5

БЕЗБЕДНОСНИ МЕРКИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

ДИРЕКЦИЈА ЗА ЗАШТИТА
НА ЛИЧНИТЕ ПОДАТОЦИ

CIP - Каталогизација во публикација
Национална и универзитетска библиотека “Св. Климент Охридски”, Скопје

342.738(497.7)(036)

УГРИНОВСКА, Нина
Безбедносни мерки за обработка на лични податоци / автори на документот Нина Угриновска. - Скопје : Дирекција за заштита на личните податоци, 2018. - 79 стр. : илустр. ; 21 см

ISBN 978-608-4682-34-9

а) Заштита на лични податоци - Безбедносни мерки - Македонија - Водичи COBISS.
MK-ID 108238090

БЕЗБЕДНОСНИ МЕРКИ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Издавач
Дирекција за заштита на личните податоци

Автор на документот
Нина Угриновска

Лектура
Дијана Ристова

Дизајн
Маја Димеска-Крпач

Печатење
Пропоинт

Тираж
50 примероци

Февруари, 2018

Овој документ е изработен во рамки на проектот „Поддршка за пристап до правото на заштита на личните податоци“ EuropeAid 135668/IH/SER/MK, финансиран од Европската Унија преку ИПА ТАИБ 2012 програмата и спроведен од Vialto Consulting од Унгарија, во соработка со IPS Институт од Словенија и Националното тело за заштита на личните податоци и слобода на информации од Унгарија. Ставовите и мислењата наведени во овој прирачник во ниеден случај не ги изразуваат ставовите на Европската Унија.

СОДРЖИНА

ВОВЕД

За да ја исполнат својата мисија и да се усогласат со законодавството, секоја организација мора да обезбеди соодветно ниво на сигурност на нивните информации, особено приватните и личните информации.[1]

Операциите кои се занимаваат со обработка на приватни и лични информации се под континуирано влијание на постојаната менливост на средината. Процесите постојано се менуваат со бројни внатрешни или надворешни фактори. Несигурностите создадени од такви промени ќе влијаат врз тоа како организацијата треба да реагира за да се осигури дека нејзините информациски средства се соодветно заштитени. Затоа, постои потреба од посебен систем за управување кој ѝ помага на организацијата да управува со неизвесностите кои можат да влијаат врз безбедноста на нивните информации.

Луѓето и средствата доаѓаат и си одат, тие се движат внатре во организацијата, се воведуваат нов софтвер и хардвер, а се случуваат и физички промени во инфраструктурата. Секоја промена воведува нов ризик во форма на можна површина за напади - освен ако не се усвои методички, процедурален пристап.

Редовно се воведуваат промени на прописите. Секоја промена може да воведе нови барања од системот за управување со безбедноста на информациите и да претставува нов ризик за приватните и личните информации.

Безбедносните мерки што ги штитат приватните и личните информации не можат општо да се дефинираат, бидејќи тие мора да потекнуваат од процесот на управување со ризици за безбедност на информациите. Управувањето со ризици за БИ е единствено за организацијата и е специфично за контекстот на организацијата во која се обработуваат приватните и личните податоци.

1. Приватни и лични информации исто така може да се ословуваат и како лични идентификувачки информации (ЛИИ)

Контекстот на организацијата се состои од природата на обработката (збирот на приватни и лични податоци, обемот на обработка на интеракцијата со други внатрешни и надворешни процеси итн.), организациската структура на организацијата (големината на организацијата, бројот на вработените, географската дистрибуција и сл.), регулаторните фактори кои организацијата ги почитува и сл. Затоа, безбедносните мерки не можат да се генерализираат и треба да бидат испорачани од процесот на управување со ризици за безбедност на информациите.

Не постои „универзална мера“ кога станува збор за безбедносните мерки. Мерките за безбедност кои се соодветни за една организација ќе зависат од околностите и треба да се усвои пристап базиран на ризик за да се одлучи кој степен на безбедност ѝ е потребен на организацијата. Мерките се применуваат на различен опсег во различни организации.

ЦЕЛ

Целта на овој водич е да ги претстави главните концепти за безбедност на приватни и лични податоци и да предвиди насоки за дефинирање на технички и организациски мерки за исполнување на условите за безбедност на обработката на приватни и лични податоци.

Документот е наменет за раководството на организацијата и персоналот одговорен за обезбедување на обработка на лични податоци, како и за мониторингот на вработените и за обезбедување на усогласеност со обврските за заштита на податоците.

Се основа на општоприфатените добри практики во управувањето со ризици за безбедност на информациите.

ПРОПИСИ ЗА ЗАШТИТА НА ПОДАТОЦИТЕ

Покрај предвидувањето на подобри работни практики кои ги поддржуваат целите на организацијата, ублажуваат безбедносни ризици и ги намалуваат трошоците поврзани со тие ризици, спроведувањето на безбедносните мерки исто така е барано од различно законодавство и регулатива за заштита и обезбедување на обработката на приватни и лични податоци.

ВО РЕПУБЛИКА МАКЕДОНИЈА

Закон за заштита на личните податоци

Дирекцијата за заштита на личните податоци како независен орган во Република Македонија е одговорна за надгледување на законитоста на заштитата на личните податоци во земјата.

V. ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 23

За да се обезбеди тајност и заштита на обработката на личните податоци на субјектот, контролорот и обработувачот мора да применат соодветни технички и организациски мерки за заштита од случајно или незаконско уништување на личните податоци, или нивно случајно губење, преправање, неовластено откривање или пристап, особено кога обработката вклучува пренос на податоци преку мрежа и заштита од какви било незаконски облици на обработка.

Слика 1 Закон за заштита на личните податоци, фрагмент - Безбедност при обработка

ВО ЕВРОПСКАТА УНИЈА

Законите за приватност на податоци се конвергираат во ЕУ, со помош на Националните органи за заштита на податоците, Директивата за заштита на податоците усвоена во 1995 година и предложената Регулатива за е-приватност. Општата регулатива за заштита на личните податоци ќе ја замени Директивата за заштита на податоци (официјално Директива 95/46/ЕЗ) од 1995 година, кога ќе стапи на сила на 25 мај 2018 година. **Општата регулатива за заштита на личните податоци** ја регулира заштитата на физичките лица во однос на обработката на личните податоци и на слободното движење на таквите податоци.

Преноси на податоци надвор од ЕУ - Регулативата забранува пренос на лични податоци надвор од ЕУ на трета земја која нема соодветна заштита на податоците.

Европската комисија има овластување да одобри одделни земји како земји кои имаат обезбедено соодветно ниво на заштита на податоците, имајќи ги предвид законите за заштита на податоците кои се во сила во таа земја и нејзините меѓународни обврски.

Член 32
Безбедност на обработката

1. Земајќи ги предвид најновите достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста на правата и слободите на физичките лица, контролорот и обработувачот, применуваат соодветни технички и организациски мерки за обезбедување на соодветно ниво на безбедност во врска со ризикот, вклучувајќи, меѓу другото, каде што е соодветно:

а) псевдонимизација и енкрипција на личните податоци;

б) способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка;

в) способност за навремено обновување на достапноста и пристапот до личните податоци во случај на физички или технички инцидент;

г) процес на редовно тестирање, проценка и евалуација на ефикасноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.

2. При проценката на соодветното ниво на безбедност се земаат предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до пренесени, складирани или лични податоци обработени на друг начин.

3. Придржувањето кон одобрени кодекси на однесување наведени во член 40 или одобрени механизми за сертификација наведени во член 42, може да се користи како елемент за докажување на усогласеноста со барањата утврдени во став 1 од овој член.

4. Контролорот и обработувачот преземаат чекори за да обезбедат дека секое физичко лице кое дејствува под раководство на контролорот или на обработувачот на личните податоци, нема да ги обработува овие податоци само по упатства на контролорот, освен ако од засегнатото лице не се бара да го прави тоа според правото на Унијата или правото на земја членка.

Слика 2 Општа регулатива за заштита на лични податоци - Безбедност при обработка

ВО СВЕТОТ

Членот 17 од Меѓународниот пакт за граѓански и политички права на Обединетите нации од 1966 исто така ја штити приватноста: „Никој не смее да биде подложен на произволно или незаконско мешање во неговата приватност, семејство, дом или преписка, ниту на незаконски напади врз негова чест и углед. Секој има право на заштита од законот против таквото мешање или напади".

Врз основа на оваа рамка за приватност, различни земји имаат имплементирано сопствени закони за заштита на податоците.

КЛАСИФИКАЦИЈА НА ИНФОРМАЦИИТЕ И ПОЛИТИКИ НА ЗАДРЖУВАЊЕ

Со цел да се обезбеди дека личните и приватните информации добиваат соодветно ниво на заштита во согласност со нивната важност за организацијата и сензибилитетот, треба да се постави соодветна класификација. Ова значи дека треба да се направат следниве чекори:

- Да се дефинираат различни нивоа на класификација за различни групи на информации врз основа на нивната доверливост, вредност, важност, итн. За секое ниво на класификација треба да се постават различни правила за ракување со информациите.
- Секој збир на информации треба да биде соодветно обележан, така што секое лице кое доаѓа во допир со тие информации, треба несомнено да знае со какви информации тој / таа се занимава и да знае како правилно да ракува со тие информациите според нивниот степен на класификација.
- Потребно е да се подготват постапки за справување со средствата според нивната класификација.

Основни правила што треба да се следат:

- Сите информации имаат сопственик.
- Сопственикот на информациите мора да ги класифицира информациите на едно од нивоата на безбедност - во зависност од законските обврски, трошоци и деловни потреби.
- Ако сопственикот не е сигурен на кое ниво треба да бидат класифицирани податоците, треба да се користи највисокото ниво.

- Сопственикот мора да објави на кого му е дозволен пристап до информациите.
- Сопственикот мора редовно да ја прегледува класификацијата на информациите во случај информациите да го променат нивото во зависност од проценетото време, промената на прописот (внатрешен или надворешен), методот на обработка или кое било друго внатрешно решение во врска со класифицирани информации.
- Сопственикот е одговорен за неговите/нејзините информации и мора да ги обезбеди или некој друг да ги обезбеди (на пр. преку администратор за безбедност) според неговата класификација.

ЗАДРЖУВАЊЕ И АРХИВИРАЊЕ

Личните и приватните податоци не треба да се чуваат подолго отколку што е потребно за целта за која се обработуваат.

Но, овие податоци многу често треба да се складираат и чуваат за целта за која се обработуваат, поради различни деловни причини или причини за усогласување. Податоците кои не се користат активно, или целта за нивната обработка повеќе не постои, но треба или мора да се чуваат, се нарекуваат записи.

Записите се чуваат во архиви (или се архивираат). Обично постојат три видови архиви:

- Бази на активни податоци или тековни архиви: ова се податоци за тековната употреба што ги користат одделенијата задолжени за спроведување на обработката.
- Средни архиви: ова се податоци кои повеќе не се користат, но кои сè уште претставуваат административен интерес за организацијата. Податоците се чуваат на посебни медиуми и се пребаруваат на специфичен и навремен начин.
- Конечни архиви: ова се податоци што претставуваат историски, научен или статистички интерес што го оправдува фактот

дека тие не се предмет на уништување. Архивите мора да бидат обезбедени и шифрирани ако архивираните податоци се чувствителни податоци или се сметаат за деловно доверливи.

Со цел да се одреди периодот на задржување на различни видови на записи, за збирки на податоци, треба да се земат предвид различни извори, како што е законодавството, деловните барања итн.

За да може да им се додели на записите соодветен период за задржување, мора да се создаде попис на збирките на податоци во организацијата.

КОНТРОЛА НА ПРИСТАП И АВТОРИЗАЦИЈА

Во областа на физичката безбедност и безбедноста на информациите, контролата на пристапот е селективно ограничување на пристап до место или друг ресурс. Чинот на пристапување може да значи консумирање, внесување или користење. Дозволата за пристап до ресурс се нарекува авторизација.

Пристапот до информацискиот систем каде што се обработуваат приватни и лични податоци треба да се контролира на сите три нивоа: физички, административен (логички) и технички.

Физичката заштита треба да се воспостави преку контролирање на физичкиот пристап до организациската област. Заштитата е организирана за печатена документација, компјутерска и мрежна опрема која е вклучена во обработката на приватни и лични податоци.

Административната (логичка) заштита треба да се воспостави со политики, процедури и документација за сите кориснички привилегии за целиот систем. Сите промени во шемата за пристап потребно е да бидат снимени.

Техничката заштита треба да се воспостави во секој дел од системот за информации кој ги користи сите достигнувања и можности за информатичката технологија. Заштитата се ревидира со најновата верзија на софтверот, хардверот и мрежниот протокол и соодветно се обликува.

Општиот принцип, на кој треба да се потпре дефиницијата за контрола на пристап, е дека сè е забрането, освен ако е експлицитно дозволено.

