SLUŽBENI GLASNIK BOSNE I HERCEGOVINE
Izdanje na hrvatskom, srpskom i bosanskom jeziku

СЛУЖБЕНИ ГЛАСНИК БОСНЕ И ХЕРЦЕГОВИНЕ
Издање на хрватском, српском и босанском језику

Godina XXVI
Utorak, 13. rujna/septembra 2022. godine

Broj/Број
62

Година XXVI
Уторак, 13. септембра 2022. године

ISSN 1512-7494 - hrvatski jezik
ISSN 1512-7508 - srpski jezik
ISSN 1512-7486 - bosanski jezik

VIJEĆE MINISTARA BOSNE I HERCEGOVINE

607

Na temelju članka 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 informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 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. srpnja 2022. godine, donijelo je

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

Članak 1.
(Predmet Odluke)

(1) Ovom odlukom usvajaju se smjernice iz Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 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 stavka (1) ovog članka su privici ove odluke i čine njen dio.

Članak 2.
(Praćenje realiziranja Odluke)

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

Članak 3.
(Stupanje na snagu)

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

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

Predsjedatelj
Vijeća ministara BiH
Dr. **Zoran Tegeltija**, v. r.

SMJERNICE
O KORISNIČKIM RAČUNIMA I PRAVIMA PRISTUPA

1. Suština

Suština dokumenta je osigurati kontrolu nad otvaranjem, izmjenom, zamrzavanjem i zatvaranjem korisničkih računa u informacijskom sustavu, u cilju sprječavanja zastarjelih, redundantnih i korisničkih računa otvorenih na neispravan način. Pravo pristupa vrijednostima informacijskog sustava jedna je od najkritičnijih točki 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 informacijskog sustava.

Obavljanje temeljne djelatnosti institucije povezano je sa rukovanjem podacima koji se nalaze u informacijskom sustavu. Zbog toga je neophodno da zaposlenima bude omogućen pristup različitim podacima u okviru sustava. Međutim, pristup zaposlenih ovim podacima treba da bude usuglašen sa procesnom strukturom organizacijskog sustava. Zaposlenima je potrebno osigurati pristup samo onim podacima i dijelovima informacijskog sustava koji su im potrebni za realiziranje aktivnosti za koje su nadležni, a ne kompletnom informacijskom sustavu. Iz tog razloga potrebno je prilagoditi prava pristupa informacijskom sustavu opisima poslova iz važećeg pravilnika o unutrašnjoj organizaciji i sustavatizaciji radnih mjesta. Također, ukoliko je institucija implementirala sustav

upravljanja kvalitetom, potrebno je usuglasiti prava pristupa zaposlenih sa njihovim ulogama u procedurama.

Neophodno je osigurati da je pristup informacijskom sustavu omogućen samo onima koji za to imaju pravni temelj, uz odgovarajuću evidenciju svakog pristupa i eventualnog ažuriranja. Zbog toga je neophodno implementirati sustav korisničkih uloga (rola), kojim će bit definirane odgovarajuće razine prava pristupa prikupljenim podacima u informacijskom sustavu. Sustav 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 informacijskog sustava, kako aktivnim, tako i ukinutim nalozima. Institucija propisuje procedure dodjele i ukidanja naloga, te provjere adekvatne razine pristupa i dodjele jedinstvene identifikacione oznake svakog naloga.

2. Pristup informacijskom sustavu

Pristup informacijskom sustavu 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.

Temeljno 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 milijune 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 čas vremena. Sa tehnologijom u slobodnoj prodaji, potrebno je oko pet milijuna godina da bi se probila šifra iste dužine koja, izuzev brojeva, sadrži velika i mala slova i specijalne karaktere. Kod informacijskih sustava 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 elektroničkom poštom. Prilikom razvitka informacijskih sustava, sustav 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 sustav, 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 sustav administrator ne može da ih pročita. Iz praktičnih razloga administratoru treba ostaviti mogućnost da resetuje lozinke.

Jak sustav 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 sustava nalazi se u dodatnoj prepreci, u slučaju da je lozinka ukradena. Pored informacijskih sustava, dvostruku provjeru bi trebalo koristiti i za ostale naloge zaposlenih (elektronska pošta, nalozi na društvenim mrežama, financijske 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 sustava, odnosno svih aktivnosti korisnika - od prijave, preko unosa podataka do njihovih promjena, štampanja, brisanja i drugih postupaka. Logovi mogu biljažiti aktivnosti u različitim dijelovima sustava. Temeljni oblik je pristupni log (access log), a njegovu strukturu, kao i strukturu svih logova, podešava administrator informacijskog sustava. Prilikom podešavanja treba imati na umu da log treba da bude dovoljno detaljan da omogući jasno utvrđivanje zlouporaba (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 sustav 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 sustav. Kako bi to bilo moguće, institucija, zajedno sa trećim licem koje razvija informacioni sustav, treba da dokumentuje, sustavatizuje i kvalificira sve vrste sigurnosnih zahtjeva i standarda koje informacioni sustav treba da sadrži, još prije početka projektovanja. Kasnije, tokom naprednijih faza razvitka, implementiranje ovih standarda također treba dokumentovati.

Dodjela prava pristupa:

- svaki korisnik prilikom otvaranja korisničkog računa, ovisno kojoj skupini korisnika pripada, ima minimalna, tzv. temeljna prava,
- svakom korisniku moguće je proširiti temeljna 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 informacijskom sigurnošću u institucijama BiH za razdoblje 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 informacijskom sigurnošću u institucijama BiH za razdoblje 2017.-2022. godine,
- ukoliko treća strana zahtjeva pristup osjetljivim ili tajnim podacima, potrebna je suglasnost rukovoditelja 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 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.