# INTERNET RIZICI

**Dr Mirko Kosanović; Miloš Kosanović**
Visoka tehnička škola strukovnih studija, Niš, SRBIJA, mirko.kosanovic@mts.rs

***Apstrakt:*** *Živimo u doba kada informacija postaje osnovno sredstvo koje donosi primat gotovo na svim poljima ljudske delatnosti. Danas je pravovremeno posedovanje prave informacije osnovni preduslov kod donošenja mnogih važnih odluka. Zahvaljujući tehnološkom napredku, a pre svega jevtinim računarima i Internetu, više se ne postavlja problem pronalaženja tih informacija, jer su one sada dostupne gotovo svima. Ali baš iz tog razloga, lake dostupnosti velikog broja različitih informacija, javili su se neki drugi problemi koji se odnose pre svega na celovitost, pouzdanost i bezbednost tih informacija. Cilj ovog rada je da prikaže koje sve vrste opasnosti vrebaju kod prikupljanja informacija sa Interneta, kao i da ukaže na osnovna pravila kojih se moramo pridržavati kada prikupljamo i koristimo te informacije, kako bi se sa bezbedonosnog aspekta,maksimalno zaštitili.*

***Ključne reči:*** *Internet, rizici, maliciozni softver, preventiva, preporuke*

## 1. UVOD

Jedna od osnovnih karakteristika današnjeg doba je sve veći i veći broj informacija do kojih dolazimo iz različitih izvora kao što su dnevna štampa, TV, propagadni materijal ili Internet. Sa jedne strane veliki broj tih informacija omogućio je sve brži razvoj ljudskog društva a sa druge strane zahtevao je dodatna tehnička pomagala koja su sve te informacije trebalo da upamte, sortiraju i pravovremeno prezentuju. Ogromna brzina, laka dostupnost, manipulativnost, i praktično neograničene mogućnosti skladištenja koje Internet pruža, otvaraju neviđene mogućnosti za najrazličitije upotrebe novih tehnologija koje su omogućile čoveku da donosi veliki broj brzih, potpunih i sveobuhvatnih odluka. U tom moru informacija nezamislivo je da se bilo ko snađe bez postojanja informacionih sistema. Međutim, da bismo bili u stanju da sve to ostvarimo, i pored mogućnosti koju nam pruža informatička tehnologija, potrebno je ispuniti odgovarajuće preduslove za njeno efikasno funkcionisanje. Sa jedne strane računari su doneli mnoge koristi ali su sa druge strane ugrozili neke od naših najvažnijih vrednosti, kao što su sigurnost, funkcionalnost i privatnost podataka. Upravo nad pitanjem pouzdanosti, funkcionalnosti i privatnosti ovih sistema nadvio se jedan opasan problem predstavljen u vidu mnogih zlonamernih programa. Naziv zlonamerni programi ili maliciozni softver (*malicious software)*, koristi se za sve vidove programskih pretnji koje nanose štetu ili opstrukciju, bilo da se ona odnosi na sigurnost i obradu podataka na računaru ili na štetu nanetu korisnikovoj privatnosti zloupotrebom, krađom ili podmetanjem lažnih podataka. Koliko je ova tema informacione bezbednosti danas aktuelna, pokazuju i najnovija zbivanja u svetu. Nedavno objavljivanje jako poverljivih podataka na Internet sajtu *Wikileaks*, izazvalo je opštu konfuziju u čitavom svetu i rasplamsalo je mnoge, do sada neviđene polemike na ovu temu.
Ovaj rad je pokušaj da se ukaže na sve negativne stvari do kojih može da dođe prilikom prikupljanja informacija sa Interneta. Posle uvoda, u drugom poglavlju prikazani su neki od osnovnih rizika kojima smo izloženi prilikom korišćenja Interneta. Treće poglavlje prikazuje koje sve vrste napada postoje na naš informacioni sistem. Kako većina tih napada dolaze sa Interneta, a u osnovi veliki deo ovih pretnji zasniva se na radu malicioznih softvera, u četvrtom poglavlju data je podela ovih programa i prikazani su metodi i programi za otklanjanje istih. Sledeće poglavlje daje preporuke za preduzimanje preventivnih koraka kao i tehnika koje nam stoje na raspolaganju a koje će u većini slučajeva efikasno sprečiti i eliminisati ove negativne uticaje. Šesto poglavlje zaključuje ovaj rad.

## 2. TIPOVI INTERNET RIZIKA

Danas je gotovo nemoguće izbeći bilo kakav kontakt sa računarima, čak bi se usudio da kažem da bi ljudski život danas bio nezamisliv bez primene računara. Oni se koriste na svim poljima ljudskog bitstvovanja na poslu, ulici, školi i kući. Prosto je nezamislivo funkcionisanje mnogih privrednih grana bez upotrebe računara: proizvodnja, saobraćaj, banke, zdravstvo i td. Podatak da čak i mala deca, koja ne znaju da pišu i čitaju, provode mnogobrojne sate igrajući razne igrice na njima dovoljno govori. Zato možemo slobodno da kažemo da su računari ušli u gotove sve pore ljudskog života. Pojava Interneta i njegovo naglo širenje, kao i gotovo neograničene mogućnosti koje nam on pruža, još je više

apostrofiralo primenu računara i njihovu primenu. Međutim, iako je Internet doneo mnoge prednosti koje su znatno unapredile čovečiji život, on je doneo i neke negativne posledice na koje se zadnjih godina sve više ukazuje [1].

