**2.4. Educiranje o informacijskoj sigurnosti**

Svi zaposleni institucije i ukoliko se ukaže potreba, partneri i personal treće strane trebaju proći odgovarajuću obuku o svijesti o informacijskoj sigurnosti te pravodobno biti upoznati sa dopunama ili promjenama u sigurnosnoj politici institucije.

Temeljni pojmovi o sigurnosti i obuka o svijesti o informacijskoj sigurnosti trebaju bit prezentirani zaposlenima, partnerima i trećoj strani prije dodjeljivanja prava pristupa informacijama. Educiranje korisnika mora bit sukladno s ulogom, sposobnošću i odgovornosti pojedinca.

**3. Prestanak radnog odnosa**

Postupak prestanka radnog odnosa zaposlenog u instituciji važno je pravodobno i kvalitetno obaviti kako se korisniku ne bi pružila mogućnost obavljanja zlonamjernih radnji. Prilikom prestanka radnog odnosa potrebno je zadovoljiti sljedeće sigurnosne kontrole:

- najvažniji dio prestanka radnog odnosa - **ukloniti sva prava pristupa** resursima institucije; ukoliko je moguće potrebno je prava pristupa ukloniti automatski pomoću posebnih programa (pristup programskim resursima),
- svi ključevi, pametne kartice i sl. također moraju biti vraćeni,
- svu imovinu koju je dobio na korištenje korisnik mora vratiti u posjed institucije,
- svi postupci vezani uz prestanka radnog odnosa (npr. vraćena imovina) trebaju biti dokumentirani.

**4. Zaključak**

Sukladno s Politikom i Smjernicama o zaposlenju i prekidu zaposlenja preporučuje se Institucijama BiH da donesu svoj interni akt u kojem će definirat **pravila/procedure o zaposlenju i prekidu zaposlenje.**

Literatura

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za period 2017. - 2022. godina ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustav za upravljanje sigurnošću informacijama - Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija

**SMJERNICE ZA IZRADU METODOLOGIJE PROCJENE RIZIKA**

**Uvod**

Potrebe za kvalitetnim rješenjima i pouzdanim sustavom upravljanja sigurnošću unutar institucije postala je jedan od temeljnih zahtjeva za uspješno obavljane poslovnih zadataka. U vrijeme kada računarska komunikacijska infastruktura predstavlja okosnicu poslovanja gotovo svih modernih firmi i institucija, upravljanje sigurnosnim rizicima igra veoma važnu ulogu u procesu zaštite informacijskih resursa i poslovnih procesa.

Za proces upravljanja sigurnosnim rizikom slobodno se može reć da predstavlja temelj izgradnje sigurne i pouzdane računarske infrastrukture. Identifikacija kritičnih informacijskih resursa i određivanje pripadajućih sigurnosnih rizika, proces je koji omogućuje kvalitetnije i ekonomičnije donošenje odluka vezanih uz unaprjeđenje sigurnosti. Bez odgovarajućih analiza i kvalitetno razrađenih planova, razvitak i implementiranja sigurnog računarskog okruženja vrlo je često kaotičan proces koji rezultuje brojnim propustima i nedostatcima.

U ovom dokumentu opisani su temeljni ciljevi i ideje procesa upravljanja sigurnosnim rizicima, načini njegovog sprovođenja, kao i tipični problemi koji se javljaju u ovom području. Veći dio dokumenta posvećen je procjeni rizika, postupku na kojem se bazira gotovo cijeli program upravljanja sigurnosnim rizikom.

**Upravljanje sigurnosnim rizikom**

Sigurnosni rizik definira se kao mogućnost realiziranja nekog neželjenog događaja, koji može negativno utjecat na povjerljivost (engl. confidentiality), integritet (engl. integrity) i raspoloživost (engl. availability) informacijskih resursa. Pod informacijskim resursima podrazumijevaju se sva ona sredstva koja institucija koristi u svrhu ostvarivanja svojih poslovnih ciljeva (hardver, softver, ljudski resursi, podaci i sl.)

Precizno identificiranje, odnosno klasifikacija informacijskih resursa prvi je, i vrlo važan, korak procesa upravljanja sigurnosnim rizikom, budući da se na temelju njega određuje koji resursi zahtijevaju kakav tretman sa stanovišta sigurnosti. Neadekvatno obavljeno identificiranje resursa može cijeli proces odvesti u pogrešnom smjeru, čime se u potpunosti gubi njegov značaj i smisao. Upravljanje sigurnosnim rizikom (engl. Risk Management), relativno je nova disciplina u području sigurnosti IT sustava, koja je proizašla iz potrebe za standardizacijom i formalizacijom postupaka vezanih uz upravljanje sigurnošću. Definira se kao proces identifikacije onih činilaca koji mogu negativno utjecati na povjerljivost, integritet, i raspoloživost računarskih resursa, kao i njihova analiza u smislu vrijednosti pojedinih resursa i troškova njihove zaštite. Završni korak obuhvaća preduzimanje zaštitnih mjera koje će identificirati sigurnosni rizik svesti na prihvatljivu razinu, sukladno poslovnim ciljevima institucije.

