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 člana 3. Odluke o usvajanju Politke softvera u Institucijama Bosne i Hercegovine Hercegovine, a u vezi sa tačkom 3.6. Politike softvera u Institucijama Bosne i Hercegovine ("Službeni glasnik BiH", broj 143/07), na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na _____. sjednici održanoj _____ 2013. godine, donijelo je

O D L U K U
O USVAJANJU DOKUMENTA O TEHNIČKO-TEHNOLOŠKIM I ADMINISTRATIVNIM MJERAMA ZA SIGURNOST INFORMACIONIH SISTEMA U INSTITUCIJAMA BOSNE I HERCEGOVINE

Član 1.
(Predmet Odluke)

Ovom Odlukom usvaja se Dokument o tehničko-tehnološkim i administrativnim mjerama za sigurnost informacionih sistema u Institucijama Bosne i Hercegovine (u daljem tekstu: Dokument) koji je dat u prilogu ove Odluke i njen je sastavni dio.

Član 2.
(Djelokrug primjene)

Dokument iz člana 1. ove Odluke primjenjuje se u svim Institucijama Bosne i Hercegovine.

Član 3.
(Stupanje na snagu)

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

VM broj /13
_____ 2013. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Vjekoslav Bevanda, s. r.

DOKUMENT O TEHNIČKO-TEHNOLOŠKIM I ADMINISTRATIVNIM MJERAMA ZA SIGURNOST INFORMACIONIH SISTEMA U INSTITUCIJAMA BOSNE I HERCEGOVINE

U cilju obezbjeđivanja zaštite podataka na fizičkom, tehničkom i organizacionom nivou potrebno je definirati tehničke i administrativne mjere zaštite informacionog sistema kao što je utvrđivanje i provjera korisnika sistema i njihovih prava pristupa podacima i modulima sistema, bilježenje pristupa, autentifikacija vlasnika dokumenata, kriptografija i algoritmi enkripcije kojima se štiti komunikacija između web servisa.

1. Obaveza primjene

Dokument o tehničko - tehnološkim i administrativnim mjerama za sigurnost informacionih sistema u Institucijama Bosne i Hercegovine (u daljem tekstu: Dokument) primjenjuje se u Institucijama Bosne i Hercegovine (u daljem tekstu: Institucije). Zaposlenici u Institucijama, kao korisnici sistema, obavezni su da usaglase praksu zaštite sa ovim Dokumentom kao i sa drugim referentnim standardima, uputstvima i procedurama zaštite. Ukoliko dođe do povrede pravila postavljenih ovim Dokumentom i referentnim standardima, uputstvima i procedurama zaštite, administrator zaštite i/ili kontrolni organ obavezni su o tome izvijestiti nadležni organ.

2. Značenje pojedinih pojmova

Izrazi upotrijebljeni u ovom Dokumentu imaju slijedeće značenje:

a) **"Administrativna zona''** predstavlja oblast koja se uspostavlja za korištenje podataka u kontrolisanom, vidljivo označenom prostoru unutar kojeg je moguće kontrolisati pristup osoba;

b) **"Administrator sistema/sistem administrator''** je osoba odgovorna za upravljanje, održavanje i sigurnost računarskog sistema i računarske mreže unutar Institucije;

c) **"BAS''** je Državni standard Bosne i Hercegovine;

d) **"Baza podataka''** je uređena grupa podataka pohranjena na sistemski način tako da računarski program tj. klijent može poslati upit bazi podataka na koji ona odgovara. Podaci se u bazu podataka mogu upisivati, brisati i mijenjati, dok rezultat upita može biti pretraživanje, sortiranje, pregledanje, upoređivanje po zadatom kriterijumu, razni proračuni i sl.;

e) **"Demilitarizovana zona''** predstavlja segment mreže koji se može opisati kao neutralna zona između lokalne mreže i Interneta, putem koje se sprječavaju spoljašnji korisnici da pristupe lokalnoj mreži;

f) **"Enkripcija (engl. Encription)''** predstavlja proces u kriptografiji kojim se vrši izmjena podataka tako da se sadržaj učini nečitljivim za osobe koje ne posjeduju ključ, pomoću kojeg bi pročitali sadržaj;

g) **“Firewall’’** je specijalizirani softver ili hardverski mrežni uređaj čija je osnovna funkcija filtriranje mrežnog prometa i odvajanje interne mreže organizacije od Interneta, s ciljem da zaštiti mrežu od nedozvoljenog pristupa ili zlonamjernog programa;

h) **“International Electrotechnical Commission (IEC)’’** je Međunarodna elektrotehnička komisija;

i) **“Institucije Bosne i Hercegovine’’** su Vijeće ministara Bosne i Hercegovine, sve agencije, direkcije, te ostale institucije osnovane od strane Vijeća ministara Bosne i Hercegovine i Parlamentarne skupštine Bosne i Hercegovine, a u skladu sa Zakonom o upravi i Zakonom o ministarstvima i drugim tijelima uprave Bosne i Hercegovine;

j) **“Informacija’’** je rezultat obrade, manipulacije, organiziranja i interpretacije podataka koji daju određeno znanje primatelju;

k) **“Informacioni sistem’’** predstavlja sistem za prikupljanje, obradu, prenos, pohranu i distribuciju informacija, te ih čini dostupnim i upotrebljivim;

l) **“Informaciono-komunikacione tehnologije’’** (u daljem tekstu: IKT) predstavljaju skup informacionih tehnologija koje se koriste u procesu prikupljanja, odabira, obrade, prenosa, verifikacije, skladištenja, prikaza, objavljivanja i dijeljenja informacija u procesima komunikacije, kod kojih su jasno razdvojene komponente informacije i komunikacije;

m) **“Internet’’** je globalna računarska mreža, sačinjena od velikog broja međusobno povezanih računarskih mreža i uređaja, koja omogućava razmjenu podataka između računara;

n) **“IP - Internet protokol’’** predstavlja mrežni protokol za usmjeravanje i prijenos podataka u formi paketa, kojeg koriste izvorišni i odredišni čvorovi mreže za komunikaciju putem računarske mreže;

o) **“International Organization for Standardization (ISO)’’** je Međunarodna organizacija za standardizaciju;

p) **“Haker ”** predstavlja osobu koja ima znanje, sposobnost i namjeru da u potpunosti neovlašteno pristupi tuđem računarskom i komunikacionom sistemu s ciljem da napravi štetu na sistemu;

r) **“Hardver “** je materijalna osnova informacionog sistema, u koju ubrajamo: računar, ulazno - izlazne uređaje, uređaje za prenos podataka na daljinu i ostalu opremu neophodnu za obradu, prikaz, razmjenu i dijeljenje podataka;

s) **“Kriptografija”** je nauka koja proučava šifrovanje (enkripciju) i dešifrovanje (dekripciju) podataka upotrebom složenih primjenljivih matematičkih algoritama s ciljem osiguranja bezbjedne komunikacije i zaštite podataka;

t) **“Kriptografska zaštita”** je primjena programskih rješenja ili uređaja za zaštitu podataka koji osiguravaju integritet, povjerljivost i dostupnost podataka;

u) **“Lokalna mreža (Local Area Network - LAN)” -** predstavlja lokalno mrežno okruženje za umrežavanje grupe računara na jednoj fizičkoj lokaciji;

