На основу члана 26. став (1) тачка б) алинеја 8) и став (2) Закона о платама и накнадама у институцијама Босне и Херцеговине ("Службени гласник БиХ", бр. 50/08, 35/09, 75/09, 32/12, 42/12, 50/12, 32/13, 87/13, 75/15, 88/15, 16/16, 94/16, 72/17, 25/18, 60/18, 32/20, 65/20 и 59/22), члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07, 24/08) и члана 6. став (1) Одлуке о критеријима за утврђивање додатка на плату на основу обављања сложених информатичко-апликацијских послова у институцијама Босне и Херцеговине ("Службени гласник БиХ", број 38/09), Савјет министара Босне и Херцеговине, на приједлог Агенције за јавне набавке Босне и Херцеговине, на 3. сједници одржаној 23.2.2023. године, донио је

ОДЛУКУ
О ДОДАТКУ НА ПЛАТУ НА ОСНОВУ ОБАВЉАЊА СЛОЖЕНИХ ИНФОРМАТИЧКО-АПЛИКАЦИЈСКИХ ПОСЛОВА У АГЕНЦИЈИ ЗА ЈАВНЕ НАБАВКЕ БОСНЕ И ХЕРЦЕГОВИНЕ

Члан 1.
(Предмет Одлуке)

Овом одлуком утврђује се додатак на плату за упослене са високом школском спремом на основу посебне стручне оспособљености и обављања сложених информатичко-апликацијских послова у Агенцији за јавне набавке Босне и Херцеговине.

Члан 2.
(Проценат додатка на плату)

Проценат додатка на плату за обављање сложених информатичко-апликацијских послова, у зависности од степена њихове сложености и посебности за упослене у Агенцији за јавне набавке Босне и Херцеговине, дат је у сљедећој табели:

Р. бр.	Име и презиме државног службеника/Радно мјесто	Сложени информатичко- апликацијски послови и посебности	Број освојених бодова		Проценат додатка на плату
1.	**Таида Бајрамовић** Помоћница директора за информационе технологије, финансијске и опште послове	Управљање и пројектовање процеса и управљачких апликација	7	20	20%
		Пројектовање и развој процеса и управљачких апликација	6		
		Тестирање процеса и управљачких апликација	3		
		Обука корисника	2		
		Одржавање процеса и управљачких апликација	2		
2.	**Дарио Кихли,** Шеф Групе за информационе технологије	Управљање и пројектовање процеса и управљачких апликација	6	20	20%
		Пројектовање и развој процеса и управљачких апликација	7		
		Тестирање процеса и управљачких апликација	3		
		Обука корисника	2		
		Одржавање процеса и управљачких апликација	2		
3.	**Кемал Мухамедовић,** Виши стручни сарадник за администрацију информационих система	Управљање и пројектовање процеса и управљачких апликација	4	17	17%
		Пројектовање и развој процеса и управљачких апликација	4		
		Тестирање процеса и управљачких апликација	4		
		Обука корисника	3		
		Одржавање процеса и управљачких апликација	2		

Проценат додатка на плату обрачунава се од износа основне плате упосленог.

Члан 3.
(Обезбјеђење средстава)

За провођење ове Одлуке обезбијеђена су средства у буџету Агенције за јавне набавке Босне и Херцеговине, те нису потребна додатна средства.

Члан 4.
(Надлежност за реализацију)

За реализацију ове Одлуке задужује се Агенција за јавне набавке Босне и Херцеговине.

Члан 5.
(Престанак важења)

Ступањем на снагу ове Одлуке престаје да важи Одлука о додатку на плату на основу обављања сложених информатичко-апликацијских послова у Агенцији за јавне набавке Босне и Херцеговине ("Службени гласник БиХ", број 38/22).

Члан 6.
(Ступање на снагу)

Ова Одлука ступа на снагу даном доношења и објављује се у "Службеном гласнику БиХ".

СМ број 68/23
23. фебруара 2023. године
Сарајево

Предсједавајућа
Савјета министара БиХ
Борјана Кришто, с. р.

