Na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i Poglavlja 3. Odluke o usvajanju Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017 - 2022. godine ("Službeni glasnik BiH" broj 38/17), na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na 54. sjednici, održanoj 28. jula 2022. godine, donijelo je

ODLUKU
O USVAJANJU SMJERNICA IZ POLITIKE UPRAVLJANJA INFORMACIONOM SIGURNOŠĆU U INSTITUCIJAMA BOSNE I HERCEGOVINE ZA PERIOD OD 2017 - 2022. GODINE

Član 1.
(Predmet Odluke)

(1) Ovom odlukom usvajaju se smjernice iz Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period 2017-2022. godine, i to:
   a) Smjernice o korisničkim računima i pravima pristupa,
   b) Smjernice o sigurnosnim kopijama,
   c) Smjernice o zaposlenju i prekidu zaposlenja i
   d) Smjernice za izradu metodologije i procjene rizika.

(2) Smjernice iz stava (1) ovog člana su prilozi ove odluke i čine njen dio.

Član 2.
(Praćenje realiziranja Odluke)

Za praćenje realiziranja ove odluke zadužuju se Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine.

Član 3.
(Stupanje na snagu)

Ova odluka stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 93/22
28. jula 2022. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Dr. **Zoran Tegeltija**, s. r.

SMJERNICE
O KORISNIČKIM RAČUNIMA I PRAVIMA PRISTUPA

1. Svrha

Svrha dokumenta je osigurati kontrolu nad otvaranjem, izmjenom, zamrzavanjem i zatvaranjem korisničkih računa u informacionom sistemu, u cilju sprječavanja zastarjelih, redundantnih i korisničkih računa otvorenih na neispravan način. Pravo pristupa vrijednostima informacionog sistema jedna je od najkritičnijih tačaka sigurnosti. Zbog naizgled komplikovanog procesa dodjeljivanja prava pristupa, korisnicima se često dodjeljuju "uobičajena" prava, koja su najčešće puno veća od potrebnih. Što veća prava pristupa korisnik posjeduje, veće su mogućnosti da slučajnim ili namjernim radnjama ugrozi sigurnost informacionog sistema.

Obavljanje osnovne djelatnosti institucije povezano je sa rukovanjem podacima koji se nalaze u informacionom sistemu. Zbog toga je neophodno da zaposlenima bude omogućen pristup različitim podacima u okviru sistema. Međutim, pristup zaposlenih ovim podacima treba da bude usaglašen sa procesnom strukturom organizacionog sistema. Zaposlenima je potrebno osigurati pristup samo onim podacima i dijelovima informacionog sistema koji su im potrebni za realiziranje aktivnosti za koje su nadležni, a ne kompletnom informacionom sistemu. Iz tog razloga potrebno je prilagoditi prava pristupa informacionom sistemu opisima poslova iz važećeg pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mjesta. Takođe, ukoliko je institucija implementirala sistem upravljanja kvalitetom, potrebno je usaglasiti prava pristupa zaposlenih sa njihovim ulogama u procedurama.

Neophodno je osigurati da je pristup informacionom sistemu omogućen samo onima koji za to imaju pravni osnov, uz odgovarajuću evidenciju svakog pristupa i eventualnog ažuriranja. Zbog toga je neophodno implementirati sistem korisničkih uloga (rola), kojim će bit definirani odgovarajući nivoi prava pristupa prikupljenim podacima u informacionom sistemu. Sistem uloga mora precizno da definira prvo, kojim podacima korisnik kome je dodeljena određena uloga uopće može da pristupi, a zatim i na koji sve način može da ih obrađuje. Institucija treba da uspostavi mehanizam kreiranja i ukidanja korisničkih naloga, te da vodi evidenciju svih korisničkih naloga u okviru informacionog sistema, kako aktivnim, tako i ukinutim nalozima. Institucija propisuje procedure dodjele i ukidanja naloga, te provjere adekvatnog nivoa pristupa i dodjele jedinstvene identifikacione oznake svakog naloga.

2. Pristup informacionom sistemu

Pristup informacionom sistemu se bazira na podacima za autentifikaciju, kao što su lozinke, kriptografski ključevi, tokeni, smart kartice, pin kod i 2FA aplikacije. Distribuciju i čuvanje ovih podataka regulira institucija, kako bi se spriječile sigurnosne prijetnje poput otkrivanja podataka za autentifikaciju zaposlenih (kolegama, porodici ili trećim licima) ili zapisivanje šifre u notesu ili na naljepnici.