Заради едноставно контролирање, следење и дефинирање на нивоата на пристап, пристапниот систем може да се подели на неколку делови:

- Пристап до работна станица (оперативен систем на корисникот): дали е нивото дозволено за оперативниот систем на секој локален компјутер. Сите корисници имаат администраторски привилегии за своите работни станици. Секоја работна станица може да се пристапи со која било корисничка сметка на домен. Во таков случај, кога посетувате работна станица на друг корисник, моментално најавениот корисник има минимални привилегии за извршување на основните операции.
- Домен пристап: треба да се дефинира за секој корисник. Сите корисници се со исти и минимални привилегии, кои им овозможуваат да ги извршуваат потребните операции и да ги користат ресурсите за непречено функционирање на апликацијата. Администраторските привилегии не се дозволени, освен ако не е поинаку одобрено и потврдено од менаџерот за ИТ.
- Мрежен пристап: пристап до мрежните ресурси, вклучувајќи ја и WiFi мрежата, треба да се контролира со корисничка сметка на доменот.
- Пристап до системот и апликацијата: треба да се организира и да се специфицира за секој тим одделно според специфични одговорности и задачи за конкретен проект или според работното место на вработениот. Промените во структурата на

тимот мора да се применат во соодветен систем за управување со промените и со промените треба да се постапува според добро воспоставената постапка за управување со промени.

- Пристап до системски услуги (оперативни системи и бази на податоци): треба да бидат одобрени само од страна на ИТ-менаџер и ISM (Управување со информациски системи), односно нивните администратори.

Секој нов корисник дефиниран во кој било дел од системот за информации мора да потпише дека тој/таа ги разбира и се согласува со назначените права за пристап. Процедурите за барање на нови корисници, барање измени на правата за пристап на корисниците и отстранувањето на корисниците се дефинирани во соодветните документи.

Во секое време, организацијата треба да биде во можност да го извлече тековниот пристап на корисниците. Во случаи кога работникот е префрлен од една работна позиција во друга или ја напушта организацијата, привилегиите за пристап до информацискиот систем мора да се сменат или соодветно да се оневозможат (отповикаат). Организацијата треба да има силно дефинирана постапка за доделување и одземање на правата за пристап до нивниот информациски систем.

НАЈДОБРИ ПРАКТИКИ И ПРЕПОРАКИ ЗА КОНТРОЛА НА ПРИСТАП

Секој корисник мора да биде обезбеден со идентификатор кој е негов/нејзин и мора да се идентификува себеси пред секоја употреба на ресурсите за обработка на податоци.

Генеричките корисници како што се (админ, администратор, итн.) не смеат да се користат за автентикација на системот.

Распределувањето на правата за пристап на корисниците треба да се контролира од првичната регистрација на корисници до отстранување на права за пристап кога повеќе не се потребни,

вклучувајќи посебни ограничувања за привилегирани права за пристап и управување со лозинки плус редовни прегледи и надградби на правата за пристап.

Корисниците треба да бидат свесни за нивните одговорности кон одржување ефективни контроли за пристап, на пр. избирање силни лозинки и нивно чување како доверливи информации.

Информативниот пристап треба да биде ограничен во согласност со политиката за контрола на пристап, на пр. преку сигурно најавување, управување со лозинка, контрола над привилегирани услуги и ограничен пристап до изворниот код на програмата.

СИСТЕМ ЗА КОНТРОЛА НА ПРИСТАП

Дефект на контролата на пристап - Доколку системот за контрола на пристапот до компјутер или мрежа не функционира правилно, мора да се пренасочи кон одбивање на привилегиите до крајните корисници.

Посебни привилегирани корисници - Сите мултикориснички компјутерски и мрежни системи мора да поддржат посебен тип на кориснички ИД, кој има широко дефинирани системски привилегии кои ќе им овозможат на овластените лица да ја променат безбедносната состојба на системите.

Автентикација на корисник на оперативен систем - програмерите не смеат да конструираат или да инсталираат други механизми за идентификација или автентикација на идентитетот на корисниците без претходна дозвола од управата.

Модификација на системот за контрола на пристап - Функционалноста на сите системи за контрола на пристап не смее да се преиначува, да се замени или да се заобиколи преку воведување на дополнителен код или инструкции.

Пронаоѓање на лозинка - Компјутерските и комуникациските системи мора да бидат дизајнирани, тестирани и контролирани за да се спречи и пронаоѓање и неовластено користење на зачувани

лозинки, без разлика дали лозинките се појавуваат во криптирана или некриптирана форма.

Информации за контрола на пристап во е-колачиња - информациските системи никогаш не смеат да складираат какви било информации за контрола на пристап во е-колачиња, депонирани или складирани на компјутерите на крајните корисници.

Системски способности и команди – На крајните корисници мора да им се овозможат само оние системски способности и команди за кои тие имаат привилегии за користење.

ОВЛАСТУВАЊЕ

Пристап до чувствителни или вредни информации - Пристапот до чувствителните информации мора да се обезбеди само откако ќе се добие експресно овластување за управување.

Давање пристап до информации од организација - Пристапот до информации секогаш треба да биде овластен од назначен сопственик на такви информации и треба да биде ограничен на база на знаење-по-потреба на разумно ограничен број луѓе.

Употреба на привилегија на информацискиот систем - Секоја привилегија на информацискиот систем што не е посебно дозволена од страна на управата, не треба да се користи за која било деловна намена додека не биде одобрена во писмена форма.

Доделување на системски привилегии - Привилегии за компјутерски и комуникациски систем треба да се доделуваат само преку јасна хиерархија на делегирање на овластувања.

ИД на корисникот и одобрување на привилегија - Секогаш кога корисничкиот ИД, системските привилегии за бизнис-апликација или системските привилегии вклучуваат можности кои ги надминуваат оние кои рутински им се доделуваат на општите корисници, тие треба однапред да бидат одобрени од непосредниот супервизор и менаџмент на корисникот.

Овластување од сопственикот за привилегиите - Пред да

бидат доделени на корисници, привилегиите за деловната системска апликација треба да бидат одобрени од важечкиот сопственик на информациите.

Овластување на барање за пристап до системот - Сите барања за дополнителни привилегии за мултикориснички системи или мрежи треба да се достават во пополнета форма за барање за пристап до систем кое го одобрува непосредниот менаџер на корисникот.

Стандардни кориснички привилегии - Без конкретно писмено одобрување од управата, администраторите не треба да доделуваат никакви привилегии на ниту еден корисник, освен електронска пошта и обработка на текст.

Обука за компјутерски пристап - Сите корисници треба да завршат одобрен курс за обука за безбедност на информации на годишна основа.

ДОДЕЛУВАЊЕ НА ПРИСТАП И ПРИВИЛЕГИИ

Пристап до информации за оперативниот персонал - Контролите за пристап до програмите за производство и информации треба да бидат такви што персоналот за компјутерски операции е ограничен од софтверот за модифицирање на системи, апликативниот софтвер и информациите за производство.

Ограничување на привилегија - знаење по потреба - Привилегиите на компјутерот и системот за комуникации на сите корисници, системи и програми треба да бидат ограничени на основа на знаење по потреба.

Пристап на развојниот програмер до деловни информации за производството - Каде што е потребен пристап до деловни информации за производството со цел да се развиваат или тестираат нови или модифицирани бизнис-апликациски системи, треба да се одобри пристап само со„читање“ и„копирање“ на производствените машини. Овој пристап е дозволен само за времетраењето на тестирањето и поврзаните развојни дејства и после успешното завршување на овие дејства пристапот треба веднаш да биде отповикан.

Пристап до информации во производствени апликации - На персоналот за развој на деловен апликациски софтвер не треба да му биде дозволен пристап до производствените информации. Исклучок може да биде направен во случај кога производствените информации се релевантни за конкретниот апликациски софтвер на кој овој персонал тековно работи.

Пристап до лични информации - Сите информации за идентификување на клиенти, како што се броеви на кредитни картички, кредитни референци и броеви за социјално осигурување, треба да бидат достапни само на оние вработени лица на кои им е потребен таков пристап за извршување на нивните работни задачи.

СИСТЕМСКИ ПРИВИЛЕГИИ

Број на привилегирани кориснички ИД-и - Бројот на привилегирани кориснички ИД-и треба да биде строго ограничен на оние лица кои апсолутно треба да имаат такви привилегии за овластени деловни цели.

Пристап до команди на оперативниот систем - крајните корисници не треба да бидат овластени да користат команди на оперативно системско ниво.

ЗАПИСИ

Задржување на дневникот за контрола на привилегиите за пристап - Компјутеризираните записи што ги одразуваат привилегиите за пристап на секој корисник на мултикориснички системи и мрежи, треба да бидат безбедно одржувани во разумен временски период.

Содржини на дневникот на системот за производствени апликации - Сите компјутерски системи што работат преку системски производствени апликации треба да содржат дневници во кои се запишуваат дополнувањата и промените на привилегиите на корисниците.

Записи за кориснички ИД - Записите што ги одразуваат сите ко-

мпјутерски системи на кои корисниците имаат кориснички ИД-и треба да бидат актуелни.

ПРЕГЛЕД НА ПРИСТАП

Преглед на кориснички профили користени во апликации и поврзувачки софтвер - годишно треба да се прегледуваат привилегиите на посебните кориснички профили кои се користат во производствените апликации или за поврзувачкиот софтвер.

Повторно овластување на привилегиите за кориснички пристап - Системските привилегии доделени на секој корисник треба да бидат преиспитани од непосредниот менаџер на корисникот на секои три месеци за да се утврди дали тековно-одобрените системски привилегии се потребни за извршување на тековните работни задачи на корисникот.

ПОЛИТИКА ЗА АВТЕНТИКАЦИЈА НА ЛОЗИНКА

Препораки за користење на лозинки:

- Лозинките на системско ниво треба да се менуваат најмалку на секои шест месеци.
- Лозинките на корисничко ниво (на пример, е-пошта, десктоп компјутер, итн.) се менуваат барем еднаш во 90 дена.
- Корисничките профили кои имаат привилегии на системско ниво, доделени преку групно членство или програми, имаат различна лозинка од сите други профили што ги држи тој корисник.
- Внесот на лозинки во е-пораки или други форми на електронска комуникација е регулиран. Кога ќе се јави потреба за соопштување на лозинка, потребно е да се испрати со користење на алтернативен начин на комуникација, на пр. ко-

рисничкот ИД се испраќа преку е-пошта, а лозинката се доставува посебно во текстуална порака.

- Историјата на лозинката е поставена за да зачува до 24 лозинки за секој корисник. Ова ќе ги обесхрабри корисниците да одат напред и назад помеѓу множество на заеднички лозинки.

ОПШТИ ПРАВИЛА ЗА СОСТАВУВАЊЕ НА ЛОЗИНКИ

Лозинките се користат за разни намени. Некои од почестите користења вклучуваат: сметки на кориснички профили, веб-сметки, сметки за е-пошта или заштита на екранот. Секој треба да биде свесен за соодветен начин за избирање силни лозинки, а тоа значи дека лозинката треба да ги исполнува следните препораки:

- Лозинката не треба да ги содржи целото или дел од корисничкото име на сметката на корисникот. Дел од името на корисничката сметка е дефинирано како три или повеќе последователни алфанумерички знаци ограничени на двата краја со бел простор како што се простор, таб и враќање и кој било од следниве знаци: запирка (,), точка (.), цртичка (-), долна црта (_) или знак за број (#).
- Лозинката треба да биде долга најмалку 6 знаци.
- Лозинката треба да содржи знаци од најмалку три од следниве четири категории:
  - Латинични големи букви (од A до Z)
  - Латинични мали букви (од a до z)
  - Основните 10 броја (од 0 до 9)
  - Неалфанумерички знаци како што се: извичник (!), знак за долар ($), знак за број (#) или проценти (%).
- Лозинката не треба да се базира на лични податоци, имиња на семејството итн.
- Лозинката не треба да биде запишана или складирана на интернет.

Лошите и слаби лозинки ги имаат следните карактеристики:

- Содржат помалку од седум знаци.
- Тие се збор од речник (англиски или странски).
- Тие се збор со честа употреба
- o Имиња од семејството, миленичиња, пријатели, соработници, фантастични ликови итн.
- Компјутерски термини и имиња, команди, веб-страници, компании, хардвер, софтвер.
- Родендени и други лични податоци, како што се адреси и телефонски броеви.
- Обрасци од букви или броеви како што се aaabbb, qwerty, zyxwvuts, 123321, итн.
- Секое од горенаведените напишани наназад.
- Секое од горенаведените со претходно додаден број или проследено со додаден број (на пр., тајна1, 1тајна).