## 2.1. Etički aspekt

Jedan od osnovnih slogana globalne računarizacije sveta ``Brže, jače i bolje!`` učinio je da svet izgleda sasvim drugačije, jer su se sada u njemu formirale vrednosti često bez jasnih kriterijuma vrednovanja. Promene koje su nastale često dovode u pitanje definicije mnogih ranijih pojmova, praksi i institucija. Neke od osnovnih etičkih vrednosti čoveka: privatnost, tačnost i svojina postale su jako ugrožene. Tako je na primer pojam svojine doživeo velike promene kao i sa njom povezani pojmovi vlasništva, kupovine i prodaje, prava raspolaganja, krađe, pravde u distribuciji dobara, prava na pristup, itd. Mogućnosti za zloupotrebu su enormne, i često sasvim nepredvidive. Proizvodnja i „slanje" destruktivnih softverskih programa kao što su virusi, crvi, suočava nas sa potpuno novim vrstama pitanja, koje idu do granica ispitivanja ljudskog razuma i opravdanja za one koji to rade. Odsustvo unapred određenih kriterijuma vrednovanja učinilo je da računarska etika prolazi kroz svoj razvojni period i da mi prisustvujemo nastanku jedne nove oblasti primenjene računarske etike koja iz dana u dan postaje sve značajnija.

## 2.2. Zdravstveni aspekt

Zdravstveni problemi, na koje su se mnogi korisnici računara prvo počeli da žale, predstavljali su prve simtome negativnog uticaja rada na računaru. To se pre svega ogledalo u problemima sa očima, problemi prouzrokovani od elektromagnetnog zračenja CRC monitora, kao i problemi vezani za funkcionisanje lokomotornog sistema tj. za određene pokrete ruke, koji su se stalno ponavljali, i izazivali oštećenja na zglobovima *(Repetitive Strain Injuries* - RSI). Spektar računarskog zračenja sastoji se od X-zraka, ultra-violet i infra–crvenih zraka, kao i od širokog spektra elektromagnetnih talasa druge frekfencije. Specijalsti smatraju da je opasnost od X zraka veoma mala danas. Ova vrsta zračenja konzumira se sa ekrana. Ali moramo imati na umu da čak i vrlo mali intezitet X zračenja podstiče jonizaciju vazduha. U prisustvu nekoliko računara u prostoriji količina jona se može znatno povećati, a sredina sa suviše pozitivnih jona smatra se nezdravom za čoveka. Uuticaj elektromagnetnih talasa niže frekfencije (50-100Hz) koji potiču od računara i ostalih aparata iz domaćinstva i dalje su diskutabilne teme između naučnika i branioca prava potrošača[2].

## 2.3. Socijalni aspekt

Veliki tehnološki razvoj Interneta (velika brzina i jaki računari) omogućio je prenos multimedijalnih informacija – slike i zvuka. Ova činjenica omogućila je stvaranje virtuelne realnosti-okruženja koje nam pruža mogućnosti za postupke koji su ranije bili stvar mašte. Novi oblici zavisnosti, koji liče na virtuelnu narkomaniju, predstavljaju nove oblike društvenih opasnosti. Polje mogućnosti političkih i ekonomskih manipulacija takođe se enormno proširilo, uporedo sa proširenjem mogućnosti u proizvodnji i širenjem slobode i blagostanja. Sa gledišta Internet rizika ovo će u budućnosti verovatno biti jedan od najvećih problema sa kojim će se društvo suočiti. Svi socijalni aspekti mogu se posmatrati sa:

- ***Uticaj Interneta na rad pojedinca*** – predstavlja negativne i pozitivne promene koje je on doneo. Negativne promene ogledaju se pre svega na psihološku nesigurnost gubitka posla, strah od novih tehnologija, uznemirenost zbog velikog broja informacija, bojazan da se ne pronađe odgovarajuća informacija, smanjenje individualnih sposobnosti i znanja, stroga kontrola rada i radnog mesta, monotonost rutinskog posla, izolacija pojedinaca, globalizacija kulture i td. Međutim, Internet je i pozitivno uticao na pojedince i to kroz povećanje mogućnosti za razvoj sposobnosti svakog pojedinca, mogućnost za dobijanje inteligentne pomoći u radu, veliki broj različitih informacija kao prilog objektivnosti, socijalna interakcija, integracija rada u smisaonu celinu, omogućavanje rada hendikepiranim licima i td.
- ***Uticaj Interneta na organizaciju i posao*** - korišćenje Interneta donosi mnoge organizacione promene u oblasti strukture, odgovornosti, prava, sardržaja posla, razvoja karijere, upravljanja i kontrole posla.
- ***Internet društvo*** - Internet omogućava pristup informacijama, znanjima i idejama svim njegovim korisnicima, a takođe pruža i mogućnost razvoja socijalizacije, povezivanje sa prijateljima, rođacima, razmenu ideja, informacija, ali i preispitivanje sopstvenih postavki o sebi i o svetu u kome živimo. Internet kao sredstvo za komunikaciju i upoznavanje sa drugim ljudima može, u određenim okolnostima, da predstavlja i veliku opasnost za njih, jer zapravo skrivajući se iza računara u komunikaciju sa nama mogu doći osobe koje imaju loše namere. Posebno su u opasnosti maloletne osobe, koje su zbog svoje naivnosti i znatiželje, lako pogodne za iskorišćavanje svake vrste. Pored toga na Internetu postoji veliki broj sadržaja koji nije primeren deci i koji može izazvati neprijatna osećanja i imati negativne posledice na njihov dalji razvoj. Nekada su roditelji deci pričali da se paze nepoznatih ljudi koji se čudno ponašaju ili im nude razne poklone, a danas većina ne zna kakav savet da da detetu koje svakodnevno stupa u komunikaciju sa nepoznatim ljudima na Internetu. Na osnovu mnogih istraživanja, koja se bave aspektima bezbednosti dece na Internetu, navešćemo neke od osnovnih rizika kojima su deca izložena. To spadaju pre svega: izlaganje nasilnim ili seksualnim sadržajima, direkna komunikacija sa osobom koja traži neprimerene odnose, izloženost uznemirujućim, neprijateljskim i nepristojnim elektronskim porukama, preterana izolovanost deteta koja proizilazi iz prečestog/dugotrajnog korišćenja Interneta.