U kojoj mjeri i na kojim mjestima će se pristupiti umanjivanju sigurnosnog rizika, odluka je prvenstveno menadžmenta, kao one funkcije koja ima mogućnost donošenja odluka i pravo raspolaganja nad proračunom institucije. Sigurnosni rizik moguće je tretirati na nekoliko načina. Moguće ga je prihvatiti onakvim kakav je, moguće je pristupiti njegovom umanjivanju, implementiranjem odgovarajućih sigurnosnih kontrola, a moguće je i njegovo ignorisanje, odnosno prebacivanje drugim institucijama. Spomenute tehnike bit će detaljnije opisane kasnije u dokumentu. Donošenje odluka vezanih uz upravljanje rizikom vrlo je odgovoran i zahtjevan posao koji, osim određene razine stručnosti, zahtjeva i veoma dobro poznavanje IT sustava i njegove funkcije.

Proces upravljanja sigurnosnim rizicima sastoji se od tri faze:

- procjena rizika (engl. Risk Assessment);
- umanjivanje rizika (engl. Risk Mitigation);
- ispitivanje i analiza (engl. Evaluation and Assessment).

Svaka od navedenih faza ima svoju ulogu i cilj u kompletnom programu upravljanja sigurnosnim rizikom. U nastavku dokumenta biti će detaljnije opisana svaka od faza, zajedno sa svojim temeljnim karakteristikama i specifičnostima.

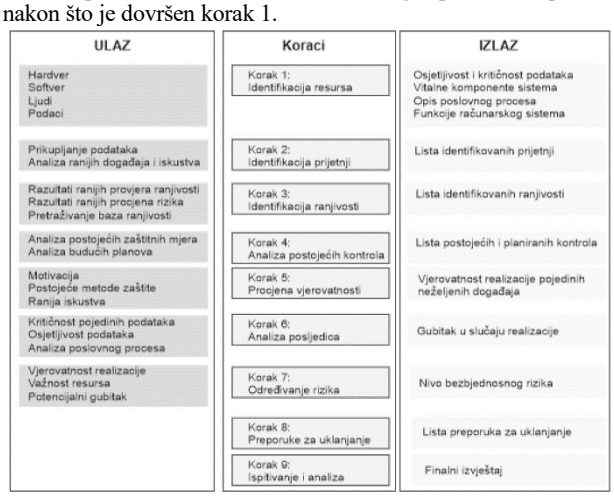
**Procjena rizika**

Procjena rizika vrlo je složen i zahtjevan postupak te stoga mora biti proveden profesionalno i temeljno kako bi se dobili mjerodavni podaci. Sam proces analize i procjene najbolje je dodjeliti sigurnosnim stručnjacima sa iskustvom na području sigurnosti informacijskih sustava (po mogućnosti neovisnim konzultantima), a razultate procjene dati menadžmentu na temelju kojih će se donosit odgovarajuće odluke. Proces procjene rizika sastoji se od devet koraka:

- Korak 1: Identificiranje i klasificiranje resursa (engl. Asset Identification);
- Korak 2: Identificiranje prijetnji (engl. Threat identification);
- Korak 3: Identificiranje ranjivosti (engl. Vulnerability Identification);
- Korak 4: Analiza postojećih kontrola (engl. Control Analysis);
- Korak 5: Vjerojatnoća pojave neželjenih događaja (engl. Likelihood Determination);

- Korak 6: Analiza posljedica (engl. Impact Analysis);
- Korak 7: Određivanje rizika (engl. Risk Determination);
- Korak 8: Preporuke za umanjivanje (engl. Control Recommendation);
- Korak 9: Dokumentacija (engl. Result Documentation).

Na sljedećoj slici ( Slika 1) priložen je dijagram na kojem je prikazan tjek navedenih faza sa ulaznim i izlaznim parametrima. Treba napomenuti da se koraci 2, 3 i 4 mogu sprovoditi u paraleli nakon što je dovršen korak 1.




Slika 1: Procjena rizika - dijagram

Iako određivanje sigurnosnog rizika zahtjeva provođenje svih ovih koraka, sam rizik matematički se može posmatrati kao funkcija tri parametra: prijetnji, ranjivosti i vrijednosti resursa (Slika 2).

**Rizik=f (Prijetnje, Ranjivosti, Vrijednost resursa)**

Što je sustav više izložen prijetnjama, što je veći broj ranjivosti i što je resurs značajniji za instituciju to je i sigurnosni rizik veći. Naravno, jasno je da se sigurnosni rizik nikada neće uklanjati smanjivanjem vrijednosti resursa, već implementiranjem odgovarajućih sigurnosnih kontrola koje će utjecat na parametre ranjivosti i prijetnji.

Vrijednost resursa koji je ovdje naveden kao jedan od parametara o kojemu ovisi razina sigurnosnog rizika, može se posmatrati i na drugačiji način. Naime, vrlo često se umjesto vrijednosti resursa kao treći parametar u obzir uzima potencijalni gubitak za instituciju u slučaju gubitka ili neraspoloživosti resursa o kojem se govori. Bez obzira o kojem je od dva navedena parametra riječ, ishod je identičan, budući da su vrijednost resursa i posljedice u slučaju gubitka dvije direktno vezane veličine.

