***SEMINARSKI RAD***

***PREDMET****:* ***ZAŠTITA INFORMACIONIH SISTEMA***

***TEMA****:* ***TIPOVI******SYBER KRIMINAL***

*Profesor: Student:*

[www.maturski.org](http://www.maturski.org/)

***SADRŽAJ***

[***UVOD*** 3](#_Toc311035943)

[***1.*** ***CYBER KRIMINAL*** 5](#_Toc311035944)

[***2.*** ***TIPOVI CYBER KRIMINALA*** 7](#_Toc311035945)

[***2.1.*** ***Najčešći tipovi napada i tehnologije koje se zloupotrebljavaju*** 10](#_Toc311035946)

[***3.*** ***ZAKLJUČAK*** 21](#_Toc311035947)

[***LITERATURA*** 22](#_Toc311035948)

# ***UVOD***

Nema oblasti ljudske djelatnosti u kojoj računari nisu našli svoju primjenu. Dostupnost, kao i brz razvoj, stvorili su mogućnost da se danas mogu zloupotrijebiti u različite svrhe. Kompjuterski kriminalitet podrazumijeva zloupotrebu kompjuterske tehnologije, kao načina i sredstva, ili kao cilja izvršenja krivičnog djela, čime se ostvaruje neka u krivičnopravnom smislu relevantna posljedica.

Kompjuterski kriminalitet ima svoje specifičnosti u odnosu na druge vrste kriminalnih djelovanja: velika dinamičnost, stalno širenje na nove oblasti, težina posljedica (imovinskog, ali i nematerijalnog karaktera), otežano otkrivanje i dokazivanje, specifičan profil učinioca, i velike mogućnosti za prikrivanje izvršenog krivičnog djela, a sve je to uzrokovano ambijentom u kojem se ova krivična djela vrše.

Jasno je da se radi o veoma složenom obliku kriminaliteta, kojem se društvo može adekvatno suprotstaviti samo ako u potpunosti sagleda sve njegove osobenosti i specifičnosti.

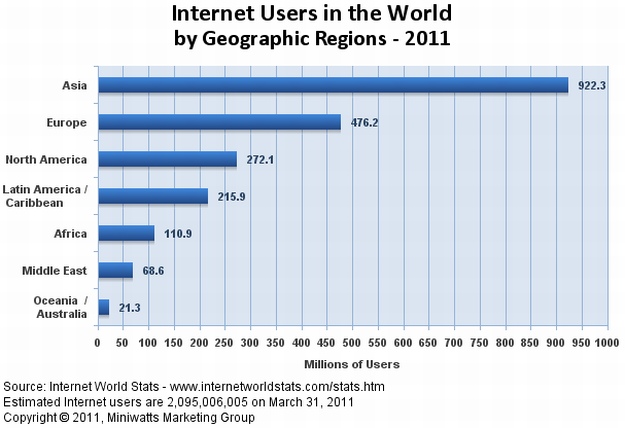
Razvoj Informaciono-komunikacionih tehnologija doveo je do poboljšanja poslovanja savremenog društva (e-poslovanje). Međutim razvoj tih istih tehnologija stvorio je, a i dalje stvara, sve više mogućnosti cyber-kriminalcima da na lak način upadnu u sistem pojedinca ili kompanije i da načine neku štetu.

Poražavajuća je konstatacija da ne postoji tehničko i tehnološko dostignuće koje u istoriji čovečanstva nije naišlo na različite vidove zloupotrebe. Specifičnost predstavljaju faze razvoja u kojima je pronalazak bio podložan zloupotrebi, zatim grupacije lica koje su vršile takve radnje i različite namjene zbog kojih su se vršile te zloupotrebe.

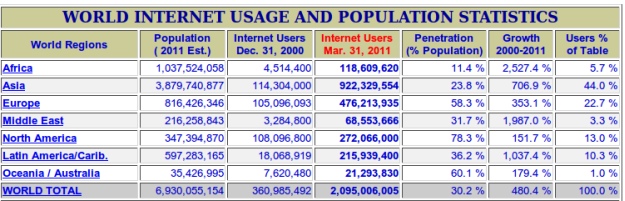
U početku primjene kompjuterske tehnologije, kompjuteri nisu bili podobni za veće zloupotrebe, jer njihova primjena nije bila masovna, tako da se njima bavio samo uzak krug korisnika – informatičkih stručnjaka. Ono što je otvorilo vrata širenju mogućnosti da se kompjuterska tehnologija zloupotrijebi u različite svrhe, jeste njen brz razvoj, pojednostavljenje njene upotrebe, kao i dostupnost iste širokom krugu korisnika.

Velika „zavisnost“ od računara i računarskih mreža omogućila je dobro tehnički potkovanim pojedincima, grupama ili organizovanim grupama da u velikoj mjeri utiče na dešavanja u cyber-svetu.

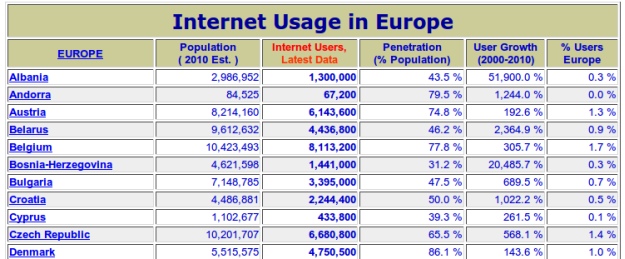
Globalna računarska mreža (Internet) je zbog ogromnog broja korisnika idealno skrovište za takve kriminalce.



Slika 1. Broj korisnika Interneta po kontinentima (u milionima)



Slika 2. Procenat svjetske korisničke populacije interneta



Slika 3. Procenat evropske korisničke populacije interneta

WEB stranica Internet World Stats je ove godine ažurirala svoju bazu podataka. Po prvi put, ukupni broj korisnika interneta premašio je dvije milijarde ljudi.   
Prema novim podacima, ukupna korisnička baza povećala se otprilike 480 posto u odnosu na 361 milijon korisnika koji su se internetom služili krajem 2000. godine.