384

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 2017. - 2022. godine ("Službeni glasnik BiH", broj 38/17), na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine, na 3. sjednici, održanoj 23. februara 2023. godine, donijelo je

ODLUKU
O USVAJANJU SMJERNICA O KONTROLI PRISTUPA I BILJEŽENJU DOGAĐAJA, SMJERNICA O FIZIČKOJ ZAŠTITI INFORMACIJA I SMJERNICA O KORIŠTENJU PRIJENOSNIH UREĐAJA U INSTITUCIJAMA BOSNE I HERCEGOVINE

Član 1.
(Predmet Odluke)

Ovom Odlukom usvajaju se Smjernice o kontroli pristupa i bilježenju događaja, Smjernice o fizičkoj zaštiti informacija i Smjernice o korištenju prijenosnih uređaja u institucijama Bosne i Hercegovine, koje su sastavni dio ove Odluke.

Član 2.
(Praćenje realiziranja)

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 71/23
23. februara 2023. godine
Sarajevo

Predsjedavajuća
Vijeća ministara BiH
Borjana Krišto, s. r.

SMJERNICE
O KONTROLI PRISTUPA I BILJEŽENJU DOGAĐAJA

1. SVRHA

Zasigurno jedan od važnijih uzroka problema sigurnosti predstavljaju ovlašteni korisnici. Oni svojim postupcima, bilo slučajnim ili namjernim, ugrožavaju sigurnost sistema u velikoj mjeri.

Neki od uzroka sigurnosnih incidenata koje izazovu ovlašteni korisnici su:

- znatiželja,
- dokazivanje,
- krađa identiteta od zlonamjernog lica,
- slučajni postupci (needuciranost korisnika),
- prikupljanje podataka u zlonamjerne svrhe itd.

Navedene prijetnje sigurnosti informacionim sistemima razlog su zbog kojih postoji potreba za kontrolom pristupa, tj. zabranom pristupa onim resursima sistema kojima korisnik nema potrebe pristupati.

Osim kontrola pristupa, u svrhu pravovremenog uočavanja odstupanja od politike pristupa i pružanja dokaza u slučaju sigurnosnog incidenta, u sistem je potrebno uvesti sigurnosnu kontrolu bilježenje događaja (nadgledanje).

2. KONTROLA PRISTUPA

2.1 Prava pristupa u skladu sa potrebama

Pristup informacionim resursima potrebno je odobriti ukoliko zaposleni ili treća strana ima realnu potrebu za pristup traženim resursima. Zahtjev za dodjelu prava pristupa na osnovu kojeg je donesena odluka o dodjeli prava pristupa treba biti dokumentiran.

Dokument treba sadržavati:

- identifikator inicijatora zahtjeva,
- identifikator lica kome je potrebno dodijeliti prava pristupa,
- opis zahtjeva,
- datum podnošenja zahtjeva,
- ukratko politiku sigurnosti traženog resursa - klasifikacija resursa, da li postoje zakonske i ugovorne obaveze i sl.,
- vrijeme trajanja prava pristupa - period u kojem će dodijeljena prava vrijediti (nakon njegovog isteka potrebno je ponovno predati zahtjev za dodjelu prava pristupa),
- odobritelja zahtjeva (ko je zahtjev pregledao i odobrio).

2.2 Upravljanje pristupom korisnika

S ciljem kvalitetne kontrole pristupa informacionim sistemima i servisima potrebno je uspostaviti odgovarajuće procedure. Te procedure trebaju obuhvatiti sve stadije u životnom ciklusu korisničkog pristupa, od početne registracije novog korisnika do konačnog odjavljivanja korisnika kojem više nije potreban pristup informacionim resursima. Posebnu pažnju treba posvetiti kontroli dodjele privilegiranih prava pristupa.

2.3. Registracija korisnika

Da bi pojedinom korisniku bila dodijeljena prava pristupa informacionom sistemu i servisima potrebno je definirati postupke registracije u i odjave iz sistema. Pristup treba kontrolirati kroz proces registracije korisnika koji uključuje:

- korićenje korisničkih imena koje je dodijelio administrator sistema ili za to odgovorno lice,
- korisnička imena trebaju biti jedinstvena kako bi se korisnici mogli povezati sa njihovim aktivnostima,
- provjeru autentifikacije korisnika preko lozinke,
- provjeru prava pristupa za korištenje informacionih resursa prema korisničkom imenu,
- zamrzavanje korisnikovog računa u slučaju planiranog dužeg izostanka sa posla,
- trenutno ukidanje svih prava korisniku ukoliko on prestane biti zaposlen ili dođe do raskida ugovara s trećom stranom.

