beskorisna. Preporučuje se prije izrade rezervne kopije provjeravanje integriteta sustava baza podataka.
- Provjera da se datoteka ne koristi tokom stvaranja rezervnog zapisa - ukoliko se datoteka koristi prilikom izrade rezervne kopije ona je beskorisna jer ne sadrži ispravnu i važeću verziju.
- Stvaranje rezervne kopije prije velikih promjena u sustavu baza podataka - korisno je imati rezervnu kopiju prije testiranja novog hardvera, popravaka na sustavu ili instalacije novih aplikacija.

Prilikom izrade rezervnih kopija institucije mogu koristitit i druge metode kao što su electronic vaulting, journaling i mirroring u ovisnosti o vrste poslovavanja i potreba institucije kada je u pitanju izrada rezervnih kopija.

5. Zaključak

Procesom stvaranja sigurnosnih kopija i povratom podataka smanjuju se rizici kojima je izložen informacijski sustav. Redovit i pouzdan postupak izrade sigurnosnih kopija je postupak koji se ne smije izbjeći. Bez obzira kako se tretira sustav ne mogu se izbjeći rizici od neželjenih posljedica. Rizici su obično veći nego su ljudi to sposobni shvatiti, a prema podacima se treba odnositi ozbiljno prije nego se osjete posljedice gubljenja istih. Po statistici 90% organizacija propada ako izgube vitalne zapise što pokazuje koliko su moderne organizacije ovisne o informacijskoj podršci. Jedan od nedostataka izrade sigurnosnih kopija je cijena. Naime, proces uključuje odgovarajuće medije, opremu na kojoj se pohranjuju informacije, zaposlenike koji su zaduženi za održavanje sigurnosnih kopija i primjenu politike izrade sigurnosnih kopija, a to organizacijama uzrokuje troškove bez jasno vidljivih rezultata. Ipak, dugoročno gledano ta cijena je zanemariva u odnosu na cijenu koju može platiti tvrtka ili pojedinac ukoliko nije u stanju obavljati posao. Dodatan problem koji je moguć kod organizacija koje provode politiku izrade sigurnosnih kopija je otpor zaposlenika. Zaposlenici često sam postupak izrade sigurnosnih kopija smatraju bespotrebnim jer nisu svjesni važnosti sigurnosnih kopija za cijelu organizaciju. Ipak svi su ovi potencijalni nedostaci izrade sigurnosnih kopija zanemarivi u odnosu na mogućnost prekida poslovanja i propadanja organizacije u slučaju izostanka podataka. Stoga je podatke potrebno adekvatno zaštiti, a jedan od neophodnih načina je i izradom sigurnosnih kopija.

Sukladno s Politikom i Smjernicama o rezervnim kopijama preporučuje se Institucijama BiH da donesu svoj interni akt u kojem će definirat **pravila/procedure za izradu rezervnih kopija.**

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 - Sistem za upravljanje sigurnošću informacijama - Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnost informacija

SMJERNICE O ZAPOSLENJU I PREKIDU ZAPOSLENJA

1. Suština

Suština smjernica o zaposlenju i prekidu zaposlenja je definirati procedure kojima će se precizirat koraci koje je potrebno preduzeti u pogledu sigurnosti prilikom zaposlenja, sklapanja ugovora o zaposlenju ili suradnji i koje definiraju na koji način kvalitetno sprovesti prekid zaposlenja ili raskid ugovora. Cilj navedenih procedura je smanjenje rizika od ljudske pogreške, krađa, prevara i zlouporabe resursa informacijskih sustava institucije.

2. Procedure sklapanja ugovora

Odgovorne osobe pri sklapanju ugovora o zaposlenju ili suradnji trebalo bi da provedu mjere definirane sljedećim procedurama:

2.1. Provjera

Provjera (eng. screening) u svrhu kontrole potencijalnih zaposlenika ili poslovnih partnera jedna je od preventivnih metoda kojima institucija može djelovati na sigurnost informacijskog sustava. Odgovorna osoba treba sprovesti ili inicirati provjeru i ispitivanje nad potencijalnim zaposlenikom. Proces provjere i ispitivanja treba uzeti u obzir sva prava i zakonske odredbe privatnosti te ukoliko je dopušteno uključiti sljedeće:
- raspoložive reference karaktera, poslovanja itd.,
- pregled dostupnih CV-a, kontrola dostavljenih podataka,
- potvrde o školovanju i profesionalnim kvalifikacijama,
- dokazi identiteta (putovnica),
- da li je osoba kazneno gonjena itd.

Prikupljene podatke potrebno je dokumentirati kao **povjerljive podatke** te prema njima napraviti procjenu da li postoji mogućnost zlouporabe informacijskog sustava od strane potencijalnog zaposlenika.

2.2. Uvjeti zaposlenja i ugovor odgovornosti

Prije zaposlenja osoba u institucijama BiH, sklapanja partnerstva sa drugom organizacijom ili uključivanja u posao treće strane neophodno je u rješenje ili ugovor uključiti dio koji sve strane obvezuje na pridržavanje pravila definiranih sigurnosnom politikom. Rješenje ili ugovor treba sadržavati dodatak sa pojašnjenjima i stavovima:
- da svaki zaposlenik, partner ili treća strana, prije dobivanja prava pristupa imovini organizacije, treba potpisati ugovor o povjerenju,
- zakonskim pravima i odgovornostima svakog zaposlenika, korisnika i poslovnog partnera,
- odgovornostima institucije o čuvanju i rukovanju informacijama o zaposlenima,
- odgovornostima u slučaju obavljanja posla izvan radnog vremena ili izvan prostorija institucije (npr. doma),
- akcijama koje je potrebno preduzeti ukoliko se utvrdi nepridržavanje pravila definiranih sigurnosnom politikom.
- Pojašnjenjima o postupcima u slučaju kad zaposlenik napušta Institucija u smislu poništavanja korisničkih naloga za pristup aplikacijama, sustavima i drugim resursima Institucije.

2.3. Odgovornosti rukovoditelja institucija

Rukovoditelji institucija treba da zahtjevaju i insistiraju na pridržavanju pravila definiranih sigurnosnom politikom od strane zaposlenih, korisnika, poslovnih partnera i treće strane. Njihova je obveza sve zaposlenike, korisnike, partnere i treće strane:
- pravilno i jasno informirati o njihovim ulogama u sprovođenju sigurnosti te o njihovim odgovornostima prije dodjeljivanja prava pristupa osjetljivim informacijama,
- pružiti im uvid u obliku smjernica o tome šta se očekuje od njih ovisno o njihovim ulogama,
- motivisati da se pridržavaju pravila definiranih sigurnosnom politikom,
- osigurati potrebnu razinu svijesti o potrebi za sigurnošću, ovisno o ulogama.

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);