- 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

предузимање заштитних мјера које ће идентификовани безбједносни ризик свести на прихватљив ниво, у складу са пословним циљевима институције.

У којој мјери и на којим мјестима ће се приступити умањивању безбједносног ризика, одлука је првенствено менаџмента, као оне функције која има могућност доношења одлука и право располагања над буџетом институције. Безбједносни ризик могуће је третирати на неколико начина. Могуће га је прихватити онаквим какав је, могуће је приступити његовом умањивању, имплементацијом одговарајућих безбједносних контрола, а могуће је и његово игнорисање, односно пребацивање другим институцијама. Споменуте технике биће детаљније описане касније у документу. Доношење одлука везаних уз управљање ризиком врло је одговоран и захтјеван посао који, осим одређеног нивоа стручности, захтјева и веома добро познавање ИТ система и његове функције.

Процес управљања безбједносним ризицима састоји се од три фазе:

- процјена ризика (енгл. Risk Assessment);
- умањивање ризика (енгл. Risk Mitigation);
- испитивање и анализа (енгл. Evaluation and Assessment).

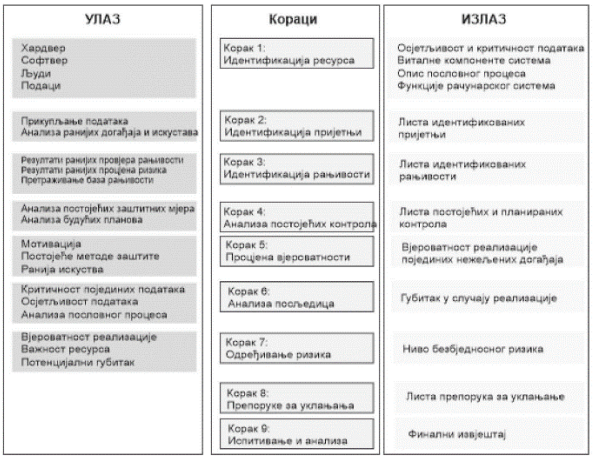
Свака од наведених фаза има своју улогу и циљ у комплетном програму управљања безбједносним ризиком. У наставку документа бити ће детаљније описана свака од фаза, заједно са својим основним карактеристикама и специфичностима.

Процјена ризика

Процјена ризика врло је сложен и захтјеван поступак те стога мора бити проведен професионално и темељно како би се добили мјеродавни подаци. Сам процес анализе и процјене најбоље је додјелити безбједносним стручњацима са искуством на подручју безбједности информационих система (по могућности независним консултантима), а разултате процјене дати менаџменту на основу којих ће се доносити одговарајуће одлуке. Процес процјене ризика састоји се од девет корака:

- Корак 1: Идентификација и класификација ресурса (енгл. Asset Identification);
- Корак 2: Идентификација пријетњи (енгл. Threat identification);
- Корак 3: Идентификација рањивости (енгл. Vulnerability Identification);
- Корак 4: Анализа постојећих контрола (енгл. Control Analysis);
- Корак 5: Вјероватноћа појаве нежељених догађаја (енгл. Likelihood Determination);
- Корак 6: Анализа посљедица (енгл. Impact Analysis);
- Корак 7: Одређивање ризика (енгл. Risk Determination);
- Корак 8: Препоруке за умањивање (енгл. Control Recommendation);
- Корак 9: Документација (енгл. Result Documentation).

На сљедећој слици (Слика 1) приложен је дијаграм на којем је приказан ток наведених фаза са улазним и излазним параметрима. Треба напоменути да се кораци 2,3 и 4 могу проводити у паралели након што је довршен корак 1.



Слика 1: Процјена ризика - дијаграм

Иако одређивање безбједносног ризика захтјева провођење свих ових корака, сам ризик математички се може посматрати као функција три параметра: пријетњи, рањивости и вриједности ресурса (Слика 2).

