UDRUŽENJE INŽENJERA SAOBRAĆAJA I KOMUNIKACIJA
U BOSNI I HERCEGOVINI

Stručni skup:

„SIGURNOST I ZAŠTITA U SAOBRAĆAJU, TRANSPORTU I KOMUNIKACIJAMA U BIH”

Zenica, 07.06.2014. g.

ZBORNIK RADOVA

Priredio Prof. dr. Osman Lindov

2014

Sarajevo, 2014.

Nejra Mujić,MA-dipl.inž.saob i kom.

„SIGURNOST I ZAŠTITA INFORMACIJSKO-KOMUNIKACIJSKIH SISTEMA“

„SECURITY AND PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS“

Nejra Mujić, MA-dipl.inž.saob. i kom.

SAŽETAK: Ovaj rad obrađuje temu sigurnost i zaštita IKS-a (informacijsko-komunikacijskih sistema). Bit će obrađeni samo neki od aspekata zaštite i sigurnosti IKS-a, radi njihove prevelike obimnosti. Moderni informacijsko-komunikacijski sistemi svakim danom postaju sve veći i kompleksniji te je iz tog razloga znatno otežan njihov nadzor i održavanje zadovoljavajuće razine sigurnosti.

KLJUČNE RIJEČI: Sigurnost, zaštita, informacijsko-komunikacijski sistem

ABSTRACT: This article discusses the topic „safety and security aspects of ICS (information and communication systems). Only some of the aspects of safety and security of ICS will be processed, due to its excessive extensiveness. Modern information and communication systems becomes bigger and more complex with each passing day and this is why their supervision and maintenance of a satisfactory level of safety are hindered.

KEY WORDS: Security, protection, information and communication system

UVOD

Sigurnost informacija postaje sve važnija u modernom društvu. Protok velike količine informacija izlaže ih brojnim prijetnjama. Sigurnost informacijsko-komunikacijskih sistema podrazumijeva niz mjera i aktivnosti koje se poduzimaju kako bi se osiguralo njegovo normalno funkcioniranje, spriječila zloupotreba njegovih resursa i osigurao autorizirani pristup podacima. Zbog raznih vrsta napada na IKS sistem, potrebno je koristiti određene mjere zaštite. IKS je kompleksan, umrežen sistem koji omogućava prikupljanje, obradu, pohranjivanje i prenos različitih oblika informacija (kao što su: podaci, govor, slika, video, multimedija).

Najčešće prijetnje računarsko-komunikacijskom sistemu predstavljaju ljudi. Te prijetnje mogu biti nezlonamjerne i zlonamjerne prijetnje. Motivi napadača su raznovrsni, od bezazlenih do najopasnijih. To su: znatiželja, dokazivanje, zabava, korist i osveta.

Da bi informacioni sistem bio zaštićen na zadovoljavajući način, potrebno je uspješno planirati, implementirati i nadzirati sve neophodne mjere zaštite. Proces sigurnosti se zasniva na četiri koraka: procjena, zaštita, otkrivanje i odgovor.

Slojevita zaštita je jedna od najefikasnijih i najraširenijih strategija, koja se zasniva na formiranju zaštitnih slojeva (ili prstenova) oko sistema. Ti slojevi zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima.

Metode zaštite IKS-a su: firewall, prisluškivanje žičnih komunikacija, autentifikacija, autorizacija, biometrijska identifikacija, kriptiranje, digitalni potpis, digitalni certifikat, sigurnost podataka i zaštita od zlonamjernih programa.

1. INFORMACIJSKO-KOMUNIKACIJSKI SISTEM

Informacijsko-komunikacijski sistem- IKS je kompleksan, umrežen sistem koji omogućuje prikupljanje, obradu, pohranjivanje i prenos različitih oblika informacija (podaci, govor, slika, video, multimedija). Postoje još mnoge definicije informacijsko-komunikacijskog sistema ovisno o aspektu promatranja. Informacijski sistem je sistem koji prikuplja, pohranjuje, čuva, obrađuje, i isporučuje potrebne informacije na način da su dostupne svim članovima neke organizacije koji se njima žele koristiti.

Internet je globalni informacijsko - komunikacijski sistem. On je svjetska, odnosno globalna računarska mreža. Ta mreža povezuje mnoge računare i računarske mreže u jednu cjelinu, s namjerom razmjene podataka i korištenja raznih sadržaja, usluga i servisa kao štu su: www, elektronska pošta i slični.

