U stavu (2) u tački b) iza riječi "KM" umjesto interpunkcijskog znaka "." treba da stoji slovo "i" i dodaje se tačka c) koja glasi:

"c) u 2023. godini 650.000 KM".

Član 3.

U članu 3. stav (1) u tački b) iza riječi "KM" umjesto interpunkcijskog znaka "." treba da stoji slovo "i" i dodaje se tačka c) koja glasi:

"c) u 2023. godini na ekonomskom kodu 8212 - nabavka građevina iznos od 650.000 KM."

Član 4.

Za realizaciju ove Odluke zadužuju se Ministarstvo finansija i trezora Bosne i Hercegovine i Uprava za indirektno oporezivanje.

Član 5.

Ova Odluka stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 59/23	Predsjedavajuća
23. februara 2023. godine	Vijeća ministara BiH
Sarajevo	**Borjana Krišto**, s. r.

Temeljem članka 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08), a u svezi sa člankom 8. stavak (2) točka e) Zakona o financiranju institucija Bosne i Hercegovine ("Službeni glasnik BiH", br. 61/04, 49/09, 42/12, 87/12 i 32/13), Vijeće ministara Bosne i Hercegovine na 3. sjednici, održanoj 23. veljače 2023. godine, donijelo je

ODLUKU
O IZMJENI I DOPUNI ODLUKE O ODOBRAVANJU VIŠEGODIŠNJEG PROJEKTA "IZGRADNJA I OPREMANJE GRANIČNOG PRIJELAZA OSOJE"

Članak 1.

U Odluci o odobravanju višegodišnjeg projekta "Izgradnja i opremanje graničnog prijelaza Osoje" ("Službeni glasnik BiH", broj 5/21 i 63/21), u članku 1. iznos "5.200.000" zamjenjuje se iznosom "5.850.000".

Članak 2.

U članku 2. stavak (1) u točki b) iza riječi "KM" umjesto interpunkcijskog znaka "."treba da stoji slovo "i" i dodaje se točka c) koja glasi:

"c) Proračuna institucija Bosne i Hercegovine u 2023. godini, na proračunskoj poziciji 8212-nabva građevina, u iznosu od 650.000 KM."

U stavku (2) u točki b) iza riječi "KM" umjesto interpunkcijskog znaka"." treba da stoji slovo "i" i dodaje se točka c) koja glasi:

"c) u 2023. godini 650.000 KM."

Članak 3.

U članku 3. stavak (1) u točki b) iza riječi "KM" umjesto interpunkcijskog znaka "." treba da stoji slovo "i" i dodaje se točka c) koja glasi:

"c) u 2023. godini na ekonomskom kodu 8212 - nabava građevina iznos od 650.000 KM."

Članak 4.

Za realizaciju ove Odluke zadužuju se Ministarstvo financija i trezora Bosne i Hercegovine i Uprava za neizravno oporezivanje.

Članak 5.

Ova Odluka stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 59/23	Predsjedateljica
23. veljače 2023. godine	Vijeća ministara BiH
Sarajevo	**Borjana Krišto**, v. r.

345

На основу члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08) и Поглавља 3. Одлуке о усвајању Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине ("Службени гласник БиХ", број 38/17), на приједлог Министарства комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и Херцеговине, на 3. сједници, одржаној 23. фебруара 2023. године, донио је

ОДЛУКУ
О УСВАЈАЊУ СМЈЕРНИЦА О УПРАВЉАЊУ БЕЗБЈЕДНОСНИМ ЗАКРПАМА, СМЈЕРНИЦА О КЛАСИФИКАЦИЈИ ИНФОРМАЦИОНИХ РЕСУРСА, СМЈЕРНИЦА О ИНФОРМАТИЧКОЈ БЕЗБЈЕДНОСТИ РАДНОГ МЈЕСТА И СМЈЕРНИЦА О УПРАВЉАЊУ БЕЗБЈЕДНОСНИМ ИНЦИДЕНТИМА

Члан 1.

(Предмет Одлуке)

Овом одлуком усвајају се Смјернице о управљању безбједносним закрпама, Смјернице о класификацији информационих ресурса, Смјернице о информатичкој безбједности радног мјеста и Смјернице о управљању безбједносним инцидентима, које су саставни дио ове одлуке.

Члан 2.

(Праћење реализовања)

За праћење реализовања ове одлуке задужују се Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине.

Члан 3.

(Ступање на снагу)

Ова одлука ступа на снагу даном доношења и објављује се у "Службеном гласнику БиХ".

СМ број 60/23	Предсједавајућа
23. фебруара 2023. године	Савјета министара БиХ
Сарајево	**Борјана Кришто**, с. р.

СМЈЕРНИЦЕ
О УПРАВЉАЊУ БЕЗБЈЕДНОСНИМ ЗАКРПАМА

УВОД

На основу Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине за период од 2017. до 2022. године (у даљем тексту: Политика), а у складу са Поглављем 3. - Закон и подзаконски акти за реализовање Политике - Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине су задужени за израду и доставу Савјету министара Босне и Херцеговине на разматрање приједлога закона и докумената дефинисаних Политиком.

СВРХА

Сврха *Смјерница о управљању безбједносним закрпама* је регулисање процеса отклањања скривених погрешака оперативних система и програмских пакета.

Благовремено отклањање постојећих погрешака оперативних система и програмских пакета спречава могућу штету због ширења вируса, црва, злонамјерних кодова и осталих напада на безбједност, који за посљедицу имају смањење оперативности, интегритета и повјерљивости информационог система.

УПРАВЉАЊЕ БЕЗБЈЕДНОСНИМ ЗАКРПАМА

Редовно прегледавање и благовремена инсталација безбједносних закрпа један је од основних услова за успостављање безбједног и поузданог информационог система. Све већи број безбједносних пропуста унутар различитих програмских пакета и оперативних система представља озбиљну пријетњу за информационе системе уколико се не предузму одговарајуће превентивне мјере које ће омогућити заштиту потенцијално рањивих система. Проблем редовног праћења безбједносних упозорења и инсталације припадајућих безбједносних закрпа додатно је наглашен у већим, хетерогеним окружењима, гдје је потребно водити рачуна о великом броју клијентских и серверских рачунара са различитим оперативним системима и сервисима. Једно од рјешења које мрежним администраторима олакшава процес прегледавања рачунара те инсталације одговарајућих закрпа су тзв. patch management алати, којима је основни циљ аутоматизовати и олакшати поступак управљања безбједносним закрпама.

Администратор је одговоран бринути лично или оформити групу задужену за управљање програмским закрпама.

Задатак управљања програмским закрпама је редовна контрола ажурности верзија оперативних система и критичних програмских пакета те документовање затеченог стања. У складу са спроведеном контролом, потребно је предузети адекватне мјере помоћу постојећих механизама за примјену програмских закрпа и/или инсталацију нових верзија. Привремено рјешење може укључивати укидање непотребног сервиса и/или промјену конфигурационих параметара.

Препорука редовних контрола је сваких мјесец дана за Windows окружење, свака три мјесеца за мрежне уређаје и централне рачунаре и/или чешће, овисно о показатељима на неисправан рад неких сервиса или добивеним/објављеним упозорењима од произвођача и одговарајућих извора.

Уколико постоји могућност, пожељно је да се инсталација закрпа спроводи централизовано – са једног рачунара истовремено на све рачунаре информационог система. Ако овакав начин инсталације закрпа није могућ, потребно је осмислити механизме којима ће се обезбиједити инсталација закрпа на сваки рачунар система.

Администратор прије одобрења треба да проучи припадајућу документацију и, по могућности, тестира програмску закрпу на издвојеној тесној околини која је што сличнија продукционој околини.

За критичне рачунаре (сервери и рачунари на којима су инсталиране апликације неопходне за нормални ток пословних процеса) је прије саме инсталације програмске закрпе потребно направити безбједносну копију која осигурава повратак на старо.

Администратор (одговорно лице/а) је обавезан водити ажурну и јединствену евиденцију примијењених програмских закрпа на рачунарима. У евиденцију се уписују и оне програмске закрпе које се нису могле примијенити на рачунаре због неадекватне верзије инсталираног софтвера и/или посебности инсталираних апликација, чија функционалност, након примјене истих, не би била могућа.

