- potrebno je omogućit uvid tko sve ima prava nad pojedinim resursom, s mogućnošću filtriranja rezultata.

3. Evidencija zahtjeva

Pravodobno zatvaranje korisničkog računa važna je karika u sigurnosti informacijskih sustava. Ukoliko "nevažeći" korisnički račun nije zatvoren, korisniku je otvoren put obavljanju zlonamjernih radnji. Kako bi proces otvaranja i zatvaranja korisničkih računa bio pravodobno i kvalitetno obavljen, potrebno je definirati načine komunikacije između podnositelja zahtjeva i administratora sustava, te način evidencije zahtjeva za otvaranjem odnosno zatvaranjem računa. Prijedlog komunikacije i evidencije zahtjeva:

- komunikacija sa osobom odgovornom za upravljanje korisničkim računima obavlja se unaprijed definiranim protokolom, npr. putem web aplikacije,
- kako bi podnositelj zahtjeva pristupio aplikaciji, potrebno je obavit provjeru autentičnosti i autorizaciju,
- podnositelj zahtjeva na svom računalu otvara aplikaciju i zadaje zahtjev za otvaranjem/zatvaranjem korisničkog računa,
- zahtjev se pohranjuje u bazu podataka,
- administrator ima mogućnost pregleda zahtjeva prema kriteriju,
- administrator je dužan redovno pregledavati zahtjeve,
- zatvaranje zahtjeva ima prednost nad otvaranjem zahtjeva.

Protokol komunikacije između podnositelja zahtjeva i odgovorne osobe, te evidencije samih zahtjeva može biti realiziran i na neki drugi način odobren od strane institucije.

4. Otvaranje korisničkog računa

Korisnički račun moguće je otvoriti:

- zaposlenima,
- trećoj strani.

Procedura otvaranja korisničkog računa:

zaposlenima:

- ovlaštena osoba institucije putem aplikacije podnosi zahtjev za otvaranje korisničkog računa novom zaposlenom,
- administrator sustava na temelju dobijenih podataka otvara korisnički račun.

trećoj strani:

- za otvaranje korisničkog računa trećoj strani potrebna je suglasnost ovlaštenog lica (administrator informacijskog sustava) institucije,
- ovlašteno lice je glavno i odgovorno lice u suradnji sa trećom stranom i kao takvo ima prava davanja suglasnosti za otvaranje korisničkih računa,
- kod otvaranja korisničkog računa za treću stranu potrebno je odrediti vremensko razdoblje koliko će račun biti aktivan.

5. Zamrzavanje korisničkog računa

U slučaju dužeg planiranog nekorištenja informacijskog sustava (npr. zbog edukacije u inozemstvu, bolesti, neplaćeno odsustvo i sl.) korisnički račun potrebno je zamrznuti (preko Active Directory za institucije koje su korisnice eVlade). Zamrzavanjem korisničkog računa izbjegavaju se nepotrebni postupci zatvaranja i otvaranja računa, ali i sprječavaju sigurnosni incidenti koji mogu nastati korištenjem korisničkog računa od strane drugih lica dok stvarni vlasnik nije prisutan. Zamrzavanje računa odvija se na način da podaci ostanu u bazi podataka o korisniku, ali se u posebno polje naznači da je račun zamrznut. Zamrznutom korisničkom računu nije potrebno mijenjati lozinku u određenom vremenskom razdoblju kako je definirano politikom. Također se zaobilaze sve druge sigurnosne kontrole od strane sustava za koje je potrebna interakcija korisnika. Zamrznuti korisnički račun moguće je vratiti u uporabu (odmrznuti) na zahtjev korisnika i odgovorne osobe, s tim da zahtjev mora biti dokumentovan i odobren kao i kod otvaranja novog zahtjeva.