# ***CYBER KRIMINAL***

Kompjuterski kriminalitet je nemoguće definisati jedinstvenim i preciznim pojmovnim određenjem. To je „opšta forma kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.“[[1]](#footnote-2)

Naime, teškoće u definisanju kompjuterskog kriminaliteta proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može obuhvatiti jednom definicijom.

Jedan od autora koji je razmatrao problem kompjuterskog kriminala jeste Don Parker. Njegov zaključak je da je: „zloupotreba kompjutera svaki događaj u vezi sa upotrebom

kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac djeluje u namjeri da sebi pribavi ili bi mogao da pribavi korist.“[[2]](#footnote-3)

Kompjuterski (Cyber) kriminal predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog djela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posljedica.

Cyber-kriminal je takođe protivpravna povreda imovine kod koje se računarski podaci sa predumišljajem mijenjaju, razaraju ili se koriste zajedno sa hardverom.[[3]](#footnote-4)

Tako u isto vreme računari, kao i cijela informaciono-komunikaciona mreža, mogu biti i meta napadača, ali i oruđe tj. alat napadača, da bi kasnije bili i dokaz u forenzičko-

istražnom postupku.

Svjetski rječnik engleskog jezika ovaj pojam određuje na sledeći način: „Kompjuterski kriminalitet obuhvata nezakonite aktivnosti koje se vrše na kompjuteru ili kod kojih je kompjuter sredstvo izvršenja. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoć u izvršenju prevara.

Na desetom Kongresu Ujedinjenih Nacija za prevenciju kriminaliteta i tretman delikvenata, razmatrana je ova problematika: Kompjuterski kriminalitet je opšti pojam koji obuhvata krivična djela koja se vrše posredstvom kompjuterskog sistema ili mreže, u kompjuterskom sistemu ili mreži, ili protiv kompjuterskog sistema ili mreže. U principu on uključuje bilo koje krivično delo koje se vrši u elektronskom ambijentu.“ [11]

Različiti dokumenti na različite načine klasifikuju oblike cyber kriminala. Još 2000. godine Ujedinjene nacije su na svom Desetom kongresu za suzbijanje kriminala i postupanju prema prestupnicima podijelile cyber-kriminal na dvije sub-kategorije:

1. Cyber-kriminal u užem smislu – svako nezakonito ponašanje usmjereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju

2. Cyber-kriminal u širem smislu – svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posjedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža

# [***TIPOVI CYBER KRIMINALA***](http://megatrender.blog.rs/blog/megatrender/megatrender-19/2008/03/06/tipovi-cyber-kriminala)

U dokumentu Ujedinjenih nacija, na Desetom kongresu, navode se i konkretni oblici syber kriminaliteta u skladu sa Preporukom Saveta Evrope i listom OECD-a iz 1989., odnosno 1985. godine.

To su:

1) neautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mjera sigurnosti (haking);

2) oštećenje kompjuterskih podataka ili programa;

3) kompjuterske sabotaže;

4) neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama; i

5) kompjuterska špijunaža.

Svaki od ovih oblika može se ukrštati sa svakim jer gotovo da ne postoji “čisti” oblik.   
Tako haking, pored neovlašćenog ulaska u kompjuterske sisteme i mreže, često obuhvata i uništenje podataka ili kompjutersku špijunažu (kao što je to slučaj sa upadima na veb sajtove i uništenje ili “prepravljanje” podataka na njima ili haking i trgovina pasvordima).  
Izmena kompjuterskih podataka i programa uključuje i “lansiranje” kompjuterskih crva i virusa što je najčešće praćeno zaustavljanjem rada kompjuterskog sistema, uništenjem podataka. U mrežama crvi i virusi se u većini slučajeva “razmenjuju” elektronskom poštom, a ne retko to čine i hakeri prlikom neovlašćenog pristupa.  
Od dijela cyber kriminala u širem smislu najčešće se pojavljuju:

1) kompjuterski falsifikati;

2) kompjuterske krađe;

3) tehničke manipulacije uređajima ili elektronskim komponentama uređaja;

4) zloupotrebe sistema plaćanja kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima.

Njima se u novije vreme dodaju i djela podržana računarima. Ova djela obuhvataju “rasturanje” materijala ili samo njihovo posjedovanje pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbjegavanje pravde. U ova djela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih i srodnih prava, prodaja zabranjene robe (oružja, kradene robe, lijekova) ili pružanje nedozvoljenih usluga (kockanje, prostitucija). Najviše pažnje u ovoj grupi djela privlači dječija pornografija i distribucija raznih materijala Internetom .

Evropska konvencija o cyber kriminalu predviđa 4 grupe djela:

a) djela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, passworda;

b) djela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;

c) djela vezana za sadržaje – dječija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posjedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka;

d) djela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primjeraka djela kompjuterskim sistemima.

Naravno, Konvencija pod kompjuterskim sistemom podrazumijeva i kompjuterske mreže.

U Enciklopediji cyber kriminala navodi se da FBI i Nacionalni centar za kriminal “bijelih kragni” SAD (National White Collar Crime Center) otkrivaju i prate sledeće oblike:

a) upade u kompjuterske mreže;

b) industrijsku špijunažu;

c) softversku pirateriju;

d) dječiju pornografiju;

e) bombardovanje elektronskom poštom;

f) “njuškanje” passworda;

g) “prerušavanje” jednog računara da elektronski “liči” na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama; i

h) krađu kreditnih kartica.

Zavisno od tipa počinjenih dijela cyber kriminal može biti:

***a) Politički, koga čine:***

1. cyber špijunaža;

2. haking;

3. cyber sabotaža;

4. cyber terorizam;

5. cyber ratovanje.