### 2.4. Tehnički aspekt

Svi protivnici uvođenja računarskih sistema kao glavni adut navodili su njegovu tehničku zasnovanost i podložnost greškama**.** Negativne posledice po računarski sistem**,** izazvane njegovim lošim radom**,** naročito se osetilo kod priključivanja ovih sistema na Internet**.** Sa njegovim naglim širenjem**,** ovaj problem je još više dobijao na značaju i obimu**.** Dugo se smatralo da je to jedini negativan uticaj koji dolazi sa Interneta iz prostog razloga što je on odmah vidljiv i prepoznatljiv**.** Tehničke opasnosti kao što su virusi raznih vrsta koji mogu da sruše sistem, naprave štetu na softveru računara ili poremete funkcionisanje elektronskih servisa korisnika (*mail, chat, e-banking, …*) istog trenutka su signalizirali da nešto nije u redu sa informacionim sistemom. Korišćenje savremenih tehnologija za zaštitu od pojednih sadržaja na Internetu i ograničavanje pristupa tim informacijama je od ključnog značaja za zaštitu podataka na Internetu. Zato ćemo u daljem izlaganju posvetiti znatno više pažnje ovom problemu.

## 3. VRSTE NAPADA NA INFORMACIONI SISTEM

Postoje više različitih izvora mogućih napada na mrežni sistem, servere ili radne stanice. Administrator informacionog sistema mora preduzeti sve mere koje mogu pomoći u zaštiti računarskih sistema od eventualnog napada. Između potencijalnih napadača i proizvođaća sistemskog softvera i servisa za zaštitu računarskih sistema vodi se neprekidan "rat". Administratori se, nažalost, nalaze između te dve suprostavljene grupe, jer njihovi računarski sistemi predstavljaju "bojno polje" na kome se odvija taj rat. Predstavićemo samo neke od njih kao i ukazati na neke tačke "ranjivosti" istih.

### 3.1 Oblici napada radi neovlašćenog pristupa

Cilj pristupnog napada (*access atack*) je potpuno jasan - napadač pokušava da pristupi podacima za koje nama dozvolu da ih koristi. Pristupni napadi su usmereni ka narušavanju poverljivosti podataka. Mogu se javiti u obliku internog ili eksternog pristupa i javljaju se u sredinama u kojima je omogućen fizički pristup podacima. "Kopanje" po kontejneru (*dumpster diving*) je uobičajeni način fizičkog pristupa podacima. Ovaj naziv nastao je iz činjenice da kompanije u svakodnevnom radu imaju ogromne količine papirnih dokumenata, od kojih najveći deo završava u kontejnerima ili korpama za otpatke. Kako veliki broj organizacija, ne uništava dokumente, u korpama se mogu naći i podaci izuzetno osetljivog sadržaja. Ista je situacija je sa digitalnim dokumentima koji se nalaze nezaštićeni na mrežnim diskovima ili se prenose putem mrežne infrastrukture. Preturanjem po tim dokumentima potencijalni napadač pokušava da pronađe poverljive informacije i iskoristi ih. Najčešće tehnike takvih pristupnih napada podrazumevaju:
1. **Prisluškivanje** (*eavesdropping*) - namerno praćenje ili slučajan pristup delovima neke konverzacije.
2. **"Njušenje"** (*snooping*) – napadač proverava sadržaj datoteka u nadi da će moći da u njima pronađe nešto zanimljivo.
3. **Presretanje** (*interception*) - podrazumeva rutinsko praćenje mrežnog prometa koje može biti pasivnog i aktivnog karaktera. Aktivno presretanje zahteva postavljanje posebnog računara između pošiljaoca i primaoca, tkz. presretača, koji će primati sve podatke koji se kreću u oba smera. Ovaj vid kontrole mrežnog saobraćaja naročito je interesantan za mnoge Vladine institucije kao što su MUP, državna bezbednost ili vojska. *FBI*, na primer, poseduje nekoliko računarskih sistema ćiji je osnovni zadatak da kontrolišu protok *E-mail* poruka i izdvajaju one koje u njihovim sadržajima imaju unapred zadate ključne reči [3].

### 3.2 Napadi radi izmene podataka i napadi poricanja

Napadi radi izmene podataka (*modification attack*) obuhvataju napade sa ciljem neovlašćenog brisanja, umetanja ili izmene podataka, i to na takav način da krajnji korisnik prihvata izmene kao potpuno legalne. Takve napade je obično vrlo teško otkriti. Oni su vrlo slični prethodno opisanim napadima, jer napadač prvo mora osigurati pristup podacima, da bi ih tek onda promenio bez znanja učesnika u komunikaciji. Motiv ovih napada može biti podmetanje lažnih podataka, izmena ocena u školi, izmena broja kreditne kartice ili nešto slično.

### 3.3 Napadi radi "gušenja" servisa

Napadi radi "gušenja" usluga (*Denial of Service, DOS attack*) usmereni su da ovlašćenim korisnicima onemoguće pristup i korišćenje resursa računara. Takvi napadi mogu sprečiti pristup podacima, aplikacijama, serverima ili komunikacijama. U slučaju *DOS* napada na neku aplikaciju, može doći do pada kompletnog *WEB* sajta, dok će komunikaciona oprema i server nastaviti normalan rad. Na primer, napadač može oboriti *WEB* stranicu koja omogućava elektronsko poslovanja (*e-commerce*) neke firme, da bi sprečio da ga koriste legitimni potrošači i tako smanji konkurenciju. *DOS* napad usmeren na komunikaciju obično podrazumeva zauzimanje celokupnog propusnog opsega

kanala i sprečavanje legitimnih korisnika da ga koriste. Ovu kategoriju karakterišu veliki broj različitih oblika napada kao što su: *TCP SYN* plavljenje (*flood*), *Smurf* napad, smrtonosnog ping (*ping of death*) - *sPing*, preopterećenje bafera (*buffer overflow*) - *Code Red, Slapper* i *Slammer*, distribuirano "gušenje" servisa (*distributed denail of service, DDoS*) i drugi.