Лозинките треба да се креираат на начин кој лесно може да се запамети. Еден начин да се направи ова е да се создаде лозинка врз основа на наслов на песна, афирмација или друга фраза. На пример, фразата може да биде: „Ова може да биде еден начин да се сеќавате“ и лозинката може да биде: „OmDb1nDsS!“ или „Omdb1N>Ss~“ или некои варијации.

Не користете ниту еден од претходните примери како лозинки!

Лозинките не се споделуваат со никого. Сите лозинки се чувствителни, доверливи информации.

Еве листа на „не“:

- Не откривајте лозинка никому по телефон.
- Не откривајте лозинка во е-порака.
- Не зборувајте за лозинка пред другите.
- Не го наговестувајте форматот на лозинка (на пр. „моето презиме“).

- Не откривајте лозинка на прашалници или безбедносни формулари.
- Не споделувајте лозинка со членовите на семејството.
- Не откривајте ваша лозинка на соработник кога одите на одмор.
- Не ја запишувајте лозинката и не ја чувајте никаде во вашата канцеларија.
- Не чувајте лозинки во датотека на кој било компјутер, вклучувајќи мобилен, без енкрипција.
- Не ја користете функцијата „Запомни лозинка“ на некоја апликација како што се Eudora, Outlook или Netscape Messenger.

ЧИСТО БИРО, ЧИСТ ЕКРАН

Додека работат на своето биро, вработените често се прекинувани од различни причини поради кои ги напуштаат бироата, како што се вонредни ситуации, планирани или непланирани состаноци или едноставно пауза. Оваа ситуација претставува голем ризик за откривање на доверливи информации кои се наоѓаат на хартиени документи оставени на работната маса, белешки во тетратка, информации што се оставени на компјутерските екрани, медиуми за чување на податоци што се оставени на бирото како што се USB-флеш дискови, CD итн. Оваа ситуација исто така може да претставува голем ризик за неовластен пристап и вршење на активности во име на отсутен работник.

На овој начин организациите треба да спроведат посебни безбедносни мерки за да ги ублажат таквите случаи. Вработените треба да бидат свесни за таквиот ризик и да бидат подготвени како да ракуваат правилно со информациите и средствата и да ги обезбедат информациите и материјалите што се чуваат на работниот простор. Одговорност на организацијата е да се посвети на политиката: чисто

биро, чист екран, со цел да се постават јасни правила и да се обезбедат прецизни постапки со цел да се насочи однесувањето на вработениот во такви ситуации.

Компјутерската опрема која е најавена во систем, а е без надзор може да претставува примамлива цел за бескрупулозниот персонал или трети лица во просториите.

Неовластен пристап на ненадгледувана работна станица може да резултира со штетни или измамнички записи, на пр. модификација на податоци, лажна употреба на е-пошта итн.

Пристап до работна станица без надзор може да резултира со оштетување на опремата, бришење на податоци и/или модификација на системски/конфигурациски датотеки.

За среќа, повеќето практики се нискотехнолошки и лесни за имплементирање, како што се:

- **Употреба на заклучени простори:** фиоки, архивски ормари, датотечни соби, да има на располагање сефови за чување на информациите. На крајот на секој ден, или кога бироата/канцелариите се испразнети, секоја чувствителна информација да е заклучена или во фиока или во датотечни ормари.
- **Отстранување на информации:** Сите хартиени отпадоци, кои имаат некакви лични или доверливи информации или податоци, треба да се уништат. Под никакви околности овој вид на отпадна хартија нема да биде фрлена со вообичаеното ѓубре во кантите за отпадоци.
- **Да се ограничи употребата на капацитетите за копирање/печатење:** Чувствителните или класифицирани информации, откако ќе се отпечатат, веднаш да се тргнат од печатачот.
- **Обезбедување на хартиените документи:** Пред клиентот да влезе во просториите за консултации, сите документи од претходниот клиент да бидат отстранети.
- **Обезбедување на уреди/информациски системи:** Секогаш кога работната станица е оставена без надзор и компјутерот е вклучен, вработениот треба да го заклучи својот ек-

ран со притискање на копчињата „Ctrl + Alt + Delete“ и потоа Enter. Заклучувањето на екранот на работната станица не само што спречува некој друг (кој не е сопственик на работната станица) да ја користи оваа работна станица, туку исто така спречува и некој да чита доверливи информации што се оставени отворени на екранот на оваа работна станица. Сите компјутери, лаптопи и работни станици треба да се обезбедени со екрански чувар (screensaver) заштитен со лозинка со автоматска функција за активирање поставена на 5 минути или помалку или со одјавување при напуштање на работната станица.

- **Обезбедување на уреди/информациски системи:** Кога вработен или негов соработник во моментот работи на чувствителни информации, а има посетител на неговото/нејзиното биро, екранот треба да е заклучен за да се спречи читање на содржината.
- **Обезбедување на уреди/информациски системи:** Компјутерите и сличните уреди треба да бидат поставени на таков начин на кој ќе се избегне луѓето што минуваат да имаат шанса да гледаат во нивните екрани.
- **Обезбедување на уреди/информациски системи:** Сите вработени и соработници се одговорни за сите терминални активности и трансакции внесени преку нивниот кориснички ИД, без разлика дали биле присутни во тоа време или не.

Едноставни совети:

- **Ако се сомневате - уништете го.**
- **Ако не сте сигурни дали треба да се зачува некое парче хартија - веројатно ќе биде подобро да го ставите некаде заклучено.**
- **Користете уништувач за канцелариската хартија која повеќе не е потребна.**
- **Не ги печатете е-писмата за да ги прочитате. Ова само создава зголемено количество на неред.**

- **Проверувајте ги работите на вашата работна маса за да бидете сигурни дека ви се потребни, а она што не ви треба фрлајте го.**
- **Справувајте се со секое парче хартија само еднаш – дејствувајте по него, поднесете го или уништете го.**
- **Секогаш расчистете ја работната површина пред да си одите дома.**
- **Размислете за скенирање на хартиените предмети и нивно поднесување во вашиот компјутер.**

ШИФРИРАЊЕ

Кога се користи во врска со другите безбедносни мерки, шифрирањето е моќен метод за обезбедување на податоци во мирување (информации зачувани на компјутери и уреди за складирање) и податоци во транзит. Тоа овозможува безбедно складирање и пренос на податоци на надворешни странки. Откако датотеката е шифрирана, станува тешко за надворешни лица да ја пробијат и да добијат пристап до чувствителни лични информации. Шифрираните податоци се потполно нечитливи за сите освен за вас или за нивниот наменет примач.

При обработка на податоци, постојат голем број области каде што употребата на шифрирање може да биде од полза. Двете главни цели за кои треба да се разгледува користење на шифрирање се складирање на податоци и пренос на податоци. Овие две активности може да се именуваат и како податоци во мирување и податоци во транзит.

Шифрирањето треба да се користи колку што е можно повеќе, на кој било уред или област, како што се следниве:

- **Сообраќај на податоци.** Користењето на небезбедна Wi-Fi мрежа на јавно место ве прави ранливи на напади. Со вир-

туелна приватна мрежа (VPN), корисниците пристапуваат кон сервер од трети лица, кој ги шифрира информациите. Шифрирањето обезбедува сигурен пренос на податоци не само на интернет-мрежи, туку и на мобилни телефони, безжични микрофони, безжични домофони, Bluetooth уреди, банкарски банкомати итн.

- **Преносни уреди.** Користењето на преносни уреди (како лаптопи, мобилни телефони, надворешни дискови, УСБ-флеш дискови итн.) е лесен начин за пренесување на датотеки и пристап до информации, но и голем ризик од кражба или загуба. За среќа, разни производи за шифрирање го задржуваат преносливиот медиум шифриран во случај да паднат во погрешни раце.
- **Комплетни хард дискови.** Лозинката за најава на компјутер нема да биде многу корисна доколку некој го украде хард дискот. Откако ќе се приклучи на друг компјутер, уредот ќе му овозможи на крадецот да ја добие целата содржина. Шифрирањето на податоците зачувани на дискови може да ја спречи загубата и злоупотребата на податоците.
- **Лозинки.** Најосновна компонента на шифрирање е вашата лозинка. За лозинка која е најотпорна на хакирање, одете на долг код - 10 или повеќе знаци - што вклучува и големи и мали букви, бројки и специјални знаци. Дајте му на секој уред или систем посебна лозинка и чувајте ги на сигурно место доколку нивното паметење ви е премногу тешко.
- **Складирање во облак.** Услугите како Dropbox овозможуваат вградено шифрирање на податоците, кое нуди заштита додека вашите информации остануваат на нивните сервери. Сепак, тие исто така поседуваат и клучеви за дешифрирање, што им дава пристап до вашите информации под одредени околности.

Претпоставката дека вашиот бизнис е премногу мал за неговите податоци да бидат привлечни за хакери, крадци на идентитети и слични непристојни ликови, може да биде опасна грешка.

Информациите се шифрираат и дешифрираат со користење на таен клуч. Без клучот, до информацијата не може да се пристапи и на тој начин е заштитена од неавторизирана или незаконска обработка.

Исто така, не треба да се потценува и важноста на добро управување со клучот. Организациите треба да ја обезбедуваат тајноста на клучевите за шифрирањето да биде ефикасно.

АНТИВИРУС СОФТВЕР

Вирус скрининг софтверот (антивирусот) треба да се инсталира и овозможи на сите интернет-врзани конекции на организациијата. Вирус скрининг софтверот е исто така потребен на сите сервери за е-пошта, одделенски сервери, и десктоп персонални компјутери. Софтверот за скрининг на содржини и софтверот што ги блокира корисниците да пристапуваат до одредени неделовни веб-страници, исто така, треба да бидат овозможени на сите интернет-врзани конекции.

Мора да се применуваат последните верзии и закрпи на дефинициите (антивирус дефиниции). Закрпувањето мора да биде редовно и по можност централизирано.

ЗАШТИТНИ ЅИДОВИ (FIREWALLS)

Клиентски, или „лични“, заштитни ѕидови - Сите компјутери на кои им е потребна поголема заштита од онаа што може да ја обезбедат заштитните ѕидови близу до работ на мрежата - определено со должно внимание или со проценка на ризикот – имаат потреба од имплементација на клиентски („личен“) заштитен ѕид. Исто така, сите преносни компјутери кои можат да се користат надвор од доверлива мрежа имаат потреба од личен заштитен ѕид.

Посветена функционалност на заштитниот ѕид – заштитните ѕидови работат на посветени машини кои не вршат други услуги, како на пример да не се користат како сервер за е-пошта; заштитниот ѕид не смее под никакви околности да се постави на виртуелен сервер. Сите непотребни и неискористени системи и мрежно управувачки софтвери и услуги треба да бидат отстранети од заштитниот ѕид на организацијата, до степен до кој оперативниот систем за поддршка го дозволува тоа.

Потребна документација - Пред распоредувањето на секој заштитен ѕид, треба да се креираат дијаграм и/или листа на дозволени патеки и опис на дозволените услуги, придружени со оправдување за секоја, а потоа да се одржуваат за секоја конфигурациска промена.

Одобрување на пристап - Дозволата за овозможување на такви патеки и услуги треба да се одобри според процедурите за контрола на пристап. Тие треба да се доделуваат само кога овие патеки или услуги се неопходни за важни деловни причини, а притоа треба постојано да се применуваат задоволителни безбедносни мерки. Секоја промена на патеки или услуги треба да помине низ истиов процес како што следува.

ИМПЛЕМЕНТАЦИЈА

Поврзувања помеѓу машините - Конекциите во реално време помеѓу два или повеќе компјутерски системи не треба да се воспостават или да се овозможат, освен ако не е јасно утврдено и одобрено од страна на одговорното лице дека таквите конекции нема да ја загрозат безбедноста на информациите. Во многу случаи, треба да се користат заштитни ѕидови или слични посредни системи. Ова барање се применува без оглед на користената технологија, вклучувајќи ги безжичните врски, микробранови врски, кабелски модеми, интегрирани услуги за дигитални мрежни линии и дигитални конекции за претплатнички линии. Секоја поврзаност помеѓу внатрешниот производствен систем на организацијата и некој надворешен компјутерски систем или која било надворешна

компјутерска мрежа или давател на услуги треба однапред да биде одобрена од одговорното лице. Улогата на одговорното лице треба јасно да се назначи и дефинира.

Надворешни врски - Сите внатрешни интернет-врски врзани во реално време со внатрешните мрежи на организацијата или со повеќекорисnички компјутерски системи треба да поминат низ заштитен sид пред корисниците да стигнат до банерот за најава. Компјутерскиот систем на организацијата може да биде прикачен на интернет само кога е заштитен со заштитниот sид. Сите лични компјутери или мобилни уреди со дигитална претплатничка линија или поврзување со кабелски модем треба да користат одобрен „личен" или клиентски, заштитен sид.