Ризик=ф (Пријетње, Рањивости, Вриједност ресурса)

Што је систем више изложен пријетњама, што је већи број рањивости и што је ресурс значајнији за институцију то је и безбједносни ризик већи. Наравно, јасно је да се безбједносни ризик никада неће уклањати смањивањем вриједности ресурса, већ имплементацијом одговарајућих безбједносних контрола које ће утицати на параметре рањивости и пријетњи.

Вриједност ресурса који је овдје наведен као један од параметара о којему зависи ниво безбједносног ризика, може се посматрати и на другачији начин. Наиме, врло често се умјесто вриједности ресурса као трећи параметар у обзир узима потенцијални губитак за институцију у случају губитка или нерасположивости ресурса о којем се говори. Без обзира о којем је од два наведена параметра ријеч, исход је идентичан, будући да су вриједност ресурса и посљедице у случају губитка двије директно везане величине.

Идентификација и класификација ресурса

Први корак у поступку процјене ризика је идентификација, односно класификација информационих ресурса. У овом кораку потребно је идентификовати све оне ресурсе који представљају значај за институцију те им додијелити одговарајућу вриједност. Уколико постоји могућност, сваком ресурсу потребно је додијелити конкретну новчану вриједност, будући да то увелике може допринијети квалитети резултата цијелог поступка.

Идентификацију и придјељивање вриједности појединим ресурсима потребно је обавити како би се у коначници имплементирале само оне безбједносне контроле које су финансијски исплативе.

Поступку додјељивања вриједности ресурсима потребно је посветити посебну пажњу, будући да лоше процјене у овом случају могу цијели процес одвести у погрешном правцу. Приликом одређивања вриједности потребно је у разматрање узети бројне друге факторе, осим иницијалних трошкова његове набавке. Неки од фактора које је потребно узети у обзир су:

- трошкови развоја;
- трошкови одржавања и администрације;
- трошкови едукације;
- трошкови замјене, надоградње и сл.

Neki od tipičnih resursa koji predstavljaju važnost za instituciju su:

- hardver;
- softver;
- mrežа i mrežni uređaji;
- podaci;
- ljudski resursi i sl.

Pod bezbjednosnim prijetnjama (engl. Threat) smatraju se svi oni neželjeni faktori koji se mogu negativno odraziti na integritet, povjerljivost i dostupnost resursa. Izvori prijetnji (engl. threat agents) mogu se podijeliti u dvije osnovne grupe:

Namjerne - oni izvori koji ciljano iskorištavaju nedostatke u sistemima u svrhu ostvarivanja neovlaštenog pristupa. U ovu grupu najčešće spadaju neovlašteni korisnici, razni maliciozni programi (crvi, virusi...) i sl.

Nenamjerne - oni izvori koji rezultuju slučajnim iskorištavanjem ranjivosti u sistemu, npr. elementarne nepogode kao što su požari, poplave, potresi, udari grома i sl.

U okviru procjene rizika vrlo je važno generisati iscrpnu listu svih onih prijetnji, namjernih i nenamjernih, koje predstavljaju potencijalnu opasnost za informacioni sistem.

Prilikom identifikacije prijetnji poželjno je u obzir uzeti sve ranije incidente i ostale neželjene događaje, motive koji mogu biti podloga za provođenje napada, lokaciju na kojoj se nalaze resursi te ostale faktore koji na bilo koji način predstavljaju prijetnju za IT sistem. Vrlo često od koristi mogu biti i razgovori sa administratorima sistema ili drugim sobljem, koje je u svakodnevnom kontaktu sa kompонentama sistema.

Neke od prijetnji koje su tipične za informacione sisteme uključuju:

- neovlaštene koriснike,
- maliciozne programe (virusi, crvi, trojanski konji,...),
- elementarne nepogode (poplave, potresi, požari,...),
- korisničke pogreške (namjerne i slučajne),
- krađu,
- greške u programiranju (namjerne i slučajne),
- neisprавno rukovanje resursima,
- industrijsku špijunažu,
- interne napade, i sl.