6. Zatvaranje korisničkog računa

Zatvaranje korisničkog računa posebno je osjetljiv postupak, a osjetljivost zavisi o organizaciji upravljanja korisničkim računima. Što je upravljanje računima nekvalitetnije izvedeno, to će zatvaranje korisničkih računa biti komplikovanije. Na primjer, ako se korisnički računi otvaraju bez dokumentiranja i na temelju trenutnih potreba, nakon npr. godine dana više se ne zna ko ima pravo pristupa nad kojim resursima. Tada je i zatvoriti korisnički račun puno teže. Ukoliko "zatvorenom" korisniku ostanu neka prava pristupa, put za počinjenje zlonamjernih akcija mu je otvoren. Ovo je još jedan primjer zašto je kvalitetna organizacija korisničkih računa potrebna.

Zatvaranje korisničkog računa odvija se kroz sljedeće faze:

- pri prekidu radnog odnosa potrebno je predati zahtjev o zatvaranju korisničkog računa zaposlenog,
- trećim licima korisnički račun se zatvara nakon definiranog vremenskog razdoblja prilikom otvaranja računa, ili ukoliko je potrebno prije na zahtjev odgovornog lica zaduženog za suradnju sa trećom stranom,
- lice odgovorno za vođenje korisničkih računa dužno je redovito pregledavati zaprimljene zahtjeve za zatvaranjem računa te ih pravovremeno zatvoriti,
- ukoliko postoji potreba, korisniku je moguće prijevremeno zatvoriti korisnički račun bez prethodne obavijesti na temelju pisanog zahtjeva ovlašćene osobe institucije.

7. ZAKLJUČAK

Sukladno s Politikom i Smjernicama o korisničkim računima i pravima pristupa preporučuje se Institucijama BiH da donesu svoj interni akt u kojem će definirati **pravila/procedure o korisničkim računima i pravima pristupa**.

Literatura

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 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
4. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", broj 54/05 i 12/09)

SMJERNICE O SIGURNOSNIM KOPIJAMA

1. Suština

Danas računari i aplikacije služe za povećavanje produktivnosti, smanjivanje troškova i uštedu vremena potrebnog za obavljanje posla. Ukoliko se nedovoljna pažnja posveti rizicima koji ugrožavaju računalske sustave, u institucijama su moguće situacije koje mogu uzrokovati zastoje u poslovanju. Da se ne bi dogodio neplanirani zastoj, institucije moraju redovno izvršavati procedure za izradu i održavanje rezervnih kopija. U protivnom može doći do katastrofalnih posljedica. Uzrok tome je što je poslovanje ovisno u informacijskim tehnologijama. Pred informatičke podatke se postavljaju visoki kriteriji zaštite koji su jednaki ili čak veći od kriterija zaštite zapisa u poslovnim knjigama. Informacijski sustav je dio infrastrukture institucije te je iz tog razloga nedostupnost istog ili uništenje podataka veliki rizik za koji treba planirati mjere kontrole i obavljati postupke kojima se povećava potpuno, sigurno i jeftino vraćanje podataka.

Izrada rezervnih kopija (eng. backup) je temeljna pretpostavka koja se postavlja pred sustav koji mora zadovoljavati rezervne zahtjeve. Postupak izrade rezervnih kopija zajedno sa postupkom povratka podataka, predstavlja temeljnu proceduru kojom se sustav štiti od gubitka podataka i osigurava brza obnova podataka u slučaju nepravilnosti u radu sustava kao što su npr. prekidi u radu računalnog sustava, infekcije virusima ili pak prirodne katastrofe poput poplava i požara. Potrebno je ispitati ispravnost rezervne kopije i procijeniti koliko je pouzdan medij na kojem je ona smještena. Rezervna kopija gubi svoju namjenu ukoliko se za vrijeme povrata podataka otkrije da je ona na pogrešnom mediju, pogrešno označena ili uništena. Rezervne kopije podataka, smještene na informacijskom sustavu institucija, rade se u svrhu osiguranja podataka od vitalnog značaja za normalno funkcioniranje institucije. Zadatak rezervnih kopija je osigurati oporavak sustava na temelju autentičnih, cjelovitih i raspoloživih prethodno pohranjenih podataka, u slučaju oštećenja nastalih povredom integriteta podataka usljed vremenskih nepogoda, potresa, ratnih razaranja, požara, poplave ili kavarije samih sustava.