**Identificiranje i klasificiranje resursa**

Prvi korak u postupku procjene rizika je identificiranje, odnosno klasificiranje informacijskih resursa. U ovom koraku potrebno je identificirati sve one resurse koji predstavljaju značaj za instituciju te im dodijeliti odgovarajuću vrijednost. Ukoliko postoji mogućnost, svakom resursu potrebno je dodijeliti konkretnu novčanu vrijednost, budući da to uveliko može doprinjeti kvaliteti rezultata cijelog postupka.

Identificiranje i dodjeljivanje vrijednosti pojedinim resursima potrebno je obaviti kako bi se u konačnici implementirale samo one sigurnosne kontrole koje su financijski isplative.

Postupku dodjeljivanja vrijednosti resursima potrebno je posvetiti posebnu pažnju, budući da loše procjene u ovom slučaju mogu cijeli proces odvesti u pogrešnom pravcu. Prilikom određivanja vrijednosti potrebno je u razmatranje uzeti brojne druge faktore, osim inicijalnih troškova njegove nabave. Neki od faktora koje je potrebno uzeti u obzir su:

- troškovi razvitka;
- troškovi održavanja i administracije;
- troškovi educiranja;
- troškovi zamjene, nadogradnje i sl.

Neki od tipičnih resursa koji predstavljaju važnost za instituciju su:

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

Pod sigurnosnim 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 temeljne skupine:

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

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

U okviru procjene rizika vrlo je važno generirati iscrpnu listu svih onih prijetnji, namjernih i nenamjernih, koje predstavljaju potencijalnu opasnost za informacijski sustav.

Prilikom identificiranja 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 sustav. Vrlo često od koristi mogu biti i razgovori sa administratorima sustava ili drugim osbljem, koje je u svakodnevnom kontaktu sa komponentama sustava.

Neke od prijetnji koje su tipične za informacijske sustave uključuju:

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

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

**Identificiranje ranjivosti**

Pod pojmom ranjivosti (engl. Vulnerability), smatraju se svi propusti i slabosti u sustavu sigurnosti koji omogućuju sprovođenje neovlaštenih aktivnosti. Ranjivosti mogu biti posljedica pogrešaka u procesu dizajna ili implementiranja sustava, kao i propusta u sustavu sprovođenja sigurnosnih 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 sigurnost, nepoznavanje i neprikladan odabir tehnologija i alata, propusti u održavanju sustava i sl.

Prema izrazu za sigurnosni rizik, za uspješno određivanje sigurnosnog rizika potrebno je također identificirati i sve ranjivosti, odnosno sigurnosne propuste u sustavu. Bez adekvatne

analize ranjivosti, gotovo je nemoguće pouzdano određivanje sigurnosnog rizika. Ovisno o broju i karakteru ranjivosti u sustavu, sigurnosni rizik može bit veći ili manji. Implementiranjem sigurnosnih kontrola kojima će se umanjiti broj ranjivosti u sustavu, direktno je moguće utjecati na umanjivanje sigurnosnog rizika.

Kada se govori o procjeni rizika, veoma je važno da se ranjivosti analiziraju u kombinaciji sa identificiranim prijetnjama, budući da su ova dva parametra međusobno povezana. Ukoliko ne postoji prijetnja koja bi iskoristila određenu ranjivost, tada ne postoji niti sigurnosni rizik. Tamo gdje nema rizika ne isplati se ulagati u zaštitu, a to je temeljni cilj postupka upravljanja sigurnosnim rizikom: implementiranje 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 sustavi, zajedno sa prijetnjama koje su vezane uz svaku od njih.

| Ranjivost | Prijetnja |
|---|---|
| Sigurnosni propusti u programskom kodu | Neovlašteni korisnici<br>Maliciozni programi<br>Nezadovoljni zaposleni<br>Teroristi |
| Neadekvatna konfiguracija Firewool | Neovlašteni korisnici<br>Maliciozni programi<br>Industrijska špijunaža |
| Nedostatak protivpožarne zaštite | Požar |
| Nedostatak antivirusne zaštite | Maliciozni programi (virusi, crvi, trojanski konj) |
| Neovlašteno korištenje telekomunikacijskih uređaja | Neovlašteni korisnici<br>Maliciozni programi<br>Bivši i nezadovoljni zaposleni |

Ono što se nameće kao temeljno pitanje kada se raspravlja o identificiranje 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 (ukoliko takvi postoje),
- analiza internih izvješća i dokumentacija vezanih uz ispitivanje, analizu i unaprjeđenje sigurnosti,
- sprovođenje specijaliziranih sigurnosnih ispitivanja (Vulnerability Scanning, Pentration Testing,Application Testing i sl.),
- pretraživanje javnih baza ranjivosti,
- razgovori sa zaposlenima i sustav administratorima itd...

Razultat ove faze treba biti detaljna lista ranjivosti prisutnih u sustavu, kao i njihova povezanost sa prijetnjama identificiranim u prethodnom koraku.