2.4. Upravljanje korisničkim lozinkama

Lozinke služe kako bi se putem mreže provjerilo da li je korisnik koji se predstavlja korisničkom lozinkom upravo taj korisnik. Stoga je potrebno sigurnosnim mehanizmima omogućiti maksimalnu sigurnost lozinki u smislu njihove tajnosti. Osim politike sigurnosti namijenjene korisnicima u kojoj se jasno definira na koji način rukovati lozinkama, lice odgovorno za sigurnost dužno je držati se sljedećih pravila prilikom raspodjele lozinki:

- korisnici su dužni prilikom preuzimanja lozinki potpisati izjavu u kojoj se obavezuju rukovati lozinkama prema pravilima definiranim u Pravilniku o informatičkoj sigurnosti radnog mjesta,
- prilikom dodjele lozinke korisnicima prvo im se dodjeljuje privremena lozinka koju u što kraćem roku, pri prvoj prijavi na sistem, moraju promijeniti, pri čemu sistem treba podesiti tako da ne dozvoljava prijavu privremenom lozinkom,
- lozinke se korisnicima smiju proslijediti isključivo na siguran način, nikako ne elektronskom poštom, telefonom ili preko treće strane,
- lozinke se ne smiju pohranjivati na računaru u nezaštićenom obliku.

2.5. Odgovornost korisnika

2.5.1.Upotreba lozinki

Od korisnika je potrebno zahtijevati da pri odabiru i rukovanju lozinkama slijede sigurnosne upute definirane Pravilnikom o informatičkoj sigurnosti radnog mjesta. Korisnike treba savjetovati da:

- čuvaju povjerljivost lozinki,
- ne bilježe lozinke na papire,
- lozinke mijenjaju isključivo nakon prijave na sistem,

- biraju kvalitetne lozinke, dugačke minimalno 6 znakova, maksimalno 10,
- lozinke budu lako pamtljive,
- lozinke sadrže brojeve i slova, po potrebi i specijalne znakove,
- lozinke ne predstavljaju imena, prezimena, gradove, datume rođenja, nadimke i sl. riječi,
- redovno mijenjaju lozinke,
- ne koriste već upotrebljavane lozinke,
- ne koriste lozinke koje već koriste na drugim sistemima.

2.5.2. Nadgledana korisnička oprema

Korisnike je potrebno educirati o potrebi zaštite opreme kada nisu u njenoj blizini. Mnogi korisnici nisu ni svjesni mogućnosti zloupotrebe računara, mobitela, ali i drugih komunikacionih uređaja ukoliko na kratko vrijeme ostanu bez nadzora. Svaki korisnik mora biti svjestan svoje odgovornosti, sigurnosnih zahtjeva i postupaka za zaštitu nenadgledane opreme.

Korisnike treba savjetovati da:

- se odjave sa sistema ili zaštite računar posebnim programima (npr. čuvar ekrana) ukoliko računar ostavljaju bez nadzora,
- računar odjave sa sistema nakon završetka posla,
- ukoliko je potrebno, računare i drugu opremu zaključaju kada je ne koriste.

2.5.3. Kontrola pristupa mreži

Svi interni i eksterni mrežni servisi moraju biti kontrolirani u svrhu zaštite resursa od korisnika koji imaju pristup mreži i mrežnim resursima. Kontrola pristupa mreži treba sadržavati sljedeće kontrole:

- korisnici smiju pristupiti samo onim mrežnim servisima za koje imaju definirane eksplicitne ovlasti,
- kontrole upravljanja i procedure za zaštitu pristupa mreži trebaju biti jasno definirane,
- u svrhu smanjenja rizika neautoriziranog pristupa potrebno je odrediti "propisani put",
- korisnike koji pristupaju resursima sa udaljenih lokacija potrebno je autentificirati posebnim metodama koje osiguravaju odgovarajući nivo zaštite.