v) **“National Institute of Standards and Technology (NIST)” -** Američki nacionalni institut za standarde i tehnologiju;

z) **“Podatak“** označava svako predstavljanje činjenica, informacija ili koncepata u obliku koji je pogodan za njihovu obradu u računarskom sistemu;

aa) **“Pristup”** označava omogućavanje dostupnosti sredstava ili usluga korisnicima, pod određenim uslovima i prema jasno definisanim pravilima korištenja, radi pružanja elektronskih komunikacionih usluga, uključujući usluge putem kojih se pružaju usluge informacionog društva ili predaju usluga sadržaja, što, između ostalog, obuhvata: pristup dijelovima mreže i pripadajućoj infrastrukturi i opremi, koji može sadržavati i priključenje opreme putem fiksnih ili bežičnih mreža, pristup fizičkoj infrastrukturi uključujući zgrade, kablovsku kanalizaciju i antenske stubove, pristup odgovarajućim softverskim sistemima, pristup informacionim sistemima i bazama podataka, pristup fiksnim i mobilnim mrežama, pristup sistemima uslovnog pristupa, kao i pristup virtuelnim mrežnim uslugama;

bb) **“Proces”** predstavlja skup povezanih, struktuiranih i koordinisanih aktivnosti koje kombinuju raspoložive resurse, kako bi na osnovu određenih ulaznih parametara proizveli određene izlaze krajnjim korisnicima;

cc) **“Računarska mreža”** je skup međusobno povezanih elektronskih uređaja i računara koji međusobno komuniciraju razmjenjujući podatke;

dd) **“Rizik”** je svaki potencijalni uzrok koji može nanijeti štetu podatku ili informacionom sistemu u kojem se koriste podaci;

ee) **“Server”** predstavlja računarski sistem koji pruža usluge drugim računarskim sistemima - klijentima koji mu pristupaju i na njemu pohranjuju podatke, te pronalaze informacije i servise. Komunikacija između servera i klijenta odvija se preko računarske mreže. Naziv server najčešće se odnosi na cijeli računarski sistem;

ff) **“Sigurnosni incident”** predstavlja neželjeni događaj koji se odražava i ugrožava sigurnost informacionog sistema;

gg) **“Sigurnost informacionog sistema”** obezbjeđuje odgovarajuću zaštitu informacija od širokog spektra prijetnji u cilju osiguranja kontinuiteta poslovanja i minimiziranja poslovnih šteta unutar organizacije;

hh) **“Socijalni inženjering”** je manipulacija ljudima, tj. prevara u svrhu otkrivanja njihovih povjerljivih informacija ili dobijanja pristupa nekim drugim resursima koje manipulator inače ne bi mogao saznati.

ii) **"Softver"** obuhvata nematerijalne elemente informacionog sistema: programe, rutine, procedure, organizaciju, obradu podataka i obezbjeđenje informacija;

jj) **"Standard"** je dokument za opću i višekratnu upotrebu, donesen konsenzusom i odobren od priznatog tijela, koji sadrži pravila, smjernice ili karakteristike aktivnosti ili njihove rezultate i koji ima za cilj postizanje optimalnog nivoa uređenosti u datom kontekstu;

kk) **"Upravljanje rizikom informacione sigurnosti"** podrazumijeva sistemski pristup koji uključuje planiranje, organiziranje i usmjeravanje aktivnosti, s ciljem osiguravanja da rizici za klasificirane podatke ostanu u zakonom utvrđenim i prihvatljivim okvirima;

ll) **"Virtuelna privatna mreža (Virtual Private Network - VPN)"** predstavlja sigurnu privatnu mrežu jedne ili više institucija, realizovane preko javne ili dijeljene infrastructure;

mm) **"Web servis"** predstavlja softverski sistem dizajniran da podrži interoperabilnost između uređaja putem mreže, koristeći se interfejsom za stupanje u interakciju sa web servisom putem mrežnih protokola i web standarda.

3. Zaštita informacionih sistema

3.1 Informaciona sigurnost

Sigurnost je proces održavanja prihvatljivog nivoa rizika. Kako bi se u domenu informacionih sistema postigao prihvatljiv nivo sigurnosti, potrebno je sigurnost posmatrati kao proces:

- procjene sigurnosnih zahtjeva i rizika (engl. Assessment),
- zaštite (engl. Protection),
- detekcije upada (engl. Detection) i
- oporavka tj. odgovora na napad (engl. Response).

S ciljem povećanja i osiguravanja informacione sigurnosti, neophodno je kontinuirano vršiti kontrolu pristupa računarskim i mrežnim resursima odnosno informacionim sistemima u cjelosti. Informaciona sigurnost postiže se implementacijom mehanizama za očuvanje povjerljivosti, integriteta i dostupnosti informacija. Pod povjerljivošću informacija podrazumijeva se da su informacije dostupne samo onima koji su ovlašteni da ih koriste. Pod pojmom integritet podrazumijeva se tačnost i kompletnost informacija, što se postiže sprječavanjem vršenja izmjena informacija od strane neovlaštenih osoba. Pod pojmom dostupnost informacija podrazumijeva se da samo ovlašteno osoblje ima pravo pristupa informacijama.

Informaciona sigurnost odnosi se na procedure, tehničke mjere i metode kojima se onemogućava neovlašteni pristup ili mijenjanje podataka, kao i krađa i fizičko oštećenje informacionih sistema unutar Institucije. To se može osigurati korištenjem različitih tehnika osiguranja hardvera, softvera, mreža komunikacije i ostalih elemenata informacionog sistema.

3.2 Politika sigurnosti informacija

Svrha politike sigurnosti informacija ogledati će se u identifikaciji rizika po imovinu, utvrđivanju vrijednosti imovine, otkrivanja ranjivosti sistema kao i potencijalnih uzroka nekog neželjenog incidenta. Nepostupanje u skladu sa politikom sigurnosti informacija dovoditi će do neželjenih incidenta koji nanose štetu informacionom sistemu ili cijeloj Instituciji. Svrha politike ogledati će se i u mogućnosti da se upravlja rizicima na prihvatljivom nivou kroz dizajniranje, implementaciji i održavanja informacionog sistema.

Namjena sigurnosti upravljanja informacijama je da se obezbjede i zaštite informacije i imovina od svih prijetnji, bilo internih ili eksternih, slučajnih ili namjernih kroz uspostavljanje, implementaciju, izvršavanje, nadzor, preispitivanje, održavanje i poboljšanje sigurnosti informacionog sistema. Implementacija politike sigurnosti informacija i pravila neophodna je zbog održavanje integriteta informacionog sistema za pružanje usluga.

Politika sigurnosti informacija osigurava i garantuje da će:

- informacije biti zaštićene od neovlaštenog pristupa;
- se održavati povjerljivost informacija;
- informacije ostati neotkrivene neovlaštenim osobama bilo slučajnim ili namjernim aktivnostima;
- se integritet informacija sačuvati kroz zaštitu od neovlaštene izmjene;
- se omogućiti pristup i izmjena informacija ovlaštenim licima kad je to potrebno;
- biti obezbjeđena usaglašenost sa svim kontrolnim i zakonskim zahtjevima;
- se pružiti podrška politici kroz kontinurane poslovne planove koji će se određivati, održavati i testirati u stalnom praktičnom radu;
- se sprovoditi kontinuirana edukacija zaposlenih u svim organizacionim dijelovima Institucija;
- se razmatrati i istražiti sve povrede sigurnog rukovanja informacija;
- se dokumentovati i istražiti sve povrede sigurnosti.

