барања за отштета, парични казни, правни трошоци, - нарушување на правото на информативно самоопределување. Губењето на доверливоста не е секогаш веднаш забележливо. Честопати станува очигледно подоцна, на пример, преку истражувачко новинарство дека неовластени лица добиле пристап до доверливи информации.
Пример(и)	- Купувачи на користени компјутери, хард дискови, мобилни телефони или на слични уреди постојано во нив наоѓаат многу доверливи информации какви што се посебни категории на лични податоци или броеви на сметки.

Информации од несигурни извори

3_0.20	Информации од несигурни извори	Дов, И, Д
Објаснување	Доколку се користат информации, софтвер или уреди што потекнуваат од несигурни извори или чие потекло и исправност не се соодветно проверени, нивната употреба може да создаде големи ризици. Меѓу другото, ова може да доведе до информации што се значајни за бизнисот да се засноваат на неточна база на податоци, пресметки што даваат неточни резултати или неточни одлуки. Сепак, и интегритетот и достапноста на системите за информатичка технологија еднакво може да бидат загрозувани.	
Пример(и)	- Примачот може да биде доведен во заблуда да преземе одредени дејства што се штетни за него или за други лица преку е-пошта, чие потекло не го проверил. На пример, е-поштата може да содржи интересни прилози или линкови при што кликувањето на нив предизвикува инсталирање злонамерен софтвер на компјутерот на примачот. Испраќачот на е-пошта може да е лажен или да го имитира профилот на познат партнер со кој комуницира лицето. - Претпоставката дека некоја изјава е вистинита затоа што е „во весник“ или „е емитувана на телевизија“, не е секогаш оправдана. Како резултат на тоа, лажните изјави може да се вклучат во извештаите што се од клучно значење за бизнисот. - Веродостојноста на информациите што се шират преку интернет многу се разликува. Кога извршувањата се преземаат од интернет без дополнителни проверки на изворот, може да се донесат погрешни одлуки. - Доколку се применуваат ажурирања или софтверски поправки од недоверливи извори, тоа може да доведе до несакани ефекти. Доколку не се провери потеклото на софтверот, постои зголемен ризик системите за информатичка технологија да бидат заразени со злонамерен код.	

Манипулација со хардвер или софтвер

3_0.21	Манипулација со хардвер или софтвер	Дов, И, Д
Објаснување	Манипулацијата се дефинира како каква било форма на насочена, но тајна интервенција за промена на целните објекти од кој било вид без да биде забележана. Манипулацијата со хардвер или софтвер, меѓу другото, може да се изврши поради чувство на одмазда, за да се предизвика штета намерно, да се стекне лична корист или за збогатување. Фокусот може да биде на уреди од секаков вид, додатоци, носачи на податоци (на пример, ДВД-дискови, USB), апликации, бази на податоци или слично. Манипулацијата со хардвер и софтвер не доведува секогаш до непосредна штета. Меѓутоа, ако се компромитирани информациите што се обработени при манипулацијата, тоа може да резултира со секакви безбедносни импликации (губење доверливост, интегритет или достапност). Упадот може да биде уште поефективен доколку се открие подоцна, со што се зголемуваат сознанијата на сторителите и влијанието врз работниот процес. Влијанијата може да бидат неовластен пристап до податоци што треба да бидат заштитени, па сè до уништување носачи на податоци или системи за информатичка технологија. Како резултат на тоа, може да се предизвика значителен застој како последица на манипулациите.	
Пример(и)	- Во една организација, вработен манипулирал со апликативниот софтвер за одредени финансиски услуги. Тоа му овозможило незаконски да прибави поголем износ на пари. - Со манипулирање со банкоматите, напаѓачите во повеќе наврати успеале незаконски да ги прочитаат податоците што се зачувани на платежните картички. Во врска со шпионираниите PIN-кодови, овие податоци подоцна биле злоупотребени за повлекување пари од сметката на сопственикот на картичката.	

Манипулација со информации

3_0.22	Манипулација со информации	И
Објаснување	Со информациите може да се манипулира на различни начини, на пример, со неправилно или намерно снимање податоци, со менување на содржината на полињата на базата на податоци или на кореспонденцијата. Начелно, ова не се однесува само на дигитални информации, туку и на хартиени документи, на пример. Сепак, сторителот може да манипулира само со информациите до кои има пристап. Колку повеќе права за пристап има едно лице до датотеките и директориумите на системите за информатичка технологија или колку повеќе има пристап до информации, толку посериозни манипулации може да изврши. Доколку манипулациите не се откријат во рана фаза, може сериозно да се наруши непреченото одвивање на деловните процеси и на специјалистичките задачи. Архивираните документи обично претставуваат информации што треба да се заштитат. Манипулацијата со вакви документи е особено сериозна затоа што може да се забележи дури по неколку години, кога повеќе не е можно да се проверат.	
Пример(и)	- Вработена била многу лута поради унапредувањето на нејзината колешка во организацијата така што неовластено пристапила до компјутерот на колешката додека накратко била отсутна. На тој начин, таа имала огромно негативно влијание врз објавените годишни резултати на организацијата, правејќи одредени промени на бројките во месечниот биланс на состојба.	

Неовластено влегување во системи за информатичка технологија

З_0.23	Неовластено влегување во системи за информатичка технологија Дов, И
Објаснување	По правило, секој интерфејс на систем за информатичка технологија не само што вклучува можност за овластено користење одредени услуги на системот за информатичка технологија преку него, туку и ризик од неовластен пристап преку него до системот за информатичка технологија.
Пример(и)	- Доколку се шпионираат корисничката идентификација и поврзаната лозинка, може да се претпостави неовластено користење на апликациите или на системите за информатичка технологија што се заштитени со нив. - Хакерите би можеле да добијат неовластен пристап до системите за информатичка технологија преку несоодветно обезбедени пристапни точки за одржување на далечина. - Во случај на несоодветно обезбедени интерфејси на активни мрежни компоненти, може да се претпостави дека напаѓачите би можеле да добијат неовластен пристап до мрежната компонента. Доколку успеат и да ги надминат локалните безбедносни механизми, на пример, да добијат административни овластувања, би можеле да ги извршуваат сите административни активности. - Многу системи за информатичка технологија имаат интерфејси за употреба на медиуми за чување податоци што може да се отстранат, какви што се помошни мемориски картички или USB медиум за чување податоци. Ако систем за информатичка технологија со соодветниот хардвер и софтвер се остави без надзор, постои ризик дека големи количини податоци би можеле да се читаат неовластено или преку тоа да се воведат злонамерен софтвер.

Уништување на уреди или медиуми за чување податоци

З_0.24	Уништување на уреди или медиуми за чување податоци Д
Објаснување	Небрежност, неправилна употреба, но и необучено ракување може да доведат до уништување на уредите и на носачите на податоци, што може сериозно да ја наруши работата на системот за информатичка технологија. Воедно, постои ризик поради уништувањето да се изгубат важни информации, кои не можат да се реконструираат или можат да се реконструираат само со голем напор.
Пример(и)	- Во една организација, вработен го искористил своето знаење дека важен сервер е сензитивен на прекумерно високи работни температури и ги блокирал отворите за вентилација на вентилаторот за напојување со предмет скриен зад серверот. Два дена подоцна, хард-дискот на серверот претрпел дефект поврзан со температурата, а серверот не функционирал неколку денови. - Еден вработен толку се налутил поради постојаното паѓање на системот, што го изразил својот гнев на својата работна станица. Во тој процес, хард-дискот бил толку многу оштетен од удари на компјутерот што станал неупотреблив. Податоците зачувани овде можело само делумно да се реконструираат со помош на сигурносна копија од претходниот ден. - Шолји за кафе што се истуриле или влага што продира при наводнување на цвеќињата, може да предизвикаат краток спој во системот за информатичка технологија.

Дефект на уреди или на системи

З 0.25	Дефект на уреди или на системи	Д
Објаснување	Доколку апликации каде што времето е од суштинско значење се користат на систем за информатичка технологија, последователните штети по дефект на системот се соодветно високи доколку нема алтернативни опции за вонредни состојби (за враќање на претходен режим).	
Пример(и)	- Фирмверот се внесува во систем за информатичка технологија што не е наменет за ваков тип систем. Системот за информатичка технологија потоа повеќе не стартува без грешки и производителот мора повторно да го доведе во оперативна состојба. - Кај давател на интернет услуги, грешка во напојувањето во системот за чување податоци предизвикала исклучување. Иако вистинската грешка брзо била отстранета, погодените системи за информатичка технологија не можеле да се рестартираат поради недоследности во системот за датотеки. Како резултат на тоа, неколку веб сервери управувани од давателот на интернет-услуги не биле достапни со денови.	

Неисправност на уреди или на системи

З 0.26	Неисправност на уреди или на системи	Дов, И, Д
Објаснување	Денес, уредите и системите што се користат за обработка на информации често имаат многу функции и затоа имаат соодветно сложена структура. Начелно, ова се однесува и на хардверските и на софтверските компоненти. Поради сложеноста, постојат многу различни извори на грешка во таквите компоненти. Како резултат на тоа, уредите и системите често не функционираат како што е предвидено, што доведува до безбедносни проблеми. Постојат многу причини за дефекти, на пример замор на материјалот, толеранции при производство, концептуални слабости, надминување на граничните вредности, ненамерни работни услови или неодржување. Бидејќи не постојат совршени уреди и системи, во секој случај секогаш мора да се прифати одредена преостаната веројатност за дефект. Сите основни вредности на безбедноста на информациите (доверливост, интегритет, достапност) може да бидат нарушени од дефекти на уредите или на системите. Покрај тоа, дефектите исто така може да останат незабележани подолг временски период. Како резултат на тоа, може да се случи, на пример, резултатите од пресметката да се фалсификуваат и да не се коригираат навреме.	
Пример(и)	- Поради затната вентилациска мрежа, системот за чување податоци се прегрева и не откажува целосно, туку се јавуваат одредени дефекти. Само неколку недели подоцна било забележано дека зачуваните информации се нецелосни. - Стандардна научна апликација се користи за вршење статистичка анализа за претходно собрана група податоци што е зачувана во база на податоци. Сепак, според документацијата, апликацијата не е одобрена за производот на базата на податоци што се користи. Се чини дека анализата функционира, но случајните проверки откриваат дека пресметаните резултати се неточни. Како причина биле идентификувани проблеми со компатибилноста помеѓу апликацијата и базата на податоци.	

Недостаток на ресурси

3_0.27	Недостаток на ресурси	Д
Објаснување	Доколку расположливите ресурси во одредена област се недоволни, тоа може да доведе до тешкотии во снабдувањето со овие ресурси, па дури и до преоптоварувања и дефекти. Во зависност од видот на засегнатите ресурси, мал настан, чија појава била исто така предвидлива, на крајот може да влијае врз голем број деловни процеси. Недостатоци на ресурси може да се појават во операциите на информатичката технологија и во врските за комуникација, но и во други области на една организација. Доколку за одредени задачи нема доволно достапен кадар, време и финансиски ресурси, тоа може да има различни негативни влијанија. На пример, можеби улогите што се потребни во проектите не ги исполнуваат соодветни лица. Доколку оперативните ресурси какви што се хардвер или софтвер повеќе не се доволни за да се исполнат барањата, специјалистичките задачи може да не бидат успешно завршени. Честопати, кадровските, временските, финансиските, техничките и други недостатоци сè уште може да се надоместат за време на редовните операции за ограничен временски период. Меѓутоа, под голем временски притисок, тие стануваат уште поочигледни, на пример во вонредни ситуации. И ресурсите може да бидат намерно преоптоварени ако некој намерно генерира интензивна побарувачка за одреден ресурс и со тоа предизвика интензивно и трајно нарушување на ресурсот.	
Пример(и)	- Преоптоварените електрични кабли се загреваат, што може да доведе до тлеене на пожар доколку каблите се постават на неправилен начин. - Ако на мрежата се користат нови апликации со поголеми барања за ширина на опсег отколку што било предвидено во времето на планирање, тоа може да доведе до губење на достапноста на целата мрежа ако мрежната инфраструктура не може да се зголеми доволно. - Ако администраторите редовно не ги проверуваат датотеките за записи на информатичката технологија што ја поддржуваат поради преоптоварување, нападите може да не се откријат навремено. - Веб серверите може да станат толку преоптоварени поради големиот обем на барања што пристигнуваат истовремено што регулираниот пристап до податоците станува речиси невозможен. - Доколку организацијата е во стечајна постапка, можеби нема финансии за резервните делови што се итно потребни или можеби нема да може да им плати на давателите на услуги.	

Софтверски недостатоци или грешки

3_0.28	Софтверски недостатоци или грешки	Дов, И, Д
Објаснување	Следното важи за секој софтвер: колку е посложен, толку почесто се јавуваат грешки. Дури и со интензивно тестирање, обично не се откриваат сите грешки пред испораката до клиентот. Доколку софтверските грешки не се откријат навреме, падовите или грешките што се случуваат во апликацијата може да доведат до далекусежни последици. Примери за тоа се неточни резултати од пресметката, погрешни одлуки на раководно ниво и доцнење во текот на деловните процеси.	

	Софтверските слабости или грешки може да доведат до сериозни безбедносни недостатоци во апликацијата, во системот за информатичка технологија или во сите поврзани системи за информатичка технологија. Напаѓачите може да ги искористат ваквите безбедносни недостатоци за да воведат злонамерен софтвер, да читаат податоци без овластување или да вршат манипулации.
Пример(и)	- Повеќето предупредувања што се издадени од CERT тимовите во последните години се поврзани со програмски грешки што се однесуваат на безбедноста. Тоа се грешки што се јавуваат при креирањето на софтверот и резултираат со подложност на тој софтвер на злоупотреба од напаѓачите. Голем дел од овие грешки биле предизвикани од максимална искористеност на меморијата. - Интернет пребарувачите се важна софтверска компонента за клиентите денес. Пребарувачите често се користат не само за пристап до интернет, туку и за внатрешни веб апликации во организациите. Поради тоа, слабостите на софтверот или грешките во пребарувачите може да имаат особено силно влијание врз безбедноста на информациите како целина.

Повреда на закони или на договори

З 0.29	Повреда на закони или на договори	Дов, И, Д
Објаснување	Доколку информациите, деловните процеси и системите за информатички технологии на организацијата се несоодветно обезбедени (на пример, преку несоодветно управување со безбедноста), тоа може да доведе до прекршување на законите што се однесуваат на обработка на информации или на постојни договори со деловни партнери. Кои закони мора да се почитуваат, во секој случај зависи од природата на организацијата или од нејзините деловни процеси и услуги. Во зависност од тоа каде се наоѓаат локациите на организацијата, можеби ќе треба да се почитуваат и други закони или договори. Примери за ова се следниве: - Раководството на една организација е должно да покаже соодветна грижа во сите деловни процеси. Ова вклучува почитување на безбедносните мерки предвидени во закони или договори. Правилната обработка на информации по правило вклучува и безбедна обработка на тие информации. - Во многу организации вообичаена практика е производителите да бараат од своите добавувачи да почитуваат одредени стандарди за квалитет и безбедност. Во овој контекст, сè повеќе се поставуваат барања и за безбедноста на информациите. Доколку договорната страна ги прекрши регулираните безбедносни барања, тоа може да доведе до казни, но и до раскинување на договорите или дури и прекин на деловните односи.	
Пример(и)	По правило безбедносните барања произлегуваат директно од законите. Меѓутоа, законите главно се засноваат на најсовремените технолошки достигнувања како општа основа за проценка на степенот на безбедност што може да се постигне. Доколку постојните безбедносни мерки на организацијата не се соодветно приспособени на вредностите што треба да се заштитат и на најсовремените технолошки достигнувања, тоа може да има сериозни последици врз деловното работење на организацијата.	

Неовластено користење или администрирање со уреди и системи

3_0.30	Неовластено користење или администрирање со уреди и системи Дов, И, Д
Објаснување	Без соодветни механизми за пристап и контрола на пристап, практично е невозможно да се спречи или да се открие неовластена употреба на уреди и системи. За системите за информатички технологии, основниот механизам е идентификација и автентикација на корисникот. Но, дури и во системи за информатичка технологија со силна функција за идентификација и автентикација, можна е неовластена употреба доколку соодветните безбедносни карактеристики (лозинки, паметни картички, токени итн.) паднат во погрешни раце. Може да се направат и многу грешки при доделување и одржување овластувања, на пример ако овластувањата се доделуваат премногу опсежно или на лица кои не треба да бидат овластени или не се ажурираат навремено. Неовластени лица може да добијат доверливи информации, да вршат манипулации или да предизвикаат дефекти преку неовластена употреба на уреди и системи. Особено важен посебен случај на неовластена употреба е неовластено администрирање. Ако неовластени лица ја променат конфигурацијата или работните параметри на хардверските или на софтверските компоненти, може да настане сериозна штета.
Пример(и)	- При проверка на податоците од записите, мрежен администратор наишол на првично необјасливи настани што се случувале во различни денови, но често рано наутро и попладне. По подетално испитување, било утврдено дека рутерот за безжична локална мрежа (WLAN) е небезбедно конфигуриран. Луѓето што чекале на автобуската постојка пред зградата на организацијата, го користеле овој пристап за пребарување на интернет со своите мобилни уреди додека чекале.

Неправилно користење или администрирање со уреди и системи

3_0.31	Неправилно користење или администрирање со уреди и системи Дов, И, Д
Објаснување	Неточното или неправилно користење уреди, системи и апликации може да ја загрози нивната безбедност, особено ако се занемарат или се заобиколат постојните безбедносни мерки. Ова често доведува до неисправности или до дефекти. Меѓутоа, во зависност од видовите уреди или системи што се користат погрешно, доверливоста и интегритетот на информациите исто така може да бидат нарушени. Особено важен посебен случај на неправилно користење е неправилното управување (администрирање). Грешките во инсталацијата, конфигурацијата, одржувањето и грижата за хардверските или за софтверските компоненти може да предизвикаат сериозни оштетувања. Слично на тоа, неправилното работење на системите за информатичка технологија или на апликациите, исто така може да предизвика случајно бришење или промена на податоците. Но, ова може да доведе и до протекување доверливи информации, на пример, доколку правата за пристап се неправилно поставени.

	Ако каблите од напојувањето или мрежните кабли се поставени незаштитено, тие може да се оштетат ненамерно, што ќе предизвика прекин на поврзувањето. Каблите за поврзување на уредот може да се скинат ако вработените или посетителите се сопнат на нив.
Пример(и)	- На пример, недоволно строги права за пристап, лозинки што лесно може да се погодат, недоволно заштитени носачи на податоци со сигурносни копии или терминали што не се заклучени за време на привремени отсуства може да доведат до безбедносни инциденти.

Злоупотреба на овластувања

З_0.32	Злоупотреба на овластувања	Дов, И, Д
Објаснување	Во зависност од нивните улоги и задачи, на вработените им се даваат соодветни овластувања за пристап и влез. Од една страна, ова е наменето за управување и контрола на пристапот до информации, а од друга страна, за да им овозможи на вработените да извршуваат одредени задачи. На пример, на вработените или на групите им требаат одредени овластувања за да можат да користат апликации или да уредуваат информации. Злоупотреба на овластувањата се случува кога легитимно или незаконски стекнатите опции намерно се користат надвор од предвидениот опсег. Честопати, целта е да се добијат лични предности или да се наштети на организацијата или на одредени физички лица. Во неколку случаи, вработените имаат повисоки или пообемни права на пристап отколку што им се потребни за нивните активности поради историски, системски или други причини. Овие права може да се злоупотребат за напади во одредени околности.	
Пример(и)	- Колку подетално и повнимателно се одредени правата за пристап до информации, толку е поголем напорот за одржување што честопати е потребен за да се ажурираат овие права. Оттука, постои ризик да се направи премала диференцијација помеѓу различните улоги при доделувањето на правата за пристап, што ја олеснува злоупотребата на овластувањата. - Во различни апликации, овластувањата за пристап или лозинките се зачувуваат во системски области до кои може да пристапат и други корисници. Ова може да им овозможи на напаѓачите да ги променат овластувањата или да читаат лозинки. - Вработените со недоволно јасни и конкретни овластувања може да се доведат до искушение да пристапат до туѓи датотеки, на пример да ја гледаат е-поштата на други вработени, бидејќи им биле потребни одредени информации.	

Недостиг на кадар

З 0.33	Недостиг на кадар	Д
Објаснување	Губењето кадар може да има значително влијание врз организацијата и врз нејзините деловни процеси. Кадарот може да биде отсутен без да може да се предвиди отсуството, на пример, поради болест, несреќа, смрт или штрајк. Понатаму, мора да се земе предвид и предвидливиот недостиг на кадар во случај на одмор, доквалификација (дополнителна обука) или редовен прекин на работниот однос, особено ако преостанатото работно време е намалено, на пример, поради право на годишен одмор. Недостигот на кадар може да биде предизвикан и од внатрешна промена на работното место.	
Пример(и)	- Поради долготрајна болест, мрежен администратор на една организација останал без работа. Во организацијата, мрежата првично продолжила да работи без грешки. Сепак, две недели подоцна, по пад на системот, никој не можел да ја поправи грешката бидејќи бил ангажиран само овој администратор што бил обучен за работа со мрежа. Ова довело до прекин на мрежата неколку денови. - Додека администраторот бил на одмор, една организација морала да почне да го користи резервниот медиум во базата за сигурносни копии на податоци. Кодот за пристап до базата на податоци бил променет неодамна и му бил познат само на овој администратор. Биле потребни неколку денови за да се вратат податоците, бидејќи администраторот повеќе не бил достапен додека бил на одмор. - Во случај на пандемија, сè повеќе вработени постепено стануваат достапни во текот на подолги временски периоди, без разлика дали поради самата болест, потребата да се грижат за роднините/блиските или да се грижат за децата. Некои вработени исто така не одат на работа поради страв од инфекција во јавниот превоз или во организацијата. Како резултат на тоа, може да се извршат само најнеопходните работи. Потребното одржување на системите, независно дали тоа е централен сервер или климатизација во центарот за податоци, повеќе не може да се обезбеди. Како резултат на тоа, сè повеќе системи откажуваат.	

Напад

З 0.34	Напад	Дов, И, Д
Објаснување	Нападот може да биде закана за една организација, за одредени области на организација или за физички лица. Постојат многу технички начини за извршување напад: фрлање тули, експлозија на експлозиви, употреба на огнено оружје, подметнување пожар. Дали и во колкава мера организација е изложена на ризик од напад не зависи само од локацијата и од околината на објектот, туку и во голема мера од нејзините задачи и политичко-социјалната клима. Организациите што работат во политички контроверзни области се изложени на поголема закана од другите. Организациите што се наоѓаат во близина на вообичаени области за одвивање демонстрации се поизложени на ризик отколку оние на далечни локации.	
Пример(и)	- Извршен е напад со експлозиви врз компјутерскиот центар на голема организација. Силниот удар на експлозивната направа не уништил само прозорци и сидови, туку и многу системи за информатичка технологија во центарот за податоци.	

Принуда, изнуда или корупција

З 0.35	Принуда, изнуда или корупција	Дов, И, Д
Објаснување	Принудата, изнудата или корупцијата може да доведат до загрозување на безбедноста на информациите или деловните процеси. На пример, со закана за насилство или други непријатности, напаѓачот може да се обиде да ја натера жртвата да ги игнорира безбедносните политики или да ги заобиколи безбедносните мерки (принуда). Наместо да се закануваат, напаѓачите можат конкретно да понудат пари или други придобивки за вработените или други лица да бидат инструмент за нарушување на безбедноста (корупција). На пример, постои ризик поткупениот вработен да проследи доверливи документи на неовластени страни. Принудата или корупцијата, начелно, можат да ги компромитираат сите основни вредности на безбедноста на информациите. Меѓу другото, нападите може да бидат насочени кон препраќање доверливи информации до неовластени лица, манипулирање со критични информации за бизнисот или нарушување на непреченото одвивање на деловните процеси.	
Пример(и)	Постои особен ризик кога таквите напади се насочени против високи раководители или лица на позиции од посебна доверба.	

Кражба на идентитет

З 0.36	Кражба на идентитет	Дов, И, Д
Објаснување	При кражба на идентитет, напаѓачот фалсификува лажен идентитет, односно користи информации за друго лице со намера да дејствува во негово име. За таа цел се користат податоци какви што се датум на раѓање, адреса, броеви на кредитна картичка или сметка, на пример, за да се регистрира кај давател на интернет-услуги на туѓ трошок или за да се збогати на некој друг начин. Кражбата на идентитет честопати директно или индиректно ѝ наштетува и на репутацијата, но исто така предизвикува да се троши многу време за разјаснување на причините и избегнување негативни последици за засегнатите лица. Некои форми на измама во врска со идентитетот се нарекуваат и маскирање/прикривање на идентитетот. Кражбата на идентитет е особено честа кога со верификацијата на идентитетот се постапува премногу невнимателно, особено кога таа е основата за скапи услуги. Лицето што е измамено во однос на идентитетот на неговиот или нејзиниот партнер за комуникација може лесно да биде измамено да открие сензитивни информации.	
Пример(и)	- Кај различни даватели на услуги за е-пошта и платформи за аукција на интернет, првично било доволно да се измисли име за да се регистрира лицето и да се направи сигурносна копија со соодветна адреса од телефонскиот именик. На почетокот, напаѓачите можеле да се регистрираат и под препознатливи измислени имиња, какви што се оние на цртани ликови. Кога биле воведени построги тестови за веродостојноста, биле користени и имиња, адреси и броеви на сметки на вистински луѓе. Засегнатите дознале за ова дури кога ги добиле првите барања за исплата. - Адресите на испраќачите на е-пошта лесно се фалсификуваат. Често се случува корисниците на овој начин да се измамат и да мислат дека е-	

	поштата потекнува од сигурен партнер за комуникација. Слични напади се можни со манипулирање со идентификацијата на повикувачот за гласовни врски или со манипулирање со идентификацијата на испраќачот за врски преку факс. - Напаѓачот може да користи прикривање за да се обиде да се приклучи на веќе постојна врска без потреба од автентикација, бидејќи овој чекор веќе го поминале првичните учесници во комуникацијата.
--	--

Одредување на дејствија

З 0.37	Одредување на дејствија	Дов, И
Објаснување	Вработените може да негираат дека извршиле одредени дејства од различни причини, на пример, затоа што овие дејства ги прекршуваат упатствата, безбедносните барања или дури и законите. Но, тие може да негираат и дека добиле известување, на пример затоа што заборавиле состанок. Според тоа, во областа на безбедност на информациите, акцентот често е на обврзаноста, својство што се користи за да се обезбеди дека преземените дејства не можат да се негираат без оправдување. Во случај на комуникација, дополнително се прави разлика дали учесникот во комуникацијата го негира приемот на пораката (одредување прием) или преносот (одредување на потеклото). Одредувањето на приемот може да биде важно во финансиските трансакции, на пример, кога некој негира дека добил фактура навреме. Може да се случи и учесник во комуникацијата да негира дека испратил порака, на пример, негира дека направил нарачка. Испраќањето или примањето на пораката, може да се негира во случај на испраќање по пошта, како и во случај на употреба на факс или е-пошта.	
Пример(и)	-Електронски се нарачува резервен дел што е итно потребен. По една недела се бара делот што недостасува, а во меѓувреме се направени високи трошоци поради изгубеното производство. Добавувачот негира дека некогаш добил нарачка.	

Злоупотреба на лични податоци

З 0.38	Злоупотреба на лични податоци	Дов
Објаснување	Личните податоци речиси секогаш се информации за кои е потребна посебна заштита. Типични примери се информации за личните или за фактичките околности на идентификувано физичко лице или физичко лице што може да се идентификува. Доколку не е соодветно обезбедена заштита на личните податоци, постои ризик социјалната положба или економските околности на субјектот на лични податоци да бидат нарушени. Може да дојде до злоупотреба на личните податоци, на пример, ако организацијата прибира обемни категории на лични податоци, ги прибрала без правна основа или согласност, ги користи за цел различна од првичната за која биле собрани, ако предоцна ги избрише личните податоци или ако неовластено ги открива.	
Пример(и)	- Личните податоци може да се обработуваат само за целта за која првично биле собрани или зачувани. Затоа, не е дозволено за следење на присуството и однесувањето да се користат датотеки за записи во кои најавувањето и одјавувањето на корисниците на системите за информатичка технологија се евидентирани исклучиво за целите на контролата на пристапот до податоците. - Вработените што имаат пристап до личните податоци би можеле да ги откријат без овластување. На пример, одреден вработен може да ги продаде податоците за клиентите на организацијата на друга организација.	

Злонамерен софтвер

З_0.39	Злонамерен софтвер	Дов, И, Д
Објаснување	Програма со злонамерен (малициозен) софтвер е софтвер што е развиен за да се извршуваат несакани и најчесто штетни функции. Вообичаени видови злонамерен софтвер вклучуваат вируси, „црви“ и „тројански коњи“. Злонамерните програми обично стануваат активни тајно, без знаење и согласност на корисникот. Во денешно време, злонамерните програми му обезбедуваат на напаѓачот опсежни комуникациски и контролни способности и поседуваат широк опсег на функции. Меѓу другото, злонамерниот софтвер може да ги таргетира лозинките, далечински да ги контролира системите, да оневозможи заштитен софтвер и да шпионира податоци. Во однос на штетата, загубата или корумпирањето информации или апликации е особено значајно. Сепак, губењето на имиџот и финансиската штета што може да резултираат од злонамерен софтвер, исто така се многу значајни.	
Пример(и)	- Во минатото, злонамерниот софтвер W32/Bugbear се ширел на два начина: пребарувал локални мрежи за компјутери со споделувања до кои бил можен пристап за пишување и се копираа на нив. Исто така, се испраќаа како HTML е-пошта до примачите во адресарот за е-пошта на заразените компјутери. Поради пропуст во HTML рутината на одредени програми за е-пошта, злонамерната програма била извршена кога била отворена пораката, без никакви дополнителни активности од примачот. - Злонамерниот софтвер W32/Klez се ширел во неколку варијанти. Заразените компјутери го испратиле вирусот до сите приматели во адресарот за е-пошта на компјутерот. Откако овој вирус го заразил компјутерот, го спречил инсталирањето антивирусни програми од популарните производители со континуирано манипулирање со оперативниот систем, со што го отежнал отстранувањето на вирусите на заразените компјутери.	

Одбивање на услуга

З_0.40	Одбивање на услуга	Д
Објаснување	Постојат многу различни форми на напади, чија цел е да ја спречат предвидената употреба на одредени услуги, функции или уреди. Општиот термин за такви напади е „одбивање на услугата“. Често се користи и терминот „DoS-напад (напад за одбивање на услугата)“. Ваквите напади може да потекнуваат од незадоволни вработени или клиенти, меѓу другото, но и од конкуренти, уценувачи или политички мотивирани сторители. Целта на нападите може да бидат средства од секаков вид што се значајни за бизнисот. Типични манифестации на DoS-напади се следните: - Нарушување на деловните процеси, на пример, со преоптоварување на прифаќањето налози со погрешни нарачки; - Оштетување на инфраструктурата, на пример, со блокирање на вратите на организацијата;	

	- Предизвикување дефекти во информатичката технологија, на пример, со намерно преоптоварување на услугите на серверот во мрежата. Овој тип напад често се поврзува со дистрибуирани ресурси, со тоа што напаѓачот ги користи овие ресурси до таа мера што тие повеќе не се достапни за вистинските корисници. На пример, нападите засновани на информатичка технологија може вештачки да ги исцрпат следните ресурси: процеси, време на централна обработувачка единица (CPU), меморија, простор на дискот, капацитет за пренос.
Пример(и)	- Силни напади за одбивање на услугата се случиле на голем број понуди на интернет во една држава во текот на подолг временски период. Како резултат на тоа, употребата на информации и услуги на интернет во оваа држава била значително нарушена.

Саботажа

З_0.41	Саботажа	Д
Објаснување	Саботажа се однесува на намерна манипулација или оштетување предмети или процеси, со цел да се предизвика штета на жртвата. Центрите за податоци или комуникациските врски на организациите можат да бидат особено привлечни цели, бидејќи овде може да се постигне големо влијание со релативно мали средства. Со сложената инфраструктура на центарот за податоци може да се манипулира селективно за да се предизвикаат оперативни нарушувања со намерно влијание врз важни компоненти, можеби од сторители однадвор, но пред сè од внатрешни сторители. Овде особено се изложени на ризик несоодветно заштитената градежна технологија или комуникациската инфраструктура, како и централните точки за снабдување, кои можеби не се надгледуваат организациски или технички и се лесно достапни за надворешни страни без да се набљудуваат.	
Пример(и)	- Во голем центар за податоци, неовластената работа со уредот за непрекинато напојување (UPS) довела до привремен целосен дефект. Сторителот постојано рачно го префрлал UPS уредот на режим на заобиколување, а потоа манипулирал со главното напојување на објектот. Вкупно четири прекини се случиле во период од три години. Во одредени случаи, имало дури и оштетување на хардверот. Прекините на услугата траеле меѓу 40 и 130 минути. - Во рамките на центарот за податоци се наоѓале и санитарни јазли. Со затнување на одводите и истовремено отворање на водоводот, водата навлегла во централните технички компоненти. Притоа, настанатите штети довеле до прекини во работата на производствениот систем. - Саботажата претставува особен ризик за електронските архиви, бидејќи многу документи што се доволно важни, за да се заштитат обично се чуваат на мал простор. Како резултат на тоа, може да се предизвика голема штета под одредени околности со насочени манипулации со мал напор.	

Социјален инженеринг

З 0.42	Социјален инженеринг	Дов, И
Објаснување	Социјалниот инженеринг е метод за стекнување неовластен пристап до информации или до системи за информатички технологии преку социјални активности. Социјалниот инженеринг ги искористува човековите карактеристики какви што се корисност, доверба, страв или почит кон авторитетот. Како резултат на тоа, вработените може да бидат изманипулирани да постапуваат неправилно. Типичен случај на напади со примена на социјален инженеринг е манипулацијата со вработените преку телефонски повик, во која напаѓачот се преправа дека е, на пример: - вработен во делот од компанијата кој директно комуницира со клиенти, чиј претпоставен сака да направи нешто брзо, но ја заборавил лозинката и сега му треба итно, - администратор што се јавува за системска грешка бидејќи сè уште му треба лозинката на корисникот за да ја поправи грешката. Кога следуваат критични прашања, љубопитната личност наводно е „само привремено вработен“ или „важна“ личност. Друга стратегија во систематскиот социјален инженеринг е да се изгради подолг однос со жртвата. Со упатување многу неважни телефонски повици однапред, напаѓачот може да се стекне со одредени сознанија и да изгради доверба што подоцна може да ја искористи. Ваквите напади можат да бидат и во повеќе фази, при што понатамошните чекори се надоврзуваат на сознанијата и на техниките што се стекнати во претходните фази. Многу корисници знаат дека не треба да споделуваат лозинки со никого. Социјалните инженери го знаат ова и затоа мора да користат други средства за да стигнат до посакуваната цел. Примери за тоа се следните: - Напаѓачот може да побара од жртвата да изврши команди или апликации што се непознати за него, на пример, затоа што ова треба да помогне при проблем со информатичката технологија. Ова може да биде скриена инструкција за промена на правата за пристап. Ова му овозможува на напаѓачот да добие сензитивни информации. - Иако многу корисници користат силни лозинки, тие се користат за повеќе сметки. Ако напаѓачот работи на корисна мрежна услуга (како што е систем за адреси на е-пошта) на која мора да се изврши автентикација на корисниците, напаѓачот може да ги добие лозинките и најавите што ги сака. Многу корисници ќе ги искористат личните детали што ги користат за таа услуга и за други услуги. Кога напаѓачите добиваат лозинки или други лични детали за автентикација без дозвола, на пример со користење социјален инженеринг, ова често се нарекува кражба на идентитетот (phishing).	
Пример(и)	Во социјалниот инженеринг, не може секогаш да се види напаѓачот. Честопати жртвата никогаш нема да дознае дека била експлоатирана. Ако ова успешно се спроведе, напаѓачот не мора да очекува кривично гонење и исто така има извор за да добие дополнителни информации подоцна.	

Вметнување пораки

З 0.43	Вметнување пораки	Дов, И
Објаснување	Во оваа форма на напад, напаѓачите испраќаат специјално подготвени пораки до системи или до луѓе, со цел да постигнат предност за себе или штета за жртвата. За да ги конструираат пораките соодветно, напаѓачите користат, на пример, описи на интерфејс, спецификации на протокол или записи за тоа како се одвивала комуникацијата во минатото. Постојат два посебни случаи на вметнување порака што се важни во практиката: - Во „репродуциран напад“ (репродукција на пораки), напаѓачите снимаат валидни пораки и подоцна повторно ги пренесуваат или ги пуштаат овие информации во (речиси) непроменета форма. Може да биде доволно да се користат и само делови од пораката, како лозинка, за да се добие неовластен пристап до систем за информатички технологии. - При напад на „човек во средината“, напаѓачот незабележано зазема посредничка позиција во комуникацијата помеѓу различни учесници. За да го стори ова, тој обично го мами испраќачот на пораката за да мисли дека тој е вистинскиот примач и го мами примачот да мисли дека тој е вистинскиот испраќач. Ако ова успее, напаѓачот на тој начин може да прима пораки што не се наменети за него и да ги процени и намерно да манипулира со нив пред да ги проследи до вистинскиот примач. Криптирањето на комуникациите не обезбедува заштита од напади од „човек во средината“ доколку не постои сигурна автентикација на партнерите што учествуваат во комуникацијата.	
Пример(и)	- Напаѓачот ги снима податоците за автентикација (на пример, корисничка идентификација и лозинка) за време на процесот на најавување на корисникот и ги користи овие информации за да добие пристап до системот. Во случај на само статични протоколи за автентикација, тоа значи дека дури и лозинката што е пренесена во криптирана форма може да се користи за да се добие неовластен пристап до систем од трето лице. - За да и нанесе финансиска штета на организацијата, вработениот неколкупати дава овластен налог.	

Неовластен влез во простории

З 0.44	Неовластен влез во простории	Дов, И, Д
Објаснување	Доколку неовластени лица влезат во некој објект или во одделни простории, тоа може да резултира со разни други опасности. Тие вклучуваат, на пример, кражба или манипулација со информации или системи за информатичка технологија. Во случај на квалификувани напади, одлучувачки фактор е времетраењето кога сторителите можат непречено да ја остварат својата цел. Честопати, сторителите сакаат да украдат вредни компоненти за информатичка технологија или други производи што лесно може да се отстранат. Меѓутоа, целта на упадот може да биде, меѓу другото, да се добијат доверливи информации, да се извршат манипулации или да се нарушат деловните процеси. Оттука, од неовластен упад во просториите може да произлезат неколку видови штета:	

	- Може да се предизвика имотна штета само како резултат на неовластен влез. Прозорците и/или вратите се отвораат насила и притоа се оштетуваат, поради што е потребна поправка или замена. - Украдената, оштетената или уништената опрема или компоненти мора да се поправат или да се заменат. - Може да настане оштетување од нарушување на доверливоста, интегритетот или достапноста на информации или апликации.
Пример(и)	- Вандализам. - При кражба во организација во текот на викендот, предизвикана е само помала штета со кршење прозорец; биле земени само мала касичка и ситен инвентар. Сепак, при рутинска проверка подоцна било утврдено дека вешто било работено со централниот сервер за време на упадот.

Губење податоци

3_0.45	Губење податоци	Д
Објаснување	Губењето податоци е настан што предизвикува заливот на податоци повеќе да не може да се користи како што е потребно (губење достапност). Вообичаена форма на губење податоци е кога податоците се бришат ненамерно или без овластување, на пример поради неправилно работење, дефекти, прекини на напојувањето, контаминација или злонамерен софтвер. Сепак, губењето податоци може да биде последица и на оштетување, губење или кражба на уреди или на носачи на податоци. Овој ризик честопати е особено висок за мобилните уреди и за мобилните носачи на податоци. Понатаму, треба да се забележи дека многу мобилни системи за информатичка технологија не се секогаш приклучени на интернет-мрежа. Затоа, податоците што се зачувани на овие системи не се секогаш ажурирани. Кога заливите на податоци се синхронизираат помеѓу мобилните системи за информатичка технологија и фиксни системи за информатичка технологија, губењето на податоците може да настане поради невнимание или неисправност.	
Пример(и)	- Мобилен телефон испаднал од џебот на кошулата и се скршил на плочките, а кучето наместо весник го носело таблетот, за жал со последици. Ваквите и слични настани се причина за многу целосни губења податоци од мобилните уреди. - Постојат злонамерни (малициозни) програми, кои конкретно бришат податоци на заразени системи за информатичка технологија. Кај некој злонамерен софтвер, функцијата за бришење не се извршува веднаш по инфицирањето, туку само кога ќе се случи конкретен настан, на пример, кога системскиот часовник ќе достигне одреден датум. - Многу интернет услуги може да се користат за зачувување информации на интернет. Ако лозинката е заборавена и не е зачувана, зачуваните информации можеби повеќе нема да бидат достапни освен ако давателот на услугата не понуди соодветна процедура за ресетирање на лозинката. - Хард дисковите и другите медиуми за чување на податоци имаат само ограничен работен век. Доколку не се преземат соодветни мерки за редундантност, податоците може да се изгубат поради технички дефекти.	

Губење на интегритетот на информациите што треба да се заштитат

З_0.46	Губење на интегритетот на информациите што треба да се заштитат И
Објаснување	Интегритетот на информациите може да биде загрозен од различни причини, на пример, неовластено користење, несоодветно однесување на некои лица, неправилно работење на апликациите, неисправности на софтверот или грешки во преносот и тоа: - Информациите може да се изгубат поради стареење на носачите на податоци. - Грешки во преносот: може да се појават грешки при преносот на податоци. - Злонамерен софтвер: Злонамерните програми можат да изменат или да уништат цели групи податоци. - Неточни записи: Неточните записи може да доведат до трансакции што се толку непожелни што често остануваат незабележани долго време. - Напаѓачите може да се обидат да манипулираат со податоците за свои цели, на пример, да добијат пристап до други системи за информатичка технологија или бази на податоци. - Со манипулирање со индексот на базата на податоци, електронските архиви може да се поттикнат да архивираат или да репродуцираат фалсификувани документи. Кога повеќе нема интегритет на информациите, може да настанат различни проблеми: - Во наједноставниот случај, информациите повеќе не можат да се читаат, односно дополнително да се обработуваат. - Податоците може ненамерно или намерно да се фалсификуваат на таков начин што ќе се пренесат лажни информации. На пример, ова може да предизвика трансфери со погрешен износ или до погрешен примач, може да се манипулира со информациите за испраќачот на е-пошта или со многу други дејства. - Доколку криптираните или компримираните групи податоци го изгубат својот интегритет (тука е потребна промена од само еден бит), можеби повеќе нема да може да се декриптираат или да се декомпримираат. - Истото важи и за криптографските клучеви и овде промената на еден бит е доволна за да станат клучевите неупотребливи. Ова значи дека податоците повеќе не може да се декриптираат или да се проверуваат во однос на автентичноста.
Пример(и)	- Документите што се чуваат во електронски архиви ја губат доказната вредност доколку не може да се докаже нивниот интегритет.

Штетни несакани ефекти

З 0.47	Штетни несакани ефекти	Дов, И, Д
Објаснување	Нападите што се поддржани од информатичка технологија може да имаат влијанија кои: - сторителите не ги планирале или - не влијаат директно врз нападнатите целни објекти или - наштетуваат на неинволвирани трети лица. Причините за тоа се големата сложеност и мрежното работење на современата информатичка технологија и фактот што зависностите на нападнатите целни објекти и поврзаните процеси обично не се очигледни. Меѓу другото, ова може да резултира со погрешна процена на реалната потреба за заштита на целните објекти или на лицата што се одговорни за целните објекти да немаат личен интерес да ги отстранат сите недостатоци на овие целни објекти.	
Пример(и)	- Ботовите што се инсталирани на системи за информатичка технологија кои им овозможуваат на сторителите да вршат дистрибуирани напади со одбивање услуга (DDoS), често не претставуваат директна закана за самите заразени системи за информатичка технологија бидејќи DDoS-нападите обично се насочени против системи за информатичка технологија од трети лица. - Сторителите може да ги користат недостатоците на уредите за „интернет на нештата“ (IoT) во безжичните локални мрежи (WLAN) како премин за напад на други поважни уреди во истата безжична локална мрежа. Затоа, таквите уреди за „интернет на нештата“ мора да бидат заштитени дури и ако тие самите имаат ниски барања за заштита. - Нападите на уценувачки софтвер на системи за информатичка технологија во одредени околности можат да предизвикаат верижни реакции и на тој начин можат да влијаат и врз клучните инфраструктури. Ова, пак, може да доведе до тешкотии за снабдување на населението, иако сторителите можеби немале таква цел.	

4. Закани и мерки

4.1. Организација

4.1.1. Вовед

Секоја организација има потреба од служба која што ќе биде одговорна за контрола и регулирање на општите операции, како и планирање, организирање и спроведување на услуги. За таа цел, повеќето организации имаат организациска единица што ја контролира интеракцијата на различни улоги и единици со соодветните деловни процеси и ресурси. На вакво сеопфатно ниво, треба да се вклучат и да се дефинираат аспектите на безбедноста на информациите, така што истите ќе претставуваат обврска.

4.1.2. Цел

Целта е да се опишат општите и сеопфатни барања во областа на организацијата, кои помагаат да се зголеми и да се одржува безбедноста на информациите. За да се постигне ова, мора да се регулираат тековите на информациите, процесите, распределбата на улогите и структурната и процедуралната организација.

4.1.3. Закани

Недоволно правила

Недостатокот на правила може да доведе до сериозни потешкотии, бидејќи на пример, вработените не знаат како да реагираат ако се случи инцидент. Проблемите може да произлезат и од правила што се застарени, непрактични или нејасно формулирани.

Важноста на овие сеопфатни организациски прописи се зголемува со сложеноста на деловните процеси и опсегот на обработка на информациите, но воедно и со барањата за заштита на информациите што треба да се обработуваат.

Непочитување на прописите

Применливите прописи мора да им бидат познати и достапни на сите вработени. Искуството покажува дека не е доволно само да се утврдат правила за безбедност. Од суштинско значење е да им се соопштат правилата на вработените за да им се овозможи на сите засегнати страни активно да ги користат овие правила во својата секојдневна работа.

Доколку вработените не ги почитуваат прописите, може да се појават следните недостатоци во однос на безбедноста, на пример:

- Разговорите за доверливи информации може да ги слушнат надворешни лица во близина кои го слушаат разговорот – на пример, додека разговараат за време на пауза, на состанок или на мобилен телефон во јавна средина;
- Документите може да се објавуваат на веб страница без да се провери дали се навистина наменети и одобрени за објавување или не;
- Поради неправилно администрирање на правата за пристап, вработениот би можел да ги менува податоците без да го разбере клучното влијание што може да го има ова нарушување на интегритетот.

Несоодветни или некомпатибилни ресурси

Доколку потребните ресурси не се достапни во доволни количини или не се навремено обезбедени, тоа може да доведе до прекини во организацијата. Во некои случаи се купуваат и несоодветни, па дури и некомпатибилни ресурси што не можат да се користат.

Пример: Просторот за чување податоци на хард дисковите кај клиентите и серверите, исто како и просторот на мобилните медиуми за чување податоци, постојано се зголемува. Луѓето често немаат навика да купуваат компоненти за информатичка технологија и медиуми за чување податоци со доволен капацитет за редовни сигурносни копии.

Треба да се обезбеди и правилно функционирање на ресурсите, при што несоодветното одржување може да доведе до значителна штета.

Примери:

- Капацитетот на батериите на уредот за непрекинато напојување (UPS) не бил проверен навреме. Ако капацитетот или содржината на киселина се на премногу ниско ниво, UPS системот повеќе нема да може доволно долго да надомести за прекин на напојувањето;
- Противпожарните апарати не биле навремено сервисирани и затоа повеќе немаат доволно притисок. Нивниот капацитет за гаснење повеќе нема да биде загарантиран во случај на пожар.

Закани надвор од организацијата

Во случаи во кои се вклучени надворешни лица, не може да се претпостави дека тие ќе ракуваат со информациите и со информатичката технологија според правилата што ги утврдила самата организација.

Посетителите, кадарот задолжен за чистење и вработените на трети лица може да претставуваат закана за внатрешните информации, за деловните процеси и за системите за информатичка технологија на различни начини, почнувајќи од несоодветно ракување со техничката опрема и обиди да се „игра“ со системи за информатичка технологија до кражба на документи или компоненти за информатичка технологија.

Примери:

- Посетители без придружба можат да пристапат до документи, медиуми за чување податоци или опрема, да ги оштетат овие предмети или да преземат сензитивни информации;
- Вработените што се задолжени за чистење може случајно да ги олабаат конекторите, да остават вода да истече во опремата, да ги поместат овие предмети или да ги фрлат заедно со ѓубрето.

4.1.4. Мерки

Прецизирање одговорности и прописи

Во рамките на една организација, сите релевантни задачи и улоги мора да бидат јасно дефинирани и одделени една од друга. Обврзувачките одредби за заштита на личните податоци и безбедноста на информациите мора да се дефинираат на глобално ниво за различните достапни оперативни аспекти. Организационските структури и обврзувачките прописи мора да се ревидираат кога тоа е потребно, а сите вработени мора да бидат известени за ваквите промени.

Доделување одговорности

За сите деловни процеси, апликации, системи за информатичка технологија, простории, објекти и комуникациски врски, мора да се дефинираат лицата што се одговорни за нив и за нивната безбедност. Сите вработени мора да бидат соодветно известени, особено во однос на тоа за што се одговорни и за поврзаните задачи што треба да ги извршуваат.

Надзор или придружба на надворешни лица

Лицата надвор од организацијата мора да бидат придружувани до просториите од страна на вработените. Вработените во организацијата мора да ги надгледуваат и надворешните лица во сензитивните области. Вработените треба да се поттикнат да не оставаат надворешни лица без надзор во просториите на својата организација.

Поделба на улоги помеѓу некомпатибилни задачи

Задачите како и улогата и функциите што се потребни за нив мора да бидат структурирани на таков начин што некомпатибилните задачи (какви што се оперативните и контролните улоги) се доделуваат на различни лица. Поделбата на некомпатибилните улоги мора да биде дефинирана и документирана. Исто така, надворешните претставници мора да подлежат на поделба на улогите.

Лица за контакт за прашања во врска со безбедноста на информациите

Во секоја организација мора да има лица за контакт за безбедносни прашања, кои можат да одговорат и на навидум едноставни и сложени прашања. Овие лица за контакт мора да им бидат познати на сите вработени во организацијата. Соодветните информации мора да бидат ставени на располагање и да бидат лесно достапни за сите во организацијата.

Управување со ресурси и уреди

Сите уреди и ресурси што влијаат врз безбедноста на информациите и кои се потребни за извршување задачи и почитување на безбедносните барања, треба да бидат достапни во доволни количини. Пред да се користат овие уреди и ресурси, треба да се извршат соодветни процеси за верификација и одобрување. Уредите и ресурсите треба да бидат наведени во соодветните инвентарни списоци. За да се спречи злоупотреба на податоци, треба да се регулира бришењето или уништувањето на уреди и ресурси.

Политика за безбедно користење информатичка технологија

Организацијата треба да подготви политика за сите вработени, која транспарентно ги опишува условите што мора да се почитуваат при користење на информатичката технологија и безбедносните заштитни мерки што мора да се имплементираат. Политиката треба да ги опфаќа следните аспекти:

- Безбедносните цели на организацијата;
- Важни термини;
- Задачи и улоги во однос на безбедноста на информациите;
- Лица за контакт за прашања што се однесуваат на безбедност на информациите;
- Имплементирање на безбедносни заштитни мерки и нивно почитување и применување од страна на вработените.

На сите корисници треба да им се укаже за оваа политика. Секој нов корисник треба писмено да потврди дека ја прочитал и дека ќе се придржува кон политиката пред да му биде дозволено да користи информатичка технологија. Корисниците треба да се известуваат за секоја промената на политиката, за да можат истата да ја применуваат. Политиката треба да биде лесно достапна за да може да ја прочитаат сите вработени (на пример, на интранетот на организацијата).

Организација - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.38	Злоупотреба на лични податоци
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.2. Кадар

4.2.1. Вовед

Вработените на една организација се од клучно значење за нејзиниот успех или неуспех. Конкретно, вработените имаат важна задача при спроведувањето на заштитата на личните податоци и безбедноста на информациите. Дури и најразвиените мерки на претпазливост за безбедноста можат да бидат некорисни ако не се применуваат истите активно. Основното значење на заштитата на личните податоци и безбедноста на информациите за организацијата и за нејзините деловни процеси мора да биде транспарентно и разбирливо за нејзиниот кадар.

4.2.2. Цел

Целта е да се истакнат заштитните мерки за безбедноста што мора да ги преземат организационата единица за човечки ресурси и раководните лица за да се уверат дека вработените одговорно ракуваат со информациите на нивната организација и се однесуваат во согласност со воспоставените внатрешни процедури.

4.2.3. Закани

Недостиг на кадар

Недостигот на кадар може да значи дека одредени задачи повеќе нема да се извршуваат навремено или воопшто нема да се извршуваат.

Недоволно познавање правила и процедури

Самото донесување на правила и процедури не е доволна гаранција дека тие ќе се почитуваат, ниту, пак, обезбедува спроведување на активностите без проблеми. Сите вработени мора да бидат запознаени со правилата и процедурите што се применуваат. Штетата што произлегува од недоволното познавање на постојните правила и процедури, не може да се правда едноставно поради „незнаење“.

Негрижа при постапување со информации

Иако може да има многу организациски и технички безбедносни процедури во организацијата, често се случува тие да бидат заобиколени со невнимателно односно не грижливо постапување на вработените. Типичен случај е кога вработен на својот монитор има залепено лист што содржи список со сите негови лозинки.

Недоволни квалификации на вработените

Во секојдневното користење на информатичката технологија во една организација може да се појават многу недостатоци и грешки. Овие недостатоци и грешки можат да настанат ако одговорните вработени не се доволно квалификувани, свесни и обучени односно имаат застарени познавања на задачите што ги извршуваат, при што тие нема да бидат во можност да ги идентификуваат настаните што се од значење за безбедноста со што би се овозможило нападите да останат неоткриени. Дури и ако вработените се соодветно квалификувани, обучени и свесни за прашањата во врска со безбедноста на информациите, не може да се исклучи можноста дека и тие може да не ги препознаат безбедносните инциденти. Во одредени ситуации (недостиг на кадар или отпуштања), вработените можеби ќе треба привремено да преземат задачи на други вработени, при што може да се случат грешки особено ако вработените ги немаат потребните квалификации или се недоволно обучени за задачите што ги преземаат.

4.2.4. Мерки

Добра регулирана ориентација на новите вработени

Организационата единица за човечки ресурси и раководните лица во организацијата мора да се погрижат вработените да бидат насочени во однос на нивните задачи на почетокот на нивното вработување. Вработените мора да бидат известени за постојните прописи, правила, упатства и процедури. Притоа, како добра практика може да се изготви листа за проверка на работењето на новите вработени лица и да се одреди лице за контакт (ментор).

Регулирана постапка за вработените што ја напуштаат организацијата

Ако некој вработен ја напушти организацијата, неговиот наследник односно вработениот којшто ќе ги преземе неговите задачи мора да биде навремено известен од страна на организационата единица за човечки ресурси. Доколку не постојат услови за директно примопредавање на задачите, вработениот што ја напушта организацијата мора да подготви детална документација за самите задачи што ги извршувал во организацијата. Покрај тоа, вработените што ја напуштаат организацијата мора да ги вратат сите документи, клучеви и уреди, како и картичките за идентификација/евидентирање и овластувањата што ги добиле во врска со задачите. Пред некој вработен да ја напушти организацијата, мора да биде потсетен во однос на неговите обврски за доверливост. Конкретно, треба да се обезбеди дека нема да дојде до судир на интереси, а за да се избегнат вакви судири кога некој почнува со работа на позиција во друга организација, во договорите треба да се вградат и конкурентски клаузули. Покрај тоа, сите засегнати страни во организацијата, како што се вработените за безбедност или за информатичка технологија, исто така мора да бидат известени за вработениот што ја напушта организацијата. Притоа, како добра практика може да се изготви листа за проверка на активностите кои се преземаат кога вработен ја напушта организацијата и да се одреди лице од организационата единица за човечки ресурси, кое ќе го контролира овој процес.

Дефинирање правила за замена

Раководните лица мора да се уверат дека правилата за замена се спроведуваат во секојдневното работење. Ова мора да се направи така што ќе се обезбеди дека постојат функционални правила за замена за сите клучни деловни процеси и задачи. Во однос на овие процеси, обемот на задачите на лицето коешто ќе го заменува вработениот мора однапред да биде јасно утврден. Потоа, мора да се обезбеди дека лицето коешто ќе биде определено да го заменува вработениот го има потребното знаење за извршување на конкретните задачи. Доколку, организацијата не располага со таков кадар, тогаш мора да се размисли како лицето коешто ќе го заменува вработениот да биде обучено за извршување на конкретните задачи. Ако е невозможно да се обучи лице коешто ќе го заменува вработениот од постојниот кадар, тогаш организацијата мора да има воспоставено и правила за ангажирање на надворешни лица за извршување на конкретни задачи како замена.

Дефинирање процедури при користење кадар за определено време

Доколку во организацијата е вработено лице на определено време, тогаш мора од тоа лице да се побара да ги почитува и применува законите, упатствата, правилата и процедурите, како и да добие инструкции за задачите коишто ќе ги извршува на ист начин како и вработените во самата организација. Лицето коешто е вработено на определено време мора да биде надгледувано во областите што се важни за безбедноста во организацијата. Организацијата мора да воспостави правила за замена и за овие вработени лица. При завршување на работниот ангажман или напуштање на организацијата пред истекот на договорот, лицата мора да ги почитуваат и применат воспоставените постапки коишто се однесуваат за вработените што ја напуштаат организацијата.

Договори за доверливост при користење кадар за определено време

Пред да им се одобри пристап до податоци и доверливи информации на лицата вработени на определено време, организацијата мора со нив да склучи договори за доверливост во писмена форма, во кои ќе бидат опфатени сите аспекти што се однесуваат на заштитата на информациите на организацијата.

Задачи и одговорности на вработените

Сите вработени мора да бидат обврзани да ги почитуваат и применуваат законите, упатствата, правилата и процедурите на организацијата. Вработените мора да бидат свесни за правната рамка со која се регулира нивната работа. Задачите и одговорностите на вработените мора да се документираат на соодветен начин. Понатаму, сите вработени мора да бидат известени дека сите информации што ги добиваат во текот на работата се наменети само за внатрешна употреба. Вработените мора да бидат свесни за своите обврски да ја заштитат безбедноста на информациите на својата организација и надвор од работното време и од просториите на организацијата.

Квалификации на кадарот

Вработените мора редовно да се обучуваат и да добиваат можности за понатамошен професионален развој. Во сите области мора да се обезбеди дека ниту еден вработен не работи со „застарено“ знаење. Понатаму, на вработените треба да им се даде можност да стекнат и нови вештини во нивното поле на работа за времетраењето на нивниот работен однос.

При пополнување на работни позиции, организацијата мора јасно да ги наведе потребните квалификации и вештини за секоја позиција. Потоа треба да се провери дали кандидатите за работа ги исполнуваат овие критериуми и притоа мора да се обезбеди дека на позициите се вработуваат квалификувани кадри.

Кадар - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.19	Откривање на информации што треба да се заштитат
3_0.22	Манипулација со информации
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.32	Злоупотреба на овластувања
3_0.33	Недостиг на кадар
3_0.36	Кражба на идентитет
3_0.37	Одредување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.41	Саботажа
3_0.42	Социјален инженеринг
3_0.44	Неовластен влез во простории
3_0.45	Губење податоци

4.3.Свесност и обука за безбедност на информациите

4.3.1.Вовед

Вработените се клучен фактор за обезбедување високо ниво на безбедност на информациите во една организација. Затоа, важно е секој од нив да ги знае безбедносните цели на својата организација, да ги разбере соодветните безбедносни заштитни мерки и да биде подготвен истите да ги спроведе. За ова е потребна свесност за обезбедување на безбедност на информациите во организацијата. Понатаму, треба да се воспостави култура за безбедност на информациите, која ќе претставува активен дел од секојдневната работа на вработените. Вработените треба да бидат свесни за соодветните ризици и да знаат како тие можат да влијаат врз безбедноста на информациите во нивната организација. Вработените мора да знаат што се очекува од нив во однос на безбедноста на информациите и како треба да реагираат во ситуации што се од суштинско значење за обезбедување на безбедноста.

4.3.2.Цел

Целта е да се воспостави и да се одржува ефективна политика за подигнување на свеста на вработените и за спроведување на обуки за безбедност на информациите. Целта на политиката е подигнување на свесноста на вработените за безбедносните ризици и да им се обезбедат знаење и вештини кои се потребни за да ожат да дејствуваат од аспект на безбедноста на информациите.

4.3.3.Закани

Недоволно познавање правила и процедури

Самото дефинирање правила и процедури за безбедност на информациите не гарантира дека тие и ќе се почитуваат. Сите вработени, а особено оние што имаат раководна позиција, мора да бидат запознаени со правилата и процедурите што се применуваат. Иако непочитувањето на правилата и процедурите не е единствената причина за настанување на безбедносни инциденти, сепак тоа е една од причините зошто се случуваат инцидентите. Тешкотиите што произлегуваат од недоволното познавање на правилата и процедурите може да претставуваат закана за нарушување на доверливоста, достапноста и интегритетот на информациите. Ова може да го загрози исполнувањето и извршувањето на деловните процеси и на специјализираните задачи во организацијата.

Недоволна свесност за безбедноста на информациите

Искуството покажува дека не е доволно само да се воспостават безбедносни заштитни мерки. Вработените треба да ја знаат важноста и целта на овие мерки, во спротивно тие би можеле да се игнорираат во секојдневната работа. Доколку вработените не се доволно свесни за прашањата што се однесуваат на безбедноста на информациите, безбедносната култура, безбедносните цели и безбедносната стратегија на нивната организација, организацијата може да биде изложена на ризик при извршувањето на нејзините деловните процеси и задачи.

Неефективни активности за подигнување на свеста и обука

Активностите што се спроведуваат за подигнување на свеста и за обезбедување на обуки за безбедност на информациите, не се секогаш успешни како што се очекувало. Ова може да се должи на следното:

- недостаток на поддршка од највисокото раководство;
- нејасни цели;
- лошо планирање;
- недостаток на следење на ефикасноста;
- недостаток на континуитет;
- недоволни финансиски или кадровски ресурси.

Доколку не се преземат соодветни мерки за да се обезбеди успех на спроведените активности за обука, честопати не е можно да се постигнат нивните цели. Ако организацијата не спроведува доволно активности за да обезбеди свесност и обука на вработените, аспектите на безбедноста на информациите во организацијата може да бидат изложени на ризик при извршувањето на нејзините деловните процеси и задачи.

Недоволна обука на вработените во однос на безбедносните функции

Вработените често не ги применуваат ново воведените безбедносни процедури и мерки, бидејќи не знаат како да управуваат со нив, а учењето како самостојно да ги користат паралелно со нивната секојдневна работна рутина се смета за активност што одзема премногу време. Покрај тоа, недостатокот на обука по воведувањето на новиот софтвер, може да резултира со тоа вработените да работат или да го конфигурираат софтверот погрешно, што ќе предизвика непотребно одложување во работните процеси. Од таа причина, не е доволно само да се купи и да се инсталира (безбедносен) софтвер. Особено во суштинските системи и апликации за информатичка технологија, оперативна грешка може да резултира со последици што ја загрозуваат организацијата при извршувањето на нејзините деловните процеси и задачи.

Неоткриени безбедносни инциденти

Може да се појават многу недостатоци и грешки за време на секојдневното работење на компонентите на информатичката технологија. Во такви случаи, вработените може да не ги идентификуваат безбедносните инциденти како такви и кибер нападите (или поврзаните обиди) може да останат неоткриени. Понекогаш не е лесно да се направи разлика помеѓу безбедносни инциденти и технички грешки. Доколку корисниците и администраторите не се посебно обучени да препознаваат безбедносни инциденти и соодветно да реагираат на нив, ранливостите може да останат неоткриени и да бидат искористени. Доколку безбедносните инциденти се препознаат предочна или воопшто не се препознаат, не може навреме да се преземат соодветни мерки. Малите пропусти во една организација може да прераснат во критични закани за нарушување на доверливоста, достапноста и интегритетот на информациите. Ова може да ги загрози деловните процеси, да предизвика финансиска штета или да доведе до изрекување на санкции на организацијата.

Непочитување на безбедносните заштитни мерки

Голем број причини, какви што се невнимание или расеаност на вработените во една организација, може да доведат до изложеност на доверливи документи на работните места или нивно испраќање без криптирање преку електронска пошта. Дури и навидум мало невнимание може да предизвика штета, а која што добро обучените вработени главно избегнуваат да ја предизвикаат.

Негрижа при ракување со информации

Дури и кога организацијата има воспоставено голем број на организациски и технички безбедносни процедури, тие често се заобиколуваат со негрижа односно невнимание од страна на вработените. Типичен пример за ова е познатото залепено ливче на мониторот од компјутерот на вработениот што содржи список со сите негови лозинки. На ист начин и криптирањето на хард дискот на лаптопот на некој вработен, не го спречува лицето што седи до него во воз да чита доверливи информации од неговиот екран. Дури и најдобрите технолошки безбедносни решенија се бескорисни ако листовите со доверливи информации се оставаат на печатач или завршуваат во лесно достапни корпи за отпадна хартија.

Доколку вработените невнимателно постапуваат со информациите, воспоставените процедури за безбедност на информациите стануваат неефикасни. Неовластени лица можат да ја искористат небрежноста при постапувањето со информациите, на пример, за да извршат насочена индустриска шпионажа.

Недоволно прифаќање на процедурите за безбедност на информациите

Може да има различни причини зошто вработените не ги спроведуваат барањата за обезбедување безбедност на информациите. Таквите причини опфаќаат недостаток на култура за безбедност на вработените во организацијата или ситуација кога највисокото раководство не дава добар пример за нивна примена. Меѓутоа, прекумерните безбедносни барања може да резултираат и со отфрлање односно неприфаќање на безбедносните заштитни мерки од страна на вработените. Во тој случај, може да настанат проблеми кога одредени кориснички права или одреден хардвер или софтвер се гледаат само како статусни симболи во организацијата и ограничувањата во овие процеси може да наидат на значителен отпор од вработените.

Социјален инженеринг

Социјалниот инженеринг е метод што се користи за да се добие неовластен пристап до информации или до системите за информатичка технологија преку прислушување на вработените во една организација. Кај социјалниот инженеринг, напаѓачот главно воспоставува директен контакт со жртвата (на пример, преку телефон, преку електронска пошта, па дури и на социјалните мрежи). Нападите со користење социјален инженеринг често се состојат од неколку фази. Со симулирање внатрешни сознанија и истовремено повикување на подготвеноста на вработениот да помогне, напаѓачот може да ги прошири своите сознанија во однос на организацијата, чекор по чекор. Доколку вработените не се доволно свесни за овој тип на напад, тие би можеле да бидат изманипулирани за извршување неовластени задачи преку вешто убедување. Ова може да доведе до ситуација вработените да пренесат внатрешни информации, да се заразат нивните системи за информатички технологии со злонамерен софтвер, па дури и да се префрлаат пари на наводни деловни партнери на организацијата. Во случај на измама на раководно лице на организацијата, на пример, се поттикнуваат вработените на кои им е дозволено да префрлаат пари во име на организацијата, да веруваат дека имаат фиктивна наредба од своето раководно лице, со која им е кажано да извршат трансакции за наводно итен и доверлив договор, кој е од клучно значење за непречено работење на организацијата.

4.3.4. Мерки

Свесност на највисокото раководство за прашањата што се однесуваат на безбедноста на информациите

Највисокото раководство на организацијата мора да биде доволно свесно за безбедносните прашања. Безбедносните кампањи и активности за обука мора да бидат поддржани од највисокото раководство. Поддршката од највисокото раководство мора да се добие пред воспоставување на процедура за подигнување на свеста на вработените и за спроведување на обуки за безбедност на информациите. Сите раководни лица мора да ги поддржат и применат мерките за обезбедување безбедност на информациите и со тоа да дадат добар пример на вработените. Раководните лица мора да ги имплементираат сите безбедносни барања на организацијата. Покрај тоа, тие мора да ги известат своите вработени за нивните обврски за почитување и применување на мерките за обезбедување безбедност на информациите.

Обука на вработените за безбедно ракување со информатичка технологија

Сите вработени и ангажирани лица (лица вработени на определено време) мора да бидат обучени и свесни за безбедното ракување со компонентите на информатичката технологија, доколку тоа е важно за нивната работа. За таа цел, мора да бидат достапни обврзувачки, јасни и ажурирани процедури за користење на соодветните компоненти на информатичката технологија. Доколку информатичката технологија се користи на начин што е спротивен на интересите на организација, тоа мора да биде соопштено од страна на вработените и ангажираните лица на највисокото раководство.

Дизајнирање и планирање процедури за подигање на свеста и обуки за безбедноста на информациите

За определени целни групи на вработени треба да се дизајнираат процедури за подигање на свеста и обуки за безбедност на информациите. За таа цел, претходно треба да се изврши анализа на потребите на организацијата, како и на барањата на вработените. Планираните обуки треба да се фокусираат на специфичните барања и на различните потреби за обука на вработените. Во организацијата треба да се креира процедура за подигање на свеста и обуки ориентирани кон определените целни групи на вработени на тема безбедност на информациите. Оваа процедура за обуки треба да им ги обезбеди на вработените сите информации и вештини што им се потребни за спроведување на безбедносните правила и процедури, како и за заштитните мерки што се применуваат во организацијата. Процедурата треба редовно да се проверува и да се ажурира. Сите вработени треба да следат обука за безбедност на информации во согласност со нивните задачи и одговорности во организацијата.

Мерење и евалуација на успехот на обуката

Успехот на обуката за безбедност на информации треба да се мери и да се евалуира (проценува) според определените целни групи, со цел да се одреди степенот до кој се постигнати целите што се утврдени во процедурите за подигање на свеста и обуки за безбедност на информациите. При мерењата треба да се земат предвид и квантитативните и квалитативните аспекти на процедурите за подигање на свеста и обуки за безбедност на информациите. Резултатите треба да се користат за да може да се подобри постојната процедура за свесност и обуки. Овластеното лице за безбедност на информации треба редовно да разменува информации со организационата единица за човечки ресурси и со другите лица за контакт што се значајни за безбедноста (заштита на личните податоци, здравје и безбедност, превенција од пожари итн.), за ефективност на обуките и активностите кои треба да се преземат за нивен понатамошен развој.

4.3.5.Напредни мерки

Специјална обука за директно вклучени лица од организацијата

Особено директно вклучени лица за обработка на информации треба да следат специјализирани обуки во однос на можните закани и ризици на безбедноста на информациите, како и соодветното ракување со тие информации и применување на безбедносни заштитни мерки.

Подигнување на свеста и обуки за безбедност на информации - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.24	Уништување на уреди или медиуми за чување податоци
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одрекување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.42	Социјален инженеринг
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.4.Откривање настани што се важни за безбедноста

4.4.1.Вовед

За да се заштитат системите за информатичка технологија, мора да се откријат настаните што се значајни за безбедноста и навремено да се постапи во однос на таквите настани. За таа цел, организацијата мора однапред да ги планира и применува организациските, кадровските и техничките заштитни мерки, како и редовно да го обучува својот кадар. Кога една организација има утврден и тестиран метод на кој се темели, таа може да го скрати времето на одговор и да ги оптимизира постојните процеси.

Терминот „настан што е значаен за безбедноста“ се однесува на настан што влијае врз безбедноста на информациите или може да ја наруши доверливоста, интегритетот и достапноста на информациите. Вообичаените последици од таквите настани вклучуваат пресретнување на комуникацијата, манипулирање или уништување информации. Причините за ова се многубројни, како злонамерниот софтвер, наследената системска инфраструктура или внатрешните напаѓачи може да имаат одредена улога. Сепак, напаѓачите честопати ги користат и недостатоците на софтверот што претходно не биле познати, односно недостатоци во програмите што сè уште не се поправени или подобри. Друга опасност што треба да се сфати сериозно е поврзана со напредните постојани закани. Тоа се насочени сајбер напади врз организацијата во кој напаѓачот добива постојан пристап до мрежата и последователно го проширува овој пристап до другите системи за информатичка технологија. Ваквите упади честопати тешко се откриваат и се карактеризираат со многу голем обем на искористени ресурси, како и со значителни технички вештини на напаѓачите.

4.4.2.Цел

Овој процес претставува систематски начин на кој информациите може да се прибираат, заемно да се споредуваат и да се поврзуваат, како и да се оценуваат за да се откријат настаните што се значајни за безбедноста на информациите што е можно поцелосно и навремено. Наодите што се добиени во рамките на откривањето, потоа треба да ја подобрат способноста на организацијата да открива и соодветно да одговори на настаните што се значајни за безбедноста на информациите. Тоа вклучува основни спецификации што мора да се земат предвид и да се исполнат кога се откриваат настани во врска со безбедноста. Овие барања во голема мера зависат од евиденцијата за секој пристап односно кои податоци ги содржи таа евиденција. Кога се поставуваат основите за откривање настани што се значајни за безбедноста, важно е одговорностите и надлежностите да бидат јасно утврдени и доделени. Посебно внимание треба да се посвети на начелото на поделба на должностите на вработените во организацијата.