2.5.4.Kontrola pristupa operativnom sistemu

Pristup korisnika operativnim sistemima potrebno je kontrolirati putem ugrađenih mehanizama s ciljem sprečavanja neovlaštenog pristupa. Mehanizam kontrole pristupa operativnom sistemu treba sadržavati:

- prilikom prijave na sistem korisnik treba unijeti svoje korisničko ime i lozinku, na osnovu čega se radi provjera identiteta,
- provjeru da li je period valjanosti lozinke istekao; ukoliko jeste (svaka 3 mjeseca), obavijestiti korisnika da je potrebno napraviti izmjenu,
- sistem mora bilježiti pristup informacionom sistemu i pokušaje pristupa,
- rad korisnika na klijentskim radnim stanicama treba dodatno kontrolirati na način da se prati vrijeme neaktivnosti; ukoliko je klijentska radna stanica neaktivan duže od 10 minuta, treba napraviti automatsku odjavu sa sistema,
- ukoliko je potrebno, kontrolu sa koje se lokacije pristupa sistemu,
- broj mogućih prijava na sistem treba ograničiti na 3 prijave.

3. ZAKLJUČAK

U skladu sa Politikom i Smjernicama o kontroli pristupa i bilježenju događaja preporučuje se institucijama BiH da donesu svoj interni akt u kojem će definirati **pravilo/proceduru o kontroli pristupa i bilježenju događaja.**

LITERATURA:

1. Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija
4. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", br. 54/05 i 12/09)

SMJERNICE
O FIZIČKOJ ZAŠTITI INFORMACIJA

1. SVRHA

Informacioni sistemi često su osnova poslovanja institucije koji sadrže vrlo važne informacije iz nadležnosti i ovlaštenja institucije. Narušavanje njihove sigurnosti može voditi do otkrivanja osjetljivih podataka. Jedan od aspekata sigurnosti informacionog sistema predstavlja i fizička sigurnost, tj. skup mjera koje sprečavaju nedozvoljen fizički pristup informacijama i resursima. Prijetnje fizičkoj sigurnosti dolaze od prirodnih nepogoda poput poplava i potresa te ljudskih ranjivosti poput neposlušnosti, namjere za sabotažom ili krađom. Također, postoje neke prijetnje koje su rezultat nepredviđenih okolnosti kao što je požar ili neke vrste kvarova na raznim sistemima. Kako bi se smanjila šteta nakon pojavljivanja neke od spomenutih prijetnji, potrebno je uvesti adekvatne mjere zaštite. Pod tim se podrazumijeva osiguravanje okoline i prostorija objekata te provođenje kontrole pristupa. Također, potrebno je uvesti zaštitu opreme i uređaja putem dostupnih tehnologija. Razni sistemi razvijeni su za uspostavljanje i poboljšanje fizičke sigurnosti. Neki od njih su alarmni sistemi te sistemi za nadzor, kontrolu pristupa ili zaključavanje vrijednih uređaja.

Svrha fizičke zaštite informacionog sistema je preventivnim metodama osigurati zaštitu sistema od namjernih ili slučajnih destruktivnih radnji. Fizičkom zaštitom želi se:

- spriječiti neovlašten pristup,
- spriječiti ometanje poslovnih prostorija,
- spriječiti nepotreban pristup korisnika osjetljivoj opremi,
- osigurati zaštita opreme od prirodnih utjecaja,
- osigurati sigurnost instalacija,
- osigurati održavanje opreme.

2. PODRUČJE FIZIČKE ZAŠTITE

Fizička sigurnost opisuje mjere koje sprečavaju neovlašten pristup resursima ili informacijama pohranjenim na fizičkim medijima. Radi se o skupu smjernica za dizajniranje strukture koja je otporna na razne zlonamjerne radnje, a može uključivati jednostavnu primjenu zaključavanja vrata ili zapošljavanje osiguranja. Fizička sigurnost je najosnovniji aspekt zaštite, a obuhvaća kontrolu zaštite prostorija, postrojenja, zgrada i druge imovine. Primjena fizičke sigurnosti podrazumijeva proces upotrebe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. U osnovi, fizička sigurnost odnosi se na sprečavanje oštećenja bilo kojeg dijela nekretnina, postrojenja, ureda, objekata ili zgrada. Također, ona doprinosi zaštiti ljudi i informacija, iako se na te grupe primjenjuju i druge sofisticirane mjere zaštite. Prema tome, fizička sigurnost čini dio sveukupne sigurnosti informacionog sistema kao osnove na kojoj su sve sigurnosne mjere bazirane. Mjere koje uključuje fizička sigurnost, a služe za zaštitu osoblja, opreme i imovine, mogu se podijeliti na:

1. *pasivne mjere* – efektivna upotreba arhitekture, okoline i osvjetljenja za postizanje bolje sigurnosti kroz olakšanu detekciju upada ili potencijalnih prijetnji,
2. *aktivne mjere* – uključuju upotrebu poznatih sistema i tehnika dizajniranih za detekciju i reakciju na prijetnje.