***b) Ekonomski:***

1. cyber prevare;

2. haking;

3. krađa Internet usluga i vremena;

4. piraterija softvera, mikročipova i baza podataka;

5. cyber industrijska špijunaža;

6. prevarne Internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procjena, nadgrađivanje cijene proizvoda, udruživanje radi postizanja veće cijene, trgovina robom sa crnog tržišta, višestruke ličnosti).

***c) Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja:***

1. dječija pornografija;

2. pedofilija;

3. vjerske sekte;

4. širenje rasističkih, nacističkih i sličnih ideja i stavova;

5. zloupotreba žena i djece.

***d) Manipulacija zabranjenim proizvodima, supstancama i robama:***

1. drogom;

2. ljudskim organima;

3. oružjem.

***e) Povrede cyber privatnosti:***

1. nadgledanje e-pošte;

2. Spam

3. Phishing

4. prisluškivanje, snimanje “pričaonica”

5. praćenje e-konferencija

6. “kačenje” i analiza “cookies”.

Jasno je da veliki broj različitih klasifikacija sam po sebi pokazuje raznovrsnost ovih djela i kompleksnost njihovih pojavnih oblika, ali i različitost kriterijuma koji se koriste. U svakom slučaju to bi pored upada u kompjuterske sisteme i mreže, špijunaže, sabotaže, piraterije, bombardovanja elektronske pošte primanjem neželjenih poruka, “njuškanja” passworda, “prerušavanja” jednog računara drugim, bili i virusi, odnosno njihova proizvodnja i distribuiranje, kao i cio skup nedozvoljenih i štetnih sadržaja od dečije pornografije do rasturanja vjerskih, rasističkih i sličnih sadržaja. Posebno su brojna djela diseminacije nedozvoljene robe ili pružanje nedozvoljenih usluga. Tome treba dodati i cyber sabotaže i terorizam, kao i krađu Internet vremena, usluga, indentiteta, razne zloupotrebe kreditnih kartica.

# ***Najčešći tipovi napada i tehnologije koje se zloupotrebljavaju***

Nove tehnologije u mnogome olakšavaju da posao koji obavljamo se uradi brže i bolje radeći ga preko mreže, kao i da lakše komuniciramo sa drugima i da se eventualno i zabavimo. Međutim iste te tehnologije ujedno olakšavaju posao i „cyber-kriminalcima“, ljudima koji koriste globalnu mrežu za ilegalne svrhe. Oni na različlite načine, i iz različitih pobuda pokušavaju da upadnu u sisteme kompanija, personalne računare, u našu svakodnevicu. Za ovakve „posliće“ cyber-kriminalci koriste različita sredstva i metode, a njihova inovativnost iz dana u dana sa razvojem tehnologija sve je veća.

Tehnologije koje napadači najčešće zloupotrebljavaju su:

***1. Dostupnost „žrtava“***

Iako je Internet nastao još 80-tih godina prošlog vijeka (prije toga je 1969. napravljen ARPAnet), svoju ekspanziju je doživio tek u prvoj deceniji novog stoljeća. Kao što možemo da vidimo u statističkim podacima broj Internet korisnika iz dana u dan sve je veći. Zahvaljujući Internet provajderima, globalna mreža postaje dostupna svima i u svaki čas (broadband).

Dostupnost Internetu za korisnike ima brojne koristi: poslovne, komunikacijske, zabavne... međutim kao što smo rekli ta dostupnost koristi i cyber-napadačima. Brza internet konekcija pruža mnogo veću mogućnost cyber-kriminalcima da vam za kratko vrijeme upadnu u računar i ukradu podatke, da vam sruše sistem, da vam ubace maliciozni kod, bilo to virus, trojanac, crv, spyware ili malware.

***2. Bežične mreže***

Bežično umrežavanje je još jedna tehnologija u ekspanziji, kako kod poslovnih korisnika tj. poslovnih mreža tako i za privatne korisnike. Bežični hot-spotovi postali su obavezni inventar na svim javnim mestima, kako u hotelima, na aerodromima i u parkovima, tako i u svakom modernom kafiću. Bežična tehnologija omogućava korisnicima pokretnost, i vezu sa Internetom na gotovo svakom koraku. Međutim ova tehnologija omogućava cyber-kriminalcima da lako i bez traga upadnu u vašu mrežu i sistem, jer gotovo svako sa lap-topom može presresti signal vašeg bežičnog rutera ako barem ne probate da ga zaštite.

Za ovakav vid upada kreiran je i poseban softver (kao na primjer Wi-fi Hack). Novi bežični pristupni uređaji, za razliku od starih, po defaultu koriste enkripciju, međutim treba se postarati da se koristi bezbednija enkripcija kao što je WPA/WPA2 ili 802.11i prije nego WEP enkripcija, koju je lakše provaliti.

Takođe trebala bi se primjenjivati i enkripcija aplikacija koje koriste bežičnu mrežu (SSH ili TLS/HTTPS), a može se čak i zaštiti saobraćaj koji se obavlja preko te bežične mreže(VPN-om ili Ipsec-om)

***3. World Wide Web (WWW)***

Iako WWW ne spada u novije tehnologije, i dalje spada medju omiljene tehnologije za ekspolataciju cyber-kriminalcima, jer svako ko se poveže na Internet uglavnom koristi Web pretraživače. Dok se nekad WWW bazirao uglavnom na tekstu i bio bezbjedan za korišćenje, danas WWW koriste podprograme (Java i ActiveX kontrole), kako bi se korisnicima omogućilo bogato multimedijalno iskustvo. Međutim te podprograme napadači mogu da iskoriste kako bi izvršili svoje maliciozne programe na vašem računaru. Zato je važno vršiti redovan update kako operativnih sistema tako i antivirusnih sistema.