Svi zaposleni su odgovorni za implementaciju politike i zaštite informacija i obavezni su pružiti podršku rukovodstvu koje je propisalo politiku sigurnosti informacija i pravila.

Osnovni ciljevi implementacije politike sigurnosti informacija su:

- zaštita informacija;
- zaštita informacione imovine Institucije;
- pružanje pouzdanih informacija zaposlenima i očuvanje njihove povjerljivosti u svim slučajevima pristupa postojećim informacijama.

Specifična pravila koja podržavaju politiku sigurnosti informacija uključuju:

- fizičku sigurnost;
- pristupne kontrole sistemu i podacima;
- edukacija u vezi sa sigurnošću;
- internet i elektronsku poštu;
- zaštitu podataka kroz pravljenje rezervnih kopija i arhiviranje istih (engl. Backup);
- način korištenja prenosnih uređaja;
- skladištenje i dostupnost povjerljivih informacija;
- prevencija i detekcija djelovanja virusa, trojanaca i drugog malicioznog koda.

Ostali koraci koji se izvršavaju u cilju sprječavanja propusta su:

- pisanjem i poštivanjem sigurnosnih procedura određuje se na koje se načine čuvaju podaci, kako se sa njima upravlja, kome se dodjeljuju prava i odgovornosti, spriječavaju ili se svode na minimum potencijalne greške;
- edukacija korisnika podiže se svijest o ovom problemu, načinima kako sigurno raditi, čime se sprječavaju daljnje greške;
- procjena rizika predstavlja proces sistematske identifikacije rizika, analiza i ocjena njihovih uticaja. Nakon kvalitetne ocjene rizika određuju se prioriteti rješavanja istih;
- tretman rizika - tretman rizika predstavlja prijedlog i način kako rizik umanjiti i koji rizik prioritetno rješavati;
- postojanje incident menadžmenta podrazumijeva da se upravljanjem incidentom kreira zapis o tome kada se incident dogodio, uzrok incidenta i način na koji je riješen. Incidenti se prate i ukoliko se često javljaju, predstavljaju jasan pokazatelj da određeni segment ne funkcioniše na pravi način. Prednost se ostvaruje na dugoročnom nivou, jer se kroz praćenje incidenata dobivaju podaci za analizu na osnovu čega se donose daljnje odluke;
- nadgledanjem i upozoravanjem postiže se smanjene vremena potrebnog za detekciju problema, upućuju se korisnici i servisi na reakciju, čime se sprječavaju propusti u praćenjem trenutne situacije.

4. Zaštita podataka

Kako bi se postigla učinkovita zaštita podataka, server mora biti opremljen:

- sistemom za sigurno prijavljivanje za rad sa mogućnošću evidentiranja ostvarenih pristupa, kako bi se pristup serveru mogao kontrolisati i ograničiti;
- mehanizmom za sprječavanje neovlaštenog iznošenja i unošenja podataka upotrebom prenosivih informatičkih medija, komunikacionih priključaka i priključaka za ispis podataka;
- mehanizmom zaštite od računarskih virusa i drugih štetnih programa.

Baze podataka obavezno se trebaju skladištiti na prenosive medije i to najmanje jednom sedmično, mjesečno i godišnje za potrebe obnove baze podataka.

- Sedmično skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u sedmici, nakon sprovođenja dnevnog skladištenja podataka, u onoliko sedmičnih primjeraka koliko u mjesecu ima posljednjih radnih dana u sedmici.
- Mjesečno skladištenje podataka informacionog sistema obavlja se posljednjeg radnog dana u mjesecu, za svaki mjesec posebno.
- Godišnje skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u godini. Svaki primjerak godišnje uskladištenih podataka čuva se za vrijeme određeno propisima kojima se uređuje arhivska djelatnost. Svaki primjerak prenosivog medija sa uskladištenim podacima mora biti označen brojem, vrstom (dnevno, sedmično, mjesečno, godišnje), datumom skladištenja, kao i imenom lica koje je izvršilo skladištenje podataka.

Upotrebljivost sigurnosne kopije podataka provjerava se najmanje svakih šest mjeseci, uz provjeru postupka povraćaja baza podataka uskladištenih na mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za korištenje.

4.1 Mjere zaštite

Sprovođenje informacione sigurnosti ostvaruje se pomoću procjene rizika. Potrebno je ustanoviti koje su to prijetnje koje se mogu javiti ili se javljaju u informacionom sistemu Institucija. Kada se sprovodi procjena rizika u obzir se uzimaju svi informacioni resursi sa kojima Institucija raspolaže. Nakon procjene rizika vrši se identifikacija i sprovođenje mjera zaštite kako bi se smanjio nivo rizika.
Pod smanjenjem nivoa rizika podrazumijeva se sve što smanjuje negativnu prirodu rizika. Preko analize rizika, politike sigurnosti i plana rekonstrukcije havarijskih situacija dolazi se do preostalog rizika.

Neke od osnovnih mjera zaštite koje se moraju sprovesti su:

- jasno ograničavanje prava pristupa,
- stroga kontrola protoka informacija,
- jasno obilježavanje nivoa tajnosti svake informacije,
- definisanje procedura za manipulaciju informacijama.

Pored tih osnovnih mjera može se izvršiti i potpisivanje izjave o povjerljivosti, odnosno upoznatosti sa svim procedurama vezanima za informacionu sigurnost i svjesnosti o materijalnoj i kaznenoj odgovornosti u slučaju kršenja istih. Zaposleni moraju biti upoznati također i sa disciplinskim postupcima nad počiniocima koji su prekršili pravila informacione sigurnosti unutar Institucija.

Sigurnost informacionog sistema postiže se kroz:

- mjere zaštite informacionog sistema,
- upravljanje sviješću o sigurnosti, i
- planiranje djelovanja u izvanrednim okolnostima.

Server i računarsku mrežu postavlja i ugrađuje stručno lice, u skladu sa projektnom dokumentacijom, važećim normama, standardima i tehničkim uputstvima. Svaki pristup informacionom sistemu za obradu i skladištenje podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave. Svaki pokušaj neovlaštenog pristupa informacionom sistemu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, a ako je to moguće i lokacijom sa koje se pokušalo pristupiti.

Prostorije u kojima je smješten informacioni sistem moraju imati uređaje za gašenje požara, dok u blizini, ispred i u samim prostorijama, na vidljivim i lako uočljivim mjestima moraju biti istaknuta i uputstva o postupanju u slučaju izbijanja požara.

Također potrebno je osigurati da se u blizini računarske i telekomunikacione opreme ne smije postaviti:

- izvor jakog električnog ili magnetskog polja;
- izvor elektrostatičkog elektriciteta;
- izvor jonizirajućeg zračenja.

