непоуздани потребно је периодички проводити тестирања која се односе на њихову исправност. Велика количина података похрањених на тракама или дискетама је бескорисна уколико се не могу прочитати са истих. У ту сврху потребно је периодично провјеравати исправност резервних копија.

- Чување старих верзија резервних копија - некад је потребно извјесно вријеме како би се утврдило да је нека датотека уништена или побрисана. Због таквих случајева увијек је потребно чувати старе верзије резервних копија одређено вријеме или онолико колико налаже закон. Могуће је чувати седмичне, мјесечне, полугодишње или годишње верзије резервних копија. Препоручује се старе копије чувати на различитој локацији од оне на којој су подаци.
- Провјера система база података прије израде резервних копија - уколико се ради о повратку података система који је претходно уништен онда је резервна копија бескорисна. Препоручује се прије израде резервне копије провјеравање интегритета система база података.
- Провјера да се датотека не користи током стварања резервног записа - уколико се датотека користи приликом израде резервне копије она је бескорисна јер не садржи исправну и важећу верзију.
- Стварање резервне копије прије великих промјена у систему база података - корисно је имати резервну копију прије тестирања новог хардвера, поправака на систему или инсталације нових апликација.

Приликом израде резервних копија институције могу користитит и друге методе као што су electronic vaulting, journaling i mirroring у зависности о врсте пословавања и потреба институције када је у питању израда резервних копија.

5. Закључак

Процесом стварања сигурносних копија и повратом података смањују се ризици којима је изложен информацијски сустав. Редован и поуздан поступак израде сигурносних копија је поступак који се не смије избјећи. Без обзира како се третира сустав не могу се избјећи ризици од нежељених посљедица. Ризици су обично већи него су људи то способни схватити, а према подацима се треба односити озбиљно прије него се осјете посљедице губљења истих. По статистици 90% организација пропада ако изгубе виталне записе што показује колико су модерне организације овисне о информацијској подршци. Један од недостатака израде сигурносних копија је цијена. Наиме, процес укључује одговарајуће медије, опрему на којој се похрањују информације, запослените који су задужени за одржавање сигурносних копија и примјену политике израде сигурносних копија, а то организацијама узрокује трошкове без јасно видљивих резултата. Ипак, дугорочно гледано та цијена је занемарива у односу на цијену коју може платити тврtка или појединац уколико није у стању обављати посао. Додатан проблем који је могућ код организација које проводе политику израде сигурносних копија је отпор запосленика. Запослени често сам поступак израде сигурносних копија сматрају беспотребним јер нису свјесни важности сигурносних копија за цијелу организацију. Ипак сви су ови потенцијални недостаци израде сигурносних копија занемариви у односу на могућност прекида пословања и пропадања организације у случају изостанка података. Стога је податке потребно адекватно заштити, а један од неопходних начина је и израдом сигурносних копија.

У складу са Политиком и Смјерницама о резервним копијама препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре за израду резервних копија.**

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 – Систем за управљање безбједношћу информацијама – Захтјеви
3. Стандард ISO/IEC 27002 – Безбједносне технике – Правило добре праксе за контроле безбједности информација

СМЈЕРНИЦЕ
О ЗАПОСЛЕЊУ И ПРЕКИДУ ЗАПОСЛЕЊА

1. Сврха

Сврха смјерница о запослењу и прекиду запослења је дефинисати процедуре којима ће се прецизирати кораци које је потребно предузети у погледу безбједности приликом запослења, склапања уговора о запослењу или сарадњи и које дефинишу на који начин квалитетно провести прекид запослења или раскид уговора. Циљ наведених процедура је смањење ризика од људске погрешке, крађа, превара и злоупотребе ресурса информационих система институције.

2. Процедуре склапања уговора

Одговорна лица при склапању уговора о запослењу или сарадњи требало би да проведу мјере дефинисане сљедећим процедурама:

2.1. Провјера

Провјера (енг. screening) у сврху контроле потенцијалних запосленика или пословних партнера једна је од превентивних метода којима институција може дјеловати на безбједност информационог система. Одговорно лице треба провести или иницирати провјеру и испитивање над потенцијалним запосленником. Процес провјере и испитивања треба узети у обзир сва права и законске одредбе приватности те уколико је допуштено укључити сљедеће:

- расположиве референце карактера, пословања итд.,
- преглед доступних ЦВ-а, контрола достављених података,
- потврде о школовању и професионалним квалификацијама,
- докази идентитета (пасош),
- да ли је особа казнено гоњена итд.

Прикупљене податке потребно је документовати као **повјерљиве податке** те према њима направити процјену да ли постоји могућност злоупотребе информационог система од стране потенцијалног запосленика.

2.2. Услови запослења и уговор одговорности

Прије запослења особа у институцијама БиХ, склапања партнерства са другом организацијом или укључивања у посао треће стране неопходно је у рјешење или уговор укључити дио који све стране обавезује на придржавање правила дефинисаних безбједносном политиком. Рјешење или уговор треба садржавати додатак са појашњењима и ставовима:

- да сваки запосленик, партнер или трећа страна, прије добивања права приступа имовини организације, треба потписати уговор о повјерењу,

- законским правима и одговорностима сваког запосленика, корисника и пословног партнера,
- одговорностима институције о чувању и руковању информацијама о запосленима,
- одговорностима у случају обављања посла изван радног времена или изван просторија институције (нпр. код куће),
- акцијама које је потребно предузети уколико се утврди непридржавање правила дефинисаних безбједносном политиком.
- Појашњењима о поступцима у случају кад запосленик напушта Институција у смислу поништавања корисничких налога за приступ апликацијама , системима и другим ресурсима Институције.