Da bi se osigurala fizička zaštita informacionog sistema, institucija je dužna provesti sljedeće tačke sigurnosti:

- potrebno je jasno definirati i dokumentirati ko je ovlašten pristupiti pojedinim prostorijama pod fizičkom zaštitom,
- kontrolnim mehanizmima potrebno je spriječiti svaki pokušaj neovlaštenog pristupa; ulaze u prostorije koje sadrže servere, medije za pohranu podataka i ostale osjetljive resurse potrebno je zaštititi metodama kontrole ulaska (kartice, ključ i sl.),
- vrata na ulazima u zaštićena područja moraju biti otporna na požare, poplave i probijanja,
- ulazi u prostorije koje sadrže osjetljivu opremu moraju biti jasno označeni,
- svi kontrolni mehanizmi moraju biti periodički pregledavani kako bi se na vrijeme uočili nedostaci zaštite ili pokušaji neovlaštenog pristupa.

3. SIGURNOST OPREME

Najvažniji aspekt kod fizičke zaštite informacionog sistema predstavlja pravilna zaštita opreme i uređaja. Svakom uređaju treba definirati posebne mjere zaštite s obzirom na njegovu namjenu i vrijednost. Takve mjere trebaju spriječiti sve prijetnje, uključujući prijetnje od prirodnih nepogoda ili ljudske prijetnje. Većina organizacija provodi samo osnovne mjere zaštite opreme koje često nisu dovoljne, a odnose se na zaštitu servera i personalnih računara. Razlog tome je što navedeni elementi sadrže najviše osjetljivih podataka pa njihovo oštećenje može dovesti do ozbiljnih posljedica. Ipak, potrebno je provesti dodatne sigurnosne mjere pri rukovanju opremom, kao što su:

- zaključavanje uređaja nakon upotrebe (npr. fax uređaja),
- smještaj uređaja na sigurna mjesta,
- pohrana prijenosnih medija na sigurna mjesta,
- adekvatno uništavanje starih prijenosnih medija.

Svrha osiguravanja opreme je spriječiti gubitke, štetu ili kompromitiranje imovine i prekid poslovnih aktivnosti. Oprema treba biti zaštićena od prijetnji i opasnosti iz okoline. Zaštita opreme je neophodna kako bi se smanjio rizik neovlaštenog pristupa podacima te kako ne bi došlo do gubljenja i oštećenja imovine.

3.1. Smještaj i zaštita opreme

3.1.1. Zaštita servera

Serveri predstavljaju vrlo važan aspekt za poslovanje svake organizacije jer mogu sadržavati vrlo važne informacije, a zaposleni ih svakodnevno koriste. Zbog takvih namjena, najbolja praksa je razdvajanje svakodnevnih funkcija od servera. To znači da se jedan server ne bi trebao koristiti za obavljanje svakodnevnih zadataka. Još jedan od važnih elemenata zaštite predstavlja pravilan smještaj servera. Najbolje bi bilo servere izdvojiti u posebnu prostoriju koju je moguće dobro nadzirati. Također, smještaj treba organizirati tako da se spriječi pomicanje i premještanje servera. Time se sprječava oštećenje i uzrokovanje kvarova, ali se može postići i bolja zaštita od nekih prirodnih prijetnji (npr. potres).

3.1.2. Zaštita personalnih računara

Najosnovniji način zaštite personalnih računara uključuje dobru edukaciju zaposlenih. Ukoliko su zaposleni upoznati sa pravilnim načinom rukovanja računarom, rizik od raznih prijetnji znatno je umanjen. Zaposlenima je potrebno jasno definirati pravila u obliku sigurnosnih politika te ih predstaviti na jednostavan način. U sklopu sigurnosne politike treba navesti pravilno ophođenje prema računarima u slučaju nekog kvara ili prirodne nepogode. Također, treba definirati zaštitu od krađe, špijunaže i drugih prijetnji koje donose ljudi, a odnose se na fizičku sigurnost. Upotreba nadzora u obliku postavljanja kamera i osiguranja može spriječiti zaposlene pri pokušaju oštećivanja ili krađe računara. Nadzorne kamere potrebno je postaviti na ključna mjesta koja su u blizini vrijednih uređaja ili računara.