Planiranje djelovanja u vanrednim situacijama podrazumijeva analizu potencijalnih rizika u radu informacionog sistema i utvrđivanje postupaka za rješavanje tih rizika, kao i drugih metoda korištenja resursa informacionog sistema u slučaju nedostupnosti informacionog sistema, a u cilju održavanja neprekidnog funkcionisanja, odnosno poslovanja Institucije.

Planiranje djelovanja u vanrednim situacijama obuhvata:

- izradu plana neprekidnog funkcionisanja, odnosno poslovanja Institucije;
- izradu procedura za postupanje u slučaju incidenata.

Plan neprekidnog funkcionisanja, odnosno poslovanja obuhvata uspostavljanje i testiranje adekvatne procedure sigurnog skladištenja podataka, radi vraćanja informacionog sistema i podataka u prvobitno stanje nakon sigurnosnog incidenta, koji podrazumijeva prekid rada informacionog sistema, prirodne nepogode i djelovanje računarskih virusa.

4.1 Upravljanje incidentima

Cilj upravljanja sigurnosnim incidentima je unaprijed definirati i dokumentirati odgovornosti odgovornih osoba, kao i akcije koje su dužni poduzeti kako bi se osigurali pravovremeni i kvalitetni odgovori na prijavljene incidente.

Kod definiranja procedura za upravljanje incidentima informacionog sistema potrebno je imati u vidu slijedeće:

1. Procedure trebaju obuhvatiti različite vrste sigurnosnih incidenata, uključujući:
   - prestanak rada sistema,
   - odbijanje usluge,
   - maliciozni kod,
   - kršenje tajnosti ili integriteta,
   - zloupotreba sistema i sl.

2. U slučaju nepredviđenih događaja, treba definirati sljedeće postupke:
   - plan i implementaciju akcija kako se incident ne bi ponovio,
   - analizu i identifikaciju uzroka incidenta,
   - komunikaciju s napadnutom stranom,
   - izvještavanje nadležnih o incidentu.

3. Dokumentaciju o incidentu i ostale dokaze treba pohraniti i zaštiti s ciljem:
   - interne analize problema,
   - pružanja dokaza u sudskim sporovima.

Izrada procedura za postupanje u slučaju incidenta podrazumijeva planiranje i definiranje aktivnosti sprječavanja, detekcije i oporavka od posljedica incidenta, koji utiču na povjerljivost, integritet i dostupnost podatka ili informacionog sistema, uključujući i izvještavanje o incidentima.

Učinkovitost navedenih mjera, osigurava se sistemskim pristupom koji uključuje:

- razmatranje sigurnosnih aspekata u svim fazama životnog ciklusa informacionog sistema;
- definiranje odgovornosti za provedbu svake od mjera;
- redovnu kontrolu uspostavljenih sigurnosnih pravila i provedbe istih, u cilju provjere efikasnosti i svrsishodnosti.

5. Prijetnje informacionim sistemima

Prijetnja po sigurnost nekom informacionom sistemu je svaki događaj koji može dovesti do narušavanja povjerljivosti, integriteta i dostupnosti podataka. Svaka prijetnja i neovlašteni pristup informacionom sistemu imaju različite posljedice kao što je uništavanje podataka ili narušavanje ispravnog rada cijelog informacionog sistema.

Prema klasifikaciji NIST-a prijetnje informacionim sistemima mogu se podijeliti na:

- Greške i kvarove koji mogu nanijeti značajnu štetu informacionom sistemu i koje mogu prouzrokovati zaposleni, proizvođači programskih paketa ili administratori informacionih sistema. Najčešći uzrok greškama i kvarovima su ljudske radnje;
- Prevare i krađe koje predstavljaju zlonamjernu aktivnost kojom napadač pokušava steći finansijsku ili neku drugu korist. Razlozi zbog kojih se prevare i krađe češće događaju od strane samih zaposlenika su slijedeći: zaposleni imaju pristup podacima i informacionom sistemu, znaju koje podatke sistem sadrži i koje su sigurnosne provjere, zatim postojanje prilike za prevaru i krađu, te kolika je vrijednost moguće štete;
- Sabotaže od strane zaposlenih koje predstavljaju prijetnju kako sigurnosti informacionog sistema tako i podacima informacionog sistema od strane zaposlenih koji imaju pristup i koji znaju u kojim dijelovima sistema je moguće prouzrokovati najveću štetu. Najčešći primjeri sabotaže su: fizičko uništavanje dijelova informacionog sistema, postavljanje zlonamjernog programskog koda čija je namjena izmjena, premještanje ili brisanje podataka, namjerni unos neispravnih podataka, rušenje informacionih sistema, krađa podataka i ucjena pod prijetnjom otkrivanja tih podataka široj javnosti ili konkurenciji, ili namjerno mijenjanje i brisanje podataka;
- Gubitak fizičke i infrastrukturne podrške predstavlja vrstu prijetnje koju nije moguće u potpunosti provjeriti, ponekad ni spriječiti, a može nanijeti veliku štetu sistemima. Takvi slučajevi mogu biti npr. prekid u napajanju električnom energijom, prekid komunikacija, poplava, požar, zemljotresi i sl.;
- Napadače (engl. hackers) koji predstavljaju najopasniju prijetnju sigurnosti informacionog sistema zbog tehnološkog razvoja i širenja Interneta i komunikacija, poslovanja i drugih aktivnosti putem Interneta. Napadačem se smatra osoba koja svoje znanje koristi kako bi ugrozila sigurnost računara ili podataka;
- Zlonamjerne programe (engl. malware) koji predstavljaju vrstu prijetnje kojom se narušava sigurnost informacionog sistema zlonamjernim programima poput crva, virusa, trojanskih konja, logičkih bombi i drugih;
- Otkrivanje privatnosti korisnika predstavlja oblik prijetnje koji je u porastu s obzirom da sve veći broj informacionih sistema sadrži veliki broj ličnih podataka korisnika.

6. Kreiranje kontrolisanog okruženja

U cilju smanjivanja grešaka, havarija, kriminala i povreda sigurnosti, potrebno je razvijati posebne politike i procedure koje će se uključiti u stvaranje i provjeru poslovnih informacionih sistema. Kontrola predstavlja kombinaciju manuelnih i automatizovanih mjera koje čuvaju informacioni sistem i osiguravaju njegov rad. Kontrola se sastoji od metoda, politika i procedura za osiguravanje podataka u informacionom sistemu, tajnosti i nepovredljivosti računarskih sistema i rada u skladu sa međunarodnim standardima.

Kontrola informacionog sistema mora biti sastavni dio njegovog dizajna. Prilikom definisanja kontrole, koristi se analiza troškova i koristi kako bi se odredilo koji su to optimalni mehanizmi kontrole informacionog sistema Institucije.

Bitna pitanja prilikom razvoja kontrolne strukture su:

- zaštita postojećih podataka;
- kontrola funkcionalnosti;
- nivo rizika koji nastaje kao rezultat nepravilno provedene kontrole.

Savremeni računarski sistemi kontrolišu se pomoću dva osnovna tipa kontrole:

1. **Opća kontrola** podrazumijeva kontrolu koja nadgleda dizajn, sigurnost i korištenje računarskih programa i uopće sigurnost u cijelom informacionom sistemu. Opća kontrola se primjenjuje na sve računarske programe i sastoji se od kombinacije softvera i manuelnih procedura koje stvaraju opće okruženje kontrole kao i na okruženje u kojem informacioni sistemi funkcionišu.