**Analiza postojećih kontrola**

U ovom koraku cilj je analizirati one sigurnosne kontrole koje su već implementirane ili koje se namjeravaju implementirati u svrhu zaštite informacijskih resursa. Ukoliko se želi izračunati vjerojatnost iskorištavanja pojedine ranjivosti od strane identificiranih prijetnji, što je sljedeći korak procesa procjene rizika, potrebno je u obzir uzeti sve postojeće kontrole prisutne u sustavu. Vrlo je mala vjerojatnost da će određena slabost ili nedostatak biti iskorišteni, ukoliko su implementirane kvalitetne sigurnosne kontrole ili ukoliko postoji mali interes za njenim iskorištavanjem. Sustavi koji barataju povjerljivim podacima kao što su npr. brojevi kreditnih kartica, obračuni plata i sl., predstavljaju puno veći izazov za neovlaštene korisnike u odnosu na ostale sustavi koji upravljaju manje povjerljivim podacima.

Sigurnosne kontrole mogu biti tehničke i ne-tehničke prirode. Pod tehničkim sigurnosnim kontrolama smatraju se sve one kontrole koje su implementirane u oblik hardvera, softvera ili nekog drugog sličnog rješenja (npr. firewool, antivirusna zaštita, sustavi kontrole pristupa i sl.). Pod ne-tehničkim kontrolama smatraju su kontrole poput sigurnosnih politika, preporuka i procedura i koje su najčešće rezultat usmene ili pismene predaje.

Još jedna od podjela, koja je više prisutna u krugovima koji se bave računarskom sigurnošću, je ona koja sigurnosna rješenja i mehanizme dijeli na:

- **Preventivne** (engl. Prevention) - ona rješenja koja djeluju preventivo u smislu sprečavanja neovlaštenih aktivnosti (npr. antivirusni programi, firewool, kontrola pristupa, i sl.)
- **Detekcijske** (engl. Detection) - sustavi koji omogućuju detekciju neovlaštenih aktivnosti (npr., alati za provjeru integriteta, i sl.);
- **Reakcijske** (engl. Reaction) - oni mehanizmi koji pomažu pri reakciji na detektovane neovlaštene aktivnosti (npr. forenzička analiza);

Razultat ovog koraka je lista postojećih ili predviđenih sigurnosnih kontrola kojima je cilj zaštita informacijskih resursa institucije.

**Vjerojatnost realiziranja**

Sljedeći korak u procesu procjene rizikanje određivanje vjerojatnosti iskorištavanja pojedine ranjivosti od strane pripadajućih sigurnosnih prijetnji. Neki od činilaca koje je ovdje potrebno uzeti u obzir su:

- motivacija i interes izvora prijetnji,
- karakter ranjivosti,
- prisutnost i kvalitet postojećih sigurnosnih kontrola.

Vjerojatnost iskorištavanja ranjivosti od strane određenog izvora prijetnji najbolje je izraziti stupanjski: npr. visok, srednji i niski stupanj, pri čemu svaki od definiranih stupnjeva ima određeni značaj i smisao.

U sljedećoj tabeli (Tabela 2) dat je primjer jedne takve podjele, sa tim da je moguće ići i na precizniju podjelu, ovisno od potreba.

| Vjerojatnost | Definicija |
|---|---|
| Visoka | Izvor prijetnje je posebno motiviran za iskorištavanje ranjivosti s obzirom na mogućnost dolaska do povjerljivih podataka. Postojeće sigurnosne kontrole su nedovoljne ili sadrže slabosti koje omogućavaju zaobilaženje definiranih sigurnosnih mjera. |
| Srednja | Izvor prijetnje je djelimično motiviran. Iako postoje mogućnosti za iskorištavanje ranjivosti postojeće kontrole to otežavaju |
| Niska | Izostanak motivacije za iskorištavanje ranjivosti. Sigurnosne kontrole kvalitetno su implementirane I iskorištavanje ranjivosti prilično je otežano. |

Tabela 2: Vjerojatnost iskorištavanja ranjivosti

Razultat ovog koraka sadrži vjerojatnost iskorištavanja pojedinih ranjivosti identificiranih u prethodnom koraku, s obzirom na navedene prijetnja.

**Analiza posljedica**

Cilj ovog koraka je procijeniti negativan učinak ako prijetnja uspješno iskoristi ranjivost sustava. Prije analize potrebno je prikupiti informacije o svrsi sustava, te o važnosti i osjetljivosti sustava i podataka. Negativan učinak događaja može se opisati kao narušavanje funkcionalnosti ili bilo kojeg temeljnog načela informacijskog sustava. Osnovni parametri informacione sigurnosti su:

- Povjerljivost (eng. Confidentiality) - siguran pristup informaciji i IS-u isključivo za to ovlaštenom licu.
- Cjelovitost (eng. Integrity) - zaštita ispravnosti i cjelovitosti podataka i informacija.
- Raspoloživost ili dostupnost (eng. Availability) - ovlaštenom licu omogućiti pravovremen i stalan pristup informacijama i IS-u.
- Identificiranje i autentificiranje - osigurava sigurnost informacijskog prostora institucije

- Autorizacija i neporecivost (eng. non-repudiation)

Posljedice koje mogu nastati narušavanjem temeljnih načela mogu biti gubitak konkurentske prednosti, gubitak povjerenja klijenata (curenje ličnih podataka korisnika u javnost), nepoštivanje mjerodavnih propisa (na primjer kršenje regulative u području zaštite ličnih podataka), financijski gubici, donošenje pogrešnih poslovnih odluka (zbog neispravnosti informacija), nemogućnost isporuke usluga klijentima.