Kako bi se onemogućilo zlonamjerno rukovanje računarom nekog zaposlenog potrebno je računar zaključati ukoliko nije u upotrebi. Računar koji ostaje uključen posjetitelji mogu zloupotrijebiti za otkrivanje osjetljivih podataka ili nanošenje druge štete. Smještaj računara zaposlenih također predstavlja važan aspekt zaštite. Računare je potrebno rasporediti tako da niti jedan zaposleni nema pristup podacima drugog zaposlenog. Kako bi se dodatno spriječilo otkrivanje osjetljivih podataka, treba izbjegavati da svi korisnici upotrebljavaju isti prijenosni uređaj za pohranu podataka. Sprečavanje krađe može se postići i nekim sofisticiranim uređajima. Neki od njih su sistemi za praćenje i otkrivanje lokacije ukradenih ili izgubljenih stvari. Također, postoje posebni držači za prenosive računare koji imaju mogućnost zaključavanja. Ukoliko takvi uređaji nisu dostupni, moguće je ugraditi ormariće sa karticama za sigurnu pohranu mobilnih računara. Sigurnost informacionog sistema dodatno se može povećati zaključavanjem USB priključaka kako bi se spriječilo preuzimanje podataka ili onemogućilo ubacivanje zlonamjernih programa.

Sljedeće smjernice treba uzeti u obzir pri fizičkoj zaštiti opreme:

- oprema mora biti smještena tako da je nepotrebni pristup opremi minimalan,
- jedinice za obradu podataka moraju biti smještene tako da je smanjena mogućnost posmatranja neovlaštenim korisnicima (primjer: postavljanje monitora pod takvim uglom da samo osoba za računarom vidi sliku),
- kontrole je potrebno provoditi tako da minimiziraju rizik od potencijalnih prijetnji (krađa, požar, dim, voda, vibracije, radijacija itd.),
- zabranjeno je jesti, piti i pušiti u blizini opreme,
- uvjeti okruženja (temperatura, vlaga) koji mogu utjecati na rad jedinica za obradu informacija treba definirati odgovorno lice a moraju biti strogo nadzirani.

3.2. Sigurnost instalacija

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u snabdijevanju energijom, vodom, odvodnjom otpadnih voda, grijanjem/hlađenjem itd. Sve navedene instalacije moraju biti pravovremeno pregledane i testirane kako bi se na vrijeme uočile i ispravile greške u radu.

Nestanak struje, poplavu, požar ili bilo koju drugu prijetnju bitno je alarmirati zvučnim i svjetlosnim signalima kako bi se pravovremeno preduzele propisane akcije u slučaju nezgode. Snabdijevanje vodom mora biti redovno kontrolirano kako ispravnost uređaja za gašenje požara ne bi bila upitna. Telekomunikaciona oprema mora biti instalirana tako da eventualan prekid veze ne utječe na kompletan prekid komunikacije. Primjer rješenja ovog problema je priključenje komunikacionih uređaja na više servera.

3.3. Sigurnost kod kabliranja

Kablovi za snabdijevanje električnom energijom i telekomunikacioni kablovi moraju biti adekvatno zaštićeni od oštećenja, prekida ili priključenja neovlaštenih korisnika na mrežu, ako to uvjeti na postojećoj fizičkoj lokaciji dozvoljavaju. Prije kabliranja treba biti razmotreno sljedeće:

- kablovi za napajanje jedinica za obradu podataka, ukoliko je moguće, moraju biti položeni podzemno (alternativa je adekvatna fizička zaštita),
- isto važi i za telekomunikacione kablove,
- kablovi za napajanje moraju biti razdvojeni od telekomunikacionih kako bi se izbjeglo međudjelovanje,
- označavanje kablova posebnim identifikacionim oznakama spriječit će greške u spajanju (napomena: oznake je potrebno dokumentirati).

4. ODRŽAVANJE OPREME

Održavanje opreme treba redovno obavljati stručnjak kako bi se osigurala ispravnost, tj. neprekidan rad. Pri održavanju opreme treba se pridržavati sljedećeg:

- održavanje opreme mora biti u skladu sa preporukama proizvođača, u određenim vremenskim intervalima i po zadatim specifikacijama,
- samo ovlaštena lica smiju servisirati opremu,
- prije servisiranja opreme potrebno je provesti odgovarajuće sigurnosne kontrole, ukoliko za tim postoji potreba, te je potrebno obrisati povjerljive informacije (potrebe za ovakvim mjerama nastaju ukoliko servisiranje izvršavaju vanjski partneri ili treća strana),
- pristup vanjskih partnera opremi treba biti strogo kontroliran i dokumentiran,
- pristup vanjskih partnera opremi treba biti ograničen ugovorom.