***4. E-mail poruke***

E-mail poruke su postale nezaobilazan dio naše svakodnevice i predstavljaju jedan od najlakših načina komunikacije. Gotovo svaki građanin ima svoju e-mail adresu. Baš zbog tolike rasprostranjenosti upotrebe e-mail poruka, kao i zbog nekih karakteristika lakih za zloupotrebu, e-mail poruke predstavljaju jedan od omiljenih sredstava cyber-kriminalaca. Koristeći lažne adrese oni mogu nam slati spam ili phishing poruke, prijetnje, dječju pornografiju, ili neki drugi vid nelegalne korespodencije i ostati nekažnjeni zbog toga.

***5. Unificirane komunikacije***

Velike kompanije sve više koriste ovaj vid tehnologije, dobijajući prednost u tome što mogu da objedine više vidova komunikacije: e-mail, telefoniju, IM servis, konferencijske veze. VoIP (Voice over IP) tehnologija sve češće zamjenjuje tradicionalne telefonske servise. Međutim, isto kao što su vaši podaci ranjivi isto tako su ranjivi i VoIP paketi jer se lako mogu presresti.

***6. Prenosivi mediji***

Bilo koji od prenosivih medija (flopi diskovi, CD/DVD diskovi, USB fleš diskovima ili bilo koji drugi prenosivi mediji) predstavljaju pravu „Meku“ cyber-kriminalcima. Preko njih se lako šire maliciozni kodovi, a zahvaljujući tome cyber-kriminalci lako mogu pristupiti vašim podacima, prekopirati i obrisati ih. Kako bi spriječili zloupotrbu prenosivih medija, mnoge banke i kompanije dozvoljavaju upotrebu samo kompanijskih prenosnih uređaja, koji se mogu koristiti samo i isključivo unutar kompanije. Takođe se može u Grupnim polisama ili u registru onemogućiti upotreba USB i IEEE 1394 portova.

***7. E-commerce i online banking***

Iako u našoj zemlji su ljudi još pomalo skeptični, ova tehnologija ulazi polako na sporedna vrata. Sve više i više korisnika (kako pravnih tako i fizičkih lica) završava poslove preko Interneta. Prednosti su brojne: od brzine korespodencije i ne gubljenja vremena do povezivanja sa ostalim pravnim i fizičkim licima, kao i dobrim marketingom za svoj proizvod. Ali baš zato što se ovde radi uglavnom o novcu, cyber-kriminalci vole ovu tehnologiju. Oni lako mogu doći do pozicije da upravljaju vašim novcem. Najčešći oblici zloupotreba ove tehnologije su: prevare, krađe, pronevjere, nelojalna konkurencija, manipulacije sa elektronskim novcem itd. Godine 2006. Američko udruženje za zaštitu potrošača (NLC) napravilo je istraživanje za otkrivanje najčešćih Internet prevara.

Lista 10 najčešćih Internet prevara izgledala bi ovako:

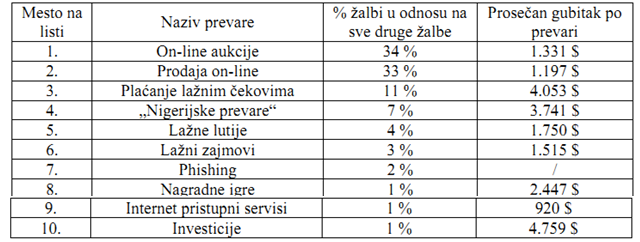


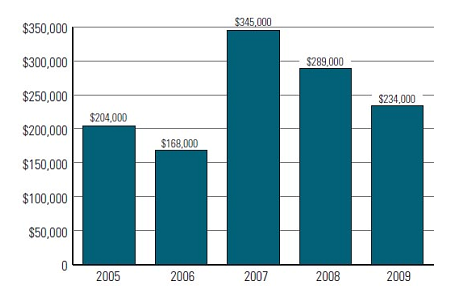
Tabela 4: Lista 10 najčešćih Internet prevara[[4]](#footnote-5)

Prema zvaničnim podacima za 2007. godinu, šteta nanijeta kompjuterskim kriminalom u USA iznosi negde oko 66 miliona dolara[[5]](#footnote-6)

Međutim vjeruje se da je cifra štete nanijete kompjuterskim kriminalom znatno veća, jer mnoge kompanije, među kojima su i one najveće, nisu prijavile štetu organima vlasti iz više razloga, prije svega misleći da će im to donijeti negativan publicitet, zatim da će konkurentske firme to znati iskoristiti, zato što ne vjeruju da organi vlasti mogu bilo šta da urade po tom pitanju kao i iz mnogih drugih razloga. Vrlo često korporacije sami angažuju vrsne stručnjake iz oblasti digitalne forenzike, kako bi izvršili unutrašnju (korporacijsku) analizu napada, odnosno nanete štete.

Američki institut za informacionu bezbjednost (Computer security institute (CSI); www.gocsi.com ) i ove godine, kao i ranijih, sproveo je istraživanje o najčešćim bezbjednosnim incidentima, kao i o štetama prouzrokovane tim incidentima. U istraživanju su učestvovali stručnjaci za bezbjednost IKT iz raznih malih i velikih kompanija, vladinih agencija, finansijskih, obrazovanih i medicinskih institucija itd. Neka od najvažnijih i najinteresantnijih zaključaka su:[[6]](#footnote-7)

:



Slika 2. Prosječan gubitak kompanije/ustanove po incidentu

Kao što možemo vidjeti na slici 2. prosječni gubici po incidentu su se smanjili za skoro 20%, sa 289.000$ na 234.000$. Ovdje treba reći da su na vrhu ove skale troškova zloupotreba wirelessa (770.000$), krađa identifikacionih podataka kao i podataka o zdravstvenom osiguranju (710.000$) i naravno finansijske prevare (450.000$). Treba reći i da su ispitanici prijavili veliku upotrebu takozvane „Return of investment“ kao bezbjednosne mjere zaštite, tj. uložili su u bezbjednost svojih informaciono komunikativnih sistema manje sredstava nego što bi izgubili da to nisu učinili. Napredak u bezbednosti IK sistema možemo uočiti ako kažemo da je 2001. godine prosječan gubitak kompanije/ustanove po incidentu prelazio višemilionske cifre.