Евиденција о програмским закрпама треба да садржи сљедеће информације:

- име закрпе,
- датум издавања закрпе,
- maximum severity (critical, important)
- величину пакета,
- статус закрпе (Currently Approved, Not Approved, Updated, New),
- кратак опис (намјена закрпе),
- веза на веб страницу са додатним информацијама о закрпи,
- информација о томе да ли закрпа захтјева поновно покретање рачунара (reboot),
- информација о овисности о другим закрпама,
- листа платформи за које је закрпа примјењива.

Иако процес инсталације безбједносних закрпа на први поглед дјелује прилично једноставно и логично, пракса и искуство показује да постоје бројни проблеми и ограничења која отежавају спровођење ових задатака. Као најбољи показатељ може се узети свакодневна појава нових безбједносних инцидената који су најчешће посљедица искоришћавања познатих безбједносних проблема за које закрпе нису благовремено инсталиране.

Управљање безбједносним закрпама могуће је имплементирати неком од сљедећих метода:

- појединачном инсталацијом безбједносних закрпа након што су јавно објављене,
- коришћењем специјализованих програма уграђених у сам оперативни систем или програмски пакет,
- коришћењем специјализованих апликација независних произвођача.

Који ће се од наведених приступа користити овиси о специфичности окружења у којем се систем користи, потребама и расположивом буџету институције те о бројним другим факторима.

ЗАКЉУЧАК

У складу са Политиком и Смјерницама о управљању безбједносним захтјевима препоручује се институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правило/процедуру о управљању безбједносним закрпама.**

ЛИТЕРАТУРА

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године ("Службени гласник БиХ", број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација - Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација

СМЈЕРНИЦЕ
О КЛАСИФИКАЦИЈИ ИНФОРМАЦИОНИХ РЕСУРСА

УВОД

На основу Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине, за

период 2017-2022. године (у даљњем тексту: Политика), а у складу са Поглављем 3. Закон и подзаконски акти за реализацију политике, Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине су задужени за израду и доставу Савјету министара Босне и Херцеговине на разматрање приједлог закона и докумената дефинисаних Политиком.

СВРХА

Сврха *Смјерница о класификацији информационих ресурса* је упутити кориснике на који начин руковати појединим ресурсом. Будући да није могуће за сваки ресурс дефинисати на који начин се према њему односити у смислу заштите, настао је појам класификације. Циљ класификације је сврстати сваки ресурс у појединu класу зависно о критеријима класификације. Класа ресурса једнозначно одређује на који начин је корисник дужан користити ресурс, са коликом пажњом и одговорношћу.

КЛАСИФИКАЦИЈА ИМОВИНЕ

Власник ресурса дужан је прије његова пуштања у употребу класификовати информацију. Класификација је поступак процјене информације према:

- вриједности,
- осјетљивости,
- доступности,
- тајности,
- важности за Институцију,
- законодавним захтјевима.

Зависно о извршеној процјени свакој имовини додјељује се класа. Институција класификује имовину према 3 постојеће класе:

- Јавно доступно
- Интерна упораба
- Повјерљиво

Јавно доступно

Класа јавно доступно представља податке:

- чија је употреба отворена за све кориснике,
- који нису тајна,
- дијељење и објављивање ових података ни на који начин не штете Институцији,
- не постоје законодавни захтјеви за "скривањем" података.

Интерна употреба

Интерна употреба означава оне податке према којима се због законодавних захтјева, моралних обавеза, права приватности и сл. мора пажљиво и одговорно односити са циљем заштите података од неовлаштеног приступа, модификовања, копирања, преноса и осталих начина злоупотребе. Подаци класификовани као *интерна употреба* намијењени су искључиво запосленицима Институције који имају легитимно право приступа оваквим подацима.

Подаци класе интерна употреба:

- морају бити заштићени од неовлаштеног приступа,
- подаци морају бити похрањени на сигурним мјестима у смислу физичке заштите,
- уколико подаци више нису потребни, морају бити уништени према правилима о уклањању медија и брисања информација.

Повјерљиво

У складу са Законом о заштити тајних података ("Службени гласник БиХ", бр. 54/05 и 12/09) и подзаконским актима произашлим из Закона.

ПРАВИЛА КЛАСИФИКАЦИЈЕ

Сви ресурси Институције морају задовољавати сљедеће критеријe:

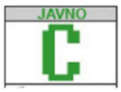
- власник је дужан провести класификацију ресурса прије његова пуштања у употребу,
- сваки ресурс (ЦД, ДВД, папирнати документи, web странице и сл.) мора имати јасно истакнуту ознаку степена класификације, осим уколико је ријеч о јавно доступним подацима,
- прије усменог саопштавања класификованих података другим особама (које имају право приступа тим подацима) обавезно се даје претходно упозорење о степену њихове класификације,
- повјерљиви подаци не смију се дијелити ни на који начин (усмено, писмено, електронским путем итд.) особама које немају право приступа тим подацима,
- сваку уочену неправилност (неовлаштени приступ, промјене, брисање, дијељење информација и сл.) корисник је дужан пријавити одговорној особи,
- класификацијске податке добивене од треће стране потребно је класификовати према правилима класификације Институције; уколико не постоји могућност класификације према интерним правилима, потребно је проширити постојећа правила у складу са указаним потребама,
- одговорна особа дужна је успоставити методе вођења евиденције о приступу *повјерљивим* подацима.

КЛАСИФИКАЦИОНЕ ОЗНАКЕ

Класификациона ознака појединог информационог система требала би бити јединствена због тога што у супротноме може доћи до мијешања неједнаких класификационих ознака више информационих система.

Приједлог класификационих ознака Институције:

Јавно доступно



Интерна употреба

Повјерљиво

Класификационе ознаке важно је што боље означити (нпр. различитим бојама, облицима) и истакнути их на уочљивим мјестима како би били сигурни да су их корисници уочили (посебно ако је ријеч о повјерљивим ресурсима).

ЗАКЉУЧАК

У складу са Политиком и Смјерницама о класификацији информационих ресурса препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правило/процедуру о класификацији информационих ресурса.**

ЛИТЕРАТУРА:

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. - 2022. година ("Службени гласник БиХ " број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање сигурношћу информација – Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", бр. 54/05 и 12/09)

СМЈЕРНИЦЕ
О ИНФОРМАЦИОНОЈ БЕЗБЈЕДНОСТИ РАДНОГ МЈЕСТА

УВОД

На основу Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине, за период 2017-2022. године (у даљњем тексту: Политика), а у складу са Поглављем 3. Закон и подзаконски акти за реализација политике, Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине су задужени за израду и доставу Савјету министара Босне и Херцеговине на разматрање приједлог закона и докумената дефинисаних Политиком.

СВРХА

Смјернице о информационој безбједности радног мјеста намијењене су корисницима информационих система Институција Босне и Херцеговине (у даљем тексту: Институције БиХ) са циљем побуде свијести о ИТ безбједности кроз обављање свакодневних задатака на рачунару, коришћењу Интернета, употреби електронске поште, поступања са осјетљивим подацима, коришћењем апликација. Корисници такође морају бити свјесни да управо они имају критичну улогу у одржавању успјешне информатичке безбједности.

РУКОВАЊЕ ЛОЗИНКАМА

Управљање безбједношћу информационих система састоји се од неколико компоненти од којих свака има за циљ описати развој, документовање и имплементацију одређених безбједносних процедура и контрола којима ће остваривати захтијеван ниво заштите. Један од аспеката информационе безбједности којем се не придаје довољно пажње јест управљање лозинкама (енгл. password management). Управљање лозинкама обухвата процедуре које се односе на развијање, документовање и ефективну имплементацију лозинки како би се обезбиједило задовољавање безбједносних захтјева дефинисаних од стране организацијске безбједносне политике. Проблем квалитетног управљања лозинкама посебно је важан за одржавање високог нивоа безбједности с обзиром да се код већине Интернет сервиса данас управо лозинке користе као основни начин аутентикације корисника.