4.4.3.Закани

Не земање предвид на законските одредби и правата на вработените од аспект на работниот однос

Софтверските програми што откриваат настани што се значајни за безбедноста и ги евалуираат евидентираните податоци за пристап, често собираат голем број информации за мрежната структура и за внатрешните процеси на организацијата. Ова може да вклучува сензитивни информации какви што се лични или доверливи податоци или податоци поврзани со извршувањето на работните процеси на вработените. Меѓутоа, бидејќи таквите податоци можат да се чуваат, може да се нарушат како личните права на вработените, така и нивните права од аспект на работниот однос. При одредени околности, организацијата исто така може да ги прекрши и прописите за заштита на личните податоци.

Недоволни квалификации на вработените

За време на секојдневните операции на организацијата, може да се појават многу пропусти и грешки, како што е ненадејно, драстично зголемување на дојдовните евидентирани податоци за пристап. Доколку одговорните вработени не се доволно свесни или обучени, тие може да не ги идентификуваат настаните што се значајни за безбедноста и на тој начин да дозволат нападот да остане незабележан. Дури и ако вработените се свесни и обучени за прашања во врска со безбедноста на информациите, тие сепак може да не ги препознаат безбедносните инциденти. Треба да се имаат предвид следните примери:

- Корисник што долго време не се најавил на локалната мрежа на организацијата, не смета дека е невообичаено што неговиот лаптоп е значително побавен додека пристапувал на интернет во период од една недела. Корисниците не забележуваат дека во заднина има активна злонамерна програма. Корисникот очигледно не бил соодветно обучен да препознава сомнителни активности и соодветно да го информира овластеното лице за безбедност на информации.
- Раководителот за производство не забележува дека податоците во системите за контролен приказ прикриено се променети. Тој не се сомнева во ништо кога самиот произведен систем прикажува необични вредности бидејќи тоа се случува само за краток временски период. Инцидентот не е пријавен бидејќи сите прикажани вредности се вратиле во нормала. Како последица на тоа, никој не забележува дека злонамерен софтвер манипулирал со вредностите на екранот.

Неправилно администрирање на системите за откривање настани што се важни за безбедноста

Неправилните конфигурации може да спречат правилна работа на системите за откривање настани важни за безбедноста. На пример, доколку поставките за аларм се неточни, тоа може да доведе до повеќе лажни аларми. Ова може да ги спречи одговорните вработени да направат разлика помеѓу лажен аларм и настан што е значаен за безбедноста. Понатаму, тие можеби нема да ги забележат пораките доволно брзо бидејќи се случуваат премногу аларми. Како резултат на тоа, нападите може да останат незабележани. Времето што е потребно за анализа на сите пораки исто така значително ќе се зголеми.

Недостиг на информации во врска со доменот на информации што треба да се заштитат

Немањето доволно информации за доменот на информации што треба да се заштитат носи ризик суштинските области од доменот на информации да не бидат доволно заштитени со системите за откривање настани што се важни за безбедноста. Како последица на тоа, напаѓачите може лесно да навлезат во мрежата на организацијата и да пристапат до сензитивни информации. Тие може да останат во системот подолг временски период и да пристапат до мрежата без тоа да биде забележано.

Недоволно користење системи за откривање настани што се важни за безбедноста

Ако не се користат ниту системите за откривање настани што се важни за безбедноста, ниту функциите што се достапни во системите за информатичка технологија и апликациите за откривање настани што се значајни за безбедноста, напаѓачите може полесно да навлезат во мрежата на организацијата без тоа да биде забележано и да пристапат до сензитивни информации без овластување. Недоволното следење на границите помеѓу мрежите е од клучно значење.

Недоволни кадровски ресурси

Доколку нема доволно кадар за анализа на евидентирани податоци за пристап, настаните што се значајни за безбедноста може да не бидат целосно откриени. Како последица на тоа, нападите може да останат незабележани подолг временски период или да бидат откриени само откако ќе бидат компромитирани голем број сензитивни информации. Доколку надворешните извори на информации не се евалуирани поради недоволни кадровски ресурси, недостатоците може да останат нерешени премногу долго. Потоа, напаѓачите може да ги искористат за да добијат неовластен пристап до системите за информатичка технологија на организацијата.

4.4.4. Мерки

Дизајнирање безбедносна процедура за откривање настани што се важни за безбедноста

Врз основа на општата безбедносна политика на организацијата, мора да се подготви конкретна безбедносна процедура за откривање настани што се важни за безбедноста. Оваа конкретна безбедносна процедура мора разбирливо да ги опишува барањата и спецификациите за тоа како да се планираат, постават и безбедно да се управува со методите за откривање настани што се важни за безбедноста. Оваа конкретна безбедносна процедура мора да им биде позната на сите вработени што се одговорни во полето на откривање настани и да служи како основа за нивната работа. Доколку се промени конкретната безбедносна процедура или има отстапувања од нејзините барања, тоа мора да се договори и да се документира со овластеното лице за безбедност на информации. Спроведувањето на оваа конкретна безбедносна процедура мора редовно да се прегледува, при што резултатите од проверките мора да се документираат во разбирлива форма.

Усогласеност со законските услови при анализа на евидентираниите податоци за пристап

При анализа на евидентираниите податоци за пристап, мора да се применуваат прописите за заштита на личните податоци. Доколку се користат системи за откривање на настани, мора да се почитуваат личните права на вработените, како и нивните права од аспект на работниот однос. Притоа, мора да се обезбеди дека се земени предвид и сите дополнителни законски одредби што се применуваат во работењето на организацијата.

Дефинирање на канали за известување и предупредување за настани што се важни за безбедноста

Предвидените канали за извештаи и предупредувања, мора да бидат дефинирани и документирани за откривање на настани што се важни за безбедноста. Организацијата мора да утврди лица за контакт кои мора да бидат информирани за кои случаи се задолжени и на кој начин да постапуваат. Настанот што е важен за безбедноста мора да се пријави со користење различни комуникациски канали во зависност од итноста. Сите засегнати лица во врска со известувањето и предупредувањата мора да бидат информирани за нивните задачи. Сите чекори од процесот на известување и предупредување мора детално да се опишат. Воспоставените канали за известување и предупредување треба да се прегледуваат, да се тестираат и да се ажурираат редовно и по потреба.

Подигање на свеста на вработените

На сите корисници мора да им се укаже едноставно да не ги игнорираат или да не ги затвораат пораките за настани што ги прикажуваат нивните клиенти. Секој корисник мора да ги користи пропишаните канали за предупредување за да пренесува пораки до одговорните лица за управување со инциденти. Секој вработен мора веднаш да пријави безбедносен инцидент што го открил на овластеното лице за управување со инциденти.

Користење на функциите за откривање на настани што се вклучени во системите

Доколку системите за информатичка технологија или апликациите имаат функции што може да се користат за откривање настани во врска со безбедноста, тие мора да се овозможат и да се употребат. Ако се случи настан што е важен за безбедноста, пораките на засегнатите системи за информатичка технологија мора да се евалуираат, како и да се проверат и евидентираниите настани на другите системи за информатичка технологија. Покрај тоа, собраните пораки треба да се проверуваат по случаен избор на задолжителни временски интервали. Мора да се провери дали треба да се инсталираат дополнителни скенери за малициозни кодови на централните системи за информатичка технологија. Доколку се користат дополнителни скенери за малициозен софтвер, тие мора да овозможат нивните пораки и записи да се оценуваат преку централна пристапна точка. Мора да се обезбеди дека скенерите на малициозни кодови автоматски ќе ги пријават настаните во врска со безбедноста на одговорните лица, а кои лица ќе мора да ги проценат и да ги испитаат овие пораки.

Континуирано следење и анализа на евидентираниите податоци за пристап

Сите евидентирани податоци треба активно да се следат и да се анализираат колку што е можно почесто. Вработените кои се одговорни за овие активности односно во случај кога треба активно да бараат настани во врска со безбедноста што се случиле (на пример, при тестирање или следење системи за информатичка технологија), таквите задачи треба да ги документаат според воспоставените инструкции за процесот. Организацијата треба да обезбеди доволно кадровски ресурси за откривање настани во врска со безбедноста.

Обука на одговорни лица

Лицата што се одговорни за прегледување на пораките за настаните треба да добијат напредна обука и дополнителни квалификации. Кога се набавуваат нови компоненти на информатичка технологија, треба да се планира и буџет за спроведување на обуки на одговорните лица. Концептот за овие обуки, треба да биде јасно дефиниран пред да започне самиот процес на обука на одговорните лица за новите компоненти на информатичката технологија.

Користење на дополнителни системи за откривање на настани

Организацијата треба планот за мрежите да го користи за да одреди кои мрежни сегменти треба да се заштитат со дополнителни системи за откривање на настани. Во доменот треба да се додадат информации за дополнителните системи за откривање на настани и сензори. Системите за откривање малициозни кодови треба да се користат и да се администрираат од централна локација. Поврзаноста помеѓу внатрешните и надворешните мрежи што е дефинирана во планот за мрежите треба да се надополни со мрежни системи за откривање упад.

Употреба на TLS/SSH посреднички (прокси) системи

При премини кон надворешни мрежи, треба да се користат TLS/SSH посреднички (прокси) системи за да се прекинат криптираните врски и да се овозможи проверка на податоците што се пренесуваат за злонамерен софтвер. Сите TLS/SSH посреднички (прокси) системи треба да бидат заштитени од неовластен пристап. Настаните што се важни за безбедноста, треба да се откријат автоматски на TLS/SSH посреднички (прокси) системи. Организација треба да донесе процедура со која се одредува како евидентираниите податоци ќе може рачно да се евалуираат во согласност со прописите за заштита на личните податоци.

Употреба на централна инфраструктура за евидентирање на секој пристап за да се евалуираат настаните што се важни за безбедноста

Пораките за настани што се генерирани од системите за информатичка технологија и апликациите и се зачувани на централна инфраструктура за евидентирање, треба да може да се вратат со помош на алатка. Избраната алатка треба да може да ги анализира пораките односно на редовни временски интервали треба да се врши проверка на овие собрани пораки. Записите од употребените системи за откривање на настани треба секогаш идентично да бидат прикажани и ажурирани, така што настаните што се важни за безбедноста да може да се откриваат и ретроспективно.

Евалуација на информации од надворешни извори

Надворешните извори треба да се користат за да се добијат нови сознанија за настаните што се важни за безбедноста, кои би можеле да влијаат врз доменот на информации на организацијата. Пораките од различните канали треба да бидат препознаени како значајни од вработените и проследени до точните примачи (овластени лица од организацијата). Информациите од сигурните извори треба да се евалуираат како општо правило. Сите примени информации треба да се евалуираат во однос на тоа дали се важни за доменот на информации на организацијата. Доколку е така, треба да се зголеми обемот на информации во согласност со процедурите кои се однесуваат на управувањето со безбедносни инциденти.

Редовни контроли на системите за откривање на настани што се важни за безбедноста

Системите за откривање и заштитните мерки на организацијата треба редовно да се контролираат за да се провери дали истите се ажурирани и ефективни. Проценетите вредности треба да ги вклучуваат оние вредности кои укажуваат колку често се евидентираат и се соопштуваат настаните што се важни за безбедноста и нивниот зголемен обем. Резултатите од контролите треба да се документираат и да се споредат со целите на организацијата, како и да се констатираат и испитаат отстапувањата од тие цели, при што истите треба транспарентно да бидат достапни.

4.4.5. Напредни мерки

Евалуација на евидентираниите податоци од страна на специјализиран кадар

Организацијата треба да има посебно определени вработени лица кои ќе ги следат сите видови на евидентирани податоци. Следењето на евидентираниите податоци треба да им биде главна задача на овие вработени лица. Определените вработени лица треба да посетат специјализирана дополнителна обука за да се стекнат со квалификации кои се потребни за овој процес. Исто така, организацијата треба да има определено и посебна група на вработени лица кои ќе бидат исклучиво одговорни за евалуација на евидентираниите податоци.

Централно откривање и испитување во реално време на пораки за настани

Централните компоненти треба да се користат за откривање и евалуирање на настани во врска со безбедноста. Треба да се вршат централизирани и автоматизирани анализи со помош на софтверски алатки. Овие централни и автоматизирани анализи засновани на софтверски алатки, треба да се користат за евидентирање и за поврзаност на сите настани што се случуваат во системската околина. Преку овие алатки треба да биде можно непречено да се прегледуваат и да се евалуираат сите податоци што се добиени во системот за администрирање на евиденцијата. Податоците треба да се анализираат што е можно почесто. Доколку се надминат утврдените вредности на прагот во системот, треба автоматски да се вклучи аларм. Засегнатите вработени лица треба да се уверат дека алармот активира квалификуван одговор, кој е соодветен на прифатената ситуација. Во овој контекст, засегнатото вработено лице исто така треба веднаш да биде информирано. Овластените вработени лица за системот треба да вршат контрола и (доколку е потребно) да ги приспособуваат параметрите за анализа на редовни временски интервали. Покрај тоа, податоците што се веќе контролирани, треба редовно автоматски да се испитуваат за настани што се важни за безбедноста. Процесите што се важни за безбедноста треба да бидат транспарентни.

Употреба на системи за откривање во согласност со барањата за заштита

Апликациите со повисоки потреби за заштита треба да бидат заштитени со дополнителни заштитни мерки за откривање на настани што се важни за безбедноста. За таа цел, организацијата треба да користи системи за откривање со кои може да се гарантира дека повисоките потреби за заштита се исполнети од технички аспект.

Автоматска реакција на настани што се важни за безбедноста

Доколку се случи настан што е важен за безбедноста, системите за откривање кои организацијата ги користи треба автоматски да го пријават настанот и да реагираат со соодветни безбедносни заштитни мерки. Во тој процес треба да се користат методи што автоматски откриваат можни напади, обиди за злоупотреба или прекршување на безбедноста. Исто така во тој процес треба да биде можно автоматски да се интервенира во протокот на податоци за да се спречи можен безбедносен инцидент.

Вршење редовни проверки на интегритетот

Интегритетот на сите системи за откривање, организацијата треба редовно да ги проверува. Исто така треба да се проверуваат и доделените кориснички права на пристап. Дополнително, сензорите што се користат треба редовно да го проверуваат интегритетот на датотеките, при што треба да се вклучи автоматски аларм доколку се променат одредени вредности.

Откривање настани што се важни за безбедноста - закани што се вклучени овде:	
3_0.18	Лошо планирање или недостаток на приспособување
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.33	Недостиг на кадар
3_0.37	Одрекување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.5. Постапување со безбедносен инцидент**4.5.1. Вовед**

Организацијата за да ја ограничи штетата и да ги избегне дополнителните несакани последици, откриените безбедносни инциденти треба да ги решава брзо и ефикасно. За таа цел, неопходно е да се воспостави дефиниран и тестиран метод за постапување со безбедносни инциденти (исто така познато како постапување со безбедносен инцидент или одговор на безбедносен инцидент). Безбедносниот инцидент може да има значителни влијанија врз организацијата и да предизвика голема штета. Примери за такви инциденти вклучуваат нарушување на безбедноста на податоците за што може да биде потребно дополнително известување, но и неточни конфигурации што предизвикуваат откривање доверливи информации или криминални дејства какви што се напади на сервери, кражба на доверливи информации, саботажа или уцена во врска со информатичката технологија. Причините за безбедносни инциденти се повеќекратни и може да вклучуваат злонамерен софтвер, застарени системски инфраструктури или внатрешни напаѓачи. Напаѓачите често ги искористуваат и предностите што произлегуваат од недостатоците на софтверот кои претходно не биле познати, односно од недостатоците во програмите што сè уште не се поправени или подобрени. Друга закана што треба да се сфати сериозно е поврзана со напредните постојани закани.

Понатаму, корисниците, администраторите или надворешните даватели на услуги може да се однесуваат несоодветно, како, на пример, со менување на параметрите на системот на начин што е од клучно значење за безбедноста или со прекршување на внатрешните процедури на организацијата. Други веродостојни причини вклучуваат повреда на правата за пристап, промени во софтверот или во хардверот или недоволна заштита на сензитивните простории и објекти на организацијата.

4.5.2.Цел

Целта на овој процес е организацијата да демонстрира системски начин на дизајнирање на концептот за постапување со безбедносен инцидент.

4.5.3.Закани

Несоодветно постапување со безбедносни инциденти

Во практика, невозможно е целосно да се отстрани можноста за појава на безбедносни инциденти. Ова важи дури и кога се спроведуваат голем број на безбедносни заштитни мерки. Со оглед на тоа, несоодветното реагирање односно одговор на акутни безбедносни инциденти (или воопшто нереагирање) може да резултира со голема штета со значителни последици за организацијата. Треба да се имаат предвид следните примери:

- Во датотеките од записи на заштитниот сид се најдени сомнителни записи. Доколку нема навремено испитување дали ова е првиот знак за можен упад, напаѓачите можат успешно да го надминат заштитниот сид без да бидат забележани и да навлезат во внатрешната мрежа на организацијата.
- Се појавуваат безбедносни недостатоци во системите и апликациите за информатичка технологија што ги користи организацијата. Доколку организацијата не ги добие овие информации навремено и не успее брзо да ги преземе потребните мерки за заштита, напаѓачите може да ги искористат овие недостатоци.
- Се претпоставува дека кражбата во една подружница на организацијата е криминал поврзан со дрога бидејќи единствените предмети што биле украдени биле лаптопите и мониторите со рамен екран. Фактот дека доверливите информации и податоците за пристап за системите за информатичка технологија во интранетот на организацијата биле зачувани на лаптопите не се сметал за важен. Поради тоа, не било информирано овластеното лице за безбедност на информации. Како резултат на тоа, организацијата не е подготвена за последователни напади врз системите за информатичка технологија на нејзиното седиште и на другите нејзини локации. За нападите биле искористени податоците што се пронајдени на украдените лаптопи.

Во итни и многу стресни ситуации, може да се донесат лоши одлуки доколку нема пропишана процедура за постапување со безбедносни инциденти. Ваквите одлуки може да доведат, на пример, до погрешно информирање на јавноста. Покрај тоа, трети лица може да претрпат штета од системите за информатичка технологија на организацијата и да бараат соодветен надомест на штета. Ако засегнатата организација не предвидела заштитни мерки за враќање на претходен режим на работа или за подобрување, штетата што ќе ја претрпи ќе биде значително поголема.

Уништување докази при постапување со безбедносни инциденти

Доколку со безбедносниот инцидент се постапува невнимателно или се занемарат воспоставените мерки, важните докази за истражување на инцидентот или за поведување на судска постапка може ненамерно да се уништат или да се влијае врз нив така што ќе бидат несоодветни за овие постапки.

Треба да се имаат предвид следните примери:

- Напаѓачот заразува клиент со злонамерен софтвер чиј начин на работа и цел може да се анализираат само кога системот работи. За оваа анализа, информациите за активните процеси и за содржината на главната меморија мора да бидат зачувани и евалуирани. Ако клиентот предвреме се исклучи, информациите повеќе не може да се користат за да се анализира и да се дојде до почетната точка на безбедносниот инцидент.
- Администраторот наоѓа активен процес на сервер што предизвикува исклучително оптоварување на централната обработувачка единица. Покрај тоа, овој процес создава привремени датотеки и испраќа непознати информации преку интернет. Ако процесот е предвреме прекинат и привремените датотеки едноставно се избришат, нема да може да се открие дали се украдени доверливи информации.

- Важен сервер станува компромитиран бидејќи администраторот не можел да ги инсталира најновите безбедносни ажурирања како што било планирано поради големото оптоварување на серверот и недостатокот на бесплатен период за превентивно одржување. За да се избегнат можни дисциплински мерки, администраторот ги инсталира ажурирањата што недостасуваат пред безбедносниот тим да може да го анализира изворот на упадот и штетата што произлегува од него. Оттука, културата на работното место со ниска толеранција за грешките на вработените ја спречила анализата на проблемот.

4.5.4. Мерки

Дефинирање безбедносен инцидент

Во рамките на организацијата, значењето на терминот „безбедносен инцидент“ мора да биде јасно дефиниран. Безбедносниот инцидент мора да се разликува од прекините за време на секојдневните операции на организацијата секогаш кога тоа е можно. Сите вработени што учествуваат во постапувањето со безбедносни инциденти мора да бидат запознаени со значењето на терминот „безбедносен инцидент“. Дефиницијата и праговите на појава на таквите инциденти треба да се базираат на потребите за заштита на засегнатите деловни процеси, системите за информатичка технологија и апликациите.

Донесување процедура за постапување со безбедносни инциденти

Организацијата мора да има донесено процедура за постапување со безбедносни инциденти. Со оваа процедура мора да се дефинираат нејзината намена и цел, како и да се регулираат сите аспекти на постапувањето со безбедносни инциденти. Затоа, мора да се опфатат сите процеси за постапување со различните видови безбедносни инциденти. Освен тоа, мора да има и упатства кои ќе бидат насочени кон целните групи и практични упатства за сите вработени. Понатаму, треба да се имаат предвид и релациите со другите области на управување, вклучително и во управувањето со обезбедувањето на континуитет на деловното работење во организацијата. Сите вработени мора да бидат запознаени со процедурата. Таа мора да биде изработена во соработка со вработените за информатичка технологија и да биде одобрена од највисокото раководство на организацијата. Процедурата мора редовно да се прегледува и да се ажурира.

Дефинирање одговорности и лица за контакт во случај на безбедносни инциденти

Од страна на организацијата мора да бидат јасно дефинирани задачите и одговорностите за сите вработени што треба да се применуваат во случај на безбедносни инциденти. Конкретно, вработените што ќе постапуваат со безбедносните инциденти мора да бидат информирани за своите задачи и одговорности. Во овој контекст, мора да се дефинира кој ќе ја донесе евентуалната одлука за потребата за форензичко вештачење, критериумите што треба да се следат при неговото спроведување и кога тоа треба да се случи. Вработените мора да ги знаат лицата за контакт за сите видови безбедносни инциденти. Информациите за контакт мора секогаш да бидат ажурирани и лесно достапни.

Известување за субјекти што се засегнати од безбедносни инциденти

Во организацијата кога ќе се случи безбедносен инцидент, сите засегнати внатрешни и надворешни субјекти мора веднаш да бидат информирани за инцидентот. Во овој процес мора да се провери дали мора да се консултираат офицерот за заштита на личните податоци, највисокото раководство и вработените за правни прашања. Исто така, мора да се земат предвид и обврските за известување на надлежните органи и институции согласно закон. Понатаму, организацијата мора да гарантира дека засегнатите (внатрешни и надворешни) субјекти се известени за активностите што треба да ги преземат.

Активности за решавање на безбедносни инциденти

За да биде успешно решен еден безбедносен инцидент, одговорното лице мора првично да го спречи проблемот или понатамошното интензивирање на проблемот и да ја најде причината. Потоа мора да ги избере заштитните мерки што се потребни за да се реши проблемот. Овластеното лице кое раководи со операциите за информатичка технологија мора да ги одобри заштитните мерки пред да бидат истите имплементирани за решавање на проблемот. Потоа мора да се отстрани причината и да се воспостави безбедна состојба. Во организацијата мора да постои ажуриран список на внатрешни и на надворешни безбедносни експерти што може да се консултираат во случај на безбедносни инциденти за да одговорот на прашањата од засегнатите области, како и да се воспостават безбедни методи за комуникација со овие експерти.

Враќање на работната околина по безбедносни инциденти

По безбедносен инцидент, засегнатите компоненти мора да се отстранат од мрежата. Освен тоа, мора да се направи сигурносна копија на сите потребни податоци што би можеле да дадат информации за природата и причината за проблемот. Мора да се провери дали има промени на оперативните системи и на сите апликации на сите засегнати компоненти. Оригиналните податоци мора повторно да се инсталираат од медиум за чување податоци со заштита од промена или бришење. Притоа, мора да се имплементираат и сите конфигурации и софтверски поправки во врска со безбедноста. Ако податоците од сигурносните копии повторно се внесуваат, мора да се обезбеди дека овие податоци не биле засегнати од безбедносниот инцидент. По нападот, сите податоци за пристап на засегнатите компоненти мора да се променат пред да се стават повторно во функција. Засегнатите компоненти треба да подложат на пенетрациско тестирање пред повторно да се употребат.

При враќање на безбедната работна околина, корисниците мора да бидат вклучени во функционалните тестови на апликациите. Откако ќе се врати сè, компонентите (вклучувајќи ги и мрежните премини) мора насочено да се следат.

Воспоставување процедура за постапување со безбедносни инциденти

Организацијата треба да воспостави процедура за постапување со безбедносни инциденти. Во процедурата треба да бидат јасно утврдени и документирани сите аспекти на постапување со различните видови безбедносни инциденти. Највисокото раководство на организацијата треба да ја спроведе оваа процедура и да ја направи достапна за сите засегнати страни. Исто така, организација треба да врши редовни проверки за да обезбеди дека процедурата е тековно ажурирана и ефективна, како и по потреба истата да ја менува.

Дизајнирање организациски структури за постапување со безбедносни инциденти

Организацијата треба да дефинира соодветни организациски структури за постапување со безбедносни инциденти. За таа цел треба да се формира тим за безбедносни инциденти, со членови што можат да бидат повикани во зависност од видот на инцидентот. Дури и ако тимот за безбедносни инциденти се состанува само кога ќе се случи конкретен инцидент, треба однапред да се определат соодветни членови и да се упатат како да ги извршуваат своите задачи. Организацијата треба да врши редовни проверки за да обезбеди дека составот на тимот за безбедносни инциденти сè уште е соодветен, како и по потреба да направи негови промени.

Дефинирање канали за известување за безбедносни инциденти

Организација треба да воспостави канали за известување, кои се соодветни за различните видови безбедносни инциденти. Овие канали треба да обезбедат брзо и лесно пријавување на безбедносни инциденти од вработените лица со користење на сигурни и доверливи канали. Доколку се воспостави централна контактна точка за пријавување проблеми или безбедносни инциденти, тоа треба да им биде соопштено на сите вработени лица. Исто така, во организацијата треба да постои стратегија за комуникација и контакт. Со оваа стратегија треба да се дефинира кој мора да биде информиран, кој може да биде информиран, кој е одговорен за постапување со соодветниот настан и по кој редослед, како и степенот на детали на информации кои ќе треба да се дадат за настанот. Исто така, треба да се прецизира кој ќе ги пренесува информациите за безбедносни инциденти на трети лица, како и да се обезбеди дека неовластени лица нема да испраќаат информации за безбедносните инциденти.

Ограничување на влијанијата од безбедносните инциденти

За време на анализата на основната причина за безбедносен инцидент, треба да се донесе одлука дали е поважно да се ограничи предизвиканата штета или да се реши инцидентот. Притоа, треба да бидат достапни доволно информации за да може да се проценат влијанијата од безбедносниот инцидент. Исто така, за одредени сценарија на безбедносен инцидент, организацијата треба однапред да се подготви за најлошиот можен случај.

Класификација на безбедносни инциденти

Организацијата треба да дефинира процедура за класификација на безбедносни инциденти и нарушувања. Оваа процедура треба да се координира помеѓу организационата единица за управување со безбедноста и организационата единица за управување со проблеми (инциденти).

Дефинирање на тоа каде постапувањето со безбедносен инцидент се преклопува со управувањето со проблеми (инциденти)

Организацијата треба да ги анализира релациите меѓу управувањето со проблеми, управувањето со обезбедување на континуитет на деловното работење и управувањето со безбедноста. Притоа, треба да се дефинираат и ресурсите што овие области би можеле да ги користат заедно. Вработените лица што учествуваат во управувањето со проблеми треба да бидат свесни за прашањата кои се поврзани со постапувањето со безбедносни инциденти и управувањето со обезбедување на континуитет на деловното работење. Раководството за управување со безбедност треба да има пристап до користените алатки за управување со инциденти, при што со пристапот се овозможува само читање.

Интеграција во управувањето со безбедноста и обезбедување континуитет на деловното работење

Постапувањето со безбедносните инциденти треба да се координира и со управувањето со обезбедување континуитет на деловното работење. Ако во организацијата веќе е воспоставена посебна функција (улога) за управување со проблеми и ова лице треба да биде вклучено во овие активности.

Стратегија за ескалација за безбедносни инциденти

Во организацијата треба да се предвиди и стратегија за ескалација, во која се опфатени веќе воспоставените процедури за комуникација и контакт за безбедносни инциденти. Оваа стратегија за ескалација треба да се координира меѓу вработените лица што се одговорни за управување со проблеми и управување со безбедноста на информациите. Истата треба да содржи јасни упатства за тоа кој, како и кога треба да се вклучи за секој тип препознатлив или сомнителен безбедносен инцидент. Воедно, треба да се дефинираат заштитните мерки што треба да се применат по ескалацијата и како засегнатите лица треба да реагираат. Организацијата треба да избере соодветни софтверски алатки во функција на дефинираната стратегија за ескалација. Тие алатки треба да бидат соодветни и за обработка на доверливи информации и треба да се обезбеди дека истите ќе бидат достапни и за време на безбедносни инциденти и итни случаи.

Стратегијата за ескалација треба редовно да се проверува и по потреба да се ажурира. Листите за проверка со соодветни сценарија за управување со проблеми, треба да се надополнуваат со области што се значајни за безбедноста и редовно да се ажурираат. Дефинираните канали на ескалација треба да се тестираат со помош на редовни вежби.

Обука на вработени во организационата единица за контакт со клиенти

Вработените во организационата единица за контакт со клиенти, треба да располагаат со соодветни алатки што ќе им овозможат да идентификуваат безбедносни инциденти. Тие треба да бидат доволно обучени за да ги користат самите алатки. Вработените во организационата единица за контакт со клиенти треба да бидат запознаени со потребите за заштита на соодветните системи за информатичка технологија.

Документација за решавање безбедносни инциденти

Организацијата треба да го има документирано процесот на решавање на безбедносни инциденти во согласност со стандардизираната процедура. Сите извршени активности и временскиот период кога се преземени активностите треба да се документираат заедно со евидентираните податоци на засегнатите компоненти. Притоа, треба да се гарантира доверливост при документирањето на информациите и архивирањето на извештаите.

Потребните информации треба да се внесат во соодветните системи за документација пред да се смета дека е решен безбедносниот инцидент. Потребните барања за обезбедување квалитет треба однапред да се дефинираат со овластеното лице за безбедност на информации.

Евалуација на безбедносни инциденти

Организацијата треба безбедноските инциденти да ги евалуира на стандардизиран начин, за да може и да се процени колку брзо се откриваат и решаваат инцидентите. Воедно, треба да се провери дали функционирале каналите за известување, дали има доволно информации за евалуација и дали заштитните мерки за откривање биле ефективни. Исто така, треба да се провери дали имплементираните заштитни мерки и активности биле ефективни и ефикасни.

Искуството стекнато од претходни безбедносни инциденти треба да се користи за да се дизајнираат процедури за слични безбедносни инциденти. За овие процедури треба да се информираат засегнатите вработени лица и редовно да се ажурираат врз основа на нови наоди.

Највисокото раководство на организацијата треба да се известува за безбедноските инциденти на годишно ниво, освен кога има потреба од итно дејство, тогаш мора веднаш да се известат раководството.

Развивање на процедурите врз основа на наодите од безбедноските инциденти и случувањата

Откако ќе се анализира безбедносниот инцидент, треба да се провери дали процедурите за постапување со безбедносни инциденти треба да се променат или дополнително да се развијат. Сите засегнати вработени лица при постапувањето со инцидентот треба да известуваат за своите соодветни искуства. Притоа, треба да се провери и дали има нови случувања во областа на управувањето со инциденти и форензиката и дали тие можат да се вклучат во постојните процедури и документација.

Доколку се користат листи за проверка и други помошни ресурси (алатки), ќе треба да се изврши проверка дали истите треба да бидат дополнети со дополнителни прашања и информации.

4.5.5. Напредни мерки

Дефинирање приоритети за постапување со безбедносни инциденти

Организацијата треба да има однапред дефинирани приоритети за постапување со безбедносни инциденти, кои и редовно ги ажурира. Притоа, треба да се има предвид и класификацијата на безбедносните инциденти.

Приоритетите треба да бидат одобрени и имплементирани од највисокото раководство на организацијата. Сите засегнати вработени лица кои се вклучени во постапувањето со безбедносни инциденти, треба да бидат запознаени со приоритетите. Дефинираните приоритети треба да бидат внесени во системот за управување со инциденти и истите да се зачувуваат.

Определување организационата единица за пријавување безбедносни инциденти

Организацијата треба да формира организационата единица за пријавување безбедносни инциденти, за која гарантира дека истата е достапна во определеното работно време. Сепак, треба да биде можно вработените да пријават безбедносни инциденти и надвор од определеното работно време. Вработените лица во организационата единица за пријавување треба да бидат соодветно обучени и запознаени со прашањата поврзани со безбедноста на информациите. Со информациите за безбедносни инциденти треба да се постапува доверливо од страна на вработените во организационата единица за пријавување.

Составување тим од експерти за постапување со безбедносни инциденти

Организацијата треба да формира тим од искусни и доверливи експерти за постапување со безбедносни инциденти, кои освен техничка експертиза, треба да имаат и познавања во областа на комуникациите. Организацијата треба да ја проверува доверливоста на членовите на експертскиот тим. Организацијата треба редовно да го проверува постапувањето на експертскиот тим и по потреба нејзиниот состав да го менува.

Експертскиот тим треба да биде вклучен во процедурите за комуникација и контакт за безбедносни инциденти. Експертскиот тим треба да биде обучен за анализа на безбедносните инциденти во системите што се користат во организацијата. За експертскиот тим треба да се организираат редовни обуки за системите што се користат за откривање и постапување со безбедносни инциденти. Експертскиот тим треба да има пристап до која било постојна документација и финансиски и технички ресурси што се потребни за брзо и дискретно постапување со безбедносните инциденти. Експертскиот тим треба да биде соодветно интегриран во организационите единици на организацијата. Одговорностите на експертскиот тим треба однапред да се координираат со активностите на тимот за безбедносни инциденти.

Преглед на ефикасноста на системот за управување при постапувањето со безбедносни инциденти

Редовните проверки треба да обезбедат тековно ажурирање и ефективност на системот за управување при постапување со безбедносни инциденти. За таа цел, треба да се спроведуваат најавени и ненајавени вежби, кои однапред се координираат со највисокото раководство на организацијата. Треба да се евалуираат параметрите што се мерат кога се евидентираат, пријавуваат и ескалираат безбедносните инциденти (на пример, времето од првичниот извештај до обврзувачката потврда на безбедносен инцидент).

Дополнително, треба да се спроведат и симулациски вежби за постапување со безбедносни инциденти.

Постапување со безбедносен инцидент - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.27	Недостаток на ресурси
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.6.Правилно администрирање на информатичката технологија

4.6.1.Вовед

Тековното администрирање на системите и на компонентите за информатичка технологија е од суштинско значење за операциите на информатичката технологија. Системските администратори ги конфигурираат системите и апликациите на информатичката технологија, ги следат операциите и преземаат мерки како одговор за одржување на функционалноста и способноста на меѓусебно поврзаните делови на компонентите на информатичката технологија. Исто така, тие ги приспособуваат системите за информатичка технологија на променетите потреби во организацијата. Притоа, системските администратори исполнуваат одредени задачи и на полето на безбедноста. Покрај тоа што обезбедуваат дека системите и понатаму се достапни, имплементираат и безбедносни заштитни мерки и ја следат нивната ефикасност. За таа цел, тие имаат соодветни овластувања, поради што е многу важно за безбедноста на доменот на информации самото системско администрирање да биде заштитено од неовластен пристап.

4.6.2.Цел

Целта е да се презентира како барањата за безбедност на апликациите, системите и мрежите на информатичката технологија може да се исполнат со соодветно администрирање на информатичката технологија.

Со имплементирање на овие барања, организацијата може да обезбеди дека активностите што се потребни за обезбедување на нејзиниот домен на информации се извршуваат правилно и систематски во администрирањето на системот. Истовремено, организацијата може да реагира на посебните закани што неизбежно произлегуваат од работењето со административни привилегии и можноста за пристап до сензитивните области на организацијата.

4.6.3.Закани

Недостатоци предизвикани од неопределени одговорности

Ако организацијата не ги има јасно определено административните одговорности во области какви што се планирање, инсталација, документација или следење (мониторинг), нема да биде можно систематски (или воопшто) да се извршуваат задачи во врска со безбедноста од овие области. Ова е случај и ако прописите не се познати и разбрани од страна на вработените. Типичните примери за ова вклучуваат нејасно разграничување на одговорностите помеѓу информатичката технологија и телекомуникациската технологија, помеѓу канцелариската информатичка технологија и производствените системи или помеѓу операциите на апликации и платформи.

Недостиг на кадар со соодветни компетенции

Организацијата треба да има предвид дека и администраторите може да бидат неочекувано отсутни подолг временски период. Доколку организацијата нема обучени вработени лица кои ги заменуваат администраторите, нема да може да се гарантира континуираното уредно работење на системите за информатичка технологија и на апликациите што ги поддржуваат тие системи. Администраторите понекогаш акумулираат многу опсежно и детално знаење за системите и за апликациите на информатичката технологија што ги надгледуваат во организацијата. Ова ги вклучува не само производите и решенијата што се користат, туку и посебните карактеристики на нивната оперативна средина и на специфичните достапни конфигурации. Ова знаење им овозможува на администраторите брзо да ги идентификуваат грешките и полесно да ги имплементираат барањата. Сепак, тоа често значи и дека сложените системи и апликации на информатичката технологија се администрираат од едно лице и доколку тоа лице е отсутно, неговото знаење повеќе не е достапно за организацијата.

Неправилно користење на администраторски овластувања

Администраторските овластувања овозможуваат сеопфатен пристап до доверливи информации во организацијата какви што се документи, комуникации и бази на податоци. Покрај извршувањето на задачите што им се доделени, администраторите може да ги користат овие овластувањата за свои цели (или за трети лица). На пример, тие може да пристапат до документите за вработените лица или до комуникациските канали на колегите. Понатаму, трети лица би можеле да вршат притисок врз администраторите или да користат други стимулации за да побараат помош за пристап и злоупотреба на податоци или на системите за информатичка технологија на организацијата.

Несоодветно извршување на административните задачи

Привилегираниот системски пристап што им е доделен на администраторите често е во фокусот на напаѓачите. Доколку административните задачи не се извршуваат правилно, станува многу полесно да се нападне доменот на информации на организацијата. Небрежноста може да предизвика грешки во конфигурацијата, да доведе до недоволно имплементирање одредени заштитни мерки (ако воопшто се имплементираат) или да резултира со пропусти во следењето на сомнителните настани. Причините за ова на пример може да вклучуваат недостаток на свесност за безбедноста, голем временски притисок за извршување на задача или недостаток на процеси и пристапи. Сето ова може да резултира со недостатоци што напаѓачите може да ги искористат.

Оперативни пречки

Административните активности директно влијаат врз работата на системите за информатичка технологија и апликациите. На пример, активните кориснички сесии може да се прекинат кога системите за информатичка технологија се рестартираат или може да се спречи овластен пристап додека се приспособуваат правилата за заштитниот сид. Доколку таквите процеси се вршат без да се земат предвид можните влијанија врз корисниците или да се координираат процесите со нив, операциите на организацијата може да бидат значително нарушени.

Недостасување можности за проверување на инциденти

Недостатоците во врска со документацијата за операциите на информатичката технологија или записите што недостасуваат, може да го оневозможат проверувањето или решавањето на безбедносните инциденти. Бидејќи честопати не е веднаш очигледно како бил извршен одреден напад, колку бил обремен или како се манипулирало со системите, прво се потребни соодветни проверки за да се одговори на таквите прашања. Меѓутоа, за ова да биде можно, мора да се документира и да може да се провери почетната состојба на системите за информатичка технологија пред безбедносниот инцидент за кој станува збор. Истовремено, мора да биде можно да се направи разлика помеѓу правилни и неовластени промени на системите за информатичка технологија врз основа на соодветни записи. Ако не се достапни соодветни информации, инцидентите тешко може да се проверат, доколку тоа е воопшто изводливо. Во такви случаи, исто така не е можно да се обезбедат и какви било правно валидни докази против напаѓачите.

4.6.4. Мерки

Правила за заменување на администраторите и планирање за итни случаи

Организацијата мора да обезбеди дека само вработените кои се овластени да ги заменуваат администраторите можат да пристапат до системите за информатичка технологија што треба да се одржуваат. Исто така, треба да се определат корисници за итни случаи со административни привилегии за постапување во итни случаи.

Контролирано определување администратори за информатичка технологија

Во организацијата, вработените лица кои извршуваат администраторски задачи во рамките на системите и на компонентите за информатичка технологија мора да бидат обучени, особено во однос на архитектурата на информатичката технологија и системите и апликациите на информатичката технологија за кои се одговорни. Администраторите мора да бидат запознаени со безбедносните процедури што се применуваат во организацијата и се значајни за нивната работа.

Престанок на должностите за администрирање на информатичката технологија

Ако во организацијата на администраторите им престанат обврските за извршување на задачите, тогаш мора да се повлечат и сите нивни доделени лични административни привилегии. Исто така, мора да се проверат и лозинките што им се познати на администраторите на кои им престанале обврските за извршување на задачите, при што овие лозинки мора да се променат.

Понатаму, мора да се провери дали администраторите на кои им престанале обврските за извршување на задачите се определени како лица за контакт (на пример, во договори или како запис на лице за контакт за интернет домени). Во овој случај, од страна на организацијата мора да се определат нови лица за контакт и да се известат третите лица. Корисниците на засегнатите системи и апликации на информатичката технологија мора да бидат известени дека на претходниот администратор на тие системи и апликации му престанале обврските за извршување на задачите.

Проверка на администраторските задачи

Организацијата мора да демонстрира кои администраторски активности биле извршени од конкретен администратор во секое време. За таа цел, секој администратор треба да има своја корисничка идентификација (корисничко име и лозинка). Вработените кои се овластени да ги заменуваат администраторите исто така треба да имаат своја сопствена корисничка идентификација.

За секоја најава со идентификација на администратор мора да постои запис во евиденцијата за секој пристап.

Заштита на администраторски задачи

Во организацијата мора преку соодветни процедури да се изврши автентикација на администраторите пред да се извршат активности со администраторски привилегии.

Постапките и активностите за кои не се потребни зголемени привилегии, не смее да се вршат со администраторски привилегии.

Организацијата мора да обезбеди дека само администраторите имаат пристап до администраторските интерфејси и функции. Конкретно, организацијата мора да обезбеди дека само администраторите можат да прават промени во врска со безбедноста на системите и на апликациите на информатичката технологија. Администрирањето мора да се изврши со помош на безбедни протоколи, при што треба да се земе предвид опцијата за поставување посебна администраторска мрежа.

Дефинирање на администраторските задачи на информатичката технологија

Делокругот на работа, задачите и обврските на администраторите во организацијата треба да се дефинираат така што ќе претставуваат обврска во соодветна процедура или политика за работа. Задачите што им се доделени на различни администратори, треба да се распределат на таков начин што ќе се избегне преклопување на одговорности, но сепак да бидат доделени сите задачи што треба да се извршат. Овие работни процедури или политики треба редовно да се ажурираат. Конкретно, нивните спецификации треба да ги спречат администраторите да прават неовластени промени во засегнатиот домен на информации, под услов промените да ги надминуваат задачите што им се изречно доделени и да не се неопходни за да се спречи безбедносен инцидент или пропуст.

Администрирање специјализирани апликации

Барањата за безбедност, организацијата треба да ги применува и за вработените со администраторски задачи што вклучуваат индивидуални специјализирани апликации. Поделбата на задачите помеѓу апликацијата и систематското администрирање треба да биде јасно дефинирано и документирано во писмена форма. Исто така треба да се дефинираат интерфејсите за комуникација помеѓу вработените што се задолжени со систематското администрирање и одговорните за администрирање на специјализирани апликации.

Доколку има администраторска интервенција во работењето на апликацијата, тоа треба однапред да се координира со засегнатата организациона единица, при што треба да се земат предвид и нејзините потреби.

Доволно ресурси за организационата единица за информатичка технологија

Организацијата треба да обезбеди доволно кадри и материјални ресурси во насока на правилно постапување со администраторските задачи. Притоа треба да се земе предвид фактот дека соодветните ресурси мора да бидат достапни и за непредвидливи задачи. Планирањето на ресурсите треба редовно да се ажурира и да се заснова на тековните барања на организацијата.

Дополнителна едукација и информации

Администраторите треба да учествуваат во мерките за обука и дополнителна едукација. Притоа треба да се земат предвид и техничките достигнувања што не се применуваат во моментот, но може да станат важни за организацијата во догледна иднина. Овие активности за обука треба да бидат предвидени со планот за обука. Кај овој план за обука треба да се земе предвид целиот тим за кој станува збор, за сите потребни квалификации да бидат обезбедени за повеќе членови. Администраторите треба редовно да добиваат информации во врска со безбедноста на апликациите, за системите, услугите и протоколите што ги администрираат, а особено во врска со тековните закани и безбедносните заштитни мерки.

Документација за администраторските задачи за информатичката технологија

Во организацијата системските промени треба да се документираат во соодветна и транспарентна форма. Оваа документација треба да го содржи следното:

- кои промени се извршени,
- кога биле извршени промените,
- кој ги извршил промените,
- основата и причините за промените.

Промените што се важни за безбедноста треба да се јасни и презентирани на разбирлив начин во документацијата.

Одредби за одржување и поправки

Системите за информатичка технологија треба редовно да се одржуваат. Организацијата треба да ги регулира безбедносните аспекти што треба да се почитуваат при одржување и поправка на опремата. Исто така, организацијата треба да ги определи и лицата што се одговорни за одржување или за поправка на опремата и да ги задолжи да ги документираат извршените задачи за одржување и поправка на опремата.

Администрирање и пуштање на уредите во функција

Организацијата треба да има преглед на сите уреди што ги користи, а кои би можеле да влијаат врз безбедноста на информациите. Покрај системите и компонентите за информатичка технологија, организацијата треба да ги има предвид и уредите што се однесуваат на т.н. „интернет на нештата“ (Internet of Things). Организацијата треба да воспостави и да примени соодветни процедури за тестирање и за одобрување на уредите пред истите да бидат ставени во функција за првпат. Прегледот треба да се ажурира и да соодветствува со документацијата за администраторските активности.

4.6.5. Напредни мерки

Безбедносна проверка на администраторите

Во ситуации што вклучуваат зголемена потреба за обезбедување на заштита, администраторите треба да подложат на дополнителна безбедносна проверка.

Организационата единица за администраторски активности

Организацијата треба да креира различни администраторски улоги за секоја одделна задача. Кога се прави разграничување помеѓу задачите, треба да се има предвид видот на вклучените податоци и поставената системска инфраструктура во организацијата.

Ограничувања што се однесуваат на администраторските пристапи

Пристапот до администраторските интерфејси треба да биде технички ограничен со мерки за филтрирање и одвојување. Интерфејсите не треба да бидат достапни за други лица кои не се дел од одговорните администраторски тимови. Администраторскиот пристап до системите за информатичка технологија во други заштитни зони треба да се воспостави само преку сервер кој обезбедува контролирана околина помеѓу засегнатите безбедносни зони на администраторите. Обидите за пристап од други системи или од други безбедносни зони треба да се одбиваат.

Двојна контрола при администрирање информатичка технологија

За одредени системи за информатичка технологија каде што безбедноста е од суштинско значење, пристапот до привилегиите со администраторски овластувања треба да се спроведува така што секогаш се потребни двајца вработени, односно еден администратор да ги извршува администраторските задачи, но под надзор на друг администратор.

Усогласено евидентирање на записите за администраторските активности

Организацијата треба да ги евидентира записите за администраторските активности во евиденцијата за секој пристап. За одредени системи за информатичка технологија каде што безбедноста е од суштинско значење, сите обиди за администраторски пристап треба да се евидентираат усогласено и целосно. Администраторите кои извршуваат администраторски активности, не треба да имаат овластување да ги менуваат или да ги бришат евидентираниите записи од евиденцијата за секој пристап. Записите од евиденцијата за секој пристап треба да се чуваат соодветен временски период согласно прописите за заштита на личните податоци или друг закон.

Согледување на барањата за висока достапност

Администраторите треба да анализираат кои од системите за информатичка технологија и мрежите што ги одржуваат подложат на барања за висока достапност. За овие системи и мрежи, тие треба да се уверат дека компонентите и инфраструктурата што се користи, како и поврзаните оперативни процеси, се соодветни за исполнување на овие барања.

Правилно администрирање на информатичката технологија - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.33	Недостиг на кадар
3_0.35	Принуда, изнуда или корупција
3_0.37	Одрекување на дејствија
3_0.42	Социјален инженеринг

4.7. Генерички објект

4.7.1. Вовед

Генеричкиот објект ги опфаќа сите работни станици и инсталираната информатичка технологија во просториите на организацијата, како и информациите што се обработуваат во тој објект, при што истиот обезбедува заштита од надворешни влијанија. Поради тоа, треба да се има предвид од една страна самиот објект (сидови, тавани, подови, покрив, прозорци и врати) и од друга страна целата инфраструктурна опрема, како и комуналните услуги што ги користи (струја, вода, гас, греење и ладење).

Генеричкиот објект кој се користи од повеќе организациони единици на организацијата, по правило имаат различни безбедносни барања. Во тој контекст, сите поврзани согледувања мора да го вклучуваат фактот дека речиси во секој објект влегуваат и лица што не ѝ припаѓаат на организацијата, какви што се физички лица, клиенти, даватели на услуги или снабдувачи. Доколку објектот го користат различни организации, неговиот дизајн и опрема мора да соодветствуваат на концептот на употреба на самиот објект. Притоа, треба да се обезбеди оптимална средина за лицата што работат таму. На неовластени лица не треба да им се дозволи пристап до делови од објектот каде што би можеле да ја загорат безбедноста. Воедно, треба да биде можно организацијата безбедно и ефикасно да функционира со технологијата што е инсталирана во објектот.

4.7.2. Цел

Целта е да се опишат барањата што треба да се исполнат за да се обезбеди оптимална заштита на објектот во однос на безбедноста на информациите. Заштитните мерки што произлегуваат од барањата зависат од видот и од големината на организацијата и на објектот. Овие барања може да се применат и на големи простори што опфаќаат неколку објекти, или за употреба на поединечни делови од објекти што ги користат повеќе организации.

4.7.3. Закани

Пожар

Објектите и опремата може да бидат сериозно оштетени од пожар, а притоа може да дојде до повреда или смрт кај присутните лица. Заедно со штетата што е директно предизвикана од пожар, мора да се има предвид и последователната штета. Обично потребни се недели, па дури и месеци за да се вратат во функција деловите што се оштетени од пожар. Токсичниот чад од пожарот исто така претставува многу голема опасност. Повеќето лични повреди поради пожар се предизвикани од вдишување чад. Чадот може да предизвика сериозни оштетувања и на опремата и на системите за информатичка технологија.

Согорувањето на пластика создава гасови на хлор, кои формираат хлороводородна киселина кога ќе дојдат во контакт со влажен воздух и со вода за гаснење. Доколку така создадените испарувања на хлороводородна киселина се шират низ системот за климатизација, може да се оштети и сензитивните електронски уреди што се наоѓаат во дел од објектот далеку од местото на пожарот.

Удар од гром

Доколку има невреме, громот (молњи) е најголемата опасност за објектите и за информатичката технологија. Удар на гром може да ослободи струја со јачина до 200.000 ампери при напон до неколку стотици илјади волти. Ова огромно количество електрична енергија се ослободува и се троши во рок од 50 до 100 микросекунди. Удар на гром со оваа јачина на растојание од приближно два километри сепак ќе предизвика варијации на напонот во електричните кабли на објектот што може да уништи сензитивни електронски уреди. Ризикот од оваа индиректна штета се зголемува колку што објектот е поблиску до ударот од гром. Ако објектот биде директно погоден од гром, голема штета може да предизвика динамичната енергија што се ослободува. Ова може да влијае врз покривот и фасадата, на пример, а последователните пожари или пренапони може да ги оштетат и електричните уреди.

Вода

Водата може да го оштети објектот и неговата опрема однадвор, на пример, како резултат на дожд, високо ниво на вода или поплави, или однатре поради настанати проблеми какви што се дефектите во водоводните цевки.

Природни опасности и катастрофи

Во зависност од нивната локација, објектите се изложени на различни степени на ризици во однос на природните опасности и катастрофи. Причините за природни катастрофи може да вклучуваат сеизмички или климатски појави какви што се земјотреси, поплави, лизгање на земјиштето, циклони или лавини. Примери за екстремни метеоролошки феномени вклучуваат грмотевици, циклони или пороен дожд.

Закани во близина

Објектите може да бидат оштетени и од настани во непосредна близина, како што се истекување токсични супстанции. Напорите за спасување, затворањето на патиштата или евакуациите исто така може да ја ограничат употребата на објектот.

Неовластен пристап

Доколку неовластени лица можат да пристапат до објектот или до одделни простории во објектот, тоа создава различни дополнителни закани. Неовластени лица може да предизвикаат штета преку намерни дејства какви што се кражба или манипулација со информации или со системи или компоненти за информатичка технологија, но и преку ненамерно недолично однесување (на пример, поради нестручност).

Во овој контекст, помалку очигледните манипулации можат да предизвикаат многу поголема штета од директните постапки на уништување. Имотната штета може да произлезе и од самиот неовластен упад, како, на пример, кога прозорците и вратите се принудно отворени и оштетени во процесот. За нивна поправка или замена обично се потребни финансиски средства и време, при што нивната заштитна функција е ограничена или воопшто ја немаат.

Повреда на закони или на други прописи

Кога се гради објект, има многу закони и прописи што мора да се почитуваат, какви што се оние што се однесуваат на заштита од пожари или на други аспекти на безбедноста на конструкцијата (структурната безбедност). Доколку се прекршат овие закони, ова може да не биде забележано подолго, но може да има катастрофални последици - на пример, ако уредите за заштита од пожар не се инсталираат како што е предвидено.

Недоволна заштита од пожар

Секој објект со функционална информатичка технологија содржи голем број вкрстени кабли и цевки, какви што се цевки за свежа вода и отпадна вода, цевки за греење или линии за снабдување со енергија или пренос на податоци. Невозможно е да се спречи овие носечки елементи за цевки и кабли да ги преминуваат таваните и сидовите за заштита од пожар. Доколку на таквите места не се монтираат соодветни направи што спречуваат пропуштање на течноста или гасовите за заштита од пожар, огнот и чадот може неконтролирано да се шират низ нив. Високодинамичната природа на информатичката технологија наметнува континуирано пренасочување на каблите, дури и преку направите што спречуваат пропуштање на течноста или гасовите за заштита од пожар. Начинот на кој тоа може правилно да се изведе зависи директно од постојната противпожарна заштита на објектот, што значи дека можните решенија може значително да се разликуваат. Ако промените на направите што спречуваат пропуштање на течноста или гасовите за заштита од пожар не се извршат според спецификациите на производителот, таа може да откаже и да не биде ефективна во случај на пожар. Пожарот потоа може да се прошири на делови што, всушност, треба да бидат заштитени со направите.

Дефект на напојувањето

Во случај на дефект/прекин на електричната енергија, цели објекти или нивни делови може да станат бескорисни. Од напојувањето не зависат само очигледните, директни потрошувачи на енергија какви што се информатичката технологија или осветлувањето, туку и целата инфраструктурна опрема што се користи денес директно или индиректно зависи од електричната енергија. Тоа вклучува лифтови, системи за климатизација, алармни системи, безбедносни врати, единици за автоматско заклучување на вратите, системи со прскалки и центри за телефони. Дури и снабдувањето со вода на катовите над или под земја, зависи од електричната енергија поради потребните пумпи.

4.7.4. Мерки

Планирање на заштита на објектот

Заштитата на објектот мора да се дефинира врз основа на (планираната) употреба на објектот и потребите за заштита на деловните процеси што се одвиваат во него. Конкретно, мора да се земат предвид безбедносните аспекти во врска со заштитата на лицата, опремата и информатичката технологија во објектот, од заштита од пожари и електрични аспекти до контрола на пристапот до местото. Барањата за безбедност од различни области мора да се координираат.

Соодветна сегментација на струјни кола

Мора да се вршат редовни проверки за да се обезбеди дека заштитата и дизајнот на струјните кола во објектот се уште ги исполнуваат реалните барања.

Усогласеност со прописите од областа за заштита од пожари

Мора да се исполнат прописите од областа за заштита од пожари и барањата наложени од прописите за градење. Патеките за евакуација мора да бидат обележани во согласност со соодветните прописи и редовно да се одржуваат. Мора да се вршат редовни проверки за да се утврди дали патеките за евакуација се употребливи и дали се блокирани од какви било пречки за да можат лицата во објектот брзо да се евакуираат во случај на опасна ситуација.

Мора да се изготви и да се имплементира концепт за заштита од пожари во врска со информатичката технологија. Мора да се избегнуваат непотребни оптоварувања од пожар. Организацијата треба да има вработен кој ќе биде обучен за заштита од пожари.

Откривање пожар во објекти

Објектите мора да бидат опремени со доволен број детектори за чад во согласност со барањата во нивните градежни дозволи и со концептите за заштита од пожари. Доколку локалното предупредување на местото на секој детектор не е доволно, сите детектори мора да се поврзат на контролна табла за аларм за пожар. Ако се открие присуство на чад во објектот, мора да се активира алармот. Сите во објектот мора да можат да го слушнат. Мора редовно да се проверува функционирањето на сите детектори за чад и на сите други компоненти на системот за аларм за пожар.

Рачни противпожарни апарати

За итни мерки за гасење пожар, мора да бидат достапни доволен број рачни противпожарни апарати со соодветни димензии со класата на пожар што е потребна за соодветната ситуација. Овие рачни противпожарни апарати мора редовно да се проверуваат и да се сервисираат. Вработените треба да добијат инструкции/упатства за употреба на рачните противпожарни апарати. Ваквите инструкции треба да се повторуваат на соодветен временски период.

Затворени прозорци и врати

Прозорците и вратите до кои може да се пристапи однадвор, како, на пример, од балкони или од тераси, мора да бидат затворени кога просторијата не се користи. Просториите мора да бидат заклучени доколку таму се оставени доверливи информации. Мора да се издадат соодветни упатства за таа цел. На сите вработени треба да им се укаже дека треба да ги почитуваат упатствата. Мора да се вршат редовни проверки за да се обезбеди дека прозорците и внатрешните и надворешните врати се заклучени по напуштањето на објектот. Вратите за пожар и чад не смеат да останат отворени подолг временски период, освен ако не се користат одобрени системи за да останат отворени.

Процедури за пристап до локацијата и контрола

Пристапот до сензитивните делови на објектите и просториите мора да се уреди со процедури и истиот да се контролира. Треба да постои концепт за контрола на пристап до локацијата. Бројот на лица со овластување за пристап до локацијата треба да се намали на минимален број за секој дел. Дополнителни лица не смеат да добијат пристап додека не се потврди соодветната потреба. Доделените овластувања за пристап до локацијата треба да бидат документирани. Мора редовно да се проверува ефективностa на заштитните мерки за контрола на пристап до локацијата. Контролите за пристап до локацијата исто така треба да останат воспоставени колку што е можно и за време на преместувања на друга локација.

Забрана за пушење

Пушењето мора да биде забрането во простории каде што пожарите или контаминацијата може да предизвикаат значителна штета, какви што се серверските простории или медиумите за чување податоци и архивите на документи. Мора да се вршат редовни проверки за да се обезбеди дека заштитата на пристапот до локацијата не е занемарена кога има означени или прифатени места за пушење.

Усогласеност со релевантните стандарди и регулативи

При планирање, подигање и пренамена на објекти и инсталирање техничка опрема, мора да се земат предвид сите релевантни стандарди и регулативи од таа област.

Безбедносен концепт за употреба на објект

Треба да постои безбедносен концепт за употреба на објектот. Безбедносниот концепт за објектот треба да се приспособи на целокупниот безбедносен концепт на конкретната организација. Треба редовно да се документира и да се ажурира. Сензитивните делови на објектите и просториите не треба да се наоѓаат во многу изложени или особено опасни области.

Управување со клучеви

Организацијата треба да има план за заклучување на сите клучеви од даден објект во посебни кутии за клучеви. Изработката, чувањето, управувањето и давањето на клучевите, треба да се организираат на централизиран начин. Резервните клучеви треба да бидат достапни и обезбедени, но да се чуваат при рака за итни случаи. Клучевите што не се издадени, треба безбедно да се чуваат. Секој издаден клуч треба да биде документиран.

Регулативи со кои се регулира пристапот до дистрибутерите

Брзиот пристап до дистрибутерите на сите капацитети за снабдување во објектот треба да биде можен кога тоа е потребно. Пристапот до дистрибутерите треба да биде ограничен на мала група овластени лица.

Уреди за заштита од гром

Системот за заштита од гром треба да се инсталира според применливиот стандард. Треба да се воспостави сеопфатен концепт за заштита од гром и пренапон. Како минимален услов, објектите со сеопфатна опрема за информатичка технологија треба да бидат опремени со уреди за заштита од гром со соодветна класа на заштита. Системот за заштита од гром треба редовно да се прегледува и да се сервисира.

Планови со детали за локацијата на линиите за снабдување

Треба да бидат достапни ажурирани планови за распоред на сите линии за снабдување за даден објект. Треба да се одреди кој е одговорен за одржување и за ажурирање на плановите за распоред на сите линии за снабдување. Плановите треба да се чуваат така што само овластени лица можат да пристапат до нив, но тие мора да бидат лесно достапни во случај на потреба.

Избегнување на упатувања на локации на сензитивни делови од објектот

Треба да се избегнуваат упатувања на локациите на сензитивните делови. Сензитивните делови на објектите не треба да бидат лесно видливи однадвор.

Структурна заштита од чад

Структурната заштита од чад на објектот треба да се провери по инсталацијата и при нејзина промена. Треба да се вршат редовни проверки за да се обезбеди дека компонентите за заштита од чад се уште функционираат.

Проверки за противпожарна безбедност на самото место

Редовно треба да се вршат проверки за противпожарна безбедност на самото место за заштита од пожари, односно најмалку еднаш или двапати годишно. Недостатоците што се утврдени при проверка на противпожарната безбедност на самото место треба веднаш да се поправат или да се отстранат.

Известување на лицето за заштита од пожари

Лицето за заштита од пожари треба да биде известен за работата што се изведува на носачите на кабли, во ходниците и на патеките за евакуација и спасување. Тоа лице треба да провери дали мерките за заштита од пожари се спроведуваат правилно.

План за предупредување и обука за противпожарна заштита

Треба да се изготви план за предупредување за мерките што треба да се преземат во случај на пожар. Планот за предупредување треба редовно да се прегледува и да се ажурира. Обуката за противпожарна заштита треба редовно да се спроведува.

Заштита од провална кражба

Треба да се спроведат соодветни заштитни мерки за заштита од провална кражба и тие треба да се приспособат на соодветните услови. Треба да се внимава при планирањето, спроведувањето и функционирањето на заштитата од провална кражба за да се обезбеди дека таа е конзистентна, вклучително и во однос на нејзиниот квалитет. Лице со соодветна стручност треба редовно да врши проверка. Вработените треба да ги применуваат правилата за заштита од провални кражби.

Редовни ажурирања на документацијата

Документацијата за објектот секогаш треба да се ажурира (на пример, планови за градба, дијаграми за поврзување, планови за патеки за евакуација, мапи на патеките на противпожарната служба). Треба да се провери дали сите релевантни планови сè уште се ажурирани и точни најмалку еднаш на секои три години. Вработените треба да бидат информирани за било какви промени.

4.7.5. Напредни мерки

Заштитни врати и прозорци

Вратите и прозорците треба да се изберат врз основа на заштитните цели на делот од објектот што треба да се обезбеди, потребите за заштита на организацијата и соодветната класификација во согласност со релевантните стандарди. Сите заштитни мерки наменети за обезбедување на прозорците, вратите и сидовите што опфаќаат даден простор, треба да бидат соодветни и со еднаков квалитет во однос на провална кражба, пожар и чад. Правилното функционирање на заштитните врати и прозорци треба редовно да се проверува.

Формирање безбедносни зони

Просториите со слични потреби за заштита треба да се обединат во зони, со цел да се постапува со споредливите ризици на еднообразен начин и да се намалат трошоците за потребните безбедносни заштитни мерки.

Автоматско одводнување

Сите области со ризик за оштетување од вода треба да бидат опремени со автоматски систем за одводнување. Треба да се вршат редовни проверки за да се обезбеди дека активните и пасивните системи за одводнување сè уште функционираат.

Избор на соодветни локации

При избор или планирање локација за објект, треба да се проверат условите на животната средина што би можеле да влијаат врз безбедноста на информациите. Треба да има преглед на заканиите во врска со локацијата. Овие закани треба да се решат со помош на дополнителни заштитни мерки.

Лица за обезбедување

Задачите на лицата за обезбедување треба да бидат јасно документирани. Лицето за обезбедување треба да ги набљудува и да ги следи сите движења на лицата на капија/влезна врата и на сите други влезови во согласност со безбедносниот концепт на организацијата. Сите вработени и посетители треба да можат да се идентификуваат пред лицето за обезбедување. Посетителите треба да бидат придружувани додека да стигнат до лицето што треба да го посетат или да бидат пречекани на влезот. Лицето за обезбедување треба да биде веднаш информирано за било какви промени во овластувањата за пристап до објектот на организацијата.

Избор на соодветен објект

При изборот на соодветен објект, треба да се провери дали може да се применат сите безбедносни барања што се значајни за подоцнежна употреба. За секој објект, постојните закани и заштитните мерки што се потребни за спречување или за намалување на штетата, треба однапред да се документираат.

Иселување од објектите

Пред да се исели од објектот, организацијата треба да изготви попис (инвентарен список) на сите предмети што се значајни за безбедноста на информациите за преселбата, какви што се хардвер, софтвер, медиуми за чување податоци, датотеки или документи. Откако ќе заврши преселбата, во сите простории треба да се провери дали има останати предмети.

Регистар на направи што спречуваат пропуштање на течноста или гасовите за заштита од пожар

Треба да се води регистар на направите што спречуваат пропуштање на течноста или гасовите за заштита од пожар. Во овој регистар треба да се евидентираат сите поединечни видови на поделби на направите. Откако ќе се изврши работата на направите што спречуваат пропуштање на течноста или гасовите за заштита од пожар, промените треба да се внесат во регистарот.

Систем за детектирање натрапник и пожар

Треба да има систем за детектирање натрапник и пожар, кој е соодветен за просториите и за соодветните ризици. Системот за детектирање натрапник и пожар треба редовно да се проверува и да се сервисира. Мора да се обезбеди дека примателите на предупредувања за упад и за детектирање на пожар се способни соодветно да одговорат, како од технички така и од кадровски аспект.

Периметарска заштита

Во зависност од потребите за заштита и соодветниот терен, објектот треба да има периметарска заштита. Како минимален услов, треба да се имаат предвид следните компоненти во однос на нивната корисност и изводливост:

- сид или ограда околу просторот,
- безбедносни заштитни мерки против случаен престап (преминување на линијата на просторот),
- безбедносни заштитни мерки против намерен престап без примена на сила,
- заштитни мерки за попречување на намерното преминување на линијата на просторот со примена на сила,
- заштитни мерки за безбедност на отворено,
- детектирање лица и возила,
- заштитни мерки за зачувување докази (на пример, видеонадзор),
- автоматски предупредувања.

Генерички објект - закани што се вклучени овде:	
3_0.1	Пожар
3_0.2	Неповолни услови во околината
3_0.3	Вода
3_0.4	Акумулирање нечистотии, прашина, корозија
3_0.5	Природни катастрофи
3_0.6	Катастрофи во животната средина
3_0.7	Поголеми настани во околината
3_0.8	Прекин или неисправност на напојувањето
3_0.10	Дефект или неисправност на мрежите за снабдување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.29	Повреда на закони или на договори
3_0.34	Напад
3_0.43	Вметнување пораки
3_0.44	Неовластен влез во простории

4.8. Центар за податоци и серверска просторија

4.8.1. Вовед

Денес, речиси сите стратегиски и оперативни функции и задачи имаат суштинска поддршка од информатичката технологија или дури и целосно зависат од неа. Како последица на тоа, барањата за ефикасност и достапност на системите за информатичка технологија и на нивните мрежни поврзувања постојано се зголемуваат. За да ги исполнат овие барања за ефикасност, за да обезбедат достапност на соодветен резервен капацитет и за да работат со информатичката технологија економично, организациите ги концентрираат своите меѓусебно поврзани делови на информатичката технологија во центри за податоци.

Центарот за податоци може да се определи на следниот начин:

1. Ако операциите на информатичката технологија на организацијата се пренесуваат на неколку делови во еден објект или во дадени простории и овие делови се поврзани и меѓусебно и со корисниците на информатичката технологија преку внатрешни врски на локална мрежа (LAN), најзначајниот дел од сите овие делови, од аспект на функцијата (како минимален критериум), мора да се третира како центар за податоци. Покрај тоа, деловите каде што операциите се клучни за 50% или поголем процент од корисниците или од кои се обезбедуваат 50% или поголем процент од услугите и податоците (пропорционално на сите области), мора да се третираат како центар за податоци.
2. Ако организацијата што користи информатичка технологија има само еден централен дел за операции на информатичката технологија, овој дел, заедно со потребните делови за поддршка, секогаш мора да се третира како центар за податоци во однос на потребите за заштита. Терминот „дел/област на операции за информатичка технологија“ се однесува на простории во кои е инсталиран и во кои работи хардвер за да се обезбедат услуги и податоци. Покрај својот дел/област за операции на информатичката технологија, центарот за податоци ги опфаќа сите други делови/области за техничка поддршка (на пример, напојување, снабдување со ладен воздух, технологија за гаснење, безбедносна технологија), кои го олеснуваат правилното работење и безбедноста на делот за операции на информатичката технологија.
3. Ако организацијата што користи информатичка технологија се наоѓа на неколку физички одвоени локации и тие се меѓусебно поврзани со врски кои што се различни од внатрешните врски на локална мрежа (LAN), секоја од локациите мора да се земе предвид и да се третира одделно според точка 1 од оваа потточка.

4. Делот за операции на информатичката технологија во кој се наоѓа информатичка технологија што е потребна за суштински деловни процеси (т.е. процеси чие нарушување или неизвршување значително ќе го наруши исполнувањето на примарните задачи на организацијата), мора секогаш да се третира како центар за податоци, независно од големината или од соодносот што е утврден во точка 2 од оваа потточка.
5. Деловите за операции на информатичката технологија од кои се вршат услуги за трети лица мора секогаш да се третираат како дел од центарот за податоци.
6. Доколку постои оправдан интерес за третирање на делот за операции на информатичката технологија (заедно со неговите делови за поддршка) како серверска просторија спротивно на погоренаведените дефиниции, мора да се наведат причините за намалувањето на барањата за безбедност.

Ако центарот за податоци отстапува од оваа дефиниција, делот за операции на информатичката технологија за кој станува збор се нарекува серверска просторија. Оваа дефиниција единствено се заснова на значењето на структурата за информатичка технологија за исполнување на задачите на организацијата што ја користи структурата за информатичка технологија.

Ако треба да се заштити серверската просторија, барањата од овој дел може соодветно да се намалат. Сепак, мора да се наведат суштински и разбирливи причини за овие околности во согласност со точката 6 од оваа потточка и мора да се имплементираат најмалку основните барања.

4.8.2 Цел

Примарната цел е да се опишат барањата што треба да се исполнат за да се обезбеди безбедна работа на центрите за податоци. Од една страна, таа е насочена кон организации што управуваат со центар за податоци и сакаат да проверат дали се спроведени соодветни безбедносни заштитни мерки во рамките на проверката, а од друга страна може да се користи и за процена на безбедносните заштитни мерки што треба да се спроведат ако информатичката технологија во центарот за податоци треба да се централизира.

4.8.3 Закани

Неправилно планирање

Ако заштитата од закани не се земе предвид при дизајнирање на центарот за податоци, постои многу голем ризик за дефект или за откажување. На пример, ризиците на локацијата какви што се воздушен сообраќај, земјотреси или поплави можат да ја загрозат оперативната безбедност и достапност. Исто така, можни се големи влијанија врз работата на центарот за податоци доколку достапната ширина на опсег или снабдувањето со енергија на избраната локација се недоволни поради неправилен концепциски дизајн.

Недоволни контроли за пристап до локацијата

Доколку контролите за пристап до локацијата се недоволни, постои зголемен ризик неовластени лица да влезат во центарот за податоци и да предизвикаат ненамерна (на пример, поради техничко незнаење) или намерна штета. Така, на пример, напаѓачите можат да преземат сензитивни податоци, да украдат уреди или да манипулираат со серверите. Според тоа, недоволните контроли за пристап до локацијата може да влијаат врз достапноста, доверливоста и интегритетот на податоците и на компонентите на информатичката технологија.

Недоволно следење

Ако информатичката технологија и инфраструктурата што функционираат во центарот за податоци се недоволно следени и одржувани, компонентите може да прекинат да работат без некој да го забележи тоа. Ова може сериозно да ја наруши достапноста и правилната функционалност на центарот за податоци. Во многу случаи, дефектите исто така се случуваат постепено во текот на подолг временски период. Без активно следење, тие може да се забележат предочна. Во тој момент, честопати веќе не е можно да се реагира навреме.