Slika 3. Najčešći bezbjednosni incidenti po kompanijama/ustanovama

Kao što se sa slike 3. može vidjeti incidenti koji su se imali najveći porast u odnosu na 2008. godinu su incidenti sa Malware-om, DoS incidenti, finansijske prevare i krađa šifri. Isto tako može se zaključiti da su incidenti sa zloupotrebom wirelessa kao i incidenti izazvani od strane insajdera u kompaniji/ustanovi u padu u odnosu na prethodnu godinu.

Najčešće metode kojima cyber-kriminalci pokušavaju da probiju našu bezbjednost su:

***1. Krađa i zloupotreba šifara***

Tehnologija u današnje vrijeme je isuviše napredovala, te tako šifre, koje predstavljaju samo niz karaktera, čak i one najsloženije, u nekom vremenskom roku mogu da se pronadju, procesuirajući ih sa nekim „cracking“ alatom kroz neki drugi računar. Metode cyber-kriminalaca da razbiju šifre su:

* Napad slučajnim pogađanjem – u nekim slučajevima šifre se mogu biti nasumičnim pogadjanjem. Ponekad korisnici čak ni ne upisuju šifru, ponekad su to tipične reči: password ili admin, ime korisnika, adresa ili broj kancelarije u kojoj korisnik radi...
* Napadi „rječnikom“ – korisnici često upotrebljavaju uobičajne riječi (GOD, LOVE, SEX ) ili kratke (kraće od 8 karaktera) i lako pamtive riječi iz rječnika koje cyber-kriminalci lako otkriju.
* Napadi „brutalnom silom“ – kod napada „brutalnom silom“ koristi se svaka moguća kombinacija, i ukoliko je to moguće uvek će se doći do željene šifre. Ali u zavisnosti od složenosti šifre, brzine računara koji pokušava da otkrije tu šifru, kao i hash funkcije pitanje je koliko vremena će proteći dok ne dodje do probijanja šifre. Cyber kriminalcima obično treba da do te šifre dođu u što kraćem vremenskom periodu.
* „Hibridni“ napadi – hibridni napadi su ustvari unapređena vrsta napada rječnikom. Isto se koriste određeni rječnici, ali i određeni koji određeno slovo zamenjuje karakterom ili brojem (npr. J0hn123)

Najbolje bi bilo kada bi pored autentifikacije šifrom koristili još neki vid autentifikacije (sigurnosni token, ID karticu, biometriju...). Međutim i sa dobrom sigurnosnom polisom i snažnim šiframa može se otežati posao cyber kriminalcima.

Prvo se polisom mora ograničiti broj pokušaja ukucavanja šifara (npr. nakon trećeg neuspješnog pokušaja blokiraće se sistem), a zatim se treba izabrati snažna šifra svakom korisniku. Broj lične karte, pasoša, telefona, mobilnog telefona, ime Vaše majke, oca, deteta, ljubimca, čak ni devojačko prezime Vaše majke i rođendani nisu podobni za snažnu šifru, a korišćenje takve šifre od strane krajnjeg korisnika čine šifru beskorisnom. Dobru i snažnu šifru čini kombinacija velikih i malih slova, brojeva kao i specijalnih karaktera.

Treba izbjegavati reči iz rječnika, a šifra treba da bude dovoljno dugačka, ali opet ne preduga kako bi je korisnik lakše zapamtio a ne zapisao jer ma koliko šifra bila jaka i snažna, ako korisnik je zapiše i drži na vidnom ili dostupnom mestu ona postaje dostupna cyber-kriminalcima. Vrlo često se umjesto jedne riječi upotrebljava i fraza sastavljena od više karaktera, brojeva i specijalnih karaktera.

***2. Trojanci***

Trojanci predstavljaju specifičan malware čija je spoljna manifestacija obično zabavna i interesantna prosečnim korisnicima., koji omogućavaju cyber-kriminalcima udaljen pristup kompjuterskom sistemu, a da korisnici čak i ne primjeti. On ne inficira ostale izvršne datoteke, jer se ne umnožava (replicira). Trojanci nisu virusi zato što se ne umnožavaju, već stoje i čekaju da budu pokrenuti, direktnim aktiviranjem, ili uz pomoć drugog programa koji ga pozove. Svako danas može napraviti Trojanca i povezati ga sa nekom benignom aplikacijom. Ta aplikacija se zajedno sa Trojancom korisnicima dostavlja na razne načine: direktnim unosom, kada neovlašćeno lice sedne za računar i preko prenosnog medija ubaci Trojanca, kao attachment u e-mail poruci, kroz download softvera od strane korisnika, kroz Web izvršive aplikacije (ActiveX), kroz propuste u programskim kodovima Web pretraživača, Media plejerima, IM klijentima, kao i mnogim drugim aplikacijama. Vrste šteta koje Trojanci prave su takođe varijabilne: neovlašćeno skidanje, prepravljanje ili brisanje podataka kao i e-mail poruka, instalacija softwarea prikrivanje drugih procesa. Međutim cilj većine Trojanaca je da omogući udaljenom korisniku pristup i punu kontrolu nad napadnutim računarom. Česti su i napadi koji iskorištavaju računar korisnika za napad na neki server, radi zloupotrebe ili kompjuterskog kriminala, što se pripisuje vlasniku sistema.