Korištenje IKS-a zahtijeva sljedeća temeljna načela:

- Efikasnost (koja se odnosi na: pravovremenost informacija, dostupnost informacija i valjanost informacija)
- Sigurnost (potrebno je obezbijediti što bolju sigurnost i zaštitu računarskih mreža)
- Ekonomičnost (koja podrazumijeva veće koristi od troškova)

IKS zahtijeva konvergenciju sistema. Povezivanje različitih usluga (telefonija, televizija, Internet itd.) u jedinstvenu digitalnu mrežu naziva se konvergencija. Do sada odvojeni sistemi su imali jedan princip rješavanja problema sigurnosti i zaštite. Konvergencija zahtijeva novi pristup rješavanju problema sigurnosti i zaštite na fizičkoj, organizacijskoj i pravnoj razini.

2.PRIJETNJE I NAPADI NA INFORMACIJSKO-KOMUNIKACIJSKI SISTEM

2.1. Tipovi napadača na informacijsko-komunikacijski sistem

Najčešće prijetnje računarsko-komunikacijskom sistemu predstavljaju ljudi. Te prijetnje mogu biti nezlonamjerne i zlonamjerne.
Nezlonamjerne prijetnje se najčešće javljaju kod zaposlenika u nekom sistemu ili kod osoba koje su u posjeti sistemu, a nisu pod nadzorom ovlaštenih osoba na adekvatan način.
Zlonamjerne prijetnje prouzrokovane ljudskim faktorom su radnje kojima se ugrožava ili narušava sigurnost računarsko-komunikacijskih sistema. Te radnje se izvršavaju iz određenih razloga i sa određenim namjerama.
Napadači mogu biti:

- unutarnji napadači, nezadovoljni ili zlonamjerni korisnici sistema,
- vanjski napadači, koji nisu korisnici sistema i namjera im je nanijeti štetu i unijeti razdor u organizaciju

Motivi napadača su raznovrsni, od bezazlenih do najopasnijih. To su: znatiželja, dokazivanje, zabava, korist i osveta. Tipovi napadača su: hakeri, krekeri, frikeri i računarski kriminalci.

Hakeri su osobe koje uživaju u učenju detalja o računarskim sistemima i proširivanju svog znanja i sposobnosti-obrnuto od većine korisnika računara, koji radije uče samo minimum onoga što im je potrebno. Oni ugrožavaju računarske sisteme unutar ili izvan organizacije u zavisnosti od toga jesu li unutrašnji ili vanjski hakeri.

Krekeri su osobe s većim stepenom znanja u odnosu na hakere. Specijalizirani su za provaljivanje u tuđe računarske sisteme, u većini slučajeva iz koristoljublja.

Frikeri su dobili naziv od riječi „phreaking“=phone + breaking. Dakle, to su osobe koje su fokusirane na telefonske sisteme. Frikeri mogu preko računarskih friker programa naizmjenično pozvati sve moguće kombinacije brojeva dok ne dobiju pravu kombinaciju za pristup određenom telefonu.

Računarski kriminalci napadaju računare vlada i visoko pozicioniranih državnih tijela kao što su: MUP, vojska i dr.

2.2. Najčešće primjenjivi napadi i prijetnje na informacijsko-komunikacijski sistem

Napadi su akcije koje su usmjerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža. Osnovne kategorije napada su:
a) Presijecanje, prekidanje
b) Presretanje
c) Izmjena
d) Proizvodnja

2.2.1. Maliciozni računarski programi

Maliciozni računarski programi ili zlonamjerni programi su programi napravljeni u namjeri da na bilo koji način oštete ili onemoguće i otežaju korištenje umreženih ili neumreženih računara. Maliciozni programi mogu raditi neprimjetno u pozadini, ili usporiti računar i periodično izazvati kočenje ili obaranje sistema.

Virusi: Najpodmuklija i najopasnija vrsta malicioznih programa su virusi. Oni imaju sposobnost kopirati se i zaraziti računar bez dopuštenja ili znanja korisnika. Virus se može širiti putem računarskih mreža s jednog računara na drugi zaraženim datotekama. Osim mreža virusi se prenose i preko USB memorije, CD/DVD-a i ostalih načina pomoću kojih se datoteke mogu prenositi sa računara na računar.