Недоволна климатизација во центарот за податоци

За компонентите на информатичката технологија се потребни специфични работни услови за да функционираат сигурно. Тие истовремено ја претвораат електричната енергија што ја апсорбираат во дополнителна топлина. Ако температурата, влажноста или содржината на прашина на воздухот во работната средина на информатичката технологија не се одржуваат во границите наведени од производителите на опремата, тоа може да доведе до понатамошно неправилно функционирање или дефект на техничките компоненти.

Пожар

Пожарот не е вообичаена закана. Меѓутоа, при појава на пожар, тој обично има сериозни последици. Тоа е затоа што пожарот и чадот може да предизвикаат голема штета. Додека пожарите на електричната инсталација се најчеста причина за пожар во деловите каде што работи информатичката технологија, може да има голем број други причини за пожар надвор од делот каде што работи информатичката технологија, а особено во деловите за поддршка што вклучуваат напојување при итен случај (EPS) и за непрекинато напојување (UPS). Ако делот каде што работи информатичката технологија, неговите делови за поддршка или други соседни делови имаат несоодветна заштита од пожар, пожарот може брзо да се прошири. Покрај тоа, пожарите што започнуваат надвор може да се прошират и во центарот за податоци.

Вода

Водата може да навлезе во центарот за податоци поради протекување на водоводни цевки, поплави, пукнати цевки, неисправни прскалки или системи за климатизација. Ова може да ја оштети опремата и да ја прекине нејзината работа. Може да се активира и краток спој, што може да предизвика прекин на работата на одделни делови на центарот за податоци или да предизвика пожар.

Недоволна заштита од провална кражба

Дури и ако има функционален систем за контрола на пристап, неовластени лица можат да влезат во центарот за податоци доколку тој не е соодветно заштитен од неовластен пристап. Престапниците потоа би можеле да украдат компоненти или да манипулираат со компонентите за информатичка технологија или да дознаат доверливи информации. Исто така, може да ги уништат уредите или да нанесат штета на центарот за податоци.

Дефект на напојувањето

Доколку дојде до прекин/дефект на напојувањето, може значително да се наруши работата на центарот за податоци, а со тоа и на целата организација. Во случај на прекин/дефект на напојувањето, услугите за информатичка технологија што ги обезбедува центарот за податоци одеднаш повеќе нема да бидат достапни. Може да се изгубат и податоци. Покрај тоа, можно е системите за информатичка технологија, телекомуникациските системи или технологијата за следење да бидат оштетени од ненадеен прекин на напојувањето.

Контаминација

Прашината и другата контаминација во центарот за податоци може да предизвикаат прекин на работата на техничките компоненти (на пример, вентилаторите). Контаминацијата предизвикува опремата почесто да откажува и побрзо да ја изгуби својата функционалност според предвидениот рок на траење.

4.8.4 Мерки

Дефинирање на барањата

Организацијата мора да дефинира и да имплементира соодветни технички и организациски барања за центарот за податоци.

При планирање на центарот за податоци или избирање соодветни простории, мора да се планираат и соодветни безбедносни заштитни мерки, кои ги земаат предвид потребите за заштита на компонентите за информатичка технологија, особено во однос на нивната достапност.

Центарот за податоци како целина мора да биде дизајниран како затворена безбедносна област. Покрај тоа, мора да има различни безбедносни зони. На пример, администрацијата, логистиката и операциите за информатичка технологија и деловите за поддршка мора да бидат јасно одвоени едни од други. Доколку станува збор за серверска просторија, треба да се провери дали е можно да се имплементираат различни безбедносни зони.

Формирање зони за заштита од пожар

За просториите на центарот за податоци мора да се дефинираат соодветни зони за заштита од пожар и чад. Зоните за заштита од пожар и чад мора да обезбедат дополнителна заштита на просториите на центарот за податоци според параметрите предвидени во прописите за градење за техничката опрема што се наоѓа во нив и нејзината достапност. Исто така, мора да се спречи ширење на огнот и чадот. Доколку станува збор за серверска просторија, треба да се провери дали може да се имплементираат соодветни зони за заштита од пожар и чад.

Користење непрекинато напојување

Организацијата мора да инсталира уред за непрекинато напојување (UPS) за сите релевантни компоненти за работата на центарот за податоци. Имајќи предвид дека потрошувачката на енергија на климатизацијата честопати е превисока за уредот за непрекинато напојување (UPS), контролата на овие системи мора да биде поврзана најмалку со UPS уредот. Доколку станува збор за серверска просторија, неопходноста од ракување со UPS уредот треба да се провери врз основа на барањата за достапност на соодветните системи за информатичка технологија. UPS уредот мора да има доволен капацитет. Доколку има релевантни промени во оптоварувањата, мора да се извршат проверки за да се утврди дали капацитетот на постојните UPS системи сè уште е доволен. Во UPS системите што користат батерија за складирање енергија, батеријата мора да се чува во рамките на потребниот температурен опсег. За таа цел, доколку е можно, треба да се чува подалеку од електрониката за напојување на UPS уредот. UPS уредот мора редовно да се сервисира и да се проверува неговата функционалност. Поради тоа, мора да се следи распоредот за одржување што е одреден од производителот.

Итно исклучување на напојувањето

Организацијата мора да има соодветни опции за исклучување на електричните потрошувачи во центарот за податоци. Мора да се внимава дали и како постојниот UPS уред е просторно и функционално интегриран во напојувањето. Доколку се користат конвенционални прекинувачи за итно исклучување, мора да се обезбеди дека целиот центар за податоци нема да биде исклучен. Системот за итно исклучување мора да се подели според потребите и приоритетите на организацијата. Сите прекинувачи за итно исклучување мора да бидат заштитени така што да не може да се активираат ненамерно или без овластување.

Одржување на температурата и на влажноста на воздухот

Организацијата мора да обезбеди дека температурата и влажноста на воздухот во работната средина на информатичката технологија се одржуваат во пропишаните граници. Топлинското оптоварување во разладените области мора редовно да се проверува, како и по настанати промени. Сите системи за климатизација што се користат мора редовно да се одржуваат. Како минимален критериум, параметрите за температура и за влажност мора да се евидентираат на начин што овозможува ретроспективно да се идентификува дали границите се надминати, за да се утврди прецизно и да се отстрани причината за отстапувањето.

Контрола на пристап до локацијата

Организацијата мора да го контролира пристапот до центарот за податоци, при што правата за пристап до локацијата мора да се доделат во согласност со нејзините барања. Мора да се обезбеди дека оние што работат во центарот за податоци немаат пристап до системите за информатичка технологија надвор од нивниот делокруг на работа. Сите можни начини за пристап до центарот за податоци мора да бидат опремени со уреди за контрола на пристап до локацијата. Секој момент кога некое лице пристапува до центарот за податоци, мора да биде евидентиран од системот за контрола на пристап до локацијата. Доколку станува збор за серверска просторија, треба да се провери дали е соодветно да се следат сите можни начини за пристап до предметната локација. Организацијата мора да врши редовни проверки за да утврди дали се почитуваат прописите во врска со користењето на контролите за пристап до локацијата. Барањата на организацијата во врска со нејзиниот систем за контрола на пристап до локацијата мора детално да се документираат.

Заклучување и обезбедување на опремата

Сите врати на центарот за податоци мора секогаш да бидат заклучени. Прозорците мора да се избегнуваат во фазата на планирање секогаш кога тоа е можно. Ако има прозорци, тие мора секогаш да бидат заклучени. Вратите и прозорците мора да обезбедат соодветна заштита за ниво на безбедност од напади и надворешни влијанија, како и за обезбедување доверливост на опремата. Мора да се земе предвид структурниот дизајн на сите елементи што ја сочинуваат просторијата и можноста да се обезбеди унифицирано ниво на заштита.

Употреба на систем за противпожарен аларм

Во центарот за податоци мора да се инсталира систем за противпожарен аларм. Со овој систем мора да се следат сите области, при што сите аларми на системот за противпожарен аларм мора соодветно да се проследат. Системот за противпожарен аларм мора редовно да се сервисира. Мора да се обезбеди дека нема голема потенцијална сериозна можност за појава на пожар во просториите на центарот за податоци.

Употреба на систем за гаснење или спречување пожар

Организацијата во центарот за податоци мора да инсталира систем за гаснење или за спречување пожар во согласност со најсовремената технологија. Ако тоа не е можно, техничките мерки (особено систем за рано откривање пожар) и организациските мерки (обучен кадар и планови за одговор за аларми за рано откривање пожар) мора да обезбедат моментална реакција на алармите за рано откривање пожар и тоа во рок од најмногу три минути.

Во серверските простории без систем за гаснење или заштита од пожар, мора да се достапни рачни противпожарни апарати со соодветни средства за гаснење, во доволен број и големина. Противпожарните апарати мора да бидат монтирани така што ќе бидат лесно достапни во случај на пожар. Секој противпожарен апарат мора редовно да се проверува и да се сервисира. Сите вработени на кои им е дозволено да влезат во центарот за податоци или во серверската просторија, мора да добијат инструкции за употреба на рачни противпожарни апарати.

Контрола и одржување на инфраструктурата

За сите компоненти на инфраструктурата, мора да се почитуваат најмалку интервалите и барањата за контрола и одржување што се препорачани од производителот или се прецизирани со соодветните стандарди. Контролите и работата за одржување мора да се документираат. Направите што спречуваат пропуштање на течноста или гасовите за заштита од пожар мора да се проверат за да се обезбеди дека се недопрени. Организацијата мора резултатите од контролата и одржувањето на инфраструктурата да ги документира.

Автоматско следење на инфраструктурната опрема

Организацијата мора автоматски да ја следи целата инфраструктурна опрема, како што е следење на истекување, климатизација и системи за напојување и UPS-уред. Откриените нарушувања мора да се проследат и да се решат на соодветен начин колку што е можно побрзо.

Доколку станува збор за серверската просторија, информатичката технологија и уредите за поддршка што не треба да ги управува лице или само повремено треба да ги управува лице, тие треба да бидат опремени со далечинска индикација за дефекти. Одговорните вработени мора брзо да се известуваат за настанатите дефекти.

Употреба на рано детектирање односно откривање на пожар

Центарот за податоци мора да биде опремен со систем за рано детектирање односно откривање на пожар. Серверската просторија треба да биде опремена со систем за рано детектирање односно откривање на пожар. Алармите за рано детектирање на пожар, мора да се насочат до организациона единица со постојано присуство на кадар што може да започне контролна и заштитна реакција во рок од најмногу три минути. Алтернативно, мора да започне автоматска заштитна реакција. За да се постигне рамнотежа помеѓу заштитата од пожар и достапноста, организацијата мора да обезбеди дека опремата што обезбедува редундантност не е поставена заедно во рамките на ефективниот опсег на истото коло за изолација на напон.

Избегнување и следење непотребно ожичување

Во центарот за податоци поставените кабли мора да бидат ограничени на кабли што директно ја снабдуваат технологијата што е инсталирана таму (обично информатичката технологија и, доколку е применливо, технологијата за ладење). Ако е неизбежно од структурни причини да поминуваат жици низ центарот за податоци за да се обезбедат деловите или областите различни од оние во центарот за податоци, ова мора да се документира заедно со соодветно оправдување односно наведување на причините. Ризиците од таквите жици мора да се сведат на минимум со соодветни заштитни мерки (на пример, мониторинг). Овие жици може да се пренасочат низ серверските простории без да се оправда зошто тоа е неизбежно, но со нив мора да се постапува на ист начин како што е наведено за центрите за податоци. Пораките од системите што ги следат таквите жици мора веднаш да се проверат и да се проценат за да се утврди дали постои закана. Заштитните мерки мора да се спроведат навремено во согласност со идентификуваното ниво на закана.

Периметарска заштита на центарот за податоци

За центрите за податоци треба да постои периметарска заштита. Во зависност од потребите за заштита што се дефинирани за даден центар за податоци и неговите простории, периметарската заштита треба да се состои од следните компоненти:

- Сид или ограда околу просторот;
- Заштитни мерки за неовластен пристап (преминување на линијата на просторот);
- Заштитни мерки за попречување намерно преминување на линијата на просторот без примена на сила;
- Заштитни мерки за попречување намерно преминување на линијата на просторот со примена на сила;
- Детектирање лица и возила;
- Автоматски предупредувања.

Планирање и инсталирање на алармни системи

Безбедносниот концепт на соодветниот објект на организацијата треба да се користи за планирање на потребните алармни системи и треба да се инсталираат за одредени делови/области на центарот за податоци. Покрај тоа, треба да се утврди процедура за постапување со пораки за аларм. Безбедносниот концепт секогаш треба да се приспособува ако и кога се менува употребата на тие делови на објектот. Организацијата треба да инсталира алармен систем погоден за намената. Известувањата од алармниот систем треба да се пренесат до центарот за прием на аларми во согласност со техничките барања за поврзување. Избраниот центар за прием на аларми мора да биде достапен во секое време, при што истиот мора да може соодветно да одговори на алармите. Патеката за пренос помеѓу алармниот систем и центарот за прием на аларм треба да биде дизајнирана според техничките барања за поврзување и доколку е можно со редундантност. Сите воспоставени патеки за пренос мора редовно да се тестираат.

Употреба на систем за напојување при итен случај

Напојувањето со кое се снабдува центарот за податоци од мрежата за снабдување со електрична енергија треба да биде дополнето со систем за напојување при итен случај (EPS). Ако има EPS, мора редовно да се одржува. При одржувањето, мора да се спроведат тестови за оптоварување и функционалност, како и тестови под оптоварување. Снабдувањето за работа на EPS, мора редовно да се проверува за да се утврди дали е доволно. Исто така, мора да се вршат и редовни проверки за да се обезбеди дека овие залихи сè уште се употребливи, а особено за да се избегне контаминација на дизел горивото со микроорганизми. Ако е можно, наместо дизел-гориво треба да се користи масло за греење со малку сулфур. Операциите за полнење гориво мора да се евидентираат. Евиденцијата мора да го содржи типот на гориво, употребените адитиви, датумот на полнење гориво и количината на полнење. Ако не се користи EPS за серверската просторија, како алтернатива треба да се имплементира UPS со соодветно време на работа за потребите за заштита.

Уреди за заштита од пренапон

Организацијата треба да подготви концепт за заштита од гром и пренапон врз основа на важечкиот стандард во моментот. Мора да се дефинираат зоните за заштита од гром (LPZ), кои се потребни за правилна работа на центарот за податоци. За целата опрема што е потребна за правилна работа на центарот за податоци и неговата способност да обезбедува услуги, треба да се обезбеди најмалку ниво 2 од зоните за заштита од гром (LPZ). Целата опрема за заштита од пренапон треба да подложи на сеопфатен тест еднаш годишно.

Климатизација во центри за податоци

Организацијата треба да обезбеди дека воспоставените климатски услови во центарот за податоци редовно се одржуваат. Системот за климатизација на центарот за податоци треба да има доволен капацитет. Сите релевантни вредности треба постојано да се следат. Доколку некоја вредност отстапува од нормалата, треба да се вклучи автоматски аларм. Системите за климатизација треба да бидат колку што е можно побезбедни од дефекти во оперативните области на информатичката технологија.

Функционално тестирање на техничката инфраструктура

Техничката инфраструктура на центарот за податоци треба редовно да се тестира (најмалку еднаш или двапати годишно), како и по направени промени или поправки на системот. Резултатите треба да се документираат.

Системи за гаснење или спречување пожари

Центарот за податоци треба да биде опремен со автоматски систем за гаснење или заштита од пожар.

4.8.5 Напредни мерки

Алтернативен центар за податоци

Организацијата треба да воспостави географски одделен алтернативен центар за податоци. Алтернативниот центар за податоци треба да има доволен капацитет за одржување на сите процеси на организацијата. Исто така, секогаш треба да биде подготвен за работа. Сите податоци на организацијата треба редовно да се отсликуваат во алтернативниот центар за податоци, а овој центар треба да се тестира и редовно да се врши обука на кадарот. Патеките за пренос до алтернативниот центар за податоци треба да бидат соодветно обезбедени и дизајнирани со соодветна редундантност.

Имплементација на мерки за заштита од прашина

За време на градежните работи во центарот за податоци, треба да се дефинираат, да се планираат и да се спроведат соодветни мерки за заштита од прашина. Лицата кои директно не се вклучени во градежните работи треба често да ги проверуваат мерките за заштита од прашина за да се уверат дека тие работат правилно и дека се почитуваат стандардите за заштита од прашина.

Употреба на системи за вршење на видео надзор

Системите за контрола на пристап до локацијата и за откривање неовластен пристап треба да бидат дополнети со системи за вршење на видео надзор. Системот за вршење на видео надзор треба да се интегрира во целокупниот безбедносен концепт. Офицерот за заштита на лични податоци мора секогаш да учествува во планирањето, дизајнирањето и имплементирање на системот за вршење на видео надзор. Централните технички компоненти што се потребни за системот за вршење на видео надзор треба да се инсталираат во соодветна средина и да бидат заштитени. Системот за вршење на видео надзор треба редовно да се тестира за да се обезбеди дека работи правилно и дека е во согласност со прописите за заштита на личните податоци.

Редундантен дизајн на непрекинато напојување

Системите на UPS уредот треба да бидат модуларни и дизајнирани да имаат вишок модул што ќе надомести за секој дефект без прекин. Ако е поставено напојување со две линии А-В за оперативни области на информатичката технологија, секоја од двете тековни патеки треба да биде опремена со независен систем на UPS уредот.

Редундантен дизајн на системи за напојување за итен случај

Системите за напојување за итни случаи (EPS) треба да бидат редундантни.

Центар за податоци или серверска просторија - закани што се вклучени овде:	
3 0.1	Пожар
3 0.2	Неповолни услови во околината
3 0.3	Вода
3 0.4	Акумулирање нечистотии, прашина, корозија
3 0.6	Катастрофи во животната средина
3 0.7	Поголеми настани во околината
3 0.8	Прекин или неисправност на напојувањето
3 0.10	Дефект или неисправност на мрежите за снабдување
3 0.11	Дефект или прекин на давателите на услуги
3 0.15	Прислушување
3 0.16	Кражба на уреди, медиуми за чување податоци и документи
3 0.24	Уништување уреди или медиуми за чување податоци
3 0.25	Дефект на уреди или на системи
3 0.26	Неисправност на уреди или на системи
3 0.29	Повреда на закони или на договори
3 0.30	Неовластено користење или администрирање уреди и системи
3 0.31	Неправилно користење или администрирање уреди и системи
3 0.32	Злоупотреба на овластување
3 0.34	Напад
3 0.41	Саботажа
3 0.44	Неовластен влез во простории

4.9. Архиви за медиуми за чување податоци

4.9.1. Вовед

Архивите за медиуми за чување податоци се затворени простории во организацијата што се користат за чување на сите видови медиуми за чување податоци. Покрај медиумот за чување податоци што се користи за дигитални информации, ова ги вклучува и хартиените документи, како и другите медиуми.

4.9.2. Цел

Целта е да се опишат вообичаените закани и барања во врска со безбедноста на информациите на архивата за медиуми за чување податоци, како и да се заштитат информациите што се чуваат во таа архива.

4.9.3. Закани

Прекумерна температура и влажност

Флуктуациите на температурата или прекумерната влажност во областите каде што се чуваат долгорочни дигитални медиуми за чување податоци може да предизвикаат грешки во податоците како и истиот побрзо да ја намали својата функционалност според предвидениот рок на траење.

Недоволно правила

Ако вработените во организацијата не ги затвараат прозорците или не ги заклучуваат вратите откако ќе ја напуштат архивата за медиуми за чување податоци, тогаш може медиумите за чување податоци или други информации да бидат украдени. Сензитивните информации потоа може да бидат прегледани или пренесени од неовластени лица. Исто така може да се појават недостатоци ако вработените не се доволно свесни за постоењето на внатрешни правила. Имено, не е доволно само во организацијата да се утврдат правила, туку правилата треба и да се следат за да се обезбеди непречено работење. Многу проблеми настануваат и кога има воспоставени правила, но вработените не се доволно запознаени со нив.

Неовластено влегување во простории што содржат сензитивни информации

Доколку се имплементирани несоодветни контроли за пристап до локацијата, неовластени лица може да влезат во архивата за медиуми за чување податоци и да прегледуваат, крадат или да манипулираат со сензитивни информации. Ова може да влијае врз достапноста, доверливоста или врз интегритетот на архивирани информации. Оттука, ова може да ги наруши операциите на организацијата, дури и ако нема видлива директна штета.

Кражба

Бидејќи многу медиуми за чување податоци се навистина мали, многу е полесно да се стават во торба незабележано или брзо да се заминат со нив криејќи ги под облеката. Ако нема други копии, информациите на украдените медиуми за чување податоци ќе бидат изгубени. Понатаму, лицата што го презеле медиумот за чување податоци може да прочитаат и да откријат доверливи информации, што може да предизвика дополнителна штета на организацијата. Во повеќето случаи, овие последици се многу позначајни од трошоците за замена на украдените медиуми за чување податоци.

4.9.4. Мерки

Рачни противпожарни апарати

Во случај на пожар, во архивата за медиуми за чување податоци мора да има лесно достапни рачни противпожарни апарати. Овие рачни противпожарни апарати мора редовно да се проверуваат и да се сервисираат. Вработените што работат во близина на архива за медиуми за чување податоци мора да добијат инструкции за употреба на рачните противпожарни апарати.

Процедури и контрола за пристап до локацијата

Архивата за медиуми за чување податоци мора да биде достапна само за овластените лица. Пристапот до локацијата мора да се намали на минимален број на вработени. Затоа, пристапот до локацијата мора да се регулира и да се контролира. Организацијата мора да развие концепт и да донесе процедури за контрола на пристапот до локацијата. Ефективноста на заштитните мерки за контрола на пристап до локацијата што ги содржат процедурите мора редовно да се прегледуваат за да се провери дали тие сè уште се ефективни. За да се спречи занемарување на контролата на пристапот до локацијата или барем да се отежне ова, организацијата мора да примени дополнителни заштитни мерки за целата просторија.

Заштита од прашина и друга контаминација

Организацијата мора да обезбеди дека медиумите во архивата за медиуми за чување податоци се соодветно заштитени од прашина и од нечистотија. Барањата за ова мора да се анализираат во фазата на планирање. Строгата забрана за пушење мора да се почитува во архивите за медиуми за чување податоци.

Затворени прозорци и заклучени врати

Архивата за медиуми за чување податоци не треба да има прозорци ако може да се избегнат. Ако има прозорци, тие мора да бидат затворени при напуштање на архивата за медиуми за чување податоци. Вратата мора да биде заклучена и при напуштање на просторијата.

Користење заштитни ормани

Организацијата треба да има соодветни заштитни ормани за медиумите кои се чуваат во архивите за медиуми за чување податоци.

Избегнување цевки за вода

Организацијата во архивите за медиуми за чување податоци треба да избегнува да има непотребни цевки што носат вода. Ако цевките за вода сепак се поставени преку архива за медиуми за чување податоци, тие треба редовно да се проверуваат за да се обезбеди дека не пропуштаат вода. Освен тоа, треба да се преземат мерки на претпазливост за да се открие какво било истекување вода во рана фаза. За архива за медиуми за чување податоци во организација со високи барања за достапност, треба да се има процедури за одговор во кои точно се одредува кој треба да биде информиран во случај на протекување и како треба да се постапува во такви околности.

Усогласеност со климатските барања

Организацијата треба да обезбеди дека максималните и минималните вредности што се дозволени за температура и влажност, како и содржина на прашина во воздухот во просторијата, се запазени во архивата за медиуми за чување податоци. Вредностите на температурата и на влажноста на воздухот треба да се евидентираат и да се документираат неколкупати годишно за период од една недела. Сите констатирани отстапувања од целната вредност треба веднаш да се коригираат. Системот за климатизација којшто се користи треба редовно да се сервисира.

Безбедни врати и прозорци

Безбедносните заштитни мерки какви што се прозорците, вратите и сидовите треба да бидат соодветни и да бидат во функција на спречување на кражба, пожар и чад. Сите безбедносни врати и прозорци треба да се проверуваат редовно за да се обезбеди дека сè уште функционираат правилно. Организацијата треба да примени соодветни стандарди во однос на безбедносните врати и прозори со цел да се обезбеди заштита на целата архива за медиуми за чување податоци.

4.9.5. Напредни мерки

Алармен систем

Организацијата треба во архивите за медиуми за чување податоци да постави и инсталира соодветен алармен систем. Овој алармен систем треба редовно да се проверува и да се сервисира. Организацијата треба да обезбеди дека примателите на алармните пораки можат соодветно да одговорат на нив.

Архива на медиуми за чување податоци - закани што се вклучени овде:	
3_0.1	Пожар
3_0.2	Неповолни услови во околината
3_0.3	Вода
3_0.4	Акумулирање нечистотии, прашина, корозија
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.24	Уништување на уреди или медиуми за чување податоци
3_0.32	Злоупотреба на овластувања
3_0.44	Неовластен влез во простории

4.10 Работа на далечина

4.10.1 Вовед

Под работа на далечина се подразбираат сите задачи што делумно или целосно се извршуваат надвор од деловните простории и од објектите на организацијата со користење информатичка и комуникациска технологија. Кога станува збор за работа на далечина од дома, вработените редовно наизменично ја менуваат работата на дневно или на часовно ниво во домашната канцеларија и на работното место во организацијата.

4.10.2 Цел

Целта е да се заштитат информациите што се чуваат, обработуваат и пренесуваат за време на работата на далечина. Оттука, произлегуваат вообичаени закани и се дефинираат посебни барања за безбедна работа на далечина. Оваа точка се однесува на формата на работа на далечина што се одвива во домашна средина т.е. работа на далечина од дома. Се претпоставува дека е достапна безбедна телекомуникациска врска помеѓу дадена домашна работна станица и организацијата за да се овозможи размена на информациите и пристап до податоците на серверите на организацијата. Барањата од оваа точка ги опфаќаат следните три области:

- Организацијата на работата на далечина;
- Компјутер на работната станица на вработениот;
- Комуникациска врска помеѓу компјутерот за работа на далечина и организацијата.

4.10.3 Закани

Недоволно правила за локации за работа на далечина

Употребата на локации за работа на далечина бара дополнителни организациски договори помеѓу вработените и нивните претпоставени. Покрај тоа, вработените и нивните претпоставени треба да знаат што да прават доколку се случат инциденти во врска со безбедноста на локациите за работа на далечина. На пример, ако доверливи информации се најдат во рацете на трети лица, тогаш организацијата може да претрпи сериозна штета.

Неовластено приватно користење компјутери за работа на далечина

Полесно е да се користи непроверен и неодобрен хардвер или софтвер во домашната средина. Меѓутоа, ако го направите тоа невнимателно или неодговорно, на пример, може да дозволите злонамерен софтвер да пристапи до компјутерот за работа на далечина. Ова може да ги загрози доверливите информации на организацијата.

Одложувања што се предизвикани од привремено ограничена достапност на вработените

Ако вработениот нема фиксно работно време кога работи на далечина и не е договорено фиксно време кога мора да биде достапен, тоа може да предизвика одложување на работните процеси на организацијата.

Слаба интеграција на вработените во протокот на информации

Вработените што работат на далечина не се физички присутни во својата организација секој ден и имаат помалку можности да учествуваат во директна размена на информации со нивните претпоставени и со другите вработени во организацијата. Информациите што се пренесуваат вербално може да се одложат или воопшто да не стигнат до вработените што работат на далечина. Ова може да го наруши работниот тек и оперативните процеси и да ја ограничи продуктивноста на овие вработени во работните процеси на организацијата.

Непочитување на безбедносните заштитни мерки

На локациите за работа на далечина, постои недостаток на можностите за мониторинг што може да доведе до тоа вработените да не успеат да имплементираат некои заштитни мерки или да не можат да ги имплементираат сите препорачани или потребни безбедносни заштитни мерки, а тоа може да придонесе доверливи информации да се најдат во рацете на трети лица.

4.10.4 Мерки

Правила за работа на далечина

Организацијата мора сите аспекти на работата на далечина да ги уреди во соодветни правила за работа. На вработените што работат на далечина мора да им се достават применливите правила во кои се објаснуваат безбедносните заштитни мерки што треба да се применуваат. Организацијата мора редовно да ги ажурира овие правила за работа.

Барања во врска со безбедноста на компјутерите за работа на далечина

Организацијата мора да ги дефинира барањата во врска со безбедноста што треба да ги исполнуваат системите за информатичка технологија за работа на далечина. Притоа, мора да се обезбеди дека само овластени лица имаат пристап до компјутерите за работа на далечина. Освен тоа, компјутерите за работа на далечина мора да бидат заштитени за да можат да се користат само за овластени цели.

Свесност и обука на вработените

Организација мора да ги информира вработените за можните ризици во врска со работата на далечина, на пример со помош на водич. Понатаму, мора да бидат едуцирани за соодветните безбедносни заштитни мерки на организацијата и да се обучат како да се справуваат со истите. Заштитните мерки за обука и свесност за вработените треба редовно да се спроведуваат.

Креирање безбедносен концепт за работа на далечина

Организацијата треба да има безбедносен концепт за работа на далечина пропишан во процедура што ги опишува безбедносните цели, потребите за заштита, безбедносните барања и вклучените ризици. Процедурата треба редовно да се проверува и да се ажурира. Безбедносниот концепт за работата на далечина треба да биде усогласен со целокупниот безбедносен концепт на организацијата.

Правила за користење на комуникациската технологија за работа на далечина

Организацијата треба да утврди јасни правила за тоа кои комуникациски технолошки решенија може да се користат под конкретни услови за целите на работа на далечина. Исто така треба да постојат правила за професионално и за приватно користење на услугите на интернет при работа на далечина. Тука, исто така треба да се објасни дали приватната употреба е дозволена или е забранета.

Проток на информации помеѓу вработените и организацијата

Организацијата треба да обезбеди редовна внатрешна размена на информации помеѓу вработените што работат на далечина и вработените во самата организација. Организацијата треба да ги информира сите вработени за безбедносните барања и за другите аспекти што се значајни за безбедноста. Вработените што работат на далечина треба да знаат кога и на кој начин да комуницираат со вработените присутни во организацијата. Техничките и организациските правила за работа на далечина за извршување на задачите, безбедносните инциденти и другите проблеми треба да се дефинираат и за тоа да се информираат вработените.

Концепт за поддршка и одржување за локации за работа на далечина

Организацијата треба да подготви посебен концепт за поддршка и одржување за локациите за работа на далечина. Со овој концепт треба да се прецизираат следните аспекти: лица за контакт за кориснички услуги, датуми на одржување, далечинско одржување, транспорт на уреди за информатичка технологија и воведување стандардни компјутери за работа на далечина. Лицата кои ќе бидат определени за контакт за хардверски и софтверски проблеми треба да располагаат со соодветни квалификации за да можат да ги решат проблемите и да им обезбедат услови на вработените за да можат да продолжат со својата работа.

Анализа на барањата за локација за работа на далечина

Организацијата треба да изврши анализа на барањата пред да се постави локација за работа на далечина. Во таа анализа треба да се вклучат хардверските и софтверските компоненти што се потребни за локациите за работа на далечина. Барањата за секоја локација за работа на далечина треба да се договорат со лицата задолжени за информатичка технологија и истите треба секогаш да се утврдат и да се документираат.

Работа на далечина - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитетни
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.24	Уништување на уреди или медиуми за чување податоци
3_0.25	Дефект на уреди или на системи
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.33	Недостиг на кадар
3_0.40	Одрекување на дејствија
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.11 Безбедност на информации при патувања во странство**4.11.1 Вовед**

Патувањата во врска со работата сега се дел од секојдневниот живот во многу организации. За да можат да продолжат да работат надвор од нормалното работно опкружување, луѓето треба да патуваат и со документи во печатена форма и со информатичка технологија, како што се лаптопи, паметни телефони, таблети, преносливи хард-дискови или USB мемориски дискови. За службените патувања, особено оние во странство, постојат голем број закани и ризици за безбедноста на информациите што не постојат за време на нормалното деловно работење.

Секое патување мора да се процени одделно бидејќи секогаш постои различно ниво на закана во зависност од комбинацијата на целта на патувањето (на пример, деловен состанок, конференција, конгрес или семинар), времетраењето и дестинацијата, што исто така влијае врз заштитата на информациите кои имаат клучно значење за деловното работење.

Заканата што произлегува од опкружувањето е особено значајна кога патуваат поради фактори какви што се јавните мрежи што не се под контрола на организацијата. Ова значи дека ризиците што организацијата веќе ги предвидела може повторно да станат реални. Во зависност од дестинацијата на земјата, ризиците со кои се соочува некој при патувањата во странство, исто така, често се значително повисоки отколку на домашните патувања.

Кога вработените постојано патуваат на различни дестинации со различни регулаторни и законски барања, не е секогаш лесно да се заштитат оперативните информации. На пример, законските барања и проверките на граничната контрола може да станат построги и со тоа да влијаат врз зачувувањето на доверливоста на податоците. Ова води до посебни барања за безбедноста на информациите, кои зависат од видот и од времетраењето на даденото патување, како и од самата дестинација. Во таа смисла, значајна улога имаат специфичните политички, општествени, религиозни, географски, климатски, правни и регулаторни согледувања.

4.11.2. Цел

Целта е да се опишат начините за заштита на доверливоста, интегритетот и достапноста на сите видови информации што се земаат предвид при патувања во странство, без разлика дали се во електронска или во хартиена форма. Доверливите информации што сите вработени кои патуваат ги носат со себе во форма на знаење, исто така се предмет на оваа точка. Понатаму, целта ги наведува соодветните прописи и заштитни мерки за постапување со информациите и податоците што треба да се заштитат при патување во странство. Мора да се земат предвид и основните услови кои се однесуваат на информатичката технологија, на заштитата на личните податоците и на законот.

Во оваа точка се истакнуваат ризиците и барањата на специфичните околности што се директно поврзани со безбедното користење на информатичката технологија, информациите и уредите при патување во странство.

Целта е предвидена да се користи од одговорните лица во организацијата како водич за воспоставување соодветни безбедносни заштитни мерки во контекст на безбедноста на информациите при такви патувања, имајќи ги предвид основните начела. Многу од овие закани се појавуваат кога се обработуваат информации во средини што не се под контрола на организацијата.

4.11.3. Закани

Прислушување и шпионирање информации / индустриска шпионажа

Шпионажата се однесува на напади чија цел е да прибираат, да проценуваат и да обработуваат информации за организации, луѓе, производи или за други целни објекти. Особено при патување во странство, постојат непознати извори на ризик на кои не можат да влијаат напорите на организацијата за управување со безбедноста на информациите. Како општо правило, во просторот во странство и во средината на информатичката технологија има многу ризици што произлегуваат од насоченото прислушување лични разговори, комуникациски линии, телефонски разговори и преноси на податоци. Особено кога лицето е во странство, ова може да биде проблематично и тешко да се процени во однос на правните опции што се достапни во такви случаи.

Заканите може да влијаат и врз јавните простори и врз просториите и околностите во други организации, како и врз канцелариите на самите претставници на организацијата во странство. Уреди какви што се мобилните телефони исто така може да се користат за снимање или за слушање разговори без да се забележи тоа. Покрај тоа, многу системи за информатичка технологија се опремени со микрофон и камера, до кои може да се добие пристап и потоа може да се искористат.

Понатаму, може да има ограничувања при влез или при напуштање одредени земји, кои ги отфрлаат или се спротивставуваат на регулаторните одредби на земјата на потекло на вработениот и безбедносните барања на организацијата. На пример, може да се побара пристап до податоците што се зачувани на преносни компјутери и на други преносливи системи за информатичка технологија. Ова може да овозможи преглед на доверливи и лични податоци, па дури и нивно копирање и зачувување до одреден степен. Бидејќи оваа информација може да вклучува работи какви што се стратегиски документи или строго доверливи нацрти од организација, потенцијалната злоупотреба секогаш мора да се предвиди во случај на контрола/инспекција (индустриска шпионажа).

При патување во странство, постојат и други сложени ризици од технички аспект, покрај прислушувањето информации. Сензитивните податоци често може едноставно да се шпионираат со користење оптички, акустични или електронски методи бидејќи стандардите на кои е навикнато некое лице во однос на прописите за безбедност на информациите не може да се очекуваат во многу случаи. Меѓу другите фактори, ова се однесува на општото ниво на безбедност во земјата и на локалните околности што самото лице не може да ги избегне.

Откривање и злоупотреба на сензитивни информации (електронски и хартиени)

Кога се разменуваат информации, ненамерно може да се пренесат сензитивни информации заедно со информациите што биле наменети да се пренесат. Ова може да се случи кога информациите се испраќаат електронски, за време на телефонски повик или кога медиумите за чување податоци се предаваат лично. При патување во странство, сигурната размена на информации понекогаш е уште потешка поради придружните околности што се технички несигурни. Покрај тоа, луѓето што службено патуваат поради невнимание може да остават доверливи документи и во хартиена и во електронска форма, кои се видливи на јавни места или во хотелски соби. Комуникацијата со непознати системи за информатичка технологија и мрежи секогаш претставува потенцијална закана за уредите на патникот. Ова може да овозможи, на пример, копирање доверливи информации. Во меѓувреме, странските медиуми за чување податоци исто така може да содржат злонамерен софтвер. Ова носи ризик важните податоци да бидат украдени, манипулирани, криптирани или избришани. Истовремено, може да бидат нарушени интегритетот и достапноста на системите за информатичка технологија. Ваквата состојба се влошува со фактот што размената на податоци во странство често се случува преку несигурни медиуми, а за кои вработените не се секогаш свесни.

Употреба на лажни идентитети

Комуникацијата за време на патување вклучува зголемен ризик дека напаѓачите може да се обидат да го фалсификуваат идентитетот (и лично и електронски) или да преземат идентитет, како на пример преку маскирања, методи на измама, киднапирање или напади од „човек во средината“. Корисниците може да бидат измамани за идентитетот на нивниот партнер во комуникацијата до тој степен што откриваат сензитивни информации. Напаѓачите можат да добијат лажен дигитален идентитет, на пример, со шпионирање корисничка идентификација и лозинка, манипулирање со полето на испраќачот на пораката или манипулирање со електронска адреса. Вработените не ги познаваат секогаш лично деловните партнери на организацијата во странство. Ако вработениот има доверба во странец што се претставува како деловен партнер и го поседува основното знаење што тоа лице би го имало, вработениот може да пренесе вредни информации. Меѓутоа, во реалноста, тоа би можело да биде измамник што се претставува како деловен партнер. Безбедносните барања во смисла на доверливост и интегритет никогаш не можат целосно да се исполнат во објекти што не ѝ припаѓаат на организацијата, особено во странство. Секогаш постои потенцијален ризик дека дури и опремата што вообичаено би била класифицирана како безбедна, може да биде манипулирана. Ова вклучува, на пример, употреба на идентификација на повикувач на телефон или идентификација на испраќач на факс за претставување лажен идентитет и добивање информации.

Недостиг на свест за безбедноста и негрижа при постапување со информации

Иако во организациите постојат организациски прописи и процедури за техничка безбедност за преносни системи за информатичка технологија и мобилни медиуми за чување податоци, тие честопати не се доволно почитувани и применети од вработените. Мобилните медиуми за чување податоци често се оставаат без надзор во салите за состаноци или дури и во возовите.

Покрај тоа, вработените може да прифатат подароци во форма на медиуми за чување податоци (пример USB) и случајно да се поврзат со нивните лаптопи. Ова носи ризик лаптопот да биде заразен со злонамерен софтвер, а како последица на тоа сензитивните податоци може да бидат украдени, манипулирани или криптирани. Во јавниот превоз, па дури и за време на состаноци, често може да се забележат луѓе како отворено разговараат за суштински информации за организацијата. Некои надворешни лица лесно може да ги слушнат овие информации и потенцијално да ги искористат за да му наштетат сериозно на вработениот или на неговата организација.

Повреда на локалните закони или регулативи

При патување во странство, треба особено да се земат предвид законите и регулативите во конкретната земја, бидејќи тие можат да бидат многу различни од правната состојба во земјата на потекло. Релевантните закони и регулативи во земјите (на пример, во врска со заштитата на личните податоци, барањата за информации, одговорноста или пристапот до информации за трети лица) честопати се непознати или неправилно оценети од лицата. Како резултат на тоа, голем број закони може да бидат прекршени не само во странство, туку и дома, како на пример, ако личните податоци за домашните клиенти се пренесуваат без заштита преку јавните мрежи додека се на службено патување во странство.

Принуда, изнуда, киднапирање и корупција

Честопати постојат и други безбедносни ризици, кои произлегуваат од политичките и од социјалните околности во странство. Безбедноста на информациите, а исто така и на самите патници, може да биде загрозувана преку принуда, изнуда или киднапирање при патување во странски земји. На пример, вработените може да подлежат на закани за насилство кои ќе ги принудат да предадат сензитивни податоци за организацијата. Во тој процес, тие може да бидат принудени да ги заобиколат или да ги игнорираат безбедносните политики и заштитни мерки. Претежно целта на напаѓачите е да украдат или да манипулираат со сензитивни информации за да се мешаат во деловните процеси или да се збогатат себеси и другите. Напаѓачите често се водени од политички, идеолошки и финансиски цели. Покрај заканата од насилство, постои и можност за поткуп или корупција: на лицата може да им бидат понудени пари или други поволности, со цел да ги убедат да предадат доверливи информации на неовластени лица или да извршат други нарушувања на безбедноста на организацијата. По правило, принудата, изнудата, киднапирањето и корупцијата ги нарушуваат или ги загрозуваат регулативите за безбедност на информациите.

Информации од несигурни извори

Додека работат во странство, на лицата може да им бидат испратени лажни или погрешни информации за да бидат измамани. Оваа измама може да доведе до вклучување неточни изјави во извештаите што се од клучно значење за организацијата. Покрај тоа, ова може да доведе до донесување на важни одлуки засновани на лажни податоци, пресметки што даваат неточни резултати и, како резултат на сето тоа, да се донесат и погрешни одлуки.

Кражба или губење уреди, медиуми за чување податоци и документи

Особено при патувања во странство, мобилните уреди лесно може да се изгубат или да се украдат. Колку се помали и попопуларни овие уреди, толку е поголем ризикот од кражба. Покрај материјалната штета што произлегува од непосредното губење мобилен уред, објавувањето сензитивни податоци (на пример, е-пошта, белешки или адреси од состаноци) може да доведе до дополнителна финансиска штета. Ова исто така може да наштети на угледот на организацијата.

4.11.4. Мерки

Политика за безбедност на информации за патувања во странство

Организацијата мора да ги разгледа и да ги регулира сите аспекти што се важни за безбедноста на информациите во врска со работата во странство. Безбедносните заштитни мерки што се преземени во овој поглед мора да се документираат во политиката за безбедност на информации за патувања во странство. На вработените што работат во различни земји мора да им се даде политика за безбедност или брошура со упатства во која детално се наведени безбедносните заштитни мерки што треба да ги почитуваат. Покрај тоа, мора да се воспостави безбедносен концепт за ракување со преносни системи за информатичка технологија при патувања во странство што доволно детално ги опишува сите безбедносни барања и заштитни мерки. Имплементацијата на безбедносниот концепт мора редовно да се проверува од страна на организацијата.

Подигање на свеста на вработените за безбедноста на информациите при патување во странство

Корисниците мора да бидат свесни и обучени за одговорно ракување со информатичката технологија и преносливите системи за информатичка технологија при патувања во странство. Корисниците мора да бидат свесни за опасностите што можат да произлезат од несоодветно постапување со информации, неправилно уништување податоци и медиуми за чување податоци или злонамерен софтвер и небезбедна размена на податоци. Исто така мора да се демонстрираат и границите на безбедносните заштитни мерки што се користат. Корисниците мора да бидат овластени и поттикнати да спречат загуба или кражба или да побараат стручен совет во случај на недоследности. Покрај тоа, на вработените треба да им се укаже за законските барања за поединечни дестинации во однос на безбедноста на патувањето. Овластеното лице за безбедност на информациите мора да ги следи законските барања во контекст на безбедноста на информациите (на пример, заштита на личните податоци, прописите за безбедност на информатичката технологија) и да ја подигне свеста на вработените во организацијата.

Идентификација на регулативи, услови за патување и услови за животна средина што се специфични за земјата

Пред патувањето, вработените за безбедност на информации и вработените за човечки ресурси на организацијата мора да ги разгледаат важечките прописи на секоја земја и да го запознаат вработениот со истите.

Организацијата мора да воспостави, да спроведе и да информира за политиките и заштитните мерки, кои овозможуваат соодветна заштита на внатрешните податоци. Притоа мора да се земат предвид индивидуалните услови за патување и условите на средината. Пред почетокот на патувањето, вработените мора да се запознаат и со климатските услови за конкретната земја и да ги одредат заштитните мерки што им се потребни (на пример, вакцини) и информатичката технологија што треба да ја земат со себе.

Користење екрани за приватност

Особено кога се во странство, корисниците мора да се погрижат да не можат да се шпионираат никакви сензитивни информации додека тие работат на мобилни уреди. За таа цел, мора да се користат соодветни екрани за приватност, кои го покриваат целиот екран на секој уред и спречуваат шпионажа на информации.

Користење на заклучување на екран/код за вклучување

Во организацијата мора да се користи заклучување на екранот или код за вклучување што спречува трети лица да пристапат до податоците на мобилниот уред. Корисникот мора да употреби соодветен код или безбедна лозинка за уредот за оваа намена. Заклучувањето на екранот мора автоматски да се активира по краток период на неактивност.

Брзо известување за губење податоци

Вработените мора веднаш да пријават какво било губење или кражба на информации, системи за информатичка технологија или медиуми за чување податоци на организацијата. За таа цел, мора да има јасни канали за известување и лица за контакт во организацијата. Организацијата мора да ги процени можните влијанија од загубата и да преземе соодветни заштитни мерки.

Безбеден далечински пристап до мрежата на организацијата

Со цел да се овозможи безбеден далечински пристап до мрежата на организацијата за вработените што се на патувања во странство, организационата единица за информатичка технологија мора однапред да постави безбеден далечински пристап (на пример, преку виртуелна приватна мрежа, VPN). Пристапот до VPN мора да биде криптографски обезбеден. Покрај тоа, корисниците мора да имаат доволно безбедни податоци за пристап за успешно да извршат автентикација на нивните крајни уреди и на мрежата на организацијата. Вработените мора да користат безбеден далечински пристап за сите комуникации што се можни во овие околности. Организацијата мора да обезбеди дека само овластени лица можат да пристапат до системите за информатичка технологија што имаат далечински пристап. Колку што е можно повеќе, мобилните системи за информатичка технологија мора да бидат заштитени од директен пристап до интернет со рестриктивно конфигуриран личен заштитен сид.

Безбедно користење јавни WLAN-мрежи

Организацијата мора да регулира дали на мобилните системи за информатичка технологија им е дозволен директен пристап до интернет. За пристап до мрежата на организацијата преку јавно достапни WLAN-мрежи, корисникот мора да користи VPN или сличен безбедносен механизам. Исто така, мора да се преземат и безбедносни заштитни мерки кога се користат WLAN точки за пристап до интернет (hotspot).

Безбедно ракување со мобилни медиуми за чување информации

Доколку се користат мобилни медиуми за чување податоци, корисниците мора однапред да обезбедат дека медиумите не се заразени со злонамерен софтвер. Пред да ги пренесат мобилните медиуми за чување податоци, корисниците мора да обезбедат дека медиумите не содржат било какви сензитивни информации. Доколку медиумот за чување податоци повеќе не се користи, мора безбедно да се избрише, особено ако треба да се пренесе на други лица. За таа цел, медиумот за чување податоци мора одново да се избрише со користење доволно безбеден метод што е предвиден од организацијата.

Криптирање на преносни системи за информатичка технологија и медиуми за чување податоци

За да се обезбеди дека неовластени трети лица не можат да пристапат до сензитивните информации, вработените мора да се погрижат сите сензитивни информации да бидат обезбедени во согласност со важечките внатрешни политики пред да патуваат. Мобилните медиуми за чување податоци и податоците за клиентите треба да бидат криптирани од корисникот или од организационата единица за информатичка технологија пред патувањето. Криптографските клучеви мора да се чуваат одделно од криптираните уреди. При криптирање на податоците, треба да се почитуваат прописите на конкретната земја. Конкретно, треба да се земат предвид прописите што се специфични за земјата за користење лозинки и декриптирање на податоци.

Безбедно уништување сензитивни материјали и документи

Организацијата мора да ги информира вработените за можностите за соодветно и безбедно уништување на сензитивни документи. Корисниците мора да ги почитуваат овие прописи. Тие не смеат да располагаат со интерната документација на организацијата додека не биде безбедно уништена. Ако ова не е можно локално или вклучува работа со документи или со медиуми за чување податоци што содржат особено сензитивни информации, овие предмети мора да се чуваат до враќањето на вработениот од службено патување и потоа соодветно да се уништат.

Употреба на уреди против кражба

За заштита на мобилните системи за информатичка технологија надвор од организацијата, корисниците треба да користат уреди за заштита од кражба, особено на места каде што има зголемен јавен сообраќај или голема флукуација (променливо движење) на корисниците. Критериумите за набавка и користење на уредите против кражба треба да се приспособат на процесите на организацијата и соодветно да се документираат.

Пренос на неопходни податоци и медиуми за чување податоци

Пред да замине на патување, вработените треба да проверат кои податоци не се неопходни за системите за информатичка технологија што ги носат со себе (лаптоп, таблет, паметен телефон итн.). Сите податоци што не треба да останат на уредот, треба безбедно да се избришат. Меѓутоа, ако е неопходно да се земат сензитивни податоци на патувања, тоа треба да се направи во криптирана форма. Покрај тоа, мобилните медиуми за чување податоци што може да се земаат при патувања во странство и соодветните безбедносни заштитни мерки што треба да се земат предвид (на пример, заштита од злонамерен софтвер, криптирање податоци што се од суштинско значење за бизнисот, чување мобилни медиуми за чување податоци) треба да се воспостават во писмена форма. Вработените треба да ги знаат и да ги следат правилата и процедурите на организацијата пред да тргнат на патување. Овие барања во врска со безбедноста треба да се разликуваат во зависност од потребите за заштита на податоците со кои треба да се постапува во странство и податоците до кои треба да се пристапи.

Криптографски обезбедена комуникација преку е-пошта

Вработените треба криптографски да ги обезбедуваат комуникациите засновани на е-пошта во согласност со внатрешните правила на организацијата. Е-поштата треба да биде соодветно криптирана или дигитално потпишана. Јавни системи за информатичка технологија, какви што се оние во хотелите или во интернет кафулињата, не треба да се користат за пристап до е-пошта. За комуникација преку услуги со е-пошта (на пример, веб-пошта), организацијата треба однапред да провери кои безбедносни механизми се имплементирани од давателите на услуги и дали тие ги задоволуваат барањата за внатрешна безбедност на организацијата. Тие вклучуваат, на пример, безбедно работење на серверот, воспоставување криптирана конекција и времетраење на чувањето на податоците.

4.11.5. Напредни мерки

Безбедност на преносните системи за информатичка технологија

Пред почетокот на патувањето, треба да се утврдат потребите за заштита на одредени информации со кои треба да се постапува на мобилниот медиум за чување податоци на вработениот или на податоци за клиентите додека е во странство. Организацијата треба да провери дали информациите што треба да се земат посебно треба да се заштитат и соодветно да користи медиум за чување податоци со ниско ниво на зрачење или медиум што е отпорен на зрачење.

Заштита на интегритетот со користење контролни суми (checksums) или дигитални потписи

Корисниците треба да користат контролни суми за да го потврдат интегритетот на податоците за време на преносот и сигурносните копии. За да се постигне уште подобро ниво на заштита во зачувувањето на интегритетот на сензитивните информации, треба да се користат дигитални потписи.

Користење наменски хардвер за патување

За да се обезбеди дека трети лица не можат да пристапат до сензитивните информации на организацијата при патување во странство, организационата единица за информатичка технологија треба да им обезбеди на вработените претходно конфигуриран хардвер за патување. Врз основа на неопходноста, овој хардвер за патување треба да ги обезбедува само функциите и информациите што се потребни за спроведување на деловните активности.

Ограничени овластувања за патувања во странство

Пред почетокот на патувањето, треба да се проверат овластувањата што навистина му се потребни на вработениот за да ја врши својата секојдневна работа додека е во странство. За таа цел, треба да се разгледа можноста организационата единица за информатичка технологија да ги повлече правата за пристап на вработениот за времетраењето на патувањето, со цел да се спречи неовластен пристап до информации во рамките на организацијата.

Патувања во странство - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.35	Принуда, изнуда или корупција
3_0.36	Кражба на идентитет
3_0.42	Социјален инженеринг
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.12. Мрежна архитектура и дизајн

4.12.1. Вовед

За извршување на своите деловни операции и процеси, на организациите им се потребни мрежи што овозможуваат размена на информации и податоци, имплементација на апликации и вклучување во разни други активности, при што овие мрежи се поврзани со мрежите на организациите со кои соработуваат и на интернет. Притоа, тие вклучуваат сè повеќе мобилни уреди и елементи поврзани со „интернет на нештата (IoT)“. Освен тоа, услугите во облак (cloud services) за податоци и услугите за унифицирана комуникација и соработка (UCC), сè повеќе се користат преку мрежи што овозможуваат размена на информации и податоци. Придобивките што произлегуваат се неспорни. Сепак, сите овие уреди и услуги создаваат и поголеми ризици. Затоа е важно организациите да ги заштитат своите мрежи со безбедна мрежна архитектура. За изградба на локална мрежа (LAN) или мрежа за пошироки области (WAN) со безбедна архитектура, потребно е претходно планирање. Дополнително, надворешните мрежи на кои може да им се верува само до одредена мера (какви што се мрежите на клиентите или самиот интернет) мора да бидат соодветно интегрирани. За да се обезбеди високо ниво на безбедност, треба да се земат предвид дополнителни безбедносни аспекти. Примерите вклучуваат безбедно одвојување различни клиенти и групи уреди на ниво на мрежа и контрола на нивните комуникации преку заштитен сид. Друг важен безбедносен елемент, особено за клиентите е контролата на пристапот до мрежата.

4.12.2. Цел

Целта е да се воспостави безбедност на информациите како составна компонента на мрежната архитектура и дизајн.

4.12.3 Закани

Дефект или недоволна ефикасност на комуникациските врски

Во случај кога комуникациските врски имаат недоволен капацитет или нивната ефикасност повеќе не е доволна како последица на настанат технички дефект или напад на одбивање услуга (DoS), комуникацијата на клиентите со серверите би можела да биде ограничена. Овие околности можат да го зголемат потребното време за пристап до внатрешните и до надворешните услуги. Како резултат на тоа, би можело да се користат овие услуги само во ограничен обем, ако воопшто и тоа е можно. Информациите што се важни за организацијата може да не бидат повеќе достапни и истото може да доведе до застој во нејзиното работење.

Несоодветно обезбеден пристап до мрежа

Доколку внатрешната мрежа е поврзана на интернет и преносот не е доволно заштитен (на пример, поради недостаток или неправилно конфигурирани заштитни сидови), напаѓачите може да пристапат до сензитивни информации на организацијата и да ги копираат или да манипулираат со нив.

Несоодветно структурирање на мрежата

Ако мрежата е неправилно структурирана или проширена, тоа може да доведе до небезбедни мрежни топологии или мрежни конфигурации. Ова би им овозможило на напаѓачите лесно да ги препознаат недостатоците и да навлезат во внатрешната мрежа на организацијата, каде што можат да украдат информации, да манипулираат со податоци или да нарушат цели системи. Во неправилно структурирана мрежа каде што следењето на безбедносните системи е ограничено, напаѓачите исто така можат да останат незабележани подолг временски период.

4.12.4. Мерки

Безбедносна политика за мрежата

Организацијата врз основа на општата безбедносна политика треба да подготви и специфична политика за нејзината мрежа. Политиката мора сеопфатно да ги опишува барањата и спецификациите за тоа како безбедно да се дизајнираат и да се конструираат мрежи. Политиката мора да содржи информации за следното:

- Случаите во кои зоните треба да се сегментираат и групите корисници или клиентите треба да се одделат логички, па дури и физички,
- Кои комуникациски односи и кои мрежни и апликативни протоколи се дозволени за секој случај,
- Како сообраќајот на податоци за администрирање и следење треба да се одвои во мрежата,
- Каков вид внатрешна комуникација (WAN, безжични мрежи) е дозволен низ локациите,
- Каково криптирање е потребно на WAN, LAN или радиоврски,
- Каков вид меѓу локациска комуникација е дозволен.

Сите вработени што се одговорни за дизајн на мрежата мора да бидат запознаени со политиката. Таа мора да ја сочинува основата на нивната работа. Доколку политиката се смени или има отстапувања од наведените барања, тоа мора да се документира и да се договори со овластеното лице за безбедност на информации. Правилното спроведување на политиката мора редовно да се проверува и резултатите од тие проверки мора да се документираат.

Документација за мрежата

Организацијата мора да подготви целосна документација за мрежата, која мора да вклучува план за мрежата и истата постојано да се ажурира. Оваа документација мора да го содржи првичното истражување на фактичката состојба (вклучувајќи ја и ефикасноста на мрежата), како и сите направени промени на мрежата. Исто така, мора да се документира логичката структура на мрежата, особено доделувањето подмрежи и зонирањето и сегментацијата на мрежата.

Спецификација за мрежните барања

Организацијата мора да подготви спецификација за барањата врз основа на безбедносната политика за соодветната мрежа. Спецификацијата мора постојано да се ажурира. Од овие барања мора да биде можно да се добијат сите суштински елементи на мрежната архитектура и дизајн.

Поделба на мрежа во зони

Целокупната мрежа мора да биде физички поделена во најмалку следните три зони: внатрешна мрежа, демилитаризирана зона (DMZ) и надворешни врски (вклучувајќи интернет и други несигурни мрежи). Премините помеѓу зоните мора да бидат заштитени со заштитен сид. Овој метод на контрола мора да го следи начелото на локална комуникација, така што заштитните сидови дозволуваат само овластени комуникации (впишување во т.н. бела листа). Несигурните мрежи (на пример, интернет) и сигурните мрежи (на пример, интранет) мора да бидат одделени со двостепена структура на заштитен сид кој се состои од филтри за пакети со статус (заштитни сидови). За да се одвои интернетот и надворешната демилитаризирана зона во мрежата, мора да се користи најмалку филтер за пакети со статус. Во двостепената архитектура на заштитниот сид, целиот дојдовен и појдовен сообраќај на податоци мора да се контролира и да се филтрира преку надворешниот филтер за пакети или внатрешниот филтер за пакети.

Структурата P-A-P што се состои од филтер за пакети, порта на апликациски слој или безбедносен посреднички (прокси) систем и филтер за пакети мора секогаш да се примени кога тоа е потребно во согласност со безбедносната политика или спецификацијата за барања.

Сегментација на однос клиент со сервер

Клиентите и серверите мора да бидат поставени во различни мрежни сегменти. Комуникацијата помеѓу овие мрежни сегменти мора да се контролира од најмалку филтер за пакети со статус. Треба да се истакне дека можните исклучоци што овозможуваат позиционирање на клиентите и на серверите во сегмент на споделена мрежа се опфатени во точките специфични за апликацијата и за системот. За пристап на гости и мрежни области каде што нема внатрешна контрола на крајните уреди, мора да се воспостават посебни мрежни сегменти.

Сегментација на краен уред во внатрешната мрежа

Крајните уреди што се позиционирани во даден мрежен сегмент мора да соодветствуваат на слично ниво на безбедност.

Заштита на сензитивни информации

Сензитивните информации мора да се пренесат со помош на протоколи што се безбедни според најсовремената технологија во безбедноста на информациите, освен ако за комуникација не се користат сигурни посебни мрежни сегменти (на пример, во рамките на мрежата за управување). Доколку не е можно да се користат такви протоколи, мора да се имплементираат соодветни техники за криптирање и автентикација според најсовремената технологија во безбедноста на информациите.

Основна заштита на пристап до интернет

Интернет сообраќајот мора да се насочува преку структура на заштитен сид. Движењата на податоци мора да бидат ограничени на потребните протоколи и комуникациски односи од структурата на заштитниот сид.

Основна заштита на комуникација со несигурни мрежи

Организацијата мора да го утврди нивото на доверливост на секоја мрежа. Несигурните мрежи (мрежите на кои не може да им се верува) мора да се третираат како интернет и соодветно да се обезбедат.

Сегментација на демилитаризирана зона (DMZ) за пристап од интернет

Структурата на заштитниот сид на организацијата мора да биде дополнета со надворешна демилитаризирана зона (DMZ) за сите услуги и апликации до кои може да се пристапи од интернет. Треба да се подготви концепт за сегментација на DMZ, кој на транспарентен начин ќе ги имплементира соодветната безбедносна политика и спецификацијата за барања. Во зависност од нивото на безбедност на системите за информатичка технологија, сегментите на DMZ мора дополнително да се поделат. Надворешната DMZ мора да биде поврзана со филтерот за надворешни пакети.

Заштита на комуникациите што влегуваат во внатрешната мрежа од интернет

Пристапот до внатрешна мрежа заснован на интернет протокол мора да се одвива преку безбеден комуникациски канал. Пристапот мора да се ограничи на доверливи системи за информатичка технологија и корисници. VPN-портите од овој вид треба да се постават во надворешна DMZ. Треба да се обезбеди дека до соодветно зајакнатите VPN-порти може да се пристапи директно од интернет. Обидите за пристап до внатрешна мрежа за кои е извршена автентикација преку VPN-портата, мора најмалку да поминат низ внатрешен заштитен сид.

Системите за информатичка технологија не смеат да пристапуваат до внатрешна мрежа преку интернет или надворешна DMZ. Треба да се обезбеди дека сите исклучоци од ова барање се опфатени во соодветните точки што се специфични за апликацијата и за системот.

Заштита на излезна внатрешна комуникација на интернет

Излезната комуникација од внатрешна мрежа до интернет мора да се одвои преку безбедносен посреднички (прокси) систем. Ова одвојување мора да се случи надвор од внатрешната мрежа. Ако се користи P-A-P структура, излезната комуникација секогаш треба да се раздвојува од безбедносните посреднички (прокси) системи на P-A-P структурата.

Мрежно планирање

Секоја мрежна имплементација мора да се планира на соодветен, сеопфатен и транспарентен начин. Во овој контекст, мора да се почитуваат безбедносната политика и спецификацијата за барања. Покрај тоа, мора да се земат предвид најмалку следните аспекти при планирањето во согласност со прифатените потреби:

- Врската со интернет и, доколку е достапна, локалната мрежа и екстранетот,
- Топологијата на целокупната мрежа и мрежни области (т.е. зони и мрежни сегменти),
- Капацитетот и редундантноста на мрежата и на безбедносните компоненти, правците за пренос и надворешните врски,
- Протоколите што ќе се користат и нивната општа конфигурација и адресирање (конкретно, IPv4/IPv6 подмрежи на групи терминални уреди),
- Администрирање и мониторинг.

Мрежните планови мора редовно да се проверуваат.

Имплементација на мрежно планирање

Планираните мрежи мора правилно да се имплементираат. Ова мора да се потврди за време на процесот на одобрување.

Редовна анализа на недостатоците (Gap analysis)

Мора да се вршат редовни проверки за да се обезбеди дека дадената мрежа соодветствува на целната состојба. Во најмала рака, мора да се провери степенот до кој мрежата е во согласност со релевантната безбедносна политика и со спецификацијата за барања. Мора да се провери и степенот до кој имплементираната мрежна структура одговара на тековните мрежни планови. За таа цел, мора да се дефинираат одговорните лица и критериумите или спецификациите за тестирање.

Спецификација на мрежна архитектура

Врз основа на безбедносната политика и спецификациите на барањата, треба да се развие и доследно да се одржува архитектура за зоните на мрежата (вклучувајќи ја внатрешната мрежа, DMZ и надворешните врски). Во овој контекст, треба да се земат предвид сите релевантни архитектонски елементи на организацијата врз основа на нејзината специфична ситуација. Сепак, потребно е најмалку следното:

- Архитектурата на внатрешната мрежа, вклучувајќи спецификации за тоа како треба да се користат технологиите за виртуелизација на мрежата, комуникацијата на слој 2 и слој 3 и процедури за редундантност,
- Мрежна архитектура за надворешни врски, вклучително архитектури на заштитен сид, DMZ и дизајн на екстранет и спецификации за спојување на локацијата,
- Спецификации на мрежните локации каде што треба да се постават безбедносни компоненти какви што се заштитни сидови или IDS/IPS и безбедносните функции што тие треба да ги обезбедат,
- Спецификации за мрежните поврзувања на различните системи за информатичка технологија,
- Мрежна архитектура во домаќините (hosts) за виртуелизација, со посебен фокус на мрежата,
- Преклопувања на мрежна виртуелизација (NVO) и архитектура во вертикално интегрирани системи (ViS),
- Спецификација на основните елементи на архитектурата за приватен облак, како и заштита на врските со виртуелни приватни облаци, хибридни облаци и јавни облаци,
- Архитектура за безбедно администрирање и следење на инфраструктурата за информатичка технологија.

Спецификација на мрежен дизајн

Врз основа на мрежната архитектура, мрежниот дизајн за зоните (вклучувајќи ја внатрешната мрежа, DMZ и надворешните врски) треба да се развива и доследно да се одржува. За таа цел, архитектонски елементи треба да се разгледаат детално, вклучувајќи ги најмалку следниве точки:

- Дозволените форми на мрежни компоненти, вклучително виртуелизирани мрежни компоненти,
- Спецификации за тоа како WAN и безжичните врски треба да бидат заштитени,
- Поврзување на крајните уреди со компоненти за мрежен преклопник (switch), врски помеѓу мрежните елементи и употреба на протоколи за комуникација,
- Механизми за редундантност за сите мрежни елементи,
- Концепт за адреса за IPv4 и IPv6, како и поврзани концепти за рутирање и преклопување,
- Виртуелизирани мрежи во домаќини за виртуелизација, вклучително преклопувања на мрежна виртуелизација (NVO),
- Структура, поврзување и заштита на приватни облаци и безбедно поврзување виртуелни приватни облаци, хибридни облаци и јавни облаци,
- Спецификации за дизајн на мрежа за безбедна администрирање и следење на инфраструктурата на информатичката технологија.

P-A-P структура за интернет-конекција

Мрежата на организацијата треба да биде поврзана на интернет преку заштитен сид со P-A-P структура. Помеѓу двете нивоа на заштитен сид мора да се имплементира порта за апликациски слој (ALG) заснован на посреднички (прокси) систем. ALG мора да се поврзе преку сопствена мрежа за пренос (dual-homed), со надворешниот филтер за пакети и со внатрешниот филтер за пакети. Преносната мрежа не смее да биде зафатена со други задачи освен оние што се извршуваат за ALG.

Ако не се користи ALG, мора да се имплементираат соодветни безбедносни посреднички (прокси) системи. Безбедносните посреднички (прокси) системи мора да се поврзат преку

посебна мрежа за пренос (dual-homed). Мрежата за пренос не смее да биде зафатена со други задачи освен оние што се извршуваат за безбедносните посреднички (прокси) системи. Мора да се провери дали се можни меѓусебни напади преку безбедносните посреднички (прокси) системи. Ако е така, мрежата за пренос мора да биде соодветно сегментирана.

Целиот сообраќај на податоци мора да се одвои преку ALG или соодветните безбедносни посреднички (прокси) системи. Не смее да се конфигурира транспортна мрежа што меѓусебно ги поврзува двете фази на заштитен сид. Покрај тоа, внатрешниот заштитен сид мора да ја намали изложеноста на ALG или на безбедносните посреднички (прокси) системи на внатрешни напаѓачи или системи за информатичка технологија во внатрешната мрежа. Авторизирани и сигурни обиди за пристап до мрежата од VPN-портата до внатрешната мрежа, не треба да минуваат низ ALG или низ безбедносните посреднички (прокси) системи на P-A-P структурата.

Поделба на инфраструктурни услуги

Серверите што обезбедуваат основни услуги за инфраструктура за информатичка технологија треба да бидат позиционирани во посебен мрежен сегмент. Комуникацијата со нив треба да биде контролирана од филтер за пакети со статус (заштитен сид).

Распределба на наменски подмрежи за IPv4/IPv6 групи на крајни уреди

Различни IPv4/IPv6 крајни уреди треба да се распределат на наменски подмрежи според протоколот што се користи (IPv4/IPv6 или IPv4/IPv6 DualStack).

Одвојување на просторот за управување

За сеопфатно управување со инфраструктурата, треба да се користи управување надвор од опсегот. Во овој контекст, сите крајни уреди што се потребни за управување со инфраструктурата на информатичката технологија треба да бидат позиционирани во наменски мрежни сегменти. Комуникацијата со овие крајни уреди треба да се контролира со филтер за пакети со статус. Комуникацијата од и до овие мрежни сегменти за управување, треба да биде ограничена на потребните протоколи за управување со утврдени крајни точки на комуникација.

Областа за управување во зависност од безбедносната политика и спецификациите на барањата треба да ги вклучува најмалку следните мрежните сегменти:

- Мрежен сегмент(и) за системи за информатичка технологија што се одговорни за автентикација и авторизација на администраторската комуникација,
- Мрежен сегмент(и) за администрирање системи за информатичка технологија,
- Мрежен сегмент(и) за следење (мониторинг),
- Мрежен сегмент(и) што го содржи централниот систем за евиденција на пристап, вклучувајќи го серверот за најава (syslog) и SIEM серверот,
- Мрежен сегмент(и) за системи за информатичка технологија што се потребни за основни услуги од областа на управување,
- Мрежен сегмент(и) за интерфејси за управување на системите за информатичка технологија што треба да се администрираат.

Различните интерфејси за управување со системите за информатичка технологија мора да се одвојат според нивната намена и нивната мрежна позиција преку филтер за пакети со статус. Покрај тоа, следните системи за информатичка технологија (интерфејси за управување) треба да се одвојат преку посебни заштитни сидови:

- системи за информатичка технологија до кои може да се пристапи од интернет,
- системи за информатичка технологија во внатрешната мрежа,
- безбедносни компоненти што се наоѓаат помеѓу системите за информатичка технологија достапни од интернет и внатрешната мрежа.

Мора да се обезбеди дека сегментацијата не може да се заобиколи со комуникација при управувањето и мора да се спречи можноста за заобиколување сегменти.

Спецификација на концептот за сегментација

Врз основа на спецификациите на мрежната архитектура и дизајнот на мрежата, треба да се подготви концепт на сегментација за соодветната внатрешна мрежа. Овој концепт на сегментација треба да ги вклучи сите постојни виртуелизирани мрежи во домаќините (host) за виртуелизација. Концептот на сегментација треба да се планира, имплементира, следи и доследно да се одржува. Концептот треба да ги содржи најмалку следните аспекти, под претпоставка дека тие се планирани во целната средина:

- Мрежни сегменти што треба да се создадат првично, како и спецификации за тоа како треба да се создадат нови мрежни сегменти и како крајните уреди треба да се позиционираат во мрежните сегменти,
- Спецификација за сегментацијата на системи за развој и тестирање (поделба по фази),
- Контрола на мрежен пристап за мрежни сегменти со клиенти,
- Поврзување мрежни области што се поврзани со мрежните сегменти преку безжични технологии или наменска линија,
- Поврзување на домаќините за виртуелизација и виртуелните машини на домаќините со мрежните сегменти,
- Автоматизација на центарот за податоци,
- Спецификации за тоа како треба да се инкорпорираат крајните уреди што снабдуваат неколку мрежни сегменти, какви што се урамнотежувачи на оптоварување (load balancer) и решенија за чување податоци и сигурносни копии.

Во зависност од безбедносната политика и спецификацијата на барањата, треба да се развие концепт што опишува како секој мрежен сегмент треба да се имплементира во мрежни услови. Дополнително, треба да се дефинираат безбедносните функции што мора да ги обезбедат елементите за спојување помеѓу мрежните сегменти (на пример, заштитен сид како филтер за пакети со статус или IDS/IPS).

Поделба на мрежни сегменти

Системите за информатичка технологија со различни потреби за заштита треба да бидат поставени во различни мрежни сегменти. Ако тоа не е можно, системите за информатичка технологија треба да бидат заштитени според највисоките потреби за заштита што се присутни во нивниот мрежен сегмент. Покрај тоа, мрежните сегменти треба дополнително да се поделат во зависност од нивната големина и барањата на соодветниот концепт на сегментација. Мора да се обезбеди дека не е можно да се заобиколат мрежните сегменти, а уште помалку зоните.

Ако виртуелните LAN-мрежи (VLAN) на преклопникот (switch) припаѓаат на различни организации, тие треба да бидат физички одвоени. Дополнително, податоците треба да бидат криптирани за да се заштитат пренесените информации од неовластен пристап.

Безбедно логичко одвојување со помош на VLAN

Ако се користат VLAN-мрежи, тие не смеат да создаваат врска помеѓу дадена внатрешна мрежа и зона пред ALG или безбедносните посреднички (прокси) системи. Мора да се обезбеди дека VLAN-мрежите не можат да бидат преоптоварени.

Детално планирање на мрежната архитектура и дизајн и имплементација

Организацијата треба да врши, документира, проверува и редовно да го ажурира деталното планирање на мрежната архитектура и дизајн.

Спецификација на работни процеси за мрежата

Работните процеси треба да се креираат, да се приспособат по потреба и да се документираат. Конкретно, треба да се земе предвид влијанието на концептите за зонирање и сегментација врз операциите (работата) на информатичката технологија.

Интеграција на мрежна архитектура во планирање за итни состојби

Влијанието што мрежната архитектура и концептите што произлегуваат од неа го имаат врз планирањето за итни состојби, треба да се анализира првично, во определени интервали и транспарентно.