Postoji mnogo vrsta Trojanaca, ipak po svojim osobinama ističu se dva najpoznatija: ***SubSeven i NetBus.***

***Subseven*** je jedan od najnaprednijih virusa naprednih karakteristika i sposobnosti.

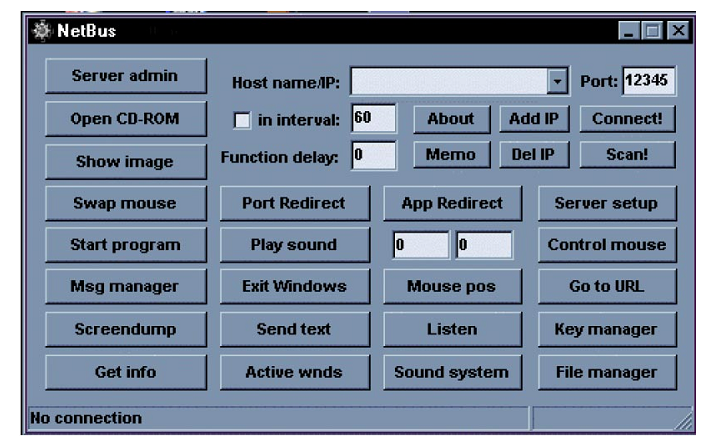
Na slici 5. možemo vidjeti izgled Trojanca SubSeven zajedno sa nekim od mogućnosti koji pruža napadaču.

Slika 5. Izgled Trojanca SubSeven



Napadač uz pomoć SubSeven Trojanca može da: prekopira cio adresar, izvrši IP skeniranje sa udaljene lokacije, host lookup, dobiti broj Windows Cdkey-a, preuzme ili špijunira sve Instant Message servise, kreira FTP root folder, rediriguje portove, preuzme ili obriše fascikle, kao i da napravi nove, preuzme menadžer procesa, preuzme dial-up konekciju(ako postoji) zajedno sa korisničkim imenom i šifrom, restartovanje servera kao i preuzimanje podataka sa njega (Adresa, ime, grad, kompanija, e-mail, ...) itd.

***Netbus*** spada u grupu starijih Trojanaca, međutim zbog brojnih mogućnosti i danas se mnogo upotrebljava. Na slici 6. možemo vidjeti izgled Trojanca NetBus zajedno sa nekim od mogućnosti koji pruža napadaču.



Slika 6. Izgled Trojanca NetBus

Odlike NetBus Trojanca su: otvaranje CD/DVD uređaja (jednom ili u određenom intervalu), zamjena f-ja miša (lijevi klik postaje desni i obrnuto), startovanje određene aplikacije, puštanje određenog zvuka (zbog starosti Trojanca u opciji je samo WAV fajl), pojačavanje i u utišavanje zvuka, gašenje računara, direkcija ka određenoj URL adresi, postavljanje (Upload), skidanje(downlaod) i brisanje (delete) podataka sa/na računar „metu“.Međutim najopasnije opcije ovog Trojanca su: redirekcija podataka kao i aplikacija sa računara „mete“ na određeni port ili na drugi računar „metu“ pri čemu taj drugi računar kao napadača vidi samo prvi računar „metu“ a ne i pravog napadača.

Trojanci se obično sastoje od server i klijent djela, pri čemu je server program koji treba da se ubaci u računar „metu“. Najčešći metod ubacivanja Trojanca u neki računar je sa nekom drugom aplikacijom. Na primjer napadači mogu uzeti neku bezazlenu igricu (kao primjer uzecu kartasku igru Texas HoldEm poker):



Aplikacija napadača lako i bezo će sjediniti ova dva fajla u jedan fajl razno.exe, koji se lako kasnije preimenuje u Texas.exe. Razlika između originalnog Texas.exe fajla i zaraženog Texas.exe fajla je samo u njihovim veličinama (i to ne znatno). Sada ostaje samo da postavi igricu na neki server. Kada korisnik skine fajl i pokrene ga, korisniku će sve izgledati normalno, pokrenuće igru pokera koju je tražio, međutim u pozadini serverski dio Trojanca se instalira i ako je korisnik na Internetu šalje podatke napadaču o podacima korisnika koga je zarazio. Napadač kroz klijentski deo Trojanca pristupa zaraženom računaru kroz Serverski deo.

Na svu sreću današnji antivirus programi kao i razni malware skeneri otkrivaju gotovo sve vidove Trojanaca. Baš zato kao najbolja odbrana od Trojanaca je redovan update kako antivirus i „antimalware“ softvera, tako i svih ostalih aplikacija na sistemu kao i operativnog sistema jer programeri kad otkriju „rupu“ u kodu nastoje da je što pre zatvore i odmah šalju zakrpe kojima se to postiže. Takođe treba se vršiti redovno skeniranje sistema, čitave mreže, a za Trojance možda i najbitnije monitoring odlazećeg saobraćaja.

***3. Iskorišćavanje podrazumijevanih vrednosti***

Nema ništa lakše i ljepše jednom cyber-kriminalcu nego kad neki korisnik koristi podrazumijevane vrednosti koje je dobio pri kupovini računara od proizvođača ili prodavca.

Mnogi napadački softveri pretpostavljaju da su na računaru tj. u računarskom sistemu koji napadaju podrazumijevane šifre i da je sistem podešen na podrazumijevane vrednosti. Internet je prepun sajtova sa katalozima podrazumijevanih korisničkih imena, pristupnih šifri, konvencija imena raznih proizvođača, ali isto tako i komponenata, servisa i konfiguracija.

Zaštitne mjere od ovoga sigurno bi bile da se promene podrazumijevane vrednosti šifara, da se isključe „gostinski“ nalozi kao i nalozi korisnika koji nisu više u kompaniji, da se isključe servisi koji se ne upotrebljavaju (npr. Telnet ili FTP). Takođe pokušajte da izbegnete instalaciju softvera u njihove standardne fascikle.

***4. Čovek u sredini***

Pri napadima „Čovek u sredini“, napadač uspijeva da zavara korisnika da pristupa pravom serveru tj. servisu, a ustvari korisnik pristupa sistemu kojeg kontroliše napadač.