Коришћење лозинки је врло добро уходан начин безбједносне контроле, иако недовољно безбједан. Управљање лозинкама за свој први циљ има дефинисање препорука по којима се одабиру јаке лозинке. Јака лозинка дефинише се као лозинка која није лака за откривање било којем програмском алату у разумном временском периоду (отприлике седам дана), која је лако памтљива, која је приватна (користи је само један корисник) и која је тајна. Самим истицањем важности одабира лозинке, апсулутно се одбацује могућност коришћења празних лозинки (енгл. null password), тј. лозинки које уопште не постоје, што значи да је корисник, приликом креирања лозинке, умјесто уписа лозинке притиснуо типку Ентер. Осим одабира лозинке, актуелно је и питање броја лозинки које се користе. Уколико се користи једна лозинка за приступе, у случају откривања лозинке нападач има приступ свим корисничким ресурсима. У случају коришћења лозинке за поједине приступе повећана је могућност заборављања или њихова записивања при чему је неизбјежно лако откривање лозинки. Као компромисно рјешење међу наведеним случајевима препоручљив је одабир лозинки према доменима корисничког приступа (електронска пошта, апликације, мрежни приступ, web сервиси, итд.). При одабиру лозинке актуелна су два начина. Први начин је самосталан одабир лозинке, а други начин је коришћење програмских производа за генерисање лозинки. Оба начина имају своје предности и мане.

Корисници често сматрају како не морају бринути о безбједности јер њихов рачунар не садржи вриједне информације. Но компромитовањем једног персоналног рачунара у локалној мрежи или једног корисничког рачуна на серверу нападач је пробио обрамбену линију и отворио пролаз за нападе на важније системе и информације. Док снага рачунара непрестано расте, људске способности стагнирају. Данашњи рачунари могу брзо дешифровати једноставне лозинке, док у исто вријеме већина корисника не може памтити сложене лозинке дугачке осам знакова. Стога је сваки корисник дужан придржавати се правила коришћења лозинки, те бити свјестан да непридржавањем правила није могуће успоставити квалитетну заштиту цјелокупног система.

Правила коришћења лозинки

Самосталан избор лозинке је за већину корисника најједноставнији начин. Сигурно је да ће корисник такву лозинку лако запамтити, али је исто тако сигурно да ће она бити лако откривена, јер је у већини случајева састављена од личних података. Како би се код корисника промијенио устаљени начин одабира лозинки, наведене су препоруке које упућују на начин одабира јаке лозинке која ће кориснику бити памтљива.

Лозинка која ће задовољити претходно наведене карактеристике да неће бити лака за откривање, да је лако памтљива, приватна и тајна треба бити одабрана слиједом и комбинацијом ових препорука:

- омогућити централно администрирање лозинки (напримјер путем доменских сервиса)
- минимална дужина лозинке за кориснички налог је 9 знакова,
- минимална дужина лозинке за налог са административним привилегијама је 13 знакова
- адмнистративне лозинке не смију бити идентичне на свим рачунарима
- треба садржавати комбинацију малих и великих слова,
- треба садржавати слова и бројеве,
- треба садржавати минимално један специјални знак,

- треба имати минимално четири различита знака (која се не понављају),
- треба се мијењати одређеном фреквенцијом,
- треба бити различита од претходно кориштене лозинке,
- треба бити лако памтљива само кориснику и треба представљати парафразу која му је лако памтљива.
- препоручљиво је избјегавати африкате
- препоручљиво је користити знакове/карактере који се налазе на истом мјесту и на ЕНГ тастатури и на Б/Х/С тастатури
- "Account Lockout"; закључавање налога услијед погрешно уписане лозинке треба бити укључен

Такође постоје и препоруке које упућују на то каква лозинка не смије бити. То су:

- не користити корисничко име или било који његов дио,
- не користити личне податке (датум рођења, ЈМБ, итд.),
- не користити претходне лозинке или било који њихов дио,
- не користити слиједна слова или бројеве (нпр. *абцдефг* или *234567*)
- не користити супротна слова на тастатури (нпр. *асдфгхјк*).

Како би се корисницима олакшао одабир лозинки које задовољавају претходно наведене ставке користе се различите методе. Једна од метода је кориштење мнемотехнике. Од реченице која има одређено значење за корисника узму се прва слова сваке ријечи која ће чинити лозинку. Уколико се користе парафразе згодно је користити измишлену парафразу из реалног живота у којој се поједина слова замјене бројевима или специјалним карактерима. Напримјер: *ВолимГолф2*, претварамо у *В0л!мболиф2* што је пуно памтљивије од $прАодР567

Административне лозинке морају бити различите на рачунарима. Унифицираност административних лозинки омогућава једноставно ширење крипто вируса. "Account Lockout" треба укључити (4 – 10 погрешено унесених лозинки, закључан налог остаје минимално 60 минута)

Код безбједности информационих система нема мјеста за мит о савршеној безбједности. Битна је процјена ризика за одређени информациони ресурс те његово смањивање увођењем одговарајуће безбједносне процедуре. Кориштење лозинки је, колико једноставан, толико и небезбједан начин безбједносне контроле. Иако је најраспрострањенија метода аутентикације, предложена су и имплементирана те се и даље развијају разна друга рјешења која ће једнако једноставно, али са већим степеном безбједности нудити исту услугу. За кориснике на свим нивоима препоручљив је одабир лозинке која је јака, по самостално одабраној методи те покушај пробијања лозинке с циљем провјере њезине ефикасности. Институцијама се препоручује провођење процеса подизање свјесности корисника те њихово образовање о безбједносним проблемима, а препоручљиво је и увођење безбједносне политике управљања лозинкама у којима ће бити прописан поступак одабира те чувања лозинки, као и услови који омогућавају пробијање лозинке. Таква безбједносна политика мора се заснивати на пословним процесима, идентификованим ресурсима те процјеном ризика јер циљ политике није ометати континуитет пословних процеса, већ обезбиједити одговарајући ниво заштите.

АНТИВИРУСНА ЗАШТИТА

Малициозни програми (у које спадају вируси, црви, тројански коњи итд.) су сви они програми којима је сврха злонамјеран учинак на рачунар (рачунарски систем) или који обављају акције на рачунару без знања (пристанка) корисника.

Малициозни програми сваким даном постају све сложенији и софистицираније те их је теже открити и спријечити у извршавању злоћудних активности. Антивирусне компаније развијају нове, напредније, технологије како би се успјеле носити са најновијим облицима злонамјерних програма. Да би се утврдила успјешност нових технологија важно је антивирусне алате редовно испитивати и евалуирати њихов квалитет. Да би се избјегли неквалитетни тестови потребно је поставити стандарде струке према којима ће се сви равнати и које ће поштивати. Управо на овом осјетљивом и важном подручју испитивања антивирусних алата такве смјернице дуго нису постојале. То је био један од главних разлога настанка бројних лоше дизајнираних тестова који су кориснике често криво информисали и тако им у суштини одмагали приликом одабира антивирусног алата. Баш из тих разлога стручњаци из струке одлучили су основати организацију AMTSO (Anti-Malware Testing Standards Organization), која је задужена за развој стандарда и смјерница за испитивање антивирусних алата те подстицање дискусија везаних уз ово подручје. AMTSO организација такође је задужена за ревизију постојећих и будућих поступака евалуације антивирусних алата. Ова иницијатива требала би у догледној будућности резултовати квалитетнијим тестовима и реалнијим прегледом могућности бројних антивирусних алата на тржишту. Тиме би у коначници највише требали профитирати крајњи корисници који ће добивати тачне информације о производима које одабиру, што је посебно важно за подизање глобалне свјетске рачунарске безбједности на виши ниво.

На који начин се заштитити

Да би рачунар био заштићен од малициозних програма, корисник је дужан придржавати се неколико битних и једноставних правила:

- на сваком рачунару мора бити инсталиран антивирусни програм,
- база података са информацијама о новим вирусима мора бити редовно ажурирана,
- корисник мора проводити провјере на присуство вируса код свих датотека на електронским медијима несигурног или неауторизираног поријекла или датотека набављених преко непровјерених мреже (укључујући Интернет),
- радити провјеру на присуство вируса код свих додатака електронске поште и преузетих датотека,
- антивирусни програм мора вршити активну контролу web browcepa у реалном времену, како би се спријечила зараза са web-а,
- корисник не смије својевољно искључивати антивирусну заштиту,
- корисник не смије отварати датотеке сумњивог садржаја,
- у програму за преглед поште треба искључити могућност аутоматског отварања примљене поште.