Osnovno pravilo pri kreiranju lozinke jeste izbjegavanje podataka iz privatnog života kao što su datum rođenja, ime kućnog ljubimca, omiljeno mjesto i slično, kao i bilo kakve riječi prirodnog jezika. Klasične metode probijanja lozinke danas podrazumjevaju automatizovane pretrage po spiskovima riječi (dictionary attack), a koji mogu obuhvatati na milion pojmova iz različitih jezika. Šifra od 12 brojeva ima 1.000.000.000.000 kombinacija, preciznije 10^12, šifra od 12 znakova koja sadrži cifre, velika i mala slova i specijalne karaktere ima 475.920.310.000.000.000.000.000 kombinacija, imajući u vidu da je ukupan broj svih alfanumeričkih i specijalnih karaktera 94. Šifra od 12 brojeva ili manje, može se razbiti za manje od sat vremena. Sa tehnologijom u slobodnoj prodaji, potrebno je oko pet miliona godina da bi se probila šifra iste dužine koja, osim brojeva, sadrži velika i mala slova i specijalne karaktere. Kod informacijskih sistema predviđenih za veliki broj korisnika, administratori uobičajeno automatski generiraju inicijalne lozinke. Nerijetko, lozinke se korisnicima šalju elektroničkom poštom, što nije siguran kanal komunikacije. Da bi se eliminirao rizik od presretanja poruke koja sadrži lozinke, ne treba ih slati elektronskom poštom. Prilikom razvoja informacijskih sistema, sistem treba postaviti tako da administrator kreira naloge samo sa korisničkim imenima, a da se korisnicima prepusti mogućnost da sami postave lozinku prilikom prve prijave u sistem, koristeći adekvatan digitalni certifikat ili token kako bi potvrdili svoj identitet. Sve lozinke se čuvaju u bazama ili datotekama koje se nalaze na serverima. Takve baze se moraju enkriptovati, tako da ni sam sistem administrator ne može da ih pročita. Iz praktičnih razloga administratoru treba ostaviti mogućnost da resetuje lozinke.

Jak sistem autentifikacije podrazumijeva više od jednog zahtjeva prilikom pristupa - ne samo korisničku lozinku, već i kvalifikacijski certifikat. Dvostruka provjera podrazumjeva zahtjev za potvrdu identiteta lozinkom i certifikatom. Prednost korištenja ovakvog sistema nalazi se u dodatnoj prepreci, u slučaju da je lozinka ukradena. Pored informacijskih sistema, dvostruku provjeru bi trebalo koristiti i za ostale naloge zaposlenih (elektronska pošta, nalozi na društvenim mrežama, finansijske

aplikacije i slično). Digitalni certifikati se mogu primjeniti na više načina, ali je najjednostavnije distribuirati ih u obliku smart kartica ili USB tokena. Ukoliko se koriste certifikati u obliku kartica, za njihovu uporabu neophodni su odgovarajući čitači, dok se USB tokeni koriste preko postojećeg USB ulaza na računaru.

Log je registar svih događaja u okviru jednog sistema, odnosno svih aktivnosti korisnika - od prijave, preko unosa podataka do njihovih promjena, štampanja, brisanja i drugih postupaka. Logovi mogu biljažiti aktivnosti u različitim dijelovima sistema. Osnovni oblik je pristupni log (access log), a njegovu strukturu, kao i strukturu svih logova, podešava administrator informacionog sistema. Prilikom podešavanja treba imati na umu da log treba da bude dovoljno detaljan da omogući jasno utvrđivanje zloupotreba (neovlašteni pristupi i druge aktivnosti) ali da ne bude previše kompleksan za analizu ili skladištenje. Svaki pristupni log bi trebalo da sadrži konkretne informacije:

- korisnik koji je pristupio bazi podataka;
- datum i vrijeme pristupa;
- IP adresa sa koje je pristupljeno bazi podataka;
- resurs kome je pristupljeno;
- vrsta obrade podatka (pregled/unos/izmjena/brisanje/ izvoz/štampa).

Logove je potrebno čuvati najmanje godinu dana, a ukoliko postoji mogućnost i duže. Pored toga, informacioni sistem je neophodno projektovati tako da se za svaki njegov segment (aplikacije, podaci, ostali resursi) od trenutka nastanka, pa sve do trenutka brisanja, pamte sve izmjene. Dakle, prilikom svake izmjene potrebno je čuvati konkretne informacije:

- korisnik koji je izvršio izmjenu;
- vrsta izmjene (unos, izmjena, brisanje podataka, nadogradnja softvera, instaliranje novih aplikacija itd);
- datum i vrijeme izmjene;
- vrijednost podatka prije izmjene.

Institucija treba da nadgleda razvojni proces kako bi imala saznanja o tome da li se naloženi standardi implementiraju u sistem. Kako bi to bilo moguće, institucija, zajedno sa trećim licem koje razvija informacioni sistem, treba da dokumentuje, sistematizuje i kvalificira sve vrste sigurnosnih zahtjeva i standarda koje informacioni sistem treba da sadrži, još prije početka projektovanja. Kasnije, tokom naprednijih faza razvoja, implementiranje ovih standarda također treba dokumentovati.