Виртуелни приватни мрежи - Сиот дојдовен сообраќај, со исклучок на интернет-пошта, одобрени известувачки услуги и пуш емитувања (push broadcasts), кој пристапува во мрежите на организацијата треба да се шифрира со еден од одобрените VPN-производи.

Заштитени подмрежи - Деловите од внатрешната мрежа на организацијата кои содржат чувствителни или вредни информации, како што се компјутерите што ги користи Одделот за човечки ресурси, треба да користат заштитена подмрежа. Пристапот до оваа и другите подмрежи треба да биде ограничен со заштитни sидови и други мерки за контрола на пристап. Врз основа на периодични проценки на ризикот треба да се идентификуваат заштитени подмрежи потребни во архитектурата на информацискатa безбедност.

Демилитаризирани зони - Сите сервери за интернет-трговија, вклучувајќи ги платежните сервери, серверите за бази на податоци и веб-серверите треба да бидат заштитени со заштитни sидови и да се наоѓаат во демилитаризирана зона (DMZ), подмрежа која е заштитена од интернет преку еден или повеќе заштитни sидови. Внатрешната мрежа, како што е интранет, исто така е заштитена од DMZ-подмрежата со еден или повеќе заштитни sидови.

Обелоденување на информации за внатрешна мрежа - Адресите на внатрешниот систем, конфигурациите, распоредените произво-

ди и слични информации за дизајн на системот за мрежни компјутерски системи се ограничени да ги спречат и системите и корисниците надвор од внатрешната мрежа на организацијата да пристапуваат до овие информации. Преводот на мрежни адреси (NAT) е најпосакувана метода за заштита на внатрешните IP-адреси. Стандардите за конфигурација и работење се имплементираат и одржуваат за да спречат внатрешните деловни информации да бидат одомаќинети на или да се обработуваат од страна на кој било заштитен sид, сервер или некој друг компјутер што се дели со друга организација во објект за аутсорсинг. (Дозволиво е обезбедување на заеднички рутери, хабови, модеми и други мрежни компоненти од страна на аутсорсинг организација).

Одредува на одбивање (Default To Denial) - Секоја патека на поврзување и услуга што не е посебно дозволена со овој стандард и поддршка треба да бидат стандардно блокирани од заштитните sидови на организациите. Листите на тековно одобрени патеки, услуги и апликации треба да бидат документирани.

Проширена автентикација на корисник - Влезниот сообраќај - со исклучок на интернет, електронска пошта, редовни дистрибуции на новости и пуш емитувања претходно одобрени од одговорното лице - побарува една или повеќе од следниве проширени мерки за проверка на корисникот, документирани подолу.

- Динамички лозинки
- Дигитални сертификати

Механизми за пристап до заштитниот sид - Сите заштитни sидови треба да се конфигурираат со единствени лозинки или други механизми за контрола на пристап и за основниот оперативен систем (ако тоа е применливо и достапно) и за резидентната апликација за заштитен sид. Групни кориснички ИД-и не се дозволени ниту иста лозинка или ист контролен код за пристап не треба да се користат на повеќе од еден заштитен sид.

Привилегии за пристап до заштитен sид - Привилегиите за менување на функционалноста, поврзаноста и услугите поддржани од заштитните sидови се ограничени на администраторите за зашти-

тниот sид.

Физичка безбедност на заштитниот sид - Сите заштитни sидови надвор од обезбедениот центар за податоци треба да се наоѓаат во затворени простории, плакари или кабинети кои ги исполнуваат стандардите за физичка безбедност и кои се достапни само за овластени администратори за заштитен sид и на организацијата за физичка безбедност. Кога заштитните sидови се стават во општ центар за обработка на податоци, тие треба да се инсталираат во посебно затворени простории, области, кафези или ормари со решетки.

ОПЕРАТИВНОСТ НА ЗАШТИТЕН SИД

Мониторинг на слабости - Администраторите за заштитен sид се очекува да се претплатат на најдобрите интернет-советници за предупредување како и други релевантни извори кои обезбедуваат тековни информации за слабостите на заштитниот sид. Секоја ранливост која се чини дека влијае врз мрежите и системите на организацијата веднаш треба да биде дадена до знаење на одговорното лице.

Детекција на упад\Спречување на упад - Сите заштитни sидови треба да вклучуваат барем една или повеќе методи за откривање на упад и/или методи/системи за спречување на упад.

Секој од овие системи за откривање/заштита од упад треба да се конфигурира според спецификациите дефинирани од мрежните операции. Алармите од овие системи за откривање \ заштита од упад се конфигурирани веднаш да го известат по пејџер, мобилен телефон или друг мобилен уред, техничкиот персонал кој е на повик за да преземе корективни мерки.

Дневници на заштитен sид - Сите заштитни sидови треба да се конфигурираат да водат дневник на настани според следниве стандарди за бележење на активности на заштитниот sид:

- Сите промени на конфигурациски параметри на заштитниот sид, овозможени услуги и дозволени патеки за поврзување.

- Сите сомнителни активности кои можат да бидат индикации за неовластена употреба или обид за компромитирање на безбедносните мерки.
- Заштита на дневниците со контролни суми, дигитални потписи и/или шифрирање.
- Навремено отстранување на дневниците од системите за снимање и складирање во физички заштитени подрачја или во сеф на најмалку шест месеци.
- Периодичен преглед на дневникот за да се обезбеди сигурно работење на заштитните ѕидови.

Системи за управување со мрежа – Заштитните ѕидови треба да се конфигурираат така што тие да:

- се видливи за внатрешните мрежни системи за управување и
- дозволуваат овластена употреба на одобрени далечински автоматски алатки за ревизија.

Редовно тестирање - Според оваа политика, отпорноста и правилната конфигурација на заштитните ѕидови на организацијата се тестираат на редовна основа. Каде што набавениот софтвер го поддржува тоа, ова тестирање користи софтверски агенти кои автоматски проверуваат за да утврдат дали заштитниот ѕид останува конфигуриран и работи на саканиот начин. Овој процес на тестирање вклучува разгледување на дефинирани конфигурациски параметри, овозможени услуги, дозволени патеки за поврзување, тековни административни практики и соодветност на распоредените безбедносни мерки. Овие тестови, исто така, вклучуваат и периодично извршување на софтверот за идентификација на ранливост и редовно изведување на тестови за пенетрација.

СОФТВЕРСКИ ЗАКРПИ

Софтверските закрпи (software patches) многу често содржат поправки на безбедносни слабости и други грешки и затоа е од голема важност редовното одржување на компјутерската опрема и софтвер. Особено, безбедносниот софтвер, како што се антивирус и антималициозен софтвер, треба редовно да се ажурира, со цел да продолжи да обезбедува соодветна заштита од нови закани.

Одржувајте го софтверот во тек со редовна проверка за надградби и нивна примена. Повеќето софтвери може да се постават на автоматско ажурирање.

Софтверските закрпи мора да бидат дел од редовните операции за одржување. Евиденција за најновите нивоа на закрпа за секој софтвер (без оглед дали е ОС или апликативен софтвер, безбедносен софтвер или системи на бази на податоци) треба да се одржува и редовно да се споредува со новите достапни закрпи.

ДАЛЕЧИНСКИ ПРИСТАП

Многу често, не може да се одбегне потребата од доделување на далечински пристап на вработените до организациската мрежа и информативните ресурси. Никогаш не знаете кога ќе се појави потреба од член на тимот итно да пристапи до својата деловна е-пошта, да се поврзе со интранетот на компанијата или да пристапи до други ранливи средства на компанијата од оддалечена локација со цел да си ја изврши својата работа.

ТЕХНОЛОШКИ ОПЦИИ

Далечински пристап може да се постигне со различни технологии:

- Поврзување со систем за обработка на податоци од оддалечена локација, на пример, преку услуга за далечински пристап или виртуелна приватна мрежа. Постојат два основни методи за распоредување VPN - базирани далечински пристапи: интернет протокол безбедност (IPsec) и безбедносен приклучен слој - Secure Sockets Layer (SSL). Додека многу решенија нудат или Ipsec или SSL, постои можност и за двете технологии интегрирани на една платформа со унифициран менаџмент
- Далечински десктоп софтвер, софтвер кој дозволува апликациите далечински да се одвиваат на сервер, додека локално го прикажува графичкиот излез
- Емулација на терминал - кога се користи за поврзување со далечински систем. Може да користи стандардни алатки како:
  - o telnet - софтвер кој се користи за интеракција преку мрежа со компјутерски систем
  - o ssh - безбедна школка: често се користи со далечински апликации
- Активирање на карактеристиките на деловниот телефонски систем надвор од просториите на бизнисот
- Далечински пристап, систем на огласни табли засновани на ДОС
- Пристап до далечинска база на податоци, протокол стандард за пристап до базата на податоци

БЕЗБЕДНОСНИ РАЗГЛЕДУВАЊА

Црвите, вирусите, шпионскиот софтвер, хакирањето, кражбата на податоци и злоупотребата на апликации се сметаат за најголемите безбедносни предизвици во денешните мрежи. Далечинскиот при-

стап и далечинското канцелариско VPN-поврзување се чести точки на влез за таквите закани, поради начинот на кој VPN-и се дизајнирани и распоредени. Незаштитената или нецелосна VPN-безбедност може да го дозволи следново:

- VPN сесии на далечински корисник да донесат малвер во мрежата на главната канцеларија, предизвикувајќи појава на вируси кои ги инфицираат другите корисници и мрежните сервери;
- Корисници да генерираат несакан сообраќај на апликации, како што е споделување на датотеки од точка до точка (peer-to-peer), во мрежата на главната канцеларија, предизвикувајќи бавни мрежни сообраќајни услови и непотребно трошење на скап WAN пропусен опсег (bandwidth);
- Поединци да крадат чувствителни информации, како што се преземени клиентски податоци, од десктоп компјутер на корисник поврзан на VPN;
- Хакери да хакираат VPN-сесии со далечински пристап, обезбедувајќи пристап на хакерите до мрежата како да се легитимни корисници.

За борба против овие закани, десктоп компјутерот на корисникот и VPN-портата на која корисникот се поврзува треба да бидат соодветно обезбедени на следниов начин:

- Кориснички десктоп компјутери: Безбедносни мерки на крајната точка, како што се безбедност на податоци за датотеки и податоци генерирани или преземени за време на VPN-сесијата, плус антишпионски софтвер, антивирус и личен заштитен ѕид.
- VPN-порта: Интегриран заштитен ѕид, антивирус, антишпионски софтвер и превенција на упад. Алтернативно, ако VPN-портата не ги овозможува овие безбедносни функции, VPN-портата може да се надгради со посебна безбедносна опрема за да обезбеди соодветна заштита.

Во безбедносната инфраструктура на многу организациски мрежи постојат технологии потребни за ублажување на малициозен софтвер, како што се црви, вируси и шпионски софтвер, како и за спречување на злоупотреба на апликации, кражба на податоци и хакерство. Во повеќето случаи, поради матично шифрирање на VPN-сообраќајот, тие не се распоредени на начин што ја штити VPN со далечински пристап.

Иако можете да купите и инсталирате дополнителна безбедносна опрема за да го заштитите вашиот VPN, најекономичен и оперативно ефикасен метод за обезбедување на далечински пристап е да барате VPN-порти кои нудат локални програми за ублажување на заканата од малициозни програми и апликации за заштитен ѕид како интегрален дел од производот.

Имате трослојна одбранбена линија за заштита за далечински пристап до вашата мрежа: антивирус, заштитен ѕид и VPN. Тимот за мрежна безбедност треба постојано да ги следи сигналите од овие одбрани.

Далечинските административни алатки треба да се конфигурираат така што, пред каква било интервенција на неговата/нејзината работна станица, треба да се добие согласност од корисникот, на пример со кликање на икона или со одговарање на порака која ќе биде испечатена на екранот.

Корисникот, исто така, треба да биде во можност да набљудува доколку далечинската помош е во тек и кога таа ќе заврши, на пример со печатење порака на екранот.

ПРЕНОСЛИВИ УРЕДИ

Преносливите уреди се погодни за употреба, но во многу ситуации, тие можат да бидат причина за компромитирање на личните податоци. Заради нивната големина лесно е да бидат украдени, изгубени, компромитирани. Но и поради нивната природа и начин на употреба, тие често може да бидат ставени во опасна компромитирана средина.

Оставањето на лаптопот во хотелскиот ресторан за време на појадокот пред состанокот, може да биде лесна цел за криминални напади.

Поврзувањето со јавна интернет-мрежа, без соодветен заштитен ѕид, може да биде опасно.

Поради тоа со преносливите уреди како што се лаптопи, мобилни телефони, отстранливи хард дискови, USB-флеш дискови, ленти итн., треба одговорно да се ракува и да се користат многу совесно.

Постојат бројни безбедносни мерки и контроли кои треба да се имплементираат за да се заштитат преносливите уреди. Овие мерки вклучуваат мерки за физичка безбедност, контроли против неовластен пристап до податоци на преносливи уреди и други мерки.

