- 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

("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. veljače 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

Članak 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 dio ove Odluke.

Članak 2.
(Praćenje realiziranja)

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 71/23
23. veljače 2023. godine
Sarajevo

Predsjedateljica
Vijeća ministara BiH
Borjana Krišto, v. 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 sustava u velikoj mjeri.

Neki od uzroka sigurnosnih incidenata koje izazovu ovlašteni korisnici su:

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

Navedene prijetnje sigurnosti informacijskim sustavima razlog su zbog kojih postoji potreba za kontrolom pristupa, tj. zabranom pristupa onim resursima sustava kojima korisnik nema potrebe pristupati.

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

2. KONTROLA PRISTUPA

2.1. Prava pristupa sukladno potrebama

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

Dokument treba sadržavati:

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

2.2. Upravljanje pristupom korisnika

S ciljem kvalitetne kontrole pristupa informacijskim sustavima 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 informacijskim resursima. Posebnu pozornost treba posvetiti kontroli dodjele privilegiranih prava pristupa.

2.3. Registracija korisnika

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

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

2.4. Upravljanje korisničkim zaporkama

Zaporke služe kako bi se putem mreže provjerilo da li je korisnik koji se predstavlja korisničkom zaporkom upravo taj korisnik. Stoga je potrebno sigurnosnim mehanizmima omogućiti maksimalnu sigurnost zaporki u smislu njihove tajnosti. Osim politike sigurnosti namijenjene korisnicima u kojoj se jasno definira na koji način rukovati zaporkama, osoba odgovorna za sigurnost dužna je držati se sljedećih pravila prilikom raspodjele zaporki:

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

2.5. Odgovornost korisnika

2.5.1. Uporaba zaporki

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

- čuvaju povjerljivost zaporki,
- ne bilježe zaporke na papire,
- zaporke mijenjaju isključivo nakon prijave na sustav,
- biraju kvalitetne zaporke, dugačke minimalno 6 znakova, maksimalno 10,
- zaporke budu lako pamtljive,
- zaporke sadrže brojeve i slova, po potrebi i specijalne znakove,
- zaporke ne predstavljaju imena, prezimena, gradove, datume rođenja, nadimke i sl. riječi,
- redovito mijenjaju zaporke,
- ne koriste već uporabljivane zaporke,
- ne koriste zaporke koje već koriste na drugim sustavima.

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 zlouporabe računara, mobitela, ali i drugih komunikacijskih uređaja ako 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 sustava ili zaštite računar posebnim programima (npr. čuvar ekrana) ako računar ostavljaju bez nadzora,
- računar odjave sa sustava nakon završetka posla,
- ako 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 s udaljenih lokacija potrebno je autentificirati posebnim metodama koje osiguravaju odgovarajuću razinu zaštite.

2.5.4. Kontrola pristupa operativnom sustavu

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

- prilikom prijave na sustav korisnik treba unijeti svoje korisničko ime i zaporku, na temelju čega se radi provjera identiteta,
- provjeru da li je razdoblje valjanosti zaporke isteklo; ako jeste (svaka 3 mjeseca), obavijestiti korisnika da je potrebno napraviti izmjenu,
- sustav mora bilježiti pristup informacijskom sustavu i pokušaje pristupa,
- rad korisnika na klijentskim radnim stanicama treba dodatno kontrolirati na način da se prati vrijeme neaktivnosti; ako je klijentska radna stanica neaktivan duže od 10 minuta, treba napraviti automatsku odjavu sa sustava,
- ako je potrebno, kontrolu s koje se lokacije pristupa sustavu,
- broj mogućih prijava na sustav treba ograničiti na 3 prijave.