Učinke je moguće mjeriti kvantitativno u obliku financijskih sredstava i vremena koje je potrebno uložiti kako bi se popravio sustav ili riješili problemi ili opisati kvalitativno (odnosi se na učinke koji se ne mogu mjeriti kao na primjer gubitak povjerenja).

**Određivanje rizika**

Cilj ovog koraka je procijeniti razina rizika kojem je izložen informacijski sustav. Utvrđivanje rizika izloženosti određenoj kombinaciji prijetnje i ranjivosti može se izraziti kao funkcija:

- Vjerojatnosti da će određeni izvor prijetnje iskoristiti ranjivost sustava,
- Jačina učinka u slučaju uspješnog izvršenja prijetnje,
- Adekvatnost planiranih ili postojećih kontrola za smanjivanje ili sprječavanje rizika.

Jedna od metoda pomoću koje se može utvrditi razina rizika je matrica procjene rizika.

**Matrica razine rizika**

Razina rizika može se izračunati pomoću matrice, tako da se pomnoži ocjena koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost IS-a sa ocjenom učinka. Matrica razine rizika (eng. Risk-Level Matrix) može bit različitih dimenzija (3 x 3, 4 x 4, 5 x 5) i sadržavati različite dodijeljene brojčane vrijednosti. Tabela 3 jednostavan je prikaz matrice 3 x 3.

| Vjerojatnost prijetnje | Učinak | | |
|---|---|---|---|
| Visoka (1.0) | mali 10 X 1.0 = 10 | srednji 50 X 1.0 = 50 | veliki 100 X 1.0 = 100 |
| Srednja (0.5) | srednji 10 X 0.5 = 5 | srednji 50 X 0.5 = 25 | srednji 100 X 0.5 = 50 |
| Niska (0.1) | mali 10 X 0.1 = 1 | mali 50 X 0.1 = 5 | mali 100 X 0.1 = 10 |

Tabela 3: Matrica razine rizika (prema Stoneburner i sar.)

Svakoj razini se dodaje vrijednost, u ovom slučaju 1.0 za visoku, 0.5 za srednju i 0.1 za nisku vjerojatnost prijetnje, te 100 za veliki, 50 za srednji i 10 za mali učinak. Gledajući Tabelu 3 skala razine rizika bila bi: visoka ako je dobijena vrijednost >50 do 100, srednja ako je >10 do 50 i niska ako je 1 do 10. Ako je procijenjeni rizik veći od 51, potrebno ga je hitno smanjiti i plan korektivnih mjera u što kraćem roku sastaviti. Ako je rizik procijenjen kao srednji (>10 do 50), plan korektivnih mjera se treba u razumnom vremenu sastaviti i sprovesti. Ako se rizik ispostavi kao nizak (1 do 10), treba procijeniti je li potrebno sprovođenje korektivnih mjera ili je rizik kao takav prihvatljiv.

**Preporuka kontrola**

Nakon određivanja rizika slijedi preporuka kontrola. U ovom koraku predlažu se kontrole i alternativna rješenja koja bi mogla smanjiti ili eliminirati već prije identificirane rizike. Cilj je pomoću predloženih kontrola smanjiti razinu rizika informacijskog sustava i podataka na prihvatljivu razinu, a faktore koje treba prilikom predlaganja uzeti u obzir su: djelotvornost predloženih kontrola, važeće propise, interne akte, te utjecaj na poslovne procese i sigurnost IS-a. Prilikom predstavljanja mogućih kontrola licu zaduženom za prihvaćanje razine sigurnosti stručnjak odnosno analitičar treba ponuditi kao opciju barem dva različita paketa protiv mjera, te za svaku opciju navesti očekivane troškove i količinu rizika koju će prihvatiti donositelj odluke.

**Dokumentiranje razultata**

Nakon sprovođenja svih prethodnih koraka, odnosno nakon što je proces procjene rizika IS-a završen, potrebno je dokumentirati razultate u obliku službenog izvješća. Izvješće o procjeni rizika pomaže menadžmentu i ostalim odgovornim licima u donošenju odluka o promjenama internih akata i proračuna te o operativnim i upravljačkim promjenama. Izvješće treba imati sustavatski i analitički pristup procjeni rizika. Takav pristup omogućava menadžmentu da razumije rizike i raspodijeli resurse potrebne za smanjenje potencijalnog gubitka.

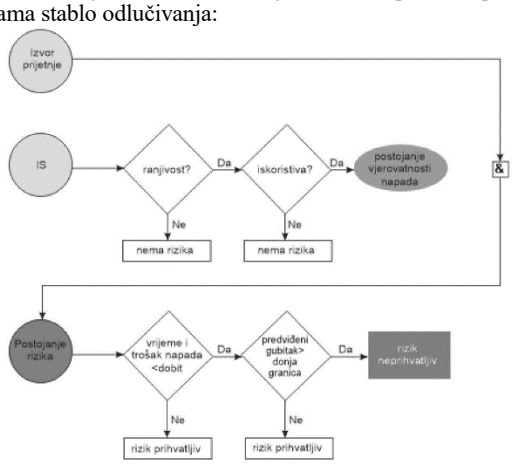
**Ublažavanje rizika**

Nakon procesa procjene rizika potrebno je razviti scenarije upravljanja rizicima. Tipični scenariji upravljanja su:

- Prihvaćanje rizika - institucija je upoznata sa intenzitetom rizika, nadgleda ga i procjenjuje njegov utjecaj na poslovanje i poslovne procese. U slučaju da razina rizika postane neprihvatljiva preduzimaju se protivmjere.
- Smanjivanje intenziteta rizika - institucija preduzima odgovarajuće aktivnosti kojima se smanjuje utjecaj rizika na poslovanje ili vjerojatnost njegova nastanka.
- Izbjegavanje rizika -institucija ili u potpunosti ili djelomično izbjegava rizik.
- Podjela rizika - institucija rizik prosljeđuje na neku drugu ili treću stranu (na primjer kupnja police osiguranja).