- **Преносливите уреди треба да се чуваат во видното поле на нивниот сопственик секогаш кога е тоа возможно. Потребна е голема претпазливост на јавни места како што се аеродроми, железнички станици или ресторани.**
- **Преносливите уреди треба да бидат заклучени и вон видик кога не се користат, по можност во сигурносен шкаф, ормар за складирање или сеф. Ова важи дома, во канцеларија или во хотел. Преносливите уреди никогаш не треба да се оставаат видливи без надзор во возило.**
- **Лаптопот треба да се носи и да се чува во цврста торба за лаптоп или цврста актовка за да се намалат шансите за случајно оштетување.**

- **Белешки за моделот и серискиот број на лаптопот треба да се чуваат заедно со него. Ако лаптопот е изгубен или украден, веднаш треба да се извести полицискиот оддел.**
- **Од податоците од мобилните уреди треба редовно да се прави резервна копија, според претходно дефинирани постапки, со цел да се зачува достапноста на информациите.**
- **На сите лаптопи треба да се користи одобрен софтвер за шифрирање. Треба, исто така, да се користат и обезбедат долги и силни лозинки за шифрирање. Шифрирањето обезбедува исклучително силна заштита од неовластен пристап до податоците, доколку преносливиот уред е изгубен или украден.**
- **Корпоративните преносливи уреди се доделуваат за службена употреба на овластени вработени лица. Тие не смеат да се позајмуваат или да бидат користени од други лица, како што се семејството и пријателите.**
- **Избегнувајте го оставањето на преносливиот уред најавен во систем и без надзор. Лаптопот секогаш треба да се исклучи, да се одјави или да се активира екранска заштита заштитена со лозинка, пред заминување од машината. Телефонот, исто така, мора да биде заштитен со лозинка, за да се избегне неовластена употреба.**

Надворешните мобилни уреди, исто така, треба да се сметаат за закани и нивното користење треба да се спроведува внимателно. Користењето на несигурни USB-флеш дискови на вашиот компјутер е потенцијален напад на вирус, што може да ја наруши безбедноста на вашиот компјутер како и на другите мрежни уреди, доколку сте најавени на интранет мрежа.

ДНЕВНИЦИ И РЕВИЗОРСКИ ТРАГИ

Дневници за критични апликации - Сите критични деловни апликации треба да бидат поддржани со дневници и ревизорски траги што дозволуваат систематските активности да се продолжат во рок од 15 минути.

Системски дневници за чувствителни апликации - Сите производствени апликациски системи кои што се справуваат со чувствителни лични и приватни информации треба да генерираат дневници кои го собираат секое додавање, модификација и бришење на таквите чувствителни информации.

Дневници за пристап до лични информации - Идентитетот на секој корисник кој пристапува кон приватни информации што се наоѓаат во информативните системи на организацијата треба да биде евидентиран.

Архитектура на системите за евиденциски активности - Софтверот за апликација и/или систем за управување со бази на податоци треба да води евиденција за корисничките активности и статистики поврзани со овие активности, што пак ќе им овозможи да детектираат и издаваат аларми кои ги одразуваат сомнителните деловни настани.

Ревизорски дневници на компјутерскиот систем - Евиденцијата за настани релевантни за безбедноста на компјутерите треба да обезбеди доволно податоци за поддршка на сеопфатни ревизии за ефикасноста и усогласеноста со безбедносните мерки.

Далечински-пресликувани дневници - Системот за информации за производството на секоја организација кој е достапен од која било надворешна мрежа треба да користи далечински пресликувани системски дневници.

Стандарди за регистрирање во системот издадени од Одделот за информациска безбедност – Внатрешниот стандард кој ја дефинира природата на информациите што треба да се евиден-

тираат во системските дневници на компјутерските и мрежни уреди, треба да бидат јасно дефинирани и документирани. Овие информации треба да се направат безбедно мрежно достапни со цел да поддржат различни мрежни безбедносни системи (како што се системи за детекција на упад).

Евиденција на активности на привилегиран кориснички ИД - Сите кориснички ИД-активности за креирање, бришење и промена на привилегии, извршени од администраторите на системот и други со привилегирани кориснички ИД-и, треба безбедно да се евидентирани и да се одразуваат во периодичните извештаи за управување.

Способност за производство, промена, реконструирање - Сите кориснички активности кои влијаат на информациите за производство треба да бидат целосно конструктибилни од дневниците.

Евиденција на обиди за најавување - Дали успешни или не, сите обиди за најавување иницирани од корисниците за да се поврзат со информатичките системи за производство на организацијата треба да бидат евидентирани.

Евиденција на физички пристап - Организацијата ќе одржува дневници на сите физички пристапи до заштитените подрачја, вклучувајќи електронски физички пристапни системи, видеомониторинг и пристап од посетители забележан на хартија.

Прекин, задржување и преглед на физички пристап - Организацијата ќе одржува дневник на сите објекти (вклучувајќи електронски, видео и рачно бележани дневници) за прекини на контрола на пристап за најмалку една календарска година. Овие дневници ќе бидат класифицирани како ДОВЕРЛИВИ информации и ќе бидат разгледувани само од одговорни и овластени лица пред уништувањето.

Евиденција за пристап до дневник - Пристапот до сите системски дневници и ревизорски траги на компјутерските и комуникациските системи на организацијата треба да се евидентира.

Евиденција за започнување на дневник - Започнувањето на

сите системски дневници и ревизорски траги на компјутерските и комуникациските системи на организацијата треба да се евидентира.

Евиденција на предмети на системско ниво - Создавањето и бришењето на предмети на системско ниво во компјутерите и комуникациските системи на организацијата треба да се евидентира.

СОСТАВУВАЊЕ НА ДНЕВНИК

Содржини на дневник на производствено апликациски систем - Сите компјутерски системи кои работат на организациски производствени апликациски системи треба да вклучуваат дневници со кои се регистрираат, како минимум, активностите во корисничка сесија, вклучувајќи кориснички ИД-и, датум и време на најава, датум и време на одјава, како и користените апликации, промени на критични датотеки на системски апликации, промени на привилегии на корисници и подигнувања и исклучувања на системот.

Евидентирање на безбедносно релевантни настани - Компјутерските системи кои ракуваат со чувствителни, вредни или критични информации треба безбедно да ги евидентираат сите значајни настани релевантни за безбедноста, вклучувајќи, но не ограничувајќи се на, обиди за нагаѓање на лозинка, обиди да се користат неовластени привилегии, модификации на продукциско-апликацискиот софтвер и модификации на системскиот софтвер.

Отчетност и следливост на привилегирани системски команди - Сите привилегирани команди издадени од оператори на компјутерски системи треба да се следливи до конкретни поединци преку употреба на сеопфатни дневници за евиденција.

Евиденција на лозинка - Нешифрирани лозинки, без разлика дали се правилно внесени или не, никогаш не треба да се запишуваат во системските дневници.

Дневници на компјутерски оператори - Сите мултикориснички производствени системи треба да имаат дневници на компјутерски

оператори кои покажуваат време на стартување и стопирање на производствените апликации, време на подигнување на системот и време на рестартирање, промени на системските конфигурации, системски грешки и преземени корективни мерки и потврда дека е постапувано правилно со датотеките и производството.

Движењето на тајните информации треба да се следи и евидентира - Електронските движења на тајните информации на организацијата треба да се следат и да се евидентираат преку систем за филтрирање на содржини одобрени од Секторот за информатичка безбедност.

Снимање на приватни информации во ревизорски траги или дневници - информативните системи треба да се конфигурираат така што нема да собираат приватни информации во ревизорските траги или дневници.

НАДГЛЕДУВАЊЕ

Зачестеност на прегледи на дневникот - Секој дневник и ревизорска трага направени од компјутерскиот или комуникацискиот систем на организацијата треба да се разгледуваат дневно.

ПРИСТАП

Пристап до дневници - Сите дневници на системот и апликацијата треба да се одржуваат во форма која не може да ја гледаат неовластени лица. Овластените лица имаат лесно докажлива потреба за ваков пристап за извршување на нивните редовни должности. Сите други кои бараат пристап до овие дневници најпрво треба да добијат одобрение од одговорното лице.

РЕЗЕРВНА КОПИЈА И ОБНОВУВАЊЕ

Резервните копии на личните податоци мора да бидат направени и тестирани редовно, во согласност со усвоената политика за резервни копии. Резевните копии на податоците се од клучно значење за да се обезбеди достапност на податоци и континуитет на работењето.

Резервни копии на податоци – За сите критични деловни информации и критичен софтвер кои се во компјутерските системи на организацијата треба да се прават резервни копии периодично, најмалку еднаш неделно.

Процес на правење резервни копии – Поединечните и целосни резервни копии за сите крајни корисници треба да се вршат редовно според претходно дефиниран распоред. Фреквенцијата на резервната копија треба да биде планирана според ризикот и вредноста на складираните информации, врз основа на проценитe на ризик и постапките за континуитет на бизнис- работењето.

Резервна копија во предобработка - Процесот на производствена серија не треба да започне, без да се направи резервна копија во предобработката која ги вклучува сите главни датотеки и главни бази на податоци.

Резервни копии на критични информации - Треба да се прават резервни копии на критичните информации и критичниот софтвер најмалку еднаш на три месеци на архивски медиуми за чување и истите и да се чуваат најмалку една година.

ПРОЦЕДУРИ

Главни копии на софтвер - Сите софтвери за лични компјутери треба да бидат копирани пред првичната употреба, овие главни копии треба да се чуваат на сигурна и безбедна локација, дополнително овие главни копии не треба да се користат за обични деловни активности.

Резервни датотеки на дофат - Најмалку една генерација на резервни датотеки треба да се одржуваат на невмрежени медиуми за чување податоци каде што се наоѓаат компјутерите за производство.

Повеќе резервни копии - Најмалку две неодамнешни и целосни резервни копии, направени на различни датуми, кои содржат критични записи за организацијата секогаш треба да се складирани надвор од локацијата.

Сите електронски комуникации се снимаат и архивираат - Сите електронски комуникации испратени преку организациските мрежи, вклучувајќи електронска пошта, инстант пораки и гласовни пораки, треба да бидат снимени и архивирани.

МЕДИУМИ

Складирање на медиумите со резервни копии - Основните деловни информации и резервни копии од софтвер треба да се чуваат на еколошки заштитена локација со контролиран пристап, која е доволно оддалечена од објектот од кој потекнува. Пристапот до овие области треба да биде контролиран и одобрен.

Шифрирање на медиум за резервна копија - Сите чувствителни, вредни или критични информации запишани на компјутерските медиуми за резервни копии и складирани надвор од канцелариите на организацијата треба да се шифрираат.

Корисниците обезбедуваат свои медиуми за резервни копии - Корисниците треба да обезбедат сопствени медиуми за чување на податоци, да си направат самите резервни копии од важни датотеки и никогаш да не користат хард дискови и други уреди за складирање на податоци прикачени на десктоп компјутерите со јавен пристап на организацијата за правење резервни копии.

ТЕСТИРАЊЕ И ПРЕГЛЕД

Тестирање на медиумите за архивско складирање - Критичните деловни информации и критичниот софтвер архивирани на компјутерски медиуми за складирање за подолг временски период треба да се тестираат најмалку еднаш годишно за да се обезбеди дека можат целосно да бидат обновени.

Преглед на резервните копии - Одделенските раководители или од нив назначените треба да обезбедат создавање на соодветни резервни копии од чувствителните, критични и вредни податоци, доколку таквите податоци се чуваат на персонални компјутери, работни станици или други мали системи во нивната област.

Преглед на складот за медиуми со резервни копии - Секоја локација што се користи за складирање на медиуми со резервни копии на организацијата треба да се прегледува најмалку еднаш годишно за да се утврди дали складот за медиуми со резервни копии е безбеден.

СПРАВУВАЊЕ СО ИНЦИДЕНТИ

Безбедноста на информациите се однесува на заштитата на информациите (приватни и лични податоци) и информативни средства од сите видови на закани, без разлика дали се внатрешни или надворешни, намерни или случајни.

Засегнатите видови на информативни средства се:

- Информации (датотеки на податоци, бази на податоци, информации за купувачи итн.)
- Писмени документи (договори, прирачници, упатства, работни документи итн.)

- Софтвер (апликации, системски софтвер, кориснички софтвер и сл.)
- Хардвер (компјутери, медиуми, итн.)
- Луѓе (вработени, персонал, клиенти, итн.)
- Услуги (комуникациски, технички, итн.)