3. ZAKLJUČAK

Sukladno Politici 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 informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustavi 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

Informacijski sustavi često su temelj 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 informacijskog sustava 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 sustavima. 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 provedba kontrole pristupa. Također, potrebno je uvesti zaštitu opreme i uređaja putem dostupnih tehnologija. Razni sustavi razvijeni su za uspostavu i poboljšanje fizičke sigurnosti. Neki od njih su alarmni sustavi te sustavi za nadzor, kontrolu pristupa ili zaključavanje vrijednih uređaja.

Svrha fizičke zaštite informacijskog sustava je preventivnim metodama osigurati zaštitu sustava 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 uporabe 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 skupine primjenjuju i druge sofisticirane mjere zaštite. Prema tome, fizička sigurnost čini dio

sveukupne sigurnosti informacijskog sustava kao osnove na kojoj su sve sigurnosne mjere utemeljene. Mjere koje uključuje fizička sigurnost, a služe za zaštitu osoblja, opreme i imovine, mogu se podijeliti na:

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

Da bi se osigurala fizička zaštita informacijskog sustava, institucija je dužna provesti sljedeće točke sigurnosti:

- potrebno je jasno definirati i dokumentirati tko 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 informacijskog sustava 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 uporabe (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. Ako su zaposleni upoznati s 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. Uporaba 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 ako nije u uporabi. Računar koji ostaje uključen posjetitelji mogu zlouporabiti 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 rabe isti prijenosni uređaj za pohranu podataka. Sprečavanje krađe može se postići i nekim sofisticiranim uređajima. Neki od njih su sustavi za praćenje i otkrivanje lokacije ukradenih ili izgubljenih stvari. Također, postoje posebni držači za prenosive računare koji imaju mogućnost zaključavanja. Ako takvi uređaji nisu dostupni, moguće je ugraditi ormariće s karticama za sigurnu pohranu mobilnih računara. Sigurnost informacijskog sustava 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 promatranja neovlaštenim korisnicima (primjer: postavljanje monitora pod takvim kutom 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 odgovorna osoba a moraju biti strogo nadzirani.

3.2. Sigurnost instalacija

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u opskrbi energijom, vodom, odvodnjom otpadnih voda, grijanjem/hlađenjem itd. Sve navedene instalacije moraju biti pravodobno 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 pravodobno poduzele propisane akcije u slučaju nezgode. Opskrba vodom mora biti redovno kontrolirana kako ispravnost uređaja za gašenje požara ne bi bila upitna. Telekomunikacijska oprema mora biti instalirana tako da eventualan prekid veze ne utječe na kompletan prekid komunikacije. Primjer rješenja ovog problema je priključenje komunikacijskih uređaja na više servera.

3.3. Sigurnost kod kabliranja

Kablovi za opskrbu električnom energijom i telekomunikacijski 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, ako je moguće, moraju biti položeni podzemno (alternativa je adekvatna fizička zaštita),
- isto vrijedi i za telekomunikacijske kablove,
- kablovi za napajanje moraju biti razdvojeni od telekomunikacijskih kako bi se izbjeglo međudjelovanje,
- označavanje kablova posebnim identifikacijskim oznakama spriječit će pogreške u spajanju (napomena: oznake je potrebno dokumentirati).

4. ODRŽAVANJE OPREME

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

- održavanje opreme mora biti sukladno preporukama proizvođača, u određenim vremenskim intervalima i po zadatim specifikacijama,
- samo ovlaštene osobe smiju servisirati opremu,
- prije servisiranja opreme potrebno je provesti odgovarajuće sigurnosne kontrole, ako za tim postoji potreba, te je potrebno obrisati povjerljive informacije (potrebe za ovakvim mjerama nastaju ako 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

Sukladno Politici 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 informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustavi 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, uporaba 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 informacijskog sustava.

2. IDENTIFIKACIJA PRIJETNJI

Sigurnost sustava uporabom 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 zaporkom 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

Ako 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

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

4.2. Povratak prijenosnog računara sa servisiranja

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

5. ZAKLJUČAK

Sukladno Politici 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 informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustavi 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)