FIREWALL/ВАТРОЗИД

Већина модерних оперативних система као једну од основних безбједносних заштита посједују firewall/ватрозид. Корисник је дужан придржавати се сљедећих правила:

- не смију се мјењати поставке firewalla/ватрозида нити исти неовлаштено искључивати,
- поставке firewalla/ватрозида се прилагођавају пословном окружењу (по потреби се отварају одређени портови).

БЕЗБЈЕДНОСТ РАДНЕ ОКОЛИНЕ

Да би безбједност радне околине била задовољена потребно је придржавати се "*чистог стола*". Између осталог корисник је дужан придржавати се сљедећих правила:

- важне информације морају бити физички недоступне свим лицима које им немају приступ,
- када није у близини радног мјеста корисник мора онемогућити приступ садржају рачунара.

УПОТРЕБА ЕЛЕКТРОНСКЕ ПОШТЕ

Електронска пошта дио је свакодневне комуникације, пословне и приватне, но њено кориштење може озбиљно угрозити безбједност информационог система.

Под злоупотребом електронске поште, односно имејла, могу се сматрати следеће активности :

- прикупљање и крађа личних и пословних информација других корисника електронске поште,
- злоупотреба података и пропаганда у комерцијалне сврхе путем електронске поште,
- лажно представљање и крађа идентитета путем електронске поште,
- кориштење електронске поште као начина дистрибуције злонамјерног софтвера (разних варијанти вируса, црва, тројанаца, кеулоггер-а …).

Потенцијалне пријетње и рањивости електронске поште:

Вируси

Електронска пошта може бити малициозног карактера – у додатку је датотека која садржи вирус.

Несигурност протокола

Поруке путују као обичан текст, те их је лако прочитати или измијенити садржај.

Лако је кривотворити адресу пошиљаоца.

Незгоде

Притиском на погрешну типку или одабиром погрешног корисника у адресару порука може доћи нежељеном кориснику (или више њих).

Да би пријетње информационом систему изазване непримјереном употребом електронске поште свели на минимум, потребно је придржавати се сљедећих правила:

- електронска пошта не смије се користити за слање увредљивих, омаловажавајућих, сексуално узнемиравајућих и других порука сличног садржаја,
- није дозвољено слање ланчаних порука којима се оптерећују мрежни ресурси,
- свака написана порука сматра се документом. Немате право поруке коју су послане кориснику лично прослиједити даље без одобрења аутора,
- сваку поруку која садржи додатак сумњивог садржаја обавезно провјерити антивирусним програмом,
- институција има право филтрирања порука са намјером да заустави нежељену електронску пошту (енг. *спам*),
- у случају инцидента, институција има право прегледа свих података (укључујући електронску пошту),
- поруке које су дио пословног процеса нужно је архивирати и чувати прописани временски период,
- корисник не смије слати масовне поруке, без обзира на њихов садржај.

СОЦИЈАЛНИ ИНЖЕЊЕРИНГ

Постоје многе технике и рањивости које злонамјерни корисници могу искористити за пробој информационе безбједности неке институције. Једну од њих представљају и људске рањивости, које је могуће искористити преко разних метода социјалног инжењеринга. Циљ напада је добити повјерење жртве како би се остварила крађа података или идентитета те упад у мрежу или систем с намјером нарушавања рада или узроковања штете. Социјални инжењеринг има одређене специфичности, али свима је заједничко усмјеравање на људски фактор безбједности неког система.

Ове методе искоришћавају људске погрешке или слабости како би се остварила права приступа систему без обзира на ниво безбједности коју је институција увела. Усмјереност на људске особине попут повјерења, жеље за помоћи или немарности основна је предност ових напада. Такође, свака особа може постати социјални инжењер и примијенити неку од бројних тактика напада. Социјални инжењеринг укључује разне технике, од једноставне крађе записаних лозинки до стварања и извођења сложених сценарија. Једна од најраширенијих и најпознатијих, је извођење *phishing* напада. Ријеч је о процесу преваре у којем се нападач представља као повјерљива страна како би дошао до осјетљивих података жртве.

Циљ социјалног инжењеринга

Основни циљ социјалног инжењеринга је повећати права приступа систему или информацијама са могућношћу:

- Извођења преваре – добивање лозинки легитимних корисника најчешће се користи за извођење превара које наносе новчану штету.
- Упада у мрежу – познавање осјетљивих корисничких података (корисничко име и лозинка) омогућује пријаву на систем са једнаким правима која су додијељена легитимном кориснику.
- Индустријског шпијунирања – откривање повјерљивих података неке организације могуће је искористити за разне сврхе попут остваривања конкурентности на тржишту или продаје идеја конкурентским организацијама.
- Крађе идентитета – добивањем корисничких имена, лозинки или других креденцијала нападач се може представити као корисник.
- Једноставног нарушавања система или мреже – добивање приступа систему омогућује нападачу наношење штете те извођење свих акција које су дозвољене кориснику чије је податке открио. То може укључивати брисање, измјену или преглед

датотека, уметање лажних података, блокирање мреже, стварање непотребних конекција и сл.

Најчешће методе преваре:

- **Лажно представљање** – најчешћа метода напада, поступак у којем се нападач представља као нека друга особа;
- **Увјеравање/Наговарање** – наговарање или увјеравање је поступак при којем нападач наговара и увјерава жртву да обави поступке које му налаже нападач;
- **Ствара одговарајуће ситуације** – нападач ствара "плодно тло" за извршење напада на начин да искористи жртвине слабост; примјер таквог напада је зближавање са жртвом како би дошао до информација, искориштавање неспремност или непажњу жртве како би учинила погрешан потез и сл.;
- **Морална одговорност** – жртва покуша помоћи нападачу јер осјећа да је то њена морална обавеза; жртве нису свјесне да на тај начин одају корисне информације нападачу;
- **Жеља за помагањем** – искориштавање жеље жртве да помогне другима: чест је случај да нападач увјери жртву да ће он поступити исто у ситуацији када жртви буде требала помоћ;
- **Искориштавање старих веза и корупције** – нападач ствара однос који је довољан за стицање повјерења или поткупљује корисника који му одаје жељене информације.

Начини извршења напада:

- **Телефонски инжењеринг** – један од најчешћих и најлакших начина извршавања социјалног инжењеринга; нападач назива нпр. једног од запосленика те својим комуникацијским вјештинама лако стиче његово повјерење;
- **Претраживање отпада** – један од начина сакупљања информација је претраживање отпада при чему се сазнаје много корисних информација за извођење напада;
- **Коришћењем Интернета** – бројни су начини прикупљања информација путем Интернета, а најчешћи је слањем лажних порука електроником поштом. На тај начин могуће је доћи до врло тајних информација као што су лозинке и лични подаци;
- **Завиривање** – тип социјалног инжењеринга при којему нападачи покушавају очитати жртвине покрете како би добили жељене податке. Примјер ове технике је гледање покрета руке приликом укуцавања PIN-а на банкомату или при уписивању лозинке приликом пријаве на систем;
- **Форензичка анализа** – до корисних информација нападач може доћи прегледом непажљиво одбачених медија (CD, DVD, меморијске картице, дискови, USB меморије и сл).

Phishing

Једна од техника социјалног инжењеринга је *phishing* напад, који се користи како би се преварило кориснике и искористило лошу имплементацију и употребу технологија за безбједност web страница. *Phishing* напад, је процес преваре у којем се покушавају открити осјетљиви подаци (попут корисничких имена, лозинки, бројева кредитних картица и сл.) представљањем као повјерљиви ентитет у електронској комуникацији. Нападачи се обично усмјеравају на комуникацију преко популарних социјалних мрежа те web страница са аукцијама или онлајн наплатом. Напад се најчешће проводи преко порука електронске поште или порука које се преносе у стварном времену (енг. instant messaging), а циљ је усмјерити корисника на лажну web страницу која изгледа идентично као и оригинална, легитимна страница. Често је врло тешко уочити разлику између лажне и оригиналне странице чак и када се користе напредне технике аутентикације корисника.

Уколико нападач успјешно обави напад и прикупи жељене информације, пружа му се могућност приступа информационим системима финансијских установа или неким другим системима преко којих може стећи одређену финансијску корист.

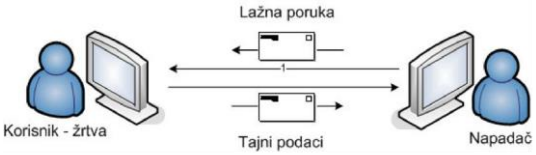
Ток провођења *phishing* напада могуће је подијелити у три фазе:

- осмишљавање и припремање напада,
- провођење напада,
- прикупљање повјерљивих информација и њихово искориштавање.