Za svaku od identifikovanih prijetnji potrebno je odrediti povezanost sa resursima institucije, motive koji stoje iza svake od njih te načine na koje prijetnje mogu utицati na poslovne procese. Što je detaljnije razrađena lista prijetnji to je jednostavnije odrediti bezbjednosni rizik povezan sa odgovarajućim resursom.

Identifikacija ranjivosti

Pod pojmom ranjivosti (engl. Vulnerability), smatraju se svi propusti i slabosti u sistemu bezbjednosti koji omogućuju provođenje neovlaštenih aktivnosti. Ranjivosti mogu biti posljedica pogrešaka u procesu dizajna ili implementacije sistema, kao i propusta u sistemu provođenja bezbjednosnih pravila i procedura. Iako se ranjivosti najčešće povezuju uz greške u programskom kodu, mogući su i brojni drugi primjeri, kao što su površno implementirana fizička bezbjednost, nepoznavanje i neprikladan odabir tehnologija i alata, propusti u održavanju sistema i sl.

Prema izrazu za bezbjednosni rizik, za uspješno određivanje bezbjednosnog rizika potrebno je takođe identifikovati i sve ranjivosti, odnosno bezbjednosne propuste u sistemu. Bez adekvatne analize ranjivosti, gotovo je nemoguće pouzdano određivanje bezbjednosnog rizika. Zavisno o broju i karakteru ranjivosti u sistemu, bezbjednosni rizik može biti veći ili manji. Implementacijom bezbjednosnih kontrola kojima će se umanjiti broj ranjivosti u sistemu, direktno je moguće utицati na umanjivanje bezbjednosnog rizika.

Kada se govori o procjeni rizika, veoma je važno da se ranjivosti analiziraju u kombinaciji sa identifikovanim prijetnjama, budući da su ova dva parametra međusobno povezana. Ukolико ne postoji prijetnja koja bi iskoristila određenu ranjivost, tada ne postoji nити bezbjednosni rizik. Tamo gdje nema rizika ne isplati se ulagati u zaštitu, a to je osnovni cilj postupka upravljanja bezbjednosnim rizikom: implementacija samo onih zaštitnih mjera koje će biti opravdane i smislene u pogledu zaštite poslovnih ciljeva institucije.

U sljedećoj tabeli (Tabela 1), dat je primjer nekih od ranjivosti koje su tipične za IT sisteme, zajedno sa prijetnjama koje su vezane uz svaku od njih.

Ranjivost	Prijetnja
Bezbjednosni propusti u programskom kodu	Neovlašteni korisnici Maliciozni programi Nezadovoljni zaposleni Teroristi
Neadekvatna konfiguracija Firewool	Neovlašteni korisnici Maliciozni programi Industrijska špijunaža
Nedostatak protivpožarne zaštite	Požar
Nedostatak antivirusne zaštite	Maliciozni programi (virusi, crvi, trojanski konj)
Neovlašćeno korišćenje telekomunikacionih uređaja	Neovlašteni korisnici Maliciozni programi Bivši i nezadovoljni zaposleni

Ono što se namеće kao osnovno pitanje kada se raspravlja o identifikaciji i analizi ranjivosti je način na koji je najbolje provesti njihovu detaljnu i temeljnu analizu. Neki od mogućih pristupa su:

- analiza rezultata ranije provedenih procjena rizika (ukolико takvi postoje),
- analiza interних izvještaja i dokumentacija vezanih uz ispitivanje, analizu i unaprjeđenje bezbjednosti,
- provođenje specijalizovanih bezbjednosnih ispitivanja (Vulnerability Scanning, Pentration Testing,Application Testing i sl.),
- pretraživanje javnih baza ranjivosti,
- razgovori sa zaposlenima i sistem administratorima itd...