Trojanski konji: Trojanski konj je program u kojem se nalazi skriveni zlonamjerni ili štetni kod kako bi lakše zaobišao antivirusnu provjeru. To su zlonamjerni programi koji se maskiraju i predstavljaju kao korisni programi kako bi se korisnici prevarili. Trojanac može da bude zlonamjerni crv upakovan u formu programa za instalaciju manje aplikacije.

Logičke bombe: Logička bomba je zlonamjerni kod koji je ugrađen u neki koristan program, koji se aktivira tek kada se ispune određeni uslovi. Ti uslovi mogu biti određeno vrijeme ili određeni datum, ukoliko na disku postoji određena datoteka ili ako se na sistem prijavi određeni korisnik. Mogućnosti zlonamjernih bombi su praktično neograničene.

Crvi: Crvi su samostalni programi koji koriste mrežu za slanje svojih kopija na ostale računare unutar mreže ili Interneta bez intervencije korisnika. Crvi se mogu klasificirati prema metodama širenja, načinu instaliranja i pokretanja i prema karakteristikama kojima se opisuje zlonamjerni softver. Crvi se prenose preko e-pošte, instant poruka, dijeljenja datoteka i razmjene datoteka između ravnopravnih računara.

2.2.2. Neželjena elektronska pošta (spam)

Neželjena elektronska pošta (spam) jedan je od najvećih problema na Internetu. Spamer mora saznati e-mail adrese potencijalnih primatelja da bi mogao poslati spam. Sakupljanje adresa obavlja se bez znanja njihovih vlasnika. Jedna spam poruka može biti poslana na milion različitih adresa, od kojih je većina nepostojeća, krivo napisana ili se više ne upotrebljava.

2.2.3. DoS napadi

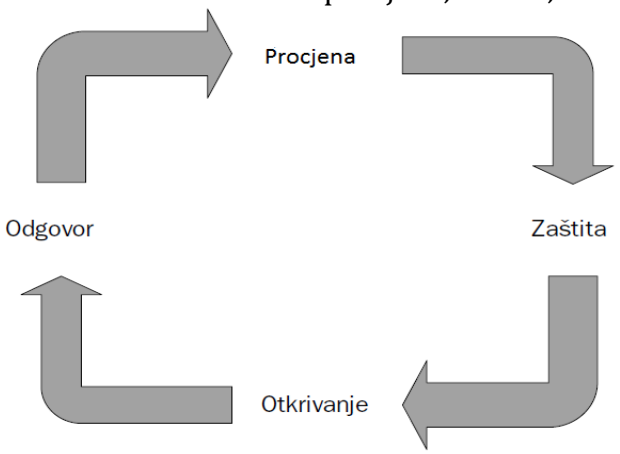
DoS napad ili napad s uskraćivanjem usluge je pokušaj stvaranja resursa računara nedostupnim ili nekorisnim za legalne korisnike. Ovaj tip napada nužno ne rezultira krađom informacija ili bilo kojim drugim materijalnim gubitkom. Iako najčešće namjerni i zlonamjerni, DoS napadi mogu se dogoditi i sasvim slučajno. Napadači DoS napade izvršavaju da bi se međusobno dokazali ili da bi nanijeli štetu napadnutim organizacijama.

2.2.4. Raspodijeljeni napadi (DDoS)

Distribuirani napad uskraćivanja usluga (DDoS – Distributed Denial of Service) su napadi koji su zasnovani na korištenju više računara kao izvora napada, pri čemu jedan računar predstavlja žrtvu. DDoS napadi predstavljaju provaljivanje u stotine ili hiljade računara putem Interneta. Zatim napadač instalira DDoS program na sve njih i time dobije kontrolu nad njima za pokretanje koordiniranog napada na krajnju žrtvu. Ovi napadi mogu dovesti do prekida povezanosti mreže i korisnika.

3. SIGURNOST I ZAŠTITA INFOROMACIJSKO-KOMUNIKACIJSKIH SISTEMA

Sigurnost je proces održavanja prihvatljivog nivoa rizika. Sigurnost je proces, a ne konačan proizvod, jer se ne može kupiti. To je proces u kome se koriste različiti proizvodi i usluge, procedure i pravila. Da bi informacioni sistem bio zaštićen na zadovoljavajući način, potrebno je uspješno planirati, implementirati i nadzirati sve neophodne mjere zaštite.
Proces sigurnosti se zasniva na četiri koraka: procjena, zaštita, otkrivanje i odgovor.