### 3.4 Napad tipa *back door*

Pojam sporedna vrata (*back door*) može imati dva različita značenja. Prvobitno je ovaj pojam korišćen za prolaze u računarskim sistemima koji su programeri namerno ostavljali radi otklanjanja eventualnih pogrešaka ili njihovog daljeg razvoja. Kroz njih su oni mogli da ispitaju i prate promenljive, bafere u samom toku izvršavanja programa, drugim rečima da vrše debagiranje svojih programa. Prolazi su se uklanjali iz programskog koda pre nego što je operativni sistem ili aplikacija dara u proizvodnju, ali se dešavalo, nepažnjom, da mnogi prolazi ostanu i u komercijalnoj verziji. Kada bi proizvođač softvera otkrio zaboravljeni prolaz, koji nije uklonjen, obično bi objavljivao sigurnosni dodatak ili "zakrpu" koja je zatvarala takav prolaz. Drugo značenje pojma *back door* vezano je za ostvarivanje pristupa nekoj mreži i ubacivanje programa ili rutine koja kreira ulaz i omogućava dalje napade. To može biti program koji dozvoljava prijavu korisnika sa određenim *ID*-om bez lozinke ili obezbeđuje privilegije administratora.

### 3.5 Napad sa lažnim predstavljanjem

Suština napada lažno predstavljanje (*spoofing*) je u pokušaju lažnog predstavljanja nekome ili nečemu. Ovaj oblik napada obično se svrstava u pristupne napade. Uobičajeni *spoofing* napad, koji je bio popularan godinama na ranim *UNIX* i drugim operativnim sistemima sa deljenjem vremena (*timesharing*), izvođena je pomoću lažnog programa za prijavu na sistem (*logon*). Takav program zahtevao je od korisnika da unese svoj *ID* i lozinku, ali je, bez obzira na unete elemente, prijavljivao grešku. Korisnik je ponovo morao da ponovi prijavljivanje, ali je sada to radio preko pravog programa za prijavu. Istovremeno, *spoofing* program je upisivao *ID* i lozinku u datoteku, radi kasnije zloupotrebe. Najpopularniji napadi ovog tipa danas su *IP spoofing* i *DNS spoofing*.

### 3.6 Napad tipa čovek u sredini

U tehničkom smislu napad čovek u sredini (*man-in-the-middle*) predstavlja prilično složen napad. On pripada grupi pristupnih napada, mada se može izvršiti i kao početni korak u napadu s ciljem izmene podataka. U ovom napadu se između legitimnog servera i klijenta neprimetno postavlja odgovarajući softver, i to tako da administrator i korisnici ne budu svesni njegovog prisustva. Ubačeni softver presreće podatke, a zatim ih šalje na server, kao da se ništa nije desilo. Server reaguje normalno na tako dobijene podatke, uveren da se komunikacija odvija s legitimnim klijentom. Softver-napadač i dalje nastavlja slanje podataka na server i celi proces se produžava. Problem je u tome što ubačen *man-in-the-middle* softver može beležiti presretnute podatke radi kasnijeg pregleda, menjati te podatke ili na bilo koji drugi način ugroziti sigurnost korisničkih sistema i veze.

### 3.7 *Replay* napad

Napadi ovog tipa postaju sve češći u praksi. Izvode se zadržavanjem podataka koji se razmenjuju na mreži, u cilju osiguranja pristupa mreži (pristupni napad) ili izmene podataka (modifikacioni napad). Između klijenta i sistema za identifikaciju, u distribuiranom okruženju, stalno se šalju podaci o imenu i lozinci korisnika. Napadač može zadržati takve podatke i naknadno ih ponovno poslati. Isto vredi i za sigurnosne sertifikate u sistemima poput *Kerberos*-a: napadač može ponovno iskoristiti uhvaćeni sertifikat, u nadi da će biti prihvaćen na sistemu za identifikaciju i da će on nadmudriti bilo kakvu zaštitu u vidu vremenske osetljivosti.

### 3.8 Napadi sa pogađanjem lozinki

Napadi sa podudaranjem lozinki (*password guessing attacks*) obuhvataju višestruki napad na jedan korisnički nalog. To se postiže sistemskim slanjem moguće lozinke za određeni nalog. Početni cilj napada je otkrivanje lozinke, dok se kasnije može proširiti u napad radi osiguravanja pristupa, ili u napad radi izmene podataka. Postoje dva oblika napada s podudaranjem lozinki i to:

**1. Napad grubom silom** *(bruto force attack)*. Napad grubom silom koristi nesavršenost izbora lozinki i nasumice isprobava razne varijante dok ne pronađe onu pravu. On se obično izvodi u dužem vremenskom razdoblju. Da bi izbor lozinke bilo savršen, one moraju biti znatno duže od dva ili tri karaktera (šest karaktera su apsolutni minimum), složene po strukturi, da se sastoje od brojeva, malih i velikih slova, znakova interpukcije, uz istovremeno ograničavanje broja neispravnih pokušaja (*password lockout*).

2. **Napad pomoću rečnika** *( dictionary attack)*. Za napad pomoću rečnika koristi se rečnik često upotrebljavanih izraza u pokušaju pronalaženja prave lozinke. U javnom domenu postoji nekoliko softverskih alata za automatizovano izvršavanje takvih napada. Pojedini sistemi obaveštavaju korisnika o ispravnosti njegovog *ID*-a čak i u slučaju neispravne lozinke. Bilo kakva indikacija napadaču o ispravnosti korisničkog *ID*-a nije poželjna. Ukoliko se identifikacija na vašem sistemu može podesiti tako da odbija nepotpune prijave, odnosno da prihvata samo kompletne korisničke podatke (*ID*/ lozinka) ili ponavlja celi proces prijave, obvezno treba primeniti tu mogućnost.