Дефиницијата за безбедноста на информациите е заштита на доверливоста, интегритетот и достапноста на информации, како што се:

- **Доверливост** - информациите се достапни само за лица кои имаат овластен пристап до нив и нема да бидат обелоденети на неовластени лица намерно или од небрежност
- **Интегритет** - значи дека информацискиот систем преку примена на соодветни мерки осигурува дека ќе се заштити од неовластени измени и дека содржи точни, целосни и веродостојни информации
- **Достапност** - овластените корисници можат да пристапуваат до информации и информациските системи секогаш кога имаат работна потреба

Ако кој било од трите принципи е повреден, тоа може да доведе до нарушување на безбедноста на системот, а тоа значи дека се случил **безбедносен инцидент**.

БЕЗБЕДНОСЕН ИНЦИДЕНТ

Безбедносен инцидент значи секој успешен или неуспешен обид да се добие неовластен пристап, злоупотреба, објавување, модификација или уништување на информации и други средства на информациски системи, нарушување на нормалното функционирање на информацискиот систем или нарушување на кој било од принципите на информацискиот систем за безбедносна политика. Безбедносен инцидент е безбедносен настан кој резултира со штета

како што се изгубени податоци. Инциденти, исто така, може да вклучуваат настани кои не вклучуваат штета, но претставуваат остварливи ризици. На пример, вработениот со кликнување на линк во спам-мејл што поминал преку филтри може да се гледа како инцидент.

Сите инциденти се настани, но сите настани не се инциденти.

БЕЗБЕДНОСЕН НАСТАН

Безбедносен настан е нешто што се случува, што потенцијално би можело да има импликации за безбедноста на информациите. Е-пошта со спам е безбедносен настан, бидејќи може да содржи линкови до малициозен софтвер. Организацијата може да биде погодена со илјадници или можеби милиони идентификувани безбедносни настани секој ден. Со нив обично се справуваат автоматските алатки или едноставно се евидентираат. Примери за безбедносни инциденти кои вработените треба да ги пријават се:

- Загуба или недостаток на услуга, опрема, простории, ресурси или средства:
  - Пречки во телекомуникациите
  - Исклучување од давателот на ИТ-услугите
  - Недостаток/прекини на електрична енергија
  - Прекин во работата на критичната опрема за климатизација
  - Инциденти/несреќи од природни катастрофи
  - Инциденти од појава на пожари

- Системски пречки/преоптоварување, дефект на софтверот, хардверот или комуникациите:
  - Продолжување на намалената ефикасност на апликациите
  - Подолги прекини на софтверски решенија

- Попречена точност и комплетност на податоците на клиентите и трансакциите
- Грешки во обработката на податоците

- Човечки грешки, злоупотреби, отстранување и откривање на информации и ресурси:
  - Намерно грешење со опремата
  - Неовластено откривање на доверливи информации (статус на сметка)
  - Откривање на лозинката, користење туѓа лозинка
  - Откривање на лични податоци на клиентите на трети неовластени лица
  - Грешки кои се резултат на нецелосни податоци
  - Повреда на одредбите за физичка безбедност

- Кражба на информативен систем на возила (хардвер, софтвер, комуникации):
  - Движење на неовластени лица во безбедносните зони на организацијата
  - Присуство на неовластени странски изведувачи во организацијата

- Неконтролирани системски промени и напади:
  - Хакерски напади
  - Напади на вируси
  - Напади на одбивање на услуга
  - Малициозен програмски код
  - Произволна инсталација на неодобрен софтвер или уред

- Неконтролирано менување на производството и конфигурацијата
- Несоодветно однесување на системот - индикација за напад

- Неовластен пристап до ресурси и информации
  - Неовластен пристап до компјутерска мрежа/апликација
  - Неовластен пристап до функции во апликациите за кои работникот не е овластен

- Други нарушувања на безбедноста на информативниот систем вклучуваат странки или можна причина за инцидент:
  - Вработени
  - Надворешни странки (консултанти, стажисти, студенти...)
  - Даватели на услуги

БЕЗБЕДНОСНИ СЛАБОСТИ

Информациите во кои се појавуваат слабости се закана за безбедноста на овие информации, на пример, поради постојните системи, услугите или практиките. Вработените и изведувачите кои ги користат информативните системи и услуги на организацијата треба да се обврзат да ги забележат и да ги пријават сите воочени или сомнителни слабости во безбедноста на информациите во системите или услугите.

ПРИЈАВУВАЊЕ НА ИНЦИДЕНТ

Кога ќе бидат откриени од страна на вработените или кој било друг корисник на информацискиот систем, инцидентите мора да се пријават веднаш по нивното откривање. Треба веднаш да се организира тим за брз и соодветен одговор на инцидентот.

Формално информациски процес за управување со системски проблеми мора да биде воспоставен и оперативен, со цел да се евидентираат проблемите со кои се соочува, да се намали нивната појава и да се спречи нивното повторување.

Пријавувањето на инциденти треба да се пријави и да се евидентираат основните информации за инцидентот:

- Време, датум, локација и контакт-информации за вработените кои пријавиле безбедносни инциденти;
- Дополнителни детали за инцидентот (доколку ги има);
- Информации за вклучените лица и кои јавни служби и органи се информирани (Служба за итна медицинска помош, единици за противпожарна заштита, цивилна заштита итн.);
- Дали има прекин во работата и на кој начин?
- Дали е инцидент што се случува прв пат или претходно се случиле инциденти од таа природа?
- Дали безбедносните инциденти компромитираат доверливи информации?
- Дали може лицето кое го пријавило инцидентот да ја идентификува причината/ите за него?

Кога вработениот пријавува безбедносен инцидент, се препорачува:

- Да се престане со работа и дискретно да се прекине работата во сите апликации;
- Не го исклучувајте компјутерот ниту која било активна апликација;
- Не продолжувајте да го користите системот или апликацијата сè додека ИСМ не соопшти дека е можно да продолжат нормалните операции;
- Не зборувајте за безбедносниот инцидент никому, освен на овластените лица вклучени во неговото разрешување.

Се препорачува вработените да ги пријават сите сомнителни безбедносни инциденти, без разлика дали им личат на вистински или не. Покрај тоа, за известување на безбедносни инциденти, постојат решенија и автоматски системи за следење кои можат да помогнат во раното откривање и решавање на инциденти. Лицата одговорни за следење на овие мониторинг системи се одговорни за пријавување на инцидентите.

ОДГОВОР НА ИНЦИДЕНТ

План за одговор на инциденти - Организацијата треба да го одржува планот за одговор на инциденти, кој ќе вклучува улоги, одговорности и комуникациски стратегии во случај на компромитација, вклучувајќи известување на релевантни надворешни партнери, на пример, издавачи на платежни картички, добавувачи.

Компјутерски тим за итни случаи - Управата на Одделот за информатичка технологија мора да организира и да одржува внатрешен компјутерски тим за итни случаи (КТИС), кој ќе обезбеди забрзано известување за проблеми, контрола на штета и услуги за корекција на проблемите во итни случаи во врска со компјутерите, како што се вирусни напади и хакерски пробивања.

Компјутерскиот тим за итни случаи мора секогаш да биде достапен за да одговори на сигнали кои вклучуваат, но не се ограничени на докази за неовластена активност, откривање на неовластени безжични пристапни точки, критични IDS-сигнали и извештаи за неовластени критични промени на системот или содржината на датотеките.

Лицата одговорни за справување со безбедносните инциденти на информациските системи мора да бидат јасно дефинирани. На овие лица мора да им се даде овластување да ги дефинираат постапките и методологиите кои ќе се користат за справување со конкретни безбедносни инциденти.

Контактните информации и постапките за пријавување на инциденти за безбедноста на информациите мора да бидат видливо при-

кажани во јавните комуникациски медиуми како што се огласни табли, простории за паузи, билтени и интранет.

План за одговор на инциденти - Постапки - Планот за одговор на инциденти мора да содржи специфични постапки за одговор на инциденти.

План за одговор на инциденти - Континуитет во работењето - Планот за одговор на инциденти мора да вклучува постапки за опоравување на бизнисот и континуитет на постапките.

План за одговор на инциденти - Резервна копија - Планот за одговор на инциденти мора да вклучува постапки за правење на резервни копии на податоците.

План за одговор на инциденти - Правни потреби - Планот за одговор на инциденти мора да вклучува анализа на правни потреби за известување на компромитирање.

План за одговор на инциденти - Критични системи - Планот за одговор на инциденти мора да вклучува покриеност и одговори за сите критични компоненти на системот.

План за одговор на инциденти - Надворешни партнери - Планот за одговор на инциденти мора да вклучува референци или да вклучува постапки за одговор на инциденти од релевантни надворешни партнери, на пример, издавачи на платежни картички, добавувачи.

Најмалку еднаш годишно, соодветноста на компјутерскиот тим за итни случаи мора да биде мобилизирана и тестирана со симулирани инциденти.

Секогаш кога еден систем е компромитиран, системите се проценуваат за потребни промени.

ОТСТРАНУВАЊЕ НА ОПРЕМА

Групата за безбедност на информации е одговорна за воспоставување стандарди за правилна санација на целата компјутерска опрема и складирање на медиумите закажани за уништување. Овие исти стандарди мора да бидат практикувани од кој било добавувач од трета страна договорен за отстранување на опремата на организацијата.

Сопствениците на податоци се одговорни да обезбедат дека сите лични и приватни податоци под нивна сопственост се правилно уништени според оваа политика.

Сите корисници на компјутерски системи, вклучувајќи ги и изведувачите и добавувачите со пристап до системите на компанијата, се одговорни за преземање на соодветни чекори, како што е наведено подолу, за да се осигура дека сите компјутери и електронски медиуми се соодветно санирани пред отстранување.

ОТСТРАНУВАЊЕ НА ПЕЧАТЕНИ ЗАПИСИ

Отстранување на печатени копии - Кога се отстрануваат, сите тајни, доверливи или приватни информации во печатена форма мора да бидат уништени или изгорени. За да се осигура дека документите се правилно уништени, треба да се користат само одобрени секачи за уништување на хартиени записи кои содржат чувствителни информации.

Контејнери за безбедни информации - Чувствителните информации кои повеќе не се потребни мора да бидат поставени во заклучен контејнер определен за материјали за уништување, внатре во канцелариите на организацијата и никогаш да не се стават во корпи за отпадоци, корпи за рециклирање или други јавно достапни простории.

ОТСТРАНУВАЊЕ НА ЕЛЕКТРОНСКИ МЕДИУМИ

Уништување на медиуми за складирање - Уништување на чувствителни информации зачувани на компјутерски медиуми за складирање може да се врши само со одобрени методи за уништување, вклучувајќи секачи или друга опрема одобрена од Секторот за информатичка безбедност.

Отстранување на електронските медиуми надвор од организацијата - Сите електронски медиуми, покрај компјутерските хард дискови, треба да се избришат, да се отстранат, или да се направат неупотребливи пред да ја напуштат организацијата. Вработените треба да користат само одобрени комерцијални добавувачи од листата на одобрени добавувачи за отстранување.

Отстранување на медиумите кои содржат тајни податоци - Организацијата не треба да препродава или рециклира медиуми кои содржат лични или приватни податоци. Таквите медиуми треба да се санираат и физички да се уништат.

ОТСТРАНУВАЊЕ НА КОМПЈУТЕРСКА ОПРЕМА

Издавање на користени компоненти на опремата - Предотстранување, донација или рециклирање, организацијата треба да потврди дека личните или приватните податоци се отстранети од која било опрема од информатички системи што била користена. Овој процес на валидација треба да се случи пред да се издаде таквата опрема на трета страна.

Отстранување на информации и опрема - Отстранувањето на вишокот на имотот што повеќе не е потребен треба да се спроведе во согласност со утврдените процедури, вклучувајќи го и неповратното отстранување на чувствителни информации и лиценциран софтвер.

Инвентар на компјутерска и мрежна опрема што е вон употреба - Организацијата треба да одржува инвентар на сите компјутерски и мрежни уреди што се вон употреба. Овој инвентар, исто така, треба да ги одразува сите активности преземени за чистење

на мемориски чипови, хард дискови и други локации за складирање на истата опрема од сите складирани информации.

Потребно означување - Опремата назначена за вишок или друга повторна употреба треба да има прикачена етикета во која се наведува дека хард дискот е правилно саниран.

ФИЗИЧКА БЕЗБЕДНОСТ

КОНТРОЛА НА ПРИСТАП

Контрола на физичкиот пристап до чувствителни информации - Пристапот до секоја канцеларија, компјутерска просторија и работна област која содржи чувствителни информации треба да биде физички ограничен за да го ограничи пристапот само на оние со потреба да знаат.

Пристап до компјутери и комуникациски системи - Згради во кои се чуваат организациски компјутери или комуникациски системи треба да бидат заштитени со физички безбедносни мерки кои спречуваат неовластени лица да се здобијат со пристап.

Неовластени обиди за физички пристап - Вработените не треба да се обидуваат да влезат во ограничени области во зградите на организацијата за кои не добиле дозвола за пристап.