Dodjela prava pristupa:

- svaki korisnik prilikom otvaranja korisničkog računa, zavisno kojoj skupini korisnika pripada, ima minimalna, tzv. **osnovna** prava,
- svakom korisniku moguće je proširiti osnovna prava ukoliko za tim postoji potreba,
- dodatna prava pristupa može dodijeliti odgovorna osoba (zaposlenik institucije koji ima pravo dodjele prava pristupa),
- za pravo pristupa osjetljivim i tajnim podacima, korisnik je dužan potpisati izjavu o pridržavanju pravila sigurnosti definiranih Politikom upravljanja informacionom sigurnošću u institucijama BiH za period 2017.-2022. godine,
- pravo pristupa trećoj strani dodjeljuje odgovorna osoba; prije dodjeljivanja prava pristupa treća strana je dužna potpisati izjavu o pridržavanju pravila sigurnosti definiranih Politikom upravljanja informacionom sigurnošću u institucijama BiH za razdoblje 2017.-2022. godine,
- ukoliko treća strana zahtjeva pristup osjetljivim ili tajnim podacima, potrebna je suglasnost rukovodioca institucije,
- sva dodijeljena prava pristupa moraju bit jasno dokumentovana,
- potrebno je omogućiti uvid u koja prava pristupa ima pojedini korisnik ili skupina korisnika,
- potrebno je omogućit uvid ko sve ima prava nad pojedinim resursom, s mogućnošću filtriranja rezultata.

3. Evidencija zahtjeva

Pravovremeno zatvaranje korisničkog računa važna je karika u sigurnosti informacijskih sistema. Ukoliko "nevažeći" korisnički račun nije zatvoren, korisniku je otvoren put obavljanju zlonamjernih radnji. Kako bi proces otvaranja i zatvaranja korisničkih računa bio pravovremeno i kvalitetno obavljen, potrebno je definirati načine komunikacije između podnosioca zahtjeva i administratora sistema, 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 podnosilac zahtjeva pristupio aplikaciji, potrebno je obavit provjeru autentičnosti i autorizaciju,
- podnosilac zahtjeva na svom računaru 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 podnosioca 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 sistema na osnovu dobijenih podataka otvara korisnički račun.

trećoj strani:

- za otvaranje korisničkog računa trećoj strani potrebna je saglasnost ovlaštenog lica (administrator informacionog sistema) institucije,
- ovlašteno lice je glavno i odgovorno lice u saradnji sa trećom stranom i kao takvo ima prava davanja saglasnosti za otvaranje korisničkih računa,
- kod otvaranja korisničkog računa za treću stranu potrebno je odrediti vremenski period koliko će račun biti aktivan.

5. Zamrzavanje korisničkog računa

U slučaju dužeg planiranog nekorištenja informacionog sistema (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 periodu kako je definirano politikom. Također se zaobilaze sve druge sigurnosne kontrole od strane sistema za koje je potrebna interakcija korisnika. Zamrznuti korisnički račun moguće je vratiti u upotrebu (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 dokumentovanja i na osnovu 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 perioda 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 redovno pregledavati zaprimljene zahtjeve za zatvaranjem računa te ih pravovremeno zatvoriti,
- ukoliko postoji potreba, korisniku je moguće prijevremeno zatvoriti korisnički račun bez prethodne obavijesti na osnovu pisanog zahtjeva ovlašćene osobe institucije.

7. ZAKLJUČAK

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

SMJERNICE O SIGURNOSNIM KOPIJAMA

1. Svrha

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 računarske sisteme, 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 zavisno u informacionim tehnologijama. Pred informatičke podatke se postavljaju visoki kriteriji zaštite koji su jednaki ili čak veći od kriterija zaštite zapisa u poslovnim knjigama. Informacioni sistem 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 osnovna pretpostavka koja se postavlja pred sistem koji mora zadovoljavati rezervne zahtjeve. Postupak izrade rezervnih kopija zajedno sa postupkom povratka podataka, predstavlja osnovnu proceduru kojom se sistem štiti od gubitka podataka i osigurava brza obnova podataka u slučaju nepravilnosti u radu sistema kao što su npr. prekidi u radu računalnog sistema, 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 informacionom sistemu institucija, rade se u svrhu osiguranja podataka od vitalnog značaja za normalno funkcioniranje institucije. Zadatak rezervnih kopija je osigurati oporavak sistema na osnovu 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 sistema.

Politika rezervnih kopija ima namjeru da jedinstveno u cijeloj instituciji definira načine postepena 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 sistema. Svaki poremećaj u radu sistema se odražava u prestanku rada istog. Posljedice nemogućnosti odvijanja poslovnih procesa se zavisno o važnosti tih procesa, mjere u različitim iznosima (od hiljadu do milion). 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 informacionog sistema usljed nepredviđenih okolnosti, čine uspješnim poslovanje institucije, dok se u slučajevima neispunjena tih uvjeta uzrokuju uz finansijske 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 računara 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 finansijskih i drugih sličnih podataka. Zavisno 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 razvoj. Naime, tokom razvoja nekog programa ili sl., koji može