## 4. TIPOVI MALICIOZNIH PROGRAMA

Softver koji je napravljen da bez znanja korisnika računara uđe i sakrije se negde u okviru operativnog sistema, aplikacije ili neke datoteke, i odatle odrađuje neki ``prljav`` posao za neku drugu osobu, nazivamo zlonamerni programom. Ovakvi programi uglavnom zahtevaju neku akciju korisnika, kao na primer pokretanje programske instalacije u kojoj se zlonamerni program nalazi ili otvaranje neke datoteke [4]. Zlonamerni program koristi sistemske greške na računarima, a ove sistemske greške mogu dovesti do pada sistema i gubljenja podataka. Današnji zlonamerni programi se uglavnom prenose preko WEB sajtova i E-mail poruka i mogu se teoretski, za nekoliko dana, proširiti na milione računara. Zajedničko za sve vrste zlonamernih programa je to da se šire uglavnom bez obzira na volju korisnika, osim ukoliko sam korisnik ne želi da "zarazi" određeni sistem, i da ga na taj način ugrozi. Motivi za ovakvo ponašanje nekih korisnika mogu biti različiti: edukativni, dokazivanje u hakerskom svetu, finansijska korist, nanošenje namerne štete, reklamiralje proizvoda, industrijska špijunaža, krađa novca elektronskim putem, prenošenje raznih drugih poruka (političkih, ličnih, pa čak i totalno besmislenih poruka). Među korisnicima računara, za sve vrste zlonamernih programa najčešće se koristi termin "virusi", a oni korisnici koji se više bave ovom problematikom, dele ih na viruse, trojanske konje, crve, tempirane bombe, itd. Teško je dati neku generalnu podelu svih zlonamernih programa, ali se u praksi oni obično dele prema tome šta rade, kako se izvršavaju i kako se šire. Međutim, razlike između tipova zlonamernih programa nisu uvek tako jasno definisane, pa se mnoge vrste "preklapaju", tako da postoje i "hibridni" zlonamerni programi koji kombinuju osobine više vrsta.

### 4.1 Virusi

Virus je softverski proizvod koji je kreiran radi „inficiranja" računarskog sistema. Pojedini virusi ne preduzimaju nikakve druge akcije, osim što se smeštaju na napadnuti računar i povremeno se aktiviraju. Drugi oblici virusa mogu oštetiti podatke na hard disku, uništiti operativni sistem i proširiti se na ostale računare. U najvećem broju slučajeva virusi pokušavaju da postignu jedan od dva moguća cilja: da onesposobe računarski sistem ili da se prošire na druge sisteme. Veliki broj virusa će se proširiti na druge sisteme ukoliko im se ukaže prilika, nakon čega će onesposobiti računar. Ukoliko je računar „zaražen", virus će verovatno pokušati da se „prikači" na sve datoteke na računaru da bi mogao da pređe i na ostale sisteme prilikom slanja dokumenata drugim korisnicima. Kada „zaraženu" datoteku damo drugom korisniku ili je iskopiramo na drugi računar, virus će „zaraziti" i taj računar. Virusi se mogu naći i u sistemima datoteka i to u programskom kodu koji izvršava makroe i skriptove - makro i skript virusi.

### 4.2 Crvi

Crvi (*worm*) se razlikuju od klasičnih virusa po tome što imaju moć reprodukcije, predstavljaju zaokruženu celinu i ne zahtevaju host-aplikaciju za prenošenje. Oni nisu destruktivni i osnovni cilj im je da spreće korišćenje nekih resursa u računarskom sistemu. Ipak, crvi mogu sadržati čak i viruse, tako da se mogu iskoristiti za isporuku virusa na ciljni sistem. Postoji više vrsta crva kao što su: *E-mail, IM* (*Instant messaging*), Internet, *File sharing* crvi.

### 4.3 *Spyware/ adware*

*Spyware* i *adware* programi su varijante malicioznog softvera, koji prikuplja i šalje podatke o ponašanju korisnika računara bez njegovog znanja. Ovi programi mogu vršiti puno različitih funkcija uključujući prikazivanje neželjenih reklama, prikupljanje privatnih podataka kao što su brojevi kreditnih kartica, re-rutiranje zahteva za *WEB* stranicama kako bi se ostvarili prihodi od referisanja novih korisnika, instaliranje teško uočljivih "*dialer*-a", itd. *Adware* se u mnogome poklapa sa definicijom *spyware* -a, sa tom razlikom da *adware* isključivo služi u komercijalne svrhe (*ad* je skraćenica od engleske reči *advertisment*). *Adware* programi prikupljaju informacije o ponašanju korisnika, *WEB* sajtovima koje korisnik posećuje i uz pomoć različitih mehanizama (najčešće *cookie, activex, javascript*), istim korisnicima se serviraju odgovarajuće reklame i nude odgovarajući proizvodi. Smatra se da su oni najrasprostranjeniji zlonamreni programi na Internetu i da je gotovo 90% računara u svetu zaraženom nekom vrstom *spyware* programa [5].

### 4.4 Trojanski konji

Uobičajena definicija Trojanskog konja je da je to program koji se nastanjuje na računaru ili na mreži, tako što se maskira u neki legitiman program koji će, kada se pokrene, napraviti neku štetu. Zlonamerni programi ovog tipa se mogu javiti i u obliku priloga ili dela nekog instalacionog programa. Oni se ne mogu širiti samostalno što ih razlikuje od virusa i crva. Danas se ovi programi najčešće krišom instaliraju i isporučuju svoj „korisni" sadržaj bez znanja korisnika. Značajan deo današnjeg kriminalnog softvera obuhvata različite tipove Trojanaca, koji su napravljeni sa ciljem da vrše određenu štetnu funkciju. Najuobičajeniji su *Backdoor* Trojanci (često uključuju *keylogger* - štetni program koji snima sve što otkucate na tastaturi i šalje napadaču), Trojanci špijuni, Trojance koji kradu šifre (*PSW*), *Proxy* Trojanci koji vaš računar pretvaraju u računar za distribuciju spamova i Trojanci koji pozivaju telefonske brojeve sa ciljem da žrtvi naprave ogroman telefonski račun [6].