4.12.5. Напредни мерки

Мрежни и безбедносни компоненти со висока достапност

Централните области на внатрешната мрежа и безбедносните компоненти треба да бидат дизајнирани за висока достапност. За таа цел, компонентите треба да се дизајнираат редундантно и да се реализираат со висока внатрешна достапност.

Имплементирање мрежни конекции за висока достапност

Мрежните врски (на пример, интернет и WAN конекции) треба да бидат дизајнирани со целосна редундантност. Во зависност од барањата за достапност, редундантните конекции со еден или со повеќе даватели на услуги треба да се имплементираат со различна технологија и ефикасност. Исто така, треба да се имплементираат редундантни мрежни патеки (redundant routes) по потреба, во и надвор од доменот на организацијата. За таа цел, треба да се земат предвид можните единечни точки на дефект (SPoF) и самите услови на животната средина.

Заштита од дистрибуирано одбивање услуга

Со цел да се одбегнат DDoS-нападите, достапната ширина на опсег треба наменски да се дистрибуира преку различни комуникациски партнери и протоколи со помош на управување со ширината на опсег. За да може да се спречат DDoS-нападите со многу високи стапки на податоци, услугите за ублажување треба да се купат преку поголеми даватели на интернет-услуги (ISP) и нивната употреба треба да биде договорно регулирана.

Физичко одвојување на мрежните сегменти

Во зависност од безбедносната политика и спецификацијата на барањата, мрежните сегменти треба да бидат физички одвоени со посебни преклопници (switch).

Физичко одвојување на сегментите на мрежата за управување

Во зависност од безбедносната политика и спецификацијата на барањата, мрежните сегменти на областа на управување треба да бидат меѓусебно физички одвоени.

Микросегментација на мрежата

Мрежата треба да се подели на мали мрежни сегменти со многу слични профили на барања и исти потреби за заштита. Ова треба да се земе предвид особено за DMZ-сегментите.

Употреба на криптографски методи на ниво на мрежа

Мрежните сегменти треба веќе да се реализирани на ниво на мрежа во дадена внатрешна мрежа, екстранет и DMZ со помош на криптографски техники. За таа цел, треба да се користат VPN техники или стандардот IEEE 802.1AE.

Ако комуникацијата во внатрешната мрежа или DMZ се одвива преку патеки за пренос што не се доволно безбедни за зголемени потреби за заштита, комуникацијата треба да биде соодветно криптирана на ниво на мрежа.

Употреба на превенција на губење податоци (DLP) заснована на мрежа

На ниво на мрежа треба да се имплементираат системи за превенција на губење податоци (DLP) на ниво на мрежа.

Одвојување со помош на VLAN за многу високи барања за заштита

Во случаите кои што вклучуваат многу високи потреби за заштита, не треба да се користи VLAN.

Мрежна архитектура и дизајн - закани што се вклучени овде:	
3_0.9	Дефект или неисправност на комуникациските мрежи
3_0.11	Дефект или неисправност на давателите на услуги
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.40	Одредување на дејствија
3_0.43	Вметнување пораки
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.13. Рутери и преклопници (Switches)

4.13.1. Вовед

Рутерите и преклопниците ја сочинуваат основата на денешните мрежи за пренесување на податоци. Дефектот на еден или на повеќе од овие уреди може да доведе до застој на цела инфраструктура на информатичката технологија и затоа е потребна посебна заштита за овие уреди.

Рутерите работат на OSI слојот 3 (мрежниот слој) и транспортираат пакети со податоци врз основа на дестинации за IP-адреси во IP-заглавијата. Рутерите можат да поврзуваат мрежи со различни топологии. Тие се користат за сегментирање локални мрежи или за поврзување локални мрежи преку мрежи за пошироки области. Рутерот идентификува соодветна врска помеѓу изворниот систем или мрежа и одредениот систем или мрежа. Во повеќето случаи, ова се врши со препраќање пакети со податоци до следниот рутер.

Првите преклопници работеа на OSI слој 2, но сега се достапни преклопници со различни функции. Производителите обично им даваат ознаки на своите уреди што укажуваат на OSI слојот што го поддржуваат. Ова резултираше со термините „преклопник од слој 2“, „слој 3“ и „слој 4“, при што преклопниците на слојот 3 и слојот 4 всушност веќе се рутери во функционална смисла. Додека функциите на преклопниците и на рутерите првично беа различни, тие сега често се комбинираат во еден уред.

4.13.2. Цел

Целта е да се опише како безбедно може да се користат рутерите и преклопниците.

4.13.3. Закани

Дистрибуирано одбивање услуга (DDoS)

Во рамките на DDoS-напад на заштитена мрежа (на пример, преку TCP-SYN поплава или бура од пакети на протокол за кориснички датаграм – UDP), големиот број мрежни врски што мора да се обработат може да резултира со откажување на рутерот. Како последица, одредени услуги во локалната мрежа (LAN) може да бидат достапни или ова може да предизвика откажување на целата LAN-мрежа.

Манипулација

Ако напаѓачот успее да пристапи до рутер или до преклопник без овластување, тој може повторно да ги конфигурира уредите или дури да започне дополнителни услуги. На пример, конфигурацијата може да се промени на начин што ги блокира услугите, клиентите или цели мрежни сегменти. Истовремено, напаѓачот може да пресретнува, чита или да манипулира со мрежниот сообраќај на преклопникот.

Неправилна конфигурација на рутер или на преклопник

Рутерите и преклопниците се испорачуваат со стандардна конфигурација во која се активирани многу услуги. На пример, банерите за најава ги даваат и броевите на моделот и верзијата на уредите. Кога рутери и преклопници со несигурни фабрички поставки се користат во производни средини, полесно е да се пристапи до нив без овластување. Во најлош случај, ова може да предизвика достапност на внатрешните услуги за напаѓачите.

Неправилно планирање и дизајн

Организациите многу често неправилно ја планираат и ја дизајнираат употребата на рутери и преклопници. Меѓу другото, ова резултира со набавка на уреди што немаат доволен капацитет (во однос на ефикасноста или бројот на приклучоци, на пример). Како последица на тоа, рутерот или преклопникот може да се преоптоварат при првото користење. Ова значи дека услугите или цели мрежи може да не бидат достапни и да бидат потребни значителни ресурси за да се поправи ситуацијата.

Некомпатибилни активни мрежни компоненти

Може да се појават проблеми со компатибилноста, особено ако активните мрежни компоненти од други производители се додадат на постојните мрежи или ако мрежите се управуваат со компоненти од различни производители. Ако активните мрежни компоненти со различни имплементации на истиот метод на комуникација работат заедно во една мрежа, може да откажат поединечни подобласти на мрежата или на одредени услуги или дури и на целата мрежа.

„Поплава“ на контрола на пристап до медиуми (MAC flooding)

За време на „поплава“ на контрола на пристап до медиуми (MAC), напаѓачот испраќа голем број барања со MAC-адреси со различен извор до преклопникот. Откако преклопникот ќе го достигне максималниот број MAC-адреси што може да ги зачува, тој започнува да ги испраќа сите барања до сите системи за информатичка технологија во мрежата. Како последица на тоа, напаѓачот може да го види мрежниот сообраќај.

Напади во форма на разгрането дрво (spanning tree)

За време на нападите во форма на разгрането дрво, напаѓачот испраќа единици за податоци за протоколот на мостот (BPDUs) со цел да ги поттикне преклопниците да го земат предвид сопствениот (злонамерен) преклопник на напаѓачот како главен мост. На тој начин, мрежниот сообраќај се насочува низ преклопникот на напаѓачот, овозможувајќи му да ги сними сите информации што се испратени преку преклопникот. Како последица на тоа, напаѓачот може да започне DDoS-напади и да ја принуди мрежата повторно да ја воспостави топологијата на разгрането дрво со помош на неточни единици за податоци за протоколот на мостот, што може да предизвика откажување на мрежата.

Напади на протокол за решавање на адреса без барање (GARP)

За време на нападите на протокол за решавање на адреса без барање ARP (GARP), напаѓачот испраќа непобарани ARP-одговори до одредени цели или до сите системи за информатичка технологија во истата подмрежа. Во овие фалсификувани одговори на протокол за решавање на адреса (ARP), напаѓачот ја внесува нивната MAC-адреса како задача на IP-адреса на трето лице и ја поттикнува целта да ја промени својата ARP-табела на таков начин што мрежниот сообраќај потоа ќе биде испратен до напаѓачот наместо неговата валидна дестинација. Како последица на тоа, напаѓачот може да ја сними или да манипулира со комуникацијата помеѓу целите.

4.13.4 Мерки

Безбедна основна конфигурација на рутер или на преклопник

Организацијата мора пред користење рутер или преклопник, истите безбедно да ги конфигурира. Сите промени во конфигурацијата треба транспарентно да се документираат. Интегритетот на конфигурациските датотеки мора да биде соодветно заштитен. Пред да се зачуваат лозинките за пристап, тие мора да бидат обезбедени со помош на ажуриран криптографски метод.

Рутерите и преклопниците мора да се конфигурираат така што ќе се користат само апсолутно неопходните услуги, протоколи и функционални екстензии. Услугите, протоколите и функционалните екстензии што не се потребни, мора да се оневозможат или целосно да се деинсталираат. Неискористените канали на рутерите и на преклопниците исто така мора да бидат оневозможени. Ако е можно, неискористените мрежни порти мора да бидат оневозможени или барем доделени на недоделена VLAN-мрежа што е поставена за оваа намена.

Доколку се користат функционални екстензии, мора да се почитуваат безбедносните политики на организацијата. Употребата на такви екстензии исто така треба да биде оправдана и документирана.

Информациите за внатрешните конфигурации и работните статуси мора да бидат скриени од трети лица. Непотребните информативни услуги мора да бидат оневозможени.

Заштита на интерфејси за администрирање

Целиот пристап до рутерите и до преклопниците за администрирање и управување мора да биде ограничен на поединечни изворни IP-адреси или одреден опсег на адреси. Организацијата мора да обезбеди дека не е возможен пристап до интерфејсите за администрирање директно од несигурни мрежи. Треба да се користат соодветно криптирани протоколи за администрирање и следење рутери и преклопници. Ако сепак се користат некриптирани протоколи, за администрирање мора да се користи посебна административна мрежа (управување надвор од опсегот). Управувачките интерфејси и врските за администрирање мора да бидат заштитени со посебен заштитен сид. Мора да се наведат соодветни временски ограничувања за интерфејсите (на пример, период за истек на времето).

Сите услуги што не се потребни за интерфејсите за управување мора да бидат оневозможени. Ако мрежната компонента има доделен хардверски интерфејс, секој неовластен пристап до него мора соодветно да се спречи.

Заштита од напади со фрагментација

Заштитните механизми мора да бидат овозможени на рутерите и на преклопниците на слојот 3 за да се одбијат нападите со фрагментација на IPv4 и IPv6.

Итен пристап до рутери и до преклопници

Администраторите мора секогаш да можат директно да пристапат до рутерите и до преклопниците за да обезбедат континуирано администрирање, дури и ако целата мрежа откаже.

Евиденција на записи за рутери и за преклопници

Рутерот или преклопникот мора да се конфигурира така што, меѓу другото ќе ги евидентира следните настани:

- Промени на конфигурацијата (автоматски секогаш кога тоа е можно),
- Операција на повторно стартирање на системот кога ќе дојде до пат (reboots),
- Системски грешки,
- Промени на статусот за секој интерфејс, систем и мрежен сегмент,
- Грешки при најавување.

Редовни сигурносни копии

Редовно мора да се прават заштитни сигурносни копии на конфигурациските датотеки на рутерите и на преклопниците. Сигурносните копии мора да се креираат така што ќе може да им се пристапи во итна состојба.

Оперативна документација

Најважните оперативни задачи на рутерот или на преклопникот мора да бидат соодветно документираны. Сите промени во конфигурацијата и задачите во врска со безбедноста треба да бидат документираны. Документацијата треба да биде заштитена од неовластен пристап.

Креирање безбедносна политика

Организацијата мора да подготви конкретна безбедносна политика за рутери и за преклопници врз основа на општата безбедносна политика на самата организација. Оваа безбедносна политика треба транспарентно да ги опишува барањата и спецификациите за безбедно работење на рутерите и на преклопниците. Политиката треба да им биде позната на сите администратори и да биде составен дел од нивната работа. Доколку се смени политиката или се дозволени отстапувања од договорените барања, тоа треба да се координира со овластеното лице за безбедност на информации и да се документира. Треба редовно да се проверува дали политиката сè уште правилно се спроведува и резултатите од таквите проверки треба соодветно да се документираат.

Набавка на рутер или преклопник

Пред да се набават рутери и преклопници, треба да се состави список со барања врз основа на безбедносната политика што може да се користи за евалуација на производите што се достапни на пазарот. Треба да се обезбеди дека потребното ниво на безбедност на организацијата може да се постигне со уредите што ќе се набават. Оттука, процесот на набавка треба да се заснова на барањата на безбедносна политика на организацијата.

Изготвување листа за проверка за конфигурација за рутери и преклопници

Треба да се креира листа за проверка за конфигурација, кој може да се користи за проверка на најважните безбедносни поставки на рутерите и на преклопниците. Бидејќи безбедните конфигурации силно зависат од намената, треба да се земат предвид различните барања на овие уреди во рамките на листата за проверка за конфигурацијата.

Администрирање со помош на посебна мрежа за управување

Рутерите и преклопниците треба да се администрираат само преку посебна мрежа за управување (управување надвор од опсегот). Доколку постои таква посебна мрежа, интерфејсот за администрирање преку мрежата за пренесување на податоци (во опсегот) треба да биде оневозможен. Треба да се активираат достапните безбедносни механизми на протоколите за управување што се користат за автентикација, обезбедување интегритет и криптирање. Сите несигурни протоколи за управување треба да се оневозможат.

Заштита од злоупотреба на ICMP-пораки

Протоколите ICMP и ICMPv6 треба да се филтрираат рестриктивно.

Филтрирање незаконска IP-адреса и измама (bogon and spoofing filtering)

Треба да се спречи влез на напаѓачите во рутери и преклопници со помош на фалсификувани, резервирани или недоделени IP-адреси.

Заштита од напади насловени „IPv6 заглавие на рутирање тип-0 (IPv6 Routing Header Type-0)“.

При користење на IPv6, треба да се користат механизми за откривање и спречување напади на заглавие на рутирање тип-0.

Заштита од DoS и DDoS напади

Треба да се користат механизми што откриваат и одбиваат напади со голем волумен и напади на исцрпување на состојбата на протоколот за контрола на пренос (TCP).

Конфигурација на контролни списоци за пристап (ACL)

Пристапот до рутери и преклопници треба да се дефинира со помош на контролни списоци за пристап (ACL). Врз основа на безбедносната политика на организацијата, во контролните списоци за пристап треба да се дефинира кои системи за информатичка технологија или мрежи (и соодветни методи) може да се користат за пристап до рутер или преклопник. Доколку не постојат конкретни правила, се смета дека треба да се има предвид пристап со т.н. рестриктивна бела листа.

Заштита на приклучоците на преклопникот (Switch Ports)

Приклучоците на преклопникот треба да бидат заштитени од неовластен пристап.

Безбедносни аспекти на протоколите за рутери

Организацијата треба да изврши автентикација на рутерите кога разменуваат информации за рутирање или пренесуваат ажурирања за табели за рутирање. Треба да се користат само протоколи за рутирање што го поддржуваат ова. Протоколите за динамично рутирање треба да се користат само во безбедни мрежи. Тие не смеат да се користат во демилитаризирани зони (DMZs). Во DMZ, наместо тоа, треба да се внесат статични патеки.

Управување со идентитет и овластување во мрежната инфраструктура

Рутерите и преклопниците треба да бидат поврзани со централен систем за управување со идентитет и овластување.

Планирање за итни состојби за рутери и преклопници

За грешките во рутерите или во преклопниците што може да се дијагностицираат во итен случај, потребни се планирање и подготовка. Воедно, потребни се планирање и подготовка за тоа како да се поправат идентификуваните грешки. Затоа треба да се дефинираат соодветни инструкции за вообичаени сценарија на дефект/откажување и редовно да се ажурираат на одреден временски период.

Планирањето за итни состојби за рутери и преклопници треба да се координира со сеопфатно планирање грешки и непредвидливи ситуации. Планирањето итни состојби треба да се заснова на општиот концепт на планирање за итни состојби. Треба да се обезбеди дека документацијата за планирање итни состојби и упатствата што ги содржи се достапни во хартиена форма. Постапката што е опишана во концептот за планирање итни состојби треба редовно да се тестира.

Контроли и пенетрациски тестови

Рутерите и преклопниците редовно треба да се проверуваат за евентуална појава на познати безбедносни проблеми. Исто така, треба редовно да се вршат контроли. Ова треба да вклучува проверка дали фактичката ситуација соодветствува на основната конфигурација што е дефинирана како безбедна. Резултатите треба да бидат јасно документирани и споредени со целната ситуација и треба да се испитаат отстапувањата.

4.13.5 Напредни мерки

Употреба на контроли за пристап до мрежата

Контролата на пристап заснована на приклучок според стандардот IEEE 802.1x треба да се имплементира врз основа на EAP-TLS. Не треба да се вршат имплементации според стандардите IEEE 802.1x-2001 и IEEE 802.1x-2004.

Напредна заштита на интегритетот на конфигурациски датотеки

Ако рутерот или преклопникот откаже, треба да се обезбеди дека не се користат наследени или неточни конфигурации (вклучително контролни списоци за пристап) при враќање и рестартирање на уредот.

Високо ниво на достапност

Имплементацијата на решение со високо ниво на достапност не треба да ја наруши работата на рутерите и на преклопниците или нивните безбедносни карактеристики или да го намали нивото на безбедност. Рутерите и преклопниците треба да се дизајнираат редундантно. Притоа, треба да се обезбеди дека се почитува безбедносната политика на организацијата.

Управување со ширина на опсег за клучни апликации и услуги

Рутерите и преклопниците треба да вклучуваат и да користат функции што можат да детектираат апликации и да дадат приоритет на ширината на опсег.

Употреба на сертифицирани производи

Треба да се користат рутери и преклопници со безбедносна процена на заедничките критериуми од најмалку EAL4.

Рутер и преклопници - закани што се вклучени овде:	
3_0.9	Дефект или неисправност на комуникациските мрежи
3_0.11	Дефект или неисправност на давателите на услуги
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одрекување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.40	Одбивање на услуга
3_0.43	Вметнување пораки
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.14. Заштитен сид

4.14.1 Вовед

Заштитен сид е систем што се состои од хардверски и од софтверски компоненти, кои се користат за безбедно поврзување на мрежи што овозможуваат размена на информации и податоци засновани на интернет протокол (IP). Организацијата треба да користи структура на заштитен сид која ќе го ограничи протокот на информации што е технички изводлив за комуникации, а кои се претходно дефинирани како безбедни во соодветната политика. Во овој контекст, „безбедни“ значи дека се дозволени само пристапот или тековите на податоци што се посакувани помеѓу различни мрежи.

Во многу случаи, обезбедувањето мрежни порти повеќе не вклучува само поединечна компонента, туку една цела група на системи за информатичка технологија кои преземаат различни задачи (на пример, исклучиво филтрирање пакети или строго исклучување на мрежните врски со помош на карактеристики на посреднички (прокси) систем). Терминот „порта за ниво на апликација“ (ALG), кој се користи во оваа точка се однесува на компонента на заштитен сид што ги контролира тековите на податоци врз основа на безбедносни посреднички (прокси) системи.

Заштитниот сид се инсталира на портата помеѓу мрежите со различни нивоа на веродостојност (доверливост). Интернетот и интранет-врските не се единствениот пример на мрежи со различни нивоа на веродостојност. Две внатрешни мрежи во иста организација исто така може да имаат различни барања за заштита. На пример, за канцелариската комуникациска мрежа обично е потребна помала заштита од мрежата на одделот за човечки ресурси, каде што се пренесуваат посебни категории на лични податоци.

4.14.2 Цел

Целта е да се пропишат барањата кои ќе обезбедат сигурни врски помеѓу мрежите со различни потреби за заштита, преку безбедно користење на заштитниот сид или на структура на заштитниот сид.

4.14.3 Закани

Дистрибуирано одбивање услуга (DDoS)

Во рамките на DDoS-напад на заштитена мрежа (на пример, преку TCP-SYN „поплава“ или UDP „бура од пакети“), големиот број мрежни врски што мора да се обработат може да резултира со откажување на заштитниот сид. Ова може да предизвика недостапност на одредени услуги во локалната мрежа (LAN) или да предизвика откажување на целата LAN.

Манипулација

Ако напаѓачот успее да пристапи до заштитниот сид или до соодветен администраторски интерфејс, тој може да манипулира со податоците на голем број начини. На пример, може да ја промени конфигурацијата, да стартува дополнителни услуги или да инсталира злонамерен софтвер. Напаѓачот може и да ги прислушува комуникациските врски во манипулираниот систем за информатичка технологија. Правилата на заштитниот сид исто така може да се променат на начин што ќе овозможат пристап до заштитниот сид и до интранетот на организацијата од интернет. Понатаму, напаѓачот може да започне напад со одбивање услуга (DoS) со користење на правилото на заштитниот сид кое е поставено за да се спречи пристапот до поединечни услуги на серверот.

Заобиколување на правилата за заштитен сид

Напаѓачите може да користат основни механизми во мрежните протоколи за да ги заобиколат правилата на заштитен сид (на пример, преку напади со фрагментација) и да влезат во заштитена област. Во заштитената област, тие потоа може да предизвикаат дополнителна штета (на пример, со пристап, манипулирање или бришење на сензитивни податоци што треба да бидат заштитени).

Неправилна конфигурација и грешки при работа со заштитен сид

Неправилно конфигуриран или ракуван заштитен сид може да има значителни влијанија врз достапноста на услугите. Ако, на пример, правилата за заштитен сид се неправилно поставени, пристапот до мрежата може да биде блокиран. Понатаму, неточните конфигурации може да резултираат со недоволна заштита на системите за информатичка технологија. Во најлош случај, ова може да ги направи внатрешните услуги достапни за напаѓачите.

4.14.4 Мерки

Креирање безбедносна политика

Организацијата мора да подготви конкретна безбедносна политика за заштитните сидови врз основа на општата безбедносна политика на самата организација. Конкретната политика мора транспарентно да ги опишува барањата и спецификациите за безбедно функционирање на заштитните сидови. Политиката мора да им биде позната на сите вработени што се задолжени за заштитните сидови и да биде составен дел од нивната работа. Доколку се промени политиката или се дозволени отстапувања од барањата, ова мора да се координира со овластеното лице за безбедност на информации и истото да се документира. Правилното спроведување на политиката мора редовно да се проверува и резултатите да се документираат на соодветен начин.

Дефинирање на правилата за заштитен сид

Сите комуникации помеѓу две дадени мрежи мора да поминуваат низ заштитен сид, кој мора обезбеди дека нема да може да се воспостават неовластени конекции однадвор со заштитена мрежа. Покрај тоа, не смее да се воспоставуваат неовластени конекции од заштитена мрежа.

За заштитен сид мора да се дефинираат недвосмислени правила, кои одредуваат кои комуникациски врски и текови на податоци се дозволени. Сите други конекции мора да бидат спречени од заштитниот сид (пристап на „белата листа“). Во правилата за заштитниот сид мора да се земат предвид комуникациските односи со поврзаните сервери за услуги што се насочуваат низ заштитниот сид.

Организацијата мора да определи одговорни лица за да ги развиваат, спроведуваат и тестираат правилата за филтрирање. Покрај тоа, мора да биде јасно наведено кој смее да ги менува правилата за филтрирање, а донесените одлуки и релевантните информации и причини за истото мора да се документираат.

Конфигурирање соодветни правила за филтрирање на филтерот за пакети

Врз основа на воспоставените правила за заштитен сид, организацијата мора да ги дефинира и да ги конфигурира соодветните правила за филтри за пакети.

Филтерот за пакети мора да се конфигурира за да ги отфрли сите неважечки комбинации на знаменце за протокол за контрола на пренос (TCP flag). По правило, филтрирањето секогаш мора да се врши така што ќе поддржува одредена состојба/статус. Правилата за филтрирање со статус мора да се конфигурираат и за протоколите без конекција UDP и ICMP. Заштитниот сид мора рестриктивно да ги филтрира протоколите ICMP и ICMPv6.

Безбедна конфигурација на заштитен сид

Пред да се користи заштитен сид, тој мора безбедно да се конфигурира. Сите промени во конфигурацијата мора да бидат транспарентно документирани. Интегритетот на конфигурациските датотеки мора да биде соодветно заштитен. Пред да се зачуваат лозинките за пристап, тие мора да се обезбедат со помош на ажуриран криптографски метод. Заштитниот сид мора да се конфигурира така што ќе бидат достапни само услугите што се апсолутно потребни. Доколку се користат функционални екстензии, безбедносните политики на организацијата мора и понатаму да се исполнуваат. Употребата на такви екстензии мора исто така да биде оправдана и документирана. Сите непотребни (информациски) услуги и функционални екстензии мора да бидат оневозможени или целосно деинсталирани. Информациите за внатрешните конфигурации и работните статуси мора да бидат скриени од трети лица секогаш кога тоа е можно.

Заштита на интерфејси за администрирање

Целиот пристап до заштитните сидови за администрирање и управување мора да биде ограничен на поединечни изворни IP-адреси или опсези на адреси. Организацијата мора да обезбеди дека не е можен пристап до администраторските интерфејси од несигурни мрежи.

За управување или за следење на заштитните сидови мора да се користат само безбедни протоколи. Алтернативно, мора да се користи наменска администраторска мрежа (управување надвор од опсегот). За корисничките интерфејси мора да се наведат соодветни временски ограничувања.

Пристап до заштитен сид во итни состојби

Секогаш мора да биде можно директно да се пристапи до заштитен сид за да се управува со него локално, дури и ако целата мрежа откажала.

Спечување динамичко рутирање

Динамичкото рутирање мора да биде оневозможено во поставките на заштитниот сид, освен ако филтерот за пакети не се користи како периметарски рутер.

Евиденција на записи

Заштитните сидови мора да бидат конфигурирани за да ги евидентираат најмалку следните настани:

- Одбиени мрежни конекции (IP-адреси на изворот и дестинацијата, приклучоци за извор и дестинација или тип на ICMP/ICMPv6, датуми, времиња),
- Неуспешни обиди за пристап до системските ресурси поради неправилна автентикација, недостаток на овластување, недостаток на ресурси,
- Пораки за грешка од услугите на заштитен сид,
- Општи системски пораки за грешка,
- Промени на конфигурацијата (автоматски секогаш кога е можно).

Доколку се користат безбедносни посреднички (прокси) системи, безбедносниот нарушувања и повреди на контролните списоци за пристап (ACL) мора да се евидентираат на соодветен начин, односно мора да се евидентираат најмалку видовите нарушувања на протоколот или повреди на контролните списоци за пристап, IP адресите на изворот и дестинацијата, приклучоците на изворот и дестинацијата, услугите, датумите и времето и доколку е потребно, времетраењето на конекциите.

Кога корисникот обезбедува автентикација на безбедносен посреднички (прокси) систем, мора да се евидентираат или податоците за автентикација или само информациите за неуспешен обид за автентикација.

Заштита од напади на фрагментација на филтерот за пакети

Мора да бидат овозможени заштитни механизми на филтрите за пакети, со цел да се одбијат нападите на фрагментација на IPv4 и IPv6.

Оперативна документација

Оперативните задачи на заштитен сид мора да се документираат на транспарентен начин. Мора да се документираат сите промени во конфигурацијата и задачите што се релевантни за безбедноста, особено промените направени на системските услуги и на групата од правила на заштитниот сид. Оваа документација мора да биде заштитена од неовластен пристап.

Набавка на заштитен сид

Организацијата пред да набави заштитен сид, мора да подготви список со барања што може да се користи за евалуација на производите што се достапни на пазарот. Исто така, треба да се обезбеди дека потребното ниво на безбедност на организацијата може да се постигне со заштитен сид што ќе го избере. Оттука, процесот на набавка мора да се заснова на барањата на безбедносната политика на организацијата. Ако се користи IPv6, филтерот за пакети мора да ги провери заглавјата на екстензијата IPv6. Понатаму, мора да биде можно соодветно да се конфигурира IPv6 за IPv4.

Креирање „P-A-P“ структура („филтер за пакети - порта за ниво на апликација - филтер за пакети“)

Организацијата треба да користи структура „филтер за пакети – порта за ниво на апликација – филтер за пакети“ (P-A-P), која мора да се состои од неколку компоненти, секоја со соодветен хардвер и софтвер. Безбедносните посреднички (прокси) системи на апликациско ниво треба да бидат достапни за главните протоколи што се користат. За други услуги, треба да се користат најмалку генерички безбедносни посреднички (прокси) системи за протокол за контрола на пренос (TCP) и протокол за кориснички датаграм (UDP). Безбедносните посреднички (прокси) системи треба да се извршуваат и во заштитено опкружување за извршување на оперативниот систем што се користи.

Оневозможување на IPv4 или IPv6

Ако протоколот IPv4 или IPv6 не е потребен во даден мрежен сегмент, тој треба да биде оневозможен на соодветната пристапна точка на мрежата на заштитен сид (на пример, во соодветниот интерфејс на заштитниот сид). Ако протоколот IPv4 или IPv6 не е потребен или не се користи, тој треба да биде целосно оневозможен на заштитниот сид.

Администрирање со користење посебна мрежа за управување

Заштитните сидови треба да се администрираат само со користење посебна мрежа за управување (управување надвор од опсегот). Кој било администраторски интерфејс што е достапен преку фактичката мрежа што овозможува размена на информации и податоци (во опсег) треба да биде оневозможен. Комуникацијата во мрежата за управување треба да биде ограничена на неколку протоколи за управување со добро дефинирани дестинации и потекло преку управувачки заштитни сидови. Треба да се активираат достапните безбедносни механизми на протоколите за управување што се користат за автентикација, обезбедување интегритет и криптирање. Сите несигурни протоколи за управување треба да се оневозможат.

Заштита од TCP SYN поплава, бура од пакети на протокол за кориснички датаграм - UDP и погодување број на секвенца на филтерот за пакети

На филтрите за пакети што ги штитат услугите на серверот што се достапни од несигурни (или помалку сигурни) мрежи, треба да се конфигурира соодветна граница за полуотворени и отворени конекции.

На филтрите за пакети што ги штитат услугите на серверот што се достапни од несигурни (или помалку сигурни) мрежи, треба да се постават ограничувања на стапката за тековите на податоци на протокол за кориснички датаграм.

На филтрите за надворешни пакети, случајното генерирање на почетни секвенци на броеви (ISN) треба да биде овозможено за излезни TCP конекции, освен ако тоа веќе е имплементирано од безбедносните посреднички (прокси) системи.

Заштита на основните интернет протоколи

Протоколите HTTP, SMTP и DNS (вклучително и нивните криптирани верзии) треба да се насочуваат преку безбедносни посреднички (прокси) системи што се специфични за протоколот.

Привремено декриптирање на сообраќајот на податоци

Криптираните врски со несигурни (недоверливи) мрежи треба да се декриптираат привремено за да се потврди протоколот и да се проверат податоците за злонамерен софтвер. Притоа, треба да се земат предвид условите предвидени со закон. Компонентата што привремено го декриптира сообраќајот на податоци треба да ја спречи употребата на застарени опции за криптирање и криптографски алгоритми. Посредничкиот (прокси) систем TLS треба и да може да провери дали сертификатите се доверливи. Ако сертификатот не е сигурен, треба да биде можно да се одбие соодветната конекција. Исто така, треба да биде можно последователно да се интегрираат сопственички сертификати за да може да се конфигурираат и да се проверуваат и „внатрешните“ главни сертификати. Однапред конфигурираните сертификати треба да се проверат и да се отстранат доколку не се потребни.

Сигурна синхронизација на времето

Системското време на заштитниот сид треба да се синхронизира со серверот за мрежен протокол за време (NTP). Заштитните сидови не треба да дозволуваат надворешна синхронизација на времето.

Следење и евалуација на системот

Заштитните сидови треба да се интегрираат во соодветен концепт за следење на системот, кој треба постојано да се следи дали правилно работи самиот заштитен сид и услугите што се управуваат на него. Доколку се појават грешки или се надминат праговите, треба да се предупредат соодветните вработени. Понатаму, пораките за аларм треба да се генерираат автоматски за дефинирани настани. Податоците од евиденцијата на записите или пораките за статус треба да се пренесуваат само преку безбедни комуникациски патеки.

Ревизии и тестови за пенетрација

Структурите на заштитниот сид редовно треба да се проверуваат за познати безбедносни проблеми и треба да се вршат редовни тестирања за пенетрација и ревизии.

Планирање за итни состојби на заштитен сид

Организацијата треба однапред да ги предвиди проблемите коишто можат да настанат со заштитните сидови и да биде подготвена за преземање на дејствија за решавање на проблемите. Притоа, треба да се дефинираат соодветни дејства за типични сценарија за појава на дефект и истите редовно да се ажурираат. Планирањето за итни состојби за заштитните сидови треба да се координира со целокупните процеси за инциденти и подготвеност за итни состојби на организацијата. Организацијата треба да обезбеди дека документацијата за планирање итни состојби и упатствата што ги содржи истата се достапни во хартиена форма. Постапката што е опишана во концептот за планирање итни состојби, организацијата треба редовно да ја тестира.

4.14.5 Напредни мерки

Напредна заштита на интегритетот за конфигурациски датотеки

При враќање на заштитниот сид што откажал, треба да се обезбеди дека не се користат наследени или неточни конфигурации (меѓу другото, списоци за пристап). Ова треба да се применува и ако напаѓачот успее да рестартира заштитен сид.

Набавување од надворешни извори на функционални екстензии на наменски хардвер

Функционалните екстензии на заштитните сидови треба да се набавуваат од надворешни извори на наменски хардвер и софтвер.

Употреба на различни оперативни системи на заштитен сид и производи во повеќеслојна архитектура на заштитен сид

Во повеќеслојна архитектура на заштитен сид треба да се користат различни оперативни системи и производи за надворешниот и за внатрешниот заштитен сид.

Централно филтрирање активна содржина

Активната содржина треба централизирано да се филтрира според безбедносните цели на организацијата. За таа цел, криптираниот сообраќај на податоци исто така треба да се декриптира. Потребните безбедносни посреднички (прокси) системи треба да го поддржуваат филтрирањето на активната содржина.

Употреба на решенија со високо ниво за достапност

Филтрите за пакети и портите на ниво на апликација треба да бидат дизајнирани за да обезбедат високо ниво на достапност. Понатаму, треба да има две независни опции за пристап до надворешни мрежи (на пример, пристап до интернет преку два различни даватели на услуги). Внатрешните и надворешните рутери и сите други вклучени активни компоненти (на пример, преклопници) исто така треба да бидат дизајнирани за да се обезбеди високо ниво на достапност.

Дури и по автоматско откажување, структурите на заштитниот сид треба да се усогласат со барањата на безбедносната политика (на пример, „безбеден од откажување (fail safe)“ или „сигурен од откажување (fail secure)“). Оваа функција треба да се следи врз основа на повеќе параметри. Следењето на функциите не треба да се заснова на еден критериум. Датотеките за евиденција на записи и предупредувањата за решенијата со високо ниво на достапност треба редовно да се проверуваат.

Управување со ширина на опсег за клучни апликации и услуги

За да се обезбеди управување со ширината на опсег за клучните апликации и услуги, на мрежните порти и на портите помеѓу различните безбедносни зони треба да се користат филтрите за пакети со соодветна функција за управување со ширината на опсег.

Употреба на сертифицирани производи

Треба да се користат заштитни сидови со безбедносна процена на заеднички критериуми од најмалку ниво EAL4.

Заштитен сид - закани што се вклучени овде:	
3_0.8	Прекин или неисправност на напојувањето
3_0.9	Дефект или неисправност на комуникациските мрежи
3_0.14	Шпионажа
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.41	Саботажа
3_0.43	Вметнување пораки
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.15 Работа на безжична локална мрежа (WLAN)

4.15.1 Вовед

Безжичните локални мрежи (WLAN) може да се користат за создавање безжични локални мрежи или за проширување на постојните мрежи. До денес, речиси сите WLAN-компоненти што се достапни на пазарот се засновани на стандардот IEEE 802.11 и на неговите додатоци. Производителот конзорциум „Wi-Fi Alliance“ има важна улога во овој поглед како креатор на стандардот „Wi-Fi“, кој е договорен од индустријата врз основа на IEEE 802.11. „Wi-Fi Alliance“ ја користи ознаката за квалитет Wi-Fi за да потврди дека уредот поминал одредени тестови за интероперабилност и сообразност.

Во организацијата, WLAN-мрежите може да се користат за флексибилна работа со мобилни уреди и да им се овозможи пристап до внатрешните мрежи. За таа цел, пристапот до мрежата се воспоставува во рамките на организацијата преку пристапни точки. Бидејќи тие обично можат да се инсталираат брзо и лесно, WLAN-мрежите се користат и за воспоставување привремени мрежи – на пример, на саеми или на помали настани. Понатаму, пристап до мрежа може да се нуди на јавни места какви што се аеродроми или железнички станици преку точки за пристап до интернет (hotspot). Ова им овозможува на мобилните корисници да се поврзат на интернет или на мрежата на својата организација. Тогаш, главно, комуникацијата се одвива помеѓу централната пристапна точка и WLAN-компонентата на крајниот уред што се користи.

4.15.2 Цел

Целта е систематски да се демонстрира како може да се воспостават WLAN-мрежи и тие да може безбедно да функционираат во организацијата.

4.15.3 Закани

Откажување или прекин на радиомрежа

Во радиомрежите, информациите се пренесуваат со помош на електромагнетни радиобранови. Ако има други електромагнетни извори што зрачат енергија во истиот фреквентен спектар, овие емисии може да ја нарушат безжичната комуникација и во екстремни случаи, да ја спречат работата на WLAN-мрежата. Ова може да биде предизвикано од други радиосистеми и уреди, какви што се Bluetooth, микробранови печки или други WLAN-мрежи. Можни се и напади со одбивање на услугата. На пример, ако одредени контролни и управувачки сигнали се испраќаат постојано, тоа може да ја попречи достапноста на радиомрежата.

Несоодветно планирање на користењето WLAN мрежа

Честопати се утврдува дека грешките во планирањето се особено сериозни, бидејќи тие лесно можат да доведат до опсежни пропусти. Ако користењето WLAN е недоволно планирано (или воопшто не), тоа може да резултира со голем број проблеми. На пример:

- Доверливите податоци може да бидат пресретнати, на пример, кога се користат WLAN-стандарди што повеќе не соодветствуваат на најсовремените технолошки решенија (WEP за криптирање).
- Расположливиот преносен капацитет може да биде недоволен. Како последица на тоа, нема да биде можно да се користат апликации со ограничување на ширината на опсег со бараниот квалитет на услугата.
- Покриеноста со WLAN мрежа може да биде недоволна за да обезбеди достапност на мрежата на одредени места.

Недоволно правила за користење WLAN

Ако WLAN-инфраструктурата не се администрира централно, пристапните точки кај кои останале стандардните поставки, главно ќе бидат однапред конфигурирани со недоволни безбедносни механизми (или без никакви безбедносни механизми). На пример, ако недостатокот на процедури доведе до тоа вработениот да поврзе неовластена или необезбедена пристапна точка со внатрешната мрежа на организацијата, тоа може да доведе до сериозни проблеми. Со тоа ќе се доведат во прашање сите безбедносни заштитни мерки што се преземени во соодветната LAN-мрежа, како што е заштитниот сид што треба да ја заштити LAN-мрежата од неовластен надворешен пристап.

Несоодветен избор на методи за автентикација

Ако методите или механизмите за автентикација недостасуваат или се несоодветни, тоа може да доведе до пропусти. На пример, EAP-MD5 (Протоколот за автентикација што може да се прошири) подложни на напади од „човек во средината“ и на напади чијашто цел е погодување на лозинката (dictionary attack). Лозинките може да се погодат ако се користи EAP-MD5, а комуникацијата исто така може да се пресретне/прислушува.

Неправилна конфигурација на WLAN-инфраструктура

Пристапните точки и другите WLAN-компоненти (на пример, WLAN-контролери) обезбедуваат многубројни конфигурациски поставки, кои особено се однесуваат на безбедносните карактеристики. Ако поставките што се конфигурирани овде се неточни, комуникацијата преку пристапна точка ќе биде невозможна или недоволно заштитена (ако воопшто е заштитена).

Недоволно безбедносни механизми за WLAN

Во нивната првична состојба, WLAN-компонентите често се конфигурирани со само неколку активирани безбедносни механизми (или воопшто нема безбедносни механизми). Некои од овие механизми исто така се недоволни и затоа не обезбедуваат соодветна заштита. Дури и денес, сè уште се користат различни WLAN-компоненти што поддржуваат само несоодветни безбедносни механизми како што е WEP. Во одредени случаи, овие уреди не можат ни да се ажурираат со посилни безбедносни механизми. Ако се користат такви уреди, напаѓачот може лесно да ги пресретнува/прислушува сите комуникации и со тоа да добие доверливи информации.

Прислушување WLAN комуникација

Бидејќи радиото е медиум што може да го споделат неколку корисници, податоците што се пренесуваат преку WLAN мрежа лесно може да се прислушуваат и да се снимат. Недоволното или не постоење на криптирање на податоците може да го олесни прислушувањето на преносите. Покрај тоа, радиомрежите или емитиваните радиобранови често ги надминуваат границите на сопствените простории на корисниците. Така, податоците може да се емитираат во области што корисниците или организацијата не може да ги контролира или да ги обезбеди.

Симулирање валидна пристапна точка (неовластени пристапни точки)

Напаѓачот може да се маскира како дел од дадена WLAN инфраструктура со инсталирање сопствена пристапна точка со соодветна SSID во близина на WLAN клиент. Симулирана пристапна точка од овој вид се нарекува „неовластена пристапна точка“. Ако оваа пристапна точка му обезбедува на WLAN клиентот посилни ефикасности од реалната пристапна точка, клиентот ќе ја користи како своја базна станица доколку не се изврши меѓусебна автентикација. Понатаму, реалната пристапна точка може да биде оневозможена со напад на одбивање на услугата. Корисниците потоа ќе се најават во мрежа што само лажно се прикажува како целната мрежа. Ова му овозможува на напаѓачот да ги прислушува комуникациите. Методите на „троење“ или на лажирање исто така може да симулираат лажен идентитет за напаѓачот или да го пренасочат мрежниот сообраќај кон системите за информатичка технологија на напаѓачот. Ова значи дека напаѓачот може да ги слуша и да ги контролира комуникациите. Особено, во јавните радиомрежи (точки за пристап до интернет), неовластените пристапни точки често се користат како средство за напад.

Незаштитен пристап до локална мрежа (LAN) на пристапните точки

Доколку точките за пристап се поставени видливо и без никаква физичка заштита, напаѓачот може да се позиционира помеѓу точките за пристап и соодветната преклопна инфраструктура, со цел да го прислушува целиот мрежен сообраќај. Дури и ако безжичните комуникации се криптираат со помош на WPA2, ова претставува ризик бидејќи овие методи само го штитат воздушниот канал и не ги земаат предвид етернет конекциите.

Оштетување на хардверот

Оштетувањето на хардверот може да предизвика прекини во радио сообраќајот. Во најлош случај, WLAN-мрежата може дури и целосно да откаже. Ова е особено применливо за WLAN-уреди што се монтирани надвор од заштитени простории (на пример, со цел да се покријат отворени простори). Тие се изложени на дополнителни закани, какви што се намерна штета предизвикана од напаѓачи или штета предизвикана од гром или од други временски услови.

Кражба на пристапна точка

Пристапните точки до WLAN-мрежа што се небезбедно инсталирани на јавни површини може да бидат украдени. Како последица на тоа, може да биде можно да се добие споделен таен клуч што се користи за автентикација со RADIUS сервер или друг тип клуч (како што е за WPA2 Personal). Овие информации може да се користат за пристап до WLAN без овластување.

4.15.4 Мерки

Дефинирање стратегија за користење WLAN

Организацијата пред да користи WLAN мрежи, мора да ја прецизира општата стратегија на организацијата за комуникација преку WLAN. Конкретно, мора да се разјаснат и да се дефинираат организациските единици во кои ќе се користат WLAN мрежите, апликациите и целите за кои ќе се користат и информациите што може да се пренесат, како и мора да се определи и областа на покриеност со WLAN. Понатаму, уште од фазата на планирање мора да се дефинира кој ќе биде одговорен за администрирање на различните WLAN компоненти, кои канали ќе бидат поставени помеѓу одговорните лица што се вклучени во WLAN операциите и кога мора да се разменуваат конкретни информации помеѓу одговорните лица.

Избор на соодветен стандард за WLAN

Во рамките на планирањето на WLAN, мора првично да се определи кој од уредите со кои управува организацијата (на пример, микробранови печки, уреди со Bluetooth) зрачат во ISM-опсегот на 2,4 GHz и во опсегот од 5 GHz. Покрај тоа, мора да се споредат безбедносните механизми што се достапни во поединечните WLAN-стандарди. Притоа, мора да се обезбеди дека ќе се користат само методи за автентикација и криптирање што главно се сметаат за безбедни. Организацијата мора да ги документа причините за избор на конкретен WLAN-стандард.

Не смее да се користат уреди што треба да се вратат на несигурни методи од признаени безбедни методи.

Избор на соодветни криптометоди за WLAN

Комуникацијата преку воздушниот канал мора да биде целосно безбедна во криптографска смисла. Не смее да се користат криптографски методи што се помалку безбедни од WPA2.

Ако WPA2 се користи со претходно споделени клучеви (WPA2-PSK), мора да се користи сложен клуч со минимална должина од 20 карактери.

Соодветна локација на пристапни точки

Пристапните точки мора да се постават така што да не може да им се пристапи или да бидат украдени. Доколку се поставени, потребните области мора да бидат соодветно покриени. Понатаму, мора да се обезбеди во најголема можна мера радиобрановите да не се емитуваат во области што не се определени за WLAN-покриеност. Надворешните инсталации мора да бидат соодветно заштитени од временски и од електрични празнења.

Безбедна основна конфигурација на пристапни точки

Пристапните точки не смеа да се користат во нивната стандардна конфигурација. Однапред поставените SSID (идентификатори на сет услуги), лозинките и криптографските клучеви мора да се променат пред да започне нивната употреба. Покрај тоа, мора да се оневозможи несигурниот пристап до администрирање. Пристапните точки мора да се администрираат само преку соодветно криптирана конекција.

Безбедна конфигурација на WLAN-инфраструктура

Организацијата мора да обезбеди дека WLAN-комуникацијата не се користи за поврзување на безбедносните зони или за заобиколување на воспоставените заштитни мерки.

Воспоставување дистрибутивен систем

Пред да се воспостави жичен дистрибутивен систем, мора да се донесе основна одлука за тоа дали раздвојувањето ќе се изврши физички или логички преку WLAN мрежи на преклопниците за пристап на жичаната LAN мрежа.

Кодекси на однесување во случај на безбедносни инциденти на WLAN

Доколку се случи безбедносен инцидент, организационата единица за информатичка технологија мора да иницира соодветни контрамерки:

- На местото каде што WLAN комуникацијата влегува во внатрешната LAN мрежа, комуникацијата треба да се блокира селективно за секоја SSID и пристапна точка или дури и за целата WLAN инфраструктура во случај на напад.
- Доколку пристапните точки се украдени, мора да се применат утврдени безбедносни заштитни мерки за да се спречи каква било злоупотреба на пристапните точки или на информациите што се зачувани на нив.
- Доколку WLAN клиентите се украдени и се користи централна автентикација заснована на сертификати, сертификатите на клиентот мора да бидат блокирани.

Организација мора да ја исклучи можноста за користење украдени уреди без овластување за да се пристапи до мрежата на организацијата.

Безбедно поврзување на WLAN со LAN

Ако WLAN мрежите се поврзани со LAN мрежа, преминот помеѓу WLAN мрежите и LAN мрежата треба да биде заштитен, на пример, со помош на филтер за пакети.

Изготвување безбедносна политика за работа на WLAN

Организацијата врз основа на општата безбедносна политика, треба да ги прецизира суштински основни аспекти за безбедно користење на WLAN. Политиката треба да им биде позната на сите одговорни лица што се вклучени во воспоставувањето и работењето на WLAN. Спроведувањето на барањата на политиката, треба редовно да се проверува. Ако политиката не се спроведува, организацијата мора да има соодветен одговор за таквите околности. Резултатите од спроведувањето на безбедносната политика за работа на WLAN треба да бидат соодветно документирани.

Избор на соодветни компоненти на WLAN

Врз основа на резултатите од фазата на планирање, треба да се состави список со барања што може да се користи за да помогне во процената на производите што се достапни на пазарот. При набавка на WLAN компоненти, треба да се има предвид заштитата на личните податоци, како и меѓусебната компатибилност на компонентите заедно со безбедноста.

Употреба на соодветно решение за управување со WLAN

Организацијата треба да користи решение за централно управување со WLAN. Функционалниот опсег на употребеното решение треба да биде во согласност со барањата на достапната WLAN стратегија.

Редовни безбедносни проверки на WLAN мрежи

WLAN мрежите треба редовно да се проверуваат во однос на безбедносните недостатоци. Дополнително, обезбедените WLAN мрежи треба редовно да се пребаруваат за пристапни точки што се инсталирани без овластување и треба да се мери нивната ефикасност и покриеност. Резултатите од безбедносните проверки треба да се документираат транспарентно и да се споредуваат во однос на целната состојба. Притоа, доколку има отстапувања, истите треба да се испитаат.

Редовни контроли на компонентите на WLAN

Сите компоненти на WLAN инфраструктурата треба редовно да се проверуваат за да се обезбеди дека сите безбедносни заштитни мерки се имплементирани и сите компоненти се правилно конфигурирани. Пристапните точки што се поставени на јавни површини треба да се проверуваат редовно и по случаен избор за да се утврди дали имало обиди за нивно напаѓање или манипулирање. Резултатите од таквите контроли треба да се документираат транспарентно и да се споредуваат со целната состојба. Притоа, доколку има отстапувања, истите треба да се испитаат.

4.15.5 Напредни мерки

Користење виртуелна приватна мрежа (VPN) за обезбедување WLAN мрежи

Организацијата треба да користи VPN за да се постигне дополнителна заштита на WLAN-комуникациите.

Дополнителна заштита при поврзување WLAN-мрежи со LAN-мрежа

Доколку WLAN-инфраструктурата е поврзана со LAN-мрежа, преминот помеѓу WLAN-мрежите и LAN-мрежата треба да се обезбеди во согласност со зголемените потреби за заштита.

Заштита на комуникацијата помеѓу пристапните точки

Комуникацијата помеѓу пристапните точки преку безжичниот интерфејс и LAN мрежата треба да биде криптирана.

Употреба на безжични системи за откривање упади/системи за безжично спречување упад

Организацијата треба да користи безжични системи за откривање или спречување упад.

Работа на безжична локална мрежа (WLAN) - закани што се вклучени овде:	
3_0.9	Дефект или неисправност на комуникациските мрежи
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.24	Уништување на уреди или медиуми за чување податоци
3_0.25	Дефект на уреди или на системи
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.40	Одбивање на услуга
3_0.43	Вметнување пораки
3_0.44	Неовластен влез во простории

4.16 Виртуелна приватна мрежа (VPN)

4.16.1 Вовед

Со помош на виртуелни приватни мрежи (VPN), информациите што треба да бидат заштитени може да се пренесат преку несигурни (недоверливи) мрежи како што е интернетот. VPN е виртуелна мрежа со која се работи во рамките на друга мрежа, но логично е одвоена од оваа мрежа. VPN ја користи мрежата само како транспортен медиум; таа е независна од структурата и од дизајнот на користената мрежа. VPN мрежите може да користат криптографски процедури за заштита на интегритетот и на доверливоста на податоците. VPN мрежите исто така овозможуваат сигурна автентикација на комуникациските партнери кога неколку мрежи или системи за информатичка технологија се меѓусебно поврзани преку изнајмени линии или јавни мрежи.

4.16.2 Цел

Целта е да се дефинираат барањата за безбедно и систематско планирање, имплементација и функционирање на VPN.

4.16.3 Закани

Несоодветно планирање на употребата на VPN

Ако VPN-мрежата не е внимателно испланирана, дизајнирана и конфигурирана, може да се појават ранливости што ќе ги нарушат сите системи за информатичка технологија поврзани со неа. Така, напаѓачите ќе можат да пристапат до доверливи информации на организацијата. На пример, несоодветното планирање на VPN може да значи дека корисниците не биле соодветно обучени. Така, тие би можеле да користат VPN во небезбедна средина или да се поврзат со несигурен клиент. Ова за возврат може да им овозможи на напаѓачите пристап до целата мрежа на организацијата. Нападите може да се откријат и предоцна ако редовните проверки на пристапот до VPN не биле соодветно испланирани. Така, нема да биде можно да се одговори навреме, а напаѓачот може да украде податоци или да саботира цели процеси без да биде откриен.

Небезбедни даватели на услуги на VPN

Ако организацијата користи давател на услуги на VPN кој не е избран внимателно, тоа може да ја загрози безбедноста на целата мрежа на организацијата. Пристапот до VPN на давателот на услуги можеби не е безбеден, на пример, и затоа може да го користат напаѓачите за да украдат конкретни информации.

Несигурна конфигурација на VPN-клиенти за далечински пристап

Ако VPN-клиентот е несигурно конфигуриран, корисниците може погрешно да ги искористат (или воопшто да не ги искористат) неговите безбедносни механизми. Тие исто така може да ја променат конфигурацијата на VPN-клиентот. Поради несигурна конфигурација, софтверот што е инсталиран од корисниците може да ја загрози безбедноста на VPN-клиентот.

Небезбедни стандардни поставки на компонентите на VPN

Во нивната стандардна поставка, компонентите на VPN обично се претходно конфигурирани со недоволни безбедносни механизми (или воопшто нема безбедносни механизми). Во многу случаи, производителите посветуваат поголемо внимание на леснотијата на користење од страна на корисниците и интеграцијата без проблеми во постојните системи отколку на безбедноста. Ако компонентите на VPN се недоволно приспособени на реалните безбедносни барања на организацијата, тоа ќе создаде ранливости и соодветни точки на напад. Ако, на пример, лозинките што се однапред поставени од производителот не се променат, целата VPN мрежа (а со тоа и внатрешната мрежа на организацијата) може да биде нападната.

4.16.4 Мерки

Планирање на употребата на VPN

Организацијата мора внимателно да го испланира воведувањето виртуелна приватна мрежа (VPN) и мора да ги утврди одговорностите за управување со VPN. Групите на корисници и нивните овластувања мора да се планираат и за VPN. Покрај тоа, мора да се утврди како ќе се документаат овластувањата за пристап што се доделуваат, менуваат или се повлекуваат.

Избор на соодветен давател на услуги за VPN

Ако треба да се користи давател на услуги за VPN, договорот за користење на услугата (SLA) мора да се регулира и да се документа во писмена форма. Почитувањето на склучените договори за користење на услуга од страна на давателот на услугата за VPN, мора редовно да се проверува.

Сигурна инсталација на крајни уреди за VPN

Ако се користи уред за кој е потребно одржување, ова мора да подлежи на важечки договор за одржување. Организацијата мора да обезбеди дека компонентите на VPN се инсталирани само од квалификуван кадар. Инсталирањето на компонентите на VPN и сите отстапувања од планираните спецификации, треба да бидат документираны. Функциите и избраните безбедносни механизми на VPN мора да се проверат пред мрежата да се стави во функција.

Безбедна конфигурација на VPN

Организација мора да воспостави безбедни конфигурации за сите компоненти на VPN. Ова треба да биде документирано на соодветен начин. Одговорниот администратор мора редовно да проверува дали овие конфигурации сè уште се безбедни и да ги приспособува на сите системи за информатичка технологија што се достапни (ако е применливо).

Блокирање непотребни кориснички VPN сметки

Организацијата мора редовно да проверува дали само овластени системи и корисници можат да пристапат до VPN. Пристапот до VPN што повеќе не е потребен мора веднаш да се оневозможи. Пристапот до VPN мора да биде ограничен на потребното време за користење.

Анализа на барањата за VPN

Организацијата треба да изврши анализа на барањата за да ги одреди сценаријата за користење за дадена VPN и да се користат како основа за извлекување на спецификациите што ќе треба да ги исполнат соодветните хардверски и софтверски компоненти. Со анализата на барањата треба да се земе предвид следното:

- Деловни процеси и специјализирани задачи,
- Пристапни патеки,
- Процедури за идентификација и автентикација,
- Корисници и кориснички овластувања,
- Одговорности,
- Канали за известување.

Планирање на имплементацијата на техничката VPN

Покрај потребното општо планирање, организацијата треба внимателно да ги испланира техничките аспекти на VPN. За VPN мрежата треба да се прецизираат методи на криптирање, крајни точки на VPN, протоколи за дозволен пристап, услуги и ресурси. Понатаму, треба да се дефинираат подмрежите до кои може да се пристапи преку VPN.

Подготвување безбедносна политика за користење VPN

Организацијата треба да подготви безбедносна политика за користење VPN и сите вработени треба да бидат запознаени со истата. Безбедносните заштитни мерки што се опишани во безбедносната политика треба да се објаснат преку соодветна обука. Ако за вработено лице е поставен пристапот до VPN, на лицето треба да му се издаде информативен лист со детали за најважните безбедносни механизми за VPN. Сите корисници на VPN треба да бидат обврзани да ја почитуваат безбедносната политика.

Избор на соодветни производи за VPN

При изборот на производи за VPN, организацијата треба да ги земе предвид нејзините барања во врска со вмрежувањето на различни локации и меѓусебното поврзување на вработените, како и на вработените што работат на далечина.

Безбедна работа на VPN

Организацијата треба да создаде оперативен концепт за VPN мрежи. Ова треба да ги вклучува аспектите на управување со квалитетот, следење (мониторинг), одржување, обука и овластување.

Безбедна интеграција на надворешна мрежа

Организацијата треба да обезбеди дека VPN конекциите се создаваат само помеѓу наменетите системи и услуги за информатичка технологија, а протоколите за тунели што се користат за ова треба да бидат соодветни за таквата употреба.

Управување со корисници и пристап за VPN со далечински пристап

Во случаите што вклучуваат VPN од далечински пристап, треба да се обезбеди централно и доследно управување со корисници и пристап.

Интеграција на VPN компоненти во заштитен сид

Компонентите на VPN треба да се интегрираат во заштитен сид и истото да се документаира.

Виртуелна приватна мрежа (VPN) - закани што се вклучени овде:	
3 0.9	Дефект или неисправност на комуникациските мрежи
3 0.11	Дефект или неисправност на давателите на услуги
3 0.14	Шпионажа
3 0.18	Лошо планирање или недостаток на приспособување
3 0.19	Откривање на информации што треба да бидат заштитени
3 0.22	Манипулација со информации
3 0.23	Неовластено влегување во системи за информатичка технологија
3 0.28	Софтверски недостатоци или грешки
3 0.32	Злоупотреба на овластувања
3 0.40	Одбивање на услуга
3 0.43	Вметнување пораки
3 0.46	Губење на интегритетот на информациите што треба да се заштитат

4.17 Далечинско одржување**4.17.1 Вовед**

Терминот „далечинско одржување“ се однесува на физички одвоен пристап до системите за информатичка технологија и апликациите што работат на нив. Овој пристап може да ја олесни работата за конфигурација, одржување или поправка. Постојат различни начини за далечинско одржување. Далечинското одржување на клиентот често вклучува пренос на сигнали од тастатурата и глумчето од системот за информатичка технологија на администраторот до далечен систем за информатичка технологија. Далечниот систем за информатичка технологија потоа го пренесува својот аутпут од екранот назад до системот за информатичка технологија на администраторот. Администраторот на тој начин може да врши активности на далечниот систем за информатичка технологија како да се на самото место (активно далечинско одржување). Во случај на одржување далечен сервер, често се пренесуваат инпутот и аутпутот од конзолата. При пасивно далечинско одржување, само содржината на екранот на системот за информатичка технологија се пренесува до администраторот. Администраторот му дава инструкции на корисникот на локацијата, кој ги извршува под надзор на администраторот. Меѓутоа, овој пристап обично одзема многу време и е сложен за спроведување во пракса, поради што на организационата единица за информатичка технологија често им се дава целосен пристап до системите за информатичка технологија. Бидејќи многу системи за информатичка технологија се наоѓаат надвор од дофат на нивните администратори (на пример, во далечни центри за податоци, индустриски објекти или локација далеку од местото без кадар за информатичка технологија), во многу организации се користи далечинско одржување. Далечинското одржување често вклучува пристап до внатрешните системи за информатичка технологија и апликации на организацијата преку небезбедни мрежи. Поради можностите за интервенција во овие системи за информатичка технологија и апликации, обезбедувањето на компонентите за одржување од далечина е особено важно.

4.17.2 Цел

Целта е да се заштитат информациите што се зачувуваат, обработуваат и се пренесуваат за време на далечинско одржување, заедно со интерфејсите за далечинско одржување на системите за информатичка технологија. За таа цел, далечинското одржување претставува барања што еднакво се однесуваат на функциите на активно и пасивно далечинско одржување.

4.17.3 Закани

Несоодветно познавање на прописите за далечинско одржување

Администраторите што поставуваат и користат далечинско одржување, зависат од прописите што дефинираат како да се користи далечинско одржување. На пример, неопходно е да се одреди како апликациите треба да се конфигурираат за далечинско одржување. Во спротивно, далечинското одржување може да создаде дополнителни ризици за соодветната внатрешна мрежа. Доколку вклучените страни не се информирани за прописите за далечинско одржување, тоа создава ризик за операциите на информатичката технологија. На пример, администраторот може да постави интерфејс за далечинско одржување и да дозволи процедура за автентикација со несигурна лозинка наместо безбедна процедура заснована на сертификати.

Несоодветно планирање и правила за далечинско одржување

Ако организацијата внимателно не го планира, воспоставува и контролира далечинското одржување, безбедноста на сите нејзини системи за информатичка технологија може да биде нарушена. Ако, на пример, се користат несигурни протоколи за комуникација, алгоритми за криптирање или механизми за автентикација, може да се појават ранливости. Несоодветно обезбедените интерфејси за далечинско одржување исто така може да ја загорзат мрежата на трето лице.

Несоодветна употреба на автентикација при одржување на далечина

За далечинско одржување може да се користат различни механизми за автентикација. Доколку се користи несигурна процедура за автентикација, неовластени трети лица може да добијат администраторско овластување за системи за далечинско одржување или за алатки за далечинско одржување. Ова може да им овозможи пристап до системите за информатичка технологија на организацијата и да предизвика штета. Пример за ова е процедурата за најавување која користи кратка лозинка. Напаѓачот може брзо да ја погоди оваа лозинка и на тој начин да добие пристап до системите за информатичка технологија на организацијата.

Неправилно далечинско одржување

Потребно е професионално и редовно далечинско одржување за да се обезбеди безбедност и правилно функционирање на системите за информатичка технологија и на апликациите. Ако таквите системи за информатичка технологија и апликации не се правилно конфигурирани и одржувани преку далечинско одржување, тие веќе нема да бидат употребливи во најлош случај. Ако процесите за далечинско одржување не се извршуваат правилно, тоа може да доведе до дефекти на одделни компоненти на оперативниот систем. Покрај тоа, може да се појават ранливости поради работи за одржување на системот за информатичка технологија што се вршат премногу доцна или неправилно.

Користење несигурни протоколи при одржување на далечина

Комуникацијата преку јавни и внатрешни мрежи со помош на несигурни протоколи претставува потенцијална закана за организацијата. Ако, на пример, се користат застарени верзии на IPSeДов, SSH или SSL/TLS за да се воспостави тунел помеѓу две мрежи или крајни точки, не може да се гарантира дека овој тунел е доволно безбеден и дека информациите што се пренесуваат во него се соодветно заштитени. Напаѓачите може да ги искористат ранливостите на овие протоколи со цел да ја вметне сопствената содржина во заштитените врски. Протоколите во кои информациите се пренесуваат во обичен текст главно се сметаат за небезбедни.

Небезбедно и неконтролирано користење на пристапот за далечинско одржување од страна на трети лица

Доколку системите за информатичка технологија се одржуваат од далечина од трети лица без договорна основа, одговорностите за далечинско одржување може да не се јасно дефинирани. Како резултат на тоа, на пример, може да се заобиколи поделбата на улогите, или да не се документира отворениот пристап за далечинско одржување.

Користење електронски услуги за далечинско одржување

Покрај случаите во кои администраторот воспоставува директна врска што овозможува размена на информации и податоци со организацијата за далечинско одржување, може да се користат и електронски услуги. Овде, системите за информатичка технологија што треба да се администрираат, воспоставуваат врска со давателот на електронски услуги и администраторите користат веб прелистувач или слични средства за пристап до системите. Доколку оваа комуникација не подложи на криптирање од крај до крај, давателот на електронски услуги може да ги прочита разменетите податоци. Освен тоа, системите за информатичка технологија може да се администрираат и од неовластени лица доколку се манипулира со конекцијата на податоци. Доколку системите за информатичка технологија автоматски воспоставуваат податочна врска со електронската услуга при стартување, може да се пристапи директно до нив без да забележат корисниците на системите или одговорниот администратор.

Непознати компоненти за далечинско одржување

Многу системи за информатичка технологија содржат компоненти што нудат интегрирани функции за далечинско одржување. Сепак, овие функции често се слабо документирани и не се земаат предвид при набавката и работењето на системите за информатичка технологија. Интегрираните компоненти за далечинско одржување имаат пристап до системите за информатичка технологија во кои се инсталирани. Овој пристап често директно влијае врз другите компоненти на системот за информатичка технологија и на тој начин може да ги заобиколи безбедносните механизми на основниот оперативен систем. Покрај тоа, интегрираните функции за далечинско одржување може да содржат ранливости што олеснуваат неовластен пристап до системите за информатичка технологија.

4.17.4 Мерки

Планирање на употребата на далечинско одржување

Употребата на далечинско одржување мора да се приспособи на потребите на секоја организација. Далечинското одржување мора да се планира на начин заснован на потребите во однос на техничките и организациските аспекти на организацијата. Како минимум, мора да се земат предвид системите за информатичка технологија што треба да се одржуваат од далечина и одговорните лица за тоа.

Воспоставување безбедна врска за далечинско одржување клиенти

Доколку до клиентите се пристапува преку далечинско одржување, корисниците на овие системи за информатичка технологија мора претходно да се согласат за овој пристап.

Обезбедување интерфејси за далечинско одржување

Можните пристапни и комуникациски врски за далечинско одржување мора да се ограничат само на она што е потребно. Сите приклучоци за далечинско одржување мора да се исклучат по далечинскиот пристап. Исто така, мора да се обезбеди дека софтверот за далечинско одржување е инсталиран само на системи за информатичка технологија каде што тоа е потребно. Врските за далечинско одржување преку несигурни (недоверливи) мрежи мора да бидат криптирани. Сите други врски за далечинско одржување треба да бидат криптирани.

Користење електронски услуги

Организацијата треба да ги утврди околностите во кои може да се користат електронски услуги за далечинско одржување кога врска е воспоставена преку надворешен давател на услуги. По правило, употребата на таквите услуги треба да биде ограничена на колку што е можно помалку случаи. Системите за информатичка технологија не треба да воспоставуваат автоматизирани врски со електронската услуга. Притоа, треба да се обезбеди дека користената електронска услуга врши криптирање од крај до крај на пренесените информации.

Подготвување политика за далечинско одржување

Организацијата треба да подготви политика за далечинско одржување во која се документирани сите релевантни прописи. Политиката треба да им биде позната на сите лица што се одговорни за конципирањето, поставувањето и изведбата на далечинското одржување.

Документација при далечинско одржување

Далечинското одржување треба да биде соодветно документирано. Документацијата треба да ги прикаже пристапните точки за далечинско одржување што постојат и дали се активирани. Документите треба да се чуваат на соодветни локации и да бидат заштитени од неовластен пристап. Документите треба да бидат достапни во рамките на управувањето со обезбедување на континуитет на деловното работење.

Безбедни протоколи за далечинско одржување

Организацијата треба да користи само протоколи за комуникација што се класифицирани како безбедни. За таа цел треба да се користат безбедни криптографски процедури. Јачината на употребените криптографски процедури и клучеви треба редовно да се проверуваат и да се приспособуваат по потреба. Ако до пристапните точки за далечинско одржување на системите за информатичка технологија во внатрешната мрежа се пристапува преку јавна мрежа што овозможува размена на информации и податоци, тогаш треба да се користи обезбедена (заштитена) виртуелна приватна мрежа (VPN).

Избор и набавка на соодветни алатки за далечинско одржување

Соодветните алатки за далечинско одржување треба да бидат избрани врз основа на оперативните и безбедносните барања и барањата за заштита на личните податоци на самата организација. Сите одлуки за набавка треба да се координираат со одговорните лица за системите и апликациите и со овластеното лице за безбедност на информации.

Управување со алатки за далечинско одржување

Организацијата треба да воспостави процедури за организациско управување, кои опишуваат како да се ракува со избраните алатки. Исто така, треба да бидат достапни оперативни упатства што опишуваат како да се користат овие алатки за одржување на далечина. Покрај овие упатства, треба да се воспостават и да бидат достапни и процедури за пасивно и за активно далечинско одржување. Покрај ова, треба да се спроведат и обуки за вработените во организационата единица за информатичка технологија со цел да бидат запознаени со упатствата и процедурите, како и да бидат обучени за користење на алатките за далечинско одржување. Исто така, треба да се определи лице за контакт за сите технички прашања во врска со алатките за далечинско одржување.

Механизми за автентикација за далечинско одржување

За далечинско одржување, организацијата треба да користи методи со повеќе фактори за автентикација. Треба да се документира изборот на методот за автентикација и причините на кои се заснова тој избор. Пристапот за далечинско одржување треба да се земе предвид при управувањето со овластувањата во организацијата.

Далечинско одржување од трети лица

Доколку далечинското одржување го вршат надворешни лица од даватели на услуги, сите поврзани активности треба да бидат надгледувани од вработените во организацијата. Сите процеси на далечинско одржување извршени од трети лица треба да бидат евидентирани. Организацијата мора да направи договорни аранжмани со давателот на услугата за одржување во врска со безбедноста на соодветните системи за информатичка технологија и информации. Ако давателот на услуги врши далечинско одржување за неколку клиенти, мора да се обезбеди дека мрежите на неговите клиенти не се меѓусебно поврзани. Должностите и квалификациите на надворешните лица од давателите на услуги за надворешно одржување треба да бидат опфатени во договорот. Интерфејсите за далечинско одржување треба да бидат конфигурирани така што само давателот на услугата да може да пристапи до системите за информатичка технологија и мрежните сегменти што се потребни за нивната работа.

Операции за далечинско одржување

Организацијата треба да воспостави процес на известување за прашањата за поддршка и далечинско одржување. Исто така, треба да се имплементираат механизми за откривање и за спречување напади со голем обем, напади на исцрпување на состојбата (статусот) на протоколот за контрола на пренос (ТСР) и напади на ниво на апликација. Сите процеси за далечинско одржување треба да се евидентираат.

Креирање план за континуитет во случај на дефект/откажување на далечинското одржување

Организацијата треба да подготви план за да се сведат на минимум последиците од дефект/откажување на компонентите за далечинско одржување. Со планот треба да се прецизира како да се реагира во случај на дефект/откажување. Планот за итни состојби треба да обезбеди дека прекините и штетите (моментални и последователни) се сведени на минимум. Исто така, треба да прецизира како нормалното работење на организацијата може да се продолжи навремено.

Обезбедување интегрирани системи за далечинско одржување

При набавка на нови системи за информатичка технологија, организацијата треба да провери дали овие системи за информатичка технологија или нивните поединечни компоненти имаат функции за далечинско одржување. Доколку овие функции не се користат, истите треба да се оневозможат. Исто така, функциите треба да се оневозможат и ако се компромитирани од познати безбедносни ранливости. Ако се користат функциите за далечинско одржување што се интегрирани во фирмверот (firmware) на поединечни компоненти, нивните функции и пристапот до нив треба да бидат ограничени до најголема можна мера. Системите за информатичка технологија треба да бидат достапни само од посебна мрежа за управување.

Одвојување на комуникација за управување со мрежа за време на далечинско одржување

Организацијата треба да избегнува директен пристап на далечинско одржување до системот за информатичка технологија од администратор од клиент за далечинско одржување надвор од соодветните мрежи за управување. Доколку е неопходен таков пристап, комуникацијата треба да се одвои. За таа цел треба да се користат сервери за отскокнување (jump servers).

4.17.5 Напредни мерки

Наменски клиенти за далечинско одржување

За далечинско одржување, треба да се користат системи за информатичка технологија што се дизајнирани исклучиво за администрирање други системи за информатичка технологија. Сите други функции на овие системи за информатичка технологија треба да се оневозможат.

Редундантни комуникациски врски

Организацијата треба да воспостави редундантни комуникациски врски за пристап на далечинско одржување, како и да обезбеди конекции за управување надвор од опсегот.