Ovisno o razultatima procjene rizika, odabire se najadekvatniji scenario. Ako se ispostavi da je rizik veliki, odnosno da postoji visoka vjerojatnost da će ranjivost informacijskog sustava biti iskorištena i time negativno utjecati na poslovanje, potrebno je pod hitno poduzeti odgovarajuće protivmjere (jer adekvatne kontrole ne postoje), te se zahtijeva promptna reakcija najviših razina menadžmenta (strategija smanjenja intenziteta rizika). Ako je rizik poznat, odnosno identificiran, prati se njegov utjecaj na poslovanje i nisu potrebne trenutačne akcije. U ovisnosti o stanju informacijskog sustava odabire se najprikladnija strategija. Prilikom odabira scenarija za upravljanje rizicima, postavljaju se pitanja poput: kada je rizik prihvatljiv, a kada nije? Ili je li i kada je potrebno sprovođenje protivmjera?

Kako donijeti odluku može se jednostavno prikazati pomoću dijagrama stablo odlučivanja:




Dijagram 1: Ispitivanje stanja informacionog sistema (prema Stoneburner i sar.)

Ako ranjivost (slabost) IS-a postoji, potrebno je povećati njegovu sigurnost (zaštitu) kako bi se smanjila vjerojatnost iskorištavanja njegove ranjivosti. U slučaju da ranjivost može biti iskorištena, potrebna je višeslojevita zaštita kao i uključivanje administrativnih kontrola kako bi se smanjio ili spriječio rizik. U slučaju da je vrijeme i trošak napada manji od potencijalnog dobitka, potrebno je tada smanjiti napadačevu motivaciju tako da se njegov trošak poveća. Ustanovi li se da predviđeni gubitak institucije nadmašuje donju granicu, potrebno je preduzeti

tehničke i netehničke protivmjere (implementacija odgovarajućih kontrola).

**Kontrole informacijskog sustava**

Ako se na temelju razultata procesa procjene rizika došlo do zaključka da je informacijski sustav izložen riziku, te da je vjerojatnoća iskorištavanja ranjivosti sustava visoka, potrebno je implementirati nove ili modificirati postojeće kontrole. Scenariji upravljanja rizicima odnose se na određivanje odgovarajućih vrsta informacijskih kontrola, odnosno ručnih, automatskih i poluautomatskih kontrola IS-a. Informacijske kontrole su kontrole ugrađene u rad informacijskog sustava, koje predstavljaju sustav (skup) međusobno povezanih komponenti koje, djelujući jedinstveno i usklađeno, potpomažu ostvarivanje ciljeva IS-a, a usmjeravaju se na neželjene događaje ili procese u IS-u koji mogu nastati iz različitih razloga koji se odnose na unutarnje djelovanje IS-a (netačni podaci, nedjelotvorni procesi, neadekvatni ulazi u sustav i slično) ili uzroke iz njegovog okruženja. Jednostavnije rečeno svrha kontrola je smanjiti vjerojatnoću nastanka neželjenog događaja kao i smanjivanje očekivanih gubitaka do kojih bi došlo kod pojave ili ostvarenja neželjenog događaja/procesa. Što su kontrole informacijskog sustava djelotvornije, to je manji rizik kojem je on izložen.

Kontrole IS-a mogu se podijeliti sa obzirom na način primjene (automatske, ručne), sa obzirom na svrhu (već prije spomenute preventivne, detektivne i korektivne), sa obzirom na hijerarhiju (korporativne, upravljačke, operativne) i sa obzirom na način funkcioniranja (prganizacione, tehnološke, fizičke).

Automatske kontrole predstavljaju zaštitne mehanizme poslovnih procesa, te su najčešće ugrađene u automatizam funkcioniranja IS-a. Ručne kontrole se odnose na ručne provjere funkcioniranja IS-a. Organizacijske se odnose na interne akte kojima se propisuju željena ponašanja prilikom korištenja IS-a, tehnološke odnose se na mrežnu infrastrukturu, podatke i opremu, a fizičke na opipljivi dio imovine informacijskog sustava.

Kako bi se smanjio rizik kojem je IS izložen, te povećala djelotvornost kontrola za rad IS-a i institucije, institucija treba uzeti u obzir korporativne, upravljačke i operativne sigurnosne kontrole ili njihovu kombinaciju.