Rezultat ove faze treba biti detaljna lista ranjivosti prisutnih u sistemu, kao i njihova povezanost sa prijetnjama identifikovanim u pretходnom koraku.

Analiza postojećih kontrola

U ovom koraku cilj je analizirati one bezbjednosne kontrole koje su već implementirane ili koje se namjeravaju implementirati u svrhu zaštite informacionih resursa. Ukolико se želi izračunati vjerovatnost iskorištavanja pojedine ranjivosti od strane identifikovanih prijetnji, što je sljedeći korak procesa procjene rizika, potrebno je u

обзир узети све постојеће контроле присутне у систему. Врло је мала вјероватноћа да ће одређена слабост или недостатак бити искориштени, уколико су имплементиране квалитетне безбједносне контроле или уколико постоји мали интерес за њеним искоришћавањем. Системи који баратају повјерљивим подацима као што су нпр. бројеви кредитних картица, обрачуни плата и сл., представљају пуно већи изазов за неовлаштене кориснике у односу на остале системе који управљају мање повјерљивим подацима.

Безбједносне контроле могу бити техничке и нетехничке природе. Под техничким безбједносним контролама сматрају се све оне контроле које су имплементиране у облик хардвера, софтвера или неког другог сличног рјешења (нпр. firewool, антивирусна заштита, системи контроле приступа и сл.). Под не-техничким контролама сматрају су контроле попут безбједносних политика, препорука и процедура и које су најчешће резултат усмене или писмене предаје.

Још једна од подјела, која је више присутна у круговима који се баве рачунарском безбједношћу, је она која безбједносна рјешења и механизме дијели на:

Превентивне (енгл. Prevention) - она рјешења која дјелују превентиво у смислу спречавања неовлаштених активности (нпр. антивирусни програми, firewool, контрола приступа, и сл.)

Детекцијске (енгл. Detection) - системи који омогућују детекцију неовлаштених активности (нпр., алати за провјеру интегритета, и сл.);

Реакцијске (енгл. Reaction) - они механизми који помажу при реакцији на детектоване неовлаштене активности (нпр. форензичка анализа);

Разултат овог корака је листа постојећих или предвиђених безбједносних контрола којима је циљ заштита информационих ресурса институције.

Вјероватности реализације

Сљедећи корак у процесу процјене ризикање одређивање вјероватности искоришћавања поједине рањивости од стране припадајућих безбједносних пријетњи. Неки од чинилаца које је овдје потребно узети у обзир су:

- мотивација и интерес извора пријетњи,
- карактер рањивости,
- присутност и квалитет постојећих безбједносних контрола.

Вјероватност искоришћавања рањивости од стране одређеног извора пријетњи најбоље је изразити степенасто: нпр. висок, средњи и ниски степен, при чему сваки од дефинисаних степена има одређени значај и смисао.

У сљедећој табели (Табела 2) дат је примјер једне такве подјеле, са тим да је могуће ићи и на прецизнију подјелу, зависно од потреба.

Вјероватност	Дефиниција
Висока	Извор пријетње је посебно мотивисан за искоришћавање рањивости са обзиром на могућност доласка до повјерљивих података. Постојеће безбједносне контроле су недовољне или садрже слабости које омогућавају заобилажење дефинисаних безбједносних мјера.
Средња	Извор пријетње је дјелимично мотивисан. Иако постоје могућности за искоришћавање рањивости постојеће контроле то отежавају
Ниска	Изостанак мотивације за искоришћавање рањивости. Безбједносне контроле квалитетно су имплементиране И искоришћавање рањивости прилично је отежано.

Табела 2: Вјероватност искоришћавања рањивости

Разултат овог корака садржи вјероватност искоришћавања појединих рањивости идентификованих у претходном кораку, са обзиром на наведене пријетња.