2. **Primijenjena kontrola** jedinstvena je za svaku računarsku aplikaciju odnosno program. Sastoji se od tehnika primijenjenih od strane korisnika programa i programskih procedura. Primijenjena kontrola može biti ručna i softverska odnosno programska.

Kontrola sigurnosti podataka predstavlja kontrolu koja omogućava sigurnost povjerljivih podataka od neovlaštenog pregledanja, preuzimanja, promjene i brisanja. Sistemi u realnom vremenu i „on - line" sistemi su izuzetno ranjivi, jer im se može pristupiti i preko terminala i preko operatora. Kontrola sigurnosti podataka može se postići tako što se pristup terminalima može fizički ograničiti na samo nekoliko ovlaštenih osoba.Također pomoću odgovarajućeg programa može se postaviti šifra ili se mogu dodijeliti različite privilegije odnosno mogu se odrediti različiti nivoi korištenja.

Provjera kvaliteta podataka ostvaruje se korištenjem neke od sljedećih metoda:

- provjera krajnjih korisnika i njihovih ocjena kvaliteta podataka;
- provjera cijelih baza podataka;
- ispitivanje uzoraka sa baza podataka.

Kao preporuka da bi se spriječili netehnički napadi i kako bi se povečao stepen zaštite od takvih vrsta napad jeste kontinuirani proces edukacije zaposlenih unutar Institucija.

6.1 Procjena i upravljanje rizicima kod informacionih sistema

Upravljanje rizicima je proces sistematske identifikacije rizika, analiza i ocjena njihovih uticaja i izrada i realizacija kompleksnih rješenja za upravljanje njima. Upravljanje rizicima je savremeni pristup koji obuhvata sve procese koji povećavaju efektivnost i produktivnost organizacije.

Upravljanje rizikom informacione sigurnosti sastoji se od trajnog procjenjivanja i obrade rizika, radi sprječavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa klasificiranim podacima. Obrada rizika je proces u kojem se za svaki procijenjeni rizik utvrđuje nivo prihvatljivosti rizika, radi njegovog prihvaćanja, smanjenja ili izbjegavanja.

Osnovna pitanja koja se razmatraju prilikom analize i upravljanju rizicima su:

- identifikacija rizika - prijetnji i ranjivosti;
- ocjena rizika - skale i kriterijumi, ocjena vjerovatnoće događaja i tehnologija mjerenja rizika - po dva ili tri faktora;
- izbor dozvoljenog nivoa rizika;
- izbor kontramjera i ocjena njihove efektivnosti.

U slučaju informacionih sistema moguće je razlikovati tri vrste rizika:

- rizike narušavanja povjerljivosti - kopiranje ili neovlašteno dostavljanje informacija;
- rizike dostupnosti - blokiranje informacija;
- rizike integriteta - modifikacija, negiranje originalnosti informacije ili unošenje lažne informacije.

Ocjena rizika informacione sigurnosti se provodi na jedan od dva moguća načina:

- putem ocjene usaglašenosti sa definiranjem skupa zahtjeva i preporuka za obezbjeđenje informacione sigurnosti, ili
- putem ocjene rizika informacione sigurnosti zasnovanih na ocjeni vjerovatnoće realizacije napada i veličine nastale štete.

Ocjena usaglašenosti sa definiranim skupom zahtjeva se vrši u odnosu na:

- normativno - pravne dokumente Institucija u oblasti informacione sigurnosti;
- zahtjeve postojećeg zakonodavstva;
- preporuke međunarodnih standarda ISO 17799 i ISO 27001;
- preporuke kompanija-proizvođača.

Ocjena rizika na osnovu procjene vjerovatnoće realizacije napada i veličine nastale štete podrazumijeva primjenu različitih statističkih, ekspertskih i sličnih metoda. U upotrebi su dva osnovna metoda ocjene rizika informacione sigurnosti:

- metod ocjene rizika zasnovan na modelu prijetnji i ranjivosti i
- metod ocjene rizika zasnovan na modelu informacionih tokova.

7. Tehničko - tehnološke mjere sigurnosti informacionih sistema

7.1 Fizička sigurnost

Mjere informacione sigurnosti fizičke zaštite određuju se zavisno od vrste, broja, oblika i načina skladištenja podataka, ovlaštenja za pristup podacima, kao i sigurnosne procjene mogućih rizika.

Mjere informacione sigurnosti fizičke zaštite su:

- uspostavljanje administrativnih zona;
- izrada plana fizičke zaštite;
- procjena efikasnosti mjera fizičke zaštite;
- kontrola lica;
- skladištenje podataka;
- fizička zaštita informacionih sistema.

Ove mjere informacione sigurnosti fizičke zaštite sprovode se radi:

- sprječavanja neovlaštenog ili nasilnog ulaska lica u objekte i prostorije u kojima se nalaze podaci odnosno uređaji sa podacima;
- sprječavanja i otkrivanja zloupotreba podataka od strane zaposlenih;
- otkrivanja i reagovanja na rizike.

Prostor u kojem se nalazi server, mrežna ili komunikaciona oprema informacionog sistema, organizira se kao administrativna zona. Kontrola pristupa u administrativnim zonama ostvaruje se provjerom identiteta za posjetitelje, a za zaposlenike uvidom u odgovarajuću službenu iskaznicu ili propusnicu, odnosno odgovarajućim automatskim sistemom kontrole pristupa.

Institucije za objekte ili prostor u kojem se vrši obrada podataka, izrađuju plan fizičke zaštite kojim se utvrđuje potreba sprovođenja mjera fizičke zaštite, u skladu sa standardima informacione sigurnosti. Institucije se dužne da sprovode kontrolu lica na ulazima i izlazima iz objekata ili prostora u kojima se nalaze podaci i o tome vode evidenciju, u cilju sprječavanja neovlaštenog iznošenja podataka ili sprječavanja unošenja nedozvoljenih predmeta, kojima se može ugroziti sigurnost podataka.

8. Administrativne mjere sigurnosti informacionih sistema

8.1 Registracija korisnika

Za sve zaposlene u Institucijama, koji na svom radnom mjestu koriste računar, potrebno je izvršiti registraciju korisnika i otvaranje korisničkog naloga. Procese otvaranja i zatvaranje korisničkog naloga potrebno je detaljno opisati kroz procedure za kontrolu pristupa sa pojašnjenjima standardnih mehanizama logičke kontrole pristupa za identifikaciju i autentifikaciju korisnika kao i za autorizaciju prava pristupa korisnika resursima sistema i mehanizmima za integraciju fizičke i logičke kontrole pristupa informacionim resursima.

Svaki pristup sistemu treba kontrolirati kroz proces registracije korisnika, koji uključuje:
- korištenje jednostavnih korisničkih imena, kako bi se korisnike moglo povezati s njihovim aktivnostima i učiniti ih odgovornim za iste;
- provjeru ovlaštenja korisnika za korištenje informacionog sistema ili servisa;
- provjeru da li dozvoljena razina pristupa odgovara poslovnim potrebama i da je u skladu s politikom sigurnosti;
- potpisivanje pisane izjave o upoznatosti sa pravima pristupa;
- osiguranje kojim se pružatelju usluge ne dozvoljava pristup dok nije proveden autorizacijski postupak;
- vođenje i redovno ažuriranje evidencije o registriranim korisnicima;
- trenutačno ukidanje prava korisnika;
- povremene provjere korisničkih imena i računa.