**Standardi i okviri informacijske sigurnosti**

Za institucije standardi i okviri predstavljaju važnu podlogu za razvijanje novih ili proširenje već poznatih tematskih područja. Kako bi se podržala informacijska sigurnost, razvili su se tijekom istorije različiti standardi i okviri. Primjenom takvih sigurnosnih standarda i okvira želi se osigurati uvođenje općepriznatih i jedinstvenih metoda za realiziranje informacijske sigurnosti.

Među najpoznatijim standardima i okvirima za informacijsku sigurnost i upravljanje informacijskim sustavima su porodice ISO 27000 standarda, CobiT 5 i ITIL.

**Porodica ISO 27000 standarda**

Međunarodna organizacija za standardizaciju (eng. International Organization for Standardization) je 2005. godine uvela ISO/IEC 27001 standard, koji je danas najraširenij standard upravljanja informacijskom sigurnošću. ISO 27001 standard direktno se odnosi na sigurnost informacija i predstavlja minimalne zahtjeve i mjere koje institucija treba poduzeti da bi se uspostavio sustav upravljanja informacijskom sigurnošću (eng. Information Security Management System - ISMS). Porodica ISO 27000 standarda obuhvata popis kontrola koje treba implementirati u informacijski sustav kako bi se sigurnosni rizik sveo na prihvatljivu razinu. Noviji standardi porodice ISO 27000 su ISO 27002 do 27005, koji bi osim sigurnosti trebale pokriti i područja upravljanja informacijskim rizicima i sprovođenje mehanizama kontrole na informacijskim sustavima u svrhu ostvarivanja sigurnosnih i drugih rizika. Najčešći razlog implementacije ISO 27001 standarda je certifikacija, jer propisuje zahtjeve prema kojima je instituciju moguće certifikovati, međutim bez ISO standarda 27002, koji predstavlja skup dobrih praksi za implementaciju kontrola vezanih uz sigurnost informacijskih sustava, certifikacija je teško izvodljiva.

**CobiT 5**

CobiT (eng. Control Objectives for Information and Related Technology) predstavlja smjernice za analizu, mjerenje i kontrolu primjene IS-a i pripadajuće tehnologije u poslovanju, te sadrži 37 ciljeva kontrole i preko 300 informacijskih kontrola i uputa za njihovu primjernu. CobiT definira radni okvir tako da su poslovni procesi institucije sukladni s arhitekturom i funkcijom IS-a, smanjeni rizici koji nastaju neispravnim ili nepotpunim postavkama IS-a i da je omogućeno upravljanje rizicima IS-a na zadovoljavajući način i korištenje informacijskih resursa na racionalan i djelotvoran način.

**ITIL**

ITIL (eng. Information Technology Infrastructure Library) jedan je od najopširnijih standarda. Iako je nastao prije trideset godina danas se nametnuo kao koristan, praktičan i u svjetskim razmjerima gotovo neizostavan skup preporuka i najbolje prakse pri upravljanju informacijskim uslugama (eng. IT Service Managment, ITSM). Prva verzija ITIL-a nastala je 1986., a sastojala se od 40 knjiga i vrijedila do 1999., nakon toga izašla je druga verzija koja se sastojala od 8 knjiga. Posljednje izdanje (v3) organizirano je u pet knjiga i u potpunosti usmjereno na pitanje pružanja IT usluga u svrhu ostvarivanja poslovnih ciljeva. Prve tri knjige obrađuju temeljne IT procese, ali i operativne IT procese poput upravljanja incidentima, a preostale dvije razmatraju upravljački dio planiranja, nadzora i kontinuiranog poboljšavanja rada informacijskog sustava. ITIL pruža poslovno usmjeren pristup menadžmentu informatike koji stavlja poseban naglasak na stratešku poslovnu vrijednost informatike i potrebu da se isporuči njezina visokokvalitetna usluga.

**Zaključak**

Zbog sve bržeg razvitka informacijsko komunikacijskih tehnologija dostupnost i raspoloživost informacijama sve je veća. Informacije su postale jedan od ključnih resursa današnjice, a primjena digitalnih tehnologija u poslovanju sve je veća. Informacijski sustavi postali su neizostavan dio svake institucije. Savremeni informacijski sustavi i informacijski sustavi uopće uveliko pridonose normalnom odvijanju poslovanja te imaju pozitivan učinak na poslovanje, zbog čega je upravljanje rizicima informacijskog sustava veoma bitan i potreban dio svake institucije.

Ponekad se shvaćanje rizika uzima olako i ne posvećuje mu se dovoljna pažnja, posebno jer se radi o složenom i dugotrajanom procesu. Ali ako institucija ne posveti dovoljno pažnje tom aspektu, štete koje mogu nastati mogu biti ponekad i nepopravljive. Štetni učinci rizika informacijskog sustava rezultuju narušavanjem svojstava informacija, a proizlaze iz djelovanja prijetnji koje iskorištavaju ranjivosti resursa informacijskog sustava.

Da bi zaštita informacijskog sustava bila što bolja potrebno je uključiti sve korake procesa upravljanja rizikom, što znači, od razumijevanja samog informacijskog sustava, identifikaciji mogućih prijetnji sve do poduzimanja odgovarajućih kontrola (protivmjera). Kada se spominje zaštita informacijskog sustava često se misli na njegovu logičku zaštitu, ali važno je reći kako je fizička zaštita informacijskog sustava jednako važna kao i njegova logička.

