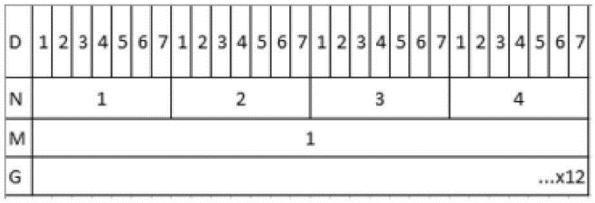
4. Vrste rezervnih kopija

Stvaranje rezervne kopije (backup) ne utiče na stepen sigurnosti samog IS, ali je od ključnog značaja kada se poslije rezervne krize javi potreba da se izgubljeni podaci povrate. Ponekad je na temelju rezervne kopije moguće utvrditi uzrok pada sistema – rekonstrukcijom rezervnih propusta ili grešaka u IS, i slično. Preporučeno je i eksterno i interno čuvanje kopija. Eksterni backup se odnosi na čuvanje datih kopija podataka na posebnim diskovima u posebnim sefovima koji su zaštićeni od mogućih nezgoda (primjer: vatrostalni sefovi). Interni backup podrazumjeva čuvanje kopija baze podataka u okviru IS, odnosno na različitim serverima ili na serveru koji je posebno namjenjen za backup. Servere treba kopirati noću. Diferencijalna kopiranja (backup promjena) treba obavljati svake noći, dok cjelokupni backup treba obavljati jednom u sedam dana. Dnevne izrade kopije treba čuvati jednu sedmicu, dok bi sedmični trebalo čuvati jedan mjesec. Mjesečne rezervne kopije treba čuvati jednu godinu, dok bi godišnje trebalo čuvati zauvijek. Podrazumijeva se da te rezervne kopije treba zaštiti od svih vrsta fizičkih povreda. Treba imati u vidu da se izbrisani podaci ponekad ne mogu povratiti.



Oznaka	Opis	Period čuvanja
D	Dnevni *backup*	7 dana
N	Nedeljni *backup*	1 mjesec
G	Mjesečni *backup*	1 godina

U nastavku slijede preporuke iz prakse za izradu rezervnih kopija:

- Provjera vraćanja podataka nakon nepravilnosti u radu sistema - u praksi se obavljaju provjere i testiranja da li je moguće nastaviti poslovanje npr. nakon kvara na čvrstom disku, ukoliko smo izgubili medije sa rezervnim kopijama ili su one ukradene. U testiranje su uključene različite smjernice koje analiziraju koliko je potrebno da se poslovanje vrati u fazu kad su izgubljeni podaci, koji su preduslovi potrebni za to, ko je odgovoran i sl. Sve ove smjernice moraju biti sadržane prilikom izrade politike rezervnih kopija.
- Periodična provjera rezervnih kopija - iz razloga što mediji i pripadajući hardver mogu biti veoma nepouzdani potrebno je periodički provoditi testiranja koja se odnose na njihovu ispravnost. Velika količina podataka pohranjenih na trakama ili disketama je beskorisna ukoliko se ne mogu pročitati sa istih. U tu svrhu potrebno je periodično provjeravati ispravnost rezervnih kopija.
- Čuvanje starih verzija rezervnih kopija - nekad je potrebno izvjesno vrijeme kako bi se utvrdilo da je neka datoteka uništena ili pobrisana. Zbog takvih slučajeva uvijek je potrebno čuvati stare verzije rezervnih kopija određeno vrijeme ili onoliko koliko nalaže zakon. Moguće je čuvati sedmične, mjesečne, polugodišnje ili godišnje verzije rezervnih kopija. Preporučuje se stare kopije čuvati na različitoj lokaciji od one na kojoj su podaci.
- Provjera sistema baza podataka prije izrade rezervnih kopija - ukoliko se radi o povratku podataka sistema koji je prethodno uništen onda je rezervna kopija beskorisna. Preporučuje se prije izrade rezervne kopije provjeravanje integriteta sistema 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 sistemu baza podataka - korisno je imati rezervnu kopiju prije testiranja novog hardvera, popravaka na sistemu ili instalacije novih aplikacija.

Prilikom izrade rezervnih kopija institucije mogu koristitit i druge metode kao što su electronic vaulting, journaling i mirroring u zavisnosti 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 informacioni sistem. Redovan i pouzdan postupak izrade sigurnosnih kopija je postupak koji se ne smije izbjeći. Bez obzira kako se tretira sistem 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 zavisne o informacionoj 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.

U skladu 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 informacionom 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. Svrha

Svrha 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 sistema institucije.

2. Procedure sklapanja ugovora

Odgovorne osobe pri sklapanju ugovora o zaposlenju ili saradnji 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 informacionog sistema. 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 (pasoš),
- da li je osoba kazneno gonjena itd.

Prikupljene podatke potrebno je dokumentirati kao **povjerljive podatke** te prema njima napraviti procjenu da li postoji mogućnost zloupotrebe informacionog sistema 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 obavezuje 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. kod kuće),
- 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 rukovodilaca institucija

Rukovodioci 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 zavisno o njihovim ulogama,
- motivisati da se pridržavaju pravila definiranih sigurnosnom politikom,
- osigurati potrebnu razinu svijesti o potrebi za sigurnošću, zavisno o ulogama.

2.4. Edukacija o informacionoj sigurnosti

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

Osnovni pojmovi o sigurnosti i obuka o svijesti o informacionoj sigurnosti trebaju bit prezentirani zaposlenima, partnerima i trećoj strani prije dodjeljivanja prava pristupa informacijama. Edukacija korisnika mora bit u skladu s ulogom, sposobnošću i odgovornosti pojedinca.

3. Prestanak radnog odnosa

Postupak prestanka radnog odnosa zaposlenog u instituciji važno je pravovremeno 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

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

Literatura

1. Politika upravljanja informacionom 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 sigurnosti informacija

SMJERNICE
ZA IZRADU METODOLOGIJE PROCJENE RIZIKA

Uvod

Potrebe za kvalitetnim rješenjima i pouzdanim sistemom upravljanja sigurnošću unutar institucije postala je jedan od osnovnih 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 informacionih resursa i poslovnih procesa.

Za proces upravljanja sigurnosnim rizikom slobodno se može reć da predstavlja temelj izgradnje sigurne i pouzdane računarske infrastrukture. Identifikacija kritičnih informacionih 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, razvoja i implementiranja sigurnog računarskog okruženja vrlo je često haotičan proces koji rezultuje brojnim propustima i nedostatcima.

U ovom dokumentu opisani su osnovni ciljevi i ideje procesa upravljanja sigurnosnim rizicima, načini njegovog sprovođenja,