Прва фаза, осмишљавање и припремање напада најважнији је дио напада. У тој фази нападач покушава скупити што више информација о жртви, о детаљима жртвиног оперативног система и информационог система итд. Што више информација посједује, нападач ће са већом вјероватношћу успјешно обавити напад и остати неоткривен.

Друга фаза је провођење напада. Начин провођења напада зависиће о прикупљеним подацима у првој фази.

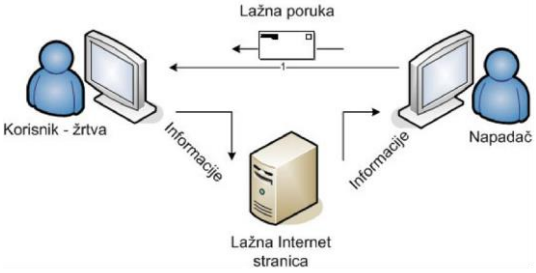
Слика 1. шематски приказује напад електронском поштом:



Слика 1. – Примјер phishing напада електронском поштом

Напад електронском поштом реализује се тако да нападач слањем електронске поште потакне корисника на одавање жељених информација. Један од примјера овог напада приказан је сликом: нападач шаље кориснику жртви лажну поруку тако да се представи као финансијска установа. У поруци тражи да жртва хитно пошаље тајне податке због провјере или губитка дијела података. Уколико корисник не примијети превару, шаље нападачу поруку у којој су садржани тајни подаци. Напад је успјешно реализован и нападач долази до жељених података. Овај напад је најједноставнији, а реализација зависи о неедукованости корисника жртве. Уколико је жртва наивна, вјероватност успјешности напада је релативно велика.

Друга метода напада електронском поштом је позивање корисника жртве на лажне Интернет странице. Слика 2. шематски приказује описани напад.



Слика 2. – Примјер *phishing* напада лажном Интернет страницом

Примјер тока напада: корисник жртва добива лажирани имејл. У поруци се позива да због одређеног разлога посјети Интернет странице финансијске установе. Иако жртва не сумња у вјеродостојност, Интернет странице наведене у поруци су лажиране. Наиме, лажне странице врло је тешко уочити. Осим сличности у називу, лажиране странице визуално су идентичне оригиналним Интернет страницама, стога корисници не сумњају у било какав облик преваре. Циљ нападача је да се корисник покуша пријавити на систем на лажној Интернет страници. Уколико се корисник покуша пријавити, вјероватно ће добити поруку о тренутном нефункционисању система. Но нападачу то више није важно. Уносом података од стране корисника нападач је добио жељене податке за приступ оригиналном систему банке или било ког другог информационог система.

Описани облици напада су напади у којима резултат напада зависи о реакцији корисника. Остали облици напада базирају се на способностима нападача да искористе пропусте у комуникационим протоколима, оперативним системима, софтверу, безбједносним контролама итд. те не зависе о реакцијама корисника.

Методе заштите

Безбједносна политика и стандарди

Добро документована и доступна безбједносна политика и стандарди кључ су добре безбједносне стратегије неке институције. Политика треба јасно дефинисати свој опсег и садржај за свако подручје на које се односи. Заједно са сваком политиком потребно је специфицирати стандарде које треба увести како би се провеле одредбе политике. Неки од уобичајених дијелова безбједносне политике у борби против социјалног инжењеринга су:

- употреба рачунарског система – управљање коришћењем система, употреба хардвера и програма који нису у власништву институције и сл.,
- класификација и руковање информацијама – обезбиједити правилну класификацију повјерљивих информација како би оне биле заштићене од неовлаштеног приступа,
- лична безбједност – провјера нових запослених како би се обезбиједило да не представљају безбједносну пријетњу,
- физичка безбједност – обезбиједити објекте знаковима, видео камерама и безбједносним уређајима и сл.,
- приступ информацијама – процеси за генерисање безбједних лозинки, удаљени приступ и сл.,
- заштита од вируса – провести мјере заштите система од вируса и других злонамјерних пријетњи,
- тренинзи за подизање свијести запослених о информационој безбједности – информисати запослене о пријетњама и мјерама,
- управљање усклађеношћу – осигуравање усклађености са законима и стандардима,
- политика о лозинкама – дефинисање стандарда за осигуравање лозинки,
- реаговање на инцидент – дефинисање поступка реакције и пријаве инцидента,
- дистрибуција документације – руковање са повјерљивим подацима.

Једном дефинисана политика мора бити лако доступна свим запосленима. Такође, потребно је спроводити стално ажурирање и провјеравање безбједносне политике како би се начиниле нужне промјене у складу с новим одредбама или пријетњама.

Едукација запослених и особља

Како би безбједносна политика била ефикасна потребно је спровести поступке едукације. Стварање свијести о пријетњама, понашању које нападачи искориштавају те методологијама чини важан дио стратегије заштите од истих пријетњи. Најбољи начин за постизање тога је представљањем стварних примјера хакирања институција путем метода социјалног инжењеринга. Постоје многи алати који се могу искористити при едукацији попут видео записа, брошура, знакова (натписа на радном мјесту, дисплеја, подсјетника и др.) и слично. Програми едукације имају улогу:

- упознавања запослених са безбједносном политиком,
- стварање свијести о ризицима и могућим губицима,
- тренирања са циљем препознавања техника социјалног инжењеринга.

Значи, није довољно запосленим указати што и како, чинити него их је потребно упознати са посљедицама које доносе пријетње социјалног инжењеринга. Будући да едукација запослених о ризицима социјалног инжењеринга представља једну од основних метода заштите, то је врло захтјеван задатак. Добар програм обуке мора бити разноврстан што значи да је потребно искористити сваку могућност и алат како би се постигло повећање свијести и разумијевање пријетња које доносе социјални инжењери.

Други поступци заштите

Један од кључних поступака заштите од социјалног инжењеринга је правилно управљање лозинкама. Организација мора имати јединствени идентификатор за сваког запосленика који ће бити повезан са правима приступа тог запосленика. Значи, идентификатором се запосленом одређују права приступа информацијама на систему. У томе се види предност коришћења посебног идентификатора за сваког запосленог. У случају да нападач сазна идентификатор неког корисника, он има право приступа само оним информацијама које су додијељене том кориснику док су остали дијелови система заштићени. Дефинирање оперативних поступака такође има важну улогу у заштити институције од напада социјалних инжењера. При томе се првенствено мисли на процедуре повезане са одобравањем приступа и издавањем дозвола. Такви поступци захтијевају вишеструку провјеру точности и вјеродостојности података. Основна сврха је смањити ризике напада опонашањем запослених.

Заштита обичних корисника

Сваки корисник Интернета може провести одређене мјере заштите од напада социјалним инжењерингом попут:

- упознавања са вриједностима података – нападачи се обично усмјеравају на корисничка имена и лозинке те бројеве кредитних картица па је потребно посебно опрезно руковање са тим подацима,
- провјеравања идентитета саговорника – социјални инжењери обично се усмјеравају на стицање повјерења корисника увјеравајући их како се ради о њима познатим лицима, сарадницима, надлежним лицима, владиним службеницима и сл.

- задржавања лозинки тајним – лозинке треба чувати у тајности те избјегавати њихово записивање или дијељење са другим лицима,
- провјеравања порука електронске поште – провјерити извор поруке, провести скенирање антивирусним алатом и сл.,
- избјегавања уписивања лозинки у несигурне странице – провјерити ваљаност web страница прије уписа лозинке преко УРЛ низа и других индикатора безбједности,
- не откривања пуно информација о себи – сазнавањем информација о неком кориснику социјални инжењер се може фокусирати на његове навике и хобије како би га навео на посјећивање лажних web страница,
- коришћења *anti-phishing* заштите – постоје алати који провјеравају поруке електронске поште како би открили изразе који су карактеристични за *phishing* поруке.

БЕЗБЈЕДНОСТ МЕДИЈА

Медији су ресурси институција који служе за похрану података. Као такви играју велику улогу у безбједности. Доласком до медија на којем су похрањени повјерљиви подаци или подаци за интерну употребу, нападачу могу бити отворена врата за обављање злонамјерних радњи.