Анализа посљедица

Циљ овог корака је процијенити негативан учинак ако пријетња успјешно искористи рањивост система. Прије анализе потребно је прикупити информације о сврси система, те о важности и осјетљивости система и података. Негативан учинак догађаја може се описати као нарушавање функционалности или било којег основног начела информационог система. Основни параметри информационе безбједности су:

- Повјерљивост (енг. Confidentiality) – безбједан приступ информацији и ИС-у искључиво за то овлаштеном лицу.
- Цјеловитост (енг. Integrity) – заштита исправности и цјеловитости података и информација.
- Расположивост или доступност (енг. Availability) – овлаштеном лицу омогућити правовремен и сталан приступ информацијама и ИС-у.
- Идентификација и аутентикација - обезбјеђује сигурност информационог простора институције
- Ауторизација и непорецивост (енг. non-repudiation)

Посљедице које могу настати нарушавањем основних начела могу бити губитак конкурентске предности, губитак повјерења клијената (цурење личних података корисника у јавност), непоштивање мјеродавних прописа (на примјер кршење регулативе у подручју заштите личних података), финансијски губици, доношење погрешних пословних одлука (због неисправности информација), немогућност испоруке услуга клијентима.

Учинке је могуће мјерити квантитативно у облику финансијских средстава и времена које је потребно уложити како би се поправио систем или ријешили проблеми или описати квалитативно (односи се на учинке који се не могу мјерити као на примјер губитак повјерења).

Одређивање ризика

Циљ овог корака је процијенити ниво ризика којем је изложен информациони систем. Утврђивање ризика изложености одређеној комбинацији пријетње и рањивости може се изразити као функција:

- Вјеројатности да ће одређени извор пријетње искористити рањивост система
- Јачина учинка у случају успјешног извршења пријетње
- Адекватност планираних или постојећих контрола за смањивање или спрјечавање ризика.

Једна од метода помоћу које се може утврдити ниво ризика је матрица процјене ризика.

Матрица нивоа ризика

Ниво ризика може се израчунати помоћу матрице, тако да се помножи оцјена која је додијељена вјеројатности да извор пријетње искористи рањивост ИС-а са оцјеном учинка. Матрица ниво ризика (енг. Risk-Level Matrix) може бити различитих димензија (3 x 3, 4 x 4, 5 x 5) и садржавати различите додијељене бројчане вриједности. Табела 3 једноставан је приказ матрице 3 x 3.

Вјероватност пријетње	Учинак		
Висока (1.0)	мали 10 X 1.0 = 10	средњи 50 X 1.0 = 50	велики 100 X 1.0 = 100
Средња (0.5)	средњи 10 X 0.5 = 5	средњи 50 X 0.5 = 25	средњи 100 X 0.5 = 50
Ниска (0.1)	мали 10 X 0.1 = 1	мали 50 X 0.1 = 5	мали 100 X 0.1 = 10

Табела 3: Матрица нивоа ризика (према Стонебурнер и сар.)

Сваком нивоу се додаје вриједност, у овом случају 1.0 за високу, 0.5 за средњу и 0.1 за ниску вјеројатност пријетње, те 100 за велики, 50 за средњи и 10 за мали учинак. Гледајући Табелу 3 скала нивоа ризика била би: висока ако је добијена

вриједност >50 до 100, средња ако је >10 до 50 и ниска ако је 1 до 10. Ако је процијењени ризик већи од 51, потребно га је хитно смањити и план корективних мјера у што краћем року саставити. Ако је ризик процијењен као средњи (>10 до 50), план корективних мјера се треба у разумном времену саставити и провести. Ако се ризик испостави као низак (1 до 10), треба процијенити је ли потребно провођење корективних мјера или је ризик као такав прихватљив.