### 4.5 Logičke bombe

Logičke bombe predstavljaju programe ili delove programskog koda koji se aktiviraju samo nakon nekog unapred definisanog događaja ili posle određenog perioda vremena i obično deluju destruktivno po zaraženi računar.

### 4.6 *Exploit*

*Exploit*-i su programi koji iskorišćavaju određenu slabost nekog programa. Oni najčešće ne nanose štetu i postoje samo da bi se iskoristila slabost nekog programa. Njihove "usluge" često koriste *worm*-ovi, virusi, *spyware* i sl. [7].

### 4.7 *Rootkit*

*Rootkit* je softver koji se ubacuje na računar pošto je napadač dobio kontrolu sistema a namena mu je da olakša udaljenu (*remote*) kontrolu i da sakrije tragove upada brisanjem *log* datoteka ili sakrivanjem procesa koji su pod kontrolom napadača. Često *rootkit*-ovi sadrže i *backdoor*-ove, omogućavajući naknadni upad ili *exploit* programe za napade na druge sisteme. Važno je primetiti da se ciljani napadi obično izvode sa sistema koji su takođe prethodno bili ugroženi, da bi se sa njih lako mogli ukloniti dokazi o identitetu napadača, jer sam napadač dobija mogućnost da ukloni dokaze. *Rootkit* -ovi se vrlo često vezuju za kernel nivo, pa ih je teško otkriti, a kada se jednom otkriju vrlo je bitno da se kompletno reinstalira sistem, kako bi se sigurno uklonili svi tragovi *rootkit* –a [7].

### *4.8 Neželjena elektronska pošta*

Jedan od najvećih problema na Internetu je neželjena elektronska pošta. *Spam* je svaka poruka koju primalac nije tražio, koju nije želeo da dobije i ako se on izjasni da je smatra netraženom i neželjenom. Ova tri uslova su potrebna i dovoljna da bi neka poruka mogla biti proglašena *spam*-om. Sadržaj poruke ne utiče na to da li je neka poruka *spam*. To da li je poruka oglas, reklama, obaveštenje, da li ima komercijalan karakter ili ne, nije bitno za određivanja poruke kao *spam*. Broj poruka takođe ne određuje da li te poruke predstavljaju *spam*. Dovoljna je i jedna poruka koja ispuni tri navedena uslova da bi bila proglašena *spam*-om. Procenu o tome da li je nešto *spam* može da napravi samo primalac poruke. On je taj koji zna da li je poruku tražio, da li je želeo i da li smatra da je poruka *spam*. Svaku akciju protiv *spam*-a pokreće upravo primalac poruke prijavom *spam*-a jer ne postoji zakonski mehanizam koji će nešto tretirati kao *spam*.

### 4.9 Pecanje i *farming*

Pecanje u računarstvu predstavlja vrstu kriminalne aktivnosti koja koristi tehnike društvenog inženjeringa, to jest prevara, pomoću kojih napadači dolaze do osetljivih informacija, kao što su razne lozinke i detalji o kreditnim karticama. Pecanje se najčešće izvodi pomoću elektronske pošte ili sistema trenutnih poruka (*instant messages*).
*Farming* je napad koji za cilj ima preusmeravanje *HTTP* zahteva korisnika na lažirane ili zlonamerne lokacije umesto na orginalne. *Farming* je napad čiji je rezultat sličan pecanju, korisnik koji je uspešno prevaren ostaviće osetljive podatke (lozinka ili broj kreditne kartice) na *WEB* stranici napadača koja je lažno predstavljena kao legitimna *WEB* lokacija. Ovaj napad se razlikuje od pecanja u tome što napadač ne mora da navodi korisnika da pritisne hipervezu u elektronskoj poruci, čak i ako korisnik tačno zada *URL* (*WEB* adresu) u adresno polje *WEB* čitača, napadač i dalje može da ga preusmeri na zlonamernu *WEB* lokaciju. *Farming* se obično izvodi tehnikama otimanja *DNS*-a ili "trovanja" *DNS* keša (*DNS cache poisoning*). Postoji nekoliko dobrih preporuka kako da se zaštitimo od ove prevare na Internetu, ali odmah se mora reći da apsolutna zaštita ne postoji.

## 5. METODE ZAŠTITE

Zaštita od zlonamernih programa nije komplikovan proces, ali zahteva pre svega obaveštenost, pedantnost i oprez. Osnovna zaštita od zlonamernih programa na samom računaru sprovodi se upotrebom programa za borbu protiv zlonamernih programa. Ovi programi označavaju se zajedničkim imenom antivirusni programi [7], i oni su dovoljni za privatnu upotrebu. Međutim, ukoliko želimo da postignemo maksimalnu bezbednost naših podataka, na profesionalnom nivou, potrebno je sprovesti zaštitu od zlonamernih programa u više zona tj. imati slojevitu zaštitu. Koliko slojeva zaštite će biti uključeno pre svega zavisi od stepena zaštite pojedinih resursa koje želimo da postignemo. Zato prilikom izbora, trebamo imati u vidu sledeća četri pitanja poverljivosti, integriteta, dostupnosti i nadležnosti tih resursa:

1. **Poverljivost** sprečava ili umanjuje mogućnost neovlašćenog pristupa i otkrivanja zaštićenih podataka i informacija.
2. **Integritet** podataka treba da osigura korektnost podataka sa kojima se radi.
3. **Dostupnost** osigurava zaštitu podataka i sprečava njihov gubitak.
4. **Nadležnost** nad podacima definiše vlasnika tih podataka ili subjekta koji je odgovoran za njihovu validnost.

Obično se kaže da poverljivost (*Confidentiality)*, integritet (*Integrity*) i dostupnost (*Availability*) predstavljaju *CIA* sistema mrežne sigurnosti, mada je i nadležnost isto tako važna. Imajući u vidu ova četri pitanja navešćemo sada neke od osnovnih tehnika koje se primenjuju kod ovakvog vida zaštite [1].