Питање трајности записа на медијима најзначајније је питање када се говори о животном вијеку података. Међутим, једнако је важно и питање смисла дугог чувања записа на технологијама данашњице. Чињеница је да технологија изузетно брзо напредује и за очекивати је значајне промјене у ближој будућности на свим пољима па тако и на пољу похране података. У складу с тим, може се уочити да на медије за похрану трајност података није једини услов, важније је одредити исправна и функционална правила која ће се примјењивати код похрањивања података.

Потреба за повећањем капацитета уређаја, односно медија за похрану података је неупитна па је врло лако формулисати предвиђања за будућност везана уз капацитете – очекује се наставак раста капацитета, а при томе смањивање величине медија и самих уређаја. Такође, реално је очекивати и повећања брзине преноса података.

Основне карактеристике уређаја за похрану података су сљедеће:

- капацитет,
- брзина преноса података и
- просјечно вријеме приступа.

Пожељне карактеристике су:

- постојаност података,
- једноставно руковање и мале димензије те
- приступачност цијене.

Уређаји који задовољавају дате карактеристике заснивају се на магнетној и оптичкој технологији.

Капацитет

Капацитет уређаја за похрану мјери се у октетима (бајтима) – из чега слиједе следеће јединице:

- B – бајти (октети)
- KB– килобајти
- MB – мегабајти
- GB – гигабајти
- TB – терабајти

На примјер, 1 KB износи 1024 B. Иако није потпуно исправно, ради једноставности ове мјере често се заокружују на 1000, нпр. 1 MB се поистовјећује с 1000 KB, односно 1 000 000 B, при чему релативна грешка износи око 5%.

Просјечно вријеме приступа

Ради се о времену потребном да управљачка јединица приступи податку на датој адреси на медију. Мјери се у милисекундама при чему је мање боље.

Упркос високој поузданости данашњих медија и уређаја за похрану података, позната препорука корисницима и даље вриједи: ваши подаци су онолико добри колико је добар ваш посљедњи бекап.

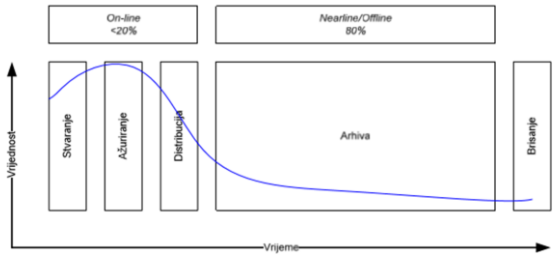
Правилник о безбједности медија треба дефинисати да:

- сви медији морају бити похрањени на безбједном и заштићеном мјесту,
- сви медији морају бити чувани према спецификацијама произвођача,
- медији са повјерљивим подацима не смију се давати на коришћење неовлашћеним корисницима,
- свако дијељење медија са повјерљивим подацима мора бити документовано,
- потребно је тражити овлаштење за уклањање медија из институције, те се мора сачинити записник о таквим активностима,
- ако више нису потребни, треба обрисати пријашње садржаје сваког поновно искористивог медија који ће бити уклоњен из институције.
- сви преносни медији базирани на flash-меморију (USB-стикови) и преносни тврди дискови морају бити криптовани доступним софтверским алатима како би били недоступни трећим лицима у случају да буду изгубљени/украдени
- сви службени "паметни" уређаји (смартпхоне/таблет) морају бити криптовани одговарајућим алатима које обезбјеђује произвођач уређаја

Управљање животним циклусом података и информација

Међу подацима разликују се активни и неактивни подаци, односно информације. Животни циклус података почиње њиховим прикупљањем. Активни подаци означавају податке који се употребљавају свакодневно у уобичајеним пословним процесима корисника. С временом ти подаци губе своју важност. Учесталост приступа опада уз поступно губљење пословне вриједности па информације свој животни вијек коначно завршавају архивирањем или њиховим одлагањем.

Активни подаци носе пословну корист институцији, подузећу, односно кориснику. Сваки успјешан и ефикасан пословни процес захтјева једноставан и несметан приступ активним подацима. Управљање подацима заснива се на врло једноставном начелу: преносу података из слоја у слој кроз вријеме, према приказу на слици 1.



Слика 3. Временски ток података

Разумијевањем начина на који се подаци преносе, односно задржавају у појединим слоју корисници развијају

стратегије и обрасце кориштења како би оптимизирали употребу медија за похрану. На тај се начин оптимизује укупна цијена спремања података током њиховог животног циклуса.

Сличан, али сложенији, приступ примјењује се код похране података у релациону базу података (енг. *Relational Database*). Комплексност у овом случају повећава инхерентна међузависност података. Релационе базе података једни су од честих и великих корисника простора за похрану података, а уједно су, због природе кориштења, један од најсложенијих механизама приступа подацима. Сложеност управљања релационим базама података чини управо та међузависност података. Због тога је врло важно развити ефикасне механизме управљања како база не би изашла ван граница надзора. У противном би сваки дохват података из базе постајао све скупљи што би у коначници резултирало лошим перформансама читавог система.

Након што подаци више нису потребни за пословни процес корисника, они постају **неактивни**. Ипак, то не значи да су и непотребни те да их се може избрисати са медија на којему су похрањени. Појам управљање животним циклусом података (енг. *DLM - Data Life Cycle Management*) односи се на координисање проласком информација кроз информациони систем; од њиховог настанка и иницијалне похране све до тренутка када исти подаци постају непотребни и слиједи им брисање. Овакви системи аутоматизују процесе укључене у управљање подацима, а ради се о организацији података у међусобно одвојене слојеве заснованој на унапријед одређеним правилима (енг. Policy), те аутоматизацији преноса података из једног слоја у други, заснованој такође на успостављеним правилима. Примјер правила може се илустровати ситуацијом када се подаци којима се чешће приступа спремају на скупље, али и брже медије, док се подаци с мањим значајем спремају на јефтиније и спорије медије.

Израз управљање животним циклусом информација (енг. ILM – Information Life Cycle Management) није исти управљању циклусом података, иако се неријетко та два појма користе равноправно. Системи орјентисани на податке користе атрибуте датотека (врсту, величину, датум настанка, уређивања и сл.) за дохват података на захтјев корисника. Системи засновани на управљању информацијама увелико су сложенији и омогућавају претрагу, односно дохват података кориштењем сложених упита попут конкретних вриједности појединих параметара спремљених у датотекама.

Хијерархијско управљање похраном података (енг. HSM – Hierarchical Storage Management) један је од могућих начина управљања подацима. Ради се о техници која омогућује аутоматски пренос података између медија различитог цјеновног ранга. Разлог потреби за таквим управљањем је првенствено у цијени уређаја за похрану. Очито је како би најједноставније и најефикасније рјешење било кориштење уређаја високих перформанси. Ипак, цијена је та која условљава кориштење уређаја лошијих карактеристика. Након успостављања коначног скупа правила о преносу података између различитих кориштених уређаја, одговорност за исправно функционисање преузима HSM систем надзирући начин кориштења података и правилним распоређивањем података.

Уклањање медија

Сврха правилника о уклањању медија је смањити ризик од "цурења" осјетљивих информација које може настати неправилним одбацивањем медија уколико медиј више није потребан. Како би се ризик "цурења" свео на минимум потребно је успоставити формалне смјернице за сигурно уклањање медија.

Све медије квалификоване као осјетљиве, који више нису за употребу, потребно је уклонити тако да нико ни на који начин није у могућности доћи до података (или дијела података) похрањених на медију, папирнате и оптичке медије потребно је уклонити помоћу апарата за уклањање медија, USB и остале меморије потребно је уклонити према правилима произвођача или физичким дјеловањем на медиј, остале медије потребно је уклонити физичким дјеловањем, посебним уређајима или на трећи начин према препорукама стручњака.

Листа докумената који могу захтијевати сигурно уклањање:

- оптички медији (CD, DVD..),
- преносни тврди дискови
- USB меморије,
- папирнати документи,
- снимљени глас,
- индиго папир,
- трака за принтер,
- системска документација итд.

Осим дефинисања смјерница, важно је нагласити да је уклањање осјетљивих медија треба бити провјерено и документовано.