Препорука контрола

Након одређивања ризика слиједи препорука контрола. У овом кораку предлажу се контроле и алтернативна рјешења која би могла смањити или елиминисати већ прије идентификоване ризике. Циљ је помоћу предложених контрола смањити ниво ризика информационог система и података на прихватљив ниво, а факторе које треба приликом предлагања узети у обзир су: дјелотворност предложених контрола, важеће прописе, интерне акте, те утицај на пословне процесе и безбједност ИС-а. Приликом представљања могућих контрола лицу задуженом за прихваћање нивоа безбједности стручњак односно аналитичар треба понудити као опцију барем два различита пакета против мјера, те за сваку опцију навести очекиване трошкове и количину ризика коју ће прихватити доносилац одлуке.

Документовање разултата

Након провођења свих претходних корака, односно након што је процес процјене ризика ИС-а завршен, потребно је документовати разултате у облику службеног извјештаја. Извјештај о процјени ризика помаже менаџменту и осталим одговорним лицима у доношењу одлука о промјенама интерних аката и прорачуна те о оперативним и управљачким промјенама. Извјештај треба имати систематски и аналитички приступ процјени ризика. Такав приступ омогућава менаџменту да разумије ризике и расподијели ресурсе потребне за смањење потенцијалног губитка.

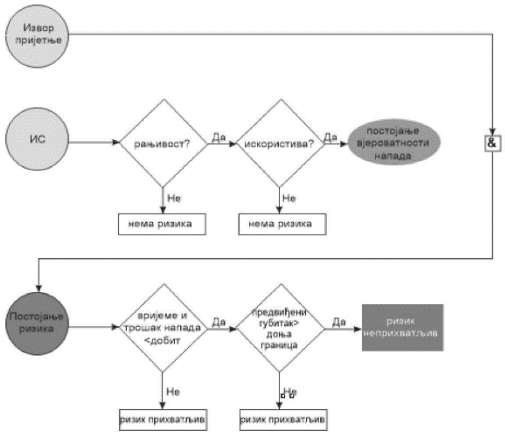
Ублажавање ризика

Након процеса процјене ризика потребно је развити сценарије управљања ризицима. Типични сценарији управљања су:

- Прихваћање ризика – институција је упозната са интензитетом ризика, надгледа га и процјењује његов утицај на пословање и пословне процесе. У случају да ниво ризика постане неприхватљива предузимају се противмјере.
- Смањивање интензитета ризика – институција предузима одговарајуће активности којима се смањује утицај ризика на пословање или вјероватност његова настанка.
- Избјегавање ризика –институција или у потпуности или дјеломично избјегава ризик.
- Подјела ризика – институција ризик прослиједјује на неку другу или трећу страну (на примјер купња полице осигурања).

Зависно о разултатима процјене ризика, одабире се најадекватнији сценарио. Ако се испостави да је ризик велики, односно да постоји висока вјероватност да ће рањивост информационог система бити искоришћена и тиме негативно утицати на пословање, потребно је под хитно предузети одговарајуће противмјере (јер адекватне контроле не постоје), те се захтијева промптна реакција највиших нивоа менаџмента (стратегија смањења интензитета ризика). Ако је ризик познат, односно идентификован, прати се његов утицај на пословање и нису потребне тренутне акције. У зависности о стању информационог система одабире се најприкладнија стратегија. Приликом одабира сценарија за управљање ризицима, постављају се питања попут: када је ризик прихватљив, а када није? или је ли и када је потребно провођење противмјера?

Како донијети одлуку може се једноставно приказати помоћу дијаграма стабло одлучивања:



Дијаграм 1: Испитивање стања информационог система (према Стонебурнер и сар.)

Ако рањивост (слабост) ИС-а постоји, потребно је повећати његову безбједност (заштиту) како би се смањила вјероватност искоришћавања његове рањивости. У случају да рањивост може бити искоришћена, потребна је вишеслојевита заштита као и укључивање административних контрола како би се смањио или спријечио ризик. У случају да је вријеме и трошак напада мањи од потенцијалног добитка, потребно је тада смањити нападачеву мотивацију тако да се његов трошак повећа. Установи ли се да предвиђени губитак институције надмашује доњу границу, потребно је предузети техничке и нетехничке противмјере (имплементација одговарајућих контрола).