### 5.1 Identifikacija korisnika

Procesom identifikacije utvrđuje se da li je neka osoba, zaista ona osoba za koju se predstavlja. Ona je ključni deo u gotovo svim sistemima zaštite. U suštini, to je deo procesa koji se naziva *Identification and Authentication (I & A*). Sistemi ili metodi identifikacije zasnovani su na sledećim faktorima:

- na nečemu što korisnik zna, kao što su lozinka ili *PIN*
- na nečemu što korisnik ima, neki identifikacioni uređaja kao što je smart kartica ili fleš memorija.
- na nečemu što fizički određuje korisnika, kao što su otisak prsta ili izgled zenice oka, *DNK* kod

Korisničko ime i lozinka jednoznačno identifikuju korisnika tokom prijave na sistem (*logon*). Većina operativnih sistema koristi korisnički *ID* i lozinku za proces identifikacije. *ID* i lozinka se preko mreže može poslati u otvorenom ili šifriranom obliku preko sledećih protokola:

1. ***Password Authentcation Protokol (PAP)*** ne nudi punu sigurnost ali je jedan od najjednostavnijih metoda identifikacije. Korisničko ime i lozinka se u obliku otvorenog teksta šalju na server radi provere. U slučaju da ime i lozinka odgovaraju podacima na serveru korisniku se odobrava pristup, u suprotnom je pristup zabranjen.
2. ***Challenge Handshake Authentication Protocol (CHAP)*** koristi proveru sistema da bi ustanovio identitet korisnika. On ne koristi mehanizam korisnički *ID*/lozinka. Korisnik šalje zahtev za prijavu sa klijentskog računara prema serveru, server šalje blok za proveru (*challenge*) ka klijentu. Klijent šifrira dobijeni blok i vraća ga do servera. Server proverava dobjenu vrednost i u slučaju da je ona ispravna potvrđuje identifikaciju.

### 5.2 Kreiranje zaštitnih zona

Ono što je u početku izgledalo kao skup računara koji međusobno dele resurse veoma brzo prerasta u elektronsku „noćnu moru". U njima se često javljaju veze između različitih organizacionih celina, kompanija i država, kao i različiti oblici javnog pristupa preko privatnih komunikacionih linija i preko Interneta. Uspostavljanjem sigurnosnih zona u mrežama postiže se efekat koji omogućava izoliranje sistema i sprečavanje neovlašćenog pristupa. U praksi se najčešće sreću četiri tipa sigurnosnih zona [8]:

1. **Internet** predstavlja globalnu mrežu koja povezuje računare i pojedinačne mreže. Može ga koristiti svako ko ima pristup preko operatera (*ISP – Internet Service Provider*). Takvo okruženje nameće potrebu za malim stepenom poverenja u ostale korisnike Interneta pa se zahteva najveći stepen predostrožnosti u zaštiti podatka.
2. **Intranet** je vrsta privatne mreže koja je uspostavljena u nekoj kompaniji ili organizaciji i predstavlja lokalni Internet čije granice ne prelaze granice kompanije. Ovde je pristup dozvoljen samo onim sistemima koji su već spojeni na tu mrežu i proverenim korisnicima unutar korporativne mreže ili korisnicima na udaljenim lokacijama.
3. **Ekstranet** znatno proširuje granice Intranet mreže, tako da u nju uključuje i veze ka spoljnim saradnicima. Saradnici mogu biti prodavači, dobavljači robe ili slične institucije kojima je neophodan pristup do baze podataka u organizaciji koja je vlasnik Intraneta. Ekstranet podrazumeva povezivanje onih organizacija koje uživaju međusobno poverenje.
4. **Demilitarizirana zona (DMZ)** predstavlja oblast u kojoj se smešta javni server radi pristupa onih osoba koje ne uživaju puno poverenje. Izoliranjem servera u okviru DMZ prikriva se ili se sprečava pristup do ostatka mreže. Serveru se i dalje može prići sa lokalne mreže, ali spoljni korisnici neće moći da koriste ostale mrežne resurse. Zona se kreira pomoću zida (*firewall*), koji potpuno izoluje ostatak mreže.

### 5.3 Implementacija kontrole pristupa

Uspostavljanje kontrole pristupa predstavlja ključni deo čitavog sistema zaštite. Kontrola pristupa definiše međusobnu komunikaciju korisnika i računarskih sistema. Ona ograničava i kontroliše pristup sistemskim resursima, uključujući i podatke, čime se sprečava neovlašćen pristup njima. Navešćemo neke od tehnika kojima možemo da se služimo [8]:

1. ***Mandatory Access Control (MAC)*** - obavezna kontrola pristupa predstavlja statički model koji koristi unapred definisani skup prava pristupa ka datotekama u nekom računarskom sistemu. Parametre definiše sistem administrator, nakon čega ih dodeljuje nalozima, datotekama ili resursima.
2. ***Discretionary Access Control (DAC),*** proizvoljna kontrola pristupa predstavlja model prava pristupa koji definiše vlasnik podataka-resursa. Za razliku od *MAC* modela, u ovom modelu labele nisu obavezne. *DAC* model omogućava deljenje datoteka između korisnika, odnosno rad sa datotekama koje su označene da su deljive. Model koristi listu kontrole pristupa (*ACL-Access Control List*) gde su navedeni svi korisnici kojima je dozvoljen pristup do podataka.
3. ***Role-Based Access Control (RBAC),*** kontrola pristupa na osnovu uloga, predstavlja model koji definiše ulogu koju korisnik ima u organizaciji. Korisnicima se dodeljuju određene uloge na nivou čitavog sistema, na osnovu kojih oni obavljaju određene funkcije ili dužnosti. *RBAC* model uobičajen je za razne uloge administratora na mreži.

### 5.4 Antivirusni programi

Upotreba antivirusnih programa predstavlja osnovnu meru zaštite od širenja zlonamernog koda. Ti programi se instaliraju na računarski sistem radi njegove zaštite i otkrivanja virusa, trojanaca i crva. Najveći broj virusa poseduje neke zajedničke karakteristike koje su specifične za tu familiju programa. Anitivirusni programi pronalaze upravo takve karakteristične "potpise" da bi identifikovali i neutralizirali viruse pre nego što nanesu bilo kakvu štetu.