Далечинско одржување - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.37	Одрекување на дејствија
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга

4.18 Управување со идентитет и пристап

4.18.1 Вовед

Пристапот до сензитивни ресурси во организацијата мора да биде ограничен на овластени корисници и овластени компоненти на информатичката технологија. Корисниците и компонентите на информатичката технологија мора да бидат идентификувани и да имаат извршено автентикација со сигурност. Управувањето со информациите што е потребно за таа цел се нарекува „управување со идентитетот“. Управувањето со пристапот дефинира дали и како корисниците или компонентите на информатичката технологија можат да пристапуваат до информации или до услуги и да ги користат (т.е. дали им е одобрен или одбиен пристап до веб-локацијата, до системот и до податоците врз основа на нивниот кориснички профил). Управувањето со пристапот ги вклучува процесите што се потребни за доделување, повлекување и контрола на правата. Бидејќи овие два термина се тесно поврзани, ќе се користи терминот „управување со идентитет и пристап“ (IAM). За да биде појасно, терминот „корисничка идентификација (ID)“ или „ID“ се користи како синоним истовремено со терминот „корисничка сметка“, „најава“ и „сметка“. Терминот „лозинка“ овде се користи како општ термин за „фраза за пристап“, „ПИН“ или „код за пристап“.

4.18.2 Цел

Целта е да се обезбеди дека корисниците и компонентите на информатичката технологија можат да пристапат само до ресурсите за информатичка технологија и до информациите што се потребни за нивната работа и за кои се овластени, како и дека не им се дава пристап на неовластени корисници и компоненти на информатичка технологија. За таа цел, управувањето со идентитетот и со пристапот, ги формулира барањата што организација треба да ги следи при воспоставување безбеден идентитет и управување со пристапот.

4.18.3 Закани

Недоволен број процеси во управување со идентитет и пристап

Доколку процесите за управување со идентитетот и пристапот се несоодветно дефинирани или имплементирани, нема гаранција дека пристапот ќе биде ограничен до потребното ниво, што ги нарушува начелата на „потребата да се знае“ или начело на „минимална привилегија“. Како резултат на тоа, администраторите може да не добиваат информации за кадровските промени, што значи, на пример, дека корисничката идентификација на вработен што заминал не може да се избрише, овозможувајќи му на вработениот да продолжи да пристапува до информации што треба да бидат заштитени. Воедно, можно е вработените да преминат во друга организациона единица, а притоа да ги задржат своите стари овластувања и со тоа да имаат овластувања со поголеми привилегии со текот на времето.

Нема централно средство за оневозможување на овластувањата за пристап на корисниците

Вработените често имаат кориснички овластувања за пристап за различни системи за информатичка технологија во својата организација, какви што се производство, тестирање, обезбедување квалитет или проектни системи. Во повеќето случаи, овие системи се наоѓаат во различни области на одговорност и често се управувани од различни администратори. Во одредени околности ова може да значи дека на сите системи за информатичка технологија не се користи идентична и единствена корисничка идентификација и дека нема централен преглед на корисничкиот пристап до поединечните системи за информатичка технологија. Во вакви ситуации, не е можно да се оневозможи целиот пристап на вработениот во еден чекор во случај на напад или кражба на лозинка. Исто така, не е можно да се блокира целиот пристап на вработениот во еден чекор, кога ќе ја напушти организацијата.

Неправилно администрирање веб локација, систем и права за пристап до податоци

Доколку доделувањето на правата за пристап до веб локација, систем и податоци е недоволно контролирано, тоа брзо може да доведе до сериозни ранливости (на пример, поради неконтролиран раст на доделените права). Кога се воведуваат системи за управување со идентитетот или се вршат контроли, често станува очигледно дека различни лица во различни организациски единици се одговорни за доделување права. Во некои околности ова може да резултира со тоа што на корисниците им се доделуваат овластувања на барање или преку непотребно комплицирани методи. Недостатокот на овластувања што се јавува како последица може да ја попречи секојдневната работа на организацијата, но давањето овластувања кога нема потреба исто така води до безбедносни ризици.

4.18.4 Мерки

Процедури за креирање и бришење корисници и кориснички групи

Организацијата мора да креира правила за да се дефинира како ќе се воспостават и ќе се бришат корисничките идентификации и корисничките групи. Мора да биде можно да се поврзе секоја корисничка идентификација со единствен корисник. Корисничките идентификации што се неактивни подолг период треба да бидат оневозможени. Сите корисници и кориснички групи мора да се креираат и да се избришат само преку посебни администраторски улоги. Корисничките идентификации што не се потребни, какви што се сметки за гости што се стандардно поставени или стандардните администраторски идентификации, мора да бидат соодветно оневозможени или избришани.

Креирање, менување и повлекување на овластувања

Корисничките идентификации и овластувања во организацијата мора да се доделуваат само врз основа на вистинска потреба во врска со специфични задачи, а во согласност со начелата на „минимална привилегија“ и „потреба да се знае“. Доколку има промени во кадарот, мора да се отстранат корисничките идентификации и овластувањата што повеќе не се потребни. Доколку вработените побараат овластувања што се надвор од соодветниот стандард, тие мора да бидат доделени само откако ќе се обезбеди дополнително оправдување и верификација. Овластувањата за пристап до системските директориуми и датотеки треба да бидат ограничени. Сите овластувања мора да се воспостават преку посебни администраторски улоги.

Документација за кориснички идентификации и профили на права

Корисничките идентификации, корисничките групи и профилите за права што се одобрени и креирани, мора да бидат и документираны од организацијата. Документацијата на овластени корисници, кориснички групи и профили за права мора редовно да се испитува за да се види дали ги одразува правата што всушност им се доделени на корисниците и на профилите и дали доделените права сè уште ги исполнуваат безбедносните барања и се соодветни за тековните задачи на корисниците. Документацијата мора да биде заштитена од неовластен пристап. Доколку документацијата е достапна во електронска форма, треба да се интегрира во процедурата за правење на сигурносна копија.

Распределба на задачи и поделба на улоги

Задачите и функциите што се дефинирани како некомпатибилни од организацијата мора да бидат одделени од нејзиниот систем за управување со идентитет и пристап.

Доделување права за пристап до веб локацијата

Организацијата мора да дефинира права за пристап до веб локацијата што треба да им се доделат или одземат на одредени лица во одредени улоги. Давањето и повлекувањето на средствата за пристап, какви што се чип картичките, мора да се документираат. Доколку ресурсите за пристап до веб локацијата се компромитирани, тие мора да се заменат. Лицата со права за пристап до веб локацијата треба да бидат обучени за правилна употреба на ресурсите за пристап до истата. Овластените лица треба да бидат привремено блокирани доколку треба да отсутствуваат подолго време од организацијата.

Доделување на права за пристап до системот

Организацијата мора да ги дефинира правата за пристап до системот што треба да им се доделат или одземат на одредени лица во одредени улоги. Ако се користат ресурси за пристап до системот, какви што се чип картички, нивното давање и нивното повлекување мора да се документира. Ако ресурсите за пристап до системот се компромитирани, тие мора да се заменат. Лицата со права за пристап до системот треба да бидат обучени за правилна употреба на ресурсите за пристап до системот. Овластените лица треба да бидат привремено блокирани доколку треба да отсутствуваат подолго време од организацијата.

Доделување права за пристап до податоци

Организацијата мора да дефинира права за пристап до податоци што треба да им се доделат или одземат на одредени лица во одредени улоги. Ако се користат ресурси за пристап до податоци, какви што се чип картички или токени, нивното давање и нивното повлекување мора да се документира. Корисниците треба да бидат обучени за правилна употреба на чип-картички или токени. Овластените лица треба да бидат привремено блокирани доколку треба да отсутствуваат подолго време од организацијата.

Процедури со кои се регулира употребата на лозинки

Организацијата мора да ја регулира употребата на лозинки со помош на процедури кои се обврзувачки за вработените. Притоа, мора да се земе предвид дали лозинките треба да се користат како единствен метод за автентикација или дали може да се користат други карактеристики или методи за автентикација како дополнување на лозинките или наместо лозинките. Лозинките не смеат да се користат за повеќе намени. За секој систем за информатичка технологија или апликација мора да се користи посебна лозинка. Не смеат да се користат лозинки што лесно се погодуваат или се чуваат во заеднички списоци со лозинки. Лозинките мора да се чуваат во тајност. Лозинките мора да ги знаат само самите корисници. Кога ги внесуваат своите лозинки, корисниците мора да внимаваат никој друг да не гледа. Лозинките не смеат да се чуваат на тастатури или на „гљувчиња“. Лозинките мора да се запишат само во случај на итност и да се чуваат безбедно. Исто така, треба да се земе предвид употребата на управител со лозинки (password manager). Ако управителот со лозинки има функции или дополнителни компоненти (plug-ins) што ги синхронизираат лозинките преку електронски услуги од трети лица или на друг начин ги пренесуваат лозинките на трети лица, овие функции или приклучоци мора да бидат оневозможени. Лозинките мора да се променат доколку се посомнева или се открие дека им станале познати на неовластени лица.

Идентификација и автентикација

Пристапот до сите системи за информатичка технологија и услуги мора да биде заштитен со соодветна идентификација и автентикација на корисници, услуги и системи за информатичка технологија. Претходно конфигурираните ресурси за автентикација мора да се променат пред да се стават во употреба во организацијата.

Регулирање на квалитетот на лозинката

Мора да се избераат безбедни лозинки со соодветен квалитет во согласност со нивната намена и барањата за заштита. Лозинките мора да бидат доволно сложени за да биде тешко да се погодат. Лозинките не смеа да бидат толку сложени што корисниците не можат редовно да ги користат со нормален напор.

Регулирање апликации за обработка на лозинки и системи за информатичка технологија

Системите за информатичка технологија или апликациите треба само да ги поттикнат корисниците да ја променат лозинката со валидна причина. Притоа, треба да се избегнуваат промени засновани само на фактот дека поминало одредено време. Мора да се преземат заштитни мерки за откривање компромитирани лозинки. Ако тоа не е можно, тогаш треба да се разгледа можноста дали лозинките може да се менуваат на одредени интервали и покрај поврзаните недостатоци. Стандардните лозинки мора да се заменат со доволно силни лозинки, а претходно дефинираните кориснички идентификации мора да се променат. Исто така, треба да се обезбеди дека системите за информатичка технологија целосно ја проверуваат можната должина и сложеноста на лозинката. Откако ќе се смени лозинката, старата лозинка не смеа повторно да се користи. Лозинките мора да се чуваат што е можно побезбедно. Во случаите што опфаќаат кориснички идентификации за технички корисници, сметки за услуги, интерфејси или слични елементи, промената на лозинката треба внимателно да се планира и доколку е потребно, да се координира со одговорните лица за апликацијата. Кога се обезбедува автентикација во мрежни системи, лозинките не смеа да се пренесуваат во некриптирана форма преку небезбедни мрежи.

Заштита на кориснички идентификации со обемни овластувања

Корисничките идентификации со големи привилегии треба да бидат заштитени со повеќефакторска автентикација (на пример, криптографски сертификати, чип-картички или токени).

Ресетирање лозинки

Организацијата треба да дефинира и да спроведе соодветна и безбедна процедура за ресетирање лозинки. Вработените за поддршка што можат да ги ресетираат лозинките треба да бидат соодветно обучени. Во случај на поголеми потреби за заштита на лозинката, организацијата треба да дефинира стратегија за случаи во кои вработениот за поддршка не е одговорен за обезбедување лозинка, а поради недостиг на достапни безбедни опции.

Развој на концепт за автентикација за системи за информатичка технологија и апликации

Организацијата треба да подготви концепт за автентикација што вклучува дефиниција за функционалните и за безбедносните барања за автентикација за секој систем за информатичка технологија и апликација. Информациите за автентикација мора да се зачуваат на криптографски безбеден начин. Информациите за автентикација не смеа да се пренесуваат некриптирани преку небезбедни мрежи.

Избор на соодветни механизми за автентикација

Организацијата треба да користи механизми за идентификација и за автентикација што ги задоволуваат потребите за заштита. Податоците за автентикација треба да бидат заштитени со системи за информатичка технологија и/или со апликации од шпионажа, модификација и од уништување за време на обработката. Системите за информатичка технологија и апликациите треба сè повеќе да ги одложуваат понатамошните обиди за автентикација по секој неуспешен обид. Треба да биде можно да се ограничи вкупното времетраење на обидот за најава. Откако ќе се надмине бројот на неуспешни обиди за автентикација, системите за информатичка технологија и апликациите треба да ја блокираат таа корисничка идентификација.

Проверка на ефективността на одвојувањето на корисниците во системи за информатичка технологија или апликации

Проверките во организацијата треба да се вршат на соодветни временски интервали за да се обезбеди дека корисниците на системи за информатичка технологија или апликации, редовно се одјавуваат откако ќе ги завршат своите задачи. Воедно, треба да се провери и дали неколку корисници работат под иста корисничка идентификација.

Пристап и дизајн на процеси на управување со идентитет и пристап

Организацијата треба да ги дефинира и имплементира следните процеси за управување со идентитетот и пристапот:

- Управување со политика,
- Управување со профилот на идентитетот,
- Управување со корисничка идентификација,
- Управување со профилот за овластување,
- Управување со улоги.

Политики за контрола на пристап до податоци и до системи

Организацијата треба да подготви политика за контрола на пристап до податоци и до системи за информатичка технологија, како и за компоненти на информатичка технологија и за мрежи што овозможуваат размена на информации и податоци. Притоа, треба да се користат стандардни профили за права кои соодветствуваат на улогите и на задачите на вработените. Исто така, треба да се воспостави правило за пристап до податоци во писмена форма за секој систем за информатичка технологија и апликација за информатичка технологија.

Соодветен избор на системи за управување со идентитет и пристап

Системот на организацијата за управување со идентитет и пристап, треба да биде соодветен за нејзините процеси, организациски структури и работни текови, како и за потребите за заштита. Системот за управување со идентитет и пристап треба да може да ги мапира спецификациите на организацијата за постапување со идентитети и овластувања. Избраниот систем за управување со идентитет и пристап треба да го поддржува начелото на поделба на улогите. Системот за управување со идентитет и пристап треба да биде соодветно заштитен од напади.

Користење централна услуга за автентикација

Централната услуга за автентикација, организацијата треба да ја користи за да се воспостави централно управување со идентитетот и пристапот. Употребата на услуга за автентикација заснована на централна мрежа треба внимателно да се планира. За таа цел, треба да се документираат безбедносните барања што се значајни при изборот на услуга од ваков вид.

Инструкции за сите вработени за ракување со методите и механизмите за автентикација

Сите вработени од страна на организацијата треба да добијат инструкции како правилно да ракуваат со методите кои се користат за автентикација. За таа цел, организацијата треба да има политики за ракување со процедурите за автентикација и да ги информира вработените за овие политики.

4.18.5 Напредни мерки

Планирање на итни состојби за системот за управување со идентитет и пристап

Организацијата треба да утврди во колкав степен неисправниот систем за управување со идентитет и пристап е од клучно значење за безбедноста на нејзините процеси. За таа цел, треба да се подготват процедури за одржување на операциите во случај на неисправен систем за управување со идентитет и пристап. Конкретно, политиката за контрола на пристап која е прецизирана во концептот за итни состојби сè уште треба да биде применлива при дефект на системот за управување со идентитет и пристап.

Повеќефакторска автентикација

За автентикација треба да се користи сигурна повеќефакторска автентикација (на пример, користење криптографски сертификати, чип-картички или токени).

Двојна контрола за администраторски активности

Услов за администраторските активности треба да биде вклучување на две лица (администратори). Доколку е потребна повеќефакторска автентикација, факторите треба да се распределат помеѓу двајцата администратори. Лозинките исто така треба да се поделат на два дела и да се доделат на секој од администраторите.

Управување со идентитет и пристап - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одрекување на дејствија
3_0.44	Неовластен влез во простории
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.19 Криптографија**4.19.1 Вовед**

Криптографијата се применува како средство за обезбедување доверливост, интегритет и автентичност во безбедноста на информациите. Криптографските процедури се користат за криптирање на информациите така што нивната содржина не може да се прочита без соодветниот клуч. Овие процедури можат да бидат симетрични, каде што истиот клуч се користи за криптирање и за декриптирање или асиметрични процедури, каде што еден клуч се користи за криптирање, а друг за декриптирање. Во хетерогена средина, податоците што организацијата локално ги чува и оние што ги пренесува, можат ефективно да се заштитат со криптографски процедури и техники, но потребни се и дополнителни заштитни мерки на организациско и на процедурално ниво, бидејќи употребата на криптографски процедури сама по себе не е доволна за да се гарантира доверливоста, интегритетот и автентичноста на криптираните информации. Во рамките на криптоконцептот, сите користени криптографски процедури и поврзаните заштитни мерки се разгледуваат заедно. Само холистичкиот поглед на оваа тема овозможува ефикасна заштита преку криптографија. Криптомодулите се посебна карактеристика што може да се користи за криптографските процедури за да се исполнат зголемените барања за заштита. Терминот „криптомодул“ се однесува на производ што ја нуди безбедносната функција што е наведена во даден криптоконцепт. Таквите производи може да се состојат од хардвер, софтвер, фирмвер или нивна комбинација. Покрај тоа, за спроведување на криптопроцесите, потребни се компоненти какви што се меморија, процесори и напојувања. Криптомодул може да се користи во информатичката технологија или во телекомуникациски системи за да се заштитат податоците и информациите.

4.19.2 Цел

Целта е да се опише како може да се креира криптоконцепт и како информациите во организациите можат да бидат криптографски обезбедени.

4.19.3 Закани

Несоодветно управување со клучеви за криптирање

Несоодветното управување со клучевите за криптирање може да им овозможи на напаѓачите пристап до криптираните податоци. На пример, недостатокот на правила може да резултира со тоа што клучевите и поврзаните криптирани информации се зачувуваат на истиот медиум за чување податоци или се пренесуваат (некриптирани) преку истиот канал за комуникација. Кога се користат симетрични методи, секое лице што може да пристапи до предметниот медиум за чување податоци или комуникациски канал ќе може да ги декриптира информациите доколку е познат користениот метод за криптирање.

Повреда на законските услови во однос на употребата на криптографски методи

Организацијата доколку користи криптографски методи и производи, тогаш мора да ги има предвид законските услови за истото. Во некои земји, на пример, криптографските методи не може да се користат без согласност на владата. Ова може да ги спречи примателите што се наоѓаат во странство да читаат криптирани групи податоци затоа што не им е дозволено да ги користат потребните криптографски производи, поради што дури може и кривично да одговараат.

Понатаму, користењето производи со силна енкрипција е значително ограничено во многу земји. Така, корисниците може да бидат во искушение да ги остават сензитивните податоци некриптирани или да ги заштитат со користење на несигурни методи. Покрај тоа што ги олеснува нападите, ова може да ги прекрши и националните закони. На пример, со прописите за заштита на личните податоци може да биде утврдено дека мора да се користат соодветни криптографски методи за да се заштитат личните податоци.

Губење на доверливоста или на интегритетот на податоците поради несоодветно однесување

Ако една организација користи криптомодули што се премногу сложени, на пример, нејзините корисници може да не ги користат од практични причини и наместо тоа може да пренесуваат информации во обичен текст. Како последица на тоа, напаѓачите може да ги пресретнуваат/прислушуваат пренесените информации. И грешките во работата на криптомодулите може да предизвикаат пресретнување доверливи информации од напаѓачите, на пример, ако информациите се пренесуваат во обичен текст затоа што режимот на обичен текст е случајно овозможен.

Софтверски недостатоци или грешки во криптомодулите

Софтверските недостатоци или грешките во криптомодулите ја нарушуваат безбедноста на криптографските процедури и може да овозможат читање на информациите што тие ги заштитуваат, меѓу другите последици. Понатаму, напаѓачите можат да манипулираат со криптомодулите (вклучително и преку злонамерен софтвер) и на тој начин да добијат податоци што се важни за организацијата, па дури и да запрат цели производствени процеси доколку податоците повеќе не можат да се декриптираат.

Дефект на криптомодул

Криptomодулите може да откажат поради технички дефекти, прекини во напојувањето или намерно уништување. Како последица на тоа, декриптирањето на податоците може да не биде можно додека потребниот криптомодул е недостапен. Ова може да резултира со застој на целиот синџир на процеси (на пример, ако другите апликации за информатичка технологија зависат од податоците).

Несигурни криптографски алгоритми или производи

Несигурни или застарени криптографски алгоритми може да бидат пробиени од напаѓач што користи мал број ресурси. Во однос на алгоритмите за криптирање (енкрипција), тоа значи дека напаѓачот може да успее да го конвертира криптираниот текст назад до оригиналниот обичен текст без да мора да знае дополнителни информации, како што е криптографскиот клуч. Ако се користат несигурни криптографски алгоритми, напаѓачите може да ја пробијат криптографската заштита и со тоа да пристапат до информациите што треба да бидат заштитени во организацијата. Дури и ако во организацијата се користат само сигурни (на пример, сертифицирани) производи, комуникацијата сепак може да стане несигурна. Ова е случај, на пример, ако комуникацискиот партнер користи криптографски процедури што не соодветствуваат на најсовремените технолошки достигнувања.

Грешки во криптирани податоци или во криптографски клучеви

Ако информациите се криптирани и криптираните податоци последователно се менуваат, можеби веќе нема да биде можно правилно да се декриптираат. Во зависност од начинот на работа на рутините за криптирање, ова може да резултира со неправилно декриптирање на само неколку битови или на сите податоци за кои станува збор. Ако нема сигурносна копија, таквите податоци ќе бидат изгубени. Грешката во користените криптографски клучеви може да биде уште покритична. Промената дури и на еден бит од криптографскиот клуч може да го оневозможи декриптирањето на податоците што се криптирани со помош на клучот.

Неовластено користење на криптомодул

Ако напаѓачот успее да користи криптомодул без овластување, тој може да манипулира со критичните безбедносни параметри. Како последица на тоа, соодветните криптографски методи веќе нема да обезбедуваат доволна безбедност. Покрај тоа, напаѓачот може да манипулира со криптомодулот така што модулот ќе работи правилно на прв поглед, но всушност е во несигурна состојба. На овој начин, напаѓачот може да остане неоткриен подолг временски период и да пристапи до голем дел од информациите што се клучни за организацијата.

Компромитирани криптографски клучеви

Безбедноста на криптографските методи во голема мера зависи од тоа колку добро се одржува доверливоста на криптографските клучеви. Затоа, потенцијалниот напаѓач обично ќе се обиде да ги одреди користените клучеви. Напаѓачот може да успее во таа намера, на пример, со читање привремена меморија или со наоѓање незаштитени клучеви што се зачувани во сигурносната копија. Напаѓачот ако го знае клучот и користениот криптометод, може лесно да ги декриптира податоците.

Фалсификувани сертификати

Сертификатите се дизајнирани да поврзат јавен криптографски клуч со личност, систем за информатичка технологија или организација. Оваа врска со клучот потоа е заштитена криптографски со помош на дигитален потпис, кој обично доаѓа од доверлива организација. Овие сертификати потоа се користат од трети лица за да ги потврдат дигиталните потписи на лицето, системот за информатичка технологија или организацијата, кои се идентификувани во сертификатот. Алтернативно, клучот што е зачуван во сертификатот може да се користи за асиметрична процедура за криптирање за да се криптира комуникацијата со носителот на сертификатот.

Ако ваквиот сертификат е фалсификуван, дигиталните потписи може лажно да бидат потврдени како точни и поврзани со лицето, системот за информатичка технологија или со организацијата во сертификатот. Понатаму, податоците може да бидат криптирани и испратени со клуч што е потенцијално небезбеден.

4.19.4 Мерки

Избор на соодветни криптографски методи

Организацијата мора да избере соодветни криптографски методи и мора да обезбеди дека се користат воспоставени алгоритми, кои се интензивно испитувани од експерти и немаат недостатоци. Притоа, мора да се користат и должини на клучот кои се препорачани за заштита на податоците и информациите според најсовремените технолошки достигнувања.

Сигурносни копии при користење криптографски методи

Во сигурносните копии, организационата единица за информатичка технологија мора да ги складира и да ги чува криптографските клучеви така што неовластените лица да не можат да пристапат до нив. Долгорочните криптографски клучеви мора да се чуваат надвор од употребените системи за информатичка технологија. За долгорочно чување криптирани податоци, треба редовно да се вршат проверки за да се утврди дали користените криптографски алгоритми и должините на клучот сè уште соодветствуваат на најсовремените технолошки достигнувања. Организацијата мора да гарантира дека до податоците што се чувани во криптирана форма сè уште може да се пристапи по подолги периоди. Употребените криптопроизводи треба да се архивираат. Исто така, треба да се направи сигурносна копија од податоците за конфигурацијата на криптопроизводите.

Криптирање комуникациски врски

Организацијата треба да утврди дали комуникациските врски можат да се криптираат на едноставен начин со разумен број ресурси и во тој случај тие врски треба да бидат соодветно криптирани.

Соодветно управување со клучеви

Криптографските клучеви треба секогаш да се креираат со соодветни генератори на клучеви во безбедна средина. Доколку е можно, криптографските клучеви треба да се користат само за една намена. Конкретно, треба да се користат различни клучеви за криптирање и за креирање потпис. Размената на криптографските клучеви треба да се изврши со метод што се смета за безбеден. Доколку се користат клучеви, треба да се проверат автентичноста на потеклото и интегритетот на податоците за клучевите. Сите криптографски клучеви треба да се менуваат доволно често. Организација треба да има утврдена процедура за сценарија во кои е откриен клучот. Сите креирани криптографски клучеви треба да се зачувуваат и безбедно да се управува со нив.

Безбедно бришење и уништување криптографски клучеви

Клучевите и сертификатите што повеќе не се потребни, треба да се избришат и безбедно да се уништат.

Идентификување на потребата од криптографски методи и производи

Организацијата треба да ги дефинира деловните процеси или специјализираните процедури за кои се потребни криптографски методи. Потоа, треба да се идентификуваат апликациите, системите за информатичка технологија и комуникациските врски што се неопходни за исполнување на задачите. Организационата единица за информатичка технологија треба да користи соодветни криптографски механизми за да ги обезбеди овие елементи.

4.19.5 Напредни мерки

Подготвување безбедносна политика за употреба на криптографски методи и производи

Организацијата врз основа на општата безбедносна политика, треба да подготви и посебна политика за користење криптопроизводи. Во оваа безбедносна политика треба да биде наведено лицето што е одговорно за безбедно работење на криптографските производи, како и да има правила за замена во врска со користените криптопроизводи. За корисниците треба да се дефинираат неопходни заштитни мерки за нивно запознавање и обука, заедно со кодекси на однесување и канали за известување за потенцијални проблеми или безбедносни инциденти. Понатаму, политиката треба да ги дефинира методите што се користат за да се обезбеди дека криптомодулите безбедно се конфигурирани, правилно се користат и редовно се одржуваат. Политиката треба да им биде позната на сите вработени и да биде составен дел од нивната работа. Доколку политиката се промени или се наметне потреба од отстапувања, тоа треба да се координира со овластеното лице за безбедност на информации и соодветно да се документира.

Организацијата треба редовно да врши проверки на политиката односно дали истата се почитува и правилно се применува, а резултатите од таквите проверки да се документираат.

Избор на соодветен криптографски производ

Организацијата пред да избере криптографски производ, треба да ги дефинира барањата што треба да ги исполни производот. Овде треба да се земат предвид аспектите какви што се опсегот на функциите, интероперабилноста, ефикасноста и заштитата од неправилно работење и неисправност. Треба да се провери дали треба да им се даде приоритет на сертифицираните производи. При процесот на селекција треба да се земат предвид и идните локации за распоредување, на пример, ограничувањата за извоз и увоз на криптографски производи. Како општо правило, производите што не овозможуваат контрола на чувањето на клучевите, не треба да се користат.

Развој на криптоконцепт

Организацијата треба да развие криптоконцепт кој што е интегриран во нејзиниот безбедносен концепт. Концептот треба да ги опишува сите технички и организациски спецификации за користените криптографски производи. Покрај тоа, треба да бидат наведени сите релевантни апликации, системи за информатичка технологија и комуникациски врски. Креираниот криптоконцепт треба редовно да се ажурира.

Безбедна конфигурација на криптомодули

Криptomодулите треба безбедно да се инсталираат и да се конфигурираат. Сите претходно поставени (почетни) клучеви треба да се променат. Потоа, треба да се тестира дали криптомодулите работат правилно и дали навистина корисниците можат да управуваат со нив.

Понатаму, треба да се дефинираат барањата за оперативното опкружување. Ако некој систем за информатичка технологија се промени, организацијата треба да тестира дали користените криптографски методи сè уште се ефикасни. Конфигурацијата на криптомодулите треба да се документира и редовно да се проверува.

Безбедно одвојување на улогите при користење криптомодули

При конфигурирање криптомодул, треба да се дефинираат корисничките улоги. За таа цел треба да се користат механизми за контрола на пристап и автентикација за да се потврди дали на вработениот навистина му е дозволено да ја користи таа услуга. Криptomодулот треба да биде конфигуриран така што информациите за автентикација треба повторно да се внесуваат секогаш кога има промена на улогата или откако ќе помине одреден период на неактивност.

Барања за безбедност на оперативниот систем при користење криптомодули

Интеракцијата помеѓу оперативниот систем и криптомодулите треба да го обезбеди следново:

- Инсталираните криптомодули не можат да се оневозможат или да се заобиколат без тоа да се забележи,
- Применетите или зачуваните клучеви не можат да бидат компромитирани,
- Податоците што треба да се заштитат може да се чуваат само на медиум за чување податоци без криптирање или без да го напуштат системот за обработка на информации со знаење и под контрола на корисникот,
- Ќе бидат откриени обиди за манипулации на криптомодулот.

Обука на корисници и на администратори

Организацијата треба да обезбеди обука за корисниците и за администраторите за ракување со соодветните криптомодули. Значењето на безбедносните поставки на криптомодулите и зошто тие се важни, треба детално да им се објасни на корисниците. Покрај тоа, тие треба да бидат свесни за опасностите од заобиколување или оневозможување на овие безбедносни поставки од практични причини. Содржината на обуката треба секогаш да се приспособува на конкретните оперативни сценарија. За администраторите, организацијата треба да обезбеди специјализирана обука за администрирање криптомодули. Воедно, треба да им се обезбеди и преглед на основните криптографски термини.

Реакција на намалување на функционалноста на криптометодот

Организацијата треба да воспостави процес што може да се користи во случај на намалување на функционалноста на криптографскиот метод и притоа треба да обезбеди мерки за подобрување на функционалноста на криптографскиот метод или истиот да се замени со соодветна алтернатива.

Физичка заштита на криптомодули

Организацијата треба да обезбеди дека е спречен неовластен физички пристап до содржината на криптомодулот. Хардверските и софтверските производи што се користат како криптомодули треба да можат да вршат самотестирање.

Криптографија - закани што се вклучени овде:	
3_0.13	Пресретнување компромитирачко зрачење
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.20 Сигурносна копија

4.20.1 Вовед

Организациите зачувуваат сè поголеми количини податоци и во исто време стануваат сè позависни од нив. На пример, ако податоците се изгубат поради неисправен хардвер, злонамерен софтвер или ненамерно бришење, тоа може да предизвика сериозно оштетување. Од друга страна, ова може да влијае врз вообичаените системи за информатичка технологија какви што се серверите или клиентите. Сепак, рутерите, преклопниците и уредите за „интернет на нештата“ исто така можат да зачувуваат информации што треба да бидат заштитени, какви што се конфигурациите. Според тоа, во контекст на ова, терминот „систем за информатичка технологија“ ги вклучува сите можни видови и форми на компоненти за информатичка технологија што зачувуваат информации што треба да бидат заштитени. Ефектите од губењето податоци може да се сведат на минимум преку редовно правење на сигурносни копии на податоците. Сигурносни копии на податоците е средство со кое се обезбедува дека операциите на информатичката технологија може да се обноват без одложување со редундантна копија од податоците на организацијата, доколку се изгубат делови од нејзините оперативни податоци.

4.20.2 Цел

Целта е да се опише како организацијата може да создаде концепт за правење на сигурносни копии и кои барања треба да се земат предвид во рамките на тој процес.

4.20.3 Закани

Недостаток на сигурносни копии

Ако податоците се изгубат и не се претходно зачувани, тоа може да има последици што ќе го загрозат постоењето на организацијата. Податоците може да се изгубат, на пример, поради злонамерен софтвер, технички дефекти или пожар, но и кога вработените бришат податоци (намерно или ненамерно). Ако податоците на системите какви што се серверите за електронска пошта немаат сигурносна копија, губењето на овие податоци може да го оневозможи продолжувањето на деловните операции на организацијата.

Недостаток на тестови за враќање на податоци (*recovery test*)

Правењето редовни сигурносни копии на податоците, само по себе не гарантира дека автоматски овие податоци може да се вратат и користат. Податоците за кои се прават сигурносни копии може да бидат неупотребливи, доколку не се вршат редовни тестирања за тоа дали податоците може да се вратат, кога тоа е потребно.

Несоодветно чување медиуми за сигурносни копии

Медиумите за сигурносни копии содржат голема количина информации на организацијата што треба да бидат заштитени. Ако медиумот за чување податоци се складира на небезбедна локација, напаѓачот (вклучувајќи го и оној во организацијата) може да пристапи до нив и да ги украде или да манипулира со овие информации. Медиумите за сигурносни копии може да станат неупотребливи и поради недоволните услови на чување. Информациите зачувани на нив, потоа нема да бидат повеќе достапни, кога ќе бидат потребни.

Недоволна документација

Ако документацијата за заштитни мерки за сигурносни копии е недоволна, враќањето на податоците може да потрае подолго од планираното. Ова може да резултира со доцнење во важни процеси (на пример, при давање на услуги на клиенти). Исто така, може да стане невозможно воопшто да се вратат податоците.

Непочитување на закони

Ако организацијата не ги почитува законите, како што е Законот за заштита на личните податоци, може да и биде изречена прекршочна санкција или да плати надомест на штета.

Користење несигурни даватели на услуги за „облак“ за сигурносни копии

Ако организацијата користи услуги за правење на сигурносни копии од давател на услуги за „облак“, нападите врз овој давател на услуги може да влијаат и врз сигурносните копии на организацијата што може да доведе и до одлив на податоци што треба да бидат заштитени. Понатаму, постои и ризик дека сигурносните копии нема да бидат достапни без одложување, кога ќе биде потребно. Во итен случај, ова за организацијата може да значи дека враќањето на податоците не е можно во времето коешто е одредено за тоа.

Недоволен капацитет за чување

Количината податоци што се обработуваат, а со тоа и се чуваат, постојано се зголемува. Недоволната меморија на медиумот за чување податоци што се користи за правење сигурносни копии може да биде пречка за правење сигурносни копии на најновите податоци. Софтверот за правење на сигурносни копии исто така може автоматски да ги презапише старите сигурносни копии што сè уште се потребни. Доколку одговорните лица не се информирани (на пример, поради недоволно следење), податоците може целосно да се изгубат или во итна состојба може да бидат достапни погрешни верзии.

Несоодветен концепт за правење сигурносни копии

Доколку не се креира и следи соодветен концепт за правење сигурносни копии, може да не биде можно да се вратат податоците за кои е направена сигурносната копија. На пример, ако сигурносната копија е криптирана и соодветниот клуч за декриптирање исто така е погоден во случај на губење податоци, тогаш нема да биде можно да се вратат податоците за кои е направена сигурносната копија. Ова може да се случи ако клучот не се чува одделно.

4.20.4 Мерки

Одредување на факторите што влијаат врз сигурносните копии

Организацијата мора да ги утврди условите за правење сигурносни копии на секој систем за информатичка технологија и на апликациите што се извршуваат на нив. За таа цел, мора да се консултираат сопствениците на процесите за апликациите и одговорните лица за соодветните системи за информатичка технологија. Организацијата мора да ги земе предвид најмалку следниве услови:

- Простор за чување,
- Промена на обемот,
- Промена на времињата,
- Барања за достапност,
- Барања за интегритет,
- Законски барања.

Резултатите мора јасно и соодветно да се евидентираат. Новите барања мора неодложно да се разгледаат.

Воспоставување процедури за правење сигурносни копии

Организацијата мора да воспостави процедура за секој систем за информатичка технологија што дефинира за кои податоци ќе се прават сигурносни копии и на каков начин. Во виртуелни средини, треба да се провери дали може да се направи сигурносна копија на системот со помош на механизми на слика за состојбата (snapshot). Процедурата за правење сигурносни копии мора да ги дефинира типот, зачестеноста и времето на правење на сигурносни копии. Ова мора да се заснова на факторите на влијание што се утврдени и ги вклучуваат сопствениците на процесот на соодветните апликации. Исто така, мора да се дефинира и медиумот за чување податоци што треба да се користи и начинот на кој податоците треба да се пренесуваат и да се зачувуваат.

Креирање на минимален концепт за правење сигурносни копии

Организацијата мора да создаде минимален концепт за правење сигурносни копии врз основа на утврдената процедура за правење на сигурносни копии. Овој концепт мора да ги дефинира минималните барања за сигурносни копии што треба да ги исполни организацијата. Концептот мора да содржи најмалку кратки описи за следново:

- системите за информатичка технологија и податоците што ќе бидат вклучени во секоја сигурносна копија,
- како може да се креираат и да се вратат сигурносните копии,
- параметрите што ќе се избераат,
- хардверот и софтверот што ќе се користат.

Редовни сигурносни копии

Организацијата мора да креира редовни сигурносни копии во согласност со минималниот концепт за сигурносни копии. Создадените сигурносни копии мора да бидат соодветно заштитени од пристап на трети лица. Притоа, мора редовно да се вршат тестирања за да се утврди дали процесот на сигурносни копии функционира на посакуваниот начин, а особено дали податоците од сигурносните копии може да се вратат без никакви проблеми и во соодветен временски период.

Развој на концепт за правење сигурносни копии

Организацијата треба да создаде концепт за правење сигурносни копии врз основа на минималниот концепт за сигурносни копии. Ова треба да ги вклучува најмалку следниве елементи:

- Дефиниции за суштински аспекти на сигурносни копии (на пример, типови податоци што треба да се разликуваат),
- Можности за закана,
- Влијателни фактори за секој систем за информатичка технологија,
- План за правење сигурносни копии за секој систем за информатичка технологија,
- Релевантни наоди од управувањето со обезбедување на континуитет на деловното работење, особено целта на точката за враќање за секој систем за информатичка технологија.

Организацијата треба да го пропише начинот на координирање на концептот за правење сигурносни копии со сопствениците на процеси што се одговорни за апликациите. Вработените треба да бидат информирани за делот од концептот за сигурносни копии што се однесува на нивното работење. Правилната имплементација на овој концепт треба редовно да се проверува.

Набавка на соодветен систем за сигурносни копии

Организацијата пред да набави систем за сигурносни копии, треба да создаде список на барања за да ги оцени производите што се достапни на пазарот. Набавениот систем за сигурносни копии треба да ги исполнува барањата на концептот за правење сигурносни копии и на целокупниот безбедносен концепт на организацијата.

Предуслови за користење услуги за „облак“ за сигурносни копии

Ако организацијата одлучи да користи услуги за „облак“ за правење сигурносни копии, тогаш треба да се регулираат најмалку следните прашања:

- Како е формулиран соодветниот договор,
- Каде се чуваат податоците,

- Договори за ниво на услуги (SLAs), особено во однос на достапноста,
- Соодветни методи за автентикација,
- Криптирање на податоците што се чуваат во „облак“.
- Криптирање при пренесување на податоците.

Обврски на вработените во врска со сигурносните копии

Сите вработени треба да бидат информирани за прописите за правење на сигурносни копии на организацијата. Тие исто така треба да бидат информирани како за задачите што треба да ги извршуваат при креирањето на сигурносните копии, така и за обврските за правење на сигурносните копии.

Сигурносни копии на софтвер што се користи

Организацијата треба да прави сигурносните копии на софтверските програми што се користат, под услов тоа да е законски дозволено и технички можно. За таа цел, треба да бидат достапни сите пакети и информации што се потребни за брзо повторно инсталирање на софтверот во итен случај. Оригиналните извори на инсталација и броевите на лиценците на софтверот што се користат треба да се чуваат на безбедно место.

Соодветно чување медиуми за чување сигурносни копии

Организацијата треба соодветно да ги чува медиумите за сигурносна копија за да спречи неовластен пристап. Таквите медиуми треба да се чуваат физички одвоени од системите за информатичка технологија за кои е направена сигурносната копија. Локацијата за чување треба да биде климатизирана така што медиумот за чување податоци да може да се чува за временскиот период што е наведен во концептот за правење сигурносни копии.

4.20.5 Напредни мерки

Користење криптографски методи за сигурносни копии

Организацијата треба да ги криптира сите сигурносни копии за да обезбеди доверливост и интегритет на податоците за кои е направена сигурносната копија. Исто така, треба да обезбеди дека криптираните податоци може да се вратат дури и по подолг временски период. Употребените криптографски клучеви треба да бидат заштитени со посебна сигурносна копија.

Сигурносна копија - закани што се вклучени овде:	
3_0.1	Пожар
3_0.2	Неповолни услови во околината
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.29	Повреда на закони или на договори
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.21 Управување со софтверски поправки и промени

4.21.1 Вовед

Соодветното и навремено ажурирање на компонентите на информатичката технологија на организацијата претставува голем предизвик. Во практиката, честопати се утврдува дека недостатоците или оперативните нарушувања потекнуваат од несоодветни софтверски поправки и промени или недостаток од нив. Затоа, занемарувањето на темата за управување со софтверски поправки и промени брзо води до потенцијални точки на напад. По правило, задачата на управувањето со софтверските поправки и промени е да ги дизајнира сите промени што се направени на апликациите, на инфраструктурата, на документацијата, на процесите и на процедурите така што тие ќе може да се управуваат и да се контролираат.

4.21.2 Цел

Целта е да се опише како да се дизајнира функционално управување со софтверски поправки во организацијата и како соодветниот процес може да се контролира и да се оптимизира. Сепак, надвор од управувањето со софтверски поправки, ова вклучува и некои основни аспекти на управувањето со промените што се значајни за безбедноста на информациите. Управувањето со промените се однесува на задачата за планирање и контролирање на промените.

4.21.3 Закани

Недоволно дефинирани одговорности

Одговорностите што се недоволно или лошо дефинирани, се преклопуваат или се нејасни, можат, на пример, да ги забават категоризацијата и приоритизирањето на барањата за промени. Ова може да ја одложи целокупната дистрибуција на софтверски поправки и промени. Истовремено, може да има сериозно влијание врз безбедноста ако софтверските поправки и промени се објавуваат набрзина без да се изврши тестирање или да се земат предвид сите технички аспекти.

Во екстремни случаи, недоволно дефинираните одговорности може негативно да влијаат врз целата организација или врз големи делови од неа. Прекините во работењето имаат негативно влијание врз достапноста. Доколку софтверските поправки што се важни за безбедноста се распределат доцна или воопшто не се распределат, доверливоста и интегритетот може да бидат загрозени.

Недоволна комуникација во управувањето со промените

Ако управувањето со софтверски поправки и промени е лошо прифатено во организацијата или ако луѓето што се вклучени слабо комуницираат, тоа може да доведе до доцнење во обработката и до неточни одлуки во врска со барањата за промени. Ова може да го намали нивото на безбедност на организацијата и сериозно да ги наруши нејзините операции на информатичките технологии. Во секој случај, последица на лошата комуникација се неефикасни процеси на промена, бидејќи за нив се потребни повеќе ресурси и повеќе време. Ова има негативни влијанија и врз способноста на организацијата да реагира во екстремни случаи што може да доведе до недостатоци или неможност да се постигнат важни деловни цели.

Слабо согледување на деловните процеси и на специјализираните задачи

Несоодветните промени, меѓу другото, можат да го нарушат непреченото постапување со деловните процеси или со специјализираните задачи, па дури и да предизвикаат целосно откажување на вклучените системи за информатичка технологија. Дури и кога се користи најсеопфатната процедура за тестирање, не може да се исклучи дека промената ќе се покаже како погрешна за време на подоцнежните операции. Доколку, во текот на процесот на промена, влијанието, категоријата или приоритетот на поднесеното барање за промена се процени неправилно во однос на вклучените деловни процеси или специјализирани задачи, организацијата може да не го достигне посакуваното ниво на безбедност. Ваквите погрешни процени најчесто се случуваат кога недостасува координација помеѓу вработените за информатичка технологија и вработените во специјализираните организациони единици.

Недоволно ресурси за управување со софтверски поправки и промени

За ефективно управување со софтверски поправки и промени се потребни соодветни ресурси во однос на кадар, време и финансирање. На пример, ако не се достапни соодветни вработени, за потребните улоги би можело да се определи неквалификуван кадар. Ова исто така може да спречи создавање интерфејси за одредени информации, на пример, помеѓу вработените за информатичка технологија и вработените во специјализираните организациони единици. Покрај тоа, може да биде невозможно да се обезбедат потребните капацитети за инфраструктурата на околните за тестирање и дистрибуција. Иако често е можно да се надомести недостигот на кадар, време и финансии за време на нормалното работење, овие недостатоци стануваат уште поочигледни под сериозен временски притисок, како, на пример, кога треба да се применат софтверски поправки за итни состојби.

Проблеми во автоматизирањето на дистрибуцијата на софтверски поправки и промени

Во многу случаи, софтверските поправки и промени не се дистрибуираат мануелно, туку централно, со софтверска поддршка. Доколку се користи таков софтвер, неточните софтверски поправки и промени може автоматски да се дистрибуираат низ цел информативен домен, што може да доведе до големи безбедносни проблеми. Ова може да биде особено сериозно ако софтверот со недостатоци се инсталира истовремено на повеќе системи. Ако грешките се јавуваат само повремено, тие често може да се поправат рачно. Сепак, може да настанат проблеми ако системите за информатичка технологија не се достапни подолго време. Еден таков пример се вработените во оваа област кои само повремено ги поврзуваат своите системи за информатичка технологија со локалната мрежа (LAN) на организацијата. Ако соодветната алатка се конфигурира така што ажурирањата се дистрибуираат само во одреден временски период и не се достапни сите системи за информатичка технологија во таа временска рамка, овие системи нема да се ажурираат.

Недоволно опции за обновување во управувањето со софтверски поправки и промени

Доколку софтверските поправки или промените се дистрибуираат без опција за обновување или рутините за обновување на користениот софтвер не се соодветни и ефективни, нема да биде можно навремено да се поправи неправилно ажурираниот софтвер. Ова може да доведе до откажување на важни системи за информатичката технологија и значителна последователна штета. Покрај потенцијалната загуба на податоци, ова особено ја загрозува достапноста и интегритетот на податоците на засегнатите системи за информатичка технологија.

Погрешна процена на релевантноста на софтверските поправки и промени

Ако приоритетите за промените се погрешно одредени, на пример, прво може да се инсталираат неважни софтверски поправки, а важните софтверски поправки може да се инсталираат подоцна и да овозможат недостатоците да останат нерешени подолго време. Управувањето со софтверски поправки и промени често е поддржано од софтверски алатки. Овие алатки може да содржат и софтверски грешки и затоа даваат недоволни или неточни информации за промената. Доколку информациите за промените што ги обезбедува алатката од овој вид не се потврдени и проверени во однос на нивната веродостојност, вистинската имплементација на промените може да се разликува од претпоставките на организацијата.

Манипулација со податоци и алатки во управувањето со промените

Управувањето со софтверски поправки и промени често се одвива од централна локација. Неговата изложена позиција значи дека е особено загрозено. Доколку напаѓачите успеат да ги преземат вклучените сервери, тие ќе можат да дистрибуираат манипулирани верзии на софтвер истовремено на повеќе системи за информатичка технологија преку оваа централна локација. Дополнителни точки на напад често се создаваат од фактот дека со овие системи се управува од надворешни даватели на услуги. Исто така, може да биде достапен и пристапот за одржување што им овозможува на напаѓачите пристап до централниот сервер за дистрибуција на промени.

4.21.4 Мерки

Концепт за управување со софтверски поправки и промени

Ако се променат компонентите на информатичката технологија, софтверот или податоците за конфигурација, мора да има спецификации што исто така ги земаат предвид безбедносните аспекти. Тие мора да се дефинираат во концептот за управување со софтверски поправки и промени и соодветно да се следат. Сите софтверски поправки и промени мора да бидат соодветно планирани, одобрени и документирани. Софтверските поправки и промени треба да бидат соодветно однапред тествирани. Ако се инсталирани софтверски поправки и се извршат промени, мора да постојат достапни алтернативни решенија. Доколку има големи промени, мора да биде вклучено и овластеното лице за безбедност на информации. Мора да се обезбеди дека потребното ниво на безбедност се одржува за време на спроведувањето и по спроведувањето на промените. Конкретно, треба да се одржуваат и потребните безбедносни поставки.

Дефинирање одговорности

За сите организациски области мора да бидат одредени лицата што се задолжени за управување со софтверски поправки и промени. Дефинираните одговорности мора да се одразат и во политиката за контрола на пристап на организацијата.

Конфигурирање механизми за автоматско ажурирање

Ракувањето со интегрираните механизми за автоматско ажурирање на користениот софтвер, мора да се дефинира во рамките на стратегијата за управување со софтверски поправки и промени. Конкретно, мора да се прецизира како овие механизми треба да се заштитат и соодветно да се конфигурираат. Освен тоа, треба да се провери видот на механизмите за ажурирање на новите компоненти.

Редовно ажурирање системи за информатичка технологија и софтвер

Системите за информатичка технологија и софтверот треба редовно да се ажурираат. По правило, софтверските поправки треба да се применат веднаш по нивното објавување. Врз основа на концептот за управување со софтверски поправки и промени, софтверските поправки мора да се проценат веднаш по нивното објавување и соодветно да се одредат приоритетите. Мора да се донесат одлуки дали треба да се применат софтверските поправки. Кога се применува софтверска поправка, треба да се провери дали е навремено и успешно применета на сите релевантни системи. Доколку не се примени софтверска поправка, мора да се документира оваа одлука, како и причините за неа.

Редовно пребарување информации за софтверски поправки и недостатоци

Организационата единица за информатичка технологија мора да биде сигурен дека редовно добива информации за утврдените недостатоци во фирмверот, оперативните системи, апликациите и во услугите што се користат. Идентификуваните недостатоци мора да се отстранат колку што е можно побрзо. Сè додека не се достапни соодветни софтверски поправки, мора да се применат други соодветни заштитни мерки за заштита на засегнатите системи во зависност од сериозноста на недостатоците и основните закани. Ако тоа не е можно, треба да се обезбеди дека хардверот, релевантните оперативни системи, распоредените апликации и услугите повеќе не се користат.

Постапување со барања за промена

Организацијата треба сите барања за промени да ги евидентира и документира. Барањата за промена треба да ги провери одговорното лице за управување со софтверски поправки и промени за да се обезбеди дека се согледани сите аспекти на безбедноста на информациите.

Координација на барањата за промени

При процесот на координација во врска со барањата за промена треба да се земат предвид сите релевантни целни групи и влијанието врз безбедноста на информациите. Целните групи што се засегнати од промената, треба да можат да ја коментираат промената така што тоа ќе може и да се провери. Поради тоа, во организацијата треба да има утврдена процедура за да се забрза постапувањето со важните барања за промени.

Интегрирање на управување со промени во деловните процеси

Процесот на управување со промени треба да биде интегриран во деловните процеси или во специјализирани задачи кои се извршуваат во организацијата. Во случаите што вклучуваат планирани промени, треба да се земе предвид моменталната состојба на засегнатите деловни процеси. Сите релевантни организациони единици треба да бидат известени за претстојните промени. Исто така, треба да има и ниво на засилување односно подигнување на важноста на ова прашање, кое вклучува членови на највисокото раководство на организацијата. Во случај на сомневање, овие членови треба да одлучат за приоритетот и за распоредот на дадена хардверска или софтверска промена.

Безбедна употреба на алатки за управување со софтверски поправки и промени

Организацијата треба да ги дефинира барањата и условите на рамката за избор на алатки за управување со софтверски поправки и промени. Понатаму, организацијата треба да подготви специфична безбедносна политика за употребените алатки.

Процедури за тестирање и прифаќање нов хардвер

Кога се избира нов хардвер, треба да се провери дали софтверот што се користи, а особено релевантните оперативни системи, се компатибилни со хардверот и неговиот драјверски софтвер. Новиот хардвер треба да се тестира исклучиво во изолирана околина пред да се користи. Понатаму, организацијата треба да има процедура за прифаќање и изјава за пуштање во употреба на системи за информатичка технологија. Одговорното лице треба писмено да ја поднесе изјавата за пуштање во употреба на соодветно место. Доколку се откријат грешки за време на тековните операции и покрај процедурите за прифаќање и пуштање во употреба, треба да има постапка и за отстранување проблеми.

Обезбедување интегритет и автентичност на софтверските пакети

Автентичноста и интегритетот на софтверските пакети треба да бидат обезбедени во текот на процесот на софтверска поправка или промена. За таа цел, треба да се провери дали се достапни контролни суми (checksums) или дигитални потписи за користените софтверски пакети. Доколку има такви, тие треба да се проверат пред да се инсталира софтверскиот пакет. Понатаму, треба да се обезбеди дека се достапни програмите што се потребни за проверка. По правило, софтверот и ажурирањата треба да се добиваат само од доверливи извори.

Континуирана документација за обработка на информации

Промените треба да се документираат во сите фази, апликации и системи и за таа цел треба да се воспостават соодветни правила од страна на организацијата.

4.21.5 Напредни мерки

Користење на алатки во управувањето со промени

Пред користење алатка за управување со промени, треба да се провери дали може соодветно да ги дистрибуира промените во засегнатиот домен на информации. Исто така, треба да биде можно да се дефинираат точки на прекин за запирање на дистрибуцијата на неточни промени.

Мерење на успехот на барањата за промени

Сопственикот на процесот за управување со софтверски поправки и промени треба да изврши последователни тестови за да потврди дали дадената промена е успешна. За таа цел, сопственикот на процесот треба да избере соодветни референтни системи како системи за обезбедување квалитет. Резултатите од овие тестови треба да се документираат во рамките на процесот на промена.

Синхронизација во рамките на управувањето со промени

Во процесот на управување со промени, соодветните механизми треба да обезбедат дека се вршат софтверски поправки и промени на уредите до кои не може да се дојде привремено или подолг временски период.

Управување со софтверски поправки и промени - закани што се вклучени овде:	
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.28	Софтверски недостатоци или грешки
3_0.39	Злонамерен софтвер
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.22 Заштита од злонамерен софтвер

4.22.1 Вовед

Злонамерен софтвер се однесува на програми што вршат штетни функции на системот за информатичка технологија, обично без знаење или согласност на корисникот. Овие штетни функции може да имаат најразлични цели, почнувајќи од потенцијална шпионажа и изнуда (користење уценувачки софтвер) до саботажа и уништување информации, па дури и уреди. По правило, злонамерниот софтвер може да се имплементира на сите оперативни системи и системи за информатичка технологија. Покрај традиционалните системи за информатичка технологија какви што се клиентите и серверите, ова вклучува и мобилни уреди какви што се паметните телефони. Денес, мрежните компоненти какви што се рутери и индустриски контролни системи, па дури и уредите за „интернет на нештата“ какви што се мрежните камери, исто така често се изложени на опасност од злонамерен софтвер. На класичните системи за информатичка технологија, злонамерниот софтвер се дистрибуира главно преку прилози на електронска пошта, манипулирани веб страници (попатни преземања) или медиуми за чување податоци. Паметните телефони обично се заразуваат преку инсталирање малициозни апликации, но можни се и ненамерни преземања. Покрај тоа, отворените мрежни канали, неточните конфигурации и недостатоците на софтверот се чести точки за влез на сите системи за информатичка технологија.

Во овој дел се користи терминот „програма за заштита од вируси“. Овде, „вируси“ се синоним за сите видови злонамерен софтвер. Затоа, програма за заштита од вируси се однесува на програма за заштита од кој било тип злонамерен софтвер.

4.22.2 Цел

Целта е да се опишат барањата што мора да се исполнат и да се имплементираат за ефикасно да се заштити организацијата од злонамерен софтвер.

4.22.3 Закани

Софтверски недостатоци и ненамерни преземања

Доколку системите за информатичка технологија не се доволно заштитени од злонамерен софтвер, напаѓачите може да ги искористат пропустите на софтверот за да спроведат малициозен код. Една ваква ситуација е ако софтверските поправки не се применат навремено и заштитните механизми на апликативните програми (какви што се прелистувачите) не се правилно конфигурирани. Во случај на ненамерни преземања, на пример, можеби е доволно да посетите веб страница што е заражена со злонамерен код. Недостаток во прелистувачот или во инсталирана дополнителна компонента, какви што се Java или Adobe Flash, потоа може да се искористи за да се зарази засегнатиот систем за информатичка технологија и да се обезбеди сеопфатна контрола на напаѓачот, како и пристап до мрежата на организацијата. Во тој поглед, системите за информатичка технологија што не се ажурираат редовно, какви што се многу паметни телефони, се изложени на посебен ризик.

Изнудување преку уценувачки софтвер

Уценувачкиот софтвер (ransomware) е широко распространет вид злонамерен софтвер, кој ги криптира податоците на заразениот систем за информатичка технологија и во многу случаи, криптира и дополнителни податоци до кои ќе успее да пристапи (на пример, преку мрежни споделувања). Во повеќето случаи, напаѓачите користат методи за криптирање што не можат да се вратат без соодветниот клуч како средство за изнуда на големи суми пари од нивните жртви. Ако не постои ефикасна заштита од злонамерен софтвер и не се преземат дополнителни мерки на претпазливост (како сигурносни копии на податоци), може значително да се ограничи достапноста на информациите, може да се изгубат податоците и може да настане огромна финансиска штета и штета на угледот на организацијата.

Насочени (целни) напади и социјален инженеринг

Организациите често се напаѓани од приспособен злонамерен софтвер. Во такви случаи, вработените (на пример) се измамани да отворат штетни прилози на електронската пошта преку социјален инженеринг. Приспособениот злонамерен софтвер често не може веднаш да биде откриен од програмите за заштита од вируси. И организационата единица за човечки ресурси на организацијата може да биде цел, на пример, ако му се испратат електронски документи за апликација за работа што се заразени со злонамерен софтверот. Ако напаѓачот успее да зарази систем за информатичка технологија со користење такви методи, тој може да се инфилтрира во други области на организацијата и да прегледува, манипулира или да уништува информации.

Ботнетови (Botnets)

Злонамерен софтвер може да ги регрутира системите за информатичка технологија на организацијата во ботнетови. Напаѓачите, кои често контролираат илјадници системи во ботнет, можат да ги користат за да испраќаат небарана рекламна порака (спам) или да започнат дистрибуирани напади на одбивање услуга (DDoS) на трети лица. Дури и ако организацијата не е директно оштетена, тоа сепак може да има негативно влијание врз достапноста и интегритетот на сопствените услуги и системи за информатичка технологија на организацијата, па дури и да доведе до правни проблеми. На пример, ако серверот за електронска пошта на организацијата е на црната листа, можеби веќе нема да биде можно да се праќа и прима електронска пошта.

Заразување производствени системи и уреди за „интернет на нештата“

Покрај класичните системи за информатичка технологија, уредите што не се очигледна цел, сè повеќе подложат на напади од злонамерен софтвер. На пример, напаѓачот може да зарази камера достапна преку интернет за да шпионира некоја организација. Сепак, дури и мрежна светилка или машина за кафе со контрола на апликации може да послужат како точки за влез во мрежата на организацијата или како дел од ботнет, освен кога овие уреди се доволно заштитени од злонамерен софтвер. Вмрежените производствени системи или индустриски контроли, исто така може да се манипулираат или дури и да се уништат преку злонамерен софтвер, што може да доведе до прекини и дополнителни ризици за организацијата и за нејзините вработени (на пример, поради пожар).

4.22.4 Мерки

Креирање концепт за заштита од злонамерен софтвер

Организацијата мора да подготви концепт што опишува кои системи за информатичка технологија мора да бидат заштитени од злонамерен софтвер и мора да ги вклучува уредите за „интернет на нештата“ и системи за услуги. Понатаму, мора да се прецизира како да се спроведува заштитата. Ако не е можна сигурна заштита, не треба да се работи со идентификуваните системи за информатичка технологија. Концептот треба да се документира доволно јасно и тековно да се ажурира.

Користење механизми за заштита што се специфични за системот

Организацијата мора да ги проверува механизмите за заштита што ги обезбедуваат користените системи за информатичка технологија и оперативните системи и апликациите што се користат на нив. Таквите механизми мора да се користат, освен ако не постои барем еднаква замена или добри причини против нивната употреба. Доколку не се користат, ова мора да се објасни и да се документира.

Избор на програма за заштита од вируси/крајна точка

Организацијата мора да избере и да инсталира програма за специфична цел на заштита од вируси во зависност од користениот оперативен систем, другите присутни механизми за заштита и достапноста на соодветни програми за заштита од вируси. За излезните порти и за системите за информатичка технологија што се користат за размена на податоци, мора да се избере и да се инсталира соодветна програма за заштита од вируси. Производите што се користат мора да бидат дизајнирани според средината на организацијата и да вклучуваат услуги и поддршка што се приспособени на потребите на истата. Производи само за домашни корисници или производи без поддршка од производителот не смеат да се користат за професионални производствени операции. Организацијата треба да користи услуги за „облак“ што се дизајнирани да ги подобрат ефикасностите на програмите за откривање и заштита од вируси. Ако се користат функциите на „облакот“ на таквите производи, мора да се обезбеди дека нема конфликти во врска со заштитата на податоците или нивната доверливост. Покрај скенирањето во реално време и на барање, мора да биде можно и да се скенираат компромитирани и криптирани податоци за злонамерниот софтвер со избраното решение.

Работење и конфигурирање програми за заштита од вируси/крајни точки

Програмите за заштита од вируси мора да се конфигурираат соодветно за нивната оперативна околина. Фокусот треба да биде на ефикасностите за откривање, освен ако заштитата на личните податоци или причините за изведбата не влијаат врз тоа во поединечни случаи. Доколку не се користат функции што се значајни за безбедноста на програмата за заштита од вируси, ова треба да се објасни и да се документира. Во случај на заштитни програми што се специјално оптимизирани за виртуелизација на работниот простор (desktop), истите треба да бидат транспарентно документирани дали одредени процедури за откривање се испуштени во корист на ефикасностите. Мора да се обезбеди дека корисниците не можат да направат какви било промени во врска со безбедноста на поставките на антивирусните програми.

Редовно ажурирање на програмите и на потписите за заштита од вируси

Механизмите за скенирање и потписите на злонамерниот софтвер на програмите за заштита од вируси, мора редовно и навремено да се ажурираат на соодветните системи за информатичка технологија.

Свесност и обврска на корисниците

Корисниците мора редовно да се информираат за закани од злонамерен софтвер. Тие мора да ги почитуваат основните кодекси на однесување за да го намалат ризикот од заразување со злонамерен софтвер. Датотеките, е-пошта, веб локациите и другите содржини од недоверливи извори не треба да се отвораат. Корисниците мора да бидат запознаени за лицата со кои треба да контактираат во случај на сомнежи за заразување со злонамерен софтвер. Корисниците мора да ги информираат определените контакт лица доколку се сомневаат дека има заразување што вклучува злонамерна програма.

Пријавување заразување со злонамерен софтвер

Користената програма за заштита од вируси треба автоматски да ги блокира и да ги пријави заразувањата со злонамерен софтвер. Овие автоматски извештаи треба да се испратат на централна локација. Тогаш, одговорните лица треба да одлучат како да постапат врз основа на конкретната ситуација. Постапката што треба да се следи во случај на извештаи и аларми од програмите за заштита од вируси треба да биде планирана, документирана и тестирана. Конкретно, треба да се наведат активностите што треба да се преземат во случај на потврдено заразување.

4.22.5 Напредни мерки

Користење специјални средини за анализа

Треба да се користат и автоматизирани анализи во специјално опкружување за тестирање врз основа на изолирани средини (sandbox) или посебни виртуелни или физички системи за процена на сомнителни податоци.

Користење неколку механизми за скенирање

За да се подобрат ефикасностите за откривање, треба да се користат програми за заштита од вируси со неколку алтернативни механизми за скенирање системи за информатичка технологија за кои е потребна посебна заштита (на пример, порти и системи за информатичка технологија за размена на податоци).

Користење заклучени медиуми за чување податоци

Пред поврзување медиум за чување податоци од трети лица со системите за информатичка технологија на организацијата, треба да се провери дали медиумот за чување податоци е заклучен.

Ракување со несигурни (недоверливи) датотеки

Доколку е неопходно да се отворат недоверливи датотеки, тоа треба да се прави само на изолиран систем за информатичка технологија. Во овој систем, соодветните датотеки, на пример, треба да се конвертираат во безбеден формат или да се отпечатаат, ако со тоа се намалува ризикот од заразување со злонамерен софтвер.

Избор и користење производи за кибер безбедност за спречување насочени напади

Организацијата треба да ја испита употребата и додадената вредност на производите и на услугите што нудат поголем опсег на заштита во споредба со конвенционалните антивирусни програми. Безбедносните производи како овие треба да се користат против насочени напади, како на пример при работа на активни датотеки во специјални средини за анализа. Пред да се донесе одлука за купување одреден безбедносен производ, треба да се тестира ефикасноста на неговата заштита и неговата компатибилност со средината за информатичка технологија на организацијата.

Заштита од злонамерен софтвер - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.27	Недостаток на ресурси
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.39	Злонамерен софтвер
3_0.42	Социјален инженеринг
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.23 Бришење и уништување податоци и уреди

4.23.1 Вовед

Бришењето и уништувањето на податоците и на уредите е основен дел од животниот циклус на информациите на медиумите за чување податоци. Во овој дел, терминот „медиум за чување податоци“ се однесува на аналогни медиуми за чување податоци, какви што се хартија или филмови, како и дигитални медиуми за чување податоци, какви што се хард-дискови, SSDs или CDs.

Ако медиумот за чување податоци се отфрли, информациите што ги содржи може да бидат откриени доколку медиумот не е безбедно избришан или целосно уништен. Покрај клиентите и серверите, ова може да влијае врз сите системи за информатичка технологија, вклучувајќи ги и уредите за „интернет на нештата“ какви што се паметните телевизори, кои наводно складираат само незначителни информации. Уредите за „интернет на нештата“ често се поврзуваат преку безжична локална мрежа (WLAN) и ги зачувуваат потребните податоци за пристап. Ова може да се податоци што треба да бидат заштитени и што не треба да се откриваат на неовластени лица.

Вообичаените процеси на бришење засновани на функциите на оперативниот систем обично не ги бришат информациите на безбеден начин кој што спречува реконструкција на податоците. Затоа се потребни посебни процедури за безбедно бришење на информациите. Меѓутоа, медиумите за чување податоци можат да се избришат безбедно и ефективно само во целост, а тоа обично е можно само во ограничен обем со поединечни датотеки. Покрај тоа, постојат закони како што е Законот за заштита на личните податоци, кои предвидуваат правила за бришење и уништување документи. Овие правила од една страна, предвидуваат периоди на чување, пред кои не треба да биде извршено бришење на документите (на пример, на деловни трансакции, биланси на состојба или договори), а од друга страна, предвидуваат правила за безбедно бришење на податоците по исполнување на целта, особено кога истите содржат лични податоци.

4.23.2 Цел

Целта е да се опише како информациите во организацијата можат безбедно да се избришат и да се уништат и како може да се создаде соодветен холистички концепт за тој процес.

4.23.3 Закани

Непостојни или недоволно документираните процедури за бришење и уништување

Доколку не постојат безбедни процеси и процедури за бришење и уништување информации и медиуми за чување податоци или тие не се користат правилно, тогаш нема гаранција дека доверливите информации ќе бидат безбедно избришани или уништени. Затоа е невозможно да се предвиди каде ќе завршат овие информации и дали ќе бидат достапни за трети лица. Оваа опасност е особено голема во случај на дигитални медиуми и системи за информатичка технологија што треба да се отфрлат, бидејќи не е секогаш веднаш видно какви (преостанати) информации има на нив. Овие информации може да ги прочитаат неовластени трети лица. Доколку станува збор за информации што треба да бидат заштитени, какви што се деловни тајни или посебни категории на лични податоци во смисла на Законот за заштита на личните податоци, тоа може да резултира со изрекување на прекршочна санкција.

Губење на доверливоста поради преостанати информации на медиумот за чување податоци

Повеќето стандардни апликации и оперативни системи не ги бришат податоците на безбеден начин кој вклучува целосно нивен неповратен процес. По правило, само референците на датотеката се отстрануваат од администраторските информации на системот за датотеки, при што блоковите што припаѓаат на датотеката се означени како слободни. Сепак, реалната содржина на блоковите на медиумот за чување податоци се задржува и може да се реконструира со соодветни алатки. Ова може да им овозможи на напаѓачите пристап до датотеките, како, на пример, кога медиумот за чување податоци им се предава на трети лица или несоодветно се отстранува. Оттука, доверливите информации може да се најдат во рацете на неовластени лица.

Помошните датотеки, помошните партиции и датотеките за режим на хибернација понекогаш содржат и доверливи податоци какви што се лозинки или криптографски клучеви. Сепак, овие податоци и нивната содржина често не се заштитени. Тие може да се читаат, на пример, ако медиумот за чување податоци се отстрани и повторно се инсталира во друг систем за информатичка технологија.

Тековното активно работење на многу апликации исто така создава датотеки што не се потребни за производствените средини, какви што се историите на прелистувачот. Овие датотеки може да вклучуваат и информации што се значајни за безбедноста. Ако помошните датотеки или привремените датотеки не се безбедно избришани, информациите што треба да бидат заштитени, лозинките и клучевите може да бидат злоупотребени од неовластени лица за да добијат пристап до дополнителни системи за информатичка технологија и податоци, да добијат конкурентна предност на пазарот или насочено да го шпионираат однесувањето на корисниците.

Несоодветно вклучување надворешни даватели на услуги во процесот на бришење и уништување

Кога надворешни даватели на услуги бришат или уништуваат медиуми за чување податоци, информациите на нив може да бидат изложени доколку нема доволно регулирани правила за тоа како надворешниот давател на услуги е интегриран во процесот на бришење и уништување. На пример, напаѓачите би можеле да украдат медиум за чување податоци од несоодветно обезбедени собирни места или да добијат пристап до преостанатите информации ако давателот на услугата не го избрише или не го уништи медиумот за чување податоци со доволно ниво на безбедност.

Несоодветно ракување со неисправни медиуми за чување податоци или уреди за информатичка технологија

Ако медиумот за чување податоци е неисправен, тоа не мора да значи дека податоците на него се неповратно оштетени. Во многу случаи, податоците или барем делови од нив може да се обноват со специјални алатки. Ако неисправните медиуми за чување податоци или уредите за информатичка технологија едноставно се отстранат без бришење или уништување на податоците на нив, овие податоци може да се откријат за време на процесот на отстранување.

Податоците во неисправните медиуми за чување податоци може да се откријат и при поправки или барања за гаранција. На пример, една организација испраќа неисправен хард-диск назад до производителот под барање за гаранција. Производителот утврдува дека контролерот е неисправен и го заменува неисправниот модел со нов. Истовремено, првично неисправниот хард-диск само брзо, а со тоа и несигурно се брише. Потоа хард дискот се враќа на пазарот. Во овој процес, информациите што треба да бидат заштитени може да се откријат во текот на целиот процес, бидејќи сè уште се на оригиналниот хард-диск.

4.23.4 Мерки

Прописи за бришење или уништување информации

Организацијата мора да го регулира бришењето и уништувањето на информациите. Притоа, сопствениците на процесот за секоја специјализирана постапка или деловен процес мора да наведат кои информации мора да се избришат и да се отстранат и под кои услови. Тие мора да ги земат предвид прописите кои:

- ги дефинираат минималните периоди на чување,
- гарантираат максимални периоди на чување и безбедно бришење на личните податоци.

Доколку се вклучени лични податоци, прописите за бришење и уништување лични податоци мора да се координираат со офицерот за заштита на личните податоци.

Исто така, пред да започне процесот на бришење и уништување информации за специјализираните постапки, деловните процеси и системите за информатичка технологија, организацијата мора да го пропише и регулира овој процес на бришење и уништување информации.

Правилно бришење и уништување сензитивни ресурси и информации

Сензитивните информации и медиумот за чување податоци мора безбедно да се избришат или да се уништат пред да се фрлат. Процесот за ова мора да биде јасно регулиран. Вработените мора да бидат информирани за задачите што треба да ги извршуваат за безбедно бришење и уништување. При процесот за бришење и уништување медиуми за чување податоци, мора да се земат предвид и сигурносните копии кога тоа е потребно. Локацијата каде што ќе се врши уништување на информациите во организацијата мора да биде јасно регулирана. Во овој поглед, мора да се земе предвид дека информациите и ресурсите може прво да се собираат, а подоцна да се избришат или да се уништат. Централното собирно место од овој вид мора да биде заштитено од неовластен пристап.

Бришење и уништување медиуми за чување податоци од страна на надворешни даватели на услуги

Доколку, организацијата ангажира надворешни даватели на услуги, процесот за бришење и уништување мора да биде доволно безбеден и транспарентен. Процедурите што ги користи надворешниот давател на услуги за безбедно бришење и уништување, мора најмалку да ги исполнуваат внатрешните барања на организацијата за процедурите за бришење и уништување. Процедурите што ќе ги користи надворешниот давател на услуги за безбедно бришење и уништување, треба редовно да се проверуваат за да се обезбеди дека нивните операции сè уште правилно се одвиваат.