„Čovek u sredini“ napad obično počinje sa phishing e-mailom, koji deluje bezazleno i koji sadrži URL adresu. Međutim ta URL adresa vodi korisnika na adresu na zloćudni sistem kontrolisan od napadača, koji ima isti interfejs kao i legitimni server tj. servis. Napadač time dobija podatke za logovanje korisnika na pravi server, a time i raspolaže i resursima korisnika na tom serveru bez njegovog znanja. Ovo je lakši metod napada „čovek u sredini“, teže metode podrazumijevaju dupliranje MAC-a (Media Access Control), trovanje ARP-a(Address Resolution Protocol) kao i tabela rutiranja i DNS(Domain Name Server) pretrage, pravljenje novih lažnih routing tabela, napad na DNS server korisnika kao i servera kojem korisnik pristupa, rerutiranje proxija...

Najbolji vid zaštite je ne kliktati na URL adrese sumnjive prirode. Takođe za ovakve napade pomaže i IDS(Intrusion Detection System) sistemi koji prate mrežni saobraćaj, kao i promene lokalnog sistema.

Osim ovih prevara u syber prevare uračunavaju se i prevare putem kontakata i to:

***„Valentino“ prevare***

Valentino prevare predstavljaju oblik internet prevara sa najvećom stopom rasta. Sama prevara povezana je sa „uslugama“ koje se pružaju usamljenim osobama i imaju za predmet sklapanje brakova ili drugi vid druženja. Budući da savremeni način života neretko dovodi do otuđenja nezanemarljiv broj ljudi spreman je da izdvoji abnormalne svote novca i pristaju na praktično sve uslove kako bi rešili svoj problem. “Srodne duše” nikada ne žive u istoj zemlji kao i žrtva, već naprotiv u zemlji koja je izuzetno udaljena, i koju karakterišu socijalna previranja. Osoba je obično veoma atraktivna, komunikativna i slabog je ili veoma lošeg imovnog stanja. Komunikacija se najčešće odvija putem e-maila i razmenom fotografija.U poslednje vrijeme nerijetko dolazi i do angažovanja školovanih osoba privlačnog izgleda kako bi se kontakt odvijao i putem web kamera - to cjelokupnom odnosu daje viši stepen realnosti, i “žrtve” brže pristaju na ispunjenje zahtjeva. Nakon proteka određenog vremena, i uspostavljanja bliže veze, prevarant iskazuje želju da upozna svoju “žrtvu”, a kako bi došlo do njihovog susreta, neophodno je da “žrtva” pošalje određenu količinu novca da bi njena “srodna duša” mogla da doputuje u udaljenu zemlju. Istog momenta kada dođe do transfera sredstava, kontakt prestaje.

Prema podacima centra za istraživanje kompjuterskog kriminala, žrtve često pristaju da isplate i sume u iznosu od 5000 $US. Valentino prevare nisu jedini tip prevara čiji mehanizam se bazira na zloupotrebi emocija, ali svakako imaju zapaženo učešće u ukupnom broju izvršenih prevara.

***„Lančana pisma“***

Lančana pisma predstavljaju takvu vrstu e- mailova u kojima se od vas traži da dobijeni mail proslijedite određenom broju u vaših prijatelja. Neka od ovih pisama funkcionišu zahvaljujući činjenici da se u istima navodi da će osobu koja ne proslijedi pismo pratiti nesreća, dok se u drugima navodi da će se određenoj osobi ( najčešće djetetu sa odredjenim tjelesnim deformitetom ) isplatiti izvjesna suma donacije za svaki e - mail koji proslijedite.

Nipošto nemojte prosleđivati lančano pismo, a najbolje bi bilo i da ih ne pročitate, odnosno da ih obrišete, budući da takva pisma sadrže kriptovane informacije koje će licu koje je poslalo lančano pismo omogućiti da zloupotrijebi vaše lične podatke,ali i podatke vaših prijatelja, kao i svake osobe koja primi i pročita lančano pismo.

***Piramidalne šeme***

Piramidalne šeme ( poznate su i pod nazivom : šeme afiniteta ) predstavljaju takve vrste prevara kod kojih se “žrtvi” obećava isplata određene svote novca za privlačenje izvesnog broja ljudi, kao i za uključivanje istih u rad same “piramide”. Provera kojom se dokazuje da se u ponudi radi o piramidalnoj šemi je prilično jednostavna i podrazumijeva samo primjenu osnovnih matematičkih operacija – naime, ukoliko saberete broj ljudi koji su neophodni da se zatvori konstrukcija piramide može se vrlo lako desiti da je potreban angažman većeg broja ljudi od onog koji trenutno nastanjuju planetu Zemlju. Najčešći broj nivoa u piramidalnoj šemi iznosi 12 ili 13, no može biti i drukčiji. Bilo kakva ponuda ovog tipa je ilegalna, ne preporučuje se da učestvujete u njoj.

***„Lutajući“ trgovci***

Lutajući trgovci su zlonamjerni prodavci koji se bave prodajom usluga i dobara. Prilikom obavljanja on - line prodaje, lutajući trgovci najčešće: reklamiraju nepostojeću robu, daju lažne izjave povodom kvaliteta robe koju tobože prodaju, prodaju robu koja je opasna po zdravlje, ne daju vam bitne informacije koje se tiču visokih prevoznih troškova, vrše isporuku robe koja je drugačija od one koju ste naručili, ne isporučuju naručenu robu na vrijeme ili nikada ne izvrše isporuku.

***Transfer novca u dobrtotvorne svrhe***

Kod ovog tipa prevara “žrtvi” se nudi određena provizija ukoliko prihvati da primi određeni transfer novca preko svog bankovnog računa. Potom se od “žrtve” traži da podigne novac sa računa, i da ga ponovo transferiše na neki račun u inostranstvu (najčešće su u pitanju ostrvske zemlje), navodno u dobrotvorne svrhe. Ovakva vrsta transfera predstavlja ozbiljno krivično delo, obzirom da za cilj ima prikrivanje porijekla novca ( pranje novca ) i učešćem u ovakvim transferima osoba postaje saučesnika u krivičnom delu. Nijedna legalna donatorska asocijacija ne vrši trarsfere novca na ovaj način.