ЗАКЉУЧАК

У складу са Политиком и Смјерницама о информационој безбједности радног мјеста препоручује се Институцијама БиХ да донесу своје интерне акте у којима ће дефинисати:

- **Правила/процедуре о кориштењу антивирусне заштите,**
- **Правила/процедуре о употреби електронске поште,**
- **Правила/процедуре о методама заштите,**
- **Правила/процедуре о безбједности медија.**

ЛИТЕРАТУРА

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. - 2022. година ("Службени гласник БиХ " број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација – Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација

СМЈЕРНИЦЕ
О УПРАВЉАЊУ БЕЗБЈЕДНОСНИМ ИНЦИДЕНТИМА

УВОД

На основу Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године (у даљем тексту: Политика), а у складу са Поглављем 3. - Закон и подзаконски акти за реализовање Политике - Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине су задужени за израду и

доставу Савјету министара Босне и Херцеговине на разматрање приједлог закона и докумената дефинисаних Политиком.

СВРХА

Смјернице о управљању безбједносним инцидентима намијењене су корисницима рачунарских система у институцијама Босне и Херцеговине (у даљем тексту: институције БиХ) у сврху управљања безбједносним инцидентима на системима које користе, уколико до њих дође. Без обзира на све већа средства и напоре који се улажу у постизање и одржавање безбједности информационих система, безбједносни инциденти и даље су честа појава. Сваки безбједносни инцидент, без обзира на величину и трајање, за институцију представља губитак, због чега је врло важно да се адекватна пажња посвети развоју стратегије и планирању активности у случају појаве безбједносних инцидената.

Инцидент се може дефинисати као сваки догађај који није стандардна операција услуге, а може проузроковати или узрокује прекиде или смањење квалитета ИТ услуге. Циљ процеса управљања инцидентима је омогућити кориснику што је прије могуће повратак до нормалног нивоа услуга са најмањим могућим утицајима на пословање. Процес управљања инцидентима мора идентификовати и снимати настале инциденте, будући да је то важно за мјерење и контролу квалитете процеса, али и за идентификацију узрока инцидената те предузимање корективних мјера и даљих побољшања.

Рачунарски безбједносни инциденти су честа појава у модерно доба. Рачунарски безбједносни инцидент је посредно или непосредно угрожавање безбједносне политике, правила и процедура. Развој технологије и рачунарске науке омогућио је и развој нових метода напада и угрожавања рачунарских система и мрежа. Како би се ограничило дјеловање злонамјерних нападача потребно је успоставити поступак за рјешавање безбједносних инцидената. Одговор на безбједносне инциденте постао је важан дио информационе технологије, а безбједносне пријетње бројне и разноврсне, али, што је најважније, и све разорније (нпр. напад ускраћивања услуга може нападнутој институцији створити велике финансијске трошкове). Активности за спречавање безбједносних пријетњи засноване на резултатима процјене ризика (нпр. примјена безбједносне метрике) могу да смање број инцидената, али не могу да спријече све инциденте. Институција треба да има способност рјешавања безбједносног инцидента у смислу људства и примјене безбједносних мјера заштите. За потребе одговора на безбједносне инциденте оснивају се посебне групе за њихово рјешавање. Оне су потребне за брзо откривање инцидената и санирање штете настале безбједносним инцидентом.

АКТИВНОСТИ У ПРОЦЕСУ УПРАВЉАЊА ИНЦИДЕНТИМА

Активности у процесу управљања инцидентима су:

- идентификација и запис инцидената: инциденти се идентификују, детектују и записују,
- инцидент се класификује и даје се почетна подршка за његово рјешавање,
- упоређивање (усклађивање) инцидената: тражи се компатибилност са већ познатим инцидентима ради лакшег рјешавања постојећег инцидента, а затим се провјерава могућност коришћења већ постојеће солуције за инцидент,
- истраживање и дијагноза: уколико је инцидент непознат, потребно је детаљније истраживање и додјела компетентније групе за подршку,
- рјешавање инцидента и затварање: након затварања инцидента, инцидент слог (запис) мора да буде потпуно ажуриран (наведена категорија и приоритет, услуга/корисник на које се негативно одразио инцидент, конфигурациони детаљи идентификовани као узроци инцидента),
- праћење инцидената: комуникација са корисницима о статусу инцидената.

Критични фактори успјеха за процес управљања инцидентима су:

- процјена инцидента с аспекта утицаја на посао и потреби временског рјешавања,
- база знања у подршци препознавања инцидената и њиховог рјешавања,
- адекватни аутоматски системи за запис и праћење инцидената,
- добра повезаност са процесом управљања степеном услуга која ће утицати на приоритете и вријеме рјешавања инцидената.

Индикатори перформанси за процес управљања инцидентима су:

- укупан број инцидената,
- просјечно вријеме рјешавања инцидената,
- % инцидената ријешених унутар СЛА циљева,
- % инцидената ријешен првом линијом подршке,
- просјечни трошкови подршке по инциденту,
- % инцидената са почетном коректном класификацијом,
- % инцидената у коректно реализованом циклусу активности.

У сврху квалитетног организовања управљања безбједносним инцидентима потребно је дефинисати:

- одговорности и улоге,
- потенцијално опасне радње,
- процедуре у случају инцидента,
- процедуре за благовремену детекцију,
- процедуре за анализу инцидента и уклањање посљедица,
- процедуре за враћање система у иницијално стање.

Управљање безбједносним инцидентима важан је сегмент пословања сваке институције. Уколико се унапријед дефинишу заштитне мјере и кораци у случају појаве инцидента, знатно се могу умањити губици и утицај инцидента на пословање институције.

ДЕФИНИСАЊЕ ОДГОВОРНОСТИ И УЛОГА

Главно одговорно лице дужно је иницирати спровођење политике управљања безбједносним инцидентима. Одговорност у институцији и спровођењу политике може да има једно лице, али и више њих. Важно је да хијерархија одговорности буде јасно дефинисана и документована.

Иницијалну одговорност над управљањем безбједносним инцидентима има главно одговорно лице. Главно одговорно лице одговорност или дио одговорности може да пренесе на друго лице/лица, уз обавезно јасно дефинисање и документовање одговорности.

БЛАГОВРЕМЕНА ДЕТЕКЦИЈА

Како би се потенцијалне пријетње и инциденти благовремено детектовали, потребно је оспособити сљедеће механизме:

- софтверско праћење дневника записа са могућношћу алармирања код детекције потенцијално опасних радњи (DDoS напади, *brute force* напади, употреба ресурса информационог система за слање нежељене поште итд.),
- периодички преглед дневника записа одговорног лица с циљем уочавања потенцијално опасних радњи које софтвер није детектовао,
- преглед пријава корисника о инцидентима корисника,
- преглед пријава корисника о рањивостима система.

Одговорна лица која прегледавају пријаве корисника дужна су водити евиденцију примљених захтјева и акција које су предузете. Дневник, између осталог, мора да садржава сљедеће податке:

- када је направљена пријава корисника,
- када је одговорно лице прегледало пријаву,
- запис пријаве,
- које су акције предузете у вези са пријавом,
- да ли је опасност отклоњена или не.

КАКО РЕАГОВАТИ У СЛУЧАЈУ ИНЦИДЕНТА

У случају инцидента одговорно лице дужно је реаговати тако да спријечи даље чињење злонамјерних радњи и покуша прикупити додатне информације о нападу (доказни материјал), локацији са које је казнено дјело извршено, времену извршења итд.

Уколико одговорно лице примијети или добије пријаву корисника о потенцијалној рањивости система, дужно је да учини сљедеће:

- направи евиденцију захтјева на исти начин као код пријема пријаве о инциденту,
- иницира рјешење проблема тако да обавијести власника ресурса о пропусту,
- у евиденцију дода ко је одговоран, датум и вријеме када је примио обавијест о рањивости и када је рањивост уклоњена,
- обавијести Тим за одговор на рачунарске инциденте (CERT) за институције Босне и Херцеговине и слиједи обавезујуће мјере и стандарде за управљање безбједносним рачунарским инцидентима које прописује CERT за институције Босне и Херцеговине.

АНАЛИЗА ИНЦИДЕНТА И УКЛАЊАЊЕ ПОСЉЕДИЦА

Након обављања иницијалних процедура у случају инцидента и након што је напад (опасност) прошао, потребно је направити анализу стања како би се утврдило шта је све обухваћено инцидентом и шта је његов циљ.