Системска евиденција на контрола на пристап - Одделот или тимот за безбедност треба да води евиденција за лицата кои во моментот или претходно биле во зградите на организацијата и безбедно да ги задржува овие информации најмалку три месеци.

Пристап за поранешните вработени до ограничени области - Кога вработениот го прекинува неговиот/нејзиниот работен однос, сите права за пристап до ограничените зони на организацијата треба веднаш да се отповикаат.

Работно време во ограничено подрачје - Овластените службе-

ници не треба да пристапуваат до ограничените објекти на организацијата, каде што се ракува со чувствителни, критични или вредни информации во кое било време освен во дозволените часови за пристап.

НАДЗОР НА КОНТРОЛАТА НА ПРИСТАП

Надзор на физичкиот пристап - Метод – Се препорачуваат видеокамери или други механизми за контрола на пристап кои ги надгледуваат точките на влез и излез на безбедните области.

Надзор на физичкиот пристап - Безбедност - Видеокамерите или другите механизми за контрола на пристап кои ги следат обезбедуваните области треба да бидат заштитени од манипулирање и онеспособување.

Процедури за значки за физички пристап - Треба да се развиваат и спроведуваат процедури кои го контролираат издавањето, менувањето и одземањето на значки за физички пристап.

Пристап до системот за значки за физички пристап - Пристапот до системот што ги контролира значките за физички пристап треба да биде ограничен само на оние вработени кои имаат одговорност да издаваат, менуваат или отповикуваат значки за физички пристап.

Обезбедување на врати од отворен компјутерски центар - Секогаш кога вратите во компјутерскиот центар се отворени, влезот треба постојано да се следи од страна на вработен или стражар на договор од Одделот за физичка безбедност.

ЗНАЧКИ ЗА ПРИСТАП

Значки за идентификација - Кога се во безбедна зграда или објект, сите лица треба да носат значка за идентификација на нивната надворешна облека, така што и сликата и информациите на значката се јасно видливи за сите луѓе со кои носителот комуницира.

Обезбедување на значките за идентификација - Кога се над-

вор од организацијата, вработените треба да ги заштитат своите идентификациски значки со исто ниво на заштита како за нивните паричници и кредитни картички.

Отстранување на значките за идентификација - Веднаш откако вработените ги напуштаат објектите на организацијата, тие треба да ги отстранат нивните идентификациски значки и да ги складираат на безбедно и пригодно место подалеку од погледот на јавноста.

Привремени значки - Вработените кои ја заборавиле својата значка за идентификација треба да добијат еднодневна привремена значка преку прикажување на возачка дозвола или друг документ за идентификација со слика.

Пристап контролиран со значка - Секој треба да ја помине својата значка преку отчитувачот на значки, пред влезот на секоја контролирана врата на просториите на организацијата.

Делење на пристап со значка - Вработените не смеат да дозволат непознати или неовластени лица да поминат низ вратите, портите и другите влезови во ограничените области во исто време кога овластените лица минуваат низ овие влезови.

Лица без идентификациски значки – На лицата без соодветна и видливо истакната идентификациска значка треба веднаш да им се побара нивната значка и доколку не можат веднаш да предочат важечка значка, тие треба да бидат однесени до рецепционерското биро.

ПОСЕТИТЕЛИ

Идентификација на посетители - Сите посетители треба да покажат идентификација со слика и да се потпишат во дневник пред да добијат пристап до ограничените области.

Физички пристап за трети лица – Пристапот од посетител или трети лица до канцелариите на организацијата, компјутерските капацитети и другите работни области кои содржат чувствителни информации треба да биде контролиран од чувари, рецепционери или друг персонал.

Придружба на посетители - Посетители, вклучувајќи, но не ограничувајќи се на клиенти, поранешни вработени, членови на семејството на вработените, изведувачи за поправки на опрема, персонал на компанија за испорака на пакети и полициски службеници, треба постојано да бидат придружувани од овластен работник.

Задолжителна придружба на сите посетители по завршување на работното време - Посетителите треба да бидат придружувани од вработен овластен од овластен менаџер секогаш кога се наоѓаат во канцелариите или објектите надвор од нормалното работно време.

Значка за гости - Идентификација - Сите посетители треба да добијат значка која јасно ги идентификува како невработени.

Значка за гости – Прекин на важење - Сите значки за посетители треба да се постават на прекин на важењето не подолго од крајот на тековниот ден.

Посетителска значка - Предавање - Сите посетители треба да ѝ ја предадат својата значка на странката која ги издава или на вработениот придружник пред да заминат од кој било објект.

Дневник на посетители - Содржина - Треба да се одржува дневник на посетители кој го содржи името на посетителот, застапуваната фирма и вработениот кој го овластува физичкиот пристап до кој било објект.

Дневник на посетители - Задржување - Евиденцијата на посетители треба да се задржи најмалку три месеци.

Надзор на трети лица - Поединци кои не се ниту вработени, ниту овластени изведувачи, ниту овластени консултанти, треба да бидат надгледувани постојано додека се наоѓаат во ограничените области кои содржат чувствителни информации.

Луѓе за поправки кои се појавуваат без да бидат повикани - Треба да му се одбие пристап до објектите на секое лице за поправки или одржување кое се појавува во просториите на организацијата без да биде повикано од вработен. Сите такви инциденти треба веднаш да се пријават.

Непридружувани посетители - Секогаш кога вработен ќе забележи непридружуван посетител во ограничените области, треба да се доведе во прашање целта на посетителот поради која е во ограничената област, а потоа да биде придружен до рецепција, чуварска станица или до лицето за кое дошол да го види.

Посетители на Центарот за податоци и Одделот за информациските системи - Посетителите кои не треба да вршат одржување на опрема или кои не мора апсолутно да бидат во Центарот за податоци или Одделот за информациски системи, не треба да влегуваат во овие области.

Тури во компјутерски објекти - Никогаш не треба да се спроведуваат јавни тури во поголеми компјутерски и комуникациски објекти.

ПРЕГЛЕД НА ПРИСТАП

Пристап на персоналот до компјутерскиот центар – Комплетен список на сите вработени кои моментално се овластени да пристапат до компјутерскиот центар треба да се одржува, разгледува и ажурира од страна на менаџерот за компјутерски операции, на три месеци.

Надзор на физичкиот пристап - Преглед на податоците - Податоците што се произведуваат од видеокамери или други механизми за контрола на пристап кои ги следат точките на влез и излез на безбедните области треба да се под надзор.

ТЕСТИРАЊЕ

Тестирање на периметарот на физичка безбедност - Организацијата треба да спроведе сеопфатно тестирање на физичките безбедносни контроли на секоја локација најмалку еднаш годишно. Ова тестирање вклучува најмалку контроли на физички пристап, надзорни контроли на физички пристап и контроли на евиденцијата.

Потреба од тестирање изведено од трета страна за можна физичка пенетрација - Организацијата треба да ангажира квалификувана, независна трета страна да спроведе тест за пенетрација на физичката безбедност најмалку еднаш годишно.

ЧОВЕЧКИОТ ФАКТОР

Луѓето се највредно средство на организацијата!

Најлесен начин да се пробие во кој било компјутерски систем е да се користи важечко корисничко име и лозинка, а најлесен начин да се добијат тие информации е да се побараат од некого.

Луѓето се најголемата нишка во безбедноста на информациите! Намерно или ненамерно, вработените можат да ги загрозат и технички најнапредните системи. Ова е причината зошто луѓето се главен дел од системот за управување со безбедноста на информациите и не смеат да бидат исклучени.

Вработените поседуваат вредни информации кои можат да ѝ наштетат на организацијата во голема мера доколку бидат обелоденети. Со едноставно корисничко име и лозинка кои можат да се најават на мрежата на организацијата можат да се украдат вредни информации.

Човечкиот фактор мора да се разгледа во секој аспект на безбедноста на информациите. Треба да се спроведат различни технички мерки за да се намали штетата од малициозни напади од самите вработени. Постапката за работа со човечките ресурси мора да ги земе предвид безбедносните елементи пред вработувањето, за време на вработувањето, а особено по престанокот и промената на работниот однос.

НИВО НА СВЕСТ КАЈ ВРАБОТЕНИТЕ

Најдобрите политики и постапки се бескорисни, освен ако не се целосно практикувани од страна на вработените во кое било време во какви било околности. Безбедноста на информациите не може да се обезбеди само со примена на најнова технологија. Секогаш постои човечки фактор зад технологијата кој е најважниот столб во безбедноста на информациите.

Постојат бројни начини да се зголеми свеста на вработениот за важноста на безбедноста на информациите, особено важноста на личните и приватните информации. Секој вработен мора да биде обучен и едуциран за секоја безбедносна политика и постапка. Ова е причината зошто секоја безбедносна политика и постапка, во рамките на тој документ, мора јасно да наведат на кој оддел и вработени се однесуваат. Исто така, секоја политика и постапка мора да ги наведат наложбите или последиците од непридржување кон нив.

Но, најважно е да се подигне свеста за важноста на безбедноста на информациите на секој вработен и лице кое е вклучено во обработката на лични и приватни податоци. Во овој процес мора да се избере најсоодветен пристап кој ќе одговара на природата на организациската поставеност и културното опкружување. Секогаш кога е можно, треба да се практикува персонализиран пристап кој може да користи методи како што се:

- Програма за обука за безбедносна свест;
- Внатрешни ревизии и внатрешни тестови;
- Анонимни известувања за инциденти;
- Казни и дисциплински мерки, итн.

Многу важен фактор за подигнување на високо ниво на свесност на вработените за безбедноста на информациите е посветеноста на раководството. Кога раководството успешно ја манифестира својата свест и силниот став кон политиките за безбедност на информаци-

ите, без разлика колку и да се чини дека се тривијални, тоа е најефикасна порака за вработените.

Кога личниот асистент ги користи информациите за профилот на менаџерот, кои му ги обезбедил самиот менаџер за да му ги проверува и да одговора на електронските пораки во негово име, тоа претставува најбрутален безбедносен пробив и кршење на безбедносната политика. Но, уште поштетно е тоа што ова пренесува лоша порака до останатите.

Вработените со ниска свесност за безбедноста на информациите се лесна цел на нападите на социјалниот инженеринг.

СОЦИЈАЛЕН ИНЖЕНЕРИНГ

Во неговото јадро е манипулирање со лице за свесно или несвесно да оддаде информации; во суштина „хакирање" на лице со цел кражба на вредни информации.

- Психолошка манипулација
- Измама или лажење заради собирање информации

Тоа е начин преку кој криминалците добиваат пристап до информациските системи. Целта на социјалниот инженеринг обично е тајно да се инсталира шпионски софтвер, друг малициозен софтвер или да ги измамат лицата да оддадат лозинки и/или други чувствителни финансиски или лични информации.

Социјалната инженерска тактика вклучува:

- **Изговори** - Креирање лажно сценарио. Напаѓачите се фокусираат на создавање на добар изговор, или лажни сценарија, кои можат да ги искористат за да ги украдат личните податоци на своите жртви. Нападите преку изговор се потпираат на градење лажно чувство на доверба кај жртвата. Ова бара напаѓачот да изгради веродостојна приказна која остава малку простор за сомневање од страна на нивната мета.
- **Рибарење (Фишинг)** - Праќање мамец со цел да се измамат жртвите да ги дадат своите информации. Вообичаено, „риба-

рот“ (fisher) испраќа е-пошта, ИП, коментар или текстуална порака која се чини дека доаѓа од легитимна, популарна компанија, банка, училиште или институција. Фишинг-пораките користат страв и итност во своја полза. Тие се обидуваат да создадат чувство на итност кај своите мети, како што се заканување од затворање на сметката на метата или бришење на нивните информации доколку не одговорат навремено.

- **Намамување (Baiting)** - Намамувањето е во многу нешта слично со рибарење (phishing) нападите. Меѓутоа, она што ги разликува од другите видови на социјален инженеринг е ветување на предмет или добра што хакерите ги користат за намамување на жртвите. „Намамувачите“ (baiters) може да им нудат на корисниците бесплатна музика или преземање на филмови, ако ги предадат своите ингеренции за најава на одредено место.
- **Quid Pro Quo** - (нешто за нешто) нападите ветуваат корист во замена за информации. Оваа придобивка обично претпоставува форма на услуга.
- **Следење** - или напад на задна врата вклучува некој што нема соодветно овластување, а следи вработен во ограничено подрачје. Од учтивост, вработениот, кој е легитимна личност, обично ќе ја задржи вратата отворена за напаѓачот или пак самите напаѓачи може да побараат од вработениот да ја придржи вратата отворена за нив.