***Lutrijske prevare***

Ovaj vid prevara na internetu ne predstavlja retkost. Sam mehanizam najčešće funkcioniše na sledeći način: mada se vjerovatno nikada niste prijavili za učešće u nekoj nagradnoj igri ovog tipa, vama stiže obavještenje u kome se saopštava da ste dobitnik premije. Nakon toga, od vas se ili zahtijeva da pošaljete izvesnu sumu novca u cilju slanja dobijene nagrade, ili se traži da predate broj vašeg bankovnog računa, kao i da date određene lične podatke. Često se od “žrtve” zahtijeva da u cilju potvrđivanja prava na nagradu pozove broj telefona, pri čemu takav poziv karakteriše abnormalno visoka tarifa.  Lutrijske prevare omogućavaju sticanje ogromnih količina novca, i iza takvih tipova prevara stoje visokoorganizovane grupe.

# ***ZAKLJUČAK***

Ono što je nesporno je da je kompjuterski kriminal više vezan za aktivnosti pojedinaca, a kriminal vezan za kompjuterske mreže više je djelo grupa i to organizovanih, profesionalizovanih pa sve češće i strogo specijalizovanih. Ove grupe su, s jedne strane, “tradicionalne” grupe organizovanog kriminala koje su se usavršile i osavremenile primjenom informaciono komunikacione tehnologije i pripremile za “izlazak” na cyber scenu.

S druge strane, javljaju se i posebne organizovane cyber grupe - cyber mafija. Ova mafija ima svoja pravila, drugačiji način ponašanja od konvencionalne mafije, kao što ima i specifično okružje. Njene aktivnosti su umnogome olakšane specifičnostima okruženja u kom deluju i oružja koja koriste.

Okruženje je virtuelno, oružje je informaciono, a znanje je specijalizovano. Internacionalizam, transnacionalnost, multidimanzionalnost samo su neka od svojstava ovih grupa.

Razmatrajući karakteristike kompjuterskog kriminaliteta, a naročito njegove posljedicice, očigledno je da se isti razlikuje od svih drugih oblika kriminalnog djelovanja po stepenu opasnosti u odnosu na napadnuta dobra. Ova konstatacija je još više došla do izražaja kada se shvatilo da mnoge kriminalne aktivnosti potpomognute uticajem oblika kompjuterskog kriminala postaju još opasnije i štetnije.

Ključ uspješne zaštite od syber mafije je u povećanom oprezu i konstantnoj budnosti. Upotrebimo zdrav razum, kao što to činimo i u pravom životu. Ne treba verovati strancima, ne surfovati na mjestima „sumnjive“ prirode, ne dajte korisne i povjerljive informacije. Preduzmemo li neke mjere predostrožnosti i dalje možemo koristiti svijet informacija a da pritom ne postanemo nečija žrtva.

Ohrabruje činjenica da su mnoge države postale svjesne ove pojave i da su u svom pozitivnom krivičnom zakonodavstvu predvidjele pojavne oblike kompjuterskog kriminaliteta kao posebna krivična djela. Sa druge strane, ohrabrujuće je i to što se u sve većem broju naučnih i stručnih radova pažnja posvećuje upravo ovom obliku kriminalnog ponašanja. Na taj način dolazi do razotkrivanja mnogih specifičnosti kompjuterskog kriminaliteta, a istovremeno se otvara mogućnost suprotstavljanju njegovim oblicima od strane društvene zajednice.

# ***LITERATURA***

Kassner Michael: “10 ways to avoid IT security breaches”, TechRepublic,

http://techrepublic.com.com/

Perrin Chad: “10 things you should do to secure every general-purpose operating

system”, TechRepublic, <http://techrepublic.com.com/>

Shinder Debra Littlejohn: “10 technologies that cybercriminals love to exploit”,

TechRepublic, http://techrepublic.com.com/

Steward James Michael: “Ten ways Hackers Breach Security”, Global Knowledge,

http://www.globalknowledge.com/

„An Introduction to Computer Security: The NIST Handbook“, National Institute

of Standards and Technology Technology Administration,

http://www.nist.gov/index.html

“Kompjuterski kriminalitet”, APIS Security Consulting, http://www.apisgroup.org/sec.html?id=29

“The top 10 Internet Frauds”, National Fraud Information Center,

http://www.nclnet.org/

Statistički podaci o korisnicima Interneta, http://www.internetworldstats.com/

Mirjana i Ratimir Drakulić, “Cyber kriminal“FON, Autor megatrender Beograd 2008.

Tenth United Nations Congress on the Prevention of Crime and the treatment of **Offenders, www.un.org**

“The top 10 Internet Frauds”, National Fraud Information Center, http://www.nclnet.org/

Computer Security Institute, http://www.gocsi.com

Robert Rihardson: „2009 CSI Computer Crime & Security Survey“, Computer Security Institute,

http://www.gocsi.com

[www.maturski.org](http://www.maturski.org/)

1. “The top 10 Internet Frauds”, National Fraud Information Center, http://www.nclnet.org/ [↑](#footnote-ref-2)
2. Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.un.org [↑](#footnote-ref-3)
3. “Kompjuterski kriminalitet”, APIS Security Consulting, http://www.apisgroup.org/sec.html?id=29 [↑](#footnote-ref-4)
4. “The top 10 Internet Frauds”, National Fraud Information Center, http://www.nclnet.org/ [↑](#footnote-ref-5)
5. Computer Security Institute, http://www.gocsi.com [↑](#footnote-ref-6)
6. Robert Richardson: „2009 CSI Computer Crime & Security Survey“, Computer Security Institute,

   http://www.gocsi.com [↑](#footnote-ref-7)