Slika 1: Sigurnost kao proces

Ciljevi sigurnosti su: povjerljivost, cjelovitost (integritet) i raspoloživost. Oni čine tzv. „veliko trojstvo“, a na engleskom jeziku, skraćenica za ovaj termin je CIA (Confidentiality, Integrity, Availability).

Sigurnosna arhitektura informacionog sistema je osnova za provođenje sigurnosne politike svake organizacije. Profesionalci iz oblasti sigurnosti trebaju da razumiju računarske arhitekture, zaštitne mehanizme, sigurnosne probleme distributivnih sistema i modele koji daju okvir za sigurnosnu politiku.

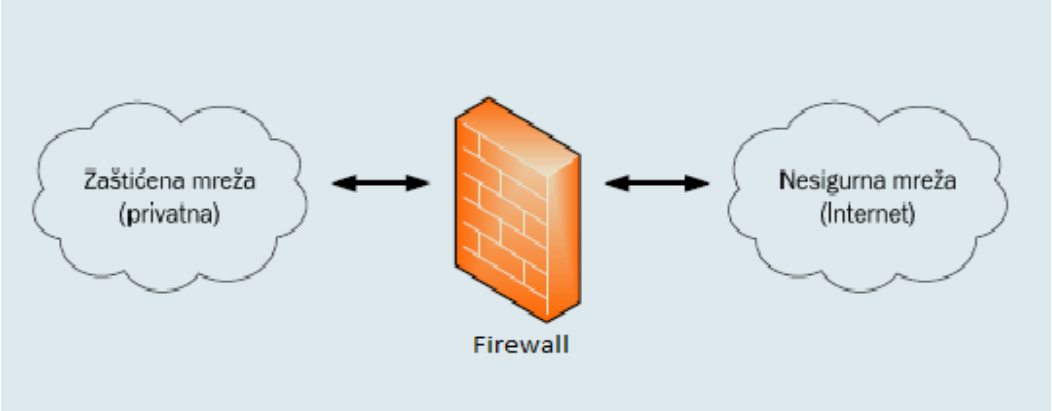
3.1. Metode zaštite informacijko-komunikacijskih sistema

3.1.1. Sigurnost mreže

Povezivanje mreže na Internet i direktna veza sa svijetom, predstavlja stalnu prijetnju za sistem i pruža mogućnost napadačima da koriste različite bezbjednosne propuste i

provale u sistem. Postoje dvije metode zaštite sigurnosti mreže: Firewall i Prisluškivanje žičnih komunikacija.

Firewall: Firewall ili mrežna barijera ili vatrozid predstavlja mehanizam zaštite u računarskim mrežama. To je softverski ili hardverski proizvod koji provjerava pakete koji dolaze do njega i na osnovu unesenih pravila, propušta ili odbija te pakete. Ako je hardwerski, firewall se često sastoji samo od rutera. Ruteri su specifični po tome što imaju mogućnost da bilježe IP adrese. Ovaj proces bilježenja adresa omogućava definiranje kojim je IP adresama dozvoljeno spajanje, a kojima ne. Druge implementacije se sastoje od jednog i drugog, hardwera i softwera. Dakle svrha firewall-a je da filtrira pakete, tj mogućnost da diskriminira ili da odbije pristup baziran na IP adresi. Firewall se obično nalazi na ulazu u mrežu, tj. između unutrašnje i spoljašnje mreže, tako da se cjelokupan saobraćaj mora odvijati preko njega. Na slici 2. je prikazan firewall u funkciji filtera na relaciji lokalne tj. privatne mreže i Interneta.



Slika 2: Firewall ili mrežna barijera vezuje privatnu i javnu mrežu

Firewall održava što bezbjedniju vezu sa spoljašnjom mrežom, tako što svaki pokušaj povezivanja privatnih i vanjskih mreža ispituje i nakon toga odobrava ili odbija povezivanje.
Najčešće funkcije firewall-a su:

- *Filtriranje paketa* – Zaglavlje paketa se analizira i upoređuje sa pravilima firewalla. Odbacuje ili dozvoljava prolaz paketa koji nisu u skladu sa pravilima.
- *Prevođenje mrežnih adresa. (Network Address Translation, NAT)* - Prevodi IP adrese računara u privatnoj mreži i na taj način sakriva identitet računara u lokalnoj mreži.
- *Proxy servisi* – Sloj između vanjske i unutrašnje mreže, koji omogućava većem broju računara da dijele jednu vezu ka Internetu i skladišti podatke, predstavlja proxy server. Dakle, proxy serveri uspostavljaju veze na aplikacijskoj razini za računare unutar mreže sa ciljem kompletnog prekidanja veze između hostova unutar i izvan mreže.