2.3. Одговорности руководилаца институција

Руководиоци институција треба да захтјевају и инсистирају на придржавању правила дефинисаних безбједносном политиком од стране запослених, корисника, пословних партнера и треће стране. Њихова је обавеза све запослене, кориснике, партнере и треће стране:

- правилно и јасно информисати о њиховим улогама у провођењу безбједности те о њиховим одговорностима прије додјељивања права приступа осјетљивим информацијама,
- пружити им увид у облику смјерница о томе шта се очекује од њих зависно о њиховим улогама,
- мотивисати да се придржавају правила дефинисаних безбједносном политиком,
- обезбједити потребан ниво свијести о потреби за безбједношћу, зависно о улогама.

2.4. Едукација о информационој безбједности

Сви запослени институције и уколико се укаже потреба, партнери и персонал треће стране требају проћи одговарајућу обуку о свијести о информационој безбједности те правовремено бити упознати са допунама или промјенама у безбједносној политици институције.

Основни појмови о безбједности и обука о свијести о информационој безбједности требају бити презентовани запосленима, партнерима и трећој страни прије додјељивања права приступа информацијама. Едукација корисника мора бити са складу са улогом, способношћу и одговорности појединца.

3. Престанак радног односа

Поступак престанка радног односа запосленог у институцији важно је правовремено и квалитетно обавити како се кориснику не би пружила могућност обављања злонамјерних радњи. Приликом престанка радног односа потребно је задовољити сљедеће безбједносне контроле:

- најважнији дио престанка радног односа – **уклонити сва права приступа** ресурсима институције; уколико је могуће потребно је права приступа уклонити аутоматски помоћу посебних програма (приступ програмским ресурсима),
- сви кључеви, паметне картице и сл. такође морају бити враћени,
- сву имовину коју је добио на кориштење корисник мора вратити у посјед институције,
- сви поступци везани уз престанка радног односа (нпр. враћена имовина) требају бити документовани.

4. Закључак

У складу са Политиком и Смјерницама о запослењу и прекиду запослења препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре о запослењу и прекиду запослење.**

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 – Систем за управљање безбједношћу информацијама – Захтјеви
3. Стандард ISO/IEC 27002 – Безбједносне технике – Правило добре праксе за контроле безбједности информација

СМЈЕРНИЦЕ
ЗА ИЗРАДУ МЕТОДОЛОГИЈЕ ПРОЦЈЕНЕ РИЗИКА

Увод

Потребе за квалитетним рјешењима и поузданим системом управљања безбједношћу унутар институције постала је један од основних захтјева за успјешно обављане пословних задатака. У вријеме када рачунарска комуникациона инфаструктура представља окосницу пословања готово свих модерних фирми и институција управљање безбједносним ризицима игра веома важну улогу у процесу заштите информационих ресурса и пословних процеса.

За процес управљања безбједносним ризиком слободно се може рећи да представља темељ изградње безбједне и поуздане рачунарске инфраструктуре. Идентификација критичних информационих ресурса и одређивање припадајућих безбједносних ризика, процес је који омогућује квалитетније и економичније доношење одлука везаних уз унапрјеђење безбједности. Без одговарајућих анализа и квалитетно разрађених планова, развој и имплементација безбједног рачунарског окружења врло је често хаотичан процес који резултује бројним пропустима и недостатцима.

У овом документу описани су основни циљеви и идеје процеса управљања безбједносним ризицима, начини његовог провођења, као и типични проблеми који се јављају у овом подручју. Већи дио документа посвећен је процјени ризика, поступку на којем се базира готово цијели програм управљања безбједносним ризиком.

Управљање безбједносним ризиком

Безбједносни ризик дефинише се као могућност реализације неког нежељеног догађаја, који може негативно утицати на повјерљивост (енгл. confidentiality), интегритет (енгл. integrity) и расположивост (енгл. availability) информационих ресурса. Под информационим ресурсима подразумијевају се сва она средства која институција користи у сврху остваривања својих пословних циљева (хардвер, софтвер, људски ресурси, подаци и сл.)

Прецизна идентификација, односно класификација информационих ресурса први је, и врло важан, корак процеса управљања безбједносним ризиком, будући да се на основу њега одређује који ресурси захтијевају какав третман са становишта безбједности. Неадекватно обављена идентификација ресурса може цијели процес одвести у погрешном правцу, чиме се у потпуности губи његов значај и смисао. Управљање безбједносним ризиком (енгл. Risk Management), релативно је нова дисциплина у подручју безбједности ИТ система, која је произашла из потребе за стандардизацијом и формализацијом поступака везаних уз управљање безбједношћу. Дефинише се као процес идентификације оних чинилаца који могу негативно утицати на повјерљивост, интегнтет, и расположивост рачунарских ресурса, као и њихова анализа у смислу вриједности појединих ресурса и трошкова њихове заштите. Завршни корак обухваћа