Paralelno sa razvitkom informacijsko komunikacijskih tehnologija i primjenom informacijskih sustava u poslovanju i uopće, razvila se i svijest o važnosti informacijske sigurnosti. Kao

razultat toga razvili su se standardi i okviri koji danas čine podlogu za uspješno upravljanje informacijskom sigurnošću i informacijskim sustavima.

Sukladno s Politikom i Smjernicama za izradu metodologije procjene rizika preporučuje se Institucijama BiH da donesu svoje interne akte sukladno koracima definiranim u dijagramu procjene rizika.

**LITERATURA:**


1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za period 2017. -2022. godina ("Službeni glasnik BiH " broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - sustavi za upravljanje sigurnošću informacija - Zahtjevi Standard ISO/IEC 27002
3. Stoneburner, G., Goguen, A., Feringa, A.(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.


---

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 за период од 2017 - 2022. године ("Службени гласник БиХ", број 38/17), на приједлог Министарства комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и Херцеговине на 54. сједници, одржаној 28. јула 2022. године, донио је

# ОДЛУКУ
## О УСВАЈАЊУ СМЈЕРНИЦА ИЗ ПОЛИТИКЕ УПРАВЉАЊА ИНФОРМАЦИОНОМ БЕЗБЈЕДНОШЋУ У ИНСТИТУЦИЈАМА БОСНЕ И ХЕРЦЕГОВИНЕ ЗА ПЕРИОД ОД 2017 - 2022. ГОДИНЕ

Члан 1.

(Предмет Одлуке)

(1) Овом одлуком усвајају се смјернице из Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године, и то:
   а) Смјернице о корисничким рачунима и правима приступа,
   б) Смјернице о безбједносним копијама,
   ц) Смјернице о запослењу и прекиду запослења и
   д) Смјернице за израду методологије и процјене ризика.

(2) Смјернице из става (1) овог члана су прилози ове одлуке и чине њен дио.

Члан 2.

(Праћење реализације Одлуке)

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 93/22
28. јула 2022. године
Сарајево

Предсједавајући
Савјета министара БиХ
Др **Зоран Тегелтија**, с. р.

## СМЈЕРНИЦЕ
## О КОРИСНИЧКИМ РАЧУНИМА И ПРАВИМА ПРИСТУПА

### 1. Сврха

Сврха документа је обезбједити контролу над отварањем, измјеном, замрзавањем и затварањем корисничких рачуна у информационом систему, у циљу спрјечавања застарјелих, редундантних и корисничких рачуна отворених на неисправан начин. Право приступа вриједностима информационог система једна је од најкритичнијих тачака безбједности. Због наизглед компликованог процеса додјељивања права приступа, корисницима се често додјељују "уобичајена" права, која су најчешће пуно већа од потребних. Што већа права приступа корисник посједује, веће су могућности да случајним или намјерним радњама угрози безбједност информационог система.

Обављање основне дјелатности институције повезано је са руковањем подацима који се налазе у информационом систему. Због тога је неопходно да запосленима буде омогућен приступ различитим подацима у оквиру система. Међутим, приступ запослених овим подацима треба да буде усаглашен са процесном структуром организационог система. Запосленима је потребно обезбједити приступ само оним подацима и дијеловима информационог система који су им потребни за реализацију активности за које су надлежни, а не комплетном информационом систему. Из тог разлога потребно је прилагодити права приступа информационом систему описима послова из важећег правилникао о унутрашњој организацији и систематизацији радних мјеста. Такође, уколико је институција имплементирала систем управљања квалитетом, потребно је усагласити права приступа запослених са њиховим улогама у процедурама.

Неопходно је обезбједити да је приступ информационом систему омогућен само онима који за то имају правни основ, уз одговарајућу евиденцију сваког приступа и евентуалног ажурирања. Због тога је неопходно имплементирати систем корисничких улога (рола), којим ће бити дефинисани одговарајући нивои права приступа прикупљеним подацима у информационом систему. Систем улога мора прецизно да дефинише најпре којим подацима корисник коме је додељена одређена улога уопште може да приступи, а затим и на који све начин може да их обрађује. Институција треба да успостави механизам креирања и укидања корисничких налога, те да води евиденцију свих корисничких налога у оквиру информационог система, како активним, тако и укинутим налозима. Институција прописује процедуре додјеле и укидања налога, те провјере адекватног нивоа приступа и додјеле јединствене идентификационе ознаке сваког налога.

### 2. Приступ информационом систему

Приступ информационом систему се базира на подацима за аутентификацију, као што су лозинке, криптографски кључеви, токени, смарт картице, пин код и 2ФА апликације. Дистрибуцију и чување ових података регулише институција, како би се спријечиле безбједносне пријетње попут откривања података за аутентификацију запослених (колегама, породици или трећим лицима) или записивање шифре у нотесу или на наљепници.

Основно правило при креирању лозинке јесте избјегавање података из приватног живота као што су датум рођења, име кућног љубимца, омиљено мјесто и слично, као и било какве ријечи природног језика. Класичне методе пробијања лозинке данас подразумијевају аутоматизоване претраге по списковима ријечи (dictionary attack), а који могу обухватати на милионе појмова из различитих језика. Шифра од 12 бро-