U dodatne funkcije firewall-a spadaju:

- *Kriptirana autentifikacija*- omogućuje korisnicima javne mreže da dokažu svoj identitet firewall-u.
- *Virtuelno privatno umrežavanje*- uspostavljanje kriptografski zaštićene veze između dvije privatne mreže preko javnog nesigurnog medija poput Interneta.

Mreža zaštićena firewall-om, ipak neće u potpunosti biti imuna na sve vrste nedozvoljenog pristupa. Firewall ne pruža adekvatnu zaštitu protiv virusa, već je za to neophodna i upotreba posebnih anti-virus programa.

3.1.2. Sigurnost pristupa

Sigurnost pristupa se osigurava: autentifikacijom, autorizacijom i biometrijskom identifikacijom.

Autentifikacija: Autentifikacija predstavlja proces provjere korisničkog identiteta, odnosno da li je korisnik zaista onaj za kojeg se predstavlja. Provjera identiteta korisnika se može izvoditi na sljedeće načine:

- šta „korisnik zna“ (lozinka, PIN, itd.),
- šta „korisnik posjeduje“ (pametna kartica, token, itd.),
- šta „korisnik jeste“ (biometrijski podaci)
- ili kombinacijom navedenih načina.

Proces autentifikacije predstavlja prvi korak prilikom prijave korisnika u sistem.

Autorizacija: Pravo korištenja podataka, informacija i drugih resursa određenog sistema, imaju samo autorizirani korisnici. Autorizacija može biti bez ograničenja, i može biti selektivna. Tj. ograničena samo na pravo pristupa do određenih podataka i informacija.

Proces autorizacije predstavlja davanje skupa ovlasti autentificiranim korisnicima. Proces autorizacije osigurava:

- da samo autorizirani korisnici smiju obavljati radnje koje su dozvoljene unutar njihovih ovlasti
- upravljanje pristupom zaštićenim resursima odlučivanjem na temelju uloge ili razini ovlasti
- spriječavanje napada podizanjem razine ovlasti korisnika.

Biometrijska identifikacija: Biometrija je skup metoda za identifikovanje pojedinaca na osnovu bioloških karakteristika i/ili karakteristika ponašanja. Biometrijska provjera identiteta predstavlja postupke prikupljanja i analiziranja fizičkih karakteristika, kao što su: otisci prstiju i snimak rožnjače oka, i drugih karakteristika koje se teško mogu oponašati kao npr. rukopis. Te karakteristike se prikupljaju korištenjem specijalnih uređaja i analiziraju pomoću programa koji se oslanjaju na principe umjetne inteligencije.

Postoje dvije vrste biometrijskih tehnika: fizička biometrija i biometrija ponašanja. Fizička biometrija se bavi uzrokovanjem fizionomije ljudskoga tijela i njegovim jedinstvenim karakteristikama. To su: otisak prsta, rožnjača oka, geometrija šake, prepoznavanje lica i DNK. Biometrija ponašanja opisuje fizičke karakteristike čovječijeg tijela koje su dijelom jedinstvene za svaku osobu. To su: prepoznavanje glasa, prepoznavanje rukopisa i potpisa i dinamika kucanja.

3.1.3. Sigurnost poruka i transakcija

Kod obavljanja transakcija posredstvom Interneta i slanja poruka e-poštom postoji ozbiljna opasnost:

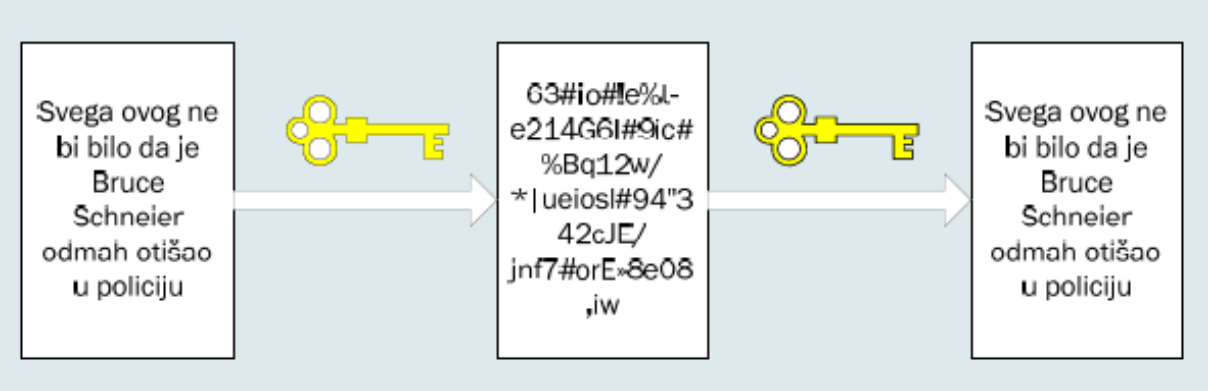
- da neko nepozvan dođe do sadržaja poruke ili transakcije,
- da promijeni sadržaj poruke ili transakcije,
- da se prikaže da je on neko drugi i u njegovo ime obavlja transakcije za koje nije ovlašten.

Postoje slijedeće tehnike koje omogućavaju sigurnost poruka i transakcija: kriptiranje, digitalni potpis i digitalni certifikat.

Kriptiranje: Kriptografija znači „skriveno pisanje“. Kriptografija je nauka koja se bavi metodama očuvanja tajnosti informacija.

Šifrovanje predstavlja matematičke postupke modifikacije podataka, tako da šifrovane podatke mogu pročitati samo korisnici sa odgovarajućim ključem. Otvoreni tekst, tj. originalna poruka ili datoteka se pomoću ključa transformiše u zaštićen, šifrovan tekst, tj. šifrat.

Dešifrovanje predstavlja obrnut proces, tj. šifrovani podaci se pomoću ključa transformišu u originalnu poruku ili datoteku.
Šifrovani podaci su zaštićeni od neovlaštenog korinika.



Slika 3: Šifrovanje i dešifrovanje podataka

Digitalni potpis: Digitalni potpis je elektronska verzija potpisa, koja se primjenjuje da bi se identifikovao pošiljalac i dokazala vjerodostojnost poruke. Digitalni potpis liči na potpis rukom. Ako se pravilno implementira, nemoguće ga je falsificirati, daje dosta veliku sigurnost da je poruka došla od stranke čiji se potpis nalazi na poruci. Zatim garantuje da poruka nije bila mijenjana od trenutka potpisa do primanja i čitanja same poruke.

Digitalni certifikat: Digitalni certifikat je potvrda u elektronskom obliku koja povezuje podatke za verificiranje elektronskog potpisa s nekom osobom i potvrđuje identitet te osobe. Ovjera certifikata je digitalni potpis, ali se potpisom ne ovjerava cijeli certifikat, nego samo veza između identiteta korisnika i javnog ključa. Dakle, certifikat je javni ključ sa opisom identiteta korisnika i potpisom koji je izdala strana kojoj se vjeruje. Digitalni certifikati se koriste za identifikaciju pojedinca, servera ili kompanije.

3.1.4. Sigurnost podataka

Sigurnost podataka predstavlja proces kojim se osiguravaju podaci od mijenjanja pri prijenosu i kontrolira pristup podacima u računaru. Na taj način sigurnost i zaštita podataka osigurava privatnost. Privatnost podataka je važna kako za privatne, tako i za javne podatke. Da bi podaci na svoje odredište stigli netaknuti i u istom obliku u kojem su poslani, štite se od oštećenja u prijenosu i neovlaštenih napada ili preusmjeravanja tokom prijenosa. Metode zaštite podataka su: enkripcija podataka, sigurnosne kopije, maskiranje podataka i brisanje podataka.

Enkripcija podataka: Enkripcija podataka je tehnologija za zaštitu podataka koja šifrira tj. mijenja podatke na tvrdom disku, tako da se podaci čine nečitljivim za osobe koje ne posjeduju ključ. Na taj način se dobija šifrovana informacija. Da bi podaci postali razumljivi i upotrebljivi, potrebno je da se dekodiraju.

Sigurnosne kopije: Backup ili sigurnosna kopija je kopija podataka koja se izrađuje u svrhu osiguranja u slučaju oštećenja ili gubljenja izvornih podataka. Proces izrade sigurnosne kopije se sastoji od nekoliko faza: identifikacija podataka, određivanje prikladnog medija, označavanje sigurnosnih kopija, čuvanje sigurnosnih kopija, smještaj sigurnosnih kopija i testiranje sigurnosnih kopija.