8.2 Upravljanje privilegijama

Kod davanja prava pristupa potrebno je primjenjivati princip davanja minimalnih privilegija. Minimum privilegija je sigurnosni zahtjev koji zaposlenima daje samo onoliko prava pristupa koliko je neophodno za obavljanje redovnih poslova, a da pri tom ne ometa poslovanje.

Potrebno je:

- identificirati privilegije i korisnike kojima se privilegije dodjeljuju,
- privilegije dodjeljivati pojedincima na osnovu potreba i situacija,
- obezbijediti minimalnu razinu privilegija potrebnih za normalno funkcioniranje,
- bilježiti sve dodijeljene privilegije,
- dodjeljivati privilegija pod novim korisničkim imenom.

8.3 Upravljanje korisničkim šiframa

Pristup bazi podataka dozvoljen je samo licima zaduženim za održavanje i razvoj informacionog sistema.

Pristup telekomunikacionom, računarskom i aplikativnom sistemu za obradu podataka, dozvoljen je uz upotrebu odgovarajućeg korisničkog imena i pripadajuće šifre. Korisničko ime i pripadajuća šifra ne smiju se otkriti i dati na upotrebu drugom licu.

Upravljanje sistemom korisničkog pristupa podrazumijeva razvoj, primjenu i održavanje informacionog sistema, na način koji omogućava prepoznavanje i pruža zaštitu identiteta korisnika. Institucije moraju da skladište sve podatke iz informacionih sistema na informatičke medije korištenjem metoda koje garantuju sigurnost, povjerljivost, integritet i dostupnost uskladištenih podataka.

Korisničku šifru potrebno je koristiti na ograničenom broju poslovnih procesa a koju je potrebno definirati procedurom za kontrolu pristupa. Administrator sistema postavlja inicijalnu šifru prilikom otvaranja naloga, dok je krajnji korisnik dužan šifru promjeniti odmah nakon prve uspješne autentifikacije sistemu. Krajnji korisnik je dužan da štiti povjerljivost šifre koju treba da pamti u periodu trajanja važnosti naloga. Svaki zaposleni je dužan da korisničku šifru mijenja poslije isteka perioda od tri mjeseca. Šifre se ne mogu dijeliti ni sa jednim drugim licem ni u kojem slučaju.

Na svakom računarskom sistemu treba da postoji jedan korisnik sa administratorskim privilegijama i šifrom koja je poznata samo administratorima sistema. Ovim nalogom administrator sistema može pomoći korisniku da se prijavi na sistem, ako korisnik zaboravi šifru.

Raspodjelu šifri treba kontrolirati kroz formalni proces upravljanja šiframa koji uključuje:

- potpisivanje izjave od strane administratora sistema, u kojoj se obavezuju da će čuvati šifre povjerljivima;
- obavezu da se šifre dostavljaju korisnicima na siguran način;
- izbjegavanje upotrebe elektronske pošte za saopštavanje šifre ili prenošenja putem treće osobe;
- izbjegavanje pohranjivanja šifri na računaru u nezaštićenom obliku.

Korisnici su obavezni prilikom korištenja šifri pridržavati se sigurnosnih uputa koje su definirane politikom sigurnosti. Kod korisnika mora postojati svijest da se šifrom potvrđuje njihov identitet, omogućavajući im time pravo pristupa do jedinica i servisa za obradu podataka.

Korisnici su dužni:

- čuvati povjerljivost šifri;
- ne zapisivati šifre na papire i ljepljive stikere i ne čuvati ih u blizini računara;
- šifre ne odavati drugim korisnicima, čak ni administratorima ili drugim odgovornim osobama;
- ne mijenjati šifre ukoliko sumnjaju na nepravilnosti u radu servisa, kao što je to primjer lažnog predstavljanja, socijalni inženjering i o tome obavijestiti administratora ili kontrolni organ;
- birati kvalitetne šifre, duge minimalno osam znakova, da nisu vezane uz imena, datume, telefonske brojeve i sl.;
- voditi računa da šifre sadrže i brojeve i slova, ako je moguće i specijalne znakove;
- izbjegavati ponovnu upotrebu starih šifri;
- izbjegavati šifre koje već koriste na drugim sistemima;
- redovito mijenjati šifre.

Osim odgovornosti nad pravilnim korištenjem šifri, korisnici su dužni i prikladno zaštititi opremu kada nisu u njezinoj blizini.

Svi korisnici moraju biti svjesni svojih odgovornosti nad zaštitom neosigurane opreme, što prvenstveno uključuje:

- da ukoliko se udaljavaju od računara za vrijeme radnog vremena, obavezno osiguraju računar primjerenim sigurnosnim mehanizmima (CTRL + L, screen saver s šifrom i sl.),
- da se prilikom gašenja računara prethodno odjave sa sistema, jer nije preporučljivo samo ugasiti terminal ili računar,
- preduzimanje mjera kojim se sprečava neovlašteno korištenje računara i terminala od strane trećih lica i to naručito kada nisu u upotrebi.

8.4 Praćenje upotrebe sistema

Kako bi se osiguralo da korisnici izvršavaju samo one aktivnosti za koje su ovlašteni, nužno je definirati postupke za praćenje korištenja jedinica za obradu podataka. Razinu praćenja pojedinih jedinica treba utvrditi kroz procjenu rizika.

Područja o kojima je potrebno voditi računa su:

- ovlašteni pristup - korisnička imena, datum i vrijeme događaja, tipovi događaja, datoteke kojima je pristupano, korišteni programi,
- privilegirane aktivnosti,
- neovlašteni pokušaji pristupa,
- sistemska upozorenja i greške.

Rezultate dobivene praćenjem potrebno je redovito pregledavati i analizirati. Učestalost pregleda ovisi o postojećim rizicima.

Faktore rizika koje treba razmotriti su:

- kritičnost aplikacija,
- vrijednost, osjetljivost i kritičnost informacija,
- iskustva o zloupotrebama, neovlaštenim upadima i sl.

Posebnu pažnju treba obratiti na sigurnost dnevnika zapisa o događajima. Prilikom dodjele odgovornosti za pregled dnevnika potrebno je razdvojiti uloge osoba koje obavljaju pregled i onih čije se aktivnosti prate. Također je potrebno omogućiti filtriranje zabilješki, iz razloga što dnevnici sadrže veliku količinu informacija od koje je većina nebitna za praćenje sigurnosti.

Dnevnike zapisa potrebno je zaštititi od aktivnosti kao što su:

- isključivanje sistema za zapisivanje;
- izmjene tipa zabilježenih informacija;
- izmjena ili brisanje podataka;
- prekida nadziranja zbog nedostatka diskovnog prostora i sl.