Politika rezervnih kopija ima namjeru da jedinstveno u cijeloj instituciji definira načine postupanja prema podacima, načine izrade rezervnih kopija te vraćanja podataka u slučaju određenih gubitaka. Rizik koji se odnosi prema informacijama određuje svaka institucija zasebno, a učestalost izvođenja izrade rezervnih kopija se određuje sukladno važnošću informacija i pripadajućim rizikom. Postupak izrade rezervnih kopija i vraćanje podataka treba biti dokumentovan u obliku procedure i primjenjiv u svim dijelovima institucije.

2. Razlozi za izradu rezervnih kopija

Jedan od glavnih razloga za izradu rezervnih kopija je raspoloživost sustava. Svaki poremećaj u radu sustava se odražava u prestanku rada istog. Posljedice nemogućnosti odvijanja poslovnih procesa se ovisno o važnosti tih procesa, mjere u različitim iznosima (od hiljadu do milijun). S tim razlogom je potrebno osigurati izradu rezervnih kopija kako bi se u izvanrednim okolnostima moglo nastaviti sa poslovanjem. Osiguranje neprekidne raspoloživosti i mogućnost nastavka rada informacijskog sustava usljed nepredviđenih okolnosti, čine uspješnim poslovanje institucije, dok se u slučajevima neispunjena tih uvjeta uzrokuju uz financijske i neke nepopravljive štete kao što su gubitak ugleda, nepovjerenje građana i prestanak suradnje sa međunarodnim institucijama. Ukoliko institucija raspolaže rezervnim kopijama, u slučajevima elementarnih nepogoda (požar, potres, poplava, sabotaže, teroristički napadi, itd…) ili drugih uzroka prekidanja rada, institucija posjeduje mogućnost uspostave poslovanja na drugim lokacijima. Neki od uzroka koji mogu prouzročiti prekid poslovanja su kvarovi na strujnom napajanju, kvarovi računala ili diskovnih medija čime se trenutno gube informacije. Izuzev tih uzroka prekidanja poslovanja postoje i oni uzrokovane ljudskim faktorom, a to su ljudska pogreške, zlonamjerne aktivnosti lokalnih korisnika ili udaljenih napadača. Također, virusi i drugi maliciozni programi mogu uništiti vrijedne podatke. Još jedan razlog za izradu rezervnih kopija je zakonska obveza čuvanja financijskih i drugih sličnih podataka. Ovisno o propisanim rokovima za čuvanje određenih podataka definira se i politika izrade rezervnih kopija. Rezervne kopije su također validan dokaz u sudskim procesima i zato je ponekad važno posjedovati periodične rezervne kopije kojima se može dokazati postojanje određenih informacija. Institucije često trebaju čuvati stare podatke kada rade na poslovima koji uključuju istraživanje i razvitak. Naime, tijekom razvitka nekog programa ili sl., koji može trajati i više mjeseci ili godina, moguće su situacije u kojima je potrebno odustati od odabranog smjera rada i vratiti se u neku staru fazu koja može biti unazad i nekoliko mjeseci.