Контроле информационог система

Ако се на основу разултата процеса процјене ризика дошло до закључка да је информациони систем изложен ризику, те да је вјероватноћа искоришћавања рањивости система висока, потребно је имплементирати нове или модификовати постојеће контроле. Сценарији управљања ризицима односе се на одређивање одговарајућих врста информационих контрола, односно ручних, аутоматских и полуаутоматских контрола ИС-а. Информационе контроле су контроле уграђене у рад информационог система, које представљају систем (скуп) међусобно повезаних компоненти које, дјелујући јединствено и усклађено, потпомажу остваривање циљева ИС-а, а усмјеравају се на нежељене догађаје или процесе у ИС-у који могу настати из различитих разлога који се односе на унутрашње дјеловање ИС-а (нетачни подаци, недјелотворни процеси, неадекватни улази у систем и слично) или узроке из његовог окружења. Једноставније речено сврха контрола је смањити вјероватноћу настанка нежељеног догађаја као и смањивање очекиваних губитака до којих би дошло код појаве или остварења нежељеног догађаја/процеса. Што су контроле информационог система дјелотворније, то је мањи ризик којем је он изложен.

Контроле ИС-а могу се подијелити са обзиром на начин примјене (аутоматске, ручне), са обзиром на сврху (већ прије споменуте превентивне, детективне и корективне), са обзиром на хијерархију (корпоративне, управљачке, оперативне) и са обзиром на начин функционисања (прганизационе, технолошке, физичке).

Аутоматске контроле представљају заштитне механизме пословних процеса, те су најчешће уграђене у аутоматизам функционисања ИС-а. Ручне контроле се односе на ручне провјере функционисања ИС-а. Организационе се односе на интерне акте којима се прописују жељена понашања приликом коришћења ИС-а, технолошке односе се на мрежну инфраструктуру, податке и опрему, а физичке на опипљиви дио имовине информационог система.

Како би се смањио ризик којем је ИС изложен, те повећала дјелотворност контрола за рад ИС-а и институције, институција треба узети у обзир корпоративне, управљачке и оперативне безбједносне контроле или њихову комбинацију.

Стандарди и оквири информационе безбједности

За институције стандарди и оквири представљају важну подлогу за развијање нових или проширење већ познатих тематских подручја. Како би се подржала информациона безбједност, развили су се током историје различити стандарди и оквири. Примјеном таквих безбједносних стандарда и оквира жели се обезбједити увођење општепризнатих и јединствених метода за реализацију информационе безбједности.

Међу најпознатијим стандардима и оквирима за информациону безбједност и управљање информацијским системима су породице ИСО 27000 стандарда, CobiT 5 и ITIL.

Породица ИСО 27000 стандарда

Међународна организација за стандардизацију (енг. International Organization for Standardization) је 2005. године увела ИСО/ИЕЦ 27001 стандард, који је данас најраширенији стандард управљања информационом безбједношћу. ИСО 27001 стандард директно се односи на безбједност информација и представља минималне захтјеве и мјере које институција треба предузети да би се успоставио систем управљања информационом безбједношћу (енг. Information Security Management System – ISMS). Породица ИСО 27000 стандарда обухвата попис контрола које треба имплементирати у информациони систем како би се безбједносни ризик свео на прихватљив ниво. Новији стандарди породице ИСО 27000 су ИСО 27002 до 27005, који би осим безбједности требале покрити и подручја управљања информационим ризицима и провођење механизама контроле на информационим системима у сврху остваривања безбједносних и других ризика. Најчешћи разлог имплементације ИСО 27001 стандарда је цертификација, јер прописује захтјеве према којима је институцију могуће цертификовати, међутим без ИСО стандарда 27002, који представља скуп добрих пракси за имплементацију контрола везаних уз безбједност информационих система, цертификација је тешко изводљива.