5. ZAKLJUČAK

U skladu sa Politikom i Smjernicama o fizičkoj zaštiti informacija preporučuje se institucijama BiH da donesu svoj interni akt u kojem će definirati **pravila/procedure o fizičkoj zaštiti informacija.**

LITERATURA:

1. Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija
4. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", br. 54/05 i 12/09)

SMJERNICE
O KORIŠTENJU PRIJENOSNIH UREĐAJA

1. SVRHA

Prijenosni računari su sve popularniji. Cjenovno blizu, a praktičnošću puno ispred desktop računara, postali su čest izbor pri kupovini računara, bilo da se radi o poslovnim ili privatnim korisnicima.

Ali, upotreba prijenosnih računara od zaposlenih, partnera ili drugih korisnika donosi potrebu za uvođenjem dodatnih sigurnosnih kontrola. One moraju spriječiti svaku neovlaštenu radnju koja može ugroziti sigurnost informacionog sistema.

2. IDENTIFIKACIJA PRIJETNJI

Sigurnost sistema upotrebom prijenosnih računara možete biti ugrožena na sljedeće načine:

- slučajni postupci ovlaštenog korisnika prijenosnog računara,
- namjerni postupci ovlaštenog korisnika prijenosnog računara,
- namjerni postupci neovlaštenog (zlonamjernog) korisnika,
- pokretanje malicioznog kôda na prijenosnom računaru,
- krađa, gubitak ili mijenjanje podataka zbog nepravilnog rukovanja prijenosnim računarom.

3. FIZIČKA ZAŠTITA PRIJENOSNOG RAČUNARA

3.1. Unutar prostorija institucije

Unutar prostorija institucije korisnik je dužan pridržavati se pravila definiranih Pravilnikom o informatičkoj sigurnosti radnog mjesta. To znači da računar ni u kojem trenutku ne smije ostaviti nezaštićen bez nadzora. Kod kraćih odsustvovanja računar je potrebno zaštititi nekim od jednostavnijih oblika zaštite (npr. čuvarom ekrana sa lozinkom i sl.). Kod dužih odsustvovanja (godišnji odmor, bolovanje) korisnik je dužan računar smjestiti u prostor pod fizičkom zaštitom (u zaključani ormar ili prostoriju).

3.2. Izvan prostorija institucije

Ukoliko se prijenosni računar iznosi izvan prostorija institucije (na putovanje ili sl.), potrebno je pridržavati se sljedećeg:

- vrijeme bez nadzora računara treba biti što kraće,
- računar ne treba ostavljati u automobilu na vidljivom mjestu,
- računar ne treba ostavljati bez nadzora u nezaključanom prostoru,
- ostavljeni prijenosni računar treba biti isključen, zaključan u spremištu gdje nije vidljiv.

4. SERVIS OPREME

4.1. Servisiranje

- ukoliko je moguće, prije servisiranja potrebno je napraviti sigurnosne kopije svih (važnih) podataka sa računara u skladu sa *Pravilnikom o sigurnosnim kopijama*,
- ako servisiranje provodi treća strana, podatke sa računara potrebno je zaštititi ovisno o njihovoj klasifikaciji (nekom od kriptografskih metoda), a ukoliko postoji potreba, podaci sa računara moraju biti izbrisani (nakon izrade sigurnosne kopije podataka).

4.2. Povratak prijenosnog računara sa servisiranja

- sve lozinke moraju biti promijenjene,
- sve funkcionalnosti trebaju biti provjerene,
- sve se mora podvrgnuti antivirusnoj provjeri.

5. ZAKLJUČAK

U skladu sa Politikom i Smjernicama o korištenju prijenosnih uređaja preporučuje se institucijama BiH da donesu svoj interni akt u kojem će definirati **pravila/procedure o korištenju prijenosnih uređaja.**

LITERATURA:

1. Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija
4. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", br. 54/05 i 12/09)

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. do 2022. godine