3. Postupci u izradi rezervnih kopija

Svaki institucija sam za sebe treba donijeti odluku o tome koji su im podaci važni i za koje podatke je potrebno izrađivati rezervne kopije. U praksi se obično izrađuju rezervne kopije podataka generiranih aplikacijama dok se za same aplikacije u pravilu ne izrađuju rezervne kopije. Prilikom procesa izrade rezervnih kopija pažnju je potrebno posvetiti i smještaju podataka. Naime, podaci se mogu spremati na lokalnom računalu, na udaljenom računalu koji služi kao "data" server ili na nekim prenosnim medijima. Sam proces izrade rezervnih kopija odvija se u nekoliko faza:

Identificiranje podataka

Institucije trebaju odlučiti koji podaci su važni za instituciju ili korisnike. U praksi se kao najbolja praksa pokazala simulacija kojom se definiraju podaci koje je potrebno vratiti u slučaju kvara računala. Obično su to podaci koje generišu tekstualni i tabelarni programi, baze podataka i elektronička pošta. Mnogi od njih posjeduju mogućnost stvaranja jedinstvene backup datoteke iz koje je naknadno moguće vratiti podatke. Svakako je dobro posavjetovati se sa stručnjacima prilikom odlučivanja o tome što sve je potrebno staviti u sigurnosnu kopiju.

Određivanje prihvatljivog medija

S obzirom na prirodu sadržaja čija rezervna kopija se kreira, potrebno je odrediti i prikladan medij. Najčešće se odabire onaj medij koji je na jednostavan način podržan od računala, što znači da spremanje tekstualnih datoteka u obliku ispisanih stranica nije najpristupačniji oblik. Također Institucija može da radi bekap na više od jednog medaja radi povećanja redudandnosti navedenih bekapa.

Označavanje rezervnih kopija

Svi mediji koji sadrže rezervne kopije moraju biti jedinstveno i precizno označeni. Informacije koje su istaknute označavaju datum stvaranja kopije, broj kopije u nizu kopija i datum stvaranja. Preporučuje se održavanje zapisa o rezervnim kopijama u pisanom obliku gdje su navedene detaljnije informacije i reference. Također u slučaju korištenja softvera za kreiranje automatskog bekapa prepuručuje se da isti generiše navedene podatke o datumu broju rezervne kopije u elektroničkom obliku.

Čuvanje rezervnih kopija

Zapise o rezervnim kopijama potrebno je određeno vrijeme čuvati. U praksi se koriste zapisi stari jedan dan, sedmični, mjesečni, polumjesečni, polugodišnji i godišnji - ovisno o tome koja je količina podataka koju želimo sačuvati. Ovim postupkom se institucije osiguravaju od gubitka podataka i postupak je za korisnike potpuno transparentan. Sam postupak se u praksi najčešće naziva "generacijska rezervna kopija" koja može sadržavati i po nekoliko generacija zapisa rezervnih kopija.

Smještaj rezervnih kopija

Rezervne kopije se trebaju smjestiti zajedno sa pripadajućim zapisima na sigurnu lokaciju. U idealnoj situaciji se kopije drže na drugoj lokaciji dovoljno udaljenoj od originalne kako bi se izbjegle prirodne nepogode (vatra, poplava, …) i time omogućilo sigurno vraćanje podataka i odvijanje procesa poslovanja.

Testiranje rezervnih kopija

Nakon obavljanja procesa izrade rezervnih kopija potrebno je testirati vraćanje podataka s medija. Ovim postupkom se provjerava da li su svi podaci iz rezervne kopije ispravno vraćeni. Time se osigurava proces eventualnog vraćanja podataka u slučaju neke opasnosti. Institucije uvijek moraju posjedovati plan za najgori mogući scenarij kao što je npr. potpuni gubitak podataka na sustavu. Zbog toga treba postojati definiran postupak vraćanja

podataka na zamijenjeni hardver i uspostava prethodnog operativnog stanja. Nakon obavljene procedure vraćanja podataka često je potrebno obnoviti licence za pripadajuće aplikacije jer su postupci kojima se generiše lozinka često vezani uz konfiguraciju hardvera na računaru kao što je čvrsti disk, MAC adresa mrežne kartice ili ime servera. Postupak testiranja vraćanja podataka moguće je izvršiti u dvije faze:

- testiranje na postojećem računalu ili
- testiranje na računalu slične konfiguracije.