Минимални барања за процедури за бришење и уништување

Организацијата мора да ги спроведе следните минималните барања за процедури за бришење и уништување медиуми за чување податоци и тоа:

- Дигитални медиуми што можат повторно да се запишуваат и кои не се криптирани за време на употребата мора да бидат целосно презапишани со проток на податоци од случајни вредности (на пример, PRNG тек).
- Доколку се користат криптирани дигитални медиуми, тие мора да се избришат преку безбедно бришење на соодветниот клуч во согласност со соодветниот криптоконцепт.
- Оптичките медиуми за чување податоци мора да се уништат во согласност со безбедносното ниво О-3 (најмалку) како што е дефинирано во ISO/IEC 21964-2.
- Паметните телефони и другите паметни уреди треба да бидат криптирани во согласност со предметниот криптоконцепт. Паметните телефони и другите паметни уреди мора да се ресетираат на фабрички поставки. Потоа треба да се изврши процесот на поставување за да се заврши бришењето.

- Уредите за „интернет на нештата“ мора да се ресетираат на фабрички поставки. Сите структури на податоци што се зачувани во таквите уреди потоа мора да се променат.
- Хартијата мора да се уништи во согласност со безбедносното ниво P-3 (најмалку) како што е дефинирано во ISO/IEC 21964-2.
- Медиумите за чување податоци што се интегрирани во други уреди мора безбедно да се избришат преку интегрираните функции на уредите. Ако ова не е можно, компонентите за обемно чување податоци мора да се отстранат или безбедно да се избришат како конвенционалните дигитални медиуми од посебен систем за информатичка технологија или да се уништат во согласност со нивото на безбедност E-3 или H-3 (најмалку) како што е прецизирано во ISO/IEC 21964-2.

Овие процедури организацијата треба да ги прегледува и приспособува по потреба, во зависност од потребите за заштита на податоците што се обработуваат.

Избор на соодветни методи за бришење или уништување медиум за чување податоци

Организацијата треба да потврди дека минималните барања за процедурите за бришење и уништување се доволно безбедни за медиумите и информациите што навистина се користат. Врз основа на своите наоди, организацијата треба да утврди соодветни процедури за бришење и уништување на секој медиум за чување податоци. За сите видови медиуми за чување податоци што организацијата ги користи, ги брише или ги уништува, треба да има соодветни уреди и алатки со кои одговорните вработени можат да ги избришат или да ги уништат зачуваните информации. Со избраните процедури треба да бидат запознаени сите одговорни лица. Организацијата треба редовно да проверува дали избраните методи сè уште одговараат на најсовремените технолошки достигнувања и дали се доволно безбедни за нејзините цели.

Креирање политика за бришење и уништување информации

Организацијата треба да ги документира своите правила за бришење и уништување во соодветна политика. Со политиката треба да бидат запознаени сите вработени во организацијата и да претставува основа за нивните активности и работа. Во однос на нејзината содржина, политиката треба да ги вклучува сите употребени медиуми за чување податоци, апликации, системи за информатичка технологија и други ресурси и информации што подлежат на бришење и на уништување. Почитувањето и применувањето на политиката од страна на вработените, организацијата треба редовно да го проверува и по случаен избор. Политиката треба редовно да се ажурира.

Уништување неисправни дигитални медиуми за чување податоци

Доколку, поради дефект, дигиталните медиуми за чување што содржат информации што треба да бидат заштитени не можат безбедно да се избришат во согласност со важечките процедури за бришење медиум за чување податоци, тие треба да се уништат во согласност со безбедносното ниво 3 (најмалку) како што е предвидено во ISO/IEC 21964-2.

Во случај да се заменат или да се поправат неисправните медиуми за чување податоци, треба да се склучи договор со давателот на услуги кој е избран за оваа цел, дека овие медиуми ќе бидат безбедно избришани или уништени од негова страна. Процедурите на давателот на услугата треба да ги исполнуваат најмалку внатрешните барања на организацијата за процедурите за бришење и уништување.

4.23.5 Напредни мерки

Уништување медиуми за чување податоци на зголемени нивоа на безбедност

Организацијата треба да го одреди нивото на безбедност што е потребно за уништување на нејзините медиуми за чување податоци во согласност со ISO/IEC 21964-1 врз основа на потребите за заштита на медиумот што треба да се уништи. Медиумите треба да се уништат во согласност со доделеното безбедно ниво наведено во ISO/IEC 21964-2.

Бришење и уништување податоци и уреди - закани што се вклучени овде:	
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.24	Уништување на уреди или медиуми за чување податоци

4.24 Размена на информации

4.24.1 Вовед

Информациите се пренесуваат помеѓу испраќачите и примателите преку комуникациски канали какви што се лични разговори, телефонски повици, писма, преносливи медиуми и мрежи што овозможуваат размена на информации и податоци. Правилата за размена на информации гарантираат дека доверливите информации се пренесуваат само на овластени лица. Ваквите правила се особено неопходни кога информациите се пренесуваат преку надворешни мрежи што овозможуваат размена на информации и податоци.

4.24.2 Цел

Целта е да се обезбеди размена на информации помеѓу различни партнери во комуникацијата така што ќе и се помогне на организацијата да создаде соодветни концепти.

4.24.3 Закани

Одложена достапност на информации

Размената на информации може да биде нарушена, одложена или прекината. Доколку користената технологија предизвикува грешки во преносот, преносот на информации може да биде одложен, нецелосен или премногу бавно обработен. Под одредени околности, размената на информации може целосно да запре, бидејќи интерфејсите или оперативните ресурси не се доволно моќни или откажуваат поради некоја друга причина. Деловните процеси може значително да се нарушат доколку не се испочитуваат бараните рокови за доставување информации. Во екстремни случаи, договорните рокови може да не се испочитуваат, ако преносот на податоци не успее поради технички прекини или човечка грешка.

Нерегулирано проследување информации

Информациите коишто треба да бидат заштитени можат да се најдат во рацете на неовластени лица. Доколку, на пример, не се склучи договор за доверливост пред да се разменат информациите, нема да може да се контролира кој ги прима и ги користи информациите. Ризикот од злоупотреба на податоците исто така се зголемува доколку договорот за доверливост е непрецизен или нецелосно формулиран.

Споделување лажни или внатрешни информации

Информациите коишто треба да бидат заштитени може да се испратат до неовластени примачи. Ваквите информации може ненамерно да паднат во рацете на неовластени корисници доколку вработените не се доволно свесни за оваа опасност и не се соодветно обучени. На пример, може да се пренесат медиуми за чување податоци што содржат преостанати информации какви што се недоволно избришани наследени податоци. Други преостанати информации вклучуваат неизбришани внатрешни коментари, кои може ненамерно да се пренесат на надворешен примач во електронски документ (на пример, како прилог на електронска пошта). Во други случаи, доверливите документи може случајно да се испратат до погрешен примач, бидејќи не постојат јасни упатства за постапување со нив.

Неовластено копирање и менување информации

Напаѓачите можат да пресретнат информации и податоци или да влијаат врз нив без да бидат забележани. Тие можат и да украдат информации доколку не се доволно заштитени. На пример, напаѓачот може да пресретне медиум за чување податоци во поштата или да ја чита содржината на незаштитената електронска пошта без да биде забележан. Напаѓачот исто така на пример може да менува незаштитени информации додека се пренесуваат, со цел да вметне злонамерен софтвер во датотеките.

Несоодветна примена на процедури за криптирање

Заштитата на информациите при пренос со користење криптографски процедури може да биде нарушена од напаѓачите. Напаѓачот што го знае криптографскиот метод што се користи, може да ги пресретне криптираните податоци и поврзаниот клуч доколку вработените не го користат правилно методот на криптирање. Вработените што не биле доволно обучени можат, на пример, да ги испратат клучот и податоците на истиот медиум за податоци. Често се користат и клучеви што премногу лесно може да се погодат.

4.24.4 Мерки

Дефинирање овластени примачи

Организацијата мора да се погрижи откривањето на информациите да биде во согласност со барањата предвидени во закон. Организацијата мора да дефинира кои приматели смеат да примаат и да споделуваат конкретен вид информации. Мора да се дефинираат каналите преку кои може да се разменуваат соодветните информации. Пред размената на информации, секој вработен мора да се погрижи примачот да ги има потребните овластувања за примање и обработка на информациите.

Регулирање на размената на информации

Пред да се разменат информациите, сопственикот на информациите мора да го одреди нивното ниво на сензитивност. Сопственикот на информации мора да одреди како да ги заштити информациите за време на преносот. Ако се пренесуваат информации што треба да бидат заштитени, сопственикот на информациите мора да го информира примачот за нивното ниво на сензитивност. Доколку информациите се сензитивни, сопственикот на информациите мора да го извести и примачот дека може да ги користи информациите само за целта за која се пренесени.

Упатство за кадарот за размена на информации

Сопственикот на процесот мора да ги извести вклучените вработени при размената на информации за условите за секоја нивна размена. Сопственикот на процесот мора да се погрижи вработените да знаат кои информации можат да ги пренесат, како и кога, каде и како.

Договори за размена на информации со надворешни страни

Доколку информациите редовно се разменуваат со други организации, организацијата треба формално да се договори за соодветната рамка. Овој договор за размена на информации треба да содржи информации за заштита на сите доверливи информации.

Отстранување на преостанати информации пред споделување

Покрај општата обука, организацијата дополнително треба да ги информира своите корисници и за опасностите од преостанати и дополнителни информации во документите и датотеките. Корисниците треба да се научат како да избегнуваат преостанати и дополнителни информации во документите и датотеките. Организацијата треба да му укаже на секој корисник како да ги исклучи несаканите преостанати информации од размената на информации. Корисниците треба да ја проверат секоја датотека и документ за несакани преостанати информации пред да ги споделат. Корисниците треба да ги отстранат несаканите преостанати информации од документите и од датотеките.

Проверки на компатибилност на системи за испраќач и за примач

Пред размената на информации, треба да се провери компатибилноста на системите за информатичка технологија и производите на испраќачот и на примачот.

Сигурносни копии од пренесените податоци

Корисниците треба да направат сигурносна копија на пренесените информации во случај кога информациите не можат да се вратат од други извори.

Криптирање и дигитални потписи

Организацијата треба да провери дали информациите можат да бидат криптографски обезбедени за време на размена. Ако информациите треба да бидат криптографски обезбедени, тогаш треба да се користат доволно безбедни процедури за таа цел.

4.24.5 Напредни мерки

Договори за доверливост

Пред да открие доверливи информации на надворешни лица, корисникот треба да ја извести организацијата. Организацијата треба да склучи договор за доверливост со примачите. Договорот за доверливост треба да регулира како информациите може да се чуваат од страната што ги прима. Договорот за доверливост треба да определи кој од страната што ги прима информациите може да има пристап до конкретните пренесени информации.

Размена на информации - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.29	Повреда на закони или на договори
3_0.45	Губење податоци

4.25 Евиденција на пристап (Logging)

4.25.1 Вовед

За да се обезбедат сигурни операции на информатичката технологија, системите за информатичка технологија и апликациите треба да ги евидентираат сите или барем некои одбрани настани што се од значење за операциите и за безбедноста т.е. да ги снимаат автоматски и да ги дадат за проценка. Евиденцијата се користи во многу организации како средство за навремено идентификување на хардверските и софтверските проблеми и препреките кај ресурсите. Сепак, безбедносните проблеми и нападите на мрежните услуги може да се следат и врз основа на податоците од оваа евиденција. Преку форензичко испитување, може да се обезбедат докази од таквите податоци откако ќе се дознае за напад на системите за информатичка технологија или на апликациите.

Во секој информативен домен, податоците од евиденцијата се генерираат локално од голем број системи за информатичка технологија и апликации. Меѓутоа, за да се добие целосен преглед на даден домен на информации, записите генерирани од различни системи за информатичка технологија и апликации може да се испратат до посебна инфраструктура за евидентирање на записите за централно зачувување. Само тогаш генерираните записи може да се избераат, филтрираат и систематски да се анализираат на една централна локација.

4.25.2 Цел

Овој дел содржи барања што мора да се исполнат за да се олесни евиденцијата на колку што е можно повеќе записи што се значајни за безбедноста. Целта е безбедно да се приберат и да се зачуваат сите релевантни податоци и да бидат достапни за евалуација.

4.25.3 Закани

Недоволна евиденција

Во доменот на информации, често има системи за информатичка технологија и апликации со стандардни поставки во кои е овозможена евиденција. Понекогаш, поединечните системи за информатичка технологија или апликации воопшто не можат да вршат евиденција. Во двата случаи, може да се изгубат важни информации и може да биде невозможно навремено да се откријат нападите. Ова е можно и ако евиденцијата се користи за поединечни системи за информатичка технологија или апликации, но записите од настаните кои се генерираат не се прибираат на централна локација. Во домените на информации без централизирана евиденција, тешко е да се обезбеди дека евидентираните записи за сите системи за информатичка технологија и апликации ќе бидат зачувани и анализирани.

Понатаму, записи од настаните кои се генерираат мора да содржат значајни информации. Настаните што треба да се евидентираат зависат, меѓу другото, од потребите за заштита на соодветните системи за информатичка технологија или апликации. Ако ова се занемари, на пример, само со користење на стандардните поставки на системите за информатичка технологија и апликациите за евиденција, може да доведе до тоа да не се евидентираат особено важни настани за безбедноста. Како резултат на тоа, може да не се откријат нападите.

Неправилан избор на релевантни записи

Записите од настаните кои се генерираат честопати обезбедуваат важни информации што помагаат во откривање безбедносни инциденти. Сепак, филтрирањето на релевантните пораки од големиот број различни настани во записите претставува посебен предизвик. Причината за тоа е што многубројните записи се само информативни по природа и го одвлекуваат вниманието од оние пораки што се навистина важни. Ако се избераат премногу записи, анализата на сите нивни информации ќе биде тешка и ќе бара многу време.

Понатаму, записите од настаните може да се отфрлат или да се презапишат, ако капацитетот на RAM-меморијата или на хард-дискот на системот за информатичка технологија или инфраструктурата за евиденција е недоволен. Ако ова резултира со снимање премалку релевантни записи од настани, инцидентите што се клучни за безбедноста може да останат неоткриени.

Недостаток на соодветна временска синхронизација во текот на евиденцијата

Доколку времето не е синхронизирано на сите системи за информатичка технологија во доменот на информации, можно е да нема корелација помеѓу записите од настаните што тие ги произведуваат, а обидот да се поврзат може да резултира со погрешни изјави. Ова се должи на недостатокот на заедничка основа за различните временски печати на настаните. Затоа е потешко да се проценат записите од настаните кои се генерирани каде што нема временска синхронизација, особено ако податоците се зачувани на централен сервер за евиденција. Понатаму, недостатокот на соодветна временска синхронизација може да го оневозможи користењето на записите од настаните за обезбедување докази.

Слабо планирање на евиденцијата

Ако евиденцијата не е доволно испланирана, системите за информатичка технологија или апликациите може да не се следат, а настаните што се значајни за безбедноста може да не се препознаат и како резултат на тоа, нема соодветно да се решат. Дополнително, нема да може да се следат и непочитувањата на прописите за заштита на личните податоци.

Губење доверливост и интегритет во записите од настаните

Некои системи за информатичка технологија во домен на информации генерираат записи од настани (какви што се кориснички имиња, IP-адреси, адреси на е-пошта и имиња на компјутери) кои можат да се поврзат со одредени лица. Таквите информации може да се копираат, да се пресретнат и да се манипулираат доколку не се криптирани и безбедно зачувани. Како резултат на тоа, напаѓачите може да пристапат до доверливи информации или да користат манипулирани записи од настани за намерно прикривање безбедносни инциденти. Понатаму, ако напаѓачите добијат голема количина на записи од настани, тие може да ги користат за да ја утврдат внатрешната структура на соодветниот домен на информации и да извршат повеќе насочени напади.

Неправилно конфигурирана евиденција

Ако најавувањето во системите за информатичка технологија е неправилно конфигурирано, важните информации ќе бидат пропуштени или нема да бидат правилно евидентирани. Можно е и да се евидентираат неточни или прекумерни информации. На пример, личните податоци може да се евидентираат и да се чуваат без овластување. Според тоа, организацијата може неправилно да ги примени законските барања. Поради неправилно конфигурирана евиденција, записите од настаните може да бидат достапни и во неконзистентни или во сопственички формати. Во такви случаи, може да биде тешко да се проценат записите и безбедносните инциденти може да останат неоткриени.

Откажување на изворите на записите од настаните

Ако системите за информатичка технологија во доменот на информации повеќе не ги обезбедуваат потребните записи од настани, нема да биде можно соодветно да се детектираат безбедносни инциденти. Грешките во хардверот и во софтверот, како и неправилно администрираните системи за информатичка технологија, може да бидат причина за такви откажувања на изворот на записите од настаните. Конкретно, ако не се открие откажување на изворите на записите од настаните, тоа може да создаде лажна перцепција за безбедносната состојба на организацијата. Така, на пример напаѓачите можат да бидат неоткриени долго време и можат да пресретнуваат информации што се важни за организацијата или да манипулираат со системите за услуги.

Недоволен капацитет на инфраструктурата за евиденција

Поради сложените домени на информации и опсежните сценарија за напади, барањата што треба да ги исполнат системите за евиденција се зголемуваат бидејќи мора да се зачува и да се обработува многу голема количина на записи од настани. Покрај тоа, вообичаено е да се зголемува интензитетот на евиденцијата кога се случуваат безбедносни инциденти. Меѓутоа, ако соодветната инфраструктура за евиденција не е дизајнирана за ова, зачуваните записи од настаните може да бидат нецелосни. Како резултат на тоа, настаните што се значајни за безбедноста ќе бидат недоволно оценети или воопшто нема да бидат оценети и безбедносните инциденти ќе останат неоткриени.

4.25.4 Мерки

Изработување безбедносна политика за евиденција на секој пристап

Организацијата треба врз основа на нејзината општата безбедносна политика, да изработи специфична безбедносна политика за евиденција на секој пристап. Оваа безбедносна политика мора транспарентно да ги опишува барањата и спецификациите за тоа како да се испланира, да се постави и безбедно да се управува со евиденцијата за секој пристап. Оваа безбедносна политика мора да прецизира што треба да се евидентира, како и каде. Во овој поглед, видот и обемот на евиденцијата за секој пристап треба да се заснова на потребите за заштита на информациите во организацијата.

Оваа безбедносна политика мора да ја изработи овластеното лице за безбедност на информации заедно со сопствениците на процесот. Со безбедносната политика мора да бидат запознаени и информирани сите вработени кои се задолжени за евиденцијата за секој пристап и истата да ја применуваат при нивната работа. Доколку се промени оваа безбедносна политика или се дозволат отстапувања од барањата, тоа мора да се документира и да се координира со овластеното лице за безбедност на информации. Безбедносната политика мора редовно да се проверува и резултатите од овие проверки мора да се документираат.

Конфигурирање евиденција на ниво на систем и мрежа

Мора да се евидентираат сите настани во врска со безбедноста на системите за информатичка технологија и апликациите. Ако системите за информатичка технологија и апликациите што се дефинирани како релевантни во политиката за евиденција за секој пристап имаат функција за евиденција, таа мора да се користи. При поставување на евиденцијата, мора да се земат предвид спецификациите на производителот за соодветните системи за информатичка технологија или апликации.

Мора да се извршат проверки на самото место на соодветни временски интервали за да се обезбеди дека евиденцијата сè уште функционира правилно. Интервалите на овие проверки мора да бидат дефинирани во политиката за евиденција на секој пристап.

Доколку настаните што се значајни за операциите и за безбедноста не може да се евидентираат на систем за информатичка технологија, тогаш мора да се интегрираат дополнителни системи за информатичка технологија за евиденција (на пример, за настани на ниво на мрежа).

Временска синхронизација на системи за информатичка технологија

Системското време за евиденција на сите системи за информатичка технологија и апликации секогаш мора да биде синхронизирано. Мора да се обезбеди дека форматите на датумот и времето на датотеките за записите се еднообразни.

Усогласеност со условите на правната рамка

При водење на евиденцијата за секој пристап мора да се применуваат прописите за заштита на личните податоци, да се почитуваат основните права и слободи на вработените во организацијата, како и сите барања предвидени со други закони.

Податоците од записите мора да се избришат во согласност со определен и дефиниран процес. Техничките мерки мора да спречат неконтролирано бришење или менување на податоците од записите.

Основна структура на централизирана инфраструктура за евиденција на секој пристап

Особено во поголемите домени на информации, сите прибрани податоци од записите што се значајни за безбедноста треба да се зачуваат на централна локација. За таа цел, треба да се дизајнира централна инфраструктура за евиденција (систем на сервер за записи) и да се постави во мрежен сегмент креиран за оваа намена.

Покрај настаните што се значајни за безбедноста, централната инфраструктура за евиденција треба да ги евидентира и општите оперативни настани што укажуваат на грешки.

Инфраструктурата за евиденција за секој пристап треба да има доволен капацитет. Исто така, треба да се разгледа можноста за зголемување на капацитетот на оваа инфраструктура за да се овозможи евидентирање на зголемениот обем на евиденцијата. За таа цел, треба да бидат достапни доволно технички, финансиски и кадровски ресурси.

Архивирање на податоците од записите

Податоците од записите треба да се архивираат и во овој поглед треба да се земат предвид и барањата предвидени со закон.

Обезбедување податоци од евиденцијата за секој пристап

Прибраните податоци од записите треба да се филтрираат, да се нормализираат, да се спојат и да се доведат во заемна врска. Податоците од записите што се обработени на овој начин, треба да бидат достапни така што ќе бидат соодветни за процена. Апликациите за евиденција треба да имаат соодветни интерфејси за програмите за оценување за да може податоците да се проценат автоматски. Треба да се обезбеди дека евалуацијата на податоците од записите е во согласност со безбедносните барања што се дефинирани во соодветната политика за евиденција на конкретната организација. Треба да се земат предвид и оперативните и внатрешните договори кога ќе бидат достапни податоците од записите. Податоците од записите треба да се зачувуваат во непроменета форма, односно во нивниот оригинален формат.

Заштита на пристап за податоци од записите

Организацијата треба да обезбеди дека администраторите што ја одржуваат евиденцијата за секој пристап немаат овластување да ги менуваат или да ги бришат зачуваните податоци од записите.

4.25.5 Напредни мерки

Зголемување на опсегот на евиденцијата за секој пристап

Ако е потребна поголема заштита на апликациите или на системите за информатичка технологија, тогаш треба да се евидентираат повеќе настани за да може колку што е можно поцелосно да се следат инцидентите во врска со безбедноста.

За да се обезбеди дека податоците од записите може да се проценат во реално време, треба да се зачуваат централно во пократки интервали од соодветните системи за информатичка технологија и апликации. Евиденцијата за секој пристап треба да овозможи процена на целиот соодветен домен на информации. Апликациите и системите за информатичка технологија што не овозможуваат централна евиденција не треба да се користат во случај на зголемени потреби за заштита.

Криптирање на податоците од записите

Податоците од записите треба да се криптираат за безбеден пренос. Сите зачувани записи треба да бидат дигитално потпишани. Архивираните податоци од записите и податоците за записите што се зачувани надвор од соодветната инфраструктура за евиденција на секој пристап, треба исто така секогаш да се зачувуваат во криптирана форма.

Високодоступна инфраструктура за евиденција на секој пристап

Организацијата треба да создаде високодоступна инфраструктура за евиденција на секој пристап.

Евиденција - закани што се вклучени овде:	
3_0.9	Дефект или неисправност на комуникациските мрежи
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.32	Злоупотреба на овластувања
3_0.37	Одредување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.40	Одбивање на услуга
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.26 Сервери за датотеки**4.26.1 Вовед**

Сервер за датотеки е мрежен сервер што обезбедува датотеки централно од внатрешни или од мрежни хард дискови за сите корисници или клиенти со овластување за пристап. На тој начин, овластените корисници можат да споделуваат податоци без да мора да ги пренесуваат до пренослив медиум или да ги дистрибуираат преку е-пошта, како на пример. Бидејќи податоците се чуваат централно, тие можат да бидат структурирани и обезбедени во различни директориуми и датотеки. Со серверите за датотеки, правата за пристап до датотеките исто така може да се доделат централно. Покрај тоа, зачувувањето на сите податоци на централна локација, го прави поедноставно создавањето на сигурносни копии.

Серверот за датотеки главно управува со уредите за масовно чување поврзани преку интерфејси какви што се SCSI (мал компјутерски системски интерфејс), SAS (сериски прикачен SCSI) или SSD (полупроводнички диск). Самата меморија за зачувување податоци се наоѓа директно или во кукиштето на серверот или пак е поврзана надворешно. Надворешното поврзување често се нарекува „директно прикачено зачувување“ (DAS). Серверот за датотеки може да се ракува на конвенционален серверски хардвер или на наменски уред. За големи количини податоци, уредите на централната мрежа за зачувување податоци (SAN) може да се поврзат и преку главните адаптери (HBA - host bus adapter) во серверот, како и со SAN преклопници.

4.26.2 Цел

Целта е да се опишат главните закани што се специфични за серверите за датотеки и барањата што произлегуваат за безбедна работа на таквите сервери.

4.26.3 Закани

Откажување на серверот за датотеки

Ако серверот за датотеки откаже, може да биде засегнат целиот околен домен на информации, вклучително важни деловни процеси и специјализирани задачи во рамките на организацијата. Покрај корисниците, апликациите може да зависат од податоците од серверот за датотеки за правилно функционирање. Доколку податоците и услугите не се достапни, би можело да не биде можно да се запазат роковите и суштинските деловни процеси да бидат неуспешни. Во меѓувреме, немањето соодветен концепт за управување со обезбедување на континуитет на деловното работење, може дополнително да го зголеми времето што е потребно за враќање на засегнатите системи на интернет. Ова во многу случаи може да доведе до финансиски загуби. Откажувањето на серверот за датотеки може да има влијание и врз други организации.

Недоволни карактеристики на серверот за датотеки

Ако линијата за поврзување или капацитетот за зачувување на серверот за датотеки не се доволни, тоа може да доведе до зголемени времиња на пристап или препреки за зачувувањето. Како последица на тоа, на пример, вработените може да бидат фрустрирани и да почнат да зачувуваат податоци локално поради долгото време на чекање, што значи дека веќе нема да може да се следи кој има одредени податоци и каде се зачувани. Апликациите што се засноваат на правилно (посредничко) зачувување информации, исто така нема да можат повеќе да функционираат сигурно.

Недоволна проверка на зачуваните датотеки

Доколку серверот за датотеки не е доволно вклучен во концептот за заштита од злонамерен софтвер на организацијата, напаѓачите може незабележано да го постават злонамерниот софтвер на серверот за датотеки. Сите системи за информатичка технологија и апликации што пристапуваат до податоците на серверот за датотеки би можеле да бидат заразени со злонамерен софтвер, предизвикувајќи тој многу брзо да се шири низ самата организација.

Недоволен концепт за овластување за пристап

Доколку овластувањата и одобренијата за пристап не се правилно дизајнирани и доделени, неовластени трети лица би можеле да пристапат до податоците. Така, напаѓачите или неовластените корисници би можеле да менуваат, да бришат или да копираат податоци.

Неструктурирано зачувување податоци

Доколку структурата за зачувување податоци не е прецизирана или вработените не се придржуваат кон неа, податоците може да се зачуваат некоординирано на серверот за датотеки. Ова доведува до различни проблеми, како што е беспотребно потрошен простор на дискот поради повеќекратно зачувување на истите датотеки. Може да се зачуваат и различни верзии на датотека. Освен тоа, можен е неовластен пристап, на пример, ако датотеките се наоѓаат во директориуми или во системи на датотеки што се достапни за трети лица.

Губење податоци зачувани на сервери за датотеки

Ако серверот за датотеки целосно откаже или се утврди дека поединечните компоненти се неисправни, може да се изгубат важни податоци во отсуство на функционална сигурносна копија или синхронизација на податоците. Истото важи и кога вработените ненамерно бришат датотеки. Понатамошни проблеми може да настанат, на пример, ако не е обезбедена доволна редундантност со помош на редундантна низа на независни дискови (RAID). Откажувањето на поединечни медиуми за чување податоци, тогаш ќе има директно влијание врз операциите, бидејќи датотеките повеќе нема да бидат достапни.

Уценувачки софтвер

Уценувачки софтвер е посебна форма на злонамерен софтвер што криптира податоци на заразени системи за информатичка технологија. Напаѓачите потоа бараат исплата на откуп, тврдејќи дека потоа ќе ѝ овозможат на жртвата повторно да ги декриптира податоците. Сепак, дури и откако ќе се плати откупот, нема гаранција дека податоците може да се вратат.

Криптирањето не е ограничено на локалните податоци на заразениот систем за информатичка технологија. За многу форми на уценувачки софтвер се потребни мрежни дискови со пристап за пишување за да ги криптираат и сите нивни податоци. Ова значи дека сите криптирани информации што датираат од последната сигурносна копија може да се изгубат, дури и ако се плати откуп. Заедно со првично заразениот систем за информатичка технологија, ова може да влијае врз централно зачувување информации до кои пристапуваат повеќе системи за информатичка технологија.

4.26.4 Мерки

Употреба на системи за редундантна низа на независни дискови (RAID)

Организацијата мора да дефинира дали системот за редундантна низа на независни дискови (RAID) треба да се користи на сервер за датотеки. Секоја одлука против воспоставување односно користење на таков систем мора транспарентно да се документира. Ако треба да се користи систем за RAID, организацијата мора да одлучи за следното:

- кое ниво на редундантна низа на независни дискови (RAID) треба да се користи,
- колку време ќе биде дозволено за процес на обнова на RAID,
- дали да се користи софтверска или хардверска RAID низа. Во RAID треба да има достапни резервни хард-дискови.

Употреба на антивирусни програми

Сите податоци мора да се скенираат за присуство на злонамерен софтвер со програма за заштита од вируси пред истите да се зачуваат на сервер за датотеки.

Планирање на сервери за датотеки

Пред организацијата да воведо еден или повеќе сервери за датотеки, треба да одлучи за што ќе се користат серверите за датотеки и кои информации ќе се обработуваат на нив. Организацијата треба да ја испланира секоја функција на серверот за датотеки што ќе се користи, вклучително и неговите безбедносни аспекти. Персоналните компјутери не смеат да се користат како сервери за датотеки.

Просторот за зачувување податоци на серверот за датотеки мора да биде со соодветна големина и треба да се има на располагање и доволно резерви за зачувување. Притоа, треба да се користи само масовно зачувување кое е дизајнирано за континуирано работење. Брзината и поврзувањата на масовното зачувување мора да бидат соодветни за неговата намена.

Набавување сервер за датотеки и избор на услуга

Организацијата треба да избере соодветен софтвер за сервер за датотеки. Услугата за сервер на датотеки треба да ја поддржува намената на серверот за датотеки, на пример, интеграција на мрежни дискови на клиенти, прием и пренос на мултимедијална содржина, пренос на слики за подигање од системи за информатичка технологија без диск или едноставни преноси на датотеки преку протокол за пренос на датотеки (FTP). При набавување сервер за датотеки, организацијата треба да ги има предвид ефикасноста, капацитетот за чување, ширината на опсег и бројот на лица што ќе го користат.

Избор на систем за датотеки

Организацијата треба да подготви список со барања и да го користи како основа за евалуација на системите за датотеки на различни сервери за датотеки. Избраниот систем за датотеки треба да ги исполнува стандардите на самата организација. Системот за датотеки треба да обезбеди и функција за водење евиденција за секој пристап. Покрај тоа, треба да се има и механизам што спречува неколку корисници или апликации да пристапат до датотеката со овластувања за пишување во исто време.

Структурирано зачувување податоци

Организацијата треба да ја прецизира структурата за зачувување податоци. Корисниците редовно треба да добиваат информации за барањата за структурирано зачувување податоци. Датотеките треба структурирано да се зачуваат само на сервер за датотеки. Видовите податоци што можат да се зачуваат локално и оние што можат да се чуваат на серверот за датотеки, треба да бидат наведени во писмена форма. Програмските и работните датотеки треба да се зачувуваат во посебни директориуми. Организацијата треба редовно да ја проверува усогласеноста со барањата за структурирано зачувување податоци.

Безбедно управување со зачувувањето на податоци

Организацијата треба редовно да проверува дали масовното зачувување на серверите за датотеки сè уште функционира според планираното. На располагање треба да има соодветна сигурносна копија за зачувување. Доколку е воспоставена хиерархија за складирање (примарно, секундарно и терциерно зачувување), треба да се користи (делумно) автоматизирано управување со зачувувањето. Ако податоците се дистрибуираат автоматски, правилното функционирање на користениот метод на дистрибуција редовно треба да се проверува рачно. Како минимален критериум, треба да се евидентираат неовластени обиди за пристап до датотеки и промени во правата за пристап.

Користење на ограничувања за зачувување

Организацијата треба да размисли за поставување ограничувања (квоти) на простор за зачувување податоци за поединечни корисници, доколку има повеќе корисници на серверот за датотеки. Како алтернатива, треба да се користат механизми на датотеката или оперативниот систем, кои ги предупредуваат корисниците или само даваат привилегии за пишување на системскиот администратор доколку капацитетот на хард дискот достигне одредено ниво.

Користење правила за исправка на грешки

Организацијата треба да користи систем за датотеки за откривање или исправка на грешки. За таа цел треба да се обезбеди доволно простор за зачувување. Организацијата треба да има предвид дека, во зависност од користениот метод, грешките може да се откријат само со одредена веројатност и може да се отстранат само во ограничен обем.

4.26.5 Напредни мерки

Криптирање на податоци

Уредите за масовно зачувување податоци на серверот за датотеки треба да бидат криптирани на ниво на систем за датотеки или хардвер. Доколку се користи хардверско криптирање, треба да се користат производи со сертифицирана функција за криптирање. Организацијата треба да обезбеди дека програмата за заштита од вируси што се користи, може да скенира криптирани податоци за злонамерен софтвер.

Копирање помеѓу локации

За сервери за датотеки со голема достапност, податоците треба да се копираат соодветно на неколку уреди за масовно зачувување податоци. Податоците треба да се копираат и помеѓу независни сервери за датотеки што се наоѓаат на независни локации. За таа цел, организацијата треба да избере соодветен механизам за копирање и треба да се користат и да се управуваат доволно прецизни временски услуги за да може копијата да функционира како што е планирано.

Сервер за датотеки - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.39	Злонамерен софтвер
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.27 Општ клиент

4.27.1 Вовед

Терминот „општ клиент“ се однесува на систем за информатичка технологија што работи на кој било оперативен систем што овозможува раздвојување на корисниците и не се користи за давање серверски услуги и притоа треба да биде можно да се конфигурира најмалку барем еден администратор и корисничка околина на клиентот. Системот за информатичка технологија по правило има дискови и опции за поврзување за надворешни и преносливи медиуми за чување податоци, дополнителни интерфејси за размена на податоци и други периферни уреди. Вообичаено, системот за информатичка технологија од овој вид е интегриран во мрежа клиент сервер. Системот за информатичка технологија може да биде, на пример, компјутер со или без хард диск или мобилен или статичен уред, но исто така и работна станица на Linux или Apple Mac.

4.27.2 Цел

Целта е да се опише на кој начин да се заштитат информациите што се креираат, читаат, обработуваат, зачувуваат или испраќаат на кој било тип клиент, без оглед на оперативниот систем што се користи.

4.27.3 Закани

Злонамерен софтвер

Злонамерниот софтвер е развиен за да се извршат несакани и злонамерни функции на системите за информатичка технологија. Во повеќето случаи, тој станува активен без корисниците да се согласат или да бидат свесни за тоа. Во зависност од неговата форма, злонамерниот софтвер може да му обезбеди на напаѓачот големи опции за комуникација и контрола со голем број различни функции. Меѓу другото, може конкретно да се користи за читање лозинки, далечинска контрола на системи за информатичка технологија, оневозможување заштитен софтвер и кражба или криптирање податоци.

Клиентите се особено ранливи на злонамерниот софтвер. Корисниците директно управуваат со нив и затоа клиентите често се портата за злонамерна содржина од секаков вид. Доколку корисниците посетуваат злонамерни (малициозни) веб страници, отвораат електронска пошта со злонамерна содржина од приватни сметки (private account) или копираат злонамерен софтвер преку локални медиуми за зачувување податоци на нивните клиенти, злонамерниот софтвер може да се шири преку клиентите во мрежата на организацијата. На овој начин, често може да се заобиколат централните заштитни механизми, како што е заштитата од вируси на датотека или сервер за е-пошта.

Губење податоци поради локално зачувување податоци

И покрај редовните препораки, многу корисници зачувуваат важни податоци само локално. На пример, податоците често се складираат во локални директориуми на корисници наместо на централен сервер за датотеки. И е-пошта често се архивира само локално. Податоците потоа може лесно да се изгубат, на пример, во случај на хардверски дефекти. Ако податоците што се важни за организацијата се уништени или фалсификувани, деловните процеси може да се одложат или дури и целосно да се спречат. По правило, губењето на зачуваните податоци може да доведе до непродуктивно време и дополнителни трошоци за обновување на податоците, а особено до долгорочни последици какви што се губење на довербата меѓу корисниците на неговите услуги и партнерите или негативен јавен углед. Во екстремни случаи, директната и индиректната штета како последица на губењето на податоците може да го загрози постоењето на организацијата. Покрај тоа, ако важните податоци се чуваат само локално, другите корисници не можат да пристапат до нив, на пример, ако некој заменува вработен кој е болен или е на одмор. Дури и кога се почитуваат основните спецификации за централно зачувување, сепак, често се прават дополнителни локални копии на централно зачувани податоци. Покрај неконзистентните верзии на податоци, ова често води до тоа што податоците се бришат набрзина или не се бришат како што треба.

Хардверски дефекти во системите на клиентот

За разлика од случајот со централните системи за информатичка технологија какви што се серверите, корисниците на клиентот работат директно на нивните крајни уреди. Како резултат на тоа, тие може да ги оштетат своите клиенти намерно или ненамерно. На пример, тие би можеле да ги удрат системите за информатичка технологија што се оставени на подот, да се сопнат преку кабли и да ги оштетат интерфејсите или да истурат течности на уредите. Ако не е достапна брза замена, корисникот нема да може да работи со системот за информатичка технологија додека не завршат поправките. Ако мобилниот уред како што е лаптопот откаже додека корисникот е во движење, честопати корисникот може да продолжи да работи само откако ќе се врати во организацијата.

Неовластена употреба на информатичка технологија

Намената на идентификацијата и на автентикацијата на корисниците е да се спречи неовластено користење на клиентот. Меѓутоа, неовластено може да се користат и системи за информатичка технологија на кои од корисниците се бара да се идентификуваат и да извршат автентикација преку корисничка идентификација и лозинки, доколку напаѓачот успее да ги добие или да ги погоди податоците за пристап. Ако не е активирано заклучување на екранот, можно е и клиентот да се користи на неовластен начин, дури и за време на кратко отсуство.

Инсталација на непотребни компоненти и апликации на оперативниот систем

При инсталирање оперативен систем, главно постои опција да се отстрани софтвер што е по избор. Софтверот исто така редовно се инсталира и се тестира за време на активните операции. Секоја дополнителна апликација го зголемува оптоварувањето на компјутерот и меморијата на клиентот, заедно со веројатноста за појава на недостатоци. Софтверот што не е потребен, често не подложува на редовно управување со софтверски поправки, што значи дека дури и познатите недостатоци не се поправаат навремено. Ова им овозможува на напаѓачите да ги искористат недостатоците што се познати долго време.

Прислушување простории со помош на микрофони и камери

Многу клиенти се опремени со микрофон и камера. Начелно, овие уреди може да се активираат и да се користат од секој што има соодветни права за пристап, вклучително и од надворешни лица во случај на мрежни системи. Ако овие права не се внимателно доделени, неовластени лица можат да манипулираат со микрофонот или со камерата за да прислушуваат простории или да снимаат состаноци незабележано преку интернет. Ова вклучува и интелигентни лични асистенти (IPA) или гласовни асистенти, кои постојано ја слушаат околината и извршуваат одредени функции, какви што се пуштање музика, повикување контакти, контролирање на осветлувањето или менување на собната температура, кога слушаат кодирани зборови што зависат од уредот. Доколку разговорите се пренесуваат на трети страни (на пример, преку IPA), тие би можеле да бидат пресретнати од неовластени лица. Снимените разговори може и да се зачуваат и да се обработуваат понатаму од операторите на интелигентниот личен асистент на подолг временски период.

Неправилно администрирање или употреба на уреди и системи

Современите оперативни системи на клиентите се многу сложени. Затоа, погрешната конфигурација на компонентите може значително да ја загрози безбедноста, така што системите за информатичка технологија ќе функционираат неправилно или ќе бидат компромитирани. По правило, секој интерфејс на системот за информатичка технологија не само што дава можност за овластено користење одредени услуги на системот за информатичка технологија, туку исто така создава ризик за пристап до системот за информатичка технологија без овластување. На пример, ако неправилно конфигурираните механизми за автентикација овозможуваат да се добијат кориснички идентификации и соодветни лозинки, апликациите или системите за информатичка технологија може неовластено да се користат.

Неправилната или неточната употреба на уреди, системи и апликации може да ја загрози безбедноста, особено ако се занемарат или се заобиколат постојните безбедносни заштитни мерки на организацијата. Може да се случат безбедносни инциденти, на пример, кога правата за пристап се даваат генерално, лозинките може лесно да се погодат, медиумите за зачувување податоци што содржат сигурносни копии се несоодветно заштитени или работните станици не се заклучени за време на привремени периоди на отсуство. Друга можна последица од неправилното работење на системите за информатичка технологија или на апликациите, вклучува случајно бришење или менување на податоците. Исто така, можно е доверливите информации да се најдат во рацете на трети лица, на пример, доколку правата за пристап се погрешно поставени.

4.27.4 Мерки

Безбедно овластување корисник

За да користат клиенти, соодветниот систем за информатичка технологија мора да изврши автентикација на корисниците. Корисниците мора да користат заклучување на екранот кога ги оставаат своите клиенти да работат без надзор. Заклучувањето на екранот треба да се активира автоматски доколку корисникот не презел никакво дејство во текот на одреден временски период. Успешната автентикација на корисникот мора да биде единствениот начин да се оневозможи заклучувањето на екранот. Корисниците треба да имаат обврска да се одјават од системите за информатичка технологија и од апликациите откако ќе ги завршат своите задачи.

Активирање на механизмите за автоматско ажурирање

Мора да се активираат механизми за автоматско ажурирање, освен ако не се користат други механизми за ажурирање, какви што се редовно рачно одржување или централен систем за дистрибуција на софтвер. Ако може да се одреди временски интервал за механизмите за автоматско ажурирање, треба да има автоматско пребарување за ажурирања најмалку на дневна основа и тие треба да се инсталираат кога ќе се најдат.

Користење заштита од злонамерен софтвер/програми за заштита на крајна точка

Во зависност од инсталираниот оперативен систем и другите заштитни механизми на даден клиент, мора да се провери дали треба да се користат програми за заштита од злонамерен софтвер. Заштитните програми на клиентите мора да се конфигурираат така што корисниците не можат да ги оневозможат таквите програми или да направат какви било безбедносни промени во нивните поставки.

Програмите за заштита мора да бараат присуство на злонамерен софтвер кога се разменуваат или пренесуваат датотеки. Сите податоци за клиентите мора редовно да се проверуваат за присуство на злонамерен софтвер. Ако клиентот е заразен, мора да се испита во режим без интернет за да се утврди, на пример, дали откриениот злонамерен софтвер веќе собрал доверливи податоци, оневозможил какви било заштитни функции или преземал каков било код од интернет.

Заштита на постапката за стартување (boot process)

Постапката за стартување (процес на подигање) системи за информатичка технологија мора да биде заштитена од манипулации. Мора да се дефинира медиумот што може да се користи за подигање системи за информатичка технологија. Треба да се донесе одлука дали и како процесот на подигање ќе биде заштитен криптографски. Мора да се обезбеди дека само администраторите можат да ги подигнуваат клиентите од стандардниот диск или од надворешен медиум за чување податоци. Можноста за подигање на системите за информатичка технологија од пренослив или од надворешен медиум за чување податоци мора да биде ограничена на администраторите. Можноста за промена на поставките за конфигурација на процесите за подигање мора да биде ограничена и на администраторите. Сите неискористени функции во фирмверот мора да се оневозможат.

Користење функции за „облак“ и мрежни функции

Употребата на функции за „облак“ и мрежни функции на оперативните системи на клиентот мора да биде ограничена на оние што се апсолутно потребни. Треба да се документираат неопходните функции за „облак“ и мрежните функции. Мора да се проверат соодветните поставки на оперативниот систем во однос на усогласеноста со организациските спецификации за заштита на податоци и безбедност, како и да се конфигурираат според соодветните рестрикции, инаку во спротивно, таквите функции мора да се оневозможат.

Дефинирање безбедносна политика за клиентите

Врз основа на општата безбедносна политика на организацијата, треба да се подготви и политика за барањата за општите клиенти. Политиката треба да им биде позната на сите корисници и на сите лица што учествуваат во набавките и во работењето на клиентите и да биде составен дел од нивната работа. Имплементацијата на барањата на политиката треба да се проверува во редовни интервали. Резултатите треба транспарентно да се документираат.

Планирање на користењето клиенти

Однапред треба да се испланира каде и како да се користат клиентите. Ова планирање не треба да се однесува на аспектите што обично се поврзани директно со безбедноста на информациите, туку и на оперативните аспекти што наметнуваат барања во областа на безбедноста. Сите одлуки што се донесени во фазата на планирање, треба да се документираат така што секогаш ќе бидат јасни во иднина.

Набавка на клиенти

Пред да се набават клиентите, треба да се состави список со барања што може да се користи за евалуација на производителите што се достапни на пазарот. Од производителите на информатичка технологија и оперативни системи треба да се очекува веднаш да обезбедат софтверски поправки за недостатоци во текот на планираното времетраење на употреба. Системите што треба да се набават треба да имаат интерфејси за конфигурација на фирмверот за UEFI SecureBoot и за сигурен модул за платформа (TPM ако е достапен), што овозможува контрола од страна на сопственикот (организацијата) и со тоа го олеснува самоуправуваното работење на SecureBoot и на TPM.

Пристап до средина за извршување со ненабљудувано извршување на кодот

Пристап до средина за извршување со ненабљудувано извршување на кодот (подрачја за зачувување што се специјално обезбедени од оперативниот систем, области на фирмверот итн.) треба да им се дава само на корисници со администраторски права. Соодветните поставки во вградениот оперативен систем (BIOS) или фирмверот UEFI, треба да бидат заштитени од неовластени промени со лозинка. Ако контролата врз соодветните функции е делегирана на оперативниот систем, можноста за пристап до функциите таму треба да биде ограничена на корисници со администраторски овластувања.

Ажурирања и софтверски поправки за фирмвер, оперативни системи и апликации

Треба да се избегнуваат оперативни системи што се ажурираат преку модел со континуирана испорака, односно треба да се избераат и да се инсталираат само апликативни програми за кои се нуди поддршка. Не смее да се користат оперативни системи, апликативни програми и фирмвер за кои не се нудат редовни безбедносни ажурирања.

Безбедна инсталација и конфигурација на клиенти

Треба да се наведат компонентите на оперативниот систем, специјализираните апликации и други алатки што треба да се инсталираат. Инсталацијата и конфигурацијата на системите за информатичка технологија треба да ги вршат само овластени лица (администратори или даватели на услуги обврзани со договор) според дефиниран процес на инсталација во околина за инсталација. По завршувањето на инсталацијата и конфигурацијата, треба да се проверат основните поставки. Под услов инсталацијата и конфигурацијата да ги исполнуваат барањата на безбедносната политика, клиентите потоа треба да се стават во функција во соодветната производна околина. Сите чекори за инсталација и за конфигурација треба да се документираат така што да може да бидат разбрани и повторени од компетентно трето лице.

Оневозможување и отстранување непотребни компоненти и идентификатори

Компонентите, апликациите и другите алатки на фирмверот и на оперативниот систем што се инсталирани и активирани на клиенти, треба да се проверат по инсталацијата. Непотребните модули, програми, услуги, задачи и функции на фирмверот (како што е далечинско одржување) треба да се оневозможат или да се отстранат. Исто така, треба да се отстранат и непотребните околиниски за извршување, јазиците за преведување и компилаторите (compilers). Треба да се оневозможат или да се избришат непотребните кориснички идентификации. Треба да се оневозможат непотребните интерфејси и хардверот на системот за информатичка технологија (како што се веб камерите). Треба да се спречи повторно активирање на овие компоненти. Одлуките што се донесени во овој поглед треба јасно и да се документираат.

Користење криптирана комуникација

Комуникацијата треба да се заштити со криптирање секогаш кога тоа е можно. Клиентите треба да користат криптографски алгоритми и должини на клучеви што соодветствуваат на најсовремените технолошки достигнувања и ги исполнуваат безбедносните барања на организацијата. Новите сертификати од издавачите на сертификати треба да се користат само откако ќе се проверат нивните отпечатоци.

Заштита на процесот на администрирање за клиентите

Треба да се преземат соодветни безбедносни мерки врз основа на тоа дали клиентите се администрираат локално или преку мрежа. Процедурите што се користат за администрирање, треба да се усогласат со спецификациите на безбедносната политика на организацијата.

Спречување неовластена употреба на компјутерски микрофони и камери

Пристапот до микрофонот и до камерата на клиентот треба да им биде овозможен само на корисниците додека тие работат локално на соодветниот систем за информатичка технологија. Доколку не се користат микрофонот или камерата и треба да се спречи нивна злоупотреба, треба да се исклучат, да се покрие (само камерата), да се оневозможи или физички да се исклучи од соодветниот уред секогаш кога е можно. Организацијата треба да има донесено правила како да се користат камерите и микрофоните на клиентите и како се доделуваат правата за пристап.

Преференции за услуги за клиент-сервер

Доколку е можно, треба да се користат наменски серверски услуги за размена на информации и да се избегнуваат директни врски помеѓу клиентите. Ако тоа не е можно, треба да се прецизира кои услуги од клиент до клиент (често се нарекуваат и услуги од јазол до јазол - P2P) може да се користат и кои информации може да се разменуваат преку нив. Доколку е потребно, корисниците треба да се обучат за користење на таквите услуги. Директните врски помеѓу клиентите треба да се ограничат на локалната мрежа LAN. Протоколите за автоматско откривање треба да се ограничат само на потребните протоколи.

Постапување со надворешни и со преносливи медиуми

Интерфејсите до надворешните мрежи треба да бидат достапни само во ограничена мера. Треба да биде забрането поврзување на неовластени уреди или на пренослив медиум со клиенти. Главно, клиентите треба да бидат спречени од пристап до пренослив медиум од недоверливи извори. Неовластено извршување програми на или од надворешен медиум за чување податоци, треба технички да се спречи. Треба да се спречи и копирање неовластени податоци од клиенти преку преносливи дискови или надворешни интерфејси.

Заштита од искористување недостатоци во апликациите

За да се отежне искористувањето на недостатоците, треба да се активираат ASLR и DEP/NX во оперативните системи, а апликациите треба да ги користат ваквите безбедносни опции. Треба да се активираат безбедносните функции на јадрата (kernels) и стандардните библиотеки (standard libraries), како што е заштита од линеарна нефлексибилна структура на податоци и хиерархиска флексибилна структура на податоци.

Уредно отстранување клиенти

При отстранување клиент, треба да се обезбеди дека нема изгубени податоци и не остануваат сензитивни податоци. Организацијата треба да има преглед на податоците што се зачувани на системите за информатичка технологија, заедно со соодветните локации. Треба да се креира листа за проверка што може да се пополни при отстранување систем за информатичка технологија. Оваа листа најмалку треба да вклучува аспекти за создавање сигурносна копија на податоците што сè уште се потребни и последователно безбедно бришење на сите податоци.

Локална безбедносна политика за клиенти

Сите поставки што се значајни за безбедноста треба да се конфигурираат, да се тестираат и редовно да се проверуваат по потреба. За таа цел, треба да се конфигурираат безбедносни политики што ги земаат предвид препораките на соодветниот производител на оперативен систем и стандардното однесување на клиентот, под услов ова однесување да не е спротивно на другите барања за безбедноста на информатичката технологија или на организацијата. Одлуките што се донесени во овој поглед, треба да се документираат и да се оправдаат. Безбедносните политики треба да се дефинираат во секој случај, дури и ако стандардното однесување на клиентот не се промени.

Управување со безбедносната политика на клиентите

Сите поставки на клиентот треба да се администрираат со користење систем за управување и да се конфигурираат според идентификуваните потреби за заштита и достапните внатрешни политики. Промените на конфигурацијата треба да се документираат, да се оправдаат и да се координираат со лицата за управување со безбедноста за да можат брзо да се извршат и централизирано да се дистрибуираат. Воедно, треба да биде можно постојано да се следи статусот на безбедносните конфигурации.

4.27.5 Напредни мерки

Криптирање на клиенти

Ако доверливите информации се зачувани на клиентите, треба да се криптираат најмалку сензитивните датотеки и избраните делови на системот за датотеки или уште подобро, сите медиуми за чување податоци. За ова треба да се развие посебен концепт и треба да се внимава при документирање на деталите за конфигурацијата. Во овој контекст, треба да се регулира автентикацијата (со помош на лозинки, PIN-кодови, токени итн.), чувањето на информациите за сигурносните копии, дисковите што треба да се криптираат и овластувањата за користење на некриптирани медиуми. Пристапот до клучниот материјал што се користи мора да биде соодветно заштитен. Корисниците треба да бидат информирани за чекорите што треба да ги преземат доколку ги загубат ресурсите за автентикација.

Следење на системот и на клиентот

Клиентите треба да се интегрираат во соодветен концепт за следење на системот што континуирано ги следи статусот и функционалноста на нивниот систем, истовремено известувајќи за условите за грешка и прагот на било какви непочитувања од страна на соодветниот оперативен кадар.

Поставување референтна околина за клиенти

Организацијата треба да постави референтна инсталација за клиенти во која основните конфигурации и сите конфигурациски промени, ажурирања и софтверски поправки може да се тестираат пред да се инсталираат на клиентите. Треба да се креираат листи за проверки за различни вообичаени случаи што се тестираат и кои често се повторуваат, при што листите треба да се обработуваат колку што е можно повеќе автоматски за време на тестирањата. Случаите што се тестираат треба да ги земат предвид и корисникот и клиентот. Дополнително, сите тестови треба да се документираат така што подоцна ќе можат да се реконструираат.

Конфигурирање филтри за локални пакети

Покрај користените централни безбедносни порти, треба да се користат и локални филтри за пакети кај сите клиенти. Стратегијата за т.н. бела листа треба да се избере како стратегија за имплементација на филтер за пакети врз основа на потребната мрежна комуникација на организацијата.

Употреба на дополнителни заштитни мерки за заштита од искористување

Организацијата треба да имплементира дополнителни заштитни мерки за клиентите како јасна заштита од искористувања на недостатоци на системот. Доколку неопходните безбедносни заштитни мерки не можат да се имплементираат преку функциите на оперативниот систем, тогаш треба да се имплементираат дополнителни соодветни безбедносни заштитни мерки. Доколку не е можно да се спроведат одржливи заштитни мерки, треба да се имплементираат други соодветни (по правило организациски) безбедносни заштитни мерки.

Наведување во т.н. бела листа на апликации

Организацијата треба да користи наведување во т.н. бела листа на апликации за да обезбеди дека може да се извршуваат само изречно овластени програми и скрипти. Правилата треба да се постават колку што е можно порестриктивно. Доколку не е можно изречно одредување на патеките и хашовите, како алтернатива треба да се користат правила засновани на сертификати или патека.

Инкапсулација на апликации и компоненти на оперативниот систем што се од клучно значење за безбедноста

Апликациите и компонентите на оперативниот систем (какви што се автентикација или потврда на сертификатот) треба да бидат специјално инкапсулирани или изолирани од други апликации и компоненти на оперативниот систем, со цел да се спречи напаѓачот да пристапи до оперативниот систем или до други апликации, како и да се спречи пристап од оперативниот систем до особено сензитивни датотеки. Посебно внимание треба да им се посвети на апликациите што се од клучно значење за безбедноста, кои работат со податоци од несигурни извори (на пример, веб прелистувачи и апликации за канцелариска комуникација).

Активно администрирање коренски (root) сертификати

Како дел од набавката и инсталацијата на клиенти, треба да се документираат коренските сертификати што се потребни за нивното работење. На клиентите треба да бидат присутни само претходно документираните коренски сертификати што се потребни за работа. Треба да се вршат редовни проверки за тоа дали постојните коренски сертификати сè уште се во согласност со барањата на организацијата. Во овие проверки треба да бидат вклучени сите сертификати што се достапни на системот за информатичка технологија (на пример, сертификати за унифициран проширен интерфејс на фирмверот – UEFI, сертификати на веб прелистувачи).

Самоуправувана употреба на сигурносни системи за подигање (SecureBoot and TPM)

На системи што се компатибилни со унифициран проширен интерфејс на фирмверот – UEFI, управувачот за подигање, јадрото и сите потребни компоненти на фирмверот треба да бидат потпишани со самоконтролиран клучен материјал, а секој клучен материјал што не е потребен треба да се отстрани. Ако сигурниот модул за платформа (TPM) не е потребен, треба да се оневозможи.

Употреба на повеќефакторска автентикација

Организацијата треба да воспостави безбедна автентикација што вклучува повеќе различни фактори (знаење, поседување, својство) за локална најава на клиенти (на пример, користење лозинка со чип картичка или токен).

Интеграција во планирањето за итни состојби

Организацијата треба да ги земе предвид клиентите во процесот на управување со обезбедување на континуитетот на деловното работење. На клиентите треба да им се даде приоритет за обновување на услугите во однос на деловните процеси за кои се потребни. Треба да се спроведат соодветни заштитни мерки за континуитет на деловното работење со изготвување планови за обновување, генерирање медиум за подигање за обновување на системот и безбедно зачувување лозинки и криптографски клучеви.

Стабилно и непрекинато напојување

Клиентите треба да бидат поврзани на непрекинато напојување (UPS). Непрекинатото напојување треба да има доволен капацитет во однос на неговата излезна моќност и времето на резервна заштита. Клиентите треба да бидат заштитени од пренапон.

Оперативна документација

Извршувањето на оперативните задачи на клиенти или на групи клиенти, треба транспарентно да се документира во однос на тоа кој што и кога направил. Конкретно, документацијата треба да содржи транспарентни информации за промените во конфигурацијата. Треба да се документаат и одговорностите што се од значење за безбедноста (на пример, кој е овластен да инсталира нови хард дискови). Сè што може да се документа автоматски, треба да се документа автоматски. Документацијата треба да биде заштитена од неовластен пристап и губење. Безбедносните аспекти треба транспарентно да се објаснат и да се објават во организацијата.

Користење квоти за локални медиуми

Организацијата треба да размисли за поставување квоти што го ограничуваат просторот што се користи на локалните дискови. Како алтернатива, треба да се користат механизми на односната датотека или оперативен систем, кои ги предупредуваат корисниците доколку капацитетот на хард дискот достигне одредено ниво или само му даваат привилегии за пишување на системскиот администратор.

Проширена евиденција на записите

Однесувањето на клиентот што не е директно поврзано со безбедноста, исто така треба да се евидентира и да се анализира веднаш (автоматски) за да се откријат тајните активности на напаѓачите.

Општ клиент - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурен извор
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.28	Софтверски недостатоци или грешки
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.36	Кражба на идентитет
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.43	Вметнување пораки
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.28 Клиенти на Windows 10

4.28.1 Вовед

Во Windows 10, Microsoft го има приспособено својот оперативен систем за Windows клиент на нова корпоративна стратегија. Конкретно, основната филозофија исто така се има променето, оддалечувајќи се од претходниот принцип на „локален оперативен систем“ на услуга („Windows како услуга - Windows as a Service“). Ова значи дека покрај неговите претходни функции, оперативниот систем содржи и дополнителни апликации (особено, засновани на „облак“) и затоа зависи од блиската интеграција со серверската инфраструктура на производителот. Важните нови аспекти во споредба со претходните верзии на Windows, пред сè, вклучуваат интегрална и делумно неконтролирана размена на податоци помеѓу клиентите и инфраструктурата на производителот, како и зголемено надворешно добавување на основните компоненти на инфраструктурите на Windows што се од клучно знаење за безбедноста (на пример, автентикација) на „облакот“. Овие иновации треба да се земат предвид пред да се користи Windows 10.

4.28.2 Цел

Целта е да се опише на кој начин да се заштитат информациите што се обработени во Windows 10, вклучително и на соодветните клиенти.

4.28.3 Закани

Злонамерен софтвер во Windows 10

Поради распространетоста на оперативните системи Windows и компатибилноста наназад што често постои помеѓу системските генерации, заканата од злонамерен софтвер и неовластени пробивања на системите за информатичка технологија е релативно висока. Злонамерниот софтвер може да има голем број функции и да му обезбеди на напаѓачот многу голем број на опции за контрола. Меѓу другите намени, тој може да се користи за добивање специфични лозинки, системи за далечинско управување, оневозможување заштитен софтвер и прибирање податоци без овластување. Штетата предизвикана од губење или оштетување информации или апликации е особено сериозна за организацијата. Сепак, штетата во однос на угледот и финансите што може да настане од злонамерниот софтвер, честопати исто така е сериозна.

Интегрирани функции на „облак“

Windows 10 вклучува голем број функции што се користат за зачувување и за синхронизирање податоци со користење на услугите на Microsoft („услуги на облак“). Ова резултира со ризик овие услуги да се користат, без разлика дали несвесно или невнимателно, за податоци што би можеле да бидат лични или клучни за организацијата. Истовремено, чувањето податоци кај трети лица (кои обично се наоѓаат во трети земји) може да резултира со непочитување на прописите за заштита на личните податоци. Ако корисникот се најави на нов уред со користење веќе активирана сметка на Microsoft, услугите за „облак“ на Microsoft што ги користи корисникот ќе се постават автоматски на уредот. Така, податоците на организацијата може случајно да се синхронизираат со приватните уреди на вработените. Друг пример е кога стандардната поставка на Windows 10 е директно да се обезбедат клучевите за обновување на BitLocker во „облакот“ со користење на сметката на Microsoft, што претставува обезбедување сензитивни криптографски тајни на трети лица.

Нарушување на функциите на софтверот поради проблеми со компатибилноста

Софтверот што работи успешно во претходните верзии на оперативниот систем нема со сигурност да работи со тековната верзија на Windows 10. Можни причини за ова може да вклучуваат нови безбедносни функции или својства на оперативниот систем, како и прекинување на функциите или на услугите. Како резултат на тоа, употребата на одреден софтвер може да биде ограничена или невозможна. Примери за овозможени безбедносни функции што може да бидат причина за проблеми со компатибилноста со новите верзии на Windows вклучуваат контрола на корисничка сметка (UAC) или, со 64-битни верзии на оперативниот систем, Kernel Patch Guard. Покрај тоа, може да бидат неопходни потпишани драјвери, но тие се недостапни за постари уреди.

Функции на телеметрија (telemetry) на Windows 10

Windows 10 стандардно испраќа дијагностички податоци до Microsoft. Покрај тоа, Microsoft може конкретно да бара информации од клиентот преку услугата за телеметрија интегрирана во Windows 10. На телеметриското ниво „Full“, што е стандардно ниво на Windows 10 Home и Pro, ова вклучува, на пример, пристап до регистарот и извршување одредени дијагностички алатки на клиентот. Постои ризик дијагностичките или телеметриските податоци да содржат сензитивни информации што може да се пренесат на трети лица.

4.28.4 Мерки

Планирање на користењето услуги за „облак“ за Windows 10

Бидејќи уредите засновани на Windows 10 се тесно испреплетени со услугите за „облак“ на Microsoft, мора да биде стратегиски определено пред нивната употреба кои од нив би вклучувале услуги за „облак“, дали треба или може да се користат и до кој степен.

Избор и набавка на соодветна верзија на Windows 10

Функционалниот опсег и функционалните промени што се вклучени во дадена верзија на Windows 10 мора да се изберат врз основа на идентификуваните потреби за заштита и целта на употребата. Во процесот на избор мора да се има предвид можноста од примена на потребните заштитни мерки. Врз основа на резултатите од овој преглед, мора да се прошири воспоставениот процес на набавка за да го вклучи изборот на соодветен модел на лиценца и „гранки на услуги“.

Телеметрија и поставки за приватност во Windows 10

Услугите за телеметрија пренесуваат дијагностички податоци и податоци за користење што производителот ги поврзува со уникатни карактеристики, со цел да се овозможи решавање проблеми, подобрување на услугите и на производите и идентификација. Тие можат значително да се намалат само со поставување на нивото на телеметрија на 0 (Безбедност). Ако оваа поставка не се имплементира ефективно, мора да се преземат соодветни заштитни мерки (какви што се мерките на мрежно ниво) за да се обезбеди дека овие податоци не се пренесуваат до производителот.

Заштита од злонамерен софтвер во Windows 10

Освен ако не се имплементирани еквивалентни или повисоки заштитни мерки (како што е наведување во „белата листа“ на апликации) за заштита на систем за информатичка технологија од заразување со злонамерен софтвер, мора да се распореди специјализирана компонента за заштита од злонамерен софтвер на клиентите на Windows 10.

Интегрирање мрежни сметки (accounts) во оперативниот систем

Најавувањето во системот и доменот мора да биде можно само со користење сметка на самоуправувана услуга на директориум. Можноста за најава со користење локални сметки, треба да се задржи само за администраторите. Не смее да се користат сметки за мрежна најава преку интернет (на пример, сметки на Microsoft или сметки од други даватели на системи за управување со идентитетот) бидејќи со тоа се пренесуваат лични податоци до системите на производителот.

Безбедна централна автентикација на Windows мрежи

За централна автентикација треба да се користи само Kerberos. Групната политика треба да спречува употреба на постари протоколи. Ако ова не е можно, NTLMv2 мора да се имплементира како алтернатива. Автентикацијата со помош на LAN Manager и NTLMv1 не смее да биде дозволена во рамките на организацијата или производните оперативни средини. Употребените криптографски механизми треба да се конфигурираат и да се документираат според идентификуваните потреби за заштита и врз основа на важечките внатрешни правила во организацијата. Отстапувањето на поставките треба да се оправда и да се координира со кадарот за управување со безбедност.

Заштита на информациите за најава во Windows 10

Доколку верзијата на Windows 10 во организацијата е инсталирана директно (машински) на хардверски систем, треба да се овозможи виртуелен безбеден режим (VSM). Покрај тоа, треба да се овозможи Windows Defender Credential Guard за да спречи напади врз токени за автентикација и хашовите што се зачувани во системот. Ако ова не е можно, треба да се активира заштитата на акредитиви (Protected Process Light, PPL) на локалниот безбедносен орган (LSA). Треба да бидат забранети мрежни најави од локални сметки.

Овластување за датотеки и споделување во Windows 10

Пристапот до датотеки и папки на локален систем и до мрежни споделувања треба да се конфигурира во согласност со концептот за овластување и пристап. Треба да се земат предвид и стандардните администраторски одобренија на системот. Правата за пристап за пишување на корисниците треба да се ограничат на дефинирана област во системот за датотеки. Конкретно, на корисниците не треба да им се даваат права за пристап за пишување во папките на оперативниот систем или на инсталираните апликации.

Користење на функцијата SmartScreen

Функцијата SmartScreen, која ги проверува датотеките и веб содржините што се преземени од интернет и пренесува лични податоци на Microsoft во процесот под одредени околности, треба да биде оневозможена.

Користење на гласовниот асистент Cortana

Cortana треба да се оневозможи.

Користење механизми за синхронизација во Windows 10

Синхронизацијата на корисничките податоци со услугите за „облак“ на Microsoft и процесот на споделување лозинки за WLAN, треба да бидат целосно оневозможени.

Поврзување на Windows 10 со Microsoft Store

Употребата на Microsoft Store треба да се провери и да се процени во однос на нејзината компатибилност со прописите за заштита на личните податоци и прописите за безбедност на организацијата. Општата инсталација на апликациите во Windows 10 не зависи од поврзувањето со Microsoft Store, па затоа треба да се оневозможи ако не е потребна.

Нема зачувување податоци за автоматска најава

Организацијата не треба да дозволи чување лозинки, сертификати и други информации за автоматска најава на веб локации и на системите за информатичка технологија.

Користење далечинска поддршка на Windows

Ефектите врз конфигурацијата на локалниот заштитен сид треба да се земат предвид при планирање на процедурите за далечинска поддршка на Windows (ова не се однесува на RDP). Далечинската поддршка треба да се врши само по изречна покана. Кога се зачувува покана во датотека, датотеката треба да биде заштитена со лозинка. Во секој случај, корисникот што е моментално најавен треба да се согласи изречно за да започне сесијата. Поканата за далечинска поддршка треба да има соодветно максимално времетраење. Доколку оваа услуга не се користи, треба целосно да се оневозможи.

Безбедност при далечински пристап со користење далечински пристап до работната површина (RDP)

При планирање далечински пристап, треба да се земат предвид влијанијата врз конфигурацијата на локалниот заштитен сид. Групата корисници што се овластени за далечински пристап до работната површина (RDP) треба да биде одредена со доделување на соодветните кориснички права. Во сложени инфраструктури, треба да биде можно да се достигне целен систем за RDP само преку посреднички RDP-портал. За да се користи RDP, со проверката треба да се обезбеди дека следните погодни функции се во согласност со потребите за заштита на целиот систем:

- Користење на привремената меморија,
- Интеграција на печатачи,
- Интеграција на пренослив медиум и мрежни дискови,
- Употреба на архиви на датотеки и поврзувања со паметни картички.

Доколку не се планира користење далечински пристап до работната површина, ваквиот пристап треба да биде целосно оневозможен. Употребените криптографски протоколи и алгоритми треба да се усогласат со внатрешните спецификации на организацијата.

Употреба на контрола на корисничка сметка (UAC) за привилегирани сметки

За привилегирани сметки, конфигурациските параметри на контрола на корисничка сметка (UAC) треба да се постават со соодветна рамнотежа помеѓу можноста за лесно и практично користење од страна на корисникот и нивото на безбедност. Треба да се документираат одлуките во врска со параметрите за конфигурација што треба да се користат. Покрај тоа, поврзаната документација треба да ги вклучува сите сметки со администраторски права. Треба да се вршат редовни проверки за да се утврди дали е неопходна можност за продолжување на правата.

4.28.5 Напредни мерки

Употреба на систем за криптирање датотеки

Бидејќи системот за криптирање датотеки (EFS) ги штити клучевите што се користат со лозинките на корисничките сметки, треба да се користат безбедни лозинки. Покрај тоа, рестриктивните права за пристап треба да ги штитат датотеките што се криптирани со помош на EFS. Агентот за обновување (recovery agent) треба да ја има наменската сметка, а не администраторот. Во овој контекст, приватниот клуч на оваа сметка треба да биде заштитен и отстранет од системот. Треба да се креираат сигурносни копии на сите приватни клучеви. Кога се користи EFS со локални кориснички сметки, мемориите на локалните лозинки треба да се криптираат со помош на Syskey. Како алтернатива, може да се користи и Windows Defender Credential Guard. Корисниците треба да бидат обучени од организацијата за правилна употреба на системот за криптирање датотеки.

Користење Windows PowerShell

Датотеките PowerShell и WPS треба да ги извршуваат само администраторите. Извршувањето на PowerShell треба централно да се евидентира и треба да се следат записите. Извршувањето на скриптите на PowerShell, треба да биде ограничено со помош на командата Set Execution Policy AllSigned за да се спречи какво било случајно извршување на непотпишани скрипти.

Напредна заштита на информациите за најава во Windows 10

На системи засновани на UEFI треба да се користи SecureBoot, а при стартување на системот треба да се следи статусот на заштитениот режим за акредитиви на локалното тело за безбедност (LSA). Доколку далечинското одржување на клиентите е наменето со користење далечински пристап до работната површина (RDP), опцијата „restrictedAdmin“ за RDP треба да се користи за распоредување на Windows 10 во домени со функционално ниво 2012 R2 или повисоко.

Активирање запис за последното време на пристап

Доколку се создаде безбедносен концепт за систем за информатичка технологија кој користи Windows 10, треба да се провери дали може да се активира записот за последното време на пристап во системот на датотеки за да се олесни анализата на злоупотребата на системот. Анализата треба да ги земе предвид можните влијанија од оваа поставка, какви што се аспектите на ефикасноста или последователните ограничувања во поединечните сигурносни копии.

Постапување со функциите за далечински пристап на поврзаното корисничко искуство и телеметрија

Треба да се земе предвид дека компонентата за поврзано корисничко искуство и телеметрија (CUET) во Windows 10 е составен дел од оперативниот систем, кој покрај функцијата за телеметрија, му овозможува на Microsoft далечински пристап до локалните системи. Овој тип далечински пристап до клиентите на Windows 10 треба да се најави на мрежната страна и да се блокира, доколку е потребно.

Клиент на Windows 10 - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.39	Злонамерен софтвер
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.29 Активен директориум

4.29.1 Вовед

Активен директориум (AD) е услуга за директориум развиена од Microsoft, која беше претставена за првпат со оперативниот систем Windows 2000 Server. Врз основа на функциите за активен директориум што се достапни во Microsoft Windows 2000 Server, на услугата се додадени дополнителни клучни функции во секое издание на семејството на оперативни системи Windows Server.

Активен директориум главно се користи во мрежи со компоненти на Microsoft. Активниот директориум зачувува информации за објекти во мрежата, какви што се корисници или системи за информатичка технологија. Тоа им олеснува на корисниците и на администраторите да ги обезбедуваат, да ги организираат, да ги користат и да ги надгледуваат овие информации. Бидејќи активниот директориум е услуга за директориуми заснована на објекти, таа го олеснува администрирањето на објектите и нивните меѓусебни односи, што претставува вистинска мрежна средина. Оттука, активниот директориум обезбедува можности за централна контрола и следење за дадена мрежа.