Неки од могућих циљева напада су:

- искоришћавање система за обављање злонамјерних радњи (слање нежељене електронске поште, извршавање напада одбијања услуге итд.),
- напади на систем одбијања услуге, *brute force* напади,
- крађа ресурса,
- мијењање ресурса,
- уништавање ресурса итд.

Битан дио рјешавања инцидента су учење и побољшавање. Свака институција БиХ треба учити на ријешеним инцидентима како би могла што боље дјеловати у будућности која доноси нове пријетње и профињеније нападе. Питања на која треба дати одговоре приликом анализе насталог инцидента су:

- Шта се тачно догодило и у које вријеме?
- Колико су добро особље и менаџмент извели свој задатак и носили се са инцидентом?
- Јесу ли процедуре документоване и јесу ли биле одговарајуће?
- Које је информације требало дознати раније?
- Јесу ли предузети сви кораци или акције које могу да успоре опоравак?
- Шта би особље и менаџмент учинили другачије идући пут када се догоди сличан инцидент?
- Које је мјере потребно предузети за спречавање сличних инцидената у будућности?
- Који су додатни ресурси и алати потребни за откривање, анализу и ублажавање посљедица будућих инцидената?

За мале инциденте није потребно обављати обимне анализе, осим оних инцидената код којих су коришћене нове методе напада како би се слични напади брже и ефикасније санирали у будућности. Анализа ријешеног безбједносног инцидента добар је материјал за обнављање безбједносних политика и процедура за сузбијање безбједносних инцидената.

Критични фактори успјеха су:

- добро дефинисане активности, циљеви, одговорности и остали ресурси документоване процедуре,
- добра координација између процеса управљања инцидентима и процеса управљања проблемима будући да су подаци о инциденту (категорија инцидента, приоритет, статус, конфигурациони детаљи, корисник и услуга чија је испорука спријечена) важни за дефинисање, истраживање проблема и тражење узрока у циљу његове елиминације.

Индикатори перформанси су:

- смањен број инцидената управљањем и рјешавањем проблема,
- смањено вријеме за рјешавање проблема,
- смањење трошкова потребних за елиминисање поремећаја у испоруци ИТ услуга.

Предвиђање будућности у индустријској грани као што је рачунарска технологија готово је немогућ задатак. Само кратки поглед у прошлост открива колико је ситуација постала озбиљна. Рачунарски криминал толико је узнапредовао да је важност спровођења најосновнијих безбједносних мјера већа него икада. Протекли период обиљежило је значајно повећање безбједносних пријетњи на вебу те искоришћавање рањивости нових технологија (web 2.0, мобилни телефони нове генерације…). Иако је поприлично незахвално детаљније предвиђати развој догађаја на сцени рачунарског криминала, стручњаци се слажу о сљедећем:

- разноврсност напада и њихова учесталост наставиће свој раст експоненцијалном брзином, вођени жељом нападача за проваљивање у туђе рачунарске системе због крађе идентитета, ресурса или осјетљивих информација,
- цурење података постаће све већи проблем, првенствено због све већег коришћења мобилних технологија у пословним окружењима,
- компромитовани персонални рачунари и даље ће, као дио *botnet* мрежа, бити главни извор spam порука електронске поште. Botnet мреже новим

начином комуницирања, путем P2P мрежа, вјешто избјегавају откривање,
- злонамјерне поруке ће у будућности садржавати све више раширених врста докумената попут PDF и DOC датотека за које нападачи свакодневно проналазе нове рањивости.

Како интернет постаје свакодневница и у животу обичних људи а не само информатичких стручњака, очекује се да ће и нападачи и даље своје активности усмјерити највише на "мрежу свих мрежа" - интернет. Како би се безбједносни инциденти смањили на најмањи могући ниво важно је константно едуковати кориснике рачунара како би користили што више безбједносних мјера и тиме учинили свој рачунар, али и рачунар других корисника, безбједнијим. Управно је људски фактор узрок многим безбједносним инцидентима, али наша способност да учимо и мијењамо своје понашање представља подручје са највећим могућностима за развој и напредак глобалне рачунарске безбједности.

ЗАКЉУЧАК

У складу са Одлуком о одређивању Тима за одговор на рачунарске инциденте за институције Босне и Херцеговине, Политиком и Смјерницама о управљању безбједносним инцидентима препоручује се институцијама БиХ да донесу своје интерне акте у којима ће дефинисати:
- **правила/процедуре како пријавити безбједносни инцидент и потенцијалне рањивости система,**
- **правила/процедуре о начину спречавања даљих злонамјерних радњи,**
- **правила/процедуре о начину на који се могу прикупити додатни доказни материјали који су изазвали инцидент,**
- **правила/процедуре за враћање система у иницијално стање након санираног инцидента.**

Институције БиХ су у обавези да слиједе обавезујуће мјере и стандарде за управљање безбједносним рачунарским инцидентима које прописује Тим за одговор на рачунарске инциденте (CERT) за институције Босне и Херцеговине.

ЛИТЕРАТУРА:

1. Одлука о одређивању Тима за одговор на рачунарске инциденте за институције Босне и Херцеговине ("Службени гласник БиХ", број 25/17)
2. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године ("Службени гласник БиХ", број 38/17)
3. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација - Захтјеви
4. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација

Na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i Poglavlja 3. Odluke o usvajanju Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine ("Službeni glasnik BiH", broj 38/17), na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine, na 3. sjednici, održanoj 23. februara 2023. godine, donijelo je

ODLUKU
O USVAJANJU SMJERNICA O UPRAVLJANJU SIGURNOSNIM ZAKRPAMA, SMJERNICA O KLASIFIKACIJI INFORMACIONIH RESURSA, SMJERNICA O INFORMATIČKOJ SIGURNOSTI RADNOG MJESTA I SMJERNICA O UPRAVLJANJU SIGURNOSNIM INCIDENTIMA

Član 1.
(Predmet Odluke)

Ovom odlukom usvajaju se Smjernice o upravljanju sigurnosnim zakrpama, Smjernice o klasifikaciji informacionih resursa, Smjernice o informatičkoj sigurnosti radnog mjesta i Smjernice o upravljanju sigurnosnim incidentima, koje su sastavni dio ove odluke.

Član 2.
(Praćenje realiziranja)

Za praćenje realiziranja ove odluke zadužuju se Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine.

Član 3.
(Stupanje na snagu)

Ova odluka stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 60/23
23. februara 2023. godine
Sarajevo

Predsjedavajuća
Vijeća ministara BiH
Borjana Krišto, s. r.

SMJERNICE
O UPRAVLJANJU SIGURNOSNIM ZAKRPAMA

UVOD

Na osnovu Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017. do 2022. godine (u daljnjem tekstu: Politika), a u skladu sa Poglavljem 3. - Zakon i podzakonski akti za realiziranje Politike - Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine su zaduženi za izradu i dostavu Vijeću ministara Bosne i Hercegovine na razmatranje prijedloga zakona i dokumenata definiranih Politikom.

SVRHA

Svrha *Smjernica o upravljanju sigurnosnim zakrpama* je reguliranje procesa otklanjanja skrivenih pogrešaka operativnih sistema i programskih paketa.

Pravovremeno otklanjanje postojećih pogrešaka operativnih sistema i programskih paketa sprečava moguću štetu zbog širenja virusa, crva, zlonamjernih kodova i ostalih napada na sigurnost, koji za posljedicu imaju smanjenje operativnosti, integriteta i povjerljivosti informacionog sistema.

UPRAVLJANJE SIGURNOSNIM ZAKRPAMA

Redovno pregledavanje i pravovremena instalacija sigurnosnih zakrpa jedan je od osnovnih uvjeta za uspostavu sigurnog i pouzdanog informacionog sistema. Sve veći broj sigurnosnih propusta unutar različitih programskih paketa i operativnih sistema predstavlja ozbiljnu prijetnju za informacione sisteme ukoliko se ne preduzmu odgovarajuće preventivne mjere koje će omogućiti zaštitu potencijalno ranjivih sistema. Problem redovnog praćenja sigurnosnih upozorenja i instalacije pripadajućih sigurnosnih zakrpa dodatno je naglašen u većim, heterogenim okruženjima, gdje je potrebno voditi računa o velikom broju klijentskih i serverskih računara sa različitim operativnim sistemima i servisima. Jedno od rješenja koje mrežnim administratorima olakšava proces