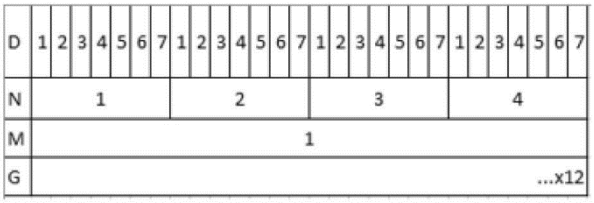
U postupcima izrade rezervnih kopija potrebno je obratiti pažnju na dodatne zahtjeve. Važno je gdje su podaci smješteni s obzirom na prirodu podataka i njihovu važnost za Instituciju. S obzirom na postojeće zakone o čuvanju podataka, ukoliko se radi o financijskim podacima ili slično, potrebno je čuvati kopije određeni broj godina. Ukoliko se pri korištenju aplikacija radi o ugovorima o korištenju u određenom periodu, potrebno je osigurati uništenje podataka nakon isteka istog ugovora. Pri izradi rezervnih kopija dobro je imati ovakvu listu za provjeru:

- da li su izrađene rezervne kopije svih podataka, operativnog sustava i pomoćnih programa adekvatno i sustavaski,
- postoje li zapisi o sadržaju rezervnih kopija i njihovom smještaju,
- postoje li zapisi o licenciranim aplikacijama,
- postoje li kopije medija ili zapisa spremljene na udaljenoj lokaciji,
- da li je povremeno proveden postupak vraćanja podataka sa medija,
- može li novi hardver čitati podatke sa postojećih medija,
- hoće li se zbog postojećih licenci aplikacija pokretati na novom hardveru i
- da li je proveden postupak potpunog vraćanja podataka u određenom vremenskom razdoblju.

U praksi se ne preporučuje korištenje samo jednog medija za potrebe arhiviranja. Rizik koji je povezan sa gubitkom podataka je manji ukoliko postoji više kopija istih podataka. Ukoliko se radi o optičkim medijima preporučuje se korištenje većeg broja jer je njihova cijena zanemariva s obzirom na štetu koja se može prouzročiti gubitkom podataka. Također, ukoliko se svakodnevno sprovodi izrada rezervnih kopija ili barem u nekim definiranim razdobljima, smanjuje se rizik gubitka podataka. Ukoliko se periodično sprovodi stvaranje rezervnih kopija uvijek postoji mogućnost vraćanja podataka. A u slučajevima kada se radi o većem kvaru kao što je npr. mehanički kvar na tvrdom disku, onda su najčešće uništeni svi podaci na njemu. Jedini način vraćanja podataka je iz rezervne kopije. Preporučuje se koristiti drugi medij od onog izvornog na kojem su podaci iz kojih su izrađene rezervne kopije. Postoji više metoda za stvaranje rezervnih kopija. Jedna od najčešćih je stvaranje vlastitih arhiva od strane Institucije. Pri tome se najčešće izrađuju rezervne kopije za one podatke koje Instituciji predstavljaju važan informacioni resurs. Izuzev takvih stvaranja arhiva određenih specifičnih informacija, često se koristi i stvaranje rezervnih kopija sustava baza podataka. Administratori u praksi sprovode stvaranje rezervnih kopija niza korisničkih direktorija. Pri tome administratori mogu raditi rezervne kopije svih podataka ili samo izmijenjenih tj. novih podataka. Pošto se kod izrade rezervne kopija najčešće koriste velike količine datoteka, u pravilu se one kompresuju odgovarajućim sustavskim alatima.

4. Vrste rezervnih kopija

Stvaranje rezervne kopije (backup) ne utječe na stupanj 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 sustava - 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 sustava - 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 preduvjeti 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 sustava baza podataka prije izrade rezervnih kopija - ukoliko se radi o povratku podataka sustava koji je prethodno uništen onda je rezervna kopija

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.