4.29.2 Цел

Целта е да се опишат активностите кои треба да се преземат за да се обезбеди активен директориум во нормални операции во организацијата што го користи за администрирање на нејзината инфраструктура на Windows системи (клиент и сервер).

4.29.3 Закани

Несоодветно планирање на безбедносните граници

Активниот директориум генерира „шума“ (AD forest) како пакет на највисоко ниво за сите домени. „Шумата“ може да вклучува еден или повеќе објекти на пакет на домен, кои се карактеризираат со заедничка логичка структура, глобален каталог, шема и автоматски транзитни односи на доверба. Така, „шумата“ (група од повеќе дрвја) е стандардната безбедносна граница во чии рамки информациите се проследуваат во активниот директориум. Ако овие граници не се планираат свесно и структурирано, информациите може да протечат ненамерно и безбедносниот концепт на организацијата може да биде нефункционален. Како последица на тоа, може да биде неопходно да се воспостават дополнителни „шуми“ доколку се применуваат различни безбедносни барања за одредени инфраструктурни компоненти. Сепак, ова го усложнува поставувањето и управувањето во организацијата.

Прекумерни или несовесни односи на доверба

Доколку не се врши редовна проценка на доверливите односи меѓу „шумите“ и домените за да се утврди дали тие сè уште се потребни и оправдани, може да се појават проблеми со овластувањата и да протекуваат информации. Воедно, потребно е редовно да се проверува дали овие односи се правилни, особено во однос на тоа дали е навистина неопходен двонасочен однос на доверба и дали безбедносните контроли за таквите односи се доволни. Конкретно, ако филтрацијата на безбедносниот идентификатор (SID) која е стандардно активна е оневозможена, може да се појават сложени пропусти што тешко може да се разберат. Истото важи и ако се отфрли селективна автентикација за односи на доверба меѓу „шумите“.

Недостаток на безбедносни функции поради постарите оперативни системи и функционалното ниво на доменот

Секоја нова генерација на оперативниот систем Windows Server вклучува дополнителни безбедносни карактеристики и екстензии, вклучително и за активен директориум. Дополнително, стандардните поставки се побезбедни со секое ново издание. Некои од нив може да се користат откако ќе се инсталира новиот систем, а други само откако ќе се зголеми функционалното ниво на доменот или „шумата“. Ако постарите оперативни системи се користат како (примарни) контролери на домени или се користат застарени функционални нивоа на домен, не може да се користат ажурирани безбедносни функции. Ова ја зголемува заканата од несигурни стандардни поставки. Несигурно конфигурираниот домен ги загрозува информациите што се обработени во него и им олеснува на трети лица да вршат напади.

Работење на дополнителни улоги и услуги на контролери на домени

Ако други услуги се управуваат на контролер на домен покрај активниот директориум, ова го зголемува бројот на можни напади на овие компоненти на централната инфраструктура поради можни дополнителни пропусти и погрешни конфигурации. Таквите услуги може да се злоупотребат ненамерно или намерно, на пример, со цел да се копираат или да се променат информациите без овластување.

Недоволно проверување и документирање на делегираните права

Доколку формирањето групи што се специфични за организацијата и делегирањето на правата на овие групи не се систематски планирани и спроведени, ова делегирање тешко ќе може да се контролира. Потоа, на пример, може да се даде многу поголем пристап од предвидениот, што може да биде злоупотребено од трети лица. Недостатокот од редовна проверка на групите и на нивните права за пристап може дополнително да го влоши проблемот. Дури и ако се користат стандардни групи и нивните права се делегирани на нивните сопствени групи како, на пример, кога „сметки на оператори“ се делегирани за да им помагаат на вработените, обично се доделуваат повеќе права отколку што навистина се потребни.

Небезбедна автентикација

Наследените (т.е. застарени) механизми за автентикација во областа на активниот директориум, какви што се LAN Manager (LM) и NT LAN Manager (NTLM) v1, сега се сметаат за небезбедни и можат лесно да бидат заобиколени од напаѓачите под одредени услови. Како последица на тоа, напаѓачот може да добие или да злоупотреби права, така што ќе ги погоди, или на друг начин ќе ги пробие корисничките лозинки и ќе може да го компромитира доменот или неговите делови.

Премногу моќни или недоволно безбедни сметки за услуги (service accounts)

Добавувачите на апликативен софтвер понекогаш бараат од организацијата права за активен директориум за сметки за услуги за да го олеснат тестирањето и распоредувањето на нивните производи, иако всушност се потребни значително помалку права за нивното работење. Напаѓачите може да ги злоупотребат дополнителните права за сметките за услуги за да пристапат до други области на доменот. Бидејќи акредитивите на услугата што се извршува во контекст на сметката на услугата се зачувани во заштитената меморија на потсистемот на локалниот орган за безбедност (LSASS), напаѓачот може да ги извлече таму. Оттука, само една слабо обезбедена сметка на услугата може да доведе до загрозување на цел домен, особено ако сметката на услугата е обезбедена со слаба лозинка. Ова се должи на тоа што напаѓачот што користи Kerberos автентикација лесно може да побара билет на TGS (Служба за доделување билети - Ticket Granting Service) во кој се обработува лозинката на сметката на услугата. Лозинката потоа може да се открие надвор од мрежата со примена на сила за пробивање.

Користење на истата локална лозинка на администратор на повеќе системи за информатичка технологија

Локалните сметки може да се најават во систем за информатичка технологија дури и ако тој не е поврзан со соодветниот домен. Ако истите акредитиви се користат на неколку системи за информатичка технологија, администраторот може да се најави и на другите системи за информатичка технологија. Ова го зголемува ризикот напаѓачот да најде акредитиви на домен со повисоки права на еден од системите за информатичка технологија и да ги злоупотреби за да го компромитира доменот.

4.29.4 Мерки

Планирање активен директориум

Избраното функционално ниво на домен мора да биде соодветно и колку што е можно повисоко. Оправданоста за овој избор треба да биде соодветно документирана. Организацијата мора да изготви политика за контрола на пристап за активен директориум во согласност со прифатените барања. На администраторските привилегии мора да им се доделат рестриктивни овластувања засновани на потреби. Планираната структура на активен директориум, вклучувајќи ги можните промени на шемата, треба јасно да се документа.

Планирање на администрирањето на активен директориум

Во големите домени, администраторските корисници мора да бидат поделени во однос на услугата и администрирањето на податоците што се однесуваат на активни директориуми. Овде, администраторските задачи мора да се распределат и во активниот директориум според модел на делегирање за да нема преклопување.

Планирање групна политика во Windows

Во организацијата мора да постои концепт за конфигурирање групни политики. Повеќекратните преклопувања мора да се избегнуваат секогаш кога тоа е можно во концептот на групната политика. Мора да биде можно да се препознаат исклучоци од концептот на групна политика во документацијата. Сите објекти на групната политика мора да бидат заштитени со рестриктивни права за пристап и да се дефинираат безбедни спецификации за параметрите во сите објекти на групната политика.

Зацврстување на активен директориум

Вградените сметки мора да се конфигурираат со сложени лозинки. Тие мора да се користат само како сметки за итни случаи. Привилегираните сметки мора да бидат членови на групата „заштитени корисници“. Управуваните сметки за услуги (за групи) мора да се користат за сметки за услуги. На сите контролери на домени мора да им се доделат рестриктивни права за пристап на ниво на оперативен систем. Режимот за обновување активен директориум мора да биде заштитен со соодветна лозинка. Работата во овој режим треба да се врши само во согласност со начелото на две лица. Редовно треба да се креира карта на контролерот на домен. Овластувањата за групата „Сите (Everyone)“ мора да бидат ограничени. Контролерот на домен мора да биде заштитен од неовластено рестартирање. Политиките за домени и за контролери на домени мора да вклучуваат безбедни поставки за лозинки, заклучување на сметката, автентикација на Kerberos, кориснички права и нивно следење односно проверка. Мора да се постави доволна големина за безбедносните записи на контролерот на доменот. Доколку постојат надворешни односи на доверба со други домени, податоците за овластување на корисникот мора да се филтрираат и да се анонимизираат.

Одржување на континуитетот на работа на активен директориум

Сите односи на доверба во активниот директориум мора редовно да се оценуваат. Групата администратори на домен мора да биде празна или колку што е можно помала. Сметките што повеќе не се користат, мора да бидат оневозможени во активниот директориум. Ваквите сметки треба да се избришат откако ќе измине реално потребниот период на чување. Сите потребни параметри на активен директориум треба да се ажурираат и јасно да се документираат во организацијата.

Имплементација на безбедни методи за администрирање за активен директориум

Во организацијата мора да биде можно јасно да се следи секоја сметка на вработен. Бројот на администратори на услуги и администратори на податоци за активен директориум мора да биде ограничен на потребниот минимален број од доверливи лица. Стандардната сметка „Администратор“ треба да се преименува и треба да се создаде сметка „Администратор“ без привилегии. Мора да се обезбеди дека сметките на администраторот на услугата се администрираат исклучиво од членови на групата администратори на услуги. Групата „Оператори на сметки“ треба да биде празна. Администраторите треба да бидат само привремено назначени во групата „Администратори на шема“ за времето што е потребно за промена на шемата. За групите „Организациски администратори“ и „Администратори на домени“ треба да се воспостави начелото на две лица за администрирање на коренскиот домен (root domain). Мора да се обезбеди дека групите „Администратори“ и „Администратори на домен“ исто така се сопственици на коренскиот објект на соодветниот домен. Треба да се избегнува употребата на локални групи на домен за контролирање на привилегиите за читање на атрибутите на објектот. Треба да се овозможи кантата за отпадоци на активниот директориум. Во големите организации треба да се користи решение за управување со идентитетот на организацијата за да се обезбеди дека правата на сите корисници се усогласени со дефинираните спецификации.

Конфигурирање безбеден канал во Windows

Безбедниот канал треба да се конфигурира во Windows во согласност со безбедносните барања и достапните локални услови на организацијата. Во процесот треба да се земат предвид сите релевантни параметри на групната политика на организацијата.

Заштита на автентикација при користење активен директориум

Протоколот за автентикација Kerberos треба постојано да се користи во околината на активен директориум. Ако привремено се користи NTLMv2 заради компатибилност, миграцијата во Kerberos треба да се планира и да се закаже. Автентикацијата на администратор на локална мрежа (LM) треба да се оневозможи. Треба да биде потпишан сообраќајот на податоци за SMB (Server Message Block). Треба да се спречи анонимен пристап до контролерите на домени.

Безбедно користење доменски именски систем (DNS) за активен директориум

Организацијата треба да користи интегрирани зони за доменски именски систем (DNS) или безбедно динамично ажурирање на податоците на DNS. Пристапот до конфигурациските податоци на DNS серверот треба да биде дозволен само од администраторски сметки. DNS меморијата на DNS серверите треба да биде заштитена од неовластени промени. Пристапот до DNS услугата на контролерите на доменот треба да биде ограничена на потребниот минимум. Треба да се следат мрежните активности во врска со барањата за DNS. Пристапот до податоците на DNS во активен директориум треба да биде ограничен на администраторите што користат списоци за контрола на пристап (ACL). Треба да се избегнуваат секундарни зони за доменски именски систем (DNS). Во најмала рака, датотеката на зоната треба да биде заштитена од неовластен пристап. Ако се користи IPsec за да се заштитат DNS комуникациите, треба да се обезбеди доволно проток на податоци во мрежата.

Следење инфраструктура на активен директориум

Во организацијата треба да се следат, да се евидентираат и да се оценуваат промените на ниво на домен и во целокупната структура на активен директориум.

Сигурносни копии за контролери на домени

Организацијата треба да има политика за сигурносна копија и обновување за контролерите на домени. Користениот софтвер за сигурносна копија треба да биде изречно одобрен од давателот за употреба при правење сигурносна копија на податоците на контролерите на домени. Треба да се постави посебна сметка за сигурносна копија со администраторски права на услугата за контролерите на доменот. Бројот на членови на групата „Оператори за сигурносна копија“ треба да се ограничи на потребниот минимум. Пристапот до објектот AdminSDHolder треба да биде ставен под посебна заштита за да се заштитат овластувањата.

Редовно треба да се прави сигурносна копија од податоците на доменските контролери. Овде треба да се користи метод со кој се избегнуваат наследените објекти секогаш кога тоа е можно.

4.29.5 Напредни мерки

Употреба на наменски привилегирани системи за администрирање

Администрирањето на активен директориум треба да се ограничи на наменски системи за администрирање. Тие треба да подлежат на особено силно зацврстување врз основа на нивните ограничени задачи.

Поделба на околии за администрирање и за производство

Системи што имаат посебно клучно значење, какви што се контролерите на домени и системите за администрирање домени, треба да се стават во посебна „шума“ со едностран однос на доверба кон производната „шума“.

Активен директориум - закани што се вклучени овде:	
3_0.11	Дефект или неисправност на давателите на услуги
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одредување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.42	Социјален инженеринг
3_0.43	Вметнување пораки
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.30 Општи клиенти и сервери за е-пошта

4.30.1 Вовед

Е-поштата е една од најстарите и најчесто користени апликации на интернет. Е-поштата се користи за испраќање текст и прикачени датотеки до други лица. За оваа намена, корисниците бараат адреса на е-пошта. За апликациите за е-пошта се потребни сервери за е-пошта, кои можат да испраќаат и да примаат електронски пораки. По правило, клиентите за е-пошта ги преземаат пораките наменети за нив од серверот за е-пошта со користење на протоколите POP3 или IMAP и испраќаат пораки до серверот за е-пошта со користење на протоколот SMTP, кој ги препраќа на друг сервер за е-пошта доколку е потребно. Бидејќи е-поштата широко се применува, особено кај организациите, серверите за е-пошта често се мета на напаѓачите. Клиентите на е-пошта исто така се во фокусот на нападите, вклучително и оние што се обидуваат да испорачаат злонамерен софтвер преку е-пошта. Покрај тоа, е-пошта често се користи како алатка за напади како дел од социјален инженеринг. Од тие причини, безбедното работење и користење на апликациите за е-пошта е особено важно.

4.30.2 Цел

Целта е да се заштитат информациите што се обработуваат со клиентите за е-пошта или на серверите за е-пошта.

4.30.3 Закани

Недоволно планирање на употребата на е-пошта

Е-поштата не може да се користи безбедно без соодветно документираните правила и дефиниран безбедносен процес во рамките на организацијата. Доколку се занемарат процедуралните, организациските и техничките правила при планирањето на системите за е-пошта, тоа може да доведе до неточни поставки и внатрешни и надворешни напади.

На пример, серверот за е-пошта што не е доволно голем, може да не функционира поради голем број дојдовни е-пораки. Доколку доволно не се планираат безбедносните заштитни мерки, клиентите на е-пошта исто така ќе бидат повеќе подложни на е-пошта што содржи злонамерен софтвер.

Неправилно конфигурирање на клиентите и на серверите за е-пошта

Бидејќи инфраструктурите за е-пошта може да бидат многу сложени, големиот број на можни поставки и вклучени меѓусебно зависни параметри може да предизвикаат голем број безбедносни проблеми. На пример, серверот за е-пошта може да одбие легитимни е-пораки од други сервери поради неисправна конфигурација. Истовремено може да се игнорираат или да се занемарат основните поставки (на пример, транспортно криптирање е-пошта). Понатаму, неточните конфигурации во клиентите за е-пошта може да доведат до нивно извршување на злонамерен код во е-пошта. Овие пропуски може значително да влијаат врз достапноста, интегритетот и доверливоста на информациите во организацијата.

Многу организации не користат безбедносни механизми што им овозможуваат на серверите за е-пошта во други организации да проверат дали е-поштата е всушност од наведениот испраќач. И неправилно поставен сервер за е-пошта може да биде злоупотребен од напаѓачите за испраќање несакана е-пошта (спам).

Несигурност на е-поштата

Е-поштата е брз и погоден начин за размена на податоци, но не е секогаш сигурен. Пораките може да се изгубат, на пример, поради неисправни сервери за е-пошта или прекинати патеки за пренос. Причините за ова може да вклучуваат филтри за спам што ги филтрираат и ги отфрлаат легитимните пораки. Е-поштата може да се изгуби и кога адресата на примачот не е правилно внесена. Во најлош случај, доверливите информации може да се испратат до погрешни примачи.

Злонамерен софтвер во е-пошта

Постојат неколку начини на кои напаѓачите можат да шират злонамерен софтвер со користење е-пошта. Злонамерниот код може да се содржи директно во е-пошта, како пример. Ако клиентот за е-пошта не е правилно конфигуриран, тој може да го изврши кодот кога ќе се отвори е-поштата. Датотеките што содржат злонамерен софтвер може да се испраќаат и како прилози на е-пошта. Доколку филтрите за несакана е-пошта (спам) или вируси не ја сортираат таквата е-пошта и корисниците ги отворат прилозите, злонамерниот софтвер се извршува. Ова може да доведе до голема штета и на други системи за информатичка технологија, на пример, ако се изврши уценувачки софтвер (исто така познат како „тројанци за изнуда“).

Социјален инженеринг

Напаѓачите често користат е-пошта за да добијат доверливи информации или да ги измамат корисниците за друго штетно однесување. На пример, напаѓачот може да испрати е-пошта во која се тврди дека е од раководител што му дава инструкции на примачот да изврши дејства што ќе ѝ наштетат на организацијата (позната како измама на извршниот директор). Ова често вклучува инструкции за пренос на пари на сметки во странство. Со лажна е-пошта од вистински и доверлив давател на услуги може да се бара и внесување на податоците за пристап на веб-локација (кражба на идентитетот). Потоа напаѓачот може да ги искористи така добиените податоци за пристап за да преземе понатамошни активности. Опасноста од социјален инженеринг се зголемува доколку корисниците редовно не се обучуваат и информираат за овие закани.

Читање и манипулирање на е-пошта

Е-поштата обично се испраќа во некриптирана форма и без потпис, што им овозможува на напаѓачите да ги читаат, па дури и да ги менуваат пораките како што сакаат. Тие потоа можат да откријат доверливи информации или да споделат лажни информации. На овој начин, напаѓачите можат да инсталираат и злонамерен софтвер.

4.30.4 Мерки

Безбедно конфигурирање клиенти за е-пошта

Организацијата мора да има безбедна конфигурација за своите клиенти за е-пошта. Клиентите за е-пошта мора да бидат претходно конфигурирани кога им се даваат на корисниците. Организацијата мора да обезбеди дека корисниците не можат да ги променат аспектите на конфигурацијата што се значајни за безбедноста. Ако тоа не е можно, организацијата мора да ги извести корисниците дека не им е дозволено сами да ја менуваат конфигурацијата. Пред да се отворат прилозите на датотеките од е-пошта, мора да се провери присуството на злонамерен софтвер од страна на заштитна програма на клиентот, доколку тоа веќе не е направено на серверот за е-пошта. Клиентите за е-пошта мора да се конфигурираат така што автоматски нема да толкуваат каков било HTML код или друга активна содржина во е-поштата. Функциите за преглед за прилозите на датотеките мора да се конфигурираат така што тие автоматски нема да ги толкуваат датотеките. Правилата за филтрирање е-пошта и неконтролираното автоматско препраќање е-пошта, мора да се ограничат на неопходните ситуации за апликација. Клиентите за е-пошта мора да користат безбедно криптирање за транспорт за комуникација со сервери за е-пошта преку недоверливи мрежи.

Безбедно работење на серверите за е-пошта

Организацијата мора да имплементира механизми за заштита од напади на одбивање услуга (DoS). Серверите за е-пошта мора да нудат безбедно криптирање за транспорт за прием на е-пошта и пристап до клиенти на е-пошта преку јавни мрежи за податоци. Доколку серверите за е-пошта испраќаат е-пошта сами, треба да користат и безбедно криптирање за транспорт за оваа намена. Организацијата мора да ги прецизира сите протоколи за е-пошта и услугите што ги дозволува. Покрај тоа, организацијата мора да ги конфигурира серверите за е-пошта за да не може да се злоупотребуваат за пренесување на несакана е-пошта (спам). Ако пораките се зачувани на сервер за е-пошта, организационата единица за информатичка технологија мора да конфигурира и да документира соодветно ограничена големина на поштенското сандаче од страната на серверот.

Сигурносна копија на податоци и архивирање е-пошта

Организацијата мора редовно да прави сигурносни копии на своите сервери за е-пошта. За таа цел, организацијата мора да регулира како се прават сигурносни копии на испратената и на примената е-пошта на клиентите на е-пошта и е-поштата на серверите. Во однос на архивирањето, организацијата треба да има предвид дека е-поштата може да се чува само локално на клиентите.

Заштита од несакана е-пошта (спам) и вируси на серверите за е-пошта

Организацијата мора да обезбеди дека дојдовната и излезната е-пошта на серверите за е-пошта, а особено прилозите на е-поштата, се проверуваат за потенцијални карактеристики на несакана е-пошта (спам) и штетна содржина. Воведувањето и користењето на програмите за филтрирање е-пошта, мора да се координираат со офицерот за заштита на личните податоци, со вработените и корисниците. Организацијата мора да прецизира како да се постапува со криптираната е-пошта, доколку не може да се декриптира од користената програма за заштита од вируси.

Воспоставување правила за замена за користење е-пошта

Организацијата треба да воспостави правила за замена за постапување со е-пошта. Доколку се препраќа е-поштата, корисниците што заменуваат некое вработено лице треба да бидат информирани за тоа. Аспектите за заштита на личните податоци мора да се земат предвид при препраќање е-пошта. Организацијата треба да воспостави правила за функциите за автоматски одговор во програмите за е-пошта што опишуваат како овие функции може безбедно да се користат. Кога вработените ги користат функциите за автоматски одговор, не треба да се откриваат никакви внатрешни информации.

Дефинирање безбедносна политика за е-пошта

Организацијата треба да воспостави и редовно да ажурира безбедносна политика за користење е-пошта. Организацијата треба да ги извести сите корисници и администратори за новите или за променетите безбедносни барања за апликациите за е-пошта. Политиката за безбедност на е-пошта на организацијата треба да е во согласност со нејзините општо применливи безбедносни политики. Организацијата треба да проверува дали безбедносната политика правилно се применува.

Политиката за безбедност на е-пошта за корисниците треба да го опфаќа следното:

- Како може да се обезбедат овие комуникации,
- Кои права за пристап на корисниците постојат,
- Како се проверува е-поштата за фалсификувани испраќачи,
- Како да се обезбедат пренесените информации,
- Како да се провери интегритетот на е-поштата,
- Кои отворени списоци за дистрибуција на е-пошта може да се користат,
- Дали е дозволено користење приватна е-пошта,
- Како да се справи со е-поштата и со поштенските сандачиња на вработените што ја напуштаат организацијата,
- Дали и како може да се користат услугите за веб-пошта,
- Кој е одговорен за групните поштенски сандачиња,
- Како треба да се постапува со прилозите на датотеки,
- Како корисниците треба да постапуваат со е-пошта во HTML-формат.

Политиката за безбедност на е-пошта треба да ги вклучува и опциите за конфигурација на апликациите за е-пошта за администратори, како и спецификациите за можен пристап до сервер за е-пошта од други сервери. Политиката треба да опфаќа и информации за овластени точки од кои може да се пристапи до серверот за е-пошта. Политиката за безбедност на е-пошта треба да го регулира постапувањето со групите за вести и списоците на примачи.

Обука за корисници за безбедносните механизми на клиентите на е-пошта

Организацијата треба да ги едуцира корисниците за ризиците од користење апликации за е-пошта и како безбедно да ја користат е-поштата. Ова едукација треба да се врши како дополнување на општата обука и активностите за подигање на свеста. Организацијата треба да им укаже на корисниците за можните опасности од отворањето на прилозите на е-пошта. Обуката треба да се однесува и на тоа како корисниците можат да препознаат е-пошта од лажни испраќачи. Организацијата треба да ги предупреди корисниците да не учествуваат во верижни писма на е-пошта или да се претплатат на голем број списоци на примачи.

Обука на корисниците за постапување со несакана е-пошта (спам)

По правило, сите корисници треба да ги игнорираат и да ги избришат сите несакани пораки (спам). Корисниците не треба да одговараат на несакана е-пошта и не треба да ги отвораат линковите во ваквата е-пошта. Ако организацијата има централно решение за управување со несакана е-пошта, корисниците треба да ја препраќаат несаканата е-пошта (спам) во организацијата и потоа да ја избришат.

Проширени безбедносни заштитни мерки на серверите за е-пошта

Серверите за е-пошта на организацијата треба да ја проверуваат дојдовната е-пошта со помош на рамката за политика на испраќачот (SPF) и кодовите на доменот (DomainKeys). Организацијата треба да користи и DomainKeys и SPF за автентичноста на е-поштата што ја испраќа. Ако се користи SPF, треба јасно да се наведе како треба да се постапува со е-поштата. Параметарот soft fail ("~") треба да се користи само за тестирање. Организацијата треба да користи автентикација, известување и усогласеност на пораките врз основа на домен (DMARC) за да одреди како е-поштата што ги испраќа треба да бидат потврдени од серверот за е-пошта што ги прима. Извештаите за DMARC треба редовно да се оценуваат. Организацијата треба да утврди дали извештаите за DMARC за примената е-пошта се испраќаат до други организации.

Организацијата треба да ги обезбеди своите комуникации за е-пошта преку DANE и MTA-STS.

4.30.5 Напредни мерки

Криптирање од крај до крај

Организацијата треба да користи криптирање од крај до крај и потписи за е-пошта. За криптирање и потписи треба да се користат само протоколи што се во согласност со најсовремените технолошки достигнувања.

Распоредување редундантни сервери за е-пошта

Организацијата треба да управува со неколку редундантни сервери за е-пошта. Редундантните сервери за е-пошта треба да се зачуваат со соодветен приоритет во информациите за доменски именски систем (DNS) на засегнатите домени. Организацијата треба да одреди како е-поштата треба да се синхронизира меѓу нејзините сервери за е-пошта.

Следење јавни црни листи

Организацијата треба редовно да проверува дали нејзините сервери за е-пошта се наведени на јавни списоци за несакана е-пошта (спам) или на црни листи.

Известување за безбедност на транспортен слој

Организацијата треба да користи известување за безбедност на транспортен слој (TLS) и треба да се утврди дали извештаите за TLS е потребно да се испраќаат и до други организации.

Општи клиенти и сервери за е-пошта - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.25	Дефект на уреди или на системи
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.33	Недостиг на кадар
3_0.36	Кражба на идентитет
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.42	Социјален инженеринг
3_0.45	Губење податоци

4.31 Microsoft Exchange и Outlook

4.31.1 Вовед

Microsoft Exchange Server („Exchange“) е решение за колаборативен софтвер за средни до големи организации. Може да се користи за електронски пренос на пораки и е опремен со дополнителни услуги за поддршка на работните текови. Exchange може да се користи за централно управување, испорака, филтрирање и испраќање пораки како што е е-пошта. Воедно, обезбедува и управува со типични апликации за група, какви што се белешки, списоци со контакти, календар и списоци со задачи. Покрај самата серверска услуга, за да се користат функциите на Exchange, неопходен е клиентски софтвер или веб-прелистувач.

Microsoft Outlook („Outlook“) е клиент за Exchange кој е директно достапен со инсталирање Office пакет од Microsoft или со негово интегрирање во оперативните системи на мобилните уреди. Понатаму, апликацијата „Outlook on the web“ („Outlook Web App“) овозможува пристап до е-пошта, контакти, календар и повеќе прелистувачи. Оваа функција е веќе вклучена во Exchange. Комбинацијата на сервери на Exchange и клиенти на Outlook во оваа точка е наречена Exchange систем.

4.31.2 Цел

Целта е да се обезбедат информации за типични закани за Exchange и за Outlook и да се покаже како Exchange и Outlook може безбедно да се користат во организациите.

4.31.3 Закани

Недоволно правила за Exchange и за Outlook

Неопходни се сеопфатни правила и спецификации за Exchange и за Outlook за да се обезбеди безбедност на информациите што се користат за обработка. На пример, податоците може случајно да се изгубат, да се променат или да се избришат, ако Exchange неправилно и неконтролирано се инкорпорира во активен директориум. Истото важи и ако базите на податоци за поштенски сандачиња нерегулирано се надвор од мрежа, ако Exchange не е доволно земен предвид во безбедносната политика на организацијата или ако клиентите на Outlook можат да пристапат до серверите на Exchange без никакви контроли.

Неправилно мигрирање на Exchange

Во практика, почесто се врши мигрирање на Exchange системите отколку што се инсталираат одново. За мигрирање на нова верзија на Exchange Server, понекогаш е неопходно да се ажурира оперативниот систем на понова верзија. Новите верзии на оперативните системи честопати вклучуваат барања во врска со постојниот концепт на домен и постојните услуги на директориумот. Ако миграцијата не е испланирана и не се изврши внимателно, внатрешните комуникации со помош на Exchange може значително да се нарушат во рамките на организацијата, што потоа може да ја намали продуктивноста. За време на миграцијата, може да се појават проблеми со конфигурацијата од причини какви што се промени во конфигурациските поставки за различните достапни верзии или опциите за поврзување со услугите на директориумот. Понатаму, неточните поставки на протоколот може да предизвикаат неправилности во врска со пренос на информации, автентикација или криптирање.

Недозволен пристап на прелистувачот до Exchange

Exchange им овозможува на корисниците пристап до нивните сопствени сметки за е-пошта преку прелистувач. Ова вклучува употреба на интернет информативни услуги (IIS), кои се составен дел на оперативниот систем Windows. Ако оваа функционалност е недоволно испланирана и неправилно конфигурирана, може да овозможи неконтролиран пристап до внатрешната мрежа однадвор. Доколку до е-поштата се пристапува преку интернет со прелистувач, тоа создава многу значителни ризици. И покрај тоа што немаат директен пристап до мрежата на организацијата, напаѓачите може да пристапат до е-поштата и со тоа да добијат пристап до адресите и до содржината на е-поштата, да ги злоупотребат функциите на е-поштата, да испраќаат несакана е-пошта (спам) или да добијат пристап до внатрешните информации на организацијата.

Неовластено поврзување други системи со Exchange

Системите за Exchange се цврсто испреплетени со оперативниот систем Windows и соработуваат само со системи од трети лица со користење конектори што им овозможуваат на другите системи да преземаат е-пошта од серверите на Exchange со користење одредени протоколи (на пример, POP3). Доколку конекторите не се земат предвид при инсталирањето или миграцијата на Exchange, тие може да бидат некомпатибилни со мигрираната верзија на Exchange. Како последица на тоа, е-поштата може да се изгуби или случајно да се промени. Надвор од хомогената средина на Microsoft, безбедносните поставки во врска со Exchange системот се нефункционални. Ако различни потсистеми се администрираат одделно, во секое време може да се појават недоследности. Неправилно поврзаните системи од трети лица, исто така, може да предизвикаат губење на податоците или блокирање на системите.

Неправилно администрирање на локацијата и на правата за пристап до податоци во Exchange и Outlook

Може да се појават недостатоци во безбедноста ако правата за пристап до клиент на Outlook или податоците зачувани во Exchange и Outlook не се креираат и администрираат правилно. Ова може да се случи, на пример, ако се доделат права што ги надминуваат потребните права, овозможувајќи им на неовластени лица да пристапат до доверливи информации.

Неправилно конфигурирање на Exchange

Успешните напади на услуги како што е Exchange често се овозможени со неправилно конфигурирани системи. Бидејќи Exchange системот е многу сложен, различните конфигурациски поставки и меѓу зависните параметри може да предизвикаат голем број безбедносни проблеми. Можните неточни конфигурации се движат од инсталација и работа на компонентите на Exchange на несоодветни системи, отсуство на криптирање и недоволни ограничувања на правата за пристап на серверите на Exchange до неправилно доделување права за пристап при креирање или иницијализирање на базата на податоци на Exchange.

Неправилно конфигурирање на Outlook

Клиентот за е-пошта Outlook е важен дел од системот Exchange. За целокупната безбедност на системот, важно е клиентите на Outlook да бидат правилно конфигурирани. Избраниот протокол за комуникација може да создаде специфични безбедносни проблеми. И приватните клучеви што се користат за криптирање и за потпишување е-пошта можат да бидат компромитирани. Ако се користи криптирање на ниво на мрежа (на пример, врз основа на IPSec или TLS), механизмот за криптирање може да стане неефикасен поради неправилно конфигуриран клиент. Неточните конфигурации може да предизвикаат безбедносни проблеми како што е губење на доверливоста поради неовластен пристап.

Неисправност и злоупотреба на внатрешни макросеквенци и програмски интерфејси во Outlook

Многу производители на софтвер ги опремуваат своите алатки и апликации со интерфејси за програмирање апликации (API). Тие овозможуваат користење одредени функции на други програми или проширување на сопствениот опсег на функции на апликацијата. Функции како овие може да се злоупотребат во Outlook за ширење злонамерен софтвер. Варијантите на злонамерен софтвер вклучуваат злонамерни алатки и макросеквенци кои директно го искористуваат Outlook и неговите поврзани функции за е-пошта, со цел да добијат, да менуваат или да бришат информации. Макросеквенците може да се користат и за препраќање или преместување пораки, датуми или задачи. Грешките во макросеквенците може да создадат поголем ризик во оваа смисла. Индексните грешки во макросеквенците може да дадат неточни резултати поради кои организацијата ќе донесе лоши одлуки. Специфичните последици може да вклучуваат непотребни трошоци или автоматско протекнување податоци од организацијата.

4.31.4 Мерки

Планирање на користење Exchange и Outlook

Организацијата пред да ги имплементира Exchange и Outlook, мора внимателно да го испланира нивното користење и притоа мора да го има предвид најмалку следново:

- Дизајн на инфраструктура за е-пошта,
- Клиентите и/или серверските системи што ќе се поврзат,
- Користење функционални екстензии,
- Протоколите што ќе се користат.

Избор на инфраструктура за размена

Врз основа на планирањето на распоредувањето на Exchange, организацијата мора да одлучи за системите, компонентите на апликацијата и за хиерархиската градација со која ќе се реализира инфраструктурата на Exchange. При избор на инфраструктура, мора да се одлучи дали системите ќе работат во „облак“ или како локална услуга.

Управување со пристап и права на пристап

Покрај општата политика за контрола на пристап, организацијата мора да креира, документира и да применува политика за контрола на пристап за системите во нејзината инфраструктура на Exchange. Организационата единица за информатичка технологија мора да користи кориснички профили од страна на серверот за кориснички пристап независен од компјутер до податоците на Exchange и притоа мора да ги приспособи стандардните овластувања за NTFS за директориумот на Exchange, така што само на овластените администратори и системски сметки им е дозволен пристап до податоците во тој директориум.

Правење сигурносна копија на Exchange

Организацијата мора да направи сигурносна копија на Exchange серверите пред какви било инсталации и промени во конфигурацијата, како и во циклични интервали. Конкретно, мора да се направи сигурносна копија на базите на податоци на Exchange серверот. Избришаните објекти на Exchange треба да се отстранат од базата на податоци по одредено време.

Мигрирање на Exchange системи

Организационата единица за информатичка технологија треба темелно да ги испланира и да ги документира сите чекори за миграција. Организационата единица за информатичка технологија треба да ги има предвид поштенските сандачиња, објектите, безбедносните политики, концептите на активните директориуми и врските со други системи за е-пошта. Исто така, треба да ги има предвид функционалните разлики помеѓу различните верзии на Exchange. Новиот систем треба да се тестира во посебна мрежа за тестирање пред да се инсталира.

Безбедно конфигурирање на Exchange серверите

Организационата единица за информатичка технологија треба да ги инсталира и да ги конфигурира Exchange серверите како што е наведено во безбедносната политика на организацијата. Конекторите треба безбедно да се конфигурираат. Организационата единица за информатичка технологија треба да овозможи евидентирање на записи од Exchange системот и да создаде соодветен концепт за постојните приспособувања што се специфични за корисникот. При користење функционални екстензии, треба да се обезбеди дека сепак се исполнети барањата што се дефинирани за одржување доверливост, интегритет и достапност во организацијата.

Безбедно конфигурирање на Outlook

Организационата единица за информатичка технологија треба да создаде посебен Outlook профил со кориснички специфични поставки за секој корисник. Организационата единица за информатичка технологија треба да го конфигурира Outlook така што само потребните информации се пренесуваат до други корисници, како и да ги извести корисниците за информациите што автоматски се пренесуваат на други корисници. Прочитаните примени пораки и информациите што нудат увид во внатрешната структура на организацијата, не треба да се пренесуваат на надворешни корисници.

Заштита на комуникациите помеѓу Exchange системите

Организацијата треба да одлучи за механизмите за заштита што треба да се користат за јасно да се обезбедат комуникациите помеѓу Exchange системите. Конкретно, Одделот за операции за информатичка технологија треба да определи како е обезбедена комуникацијата со следните интерфејси:

- Интерфејси за администрирање,
- Комуникации клиент-сервер,
- Постојни интерфејси за веб-базирано дистрибуирано авторизирање и верзионизирање (WebDAV),
- Комуникација од сервер до сервер,
- Инфраструктура на јавен клуч на која се заснова криптирањето на е-поштата на Outlook.

Користење Outlook Anywhere, MAPI over HTTP и Outlook on the Web

Организационата единица за информатичка технологија треба да ги конфигурира Outlook Anywhere, MAPI over HTTP и Outlook on the Web во согласност со безбедносните барања на организацијата. Пристапот до Exchange преку интернет треба да биде ограничен на потребните корисници.

4.31.5 Напредни мерки

Криптирање датотеки на база на податоци на Exchange

Организационата единица за информатичка технологија треба да создаде концепт за криптирање на PST и Information Store датотеки. Организацијата треба да ги информира корисниците за механизмите за заштита што се користат за криптирање на PST-датотеките и како функционираат овие механизми. Дополнителни аспекти на локалните PST-датотеки што треба да се земат предвид при криптирање на базите на податоци на Exchange системот вклучуваат:

- Сопственички функции за криптирање,
- Степени на криптирање,
- Механизми за обезбедување на податоците во PST-датотека.

Притоа, треба да се користат механизми како што е криптирање на дискот со Encrypting File System или Windows BitLocker за да се обезбедат PST-датотеките.

Microsoft Exchange и Outlook - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.36	Кражба на идентитет
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.32 Виртуелизација

4.32.1 Вовед

Кога системите за информатичка технологија се виртуелизирани, еден или неколку виртуелни системи за информатичка технологија се извршуваат на физички систем за информатичка технологија. Физичкиот систем за информатичка технологија од овој вид се нарекува сервер за виртуелизација. Може да се консолидираат неколку сервери за виртуелизација за да формираат виртуелна инфраструктура. Овде, самите сервери за виртуелизација и виртуелните системи за информатичка технологија што работат на нив може заеднички да се администрираат.

Виртуелизацијата на системите за информатичка технологија обезбедува многу предности за операциите на информатичката технологија во доменот на информации. На пример, можни се заштеди на трошоците на полето на набавка на хардвер, електрична енергија и климатизација доколку ресурсите на физичките системи за информатичка технологија се користат поефикасно. Сепак, виртуелизацијата претставува и предизвик во работењето со доменот на информации. Бидејќи употребената технологија за виртуелизација влијае врз различни области и полиња на работа во доменот на информации, потребно е знаење и искуство од овие области. Покрај тоа, проблемите на серверот за виртуелизација може да влијаат и врз сите други виртуелни системи за информатичка технологија што работат на истиот сервер. Виртуелните системи за информатичка технологија исто така можат меѓусебно да си пречат во работата.

4.32.2 Цел

Целта е да се опише како серверите за виртуелизација во доменот на информации можат безбедно да се имплементираат и да се управуваат во организацијата.

4.32.3 Закани

Слабо планирање на виртуелизацијата

Серверот за виртуелизација овозможува работа со виртуелни системи за информатичка технологија, ги интегрира овие системи во центар за податоци и притоа го контролира нивното поврзување со понатамошни инфраструктурни елементи какви што се мрежите (вклучително мрежи за чување податоци). Во отсуство на какво било планирање за тоа како серверите за виртуелизација треба да се интегрираат во постојната инфраструктура од техничка и организациска гледна точка, одговорностите за различни области можеби не се јасно дефинирани (на пример, за апликации, оперативни системи и мрежни компоненти). Покрај тоа, одговорностите за различни области може да се преклопуваат или може да нема соодветна структура на права за одвојување на администраторскиот пристап за различни области.

Слабо конфигурирање на виртуелизацијата

Виртуелизацијата го менува начинот на кој се обезбедуваат серверите. Ресурсите какви што се централните обработувачки единици, RAM меморијата, мрежните конекции и меморијата обично се конфигурираат централно со користење систем за управување и затоа повеќе не зависат од хардверот и од каблите. Ова брзо може да доведе до грешки во конфигурацијата. На пример, ако виртуелниот систем за информатичка технологија е многу сензитивен и погрешно е лоциран во надворешна демилитаризирана зона (DMZ), до системот може да се пристапи од интернет и со тоа е изложен на зголемен ризик.

Недоволно ресурси за виртуелни системи за информатичка технологија

За серверите за виртуелизација е потребен простор на дискот што е обезбеден или локално во самите сервери или во мрежа за чување податоци, со цел да работат со виртуелни системи за информатичка технологија. Ако недоволно се планираат капацитетите за чување податоци што се потребни за таа цел, ќе има големи ризици во однос на достапноста на виртуелните системи за информатичка технологија и интегритетот на информациите што тие ги обработуваат. Ова особено наоѓа примена, ако се користат специјални функции за виртуелизација какви што се слика за состојбата или прекумерно искористување простор на дискот. Може да се појават недостатоци што го вклучуваат не само просторот што е достапен на хард-дискот или на мрежите за чување податоци, туку и моќта за процесирање, меморијата за случаен пристап (RAM) или мрежните конекции. Понатаму, недоволните ресурси на серверот за виртуелизација може да доведат до попречување на меѓусебните операции на виртуелните машини, што, пак, на крајот може да предизвика нивно неправилно функционирање или целосно откажување.

Протекување информации или недостатоци на ресурси поради слика за состојбата (snapshots)

Сликата за состојбата може да се користи за препис на екранот и зачувување на состојбата на виртуелната машина. Ако сликата за состојбата од ваков вид се обнови подоцна, сите направени промени откако е направена сликата ќе бидат изгубени. Како последица на тоа, сите поправени недостатоци може повторно да се отворат. Понатаму, како последица, отворените датотеки, преносите на датотеки или трансакциите со базата на податоци кои се зачувани во моментот на сликата за состојбата може да дадат неконзистентни податоци. Покрај тоа, напаѓачите може да злоупотребат слики за состојбата за да пристапат неовластено до податоците на виртуелен систем за информатичка технологија. На пример, ако е направена слика за состојбата за време на активни тековни операции, содржината на главната меморија исто така се зачувала на хард-дискот и може да се обнови и да се анализира во виртуелна средина надвор од оригиналната инфраструктура на информатичката технологија. Сликите за состојбата исто така може да бидат доволно големи за да предизвикаат недостиг на достапен простор за чување податоци.

Дефект на административниот сервер за системи за виртуелизација

Бидејќи административниот сервер ги контролира и ги администрира сите функции на виртуелната инфраструктура, нефункционалноста на овој административен систем ќе го оневозможи извршувањето на какви било промени во конфигурацијата на виртуелната инфраструктура. Во текот на овој период, администраторите не можат да реагираат на проблеми какви што се недостатоци кај ресурсите или откажување на поединечни сервери за виртуелизација, ниту, пак, можат да интегрираат нов сервер за виртуелизација во инфраструктурата и/или да создадат нови виртуелни системи за информатичка технологија. Активната тековна миграција (и со проширување – екстензија, динамичното доделување ресурси за индивидуални гостински системи) исто така не е можна без административен сервер.

Злоупотреба на алатки за гости (guest tools)

Алатките за гости често се извршуваат со многу високи овластувања на виртуелните машини. Како последица на тоа, тие може да бидат злоупотребени, на пример, за напади со одбивање на услугата или како средство за преземање на целиот сервер за виртуелизација.

Компромитиран софтвер за виртуелизација

Софтверот за виртуелизација (исто така познат како „хипервизор“) е централна компонента на серверот за виртуелизација и ги контролира сите виртуелни машини што работат на серверот и им доделува ресурси од процесорот и од меморијата. Ако оваа компонента биде успешно нападната, ова ќе ги загрози и сите виртуелни системи за информатичка технологија што се извршуваат на серверот за виртуелизација.

4.32.4 Мерки

Безбедно користење виртуелни системи за информатичка технологија

Секој администратор на виртуелни системи за информатичка технологија мора да знае како виртуелизацијата влијае врз активните системи за информатичка технологија и врз апликациите. Правата за пристап на администраторите во однос на виртуелните системи за информатичка технологија мора да се ограничат само на оние права што навистина се потребни односно неопходни. Организацијата мора да обезбеди дека мрежните конекции што се неопходни за виртуелните системи за информатичка технологија се достапни во виртуелната инфраструктура. Воедно, мора да се провери дали се исполнети барањата за изолација и енкапсулација на виртуелните системи за информатичка технологија и апликациите што се работат на нив. Понатаму, користените виртуелни системи за информатичка технологија мора да ги задоволуваат прифатените барања на организацијата во врска со достапноста и протокот на податоци. За време на активните тековни операции, мора да се следи работата на виртуелните системи за информатичка технологија.

Безбедно конфигурирање виртуелни системи за информатичка технологија

Гостинските системи не смеат да пристапуваат до уредите и до интерфејсите на серверот за виртуелизација. Меѓутоа, доколку таквата врска е неопходна, мора да биде дополнително доделена и да се воспостави само за потребното времетраење од администраторот на главниот систем. Во тој поглед, мора да се прецизираат задолжителни правила.

Виртуелните системи за информатичка технологија треба да се конфигурираат и да се заштитат според безбедносната политика на организацијата.

Безбедно конфигурирање мрежа за виртуелни инфраструктури

Организацијата мора да обезбеди дека виртуелните мрежи не можат да ги заобиколат постојните безбедносни механизми (на пример, заштитните ѕидови) и системите за следење. Воедно, мора да се обезбеди дека виртуелните системи за информатичка технологија што се поврзани со неколку мрежи, не можат да се користат за воспоставување несакани мрежни конекции. Мрежните врски помеѓу виртуелните системи за информатичка технологија и физичките системи за информатичка технологија и за виртуелните заштитни ѕидови треба да се конфигурираат во согласност со безбедносните политики на организацијата.

Заштита на интерфејси за администрирање

Целиот пристап за администрирање и управување до системите за управување и главните системи мора да биде ограничен со цел да се обезбеди дека не е можен пристап до интерфејсите за администрирање од недоверливи мрежи.

За да се администрираат и да се следат серверите за виртуелизација или системите за управување, треба да се користат протоколи што се сметаат за безбедни. Ако сепак се користат несигурни протоколи, мора да се користи посебна мрежа за администрирање.

Најава во виртуелната инфраструктура

Работната состојба, користењето и мрежните конекции на виртуелните инфраструктури мора континуирано да се евидентираат. Доколку се достигнат ограничувањата на капацитетот, виртуелните машини треба да се преместат. Покрај тоа, треба да се прошири хардверот, доколку е применливо. Притоа, мора да се следи и дали виртуелните мрежи се правилно доделени на соодветните виртуелни системи за информатичка технологија.

Временска синхронизација во виртуелни системи за информатичка технологија

Системското време на сите виртуелни системи за информатичка технологија во производна употреба секогаш мора да биде синхронизирано.

Планирање виртуелна инфраструктура

Структурата на виртуелната инфраструктура треба детално да се испланира. Во овој процес, треба да се земат предвид важечките правила и политики за работа со системите за информатичка технологија, апликации и мрежи (вклучително мрежи за чување податоци). Ако неколку виртуелни системи за информатичка технологија работат на сервер за виртуелизација, треба да се исклучат конфликти во однос на барањата за заштита на системите за информатичка технологија. Понатаму, треба да се дефинираат и јасно да се одделат задачите на поединечните групи администратори, како и да се дефинираат вработените што се одговорни за работа со конкретни компоненти.

Мрежно планирање за виртуелна инфраструктура

Структурата на мрежи за виртуелни инфраструктури треба детално да се испланира. Треба да се провери и дали мора да се воспостави посебна мрежа и таа да се користи за одредени функции за виртуелизација (како што е активна тековна миграција). Треба да се испланираат мрежните сегменти што треба да се постават (на пример, мрежи за управување, мрежи за чување податоци). Треба да се определи како мрежните сегменти можат безбедно меѓусебно да се одвојат и да се заштитат. Овде, треба да се обезбеди дека производната мрежа е одвоена од мрежата за управување. Притоа, треба да се исполнат и барањата за достапност на мрежата.

Воведување процеси на управување за виртуелни системи за информатичка технологија

За серверите за виртуелизација и виртуелните системи за информатичка технологија, треба да се дефинираат и да се воспостават процеси за пуштање во работа, попис/инвентар, работа и деактивирање. Процесите редовно треба да се документираат и да се ажурираат. Доколку се планира користење на такви виртуелни системи за информатичка технологија, треба да се дефинираат функциите за виртуелизација што може да ги користат виртуелните системи за информатичка технологија. Околините за тестирање и развој не треба да се работат на истиот сервер за виртуелизација како и виртуелните системи за информатичка технологија во производна употреба.

Администрирање на инфраструктурата за виртуелизација со користење посебна мрежа за управување

Инфраструктурата за виртуелизација треба да се администрира само со помош на посебна мрежа за управување. Треба да се активираат достапните безбедносни механизми на протоколите за управување што се користат за автентикација, обезбедување интегритет и криптирање. Сите несигурни протоколи за управување треба да се оневозможат.

Концепт за права и улоги за администрирање виртуелна инфраструктура

Врз основа на задачите и на улогите што се определени во фазата на планирање, треба да се подготви и да се имплементира концепт за права и за улоги за администрирање виртуелни системи за информатичка технологија и мрежи на сервери за виртуелизација и во околината за управување. Сите компоненти на виртуелната инфраструктура треба да се интегрираат во централен систем за управување со идентитет и пристап. Администраторите на виртуелните машини треба да се разликуваат од администраторите на околината за виртуелизација и да им се доделат различни права за пристап. Понатаму, околината за управување треба да може да групира виртуелни машини за соодветно структурирање. Улогите на администраторите треба да бидат соодветно доделени.

Избор на соодветен хардвер за околини за виртуелизација

Користениот хардвер треба да биде компатибилен со употребеното решение за виртуелизација. Во овој случај треба да се обезбеди дека производителот на решението за виртуелизација ќе понуди и поддршка за хардверот што работи за закажаниот период на распоредување.

Еднообразни стандарди за конфигурација за виртуелни системи за информатичка технологија

Треба да се дефинираат еднообразни стандарди за конфигурација за користените виртуелни системи за информатичка технологија. Виртуелните системи за информатичка технологија треба да се конфигурираат во согласност со овие стандарди. Стандардите за конфигурација треба редовно да се прегледуваат и да се изменуваат доколку е потребно.

Работа на гостински оперативни системи со различни потреби за заштита

Доколку виртуелните системи за информатичка технологија со различни потреби за заштита работат заеднички на истиот сервер за виртуелизација, треба да се обезбеди дека виртуелните системи за информатичка технологија се доволно енкапсулирани и изолирани. Мрежното раздвојување на употребеното решение за виртуелизација треба да биде и доволно сигурно. Ако тоа не е случај, треба да се идентификуваат и да се применат дополнителни безбедносни заштитни мерки.

Енкапсулација на виртуелни машини

Функциите за копирање и прикачување на информации помеѓу виртуелни машини треба да бидат оневозможени.

Следење на работната состојба и конфигурација на виртуелната инфраструктура

Треба да се следи работната состојба на соодветната виртуелна инфраструктура. Меѓу другото, треба да се провери дали сè уште има доволно ресурси. Треба да се провери и дали има некакви конфликти со споделуваните ресурси на серверот за виртуелизација. Понатаму, треба да се обезбеди дека конфигурациските датотеки на виртуелните системи за информатичка технологија редовно се проверуваат за неовластени модификации. Треба да се следи и дали виртуелните мрежи се правилно доделени на виртуелните системи за информатичка технологија. Ако треба да се направат промени во конфигурацијата на инфраструктурата за виртуелизација, тие треба да се проверат и да се тестираат пред да се спроведат.

Редовни контроли на инфраструктурата за виртуелизација

Треба да се вршат редовни контроли за да се провери дали фактичката состојба на виртуелната инфраструктура соодветствува на состојбата што е дефинирана во планирањето. Воедно, треба да се вршат редовни контроли за да се провери дали конфигурацијата на виртуелните компоненти е во согласност со наведената стандардна конфигурација. Резултатите од контролите треба транспарентно да се документираат, а отстапувањата да се отстранат.

4.32.5 Напредни мерки

Користење архитектури со високо ниво на достапност

Виртуелните инфраструктури треба да бидат дизајнирани за високо ниво на достапност. Сите сервери за виртуелизација треба да се консолидираат во кластери.

Безбедно конфигурирање виртуелни системи за информатичка технологија за зголемени потреби за заштита

За виртуелни системи за информатичка технологија, треба да се оневозможат функциите за прекумерно искористување ресурси.

Зацврстување на серверот за виртуелизација

Серверот за виртуелизација треба да се зацврсти, а со цел дополнително да се изолираат и да се енкапсулираат виртуелните системи за информатичка технологија, меѓусебно и од серверот за виртуелизација, треба да се користат задолжителни контроли на пристап (MAC). Исто така, треба да се зацврсти системот за информатичка технологија на кој е инсталиран софтверот за управување.

Ограничување на правата на виртуелните машини

Сите интерфејси и комуникациски канали што овозможуваат виртуелен систем за информатичка технологија да бара и да добие информации за главниот систем, треба да бидат оневозможени или потиснати. Понатаму, само серверот за виртуелизација треба да има пристап до неговите ресурси. Виртуелните системи за информатичка технологија не треба да споделуваат страници од главната меморија.

Оневозможување слика на состојбата од виртуелни системи за информатичка технологија

Функцијата за слика на состојбата треба да биде оневозможена за сите виртуелни системи за информатичка технологија.

Минимална употреба на пристап до конзола до виртуелни системи за информатичка технологија

Директниот пристап до емулираните конзоли на виртуелните системи за информатичка технологија треба да се сведе на минимум. Виртуелните системи за информатичка технологија треба да се контролираат преку мрежата секогаш кога тоа е можно.

Употреба на инфраструктура со јавен клуч (PKI)

Инфраструктурата со јавен клуч (PKI) треба да се користи за комуникација заштитена со сертификат помеѓу компонентите на дадена инфраструктура за информатичка технологија.

Употреба на сертифициран софтвер за виртуелизација

Треба да се користи софтвер за виртуелизација што е сертифициран како EAL4 или на повисоко ниво.

Криптирање на виртуелни системи за информатичка технологија

Сите виртуелни системи за информатичка технологија треба да бидат криптирани.

Виртуелизација - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.32	Неправилно користење на овластување
3_0.37	Одредување на дејствија
3_0.40	Одбивање на услуга
3_0.43	Вметнување пораки
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.33 Лаптопи

4.33.1 Вовед

Лаптоп (исто така познат како пренослив компјутер) е персонален компјутер дизајниран за мобилна употреба. Има компактен дизајн, периферни уреди какви што се тастатура и монитор, батерии што го прават привремено независен од надворешно напојување и во многу случаи, хардверски компоненти што се специјално дизајнирани за мобилна употреба. Лаптопите широко се применуваат во повеќето организации и често го заменуваат традиционалниот десктоп-компјутер. Со лаптопите обично се управува со вообичаени десктоп оперативни системи какви што се Microsoft Windows, Apple macOS или Linux. Денес, границите помеѓу лаптопите и таблетите и слични уреди станаа многу мали. Некои таблети имаат десктоп оперативни системи како што е Windows 10, а додатоци за тастатура се достапни и за мобилни уреди како што е iPad, кои овозможуваат нивно користење како лаптопи. Бидејќи лаптопите често се користат и во движење, тие многупати не се трајно поврзани со локалната мрежа (LAN) на организацијата. Наместо тоа, тие обично можат да се поврзат со мрежата на организацијата со користење виртуелна приватна мрежа (VPN), вклучително и преку јавниот интернет. Инфраструктурата во традиционално канцелариско опкружување, кое има контролирани фактори на животната средина, стабилно напојување и ограничени области, не може да се претпостави за мобилна употреба на лаптопи.

4.33.2 Цел

Целта е да им се овозможи на организациите безбедно да користат лаптопи и да ги информираат вработените за специфичните закани за овој тип уреди.

4.33.3 Закани

Деградација поради променливите работни средини

Лаптопите се користат во голем број средини и затоа подложат на многу закани. Овие закани вклучуваат, на пример, оштетување на еколошките услови какви што се претерано високи или ниски температури, прашина и влага. Лаптопите може да се оштетат и при транспорт. Покрај тоа, лаптопите комуницираат со непознати системи за информатичка технологија или мрежи, особено додека се во движење, што секогаш претставува потенцијален ризик за уредот. Овде може да се пренесе злонамерен софтвер или да се копираат сензитивни информации (како на пример).

Кражба и губење на лаптопи

Вработените редовно ги користат своите лаптопи надвор од своите организации. Уредите се транспортираат во автомобили или во јавен превоз, се оставаат во канцелариите на други луѓе за време на паузите или се оставаат без надзор во хотелски соби. На тој начин, лаптопите се изложени на поголем ризик од кражба и може лесно да се заборават или да се изгубат. Ако лаптопот се изгуби, неговата замена вклучува трошоци и труд. Покрај тоа, податоците за кои не е направена сигурносна копија, исто така се губат. Неовластени лица може да пристапат и до сензитивни податоци, што може да доведе до дополнителна штета. Во многу случаи, ова е значително посериозно од материјалната загуба на лаптопот.

Нерегулирани промени на корисници на лаптоп

Ако на вработените им требаат мобилни системи за информатичка технологија само во исклучителни случаи, како, на пример, за повремени деловни патувања, честопати е попрактично повеќе корисници да споделуваат мал број лаптопи. Меѓутоа, ако лаптопот едноставно му се предаде на следниот вработен, постои ризик да се пренесат сензитивни податоци што сè уште се на уредот. Лаптопот може да биде заразен и со злонамерен софтвер. Без соодветни внатрешни процедури, може да биде тешко да се пронајде кој и кога го користел лаптопот или кој во моментот го користи.

4.33.4 Мерки

Правила за користење лаптоп

Аспектите што вработените мора да ги земат предвид кога користат лаптопи мора да бидат јасно дефинирани. Конкретно, мора да се наведат лаптопите што се достапни за мобилна употреба, кому му е дозволено да ги користи и кои основни безбедносни заштитни мерки треба да се следат. Корисниците мора да бидат известени за овие правила и истите да ги почитуваат и применуваат.

Користење лични заштитни сидови

На сите лаптопи мора да се активира личен заштитен сид, ако тие треба да се користат надвор од мрежата на организацијата. Правилата за филтер за лични заштитни сидови мора да се конфигурираат колку што е можно порестриктивно. Тие мора редовно да се тестираат. Личните заштитни сидови мора да се конфигурираат за да се избегне вознемирување на корисниците со предупредувања што не можат да ги протолкуваат.

Безбеден далечински пристап со лаптопи

Кога користат јавно достапни мрежи, корисниците мора да пристапуваат до внатрешната мрежа на организацијата само преку безбедни комуникациски канали.

Безбедносни упатства за лаптопи

Треба да се воспостават безбедносни политики што регулираат како може да се користат лаптопите. Корисниците треба да бидат свесни за потребите за заштита на лаптопите и на податоците што се зачувани на нив. Тие треба да бидат и свесни за специфичните закани и за соодветните барања за употреба. Покрај тоа, треба да бидат известени за видовите информации што можат да ги обработуваат на лаптопите.

Уредно задолжување и раздолжување (враќање) на лаптопите

Доколку различни лица наизменично користат исти лаптопи, треба да се утврдат безбедни методи за задолжување лаптопи на вработените. Треба да се регулира и нивното безбедно враќање односно раздолжување. Кога се менуваат корисниците на лаптопот, сите сензитивни податоци треба безбедно да се избришат. Ако лаптопот не се ресетира при промена на корисници, треба да се внимава да нема злонамерен софтвер на соодветниот систем за информатичка технологија или на кој било медиум за чување податоци поврзан со него. Кога вработениот се задолжува со лаптоп треба да добие и информативен лист за безбедно ракување со уредот.

Безбедно поврзување лаптопи со мрежи за пренесување на податоци

Треба да се дефинираат безбедни методи за поврзување лаптопи со внатрешни или со надворешни мрежи за пренесување на податоци и интернет. Само овластени лаптопи треба да можат да се најават на внатрешната мрежа на организацијата.

Синхронизација на зачувани податоци на лаптопите

Треба да се регулира начинот на кој податоците се пренесуваат од лаптопите до информативниот домен на организацијата. Ако се користи алатка за синхронизација, треба да се внимава да се обезбеди дека може да се решат конфликтите во синхронизацијата. Процесот на синхронизација треба да се евидентира. На корисниците треба да им се наложи и да ги проверат записите за синхронизација.

Обезбедување на напојување за лаптопи

Сите корисници треба да добиваат информации за тоа како најдобро да го гарантираат напојувањето на нивниот лаптоп за време на мобилната употреба. Резервните батерии треба да се чуваат и да се пренесуваат во соодветни кутии.

Пријавување изгубен лаптоп

Ако лаптопот е изгубен или украден, корисникот треба веднаш да го пријави тоа. Организацијата треба да има јасни канали за известување за таа цел. Ако се најде изгубениот лаптоп, треба да има истрага дали можеби имало манипулации со лаптопот. Софтверот што се користи на него, вклучително и оперативниот систем, треба целосно да се инсталира повторно.

Криптирање на лаптопи

Медиумите за чување податоци што се инсталирани во лаптопи, какви што се хард-дискони или SSD-дискони, треба да бидат криптирани.

Соодветно чување лаптопи

Сите корисници треба да бидат советувани за тоа како безбедно да ги чуваат лаптопите надвор од организацијата. Во зависност од нивото на заштита што е потребно за податоците што се зачувани на нив, лаптопите треба да бидат заштитени од кражба или да се чуваат на заштитена локација кога не се користат во просториите на организацијата.

Соодветен избор на лаптопи

Пред да се набават лаптопи, одговорните лица треба да извршат анализа на барањата на организацијата. Сите можни уреди треба да се проценат врз основа на резултатите. Одлуката за тоа кои лаптопи ќе се набават, треба да се договори со организационата единица за информатичка технологија.

4.33.5 Напредни мерки

Централно администрирање лаптопи

Организацијата треба да подготви и донесе процедура за централно администрирање на лаптопите. Алатката за централно управување со лаптопот, треба да ги поддржува сите оперативни системи што се користат во најголема можна мера.

Задничко чување лаптопи

Неискористените лаптопи треба да се чуваат во соодветно обезбедена просторија.

Употреба на уреди против кражба

Треба да се регулираат уредите против кражба што ќе се користат за лаптопи. Во контекст на механичките уреди, треба да се внимава да се обезбеди дека тие добро се заклучуваат.

Лаптопи - закани што се вклучени овде:	
3_0.4	Акумулирање нечистотии, прашина, корозија
3_0.14	Шпионажа
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.39	Злонамерен софтвер
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.34 Преносливи медиуми

4.34.1 Вовед

Преносливите медиуми често се користат за транспорт, за чување податоци или за пристап до податоци додека лицето е во движење. Преносливите медиуми вклучуваат надворешни хард-дискови, CD-ROM, ДВД-уреди, мемориски картички, магнетни ленти и USB преносливи дискови. Медиумите за чување податоци може да се класифицираат според тоа дали се само за читање, за запишување еднаш или за презапишување. Исто така, постојат разлики во видот на чување на податоците (аналогно или дигитално), достапните опции за обработка и формата на медиумот. На пример, има пренослив медиум за чување податоци (на пример, вградени хард-дискови) и надворешни медиуми за чување податоци (на пример, USB преносливи дискови).

4.34.2 Цел

Целта е да се опише како преносливите медиуми може да се користат на безбеден начин во организацијата и како да се спречи ненамерното откривање информации преку нив.

4.34.3 Закани

Негрижа при ракување со информации

Иако организациите често имаат внатрешни организациски процедури и процедури за техничка безбедност за преносливи медиуми, тие често се заобикојуваат со невнимателно ракување од страна на вработените. Преносливиот медиум може да се остави без надзор, на пример, во просторија за состаноци, за време на пауза.

Недоволно познавање правила и процедури

Доколку вработените не се соодветно запознаени со правилата за правилно ракување со преносливи медиуми, тие нема да можат да се придржуваат до нив. Ова создава голем број закани за безбедноста на информациите, на пример, ако непроверените USB-дискови се поврзани со системите за информатичка технологија на организацијата.

Кражба или губење пренослив медиум

Со пренослив медиум, ризикот од губење податоци е поголем отколку кај статични системи, бидејќи кај таквите медиуми е поголема веројатноста да бидат изгубени или украдени. Информациите за изгубениот медиум за чување податоци, често се неповратно изгубени. Оваа информација може да падне и во рацете на трети лица.

Неисправни медиуми за чување податоци

Преносливите медиуми се склони кон оштетување, грешки и дефекти поради нивната големина и области на примена. Постојано променливите работни средини и механичките влијанија се само дел од причините.

Деградација поради променливи работни средини

Преносливите медиуми се користат во голем број средини и затоа се изложени на многу закани. Ваквите закани вклучуваат штетни услови на животната средина какви што се претерано високи или ниски температури, како и прашина и влага. Штетите при пренесување се уште еден пример. Друг важен аспект е тоа што медиумите за чување податоци често се користат во области со различни нивоа на безбедност.

Ширење злонамерен софтвер

Преносливите медиуми често се користат за размена на податоци помеѓу различни уреди и различни работни места. Злонамерен софтвер може да ги компромитира податоците на преносливите медиуми и со тоа може да се прошири на системите на работното место во организацијата.

4.34.4 Мерки

Подигање на свеста на кадарот за безбедно ракување со преносливите медиуми

Сите вработени мора да бидат свесни за тоа како да ракуваат со преносливите медиуми на безбеден начин. Вработените мора посебно да се советуваат за тоа како да ракуваат со пренослив медиум за да се спречи загуба и кражба и да се обезбеди долг рок на употреба на медиумот. Организацијата мора да ги извести своите вработени дека не смеат да поврзуваат пренослив медиум од непознати извори со нивните системи.

Пријавување загуби/манипулации

Корисниците мора веднаш да пријават пренослив уред за чување податоци што бил украден или станал сомнителна цел на манипулација. Во таквите извештаи, корисниците мора да ги наведат информациите што се зачувани на уредот. За оваа намена, треба да има јасни правила за известување и лица за контакт во секоја организација.

Криптирање на медиум за чување податоци

Доколку пренослив медиум се користи или се пренесува надвор од безбедна област и содржи доверливи податоци, медиумот мора да се криптира со безбеден метод.

Заштита од злонамерен софтвер

Податоците мора да се проверат за потенцијално присуство на злонамерен софтвер пред да се префрлат на пренослив медиум. Податоците од преносливиот медиум исто така мора да се скенираат за присуство на злонамерен софтвер пред да бидат обработени.

Подготовка на политика за безбедно ракување со преносливи медиуми

Организацијата треба да воспостави политика за правилно ракување со преносливите медиуми и при донесување на истата треба да се земат предвид следниве основни аспекти:

- Кои преносливи медиуми може да се користат и од кого,
- Кои податоци може да се зачуваат на пренослив медиум,
- Како податоците што се зачувани на пренослив медиум ќе бидат заштитени од неовластен пристап, манипулација и губење,
- Како треба да се избришат податоците на преносливите медиуми,
- Дали и како е дозволено да се користи приватен медиум за чување податоци,
- Надворешните вработени или давателите на услуги со кои може да се разменуваат медиуми за чување податоци и кои безбедносни прописи треба да се почитуваат,
- Како треба да се испраќаат медиуми за чување податоци,
- Како да се спречи ширењето на злонамерен софтвер преку пренослив медиум.

Организацијата во својата безбедносна политика треба да ги прецизира и условите во кои треба да се чуваат медиумите за чување податоци, при што поконкретно да наведе дека само овластени корисници имаат пристап до тие медиуми. Истовремено, треба да наведе дека треба да се земат предвид и упатствата на соодветните производители за ракување со медиумите. Организацијата треба да врши редовни проверки за да обезбеди дека безбедносните спецификации за ракување со преносливи медиуми сè уште се ажурирани.

Правила за пренесување на преносливи медиуми

Организацијата треба да има воспоставени јасни пишани правила за тоа дали, како и во кои околности може да се пренесуваат преносливите медиуми. Тие треба да прецизираат кои медиуми може да се пренесат од локацијата, од кого и кои безбедносни заштитни мерки треба да се почитуваат.

Управување со медиуми за чување податоци

Организацијата треба да воспостави процедури за управување со преносливи медиуми. Медиумите за чување податоци треба да се означуваат на еднообразен начин. Концептот за управување со медиум за чување податоци треба да обезбеди дека со преносливите медиуми соодветно се ракува, соодветно се чуваат и се користат, како и правилно се пренесуваат.

Безбедно бришење медиум за чување податоци пред и по употреба

Пред да се пренесат, повторно да се користат или да се отфрлат, медиумите за повеќекратно снимање треба да се избришат на соодветен начин.

Соодветно означување на медиумот за чување податоци за испорака

Корисниците треба да ги означат медиумите за чување податоци што ќе бидат испратени така што испраќачот и примачот веднаш ќе можат да ги идентификуваат. Означувањето на медиумите или нивното пакување треба да биде недвосмислено за примачот. Означувањето на медиумите за чување податоци што содржат сензитивни информации треба да обезбеди дека трети лица не можат да извлечат никакви заклучоци во врска со видот или со содржината на информациите.

4.34.5 Напредни мерки

Заштита на интегритетот со користење контролни суми или дигитални потписи

Треба да постои постапка за заштита од случајни или од намерни измени и со тоа да се обезбеди интегритет на доверливите информации. Процедурите што се дизајнирани да спречат такви промени треба да се усогласат со најсовремените технолошки достигнувања.

Безбедна испорака и пакување

Организацијата треба да примени мерки како доверливите информации можат да бидат соодветно заштитени за време на испораката. Корисниците треба да користат безбеден материјал за испорака за медиум за чување податоци што го прави манипулирањето веднаш видливо. Испраќачот треба да ги извести сите вклучени вработени за потребните видови испорака и пакување.

Сертифицирани производи

Организацијата треба да користи само преносливи медиуми што се сертифицирани. При ваквото сертифицирање, особено треба да се земе предвид можноста на даден медиум да го зачува интегритетот на податоците и секое криптирање што може да постои.

Употреба на наменски системи за скенирање податоци

Организацијата треба да користи наменски системи какви што се механизми за заклучување на податоците во кои податоците се пренесуваат од еден на друг пренослив уред за чување податоци и се скенираат за злонамерен софтвер.

Преносливи медиуми - закани што се вклучени овде:	
3_0.2	Неповолни услови во околината
3_0.4	Акумулирање нечистотии, прашина, корозија
3_0.14	Шпионажа
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.29	Повреда на закони или на договори
3_0.39	Злонамерен софтвер
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.35 Паметни телефони и таблети

4.35.1 Вовед

Паметните телефони се системи за информатичка технологија што се дизајнирани за мобилна употреба и имаат приспособен интерфејс со кој се управува преку голем екран, кој обично е чувствителен на допир. Покрај телефонијата, паметните телефони комбинираат својства на мултимедијален изведувач (media player), управување со лични информации и дигитална камера во еден уред, а на корисниците им нудат и многу други апликации и функции, какви што се прелистување мрежа, пристап до е-пошта и локација (на пример, преку GPS). Тие се опремени со интерфејси за мобилни мрежи, WLAN, Bluetooth и NFC. Едноставно кажано, таблетите се паметни телефони со голем облик, кои обично не можат да воспоставуваат телефонски повици преку мобилни мрежи.

4.35.2 Цел

Целта е да им се обезбедат информации на лицата што се задолжени за управување со безбедноста и со операциите за информатичка технологија за типичните закани за паметните телефони и за таблетите, како и за барањата што треба да се исполнат за да се избегнат или да се отстранат овие закани. Понатаму, целта е на одговорните лица да им се дадат пристапи за изготвување конфигурациски профили во согласност со достапните потреби за заштита. Овие конфигурациски профили може да се дистрибуираат и да се управуваат со користење централна инфраструктура и систем за управување со мобилни уреди (MDM). Сепак, со оглед на големиот број различни мобилни оперативни системи, главно не може да се претпостави дека мобилните уреди можат да се интегрираат во систем за управување со мобилни уреди (MDM).

4.35.3 Закани

Недостаток на ажурирања на оперативниот систем

Новите верзии и ажурирања на мобилните оперативни системи редовно се објавуваат. За уреди со екстензии што се специфични за производителот на нивните соодветни оперативни системи, производителите мора прво да ги интегрираат овие екстензии во нивните верзии пред да продолжат со дистрибуцијата. Обично се обезбедуваат ажурирања за најновата генерација уреди и за голем број постари генерации уреди. Сепак, сите претходни верзии на оперативниот систем не се испорачуваат со безбедносни ажурирања до ист степен. Во одредени случаи, оперативните системи не се дополнително развиени од економски причини. Потоа, недостатоците на оперативниот систем од генерацијата уреди што е прекината, повеќе не може да се затворат со ажурирања, што ги прави особено лесни за искористување од напаѓачите.