Sve nabrojane kontrole ne bi imale očekivani učinak ukoliko nije obavljeno sinhroniziranje računarskih satova. Dnevnici događaja služe kao dokaz u sudskim ili disciplinskim postupcima, te se isti, na način propisan drugim propisima, moraju osigurati i dostaviti svim strankama u postupku. Satove na računarskim ili komunikacijskim uređajima potrebno je podesiti na definirani standard, npr. lokalno standardno vrijeme, te moraju postojati mehanizmi koji će provjeravati i ispravljati varijacije.

8.5 Kontrolisanje pristupa lokalnoj mreži putem Interneta

Pristup lokalnoj mreži (u daljem tekstu: LAN) preko Interneta zahtjeva proces dodjele višeg nivoa privilegija. Računar sa koga se vrši pristup serveru virtuelne privatne mreže (u daljem tekstu: VPN server) mora da posjeduje validan digitalni certifikat, potpisan od strane povjerljivog certifikacionog tijela, sa kojim vrši potvrdu svog identiteta.

VPN server vrši autentifikaciju računaru koji zahtjeva VPN pristup svojim validnim digitalnim certifikatom potpisanim od strane povjerljivog certifikacionog tijela.

Zaposleni koji uspostavlja VPN konekciju autentifikuje se VPN serveru upotrebom digitalnog certifikata i mora pripadati grupi koja ima pravo na ostvarivanje VPN konekcije. Neophodno je strogo voditi računa o malicioznim kodovima i neodgovarajućim materijalima prilikom preuzimanja informacija i fajlova sa Interneta.

8.6 Razdvajanje (separacija) u internim mrežama IKT sistema

Kontrolu pristupu internim mrežama sistema i minimizaciju vanjskih utjecaja sa Interneta treba izvršiti segmentacijom sistema na funkcionalne cjeline. Arhitekturu sistema informaciono-komunikacione tehnologije (u daljem tekstu: IKT) treba dizajnirati tako da izdvaja segmente sistema koji podržavaju relativno nezavisne funkcionalne cjeline.

U prvom segmentu obavezno uspostaviti demilitarizovanu zonu za komunikaciju sa javnom mrežom - Internetom. U ovoj zoni treba da se nalaze svi publikovani javni servisi Institucija. Ovaj segment mreže komunicira sa vanjskim sistemima i treba ga kontrolisati i nadgledati firewall servisima na mrežnoj kapiji kroz koje prolazi cjelokupni promet. Iza ovog firewall treba instalirati detektor upada u internu mrežu koji detektuje sve napade na mrežu, ali i slabosti konfigurisanja graničnog firewall. Dodatni nivo zaštite može se obezbjediti izolovanjem demilitarizovane zone internim firewall u odnosu na interni segment mreže.

Drugi segment mreže predstavlja produkcioni dio sistema. U okviru ovog segmenta nalaze se svi korisnici, računari i interni servisi. Segment je potrebno izolovati firewall serverom od ostalih mreža, da se kompletna komunikacija registruje i nadgleda.

Treći segment mreže predstavlja domen za razvoj i testiranje novih aplikativnih rješenja. Ovaj segment treba izdvojiti u zaseban domen, u okviru internog segmenta mreže, a svi korisnici u okviru ovog domena imaju uloge koje zaposleni preuzimaju u procesu razvoja i prilikom testiranja rješenja.

Četvrti segment mreže obezbjeđuje tehničku podršku IKT sistemima Institucija za testiranje uspostavljenih aplikativnih rješenja u izolovanom okruženju kroz ograničene pilot-projekte.

8.7 Identifikovanje opreme u mrežama Institucija

Svaki mrežni uređaj u IKT sistemu Institucija treba da ima jedinstvenu IP adresu. Dodjeljivanje adresa računarima krajnjih korisnika, štampačima i bežičnim pristupnim tačkama treba da se vrši dinamički, dok serverske stanice treba da imaju statičke adrese. Ukoliko postoji potreba, treba konfigurisati rezervaciju adresa (adresa se dinamički dodjeljuje, ali je uvijek ista). U logovima sistema svakog računara potrebno je zapisivati svaku promjenu adrese. Filtriranje pristupa po IP adresi potrebno je implementirati kod kritičnih servisa infromacionog sistema.

8.8 Implementacija politike kontrole pristupa

Prilikom implementacije politike kontrole pristupa potrebno je razmotriti sljedeće:

- može li nedostatak odgovarajućih standarda za kontrolu pristupa informacijama i sistemima dovesti do neusklađenosti i slabosti, što može biti zloupotrebljeno ili iskorišteno u druge svrhe;
- da li će rizik od narušavanja povjerljivosti značajno porasti ako kontrola pristupa nije prilagođena da odgovori na povećanu osjetljivost informacija u obradi;
- mogu li standardi za kontrolu pristupa koji su previše strogi ili previše fleksibilni ometati svakodnevne aktivnosti Institucija i zaposlenih.

8.9 Kontrolisanje pristupa mreži

Svaki servis u okviru IKT sistema Institucija treba štititi sa implementiranim autentifikacionim i autorizacionim mehanizmima. Zaposleni mora da pripada grupi koja ima pravo na korištenje servisa ili da to pravo isključivo dobije pokretanjem procesa dodjele novih privilegija.

Kontrola pristupa internim i eksternim mrežnim servisima je nužna kako bi se spriječilo kompromitiranje sigurnosti od strane korisnika koji imaju pristup mreži i mrežnim resursima.

Sigurnost mrežnih servisa potrebno je provesti kroz:

- osiguranje odgovarajućih interfejsa,
- osiguranje mehanizama za provjeru vjerodostojnosti korisnika i opreme,
- kontrolu korisničkog pristupa do informacionih servisa.

Jedan od koraka uspostave sigurnosti pristupa mreži je definiranje putanje prema kojoj korisnici smiju pristupiti samo onim servisima za koja imaju uređena prava pristupa. Ukoliko korisnik nema definirana prava pristupa, pristup servisu je zabranjen. Kako bi zabrana ili dozvola pristupa bila moguća, potrebno je implementirati kvalitetne kontrole identifikacije i autorizacije, te definirati procedure za zaštitu pristupa mrežnim servisima.

Definiranje propisanog puta od terminala do servisa sigurnosna je kontrola koja sprječava zlonamjernog korisnika da karakteristiku mreže - maksimalno dijeljenje resursa, iskoristi za neautorizirani pristup aplikacijama i uređajima za obradu podataka. Definiranjem propisane putanje korisniku, moguće je birati samo propisane putanje od terminala do servisa i to po principu kontrole unaprijed dopuštene putanje na svakom čvoru.

Kako bi se osigurala dobro propisana putanja potrebno je izvršititi:

- dodjelu stalnih linija,
- automatsko spajanje ulaza na određene aplikacije,
- limitiranje opcija u izbornicima za određenu grupu korisnika,
- kao i sve druge vrste aktivnih kontrola.

8.10 Osiguranje povjerljivosti, integriteta i autentičnosti podataka

Kriptografske metode predstavljaju drugi način ograničavanja pristupa podacima i naručito su značajne kada se povjerljivi podaci šalju računarskom mrežom. Tehnike enkripcije određuju koliko će proces biti složen. Kriptografske metode mogu osigurati i pomoći u ostvarenju i očuvanju:

- povjerljivosti izvornog teksta – sprječava neovlašten uvid u sadržaj izvornog teksta,
- integriteta izvornog teksta – sprječava neovlašteno mijenjanje sadržaja izvornog teksta, te slučajno ili namjerno oštećenje ili brisanje,
- autentičnosti izvornog teksta – osiguranje vjerodostojnosti sadržaja poruke.