Maskiranje podataka: Maskiranje strukturiranih podataka je proces prikrivanja određenih podataka u tablici baze podataka. Maskiranje podataka se obavlja s ciljem da bi podaci bili osigurani i da neautorizirane osobe ne bi mogle doći do korisnikovih informacija osjetljivog sadržaja.

Brisanje podataka: Brisanje podataka je metoda kojom se u potpunosti uništavaju svi elektronski podaci na tvrdom disku ili nekom drugom digitalnom mediju. Ova metoda se obavlja nakon što se uređaj prestane koristiti, kako neautorizirane osobe ne bi mogle doći do korisnikovih podataka.

3.1.5. Zaštita od zlonamjernih programa

Inficirani sistemi se čiste specijalnim programima za uklanjanje virusa, crva, trojanaca i špijunskih programa. Kvalitetniji zaštitni programi koriste taktiku „bolje spriječiti nego liječiti“ i štite sistem u realnom vremenu. Razlog tome je što veliki problem predstavljaju zlonamjeni programi koji su sposobni svoje komponente prikriti i tako otežati njihovo uklanjanje iz inficiranog sistema.

Instaliranje antivirusa je jedno od najboljih rješenja zaštite od malicioznih programa. Neki antivirusni programi su besplatni. Dvije osnovne komponente kvalitetnog antivirusnog programa su klasični skener i rezidentni skener koji obezbjeđuje provjeru u realnom vremenu. Antivirusni program mora biti sposoban da aktiviranog trojanca ukloni iz liste procesa, pronađe virus u izvršnoj datoteci i provjeri arhive. Potrebno je virus pronaći prije aktiviranja, jer ga je kasnije nemoguće ukloniti.

Potrebno je instalirati i programe za zaštitu od špijunskog softvera. Ovih programa ima dosta koji su besplatni i komercijalni. Antišpijunski programi treba da ograničavaju i uklanjaju adware i spyware komponente i treba da obezbijede neke funkcije sistema za detekciju upada.

ZAKLJUČAK

Sigurnost podataka, informacija i računarskih resursa može biti ugrožena nenamjernim i namjernim akcijama čiji je cilj zloupotreba ili uništenje podataka, informacija ili drugih resursa. Masovno korištenje telekomunikacijskih mreža za pristup udaljenim računarskim resursima znatno povećava ranjivost sistema. Zato treba posebnu pažnju posvetiti zaštiti sistema od zloupotreba i nezgoda kojima su podložni informacijsko-komunikacijski sistemi.

Potpunu sigurnost (100 %) nekog komunikacijskog sistema je nemoguće ostvariti, ali uz dobru sigurnosnu politiku i primjenu razvijenih mehanizama zaštite, moguće je postići vrlo visok stupanj zaštite i sigurnosti.

Osim osoba čiji računari ne sadrže informacijske vrijednosti, postoji velika većina onih koji svoje podatke žele zaštititi. U poslovnom svijetu danas je veliki trend elektronsko poslovanje, sklapanje poslova putem elektronske pošte i potpisivanje ugovora digitalnim potpisom. Iako je komuniciranje, dogovaranje poslova i potpisivanje dokumenata putem Interneta ili drugih komunikacijskih kanala danas postalo neizbježno, također je neizbježno i suočiti se s prijetnjama koje takve metode poslovanja donose. Definiranje sigurnosnih mjera je neophodno onima čiji računari sadrže vrijedne podatke, ali i onima čiji računari takve podatke ne sadrže.

LITERATURA

[1] Andreus Tanenbaum preveo Dejan Smiljanić; "**Computers Networks- Računarske mreže**"; treće izdanje, Holandija 1996. godina

[2] Cheswick, W. R., Bellovin, S. M., Rubin, A. D.; „**Firewalls and Internet Security**"; Adison-Wesley, 2003. godina

[3] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić; „**Sigurnost računarskih sistema i mreža**"; Beograd 2007. godina

[4] Nenad Desimirović, Vladimir Đurić; „**Kompjuterske tajne**"; Beograd 2009. godina

[5] CCNA Exploration Course Booklet; „**LAN Switching and Wireless"**; Cisco Systems 2010. godina

UISK uBiH

UDRUŽENJE INŽENJERA SAOBRAĆAJA I KOMUNIKACIJA
U BOSNI I HERCEGOVINI

2014

Sarajevo, 2014.