### 5.5 Rad sa novim tehnologijama

Privlačna strana tehnologije sadržana je u činjenici da se ona stalno menja i napreduje. Zadnjih godina na tržištu se pojavilo nekoliko relativno novih tehnologija koje mogu pomoći u formiranju manje ranjivih računarskih sistema. Navešćemo tri takve tehnologije: virtualne lokalne mreže (*VLAN*), *Network Address Translation* (*NAT*) i tunelovanje. Uz minimalne dodatne troškove one omogućavaju poboljšanje stepena zaštite mreže.

**Virtualna privatna mreža (*virtual local area network* - *VLAN*)** -omogućava grupisanje korisnika i računarskih sistema u okviru segmenta na mreži. Podela mreže na segmente omogućava njihovo međusobno prikrivanje, čime se osigurava i kontrola pristupa. *VLAN* se može podesiti da kontroliše put podataka od jedne tačke do druge. On predstavlja dobar način za zadržavanje mrežnog prometa u okviru određenog dela mreže.

***Network Address Translation* (*NAT*)** pruža zasebnu mogućnost za poboljšanje zaštite mreže. Povećanje broja upotrebljivih Internet adresa je osnovna namena *NAT*-a. Pomoću njega organizacija može povezati sve računare na Internet preko jedne jedine *IP* adrese. *NAT* server osigurava *IP* adrese za sve računare u lokalnoj mreži, uz istovremeno praćenje dolaznog i odlaznog saobraćaja. Ukoliko neka organizacija koristi *NAT* servis, ona se na Internetu pojavljuje kao jedna jedina konekcija sa jednom jedinom *IP* adresom. Ta konekcija se realizira putem rutera ili preko *NAT* servera. Eventualni napadač može dobiti samo podatak o adresi te konekcije. *NAT* praktično skriva lokalnu mrežu od ostatka sveta, tako da napadači teško mogu da utvrde vrstu računarskih uređaja sa druge strane *NAT* servera.

**Tuneliranje** podrazumeva kreiranje namenske virtualne veze između dva sistema ili mreže. Tunel između dve tačke kreira se enkapsulacijom podataka u zaseban protokol prenosa koji je ugovoren između dve strane. U većini implementacija podataka koji prolaze kroz tunel izgledaju kao da potiču sa drugog dela mreže. Protokoli tuneliranja obično osiguravaju i zaštitu podataka i njihovo šifriranje

## 6. ZAKLJUČAK

Ne postoji veća opasnost koja se nadvila nad računarima i njihovom umrežavanju od pojave zlonamernih programa. Mnogi teoretičari smatraju da je to potencijalna opasnost koja lako može da uništi Internet. Zato se u pravnim sistemima mnogih zemalja posebna pažnja poklanja ovom problemu i mnogi ih sistemi kvalifikuju kao najteže krivično delo. Nažalost, kod nas u Srbiji problem informacione bezbednosti nije dovoljno razmatran i njemu se slabo daje pažnja. Nadamo se da će ovaj rad dati skroman doprinos ovoj problematici i zato ćemo ga završiti sa citiranjem 10 osnovnih pravila za rad sa računarom koje je propisao Institut za računarsku etiku (*The Computer Ethics Institute*), koji je neprofitna istraživačka organizacija koju čine *Brookings Institute, IBM, The Washington Consulting Group i Washington Theological Consortiu* [9]. Ta pravila su:

1. Ne koristi računar tako da ugrožavaš ili povređuješ ostale ljude.
2. Pri korišćenju svog računara nemoj da ometaš rad drugih računara.
3. Nemoj da pristupaš sadržajima fajlova drugih ljudi za koje nemaš dozvole.
4. Ne koristi računar kao sredstvo za krađu.
5. Ne koristi računar u cilju lažnog svedočenja.

6. Ne koristi kopije softvera koje nisi kupio (za koji nemaš licencu).
7. Ne koristi računarske resurse drugih ljudi bez njihove saglasnosti.
8. Ne prisvajaj intelektualne rezultate rada drugih ljudi.
9. Vodi računa o socijalnim posledicama programa koji pišeš ili sistema koji dizajniraš.
10. U svakoj situaciji koristi računar na takav način da poštuješ ugled i integritet drugih.

Kada bi se svi korisnici računara i Interneta pridržavali ovih pravila verovatno da ne bi ni bilo svih ovih pretnji u vidu zlonamernih programa. Nadamo se da će primena ovih preporuka i pridržavanje istih doprineti da rad na Internetu bude bezbedniji, udobniji i delotvorniji a ne da to predstavlja noćnu moru za mnoge korisnike Interneta.

## LITERATURA

[1] www.scribd.com/doc/18284213/Sigurnostracunalnihmreza, pos.12.11.2016.
[2] M.Kosanović, "Bezbedonosni aspekti rada na računaru", Tempus projekat 'Bezbednost i zdravlje na radu', knjiga II, modul 1.0, str. 8-18, 06.2011.
[3] www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava, pos.15.11.2016.
[4] Mike Pastore, Emmett Dulaney, "Security Study Guide Second Edition", Venice, Italy, 2003.
[5] http://www.borea.hr/upload/files_tbl_korisni/Spyware.pdf , pos.22.05.2017.
[6] Mario Baksa, "*Sigurnost računalnih mreža*", magistarski rad, Elektrotehnički fakultet u Zagrebu, 2004.
[7] Osokoljić Ivica, "*Vrste napada i zaštita*", magistarski rad, Fakultet organizacionih nauka u Beogradu, 2005.
[8] D.Pleskonjić, N.Maček, B.Đorđević, M.Carić, „*Sigurnost u računarskim sistemima i mrežama*", Mikro knjiga, Beograd, 2007.
[9] http://computerethicsinstitute.org/publications/tencommandments.html , pos 2.06.2017.