Во 2003 година, беше направена **измама со рибарење (phishing)** во која корисниците добиле е-порака, наводно, од eBay, тврдејќи дека сметката на корисникот ќе биде суспендирана, доколку не биде кликната врската со која се врши ажурирање на кредитната картичка (информации што вистинските eBay веќе ги имале). Поради тоа што е релативно едноставно да се направи веб-страница да личи на веб-страницата на легитимната организација, имитирајќи го HTML-кодот и логоата, измамата се базирала на луѓето да се измамат и да помислат дека биле контактирани од eBay и следствено дека

одат на веб-страницата на eBay за да ги ажурираат своите информации за сметката.

Канадски универзитет ненамерно изгубил речиси 10 милиони долари по паѓањето како плен на онлајн измама со рибарење (phishing). Официјални лица на Универзитетот MacEwan во Едмонтон, Алберта, неодамна добиле лажни е-писма кои тврделе дека се од еден од главните добавувачи на училиштето и дека добавувачот ги менува своите банкарски информации. Вработените потоа префрлале средства на новата банкарска сметка – кои не стасале до нивниот клиент.

Препораки:

- **Забавете.** Спамерите сакаат вие прво да дејствувате, а потоа да размислувате.
- **Истражувајте ги фактите.** Бидете сомничави за сите несакани пораки. Ако добиете е-порака од некој кој вели дека работник за одржување ќе помине, контактирајте ја компанијата на испраќачот, а не испраќачот.
- **Препознавајте ги несоодветните барања за информации.** Здобивање со едноставни информации, како што се името на вашето домашно миленичe, од каде сте, местата што сте ги посетиле; информации што би им ги дале слободно на вашите пријатели. Потоа оваа информација се користи за да се најавува на некои веб-страници. Бидејќи некои веб-страници имаат „тајно прашање“, на кое мора да одговорите, доколку не можете да се сетите на вашето корисничко име или лозинка. Прашањата изгледаат тешки за аутсајдерот кој се обидува да пробие во вашиот профил. Како се вика вашето прво домашно миленичe? Кое е твоето моминско име? Кога била родена твојата мајка/татко? Каде сте родени? Итн.
- **Не отворајте какви било е-пораки од недоверливи извори.** Осигурете се преку контактирање со пријателот или членот на семејството лично или преку телефон доколку не-

когаш добиете е-пошта која не им доликува на кој било начин.

- **Одбивајте барања за помош или понуди за помош.** Не потпаѓајте на понуди од непознати лица. Ако изгледаат премногу добро за да бидат вистинити, веројатно и се.
- **Пазете се од секое преземање.** Ако не го знаете испраќачот лично, а очекувате датотека од нив, преземањето на сешто е грешка.
- **Обезбедете ги вашите компјутери.** Инсталирајте антивирусен софтвер, заштитни ѕидови, филтри за е-пошта и тековно одржувајте ги. Поставете го вашиот оперативен систем автоматски да се ажурира, а доколку вашиот паметен телефон не се ажурира автоматски, рачно ажурирајте го секогаш кога ќе добиете известување за тоа. Користете антифишинг алатка понудена од вашиот веб-прелистувач или од трета страна за да ве предупреди за ризици.

Здрава доза на скептицизам може да помогне за заштита од многу напади на социјален инженеринг.

Треба редовно да се спроведува внатрешно тестирање со цел да се утврди подготвеноста и спремноста на вработените за нападите на социјалниот инженеринг.

СЕРТИФИКАЦИЈА

Постојат многу можности за сертифицирање на вашиот систем за управување со безбедноста на личните податоци и системот за управување со безбедноста на информациите. Стандард кој се применува за ISMS-сертификација е ISO 27001 и ISO 27018 - Кодекс на пракса за заштита на лични идентификувачки информации (ЛИИ) во јавни облаци кои дејствуваат како обработувачи на ЛИИ.

Исто така, постојат некои добри стандарди кои ја дефинираат ЛИИ-рамката - ISO 29100 и ISO 31000 за рамка за управување со ризици.

ГДПР (Општа регулатива за заштита на личните податоци) ја дефинира сертификацијата со цел да се зголеми транспарентноста и усогласеноста со Регулативата. ГДПР вели дека треба да се поттикне воспоставувањето на механизми за сертификација и печати и ознаки за заштита на податоците, овозможувајќи им на субјектите на податоците брзо да го проценат нивото на заштита на податоците на релевантните производи и услуги.

Членот 42 од ГДПР ја дефинира сертификацијата:

Сертификација

1. Земјите членки, надзорните органи, Одборот и Комисијата го поттикнуваат, особено на ниво на Унијата, воспоставувањето на механизми за сертификација за заштита на податоците и на печатите и ознаките за заштита на податоците со цел да се докаже усогласеност со оваа регулатива при операциите на обработка од страна на контролорите и обработувачите. Се земаат предвид конкретните потреби на микро, малите и средните претпријатија. 4.5.2016 L 119/58 Службениот весник на Европската Унија EN.

2. Покрај исполнувањето на оваа регулатива од контролорите или обработувачите кои се предмет на оваа регулатива, механизмите за сертификација за заштита на податоците и на печатите и ознаките одобрени во согласност со став 5 од овој член може да се

воспостават за целите на докажувањето на постоењето на соодветни заштитни мерки обезбедени од контролорите или обработувачите кои не се предмет на оваа регулатива во согласност со член 3, во рамките на преносот на лични податоци на трети земји или меѓународни организации под условите наведени во точка (ѓ) од член 46(2). Овие контролори или обработувачи преземаат обврзувачки и применливи обврски преку договорни или други законски обврзувачки инструменти, за примена на овие соодветни заштитни мерки, вклучително и во однос на правата на субјектите на податоци.

3. Сертифицирањето е доброволно и е достапно преку постапка која е транспарентна.

4. Сертификацијата според овој член не ја намалува одговорноста на контролорот или на обработувачот за усогласување со оваа регулатива и не е во спротивност на задачите и овластувањата на надзорните органи кои се надлежни во согласност со член 55 или член 56.

5. Сертификацијата според овој член се издава од сертификациони тела наведени во член 43, или од страна на надлежниот надзорен орган, врз основа на критериумите одобрени од надлежниот надзорен орган во согласност со член 58(3), или од Одборот во согласност со член 63. Кога критериумите се одобрени од Одборот, тоа може да доведе до единствена сертификација, европски печат за заштита на податоците.

6. Контролорот или обработувачот, кој ја поднесува својата обработка на механизмот за сертификација на сертификационото тело како што е наведено во член 43, или ако е применливо - на надлежниот надзорен орган, му ги обезбедува сите информации и пристап до своите активности на обработка, кои се потребни за извршување на постапката за сертификација.

7. Сертификатот се издава на контролорот или обработувачот за максимален период од три години и може да биде обновен под истите услови, ако соодветните барања продолжуваат да бидат исполнети. Сертификатот се повлекува, доколку е применливо, од

страна на сертификационите тела наведени во член 43, или од страна на надлежниот надзорен орган, ако барањата за сертификација не се исполнети или веќе не се почитуваат.

8. Одборот ги внесува во регистар сите механизми за сертификација и сите печати и ознаки за заштита на податоците и обезбедува јавен пристап до нив на соодветен начин.

Член 43 ги дефинира органите за сертификација.

Овој процес не е целосно воспоставен и сè уште е во тек. Дополнително се препорачува сите контролори и обработувачи, секогаш кога е можно, да побараат сертификација.

ФОРМУЛАР ЗА САМОПРОЦЕНКА ЗА УСОГЛАСЕНОСТ СО ПРОПИСИТЕ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

ЗАКОНИТОСТ, ПРАВЕДНОСТ И ТРАНСПАРЕНТНОСТ

Информации што ги имате

Вашиот бизнис спроведе ревизија на информациите за да го прикаже протокот на податоци.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Вашиот бизнис ги документираше личните податоци што ги поседувате, од каде доаѓаат, со кого ги споделувате и што правите со нив.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Законска основа за обработка на лични податоци

Вашиот бизнис ги идентификуваше вашите законски основи за обработка и ги документираше.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Согласност

Вашиот бизнис прегледа како барате и регистрирате согласност.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Вашиот бизнис има системи за снимање и управување со постојната согласност.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Согласност за обработка на личните податоци на децата за онлајн услуги

Доколку вашиот бизнис се потпира на согласност за да им понуди онлајн услуги директно на децата, имате системи спремни за управување со тоа.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Регистрирање

Вашиот бизнис моментално е регистриран во Канцеларијата на комесарот за информации.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

ПРАВА НА ПОЕДИНЦИ

Право да бидат информирани вклучувајќи известувања за приватност

Вашиот бизнис има обезбедено известувања за приватноста на поединците.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Комуницирајте ја обработката на личните податоци на децата

Ако вашиот бизнис нуди онлајн услуги директно на децата, вие ги комуницирате информациите за приватност на начин што детето ќе ги разбере.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Право на пристап

Вашиот бизнис има процес да препознае и да одговори на барањата на поединците за пристап до нивните лични податоци.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Право на исправка и квалитет на податоците

Вашиот бизнис има процеси за да осигура дека личните податоци што ги чувате остануваат точни и ажурирани

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Право на бришење, вклучувајќи задржување и отстранување

Вашиот бизнис има процеси за безбедно отстранување на лични податоци што повеќе не се потребни или каде што поединец побарал да ги избришете.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Право да се ограничи обработката

Вашиот бизнис има процедури за да се одговори на барање на поединецот за ограничување на обработката на нивните лични податоци.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Право на преносливост на податоци

Вашиот бизнис има процеси кои им овозможуваат на поединците да ги пренесат, копираат или префрлат своите лични податоци од една ИТ - средина во друга на безбеден и сигурен начин, без пречка за употребливоста.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Право на приговор

Вашиот бизнис има процедури за да се справи со приговор на поединец за обработката на нивните лични податоци.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Права поврзани со автоматизирано донесување одлуки вклучувајќи профилирање

Вашиот бизнис идентификува дали некоја од вашите операции за обработка претставува автоматизирано донесување одлуки и има процедури за справување со барањата.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

ОДГОВОРНОСТ И УПРАВУВАЊЕ

Одговорност

Вашиот бизнис има соодветна политика за заштита на податоците.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Вашиот бизнис ја следи вашата усогласеност со политиките за заштита на податоците и редовно ја разгледува ефикасноста на обработката на податоците и безбедносните контроли.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Вашиот бизнис обезбедува обука за подигнување на свеста за сите вработени.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Договори за обработувачи на податоци

Вашиот бизнис има писмен договор со секој обработувач на податоци што го користите.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Информациски ризици

Вашиот бизнис управува со информациските ризици на структуриран начин, така што раководството го разбира деловното влијание на ризиците поврзани со личните податоци и ефикасно управува со нив.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Заштита на податоците по дизајн

Вашиот бизнис има имплементирано соодветни технички и организациски мерки за интегрирање на заштитата на податоците во вашите активности за обработка.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Проценка на влијанието врз заштитата на податоците (ПВЗП)

Вашиот бизнис разбира кога мора да се спроведе ПВЗП и има процеси спремни да го спроведе тоа во акција.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Вашиот бизнис има ПВЗП-рамка која се поврзува со вашите постоечки процеси за управување со ризици и управување со проекти.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Офицери за заштита на лични податоци

Вашиот бизнис има назначено лидер за заштита на податоци или офицер за заштита на лични податоци (ДПО).

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Одговорност на раководството

Одлучувачите и клучните луѓе во вашиот бизнис демонстрираат поддршка за законодавството за заштита на податоци и промовираат позитивна култура за заштита на податоците во целиот бизнис.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Безбедност на податоците, меѓународни трансфери и прекршоци

Безбедносна политика

Вашиот бизнис има политика за безбедноста на информациите поддржана со соодветни безбедносни мерки.

- Сè уште не се имплементира или планира
- Делумно имплементирано или планирано
- Успешно имплементирано
- Не е применливо

Меѓународни трансфери

Вашиот бизнис обезбедува соодветно ниво на заштита за сите лични податоци што ги обработуваат други лица во ваше име и се пренесуваат надвор од европската економска област.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Известување за прекршување

Вашиот бизнис има ефикасни процеси за идентификување, пријавување, управување и решавање на какви било прекршувања на лични податоци.

- ◯ Сè уште не се имплементира или планира
- ◯ Делумно имплементирано или планирано
- ◯ Успешно имплементирано
- ◯ Не е применливо

Вкупниот рејтинг е бројот на секој одговор по категорија. Само ако повеќе од 80 % од одговорите се „Успешно имплементирано“ тогаш сте на прав пат. Сите други резултати укажуваат на потреба од ваше дејствување за понатамошна имплементација.

БЕЗБЕДНОСНИ МЕРКИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

ДИРЕКЦИЈА ЗА ЗАШТИТА
НА ЛИЧНИТЕ ПОДАТОЦИ

бул.„Гоце Делчев“ бр. 18,
П. фах 417, 1000 Скопје,
Р. Македонија

Тел./Факс:
++ 389 2 3230 635