CobiT 5

CobiT (енг. Control Objectives for Information and Related Technology) представља смјернице за анализу, мјерење и контролу примјене ИС-а и припадајуће технологије у пословању, те садржи 37 циљева контроле и преко 300 информационих контрола и упута за њихову примјерну. ЦобиТ дефинише радни оквир тако да су пословни процеси институције у складу са архитектуром и функцијом ИС-а, смањени ризици који настају неисправним или непотпуним поставкама ИС-а и да је омогућено управљање ризицима ИС-а на задовољавајући начин и коришћење информационих ресурса на рационалан и дјелотворан начин.

ITIL

ITIL (енг. Information Technology Infrastructure Library) један је од најопширнијих стандарда. Иако је настао прије тридесет година данас се наметнуо као користан, практичан и у свјетским размјерима готово неизоставан скуп препорука и најбоље праксе при управљању информационим услугама (енг. ИТ Service Managment, ITSM). Прва верзија ITIL-а настала је 1986., а састојала се од 40 књига и вриједила до 1999., након тога изашла је друга верзија која се састојала од 8 књига. Посљедње издање (в3) организовано је у пет књига и у потпуности усмјерено на питање пружања ИТ услуга у сврху остваривања пословних циљева. Прве три књиге обрађују основне ИТ процесе, али и оперативне ИТ процесе попут управљања инцидентима, а преостале двије разматрају управљачки дио планирања, надзора и континуираног побољшавања рада информационог система. ITIL пружа пословно усмјерен приступ менаџменту информатике који ставља посебан нагласак на стратешку пословну вриједност информатике и потребу да се испоручи њезина висококвалитетна услуга.

Закључак

Због све бржег развоја информационо комуникационих технологија доступност и расположивост информацијама све је већа. Информације су постале један од кључних ресурса данашњице, а примјена дигиталних технологија у пословању све је већа. Информациони системи постали су неизоставан дио сваке институције. Савремени информациони системи и информациони системи уопште увелико придоносе нормалном одвијању пословања те имају позитиван учинак на пословање, због чега је управљање ризицима информационог система веома битан и потребан дио сваке институције.

Понекад се схваћање ризика узима олако и не посвећује му се довољна пажња, посебно јер се ради о сложеном и дуготрајаном процесу. Али ако институција не посвети довољно пажње том аспекту, штете које могу настати могу бити понекад и непоправљиве. Штетни учинци ризика информационог система резултују нарушавањем својстава информација, а произлазе из дјеловања пријетњи које искоришћавају рањивости ресурса информационог система.

Да би заштита информационог система била што боља потребно је укључити све кораке процеса управљања ризиком, што значи, од разумијевања самог информационог система, идентификацију могућих пријетњи све до предузимања одговарајућих контрола (противмјера). Када се спомиње заштита информационог система често се мисли на његову логичку заштиту, али важно је рећи како је физичка заштита информационог система једнако важна као и његова логичка.

Паралелно са развојем информационо комуникационих технологија и примјеном информационих система у пословању и уопште, развила се и свијест о важности информационе безбједности. Као разултат тога развили су се стандарди и оквири који данас чине подлогу за успјешно управљање информационом безбједношћу и информационим системима.

У складу са Политиком и Смјерницама за израду методологије процјене ризика препоручује се Институцијама БиХ да донесу своје интерне акте у складу са корацима дефинисаним у дијаграму процјене ризика.

ЛИТЕРАТУРА:

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. - 2022. година ("Службени гласник БиХ " број 38/17)
2. Стандард ИСО/ИЕЦ 27001 - Сигурносне технике - Системи за управљање сигурношћу информација – Захтјеви Стандард ИСО/ИЕЦ 27002
3. Стонебурнер, Г., Гогуен, А., Феринга, А.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30.