Kriptografske metode potrebno je definirati kako bi se omogućila zaštita povjerljivosti, autentičnosti i integriteta informacija. Ove metode potrebno je koristiti kod rizičnih, osjetljivih i povjerljivih podataka. Politikom sigurnosti informacija određuju se tehnike kriptografije koje će se koristiti, način čuvanja i raspodijele ključeva, na koji način će se ostvariti digitalni potpis i sl., a koje moraju da budu u skladu s važećim zakonodavnim restrikcijama i pravima upotrebe. Metode za obezbjeđenje povjerljivosti, autentičnosti i integriteta odobravaju se od strane nadležnog organa.

8.11 Osiguranje operacijske sigurnosti

Operacijska sigurnost uključuje dva aspekta sigurnosti informacionih sistema. Prvi se odnosi na povećanje svijesti među potencijalnim žrtvama, a drugi predstavlja načine na koji se mogu spriječavaju eventualne zloupotrebe.

Povećanje svijesti postiže se tako da kad god je to moguće zaposlenici budu uključeni u sigurnosni program. U cilju uključivanja u sigurnosni program potrebno je zaposlene educirati na koji način sigurnost može biti ugrožena i kako svi dijele rizik i odgovornost. Jednom kada se analiziraju rizici sistema, potrebno je odrediti količinu informacija koja će se podijeliti sa zaposlenicima. Povjerljive informacije neće biti dostupne svima, već samo malom broju osoba kojima su one nužne za obavljanje poslova.

9. Standardi informacione sigurnosti i njihova usklađenost sa mjerama sigurnosti informacionih sistema

U svrhu implementacije informacione sigurnosti na tržištu su se pojavili standardi za sigurnost informacionih sistema. Dva najpoznatija standarda za sigurnost informacionih sistema su ISO/IEC 17799 i ISO/IEC 27001, koji se međusobno ne isključuju i koje je nužno koristiti u cilju uspostavljanja kvalitetnog sistema upravljanja sigurnošću informacija.

Bosna i Hercegovina preuzela je oba standarda pod imenima BAS ISO/IEC 17799:2007 (Informaciona tehnologija - Sigurnosne tehnike - Pravilo dobre prakse za upravljanje sigurnošću informacija) i BAS ISO/IEC 27001:2007 (Informaciona tehnologija - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi).

Mjere informacione sigurnosti usaglašena su sa standardima:

- BAS ISO/IEC 17799:2007 (Informaciona tehnologija - Sigurnosne tehnike - Pravilo dobre prakse za upravljanje sigurnošću informacija)
- BAS ISO/IEC 27001:2005(E) (Informaciona tehnologija - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi), Anex A

10. Uloge i odgovornosti

Rukovodstvo Institucija odgovorno je za uspostavljanje standarda za kontrolu pristupa informacionim objektima, kontrolu pristupa korisnika Internetu, kao i za obuku korisnike u cilju podizanja svijesti o postojanju prijetnji, što doprinosi smanjenje rizika od računarskih incidenata.

IKT odjeljenje odgovorno je za implementaciju prava pristupa kroz formiranje grupa korisnika, izradu matrice prava pristupa i obuku krajnjih korisnika. Krajnji korisnici odgovorni su za čuvanje šifri i drugih identifikacionih parametara za pristup sistemu.

O B R A Z L O Ž E NJ E

I PRAVNI OSNOV

Pravni osnov za donošenje ove Odluke sadržan je u članu 17. Zakona o Vijeću ministara Bosne i Hercegovine („Službeni glasnik BiH“, broj 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) prema kojem, Vijeće ministara Bosne i Hercegovine u ostvarivanju svojih prava i ovlaštenja donosi odluke.

Članom 3. Odluke o usvajanju Politke softvera u Institucijama Bosne i Hercegovine Hercegovine, a u vezi sa tačkom 3.8. Politike softvera u Institucijama Bosne i Hercegovine ("Službeni glasnik BiH", broj 143/07) predviđeno je donošenje dokumenta o tehničko-tehnološkim standardima informacionih sistema u Institucijama Bosne i Hercegovine.

II RAZLOZI ZA DONOŠENJE

Donošenje Dokumenta je zakonska obaveza utvrđena na 23. sjednici Vijeća ministara Bosne i Hercegovine Odlukom o usvajanju Politike softvera u Institucijama Bosne i Hercegovine, broj 143/07 od 20.9.2007. godine,a koja je donešena na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine („Službeni glasnik BiH“,broj 30/03, 42/03, 81/06), u skladu sa Strategijom razvoja informacionog društva Bosne i Hercegovine, Politikom razvoja informacionog društva u Bosni i Hercegovini i Akcionim planom razvoja informacionog društva u Bosni i Hercegovini, usvojenim na 69. sjednici Vijeća ministara Bosne i Hercegovine, održanoj 16.11.2004. godine.

Sigurnost informacionih sistema danas je nezaobilazna tema kojoj se posvećuje mnogo pažnje. Zaštita je postala moralna i poslovna obaveza, te neophodan postupak pri osmišljavanju i izgradnji informacionih sistema. Kako bi se olakšala implementacija sigurnosti u organizaciji, na tržištu su se pojavili standardi vezani uz sigurnost informacionih sistema. Implementacija sigurnosnih kontrola po standardima ne samo da onemogućava previd pojedinih kontrola, već je i dokaz kvalitete uspostavljenih sigurnosnih kontrola.

Cilj donošenja dokumenta o tehničko-tehnološkim i administrativnim mjerama za sigurnosti informacionih sistema Institucija Bosne i Hercegovine ogleda se u zaštiti podataka na fizičkom, tehničkom i organizacionom nivou za što je potrebno definirati tehničke i administrativne mjere zaštite informacionog sistema, zatim utvrđivanje i provjera korisnika sistema i njihovih prava pristupa podacima i modulima sistema, bilježenje pristupa, autentifikacija vlasnika dokumenata, kriptografija i algoritmi enkripcije kojima se štiti komunikacija između web servisa.

III OBRAZLOŽENJE PREDLOŽENIH RJEŠENJA

Članom 1. ove Odluke definisan je predmet Odluke.

Članom 2. ove Odluke utvrđen je djelokrug primjene Dokumenta o tehničko-tehnološkim i administrativnim mjerama za sigurnost informacionih sistema u Institucijama Bosne i Hercegovine.

Članom 3. ove Odluke propisano je stupanje na snagu i objava Odluke.

IV FINANSIJSKA SREDSTVA

Za realiziranje ove Odluke nije potrebno izdvojiti sredstva iz Budžeta institucija i međunarodnih obaveza Bosne i Hercegovine za 2013. godinu.

V OPIS KONSULTACIJA VOĐENIH U PROCESU IZRADE PROPISA

O Prijedlogu odluke pribavljena su pozitivna mišljenja Ministarstva finansija i trezora Bosne i Hercegovine, Ministarstva pravde Bosne i Hercegovine i Ureda za zakonodavstvo Vijeća ministara Bosne i Hercegovine.