Софтверски недостатоци во однапред инсталирани апликации

Однапред инсталираните апликации може да вклучуваат и недостатоци што може да се искористат за локални напади или за напади преку мрежни врски. Понатаму, многу апликации од развојни програмери од трети лица повеќе не се одржуваат откако ќе помине одредено време. Како последица на тоа, идентификуваните безбедносни недостатоци повеќе не може да се поправат со соодветни ажурирања.

Манипулација со паметни телефони и таблети

Напаѓачот може да добие пристап до паметни телефони или до таблети со цел насочено да манипулира со датотеките. На пример, напаѓачот би можел да менува конфигурации, да започне дополнителни услуги или да инсталира злонамерен софтвер. Така, напаѓачот може да прислушува комуникациски врски на манипулиран систем што доведува до несакано протекување податоци или да ги менува безбедносните правила за да одговараат на неговите потреби, на пример, да се овозможи пристап од интернет до целниот краен уред.

Злонамерен софтвер за паметни телефони и за таблети

Како и секој уред поврзан на интернет, така и мобилните уреди може да бидат заразени со злонамерен софтвер. Во споредба со оперативните системи на клиентот како што е Microsoft Windows, ризикот за зараза е помал, но напаѓачите сè повеќе се концентрираат на мобилни уреди. Особено, ако апликациите се добиени од недоверливи извори или не се достапни ажурирања за познати пропусти, постои ризик за зараза. Ако уредот е заразен, напаѓачите можат (на пример) да извлечат, да менуваат или да бришат податоци, да пристапат до внатрешните ресурси за информатичка технологија на организацијата, или да дејствуваат во име на сопственикот (вработениот) или организацијата.

Напади на мобилни прелистувачи засновани на мрежа

Мобилните прелистувачи, заедно со многу други апликации, можат да прикажуваат веб-локации и веб содржини. На тој начин, мобилните уреди може да бидат погодени од напади на кражба на идентитетот, придружни искористувања и други форми на напад засновани на мрежа.

Злоупотреба на податоци за здравје, физичката подготвеност или локација

Оперативните системи на многу паметни телефони и таблети вклучуваат специфични својства за управување со податоци за здравјето, физичката подготвеност и локацијата. Овие лични податоци претставуваат привлечна цел за напад и се особено сензитивни ако се собираат и се чуваат во текот на подолг временски период. За да се случи тоа, корисникот прво мора да ги активира таквите функции.

Ова може да овозможи, на пример, да се идентификува локацијата на вработениот (на пример) со напад на неговиот уред или на услугите за „облак“ поврзани со уредот. Покрај импликациите за заштита на податоците, ова може да доведе до дополнителни напади под одредени околности. Компромитираните податоци за локацијата може да откријат, на пример, дека некој вработен патува на службено патување и може да го изложат домот на вработениот на упад.

Злоупотреба на сензитивни податоци на заклучениот екран

Многу мобилни оперативни системи се опремени со функција што овозможува приказ на поттикнатите пораки од апликациите и пораките од активирани уреди на заклучениот екран. Така, доверливите информации на корисникот може да бидат откриени и искористени од неовластени трети лица. Исто така, може да се користат гласовни асистенти за пристап до телефонските функции и податоците за контакт дури и кога уредот е заклучен. Ова исто така може да дозволи неовластени трети лица да пристапат до сензитивни информации. Покрај тоа, често е можно да се конфигурираат интерфејси какви што се WLAN или Bluetooth дури и кога уредот е заклучен. Напаѓачот со физички пристап до уред може да отвори дополнителен вектор на напад, на пример, со активирање на Bluetooth интерфејсот на уредот.

Опасности од приватна употреба на службени паметни телефони и таблети

Кога вработените приватно ги користат паметните телефони и таблетите на организацијата, тоа веднаш создава неколку проблеми за безбедноста на информациите на таа организација. На пример, корисникот може самостојно да инсталира апликации што содржат злонамерни функции или да посети веб локација што го инфицира неговиот уред со злонамерен софтвер. Многу апликации што се инсталирани приватно од корисниците, исто така претставуваат ризик за информациите на организацијата што се зачувани на нивните уреди бидејќи тие можат да пристапат до адресарите и да ги испраќаат на непознати сервери или да добијат директен пристап до е-пошта или до документи. Ова може да доведе до протекување податоци или неконтролирано внесување податоци во организацијата. Типични примери на апликации што создаваат такви ризици се оние што се користат за социјални медиуми и за брзо испраќање пораки во реално време.

Закани во врска со сценарија „донесете го вашиот сопствен уред (BYOD)“

Ако приватните крајни уреди се користат за потребите на работата, тоа води до голем број потенцијални ризици. На пример, може да се појават правни проблеми во врска со софтверските лиценци. Доколку, во итен случај, податоците во врска со работата треба да се избришат од уредот преку соодветниот систем за MDM, тоа може да влијае и врз приватните податоци на корисникот. Покрај тоа, лицата за информатичка технологија не можат да го проверат секој приватен уред за да видат дали ги исполнува барањата на организацијата. Ова значи дека може да се користат уреди со кои корисниците може да ги прекршат барањата за заштита на податоците и безбедноста. Понатаму, корисниците честопати се лично одговорни за сервисирање и поправка на своите уреди. За време на таквите поправки, на пример, податоците на организацијата ќе се гледаат без овластување. Истата закана постои ако организацијата не регулира што треба да се прави со податоците на уредите на вработените што ја напуштаат.

Проширени права преку недостатоци

Постојано се откриваат недостатоци во оперативните системи на паметните телефони и на таблетите што имаат овозможено да се заобиколи безбедносниот концепт воспоставен од производителот и на тој начин да се пристапи до системските процеси и до заштитените мемориски области. Ова им овозможува на програмите да добијат ненамерни овластувања со кои можат да вршат неовластени дејства. На пример, на тој начин програмите би можеле да пристапат до податоците на оперативниот систем и до другите апликации.

„Отстранувањата на ограничен режим на работа“ ги искористуваат овие недостатоци како средство за користење алтернативни продавници за апликации или други екстензии. Техниките за отстранувањата на ограничен режим на работа може да ги користат и напаѓачите за да инсталираат злонамерен софтвер или да вршат други штетни манипулации на уредот. Покрај тоа, злонамерниот софтвер може да ги искористи недостатоците за да се инсталира на уред или да манипулира со него. Како резултат на тоа, оперативниот систем може да се користи за различна намена од предвидената, а важните безбедносни функции може да се заобиколат.

Податоците што се зачувани од мобилниот оперативен систем во заштитените области се особено погодени, бидејќи апликацијата со права на супер корисници може да ги извлече податоците. Намерните активности за добивање права на повисоко ниво („искоренување“) може да создадат слични сценарија за закана доколку пристапот до привилегираните права не е заштитен.

4.35.4 Мерки

Дефинирање политика за користење паметни телефони и таблети

Пред организацијата да ги обезбеди паметните телефони или таблети, да управува со нив или да ги користи, мора да дефинира општа политика за користење и контрола на таквите уреди. Притоа, меѓу другото, мора да се утврди кој може да пристапи до конкретни информации во организацијата со користење паметни телефони.

Изготвување стратегија за користење „облак“

Организацијата мора да дефинира општа политика за користење „облак“ и заштита и контрола на информациите во врска со паметните телефони и таблети. Дозволената употреба на услуги за „облак“ во врска со информациите на организацијата мора да се разјасни и да се дефинира. Мора да се утврди дали и до кој степен „облак“ услугите се дозволени за приватна употреба на уредите. Корисниците мора редовно да добиваат информации за прашањата во врска со користењето на таквите услуги за „облак“.

Безбедна основна конфигурација за мобилни уреди

Сите мобилни уреди мора да се конфигурираат за да го исполнуваат потребното ниво на заштита. За таа цел, мора да се воспостави и да се документира соодветна основна конфигурација на безбедносните механизми и поставки. Функциите што не се потребни, треба да се оневозможат. Активирањето на комуникациските интерфејси мора да се регулира и да се сведе на минимумот што е потребен за целите поврзани со работата. Неискористените интерфејси треба да се оневозможат.

Употреба на механизам за контрола на пристап

Паметните телефони и таблетите мора да бидат заштитени со соодветно сложена лозинка/код за заклучување на уредот. Мора да се користи заклучување на екранот. Мора да се оневозможи приказот на доверливите информации на заклучените екрани. Сите мобилни уреди мора автоматски да го активираат заклучувањето на екранот по разумно краток временски период. Овој временски период мора да биде поврзан со потребното ниво на заштита. По секој неуспешен обид за отклучување уред, корисникот треба да чека подолго пред да се обиде повторно. Треба да биде наведен бројот на заклучување на уредот по кои може да се повтори лозинката/кодот. По неколку неуспешни обиди за отклучување на екранот на мобилниот уред, уредот треба да изврши фабричко ресетирање. Податоците или криптираните кодови треба безбедно да се избришат во овој процес. Кога ги менуваат своите лозинки/кодови, корисниците треба да избегнуваат да изберат нова лозинка/код што го користеле неодамна.

Ажурирања на оперативниот систем и на апликациите

При изборот на мобилни уреди што ќе се набават, организацијата мора да се погрижи производителот да го прецизира временскиот период за кој планира да обезбеди безбедносни ажурирања за уредите. Постарите уреди што повеќе не се обезбедени со ажурирања, мора да се отстранат и да се заменат со уреди што се поддржани од соодветниот производител. Освен тоа, апликациите не треба да се користат доколку повеќе не се поддржани од производителот.

Поставки за приватност и овластувања

Пристапот до податоците и до интерфејсите на апликациите и на оперативниот систем мора да биде соодветно ограничен. Поврзаните поставки за заштита на податоците мора да се конфигурираат колку што е можно порестриктивно. Особено, мора да се провери пристапот до камерата, микрофонот, локацијата и до податоците за здравјето односно физичката подготвеност, за да се утврди дали соодветствува на внатрешните барања за заштита на податоците и безбедност на организацијата. Овој пристап мора рестриктивно да се конфигурира или да се оневозможи. Поставките за авторизација што се значајни за безбедноста мора да се постават така што корисниците или апликациите не можат да ги менуваат. Ако тоа не е технички можно, поставките за овластување мора редовно да се проверуваат и да се ресетираат. Конкретно, ова мора да се направи откако ќе се инсталираат ажурирањата.

Кодекс на однесување во случај на безбедносни инциденти

Доколку уредите се изгубат или се откријат неовластени промени на уредите и на нивниот софтвер, соодветните корисници мора веднаш да ги известат одговорните лица во организацијата.

Инсталирање апликации

Организацијата мора да регулира дали, како и кои апликации корисниците смеат да ги инсталираат на своите уреди. На корисниците треба да им биде дозволено да инсталираат само одобрени апликации. Организацијата мора да ги дефинира изворите од кои може да се инсталираат апликациите. Инсталирањето апликации од неodobрени извори, мора да се спречи.

Рестриктивна употреба на функционални екстензии

Функционалните екстензии треба да се користат само рестриктивно. Доколку е можно, функционалните екстензии воопшто не треба да се користат. Функционалните екстензии не треба да имаат никаков автоматски пристап до сензитивни информации. Тие не треба да можат да ги заобиколат или да ги менуваат наведените основни конфигурации.

Политика за вработените во однос на употребата на мобилни уреди

Организацијата треба да воспостави политика за вработените за користење мобилни уреди. Оваа политика треба да дефинира како ќе се користат и одржуваат мобилните уреди и треба да ги решава прашањата за безбедно чување и известување за губење односно кражба. Воедно, треба да им забрани на корисниците да деинсталираат софтвер за управување, да извршат рутирање односно насочување на своите уреди или да ги менуваат конфигурациите во врска со безбедноста.

Криптирање

Постојаната меморија за податоци на мобилните уреди треба да биде криптирана. Сензитивните податоци на дополнителни медиуми за чување податоци што се користат (какви што се SD картички) треба да бидат криптирани.

Употреба на неперсонализирани имиња на уреди

Имињата на уредите не треба да вклучуваат никакви информации во врска со соодветните корисници или организацијата.

Правила за споделување и емитување екран

Организацијата треба да донесе одлука дали и како функциите треба да се користат за пренос на содржина на екранот и аудио или видео содржина (споделување екран или емитување). Овие функции треба да бидат регулирани од организациски или од технички аспект. За таа цел, треба да се склучи соодветен договор со корисниците.

Оневозможување неискористени комуникациски интерфејси

Комуникациските интерфејси треба да се активираат само кога е потребно и во соодветни средини. Ако се користи систем за MDM, интерфејсите треба да се управуваат централно преку овој систем.

Употреба на биометриска автентикација

Доколку се користи биометриска процедура за автентикација (на пример, врз основа на сензор за отпечатоци), треба да се провери дали може да се постигне слично високо ниво на заштита или повисоко ниво на заштита во споредба со користењето лозинка на уредот. Ако ова е нејасно или ако нивото на заштита е пониско, биометриската процедура не треба да се користи. Корисниците треба да бидат свесни дека биометриските карактеристики може да се фалсификуваат.

Употреба на гласовен асистент

Гласовните асистенти треба да се користат само кога се неопходни. Во спротивно, треба да бидат оневозможени. По правило, не треба да биде можно да се користи гласовен асистент кога уредот е заклучен.

Интегрирање мобилни уреди во внатрешната инфраструктура преку виртуелна приватна мрежа (VPN)

Мобилните уреди треба да се интегрираат во инфраструктурата на организацијата само преку виртуелна приватна мрежа (VPN). За таа цел треба да се избере и да се употреби соодветен метод. Наместо лозинки, уредите треба да извршат автентикација на внатрешната инфраструктура преку сертификати.

Користење на опцијата за филтер за веб локации

Доколку организацијата веќе користи услуга за углед (reputation service) или соодветен посреднички (прокси) сервер, оваа услуга или сервер треба да се зачува како глобален HTTP посреднички (прокси) сервер за сите инсталирани прелистувачи што се користат. Ако таков посреднички (прокси) сервер е достапен само во рамките на внатрешната мрежа, крајните уреди треба да се интегрираат (трајно или врз основа на користените апликации) со користење VPN конекција. Доколку мобилните уреди не се интегрирани во постојниот посреднички (прокси) сервер или инфраструктура за углед на организацијата, за веб прелистувачи треба да се користат опции за филтрирање врз основа на бела или црна листа или филтри за содржина од трето лице.

Политика за мобилни плаќања

Организацијата треба да регулира дали се дозволени мобилни плаќања со паметни телефони и таблети што се користат за потребите на работата.

Употреба на управување со мобилни уреди MDM

Паметните телефони и таблетите треба да се управуваат од систем за управување со мобилни уреди (MDM).

Избор и инсталирање апликации за безбедност

Сите мобилни крајни уреди треба да бидат заштитени од злонамерен софтвер. Ако е можно, треба да се избераат соодветни апликации за безбедност за крајните уреди. Апликациите за безбедност треба да се инсталираат автоматски, како на пример, преку систем за управување со мобилни уреди (MDM).

Употребена конфигурација на DNS серверот

Стандардните внесувања на портата, како што се DNS серверите на производителот или развојниот програмер за кој станува збор, треба да се заменат со оние на давателот или на организацијата. Ако давателот на услуги нуди DNS-over-HTTPS (DoH), ова треба да се користи. Ако ова сè уште не е понудено, треба да се оневозможи.

4.35.5 Напредни мерки

Употреба на посебни работни средини

Ако на вработените им е дозволено да користат службени уреди и приватно, на овие крајни уреди треба да се користат решенија за изолирани работни средини. Ако е можно, за оваа намена треба да се купат само сертифицирани производи (на пример, оние во согласност со заедничките критериуми). Податоците во врска со работата треба да останат исклучиво во опкружувањето на организацијата.

Употреба на пакети за управување со привилегиран идентитет

Информациите за мобилните уреди треба да бидат енкапсулирани (на пример, во пакет за управување со привилегиран идентитет). Покрај тоа, овие податоци треба да бидат обезбедени со посебна автентикација и форма на криптирање податоци и пренесување што е независна од оперативниот систем што се користи во организацијата.

Употреба на специјално обезбедени крајни уреди

Во зависност од прифатените потреби за заштита, организацијата треба да користи специјално обезбедени мобилни уреди, кои се сертифицирани за обработка на информации во согласност со прописите од областа за заштита на информации.

Употреба на име за пристапна точка (APN) во врска со организацијата

Треба да се провери дали пристапната точка до мобилните мрежи во врска со организацијата (име на пристапна точка, APN) може да се користи за ограничување на групата дозволени уреди. Давателот на мобилни услуги треба да додели опсег на IP-адреси, кој е координиран со организацијата за сите уреди што го користат ова APN. За автентикација, со давателот на мобилната услуга треба да се договори сложена лозинка со најмалку 32 карактери, односно најмногу 64 карактери. При користење на APN во врска со организацијата, автентикацијата треба да се одвива врз основа на CHAP-протоколот.

Ограничена инсталација на апликација со користење бела листа

Во случај на зголемени потреби за заштита, корисниците на мобилни крајни уреди треба да можат да инсталираат само одобрени и тествани апликации. Ако се користи систем за MDM, тој треба да спречи инсталирање други апликации, а алтернативно, системот за MDM веднаш треба да ги отстрани апликациите што се инсталирани без овластување.

Употреба на заштитен сид

Треба да се инсталира и да се активира заштитен сид на паметните телефони и таблети.

Паметни телефони и таблети - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.20	Информации од несигурни извори
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.24	Уништување уреди или медиуми за чување податоци
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одрекување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.39	Злонамерен софтвер
3_0.42	Социјален инженеринг
3_0.43	Вметнување пораки
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.36 Управување со мобилни уреди

4.36.1 Вовед

За многу вработени, паметните телефони и таблетите станаа незаменлив дел од нивната работа. Сепак, организационата единица за информатичка технологија треба да обезбедат уште поголем број такви уреди со многу различни дизајни, истовремено обезбедувајќи соодветна безбедност. Покрај тоа, мобилните уреди се изложени на одредени ризици и нивното администрирање се разликува во суштински аспекти од другите системи за информатичка технологија. Следствено на тоа, системот за управување со мобилни уреди (MDM) има суштинско значење за регулирано и безбедно работење на овие уреди, особено во организации со голем број паметни телефони, и таблети. Со соодветен софтвер за управување со мобилни уреди, со крајните уреди може да се управува централно, може да се имплементираат безбедносни прописи и може да се активираат постапки за итни ситуации. Така, системот за управување со мобилни уреди обезбедува конзистентен (или барем споредлив) безбедносен стандард за сите администрирани уреди.

4.36.2 Цел

Целта е да се опише како организацијата може да ја обезбеди употребата на мобилни уреди преку системот за управување со мобилни уреди (MDM) и да обезбеди информации за работата.

4.36.3 Закани

Недоволна синхронизација со системот за управување со мобилни уреди (MDM)

За да може системот за управување со мобилни уреди (MDM) да ги имплементира прописите што се дефинирани од одговорните лица на мобилните уреди, уредите мора редовно да се синхронизираат со системот за MDM. Ако уредот не е поврзан со системот за MDM подолг временски период, на пример, може да не се инсталираат нови или ажурирани прописи. Покрај тоа, ако нема врска со изгубениот уред, податоците на него повеќе не можат далечински да се избришат.

Неправилно администрирање на управувањето со мобилни уреди

Решенијата за управување со мобилни уреди (MDM) се сложени апликации, кои обично имаат неколку стотици различни правила. Сите правила не можат меѓусебно да се комбинираат, додека некои, пак, зависат едни од други. Поради административни грешки, крајните уреди може да бидат изложени на голем број закани, кои имаат директно или индиректно влијание врз доверливоста, достапноста или интегритетот на податоците и апликациите.

Несоодветно управување со правата во системите за управување со мобилни уреди

Компонентата за управување со правата на системот за управување со мобилни уреди (MDM) одлучува кои корисници можат да конфигурираат конкретни поставки на мобилните уреди и кој може да пристапи до конкретни податоци. Ако на вработениот му се додели погрешна улога, постои ризик да му бидат доделени права на повисоко ниво од потребното. На пример, вработениот би можел да гледа податоци без овластување или да ги менува поставките на својот уред. Воедно, би било можно да инсталира и да користи апликации (или услуги за складирање на „облак“, на пример) кои не се овластени во организацијата. Ова може да доведе до протекување на сензитивните податоци на организацијата или до непочитување на прописите за заштита на личните податоци.

Неовластено креирање профили за движење преку системот за управување со мобилни уреди (MDM)

Кај повеќето производи за управување со мобилни уреди, можно е да се одреди каде се наоѓа уредот, а тоа може да се користи како основа за дозволување или за блокирање пристап до податоци или апликации (geofencing/гео-оградување). Ова доведува до детални профили за движењето за уредите, а со тоа и за нивните корисници. Доколку овие податоци се прибираат без соодветно информирање на корисниците, во одредени околности, одговорните лица можат да ги прекршат прописите за заштита на личните податоци. Исто така постои ризик напаѓачите да пристапат до овие податоци. Гео-оградувањето може да се злоупотреби и за незаконско следење на вработените.

4.36.4 Мерки

Утврдување стратегија за управување со мобилни уреди

Организацијата мора да развие стратегија што одредува како нејзините вработени можат да користат мобилни уреди и како уредите треба да се интегрираат во нејзините структури за информатичка технологија. Во овој поглед, мора суштински да се согледаат потребите за заштита на информациите што треба да се обработат. Стратегијата мора да ги опфати најмалку следниве аспекти:

- Дали системот за управување со мобилни уреди (MDM) може да работи како услуга за „облак“?
- Дали со системот за MDM треба да управува самата организација?
- Дали системот за MDM треба да ги обезбеди сите потребни апликации или корисниците можат сами да инсталираат апликации? Какви ограничувања сака да наметне организацијата на апликациите што ги обезбедува или на оние што се инсталирани од корисниците?
- Дали системот за MDM треба да се интегрира во поширока инфраструктура?
- Кои услови/барања за поддршка и одговор треба да ги исполни давателот на MDM?
- Кои услови/барања за усогласеност мора да се имплементираат?
- Кои мобилни уреди и кои оперативни системи треба да ги поддржува системот за MDM?
- Дали решението MDM треба да биде соодветно за повеќе клиенти? Дали го гарантира неопходното одвојување на клиентите?
- Дали услугите за „облак“ треба да се инкорпорираат?
- Дали треба да се вградат системи за управување со документи?
- Дали системот за MDM треба да вградува и да управува и периферни уреди?
- Што ќе вклучува оперативниот модел: приватни крајни уреди („донесете свој уред“, BYOD), персонализирани крајни уреди (сопственост на организацијата) или неперсонализирани крајни уреди (сопственост на организацијата и заеднички користени)?

Стратегијата мора да се прецизира во писмена форма и да биде одобрена од овластеното лице за безбедност на информации.

Дефинирање дозволени мобилни уреди

Организацијата мора да ги наведе мобилните уреди и оперативните системи што се дозволени. Сите овластени уреди и оперативни системи мора да ги задоволуваат барањата на стратегијата за MDM и целосно да се усогласат со безбедносните барања на организацијата. Системот за MDM на организацијата мора да биде конфигуриран така што само одобрените уреди можат да пристапат до нејзините информации. Набавката на мобилни уреди мора да биде ограничена на оние што се одобрени од организацијата.

Избор на производ за MDM

Кога треба да се купи соодветен софтвер за MDM, мора да се внимава да се обезбеди дека ги задоволува сите барања што се наведени во стратегијата за MDM во организацијата. Исто така, мора да може да ги имплементира сите потребни технички и организациски безбедносни заштитни мерки и да ги поддржува сите дозволени мобилни уреди.

Дистрибуција на основната конфигурација на мобилни уреди

Сите мобилни уреди мора да се интегрираат во системот за MDM пред да се користат. Кога уредите ќе ја добијат основната конфигурација, мора да бидат поставени на фабрички поставки. Врската помеѓу мобилните уреди и системот за MDM мора да биде соодветно обезбедена. За уредите што веќе се користат, мора прво да се избришат сите податоци во врска со организацијата. Крајниот уред што не е конфигуриран преку системот за MDM, не смее да има пристап до информациите на организацијата.

Инсталирање на клиентот за MDM

Кога мобилните уреди им се предаваат на вработените, на нив мора да биде инсталиран и конфигуриран клиент за MDM, ако веќе не е обезбеден од оперативниот систем што се користи.

Редовен преглед на системот за MDM

Поставките за безбедност мора редовно да се проверуваат. За новите верзии на оперативниот систем на мобилни уреди, мора однапред да се провери дали системот за MDM што се користи целосно ги поддржува и дали конфигурациските профили и безбедносните поставки сè уште се ефективни и доволни. Отстапувањата мора да се коригираат. Правата за пристап што им се доделени на корисниците и на администраторите, мора редовно да се проверуваат за да се обезбеди дека тие сè уште се потребни (начело за минималност).

Евидентирање на статусот на уредот

Животниот циклус на мобилниот уред (вклучувајќи ја неговата историја на конфигурација) треба да биде доволно евидентиран и централно обновлив. Доколку е потребно, администраторот треба да може да го одреди моменталниот статус на управуваните уреди (контрола на уредот).

Инсталирање апликации

Апликациите треба да се инсталираат, да се деинсталираат и да се ажурираат преку користениот систем за MDM во согласност со барањата на планираното сценарио за распоредување на организацијата. Системот за MDM треба да го поттикне процесот на инсталација, деинсталација и ажурирање веднаш штом ќе се воспостави врска со мобилен уред. Корисниците не треба да можат да деинсталираат апликации што се инсталирани преку системот за MDM. Системот за MDM треба да поддржува црна листа или бела листа за инсталација на апликации.

Заштита на работната средина за MDM

Користениот систем за MDM треба сам по себе да биде обезбеден со помош на технички заштитни мерки за да се задоволат потребите за заштита на информациите што ги зачувува или ги обработува. Основниот оперативен систем треба да се зацврсти.

Администрирање сертификати

Сертификатите за користење услуги на мобилни уреди треба да се инсталираат, да се деинсталираат и да се ажурираат централно преку користениот систем за MDM. Инсталирањето несигурни и неверификувани (коренски) сертификати што не може да се проверат од страна на корисниците, треба да се спречи од системот за MDM. Системот за MDM треба да поддржува механизми што ја потврдуваат валидноста на сертификатите.

Бришење од далечина и деактивирање на крајните уреди

Системот за MDM кој го користи организацијата треба да обезбеди дека сите податоци на мобилните уреди може да се избришат од далечина (бришење од далечина за постојните конекции за податоци). Ако се користат надворешни уреди за зачувување во мобилен уред, системот треба да провери дали и тие треба да се избришат од далечина. Оваа функција треба да биде поддржана од системот за MDM. Процесот за деактивирање мобилни уреди (одјавување), треба да обезбеди дека нема да останат сензитивни податоци на уредите или на нивните интегрирани медиуми за зачувување податоци. Ова особено треба да важи ако одјавувањето е потребно да се изврши од далечина.

4.36.5 Напредни мерки

Користење надворешни услуги за углед за апликациите

Доколку администраторите на организацијата не можат да ги изберат дозволените апликации и корисниците можат сами да инсталираат апликации на нивните уреди, тогаш треба да се користи услуга за углед. Користениот систем за MDM потоа треба да користи информации од услугата за углед најмалку за да ја ограничи инсталацијата на апликациите.

Следење на употребата на мобилни уреди

Организацијата треба да дефинира критериуми и тие треба да се користат како основа за уреди за следење без да се прекршуваат законските или внатрешните прописи. Конкретно, треба да се препознаат отстранувањата на ограничен режим на работа и обидите за добивање пристап до коренот.

Користење гео-оградување

Политиката за гео-оградување треба да обезбеди дека уредите со сензитивни информации не можат да се користат надвор од однапред определена географска област. Ако корисникот ја напушти оваа област, информациите што се назначени за бришење на неговиот уред (или самиот уред) треба целосно да се избришат. Пред селективно или целосно да се избрише уредот, треба да бидат известени одговорните администратори, лицата за управување со безбедност и корисникот. Уредот треба да се брише селективно или целосно по соодветно временско одложување и треба да се идентификуваат областите во кои се неопходни овие дополнителни безбедносни заштитни мерки. Безбедносните заштитни мерки потоа треба да се спроведат во согласност со релевантните законски и внатрешни прописи.

Спроведување на барања за усогласеност

Непочитувањата на прописите на организацијата и манипулацијата со оперативните системи на уредите, треба да се откријат со соодветно решение. Доколку постои сомневање за непочитување на прописите или манипулации со оперативните системи, организацијата треба да преземе соодветни дејствија и меѓу другото да ги обезбеди и следните функции:

- Автоматски предупредувања,
- Автономно заклучување на уредите,
- Бришење на доверливите информации на организацијата,
- Бришење на целиот уред,
- Спречување пристап до апликациите на организацијата,
- Спречување пристап до системите и до информациите на организацијата.

Доколку постои сомневање за прекршување или манипулација, треба да се испрати предупредување до одговорните администратори и до организационата единица за управување со безбедноста на организацијата.

Управување со мобилни уреди (MDM) - закани што се вклучени овде:	
3_0.11	Дефект или неисправност на давателите на услуги
3_0.13	Пресретнување компромитирачко зрачење
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.17	Губење уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.24	Уништување уреди или медиуми за чување податоци
3_0.25	Дефект на уреди или на системи
3_0.28	Софтверски недостатоци или грешки
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.32	Злоупотреба на овластувања
3_0.36	Кражба на идентитет
3_0.37	Одредување на дејствија
3_0.38	Злоупотреба на лични податоци
3_0.39	Злонамерен софтвер
3_0.45	Губење податоци

4.37 Веб прелистувачи

4.37.1 Вовед

Веб прелистувачите се апликативни програми што можат да пристапат до документи со (хипертекст), слики, видео, аудио и други формати на податоци на интернет за обработка, гледање, излез и зачувување локални системи за информатичка технологија. Веб прелистувачите можат да пренесуваат податоци и на интернет. Денес, статичните и мобилните клиенти се незамисливи без веб прелистувачи, бидејќи многу приватни и деловни апликации користат соодветна содржина. Истовремено, содржините на интернет стануваат сè поразновидни. Повеќето веб локации користат вградени видеа, анимирани елементи и други содржини во живо. Најсовремените веб прелистувачи опфаќаат многу различни дополнителни функции преку интеграција на дополнителни компоненти и надворешни библиотеки. Покрај тоа, постојат екстензии за одредени функции, формати на податоци и содржина. Сепак, сложеноста на најсовремените веб прелистувачи е проследена и од голем потенцијал за сериозни грешки во дизајнот и технички недостатоци или пропусти. Тоа ги зголемува можните ризици што се однесуваат не само на напади од интернет, туку и на програмски и оперативни грешки. Ризиците за доверливоста и интегритетот на податоците се исто така значајни. Покрај тоа, таквите недостатоци претставуваат закана за достапноста на цели системи за информатичка технологија. По правило, содржината на интернетот мора да се смета за недоверлива од перспективата на веб прелистувач.

4.37.2 Цел

Целта е да се опишат безбедносните барања за веб прелистувачите што се користат на клиенти т.е. на статични и на мобилни системи за информатичка технологија, како и на таблети и на паметни телефони.

4.37.3 Закани

Извршување малициозен код од веб прелистувачи

Веб прелистувачите редовно преземаат податоци од недоверливи извори. Таквите податоци може да содржат извршен злонамерен код, кој може да ги искористи недостатоците и да го зарази системот за информатичка технологија на корисникот без негово знаење. Ова може да вклучува код (на пример, во JavaScript) што може директно да се изврши од веб прелистувачот. Може да вклучува и извршен код на дополнителната компонента или екстензија во врска со прелистувачот, на пример Java или делови од PDF документи. На крајот, кодот може да се преземе од веб прелистувачот на клиентот и да се изврши таму надвор од процесот на прелистувачот. Доколку соодветно не се употребат основните заштитни механизми на најсовремените веб прелистувачи, се загрозува доверливоста, интегритетот и достапноста на информациите или на услугите од страната на клиентот, а потенцијално и во која било поврзана мрежа.

Комплекти за искористување (Exploit kits)

Листите на недостатоци (list of vulnerabilities) и комплетите за искористување значително го олеснуваат развојот на приспособениот злонамерен софтвер. Кибер нападите може да се автоматизираат со цел да се користат преземања или други методи на дистрибуција со едноставни средства за кои не е потребно стручно знаење. Напаѓачите може да ги искористат познатите недостатоци на веб прелистувачот или на поврзаните ресурси или екстензии за да подготват последователни напади или да вчитаат и да инсталираат злонамерен код на клиентот. Злонамерниот код што е вчитан на клиентите на овој начин, честопати предизвикува дополнително вчитување на злонамерниот софтвер, кој потоа се извршува на клиентите со кориснички привилегии.

Прислушување комуникации на интернет

Основната безбедност на комуникацијата на интернет во голема мера зависи од користените методи за автентикација и од криптирањето на податоците за време на преносот. При имплементирање на овие методи, можно е да се направат грешки што спречуваат ефективна автентикација и криптирање. Понатаму, многу веб услуги сè уште нудат застарени методи за криптирање. Како резултат на тоа, напаѓачите можат да ги заобиколат техниките за автентикација на серверот, а комуникациите или податоците може да не се доволно криптирани. Ова може да им овозможи на неовластените лица да пристапат или да ги менуваат информациите додека се пренесуваат. Исто така и телата за сертифицирање се компромитираат, со што се овозможува напаѓачите да добијат сертификати за веб локации на трети лица.

Губење на интегритетот во веб прелистувачите

Ако веб прелистувачите, дополнителните компоненти или екстензии се добиени од недоверливи извори, малициозните функции може ненамерно да се извршат без да бидат забележани. На пример, напаѓачите може да ги фалсификуваат компонентите на прелистувачот како што се алатките за да ги наважат корисниците на манипулирани копии на веб локации што се користат за напади за кражба на идентитетот. Злонамерните екстензии може да манипулираат со содржината на прегледаните веб локации или да прибираат податоци и да ги испратат до напаѓачот.

Губење на приватноста

Ако веб прелистувачите не се безбедно конфигурирани, доверливите податоци ненамерно или намерно може да им бидат откриени на неовластени трети лица. Лозинките исто така може ненамерно да се препратат до други лица. Доколку се зачуваат колачиња, лозинки, истории, влезни податоци и барања за пребарување или се активираат непотребни екстензии, ќе биде полесно трети лица или злонамерен софтвер да пристапат и да ги злоупотребат овие податоци.

4.37.4 Мерки

Употреба на основни безбедносни механизми

Користениот веб прелистувач мора да обезбеди дека секој примерок и процес може да пристапи само до сопствените ресурси (т.н. sandboxing). Веб локациите мора да бидат меѓусебно изолирани во независни процеси или барем во нивните нишки. Дополнителните компоненти и екстензии мора да се извршуваат и во изолирани области. Користениот веб прелистувач мора да ја имплементира Политиката за безбедност на содржината (CSP). Треба да се исполни тековното највисоко ниво на CSP. Прелистувачот мора да поддржува политика со исто потекло и заштитни мерки за интегритетот на вклучените средства.

Поддршка за безбедно криптирање на комуникацијата

Веб прелистувачот мора да поддржува безбедна верзија на безбедноста на транспортниот слој (TLS). Врските со веб серверите мора да бидат криптирани со TLS секогаш кога тоа е поддржано од соодветниот веб сервер. Небезбедните верзии на TLS треба да се деактивираат. Веб прелистувачот мора да го поддржува и да го имплементира безбедносниот механизам HTTP Strict Transport Security (HSTS) според RFC 6797.

Користење доверливи сертификати

Ако веб прелистувачот обезбедува свој список на доверливи коренски сертификати, мора да се обезбеди дека само администраторите можат да ги менуваат. Ако тоа не е можно преку технички заштитни мерки, на корисниците мора да им се забрани да ги менуваат овој список. Воедно, мора да се обезбеди дека веб прелистувачот може локално да ги поништи сертификатите. Веб прелистувачот мора сеопфатно да ја провери валидноста на сертификатите на серверот со користење на јавниот клуч, притоа земајќи ги предвид соодветните периоди на валидност. Веб прелистувачот мора да го потврди и статусот на заклучување на сертификатите на серверот. Синџирот на сертификати, вклучувајќи го и коренскиот сертификат, мора да биде потврден. Веб прелистувачот мора јасно и видливо да му укаже на корисникот дали комуникацијата се одвива во обичен текст или во криптирана форма. Веб прелистувачот треба да може да му го покаже на корисникот сертификатот за серверот што се користи по барање. Веб прелистувачот мора да го предупреди корисникот кога сертификатите недостасуваат, не се валидни или се поништени. Во овој случај, веб прелистувачот мора да ја прекине врската додека корисникот не го потврди тоа изречно.

Управување со лозинки во веб прелистувачи

Доколку управувачот со лозинки се користи во веб прелистувач, тој мора да создаде директна и единствена врска помеѓу секоја веб локација и лозинката која е зачувана за неа. Зачуваните лозинки мора да бидат криптирани. Мора да се обезбеди дека до лозинките што се зачувани во управувачот со лозинки може да се пристапи само откако ќе се внесе главната лозинка. Понатаму, мора да се обезбеди дека автентикацијата за пристап заштитен со лозинка е валидна само за тековната сесија. Организационата единица за информатичка технологија мора да обезбеди дека прелистувачот им овозможува на корисниците да ги бришат зачуваните лозинки.

Користење DNS преку HTTPS

Организацијата мора да провери дали прелистувачите користат DNS-over-HTTPS (DoH). Мора да се прецизира дали функцијата треба да се користи или не. Ако организацијата користи DNS сервери како разрешувач до кои се пристапува преку недоверливи мрежи, треба да се користи DoH. Ако се користи DoH, организацијата мора да наведе доверлив DoH сервер.

Економија на податоци во веб прелистувачи

Колачињата од трети лица треба да бидат одбиени во веб прелистувачите. Корисниците треба да можат да ги избришат зачуваните колачиња. Функцијата за автоматско комплетирање податоци треба да се деактивира. Доколку оваа функција сепак се користи, корисникот треба да може да ги избрише соодветните податоци. Корисникот треба да може и да ги избрише податоците од историјата на веб прелистувачот. Доколку е достапна таква опција, синхронизацијата на веб прелистувачот со услуги за „облак“ треба да се деактивира. Функциите на телеметрија и автоматското испраќање извештаи за пад на системот, URL-внесувања и внесувања за пребарување до давателот на прелистувачот или други надворешни лица, треба да се оневозможат секогаш кога тоа е можно. Споделувањата на локацијата и на периферните уреди какви што се микрофони или веб камери, треба да се овозможат само за веб локации на кои тие се апсолутно неопходни. Прелистувачот треба да понуди опција за конфигурирање и за деактивирање на WebRTC, HSTS и JavaScript.

4.37.5 Напредни мерки**Користење изолирана околина на веб прелистувач**

Во случај на зголемени потреби за заштита, треба да се користат веб прелистувачи што работат во изолирана околина (на пример, преку микровиртуелизација или на наменски системи за информатичка технологија).

Користење приватен режим

Во случај на зголемени барања во врска со доверливоста, веб прелистувачот треба да се користи во приватен режим за да нема трајно зачувување информации или содржина на системот за информатичка технологија на корисникот. Прелистувачот треба да се конфигурира така што локалната содржина ќе се избрише штом прелистувачот ќе се затвори.

Проверка за злонамерна содржина

Веб прелистувачот треба да ги проверува интернет адресите до кои пристапил корисникот за потенцијална злонамерна содржина. Веб прелистувачот треба да го предупреди корисникот доколку има информации за злонамерна содржина. Треба да се оневозможи воспоставување врска што е класифицирана како злонамерна. Постапката што се користи за проверка не смее да ги повредува прописите за заштита на личните податоци или прописите за класифицирани информации.

Стратегија со два прелистувачи

Ако веб прелистувачот што се користи има нерешени безбедносни проблеми, треба да се инсталира алтернативен прелистувач со различна платформа како резервна опција за корисникот.

Веб прелистувачи - закани што се вклучени овде:	
3_0.14	Шпионажа
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.26	Неисправност на уреди или на системи
3_0.28	Софтверски недостатоци или грешки
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.38	Злоупотреба на лични податоци
3_0.39	Злонамерен софтвер

4.38 Веб сервери

4.38.1 Вовед

Веб серверот е клучна компонента на секоја веб локација. Ги прифаќа барањата од клиентите и им ја враќа соодветната содржина. Податоците обично се пренесуваат преку протоколот за пренос на хипертекст (HTTP) или HTTP Secure (HTTPS), што е верзијата која е криптирана со безбедност на транспортниот слој (TLS). Бидејќи, веб серверите нудат едноставен интерфејс помеѓу серверските апликации и корисниците, тие исто така често се користат за внатрешни информации и апликации во сопствените мрежи на организациите (интранет). Веб серверите обично се достапни директно на интернет и на тој начин се изложени на напади. Затоа мора да бидат заштитени со соодветни безбедносни заштитни мерки.

4.38.2 Цел

Целта е да се опише како да се заштитат веб серверите и информациите што тие ги обезбедуваат и ги обработуваат.

4.38.3 Закани

Губење на угледот

Ако напаѓачите успеат да пристапат до веб сервер со административни права, тие можат да го користат за објавување манипулирана веб локација (промена на изгледот на веб локацијата). Ова може да наштети на угледот на организацијата. Слично на тоа, објавувањето неточни информации (какви што се неисправни описи на производи), може да наштети на јавната репутација на организацијата. Организацијата може да добие и официјална опомена доколку на нејзината веб локација е објавена содржина што прекршува одредени закони. Покрај тоа, организацијата може да претрпи загуби доколку нејзината веб локација не е достапна и како резултат на тоа потенцијалните клиенти се префрлаат на конкурентите.

Манипулација со веб сервер

Напаѓачот може да добие пристап до веб сервер и да манипулира со неговите податоци. На пример, напаѓачот може да ја промени конфигурацијата на веб серверот, да дистрибуира злонамерен софтвер или да ја измени веб содржината.

Одбивање услуга (DoS)

Нападите на одбивање на услугата може да се користат за да се наруши достапноста на веб локацијата на специфични начини, како, на пример, со користење неточни обиди за најава за да се заклучат поединечни сметки. Нападите за дистрибуирано одбивање услуга (DDoS), може да предизвикаат делумно или целосно откажување на веб серверот. Во таков случај, пристапот на корисниците до соодветните веб понуди ќе биде многу бавен или воопшто нема да биде достапен. За многу организации, таквите откажувања брзо можат да станат клучни за бизнисот (на пример, кога влијаат врз електронските продавници).

Губење доверливи податоци

Многу веб сервери сè уште користат застарени криптографски методи какви што се RC4 или SSL. Како резултат на недоволната автентикација или несоодветното криптирање, напаѓачите ќе можат да читаат или да менуваат комуникација помеѓу веб серверите и клиентите. Истото важи и за комуникациите помеѓу веб серверот и другите сервери, какви што се урамнотежувачи на оптоварување.

Повреда на закони или на договори

Постојат различни регулаторни барања во врска со објавувањето на веб содржини. Покрај прописите за телекомуникациите и за заштита на личните податоци, мора да се почитуваат и правилата на прописите за авторски права. Непочитувањето на овие закони, може да има правни последици за организацијата.

Недоволно решавање проблеми

Ако се појават грешки за време на операциите на веб серверот, тоа може да влијае врз достапноста на серверот, на пример. Исто така, содржината што ја прикажува може да биде нецелосна или да откажат безбедносните механизми. Неправилното решавање на грешките може да ја наруши и работата на веб серверот и заштитата на неговите функции и податоци.

4.38.4 Мерки

Безбедно конфигурирање веб сервер

Откако организационата единица за информатичка технологија ќе инсталира веб сервер, мора да изврши безбедна основна конфигурација. За таа цел, мора конкретно да го додели процесот на веб серверот на корисничка сметка со минимални права. Веб серверот мора да се извршува и во енкапсулирана средина секогаш кога тоа е поддржано од оперативниот систем. Ако тоа не е можно, секој веб сервер треба да работи на свој физички или виртуелен сервер. Од услугата на веб серверот мора да се отстранат сите непотребни дозволи за пишување. Модулите и функциите на веб серверот што не се потребни мора да се деактивираат.

Заштита на датотеки на веб серверот

Организационата единица за информатичка технологија мора да ги заштити сите датотеки на веб серверот (особено скрипти и конфигурациски датотеки) за да не можат да се читаат или да се менуваат без овластување. Мора да се обезбеди дека веб апликациите можат да пристапат само до дефинирано дрво на директориуми (коренски директориум WWW). Веб серверот мора да се конфигурира за да поддржува само датотеки што се наоѓаат во коренскиот директориум WWW. Организационата единица за информатичка технологија мора да ги оневозможи сите непотребни функции што ги наведуваат директориумите. Доверливите податоци мора да бидат заштитени од неовластен пристап. Конкретно, организационата единица за информатичка технологија мора да се погрижи доверливите датотеки да не се наоѓаат во јавните директориуми на веб серверот. Организационата единица за информатичка технологија мора редовно да проверува дали доверливите датотеки се зачувани во јавни директориуми.

Заштита на прикачувања и преземања датотеки

Сите датотеки што се објавени преку веб серверот мора однапред да се проверат за присуство на злонамерен софтвер. Мора да се одреди максималната големина за поставување датотеки и да се чува доволно простор за зачувување поставена содржина.

Евиденција на настани

Веб серверот мора да ги евидентира најмалку следниве настани:

- Успешни обиди за пристап до ресурси,
- Неуспешни обиди за пристап до ресурси поради недостаток на овластувања, недостапни ресурси или грешки на серверот,
- Општи пораки за грешка.

Податоците од евиденцијата за настани треба редовно да се анализираат.

Автентикација

Кога клиентите вршат автентикација на веб сервер со користење лозинки, овие лозинки мора да се зачуваат така што ќе бидат криптографски обезбедени и заштитени од неовластен пристап.

Услови на правна рамка за веб локации

Доколку веб серверите објавуваат содржина или нудат услуги за трети лица, мора да се почитуваат условите за релевантна законска рамка. Организацијата мора да ги почитува важечките прописи за телекомуникации, заштита на личните податоци и за авторски права.

Криптирање преку TLS

Веб серверот мора да обезбеди безбедно криптирање преку безбедност на транспортен слој – TLS (HTTPS) за сите врски што минуваат низ недоверливи мрежи. Доколку е неопходно да се користат застарени процедури поради компатибилност, тие треба да се ограничат на колку што е можно помалку случаи. Ако се користи HTTPS врска, целата содржина мора да се испорача преку HTTPS. Не смее да се користи мешана содржина.

Планирање на употребата на веб сервер

Намената на веб серверот и содржината што ја обезбедува треба да бидат испланирани и документирани. Документацијата треба да ги опишува информациите или услугите што се вклучени во односните веб понуди, заедно со соодветните целни групи. За техничките операции и за веб содржините треба да бидат поставени соодветни лица.

Дефинирање безбедносна политика на веб сервер

Организацијата треба да подготви безбедносна политика во која се наведени потребните заштитни мерки и одговорности. Треба да се дефинира и пристап за добивање информации за тековните безбедносни пропусти и недостатоци. Понатаму, треба да се дефинира начинот на кој треба да се имплементираат безбедносните заштитни мерки и чекорите што треба да се преземат во случај на безбедносен инцидент.

Избор на соодветен главен веб (Web Host)

Ако организацијата одлучи да користи надворешен давател на услуги за главен веб наместо самата да управува со својот веб сервер, треба да ги има предвид следните прашања при изборот на соодветен давател на услуги:

- Начинот на кој ќе се даваат услугите треба да биде договорно склучен. Безбедносните аспекти треба да бидат вклучени во писмена форма во договорот за ниво на услуга (SLA) како дел од договорот.
- Давателот на услуги треба редовно да ги проверува и да ги сервисира користените системи за информатичка технологија. Давателот на услугата треба да биде обврзан да реагира навремено во случај на технички проблеми или компромитирани системи на клиентите.
- Давателот на услуги треба да спроведе основни технички и организациски заштитни мерки за да го заштити својот информативен домен.

Соодветно постапување со грешки и пораки за грешки

Информациите за HTTP и прикажаните пораки за грешка, не треба да го прикажуваат името на производот или верзијата на користениот веб сервер. Пораките за грешка не треба да откриваат детали во врска со системските информации или конфигурации. Организационата единица за информатичка технологија треба да обезбеди дека веб серверот емитува само општи пораки за грешка, кои го информираат корисникот дека настанала грешка. Секоја порака за грешка треба да содржи единствена карактеристика што им овозможува на администраторите да ја следат грешката. Во случај на неочекувани грешки, треба да се обезбеди дека веб серверот нема да остане во состојба каде што подложи на напад.

Контрола на пристап за веб робот (Web Crawlers)

Пристапот до веб робот треба да се регулира во согласност со стандардот за исклучување работи. Содржините треба да се обезбедат со заштита за пристап за да се заштитат од веб работи што не се во согласност со овој стандард.

Проверки на интегритетот и заштита од злонамерен софтвер

Организационата единица за информатичка технологија треба редовно да го проверува интегритетот на конфигурациите на веб серверот и датотеките што тој ги обезбедува и да се увери дека тие не се изменети од напаѓачите. Датотеките што се наменети за објава, треба редовно да се проверуваат за присуство на злонамерен софтвер.

Пенетрациски тест и контрола

Веб серверите редовно треба да се проверуваат за потенцијална појава на безбедносни проблеми. Контролите треба да се вршат редовно. Резултатите треба да се документираат, да бидат соодветно заштитени и со нив да се постапува како со доверливи информации. Притоа, треба да се испитаат отстапувањата. Резултатите треба да му бидат презентирани на овластеното лице за безбедност на информации.

Определување лица за контакт

Организацијата што одржува обемни веб локации треба да определи лице за контакт за нив. Организацијата треба да ги дефинира процесите, процедурите и лицата што се одговорни за проблеми или за безбедносни инциденти. Организацијата треба да објави опција за контакт на својата веб локација, која ќе им овозможува на надворешните лица да пријавуваат прашања поврзани со безбедноста до организацијата. Организацијата исто така треба да ги дефинира процесите за постапување со надворешни безбедносни извештаи.

4.38.5 Напредни мерки

Редундантност

Веб серверите треба да бидат дизајнирани да бидат редундантни. Интернет врската на веб серверот и на другите системи за информатичка технологија (како што е серверот за веб апликации), исто така треба да биде дизајнирана со редундантност.

Заштита од напади со одбивање на услугата

Веб серверот треба постојано да се следи. Понатаму, треба да се дефинираат и да се имплементираат заштитни мерки што ги спречуваат или барем ги ублажуваат DDoS нападите.

Веб сервер - закани што се вклучени овде:	
3_0.11	Дефект или неисправност на давателите на услуги
3_0.15	Прислушување
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.26	Неисправност на уреди или на системи
3_0.27	Недостаток на ресурси
3_0.29	Повреда на закони или на договори
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи
3_0.39	Злонамерен софтвер
3_0.40	Одбивање на услуга
3_0.45	Губење податоци
3_0.46	Губење на интегритетот на информациите што треба да се заштитат

4.39 Печатачи, апарати за копирање и уреди сè-во-едно

4.39.1 Вовед

Денешните печатачи, апарати за копирање и уреди сè-во-едно се сложени уреди кои, покрај механичките компоненти, содржат и свои оперативни системи и обезбедуваат услуги и функции на серверот. Бидејќи овие уреди често обработуваат доверливи информации, тие мора да бидат заштитени заедно со другата инфраструктура за печатење и скенирање на организацијата. Сè-во-едно уреди се уреди што нудат неколку функции за обработка на хартија, какви што се печатење, копирање, скенирање и испраќање и примање документи преку факс. За многу деловни процеси, хартијата и денес се користи како информативен медиум. Ова ги прави печатачите, апаратите за копирање и уредите сè-во-едно важни компоненти на инфраструктурата за информатичка технологија. Ако таквите уреди откажат или се отпечатаат фалсификувани документи, тоа понекогаш може да влијае врз клучните процеси и да доведе до значителни економски загуби на организацијата.

4.39.2 Цел

Целта е да се опише како може безбедно да се ракува со печатачите, апаратите за копирање и уредите сè-во-едно за да не се извлекуваат информации од овие уреди и да не се наруши безбедноста на другата внатрешна достапна инфраструктура за информатичка технологија.

4.39.3 Закани

Неовластен пристап до печатени документи

Печатените документи често остануваат во излезната фиока на централните печатачи и на уредите сè-во-едно подолг временски период, на пример, затоа што корисниците прво печатаат неколку датотеки, а подоцна ги собираат сите заедно. Воедно, можно е погрешен печатач да е избран на клиент и документите да не се најдат на очекуваната локација. Бидејќи многу корисници ги користат печатачите на еден кат или организациона единица, неовластени лица исто така можат да прегледуваат сензитивни информации или да ги земат печатените документи со себе. Ризик се и печатените материјали што се оставени во излезните фиоки на печатачите на децентрализирани работни станици што се наоѓаат во непосредна близина на канцелариите на корисниците. Тоа е затоа што луѓето што имаат пристап до овие простории може да ги прегледуваат или да ги отстранат печатените материјали. Документите за испраќање преку факс и печатените записи за пренос во излезните фиоки претставуваат дополнителен ризик: покрај броевите на факс, датумите, времињата и броевите на страниците, тие често содржат намалена слика на првата страница. Бидејќи таквите записи се објавуваат само откако ќе се испрати факс или ќе се појави грешка во преносот, тие исто така може да останат во машината подолг временски период или воопшто да не бидат земени. Поради тоа, доверливите информации може да останат без надзор во излезната фиока каде што, во најлош случај, може да бидат украдени. На крајот корисниците ќе ги фрлат земените документи. Во ваков случај, печатените материјали најчесто се фрлаат во корпа за отпадоци по случаен избор во близина, наместо безбедно да се уништат (особено кога содржат сензитивни информации). Затоа, таквите информации можат да стигнат до јавниот систем за исфрлање отпад и потенцијално да се најдат во рацете на трети лица. Многу локации за работење на далечина исто така се опремени со печатач или со уред сè-во-едно. Ова е уште еден случај во кој може да се откријат сензитивни информации.

Видливост на метаподатоци

Задачата за печатење обично вклучува метаподатоци што содржат корисничка идентификација, датум, време и името на задачата за печатење. Овие податоци се прикажуваат на контролната табла и на веб серверот на многу печатачи и уреди сè-во-едно. Името на задачата за печатење често е добиено од името на дигиталниот документ кој се печати. Ако печатачот има интегриран веб сервер, доверливите процеси често може да се гледаат преку прелистувач. Метаподатоците на серверите за печатење се исто така видливи во обичен текст, освен кога се анонимни. Ова може да им овозможи на трети лица да добијат доверливи информации. Многу уреди исто така овозможуваат зачувување на задачите за печатење за да може да се отпечатаат подоцна по автентикацијата со PIN. Ова е уште еден случај во кој името на сите достапни документи се прикажува на контролната табла на излезен уред. Некои печатачи и апарати за копирање на хартијата, печатаат „жолти точки“ (исто така познати како код за идентификација на машината, точки за следење или тајни точки). Овие често недокументирани водени жигови, кои може да вклучуваат датум, време и сериски број на печатачот, тешко се видливи со голо око. На овој начин, отпечатакот може директно да се поврзе со организација или со конкретен корисник и на тој начин да се следи до креаторот на документот. Покрај последиците во однос на прописите за заштита на личните податоци, на овој начин информациите може случајно да се споделат и надвор од организацијата. Факс записите може да се печатаат и без заштита за пристап на многу уреди сè-во-едно. Дури и ако наведат само телефонски броеви, датуми, времиња и броеви на страници, тие овозможуваат да се извлечат заклучоци за лични податоци или за деловни трансакции.

Недоволна заштита на зачуваните информации

Печатачите, апаратите за копирање и уредите сè-во-едно често се опремени со постојана меморија за податоци на која информациите се чуваат привремено или подолго време. На пример, таму се зачувани адресари, документи, факсови и задачи за печатење. Доколку овие информации не се соодветно заштитени, трети лица можат да пристапат и да ги читаат. Под одредени околности, напаѓачите можат дури и да ги реконструираат информациите што веќе се избришани доколку се користат небезбедни методи за бришење. Податоците исто така може да се зачуваат и да се читаат на уред преку мрежни протоколи. Печатачите и уредите сè-во-едно со медиум за чување податоци често може да се користат како неовластени сервери за датотеки, ако истите не се обезбедени. На овој начин, неконтролираните информации што не се земи предвид во соодветниот концепт на сигурносна копија може децентрализирано да се зачуваат.

Некриптирана комуникација

Податоците за печатење и за скенирање често се пренесуваат преку мрежи во некриптирана форма. Ова им овозможува на напаѓачите да пресретнат пренесени документи. Може да се читаат и датотеките за печатење што се привремено зачувани на серверите за печатење. Ова се однесува и на системите за централно скенирање и обработка на документи. Некриптираните комуникациски интерфејси за администрирање такви уреди претставуваат дополнителни извори на опасност. Ако, на пример, до печатачите се пристапува преку HTTP, SNMPv2 или Telnet, вклучените информации не се заштитени кога се пренесуваат. Ова ги загрозува лозинките на уредот и другите информации за пристап.

Неовластено испраќање информации

Многу уреди сè-во-едно можат да испраќаат дигитализирани хартиени документи по е-пошта и по факс. Без посебни мерки на претпазливост, информациите може намерно или случајно да се пренесат на неовластени примачи на овој начин. Корисниците може, на пример, погрешно да внесат адреси на примачи или телефонски броеви. Како резултат на тоа, сензитивните податоци може ненамерно да бидат испратени до погрешен примач. Покрај тоа, напаѓачите можат да користат функција за е-пошта или факс за брзо испраќање доверливи документи до надворешниот свет. Многу мрежни печатачи може да се конфигурираат за да примаат задачи за печатење од интернет преку е-пошта и да испраќаат скенирани документи како прилози за е-пошта. Овде, полето за внесување што е дефинирано од корисникот за адресата на испраќачот може да се злоупотреби за испраќање е-пошта под друго име до внатрешни и до надворешни примачи.

Неконтролирана размена на податоци преку мемориски интерфејси на печатачи, апарати за копирање и уреди сè-во-едно

Документите на хартија може брзо да се копираат со помош на уреди сè-во-едно. USB или SD портите исто така овозможуваат директно дигитализирање дури и на големи количини хартиени документи и нивно зачувување на USB уред или на SD картички без никакви контроли. Овие интерфејси овозможуваат и печатење документи што се зачувани на такви медиуми. Ако печатачите, апаратите за копирање или уредите сè-во-едно се поврзани на мрежа за податоци или директно со клиенти, системите за информатичка технологија честопати можат директно да пристапат и до медиумот за чување податоци што е поврзан со овие уреди. Дури и ако интеграцијата на медиумите за чување податоци е технички спречена на самите системи за информатичка технологија, оваа работа преку интерфејсите за чување податоци овозможува неконтролирано копирање информации. На овој начин, (злонамерен) софтвер може да се прошири на клиентите што се поврзани со уредите сè-во-едно или во мрежата на податоци на организацијата преку интерфејсите за чување податоци на уредите. Во меѓувреме, доверливите (хартиени) документи може незабележано да се дигитализираат и да бидат украдени без можност за понатамошно следење.

Несоодветно обезбеден мрежен пристап на печатачи, апарати за копирање и уреди сè-во-едно

Заштитните сидови помеѓу локалната мрежа (LAN) и интернетот често се конфигурирани за да овозможат пристап до интернет на цели подмрежи. Во исто време, печатачите и уредите сè-во-едно често се доделуваат на истата подмрежа како и клиентите. Ова значи, на пример, дека мрежните печатачи можат да пристапат до информации и на интернет. Дури и ако системите за информатичка технологија на организацијата пристапуваат на интернет само преку посреднички (прокси) уреди, печатачите, апаратите за копирање и уредите сè-во-едно можат да го користат и посредничкиот (прокси) уред. Ако конекциите од интернет до уредите не се отфрлени од заштитниот сид, тоа може да дозволи протекување сензитивни информации од мрежата на податоците на организацијата под одредени околности. На истиот начин, печатач што може да се поврзе со мрежа исто така може да прима и да дистрибуира несакани податоци од интернет. Затоа, мрежниот печатач може да стане влез за напади од интернет.

Недоволна заштита за пристап за администрирање на уредот

Мрежните печатачи, апарати за копирање и уредите сè-во-едно може да се управуваат од нивните контролни табли и вградени веб сервери. Кога се испорачуваат такви уреди, тие обично имаат стандардна лозинка што е специфична за производителот (или воопшто немаат лозинка). Ако оваа лозинка не се промени или не е поставена, многу лесно може да се пристапи до уредот. Многу организации користат и вообичаени лозинки за сите свои печатачи и уреди сè-во-едно и ретко ги менуваат. Како резултат на тоа, тие често им се познати на многу внатрешни и на надворешни лица, што го олеснува пристапот до уредите од страна на неовластени трети лица.

Покрај тоа, печатачите и уредите сè-во-едно може да се ресетираат на фабричките поставки преку менијот за подигање. Ова исто така влијае врз нивните безбедносни поставки. На пример, лозинката на уредот често повеќе не постои откако печатачот или уредот сè-во-едно е ресетиран на неговите фабрички поставки. Незаштитените менија за подигање го поедноставуваат администрирањето, но истовремено ја намалуваат безбедноста. Печатачите, апаратите за копирање и уредите сè-во-едно се опремени со голем број мрежни протоколи. Сите овие протоколи обично се активираат при испорака. Ова може да им овозможи на напаѓачите, на пример, да пристапат до поставките на уредот и да ги менуваат за да извлечат сензитивни информации од околната мрежа. Многу уреди можат да ја префрлат својата контролна табла на претставник за поддршка преку мрежата. Сепак, ова може да се користи и за читање доверливи внесени податоци од корисниците на контролната табла.

Поголемите организации обично имаат повеќе печатачи, апарати за копирање и уреди сè-во-едно. За нивно ефикасно управување и следење, често се користи софтвер за управување со уреди. Сепак, многу организации не го заштитуваат соодветно овој софтвер од неовластен пристап, бидејќи се смета за помалку критичен систем. Ова овозможува ненамерно или намерно да се менуваат поединечни уреди или сите уреди.

4.39.4 Мерки

Планирање на употребата на печатачи, апарати за копирање и уреди сè-во-едно

Пред да се набават печатачи, апарати за копирање и уреди сè-во-едно, мора да се испланира нивната безбедна употреба. Притоа, треба да се земат предвид следниве критериуми:

- Поддршка на безбедни протоколи за пренос и администрирање податоци,
- Криптирање на зачуваните информации,
- Автентикација на корисници директно на секој уред,
- Употреба на механизми за физичка заштита, какви што се елементи за поцврсто прикачување кои штитат од кражба или заклучување на уредите,
- Постојно доверлив и ефикасен автоматски внесувач на страници на единиците за скенирање,
- Поддршка за соодветни формати на податоци,
- Поддршка за баркодери за одвојување документи и пренос на мета информации (доколку е потребно),
- Постојно функција за безбедно бришење зачувани податоци,
- Достапност на редовни ажурирања и договори за одржување.

Притоа мора да се наведат локациите каде што може да се наоѓаат уредите. Покрај тоа, мора да се дефинира кој може да пристапува до печатачи, апарати за копирање и до уреди сè-во-едно. Резултатите треба да се документираат.

Соодветна позиција и пристап до печатачи, апарати за копирање и уреди сè-во-едно

Организационата единица за информатичка технологија мора да постави и да обезбеди печатачи, апарати за копирање и уреди сè-во-едно така што само овластените корисници можат да ги користат уредите и да пристапат до обработените информации. Дополнително, мора да се обезбеди дека само овластени лица можат да ги администрираат уредите, да ги одржуваат и да ги поправаат. Договорите за доверливост мора да се склучат во писмена форма со давателите на услуги (на пример, за одржување). Печатачите, апаратите за копирање и уредите сè-во-едно мора да се постават со лозинки на уредот за да го блокираат пристапот до нивните веб сервери и контролни табли за администрирање. Оттука, тие мора да бидат во согласност со барањата за управување со идентитетот и овластувањата на организацијата.

Правилно отстранување печатени документи

Печатените документи што содржат доверливи информации што повеќе не се потребни, мора да се отстранат. Ако работните станици се опремени со печатачи, апарати за копирање или уреди сè-во-едно, треба да се обезбеди дека информациите што се отпечатени таму може да се уништат директно на локацијата кога повеќе не се потребни.

Подготвување безбедносна политика за употреба на печатачи, апарати за копирање и уреди сè-во-едно

Организацијата треба да подготви безбедносна политика за печатачи, апарати за копирање и уреди сè-во-едно. Исто така, треба да ги регулираат барањата и спецификациите за безбедноста на информациите на таквите уреди и како тие треба да се исполнат. Воедно, треба да се наведе и кои функции може да се администрираат или да се користат од конкретни корисници и под кои услови.

Изготвување упатства за корисникот за ракување со печатачи, апарати за копирање и уреди „сè-во-едно“

Организацијата треба да изработи и упатство за корисникот во кое јасно и разбирливо се наведени сите безбедносни барања за ракување со печатачите и уредите сè-во-едно. Сите корисници треба да бидат запознаени со упатството.

Ограничување на далечинскиот административен пристап до печатачи, апарати за копирање и уреди сè-во-едно

Организационата единица за информатичка технологија треба да обезбеди дека само јасно дефинирана група администратори и сервисери имаат далечински административен пристап до печатачи, апарати за копирање и уреди сè-во-едно. Ова треба да се обезбеди и ако организацијата користи централен софтвер за управување со уреди. Притоа, треба да се прецизира дали приказите на контролната табла може да се гледаат преку мрежата за податоци. Доколку е потребно, таквите прикази треба да се префрлаат само на лицата во организационата единица за информатичка технологија. Ова треба да се договори и со засегнатите корисници.

Ограничување на поврзувањето на печатачи, апарати за копирање и уреди сè-во-едно

Организационата единица за информатичка технологија треба да обезбеди дека преку надворешни мрежи не може да се пристапи до печатачите, апаратите за копирање и до уредите сè-во-едно. При поврзување уреди сè-во-едно на телефонската мрежа, треба да се обезбеди дека не може да се воспостават неконтролирани податочни врски помеѓу мрежата за податоци на организацијата и телефонската мрежа. Со мрежните печатачи и со уредите сè-во-едно треба да се ракува во нивниот сопствен мрежен сегмент и да се чуваат одделно од клиентите и од серверите на организацијата.

Криптирање на информации за печатачи, апарати за копирање и уреди сè-во-едно

Ако е можно, сите информации што се зачувани на медиуми со внатрешна постојана меморија за податоци, треба да бидат криптирани. Задачите за печатење треба да се пренесат и во криптирана форма ако тоа е можно и изводливо.

Заштита на кориснички информации и на метаподатоци

Корисничките податоци и метаподатоците, какви што се задачите за печатење и датотеките за скенирање, треба да се чуваат на уреди колку што е можно пократко. Податоците треба автоматски да се избришат по претходно дефинирано време. Организационата единица за информатичка технологија треба да ги оневозможи серверите за датотеки на такви уреди и функции како што е „скенирање до меморија на уредот“. Протоколите и функциите што се потребни за ова треба да се блокираат секогаш кога тоа е можно. По правило, организационата единица за информатичка технологија треба да обезбеди да нема никакви видливи метаподатоци за неовластени лица. Организацијата треба да дефинира како печатените материјали со метаподатоци треба да се пренесуваат на трети лица.

Конфигурирање печатачи, апарати за копирање и уреди сè-во-едно

Само, организационата единица за информатичка технологија треба да ги конфигурира сите печатачи и уреди сè-во-едно. Функциите на неискористените уреди треба да се исклучат, а особено да се оневозможат сите непотребни податоци и мрежни интерфејси на печатачи, апарати за копирање и уреди сè-во-едно. Со уредите треба да се управува исклучиво преку криптирани протоколи какви што се HTTPS и SNMPv3. Организационата единица за информатичка технологија треба да ги замени сите протоколи што овозможуваат некриптиран пристап до печатачите и до уредите сè-во-едно со криптирани протоколи или да ги исклучи. Ова треба да се имплементира особено за протоколи што може да се користат за промена на конфигурацијата на уредот (на пример, SNMP, Telnet, PjL).

4.39.5 Напредни мерки

Автентикација и овластување за печатачи, апарати за копирање и уреди сè-во-едно

Само овластени лица треба да имаат пристап до печатени или до копирани документи. Ако е можно, треба да се користат само централни печатачи, апарати за копирање и уреди сè-во-едно за кои е потребна автентикација на корисникот пред да се почне со задачите за печатење („безбедно печатење“). Откако корисниците ќе извршат автентикација, треба да бидат видливи само нивните сопствени задачи за печатење и притоа треба да бидат овозможени само функциите што се потребни за секој корисник.

Намалување на времето на застој за печатачи, апарати за копирање и уреди сè-во-едно

За да се сведе на минимум времето на застој на печатачите, апаратите за копирање и уредите сè-во-едно, преземените заштитни мерки треба да го вклучуваат следново:

- Треба да има достапни уреди за замена,
- Во договорите за одржување треба да се обезбеди соодветно време за одговор,
- Треба да се води список на специјализирани добавувачи, со цел брзо купување уреди за замена или резервни делови,
- Доколку е потребно, треба да се одржува складиште на потребни резервни делови што редовно се менуваат.

Засилена заштита на информации за печатачи, апарати за копирање и уреди сè-во-едно

Имињата на задачите за печатење треба да се прикажуваат само во анонимизирана форма на серверите за печатење. Сите интерфејси за надворешен медиум за чување податоци треба да се оневозможат. Понатаму, внатрешните адресари на уредот треба да се оневозможат и да им се понудат на корисниците алтернативни методи за адресирање (на пример, пребарување адреса преку LDAP). Печатачите и уредите сè-во-едно со функционалност за е-пошта треба да гарантираат дека е-поштата може да се испраќа само со помош на адресата на е-пошта на корисник што извршил автентикација. Документите треба да се испраќаат само на внатрешни адреси на е-пошта. Дојдовните документи од факс и извештаите за пренос треба да бидат достапни само за овластени корисници.

Проширена заштита на печатачи, на апарати за копирање и на уреди сè-во-едно

Организационата единица за информатичка технологија треба редовно да ги проверува безбедносните поставки на печатачите, на апаратите за копирање и на уредите сè-во-едно и да ги коригира доколку е потребно. Доколку е достапен автоматизиран систем за контрола и корекција, истиот треба да се користи. Покрај тоа, треба да има ограничување за ресетирање на уредите на фабрички поставки преку нивните менија за подигање. Треба да се обезбеди дека на печатачи и на уреди сè-во-едно не може да се инсталира фирмвер или дополнителен софтвер што не е потврден и одобрен од производителот.

Печатачи, апарати за копирање и уреди сè-во-едно - закани што се вклучени овде:	
3_0.15	Прислушување
3_0.16	Кражба на уреди, медиуми за чување податоци и документи
3_0.18	Лошо планирање или недостаток на приспособување
3_0.19	Откривање на информации што треба да бидат заштитени
3_0.21	Манипулација со хардвер или софтвер
3_0.22	Манипулација со информации
3_0.23	Неовластено влегување во системи за информатичка технологија
3_0.25	Дефект на уреди или на системи
3_0.30	Неовластено користење или администрирање уреди и системи
3_0.31	Неправилно користење или администрирање уреди и системи

5.Терминологија

Изразите кои се употребени во овој прилог го имаат следното значење:

1. **Организација** е контролор или обработувач според околностите и фактичките состојби кои може да се појават при применувањето на правилата за безбедност на обработката на личните податоци;
2. **Даватели на услуга, надворешни лица, добавувачи и снабдувачи** се обработувачи или подобработувачи во зависност од нивното ангажирање од страна на контролорот или обработувачот согласно прописите за заштита на личните податоци;
3. **Организациона единица** е внатрешно структуриран организационен облик кој е дел од внатрешната структура на организацијата;
4. **Организациона единица за информатичка технологија** е организациона единица или лица кои се грижат за имплементирањето, функционирањето и одржувањето на информацискиот систем во организацијата;
5. Под **систем за информатичка технологија** се подразбира дефинираниот информациски систем во Правилникот за безбедност на обработката на личните податоци;
6. **Овластено лице за безбедност на информации** е организациона единица или лице кое се грижи за безбедноста на информации во една организација согласно закон и подзаконски акт донесен врз основа на тој закон;
7. **Вработени** се лица кои можат да се посочат или наведат во која било форма, облик или својство и имаат воспоставен, регулиран и договорен однос со организацијата, а кои учествуваат при процесите на собирање, обработка и чување на личните податоци;
8. Со **сензитивните податоци и информации и доверливите податоци и информации** се опфатени и личните податоци коишто треба да се заштитат или коишто треба да бидат заштитени согласно правилата предвидени во прописите за заштита на личните податоци;
9. **Безбедносни инциденти** се или може да претставуваат и нарушувања на безбедноста на личните податоци според правилата предвидени во прописите за заштита на личните податоци;
10. **Концептот безбедност на информации** се однесува на безбедноста на обработката на личните податоци и истиот претставува дел кој се надополнува и е во функција на системот за заштита на личните податоци кој е воспоставен од страна на организацијата согласно прописите за заштита на личните податоци.

Термините кои се однесуваат на „мора“ значи „обврска“, а „треба“ значи „можност“ или „препорака“ по кои треба да постапува организацијата.

Изразите што се употребуваат во овој прилог чие значење не е дефинирано во оваа точка имаат значење определено со друг закон, пропис, меѓународен стандард или други технички нормативи и стандарди. Во тој контекст, изразите може да претставуваат и општоприфатени поими или стручни односно технички термини.

Дадените примери во овој прилог се од илустративен и информативен карактер и може да не ги отсликуваат денешните или идните состојби кои може да се појават во секојдневното работење на организацијата.