

UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

-STUDIJSKI PROGRAM-

SAVREMENE INFORMACIONE TEHNOLOGIJE

Đorđe Krunić

Etika, računarski kriminal i zaštita

Master rad

Mentor:
Prof dr Mladen Veinović

Student:
Đorđe Krunić
Br. indexa: 411431/2011



Beograd 2012

Etika, računarski kriminal i zaštita

Sažetak

U ovom radu opisana je etika računarski kriminal i zaštita. Etike su nacionalni stereotipi koje jedno društvo i nacija propagiraju o sebi samom i veoma se razlikuju. Tako da ono što je etički za jednu naciju ne mora da bude i za drugu. Računari i zaštita računara opisani su kroz njihovu upotrebu i zloupotrebu u radu.

Računarski kriminal i zaštita (*engleski computer crime and the protection of*) je opšti pojam koji obuhvata krivična dela koja se vrše posredstvom računarskih sistema ili mreže, u računarskom sistemu ili mreži, ili protiv računarskog sistema ili mreže. U principu on uključuje bilo koje krivično delo koje se vrši u digitalnom ambijentu. Bezbednost se odnosi na zaštiti računarskih sistema i informacija protiv neželjenog pristupa, oštećenja, modifikacije ili uništavanja.

Abstract

This paper describes the ethics of computer crime and security. Ethics are national stereotypes that a society and a nation propagated about himself and very different. So what is ethical for one nation may not be for another. Computers and computer protection are described through their use and abuse in the work.

Computer crime and the protection of is general term that covers criminal offenses are carried out by means of computer systems or networks, in a computer system or network, or against a computer system or network. Basically he includes any criminal offense which is done in digital ambience. Security refers to the protection of computer systems and information against unwanted access, damage, modification or destruction.

Sadržaj

1. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA 7

1.1. Uvodne napomene i obrazloženje rada 7
1.2. Predmet istraživanja 7
1.3. Ciljevi i zadaci istraživanja 8
1.4. Istraživačke hipoteze 8
1.5. Metodi istraživanja i tok istraživaćkog procesa 9

2. ETIKA, INFORMACIJSKA ETIKA I MORALNE NORME NOVIH TEHNOLOGIJA 10

2.1. Etika 10
2.1.1 Teorija dobrog ili vrednog 10
2.1.2 Teorija ispravnog 11
2.2. Informacijska etika 11
2.3. Etika i moralne norme novih tehnologija 13
2.4. Etičke dileme i nedoumice 16
2.5. Uticaj poslovne etike na poslovnu komunikaciju 17
2.6. Etičke norme 18
2.7. Neetičko ponašanje u elektronskom poslovanju 19
2.8. Porjeklo i pojam morala 20

3. RAČUNARSKI KRIMINAL 21

3.1. Pojam i definicija računarskog kriminala 21
3.2. Istorija računarskog kriminala 24
3.3. Karakteristike kompijuterskog (računarskog) kriminaliteta 24
3.4. Krađa preko računara 26
3.5. Računarske prevare 26
3.6. Računarska etika 28

4. SAJBER (CYBER) KRIMINAL 29

4.1. Tipovi (cyber) sajber kriminala 30
4.2. Razvoj (cyber) sajber kriminala 32
4.3. Sajber kriminal u Srbiji 33

5. SOFTVERSKA PIRATERIJA I VIRUSI 35

5.1. Softverska piraterija 35

5.2. Virusi 37
5.3. Nastanak virusa 38
5.4. Trojanski konj 38
5.5. Crv 40
5.6. Špijun 42

6. ZAŠTITA RAČUNARA I ZAŠTITA PODATAKA 43

6.1. Bezbednost – smanjenje rizika 44
6.2. Antivirusna zaštita 44
6.3. Lažni antivirusi 46
6.4. Ograničenje fizičkog pristupa 47
6.4.1. Lozinke 48

7. ZLOUPOTREBE I PREVARE PRIMENOM NOVIH TEHNOLOGIJA 49

ZAKLJUČAK 52

LITERATURA 54

Uvod

Etika je grana filozofije koja se bavi pitanjima moralnog ponašanja. Proučavanje etike može ponuditi sredstva za donošenje teških moralnih odluka, ličnih, profesionalnih. Cilj nije da se donose etičke odluke sa kojima će se svi složiti, već da se ojača naša sposobnost da na racionalnoj osnovi branimo kritičke sudove.

Reč moral izvedena je od latinske reči mos, moris, što znači (između ostalog) „način života“ ili „postupanje“. Ona se često povezuje sa religijskim verovanjem i ličnim ponašanjem. Reč etika, s druge strane, izvedena je od grčke reči ethos, što znači „običaj“, „upotreba“ ili „karakter“. O etici se često misli kao o racionalnom procesu primene postojećih principa prilikom sudara dva moralna ograničenja. Najteže etičke dileme nastaju kada dođe do sukoba dva „ispravna“ moralna ograničenja. Zato etika često podrazumeva ravnotežu suprotstavljenih ispravnih odgovora, tamo gde nema onih „tačnih“. Primer može biti radnik na poslu, koji obeća da će ćutati kada mu se kolega poveri da je potkradao firmu.

Kada se govori o računarima može se slobodno reći da oni uupravljaju našim novcem, zdravstvom železnicom, avio-saobraćajem i sl. Od nas se očekuje da verujemo u informacione tehnologije. Međutim potpuno poverenje u modernu računarsku tehnologiju može da bude apsurdno i, u dosta slučajeva opasno. U svakom ozbiljnom sistemu danas se razmatraju bezbednosni izvori primene savremenih informacionih tehnologija: pravne dileme, etička pitanja i rizici pouzdanosti. Ovi aspekti nas navode na značajnije pitanje: Kako možemo učiniti računare bezbednim tako da se možemo osjećati bezbednie u našem svakodnevnom poslovanju?[1]

Računari su jedna od najznačajnih i najrevolucionarnih tekovina razvoja tehničko-tehnološke civilizacije. Međutim pored svih prednosti i koristi koje sa sobom nose oni su postali i sredstvo zloupotrebe nesavesnih pojedninaca, grupa, čak i organizacija.

Raznovrsne forme primene računara odavno su interesantne pojedincima i grupama koje ne biraju sredstva i način protivpravnim ponašanjem pokušavaju da sebi ili drugima pribave imovinsku korist. Tako računari postaju sredstvo vršenja različitih oblika

[1] www.wikipwdija.org

nedozvoljenih, protivpravnih i društveno opasnih delatnosti. Računarski kriminal (ili visokotehnološki kriminal, sajber kriminal) obuhvata aktivnosti tokom kojih se kompijuteri, računarske mreže ili računarski podaci koriste kao izvor, sredstva, objekta ili mesta izvršenja određenog krivičnog dela.

Istorija računarskih virusa seže do početka druge polovine prošlog veka. U to vreme ozbiljniji računari su bili divovski uređaji čije dimenzije su iskazivane u metrima i tonama, smešteni u zasebne klimatizovane prostorije u blizini kojih se obično nalazilo energetsko postrojenje koje je obezbeđivalo potrebno napajanje.

Pravi procvat i masovnu pojavu virusi doživljavaju širenjem PC-a po kancelarijama i domaćinstvima, a potom razvojem Interneta, čime je stvorena ogromna baza korisnika - kako potencijalnih žrtava, tako i onih zlonamernih.[2]

Prvo poznato uklanjanje jednog računarskog virusa izvršeno je 1987. godine softverom Bernt Fiks, a radilo se o jednom od prvih poznatih virusa — Viena virusu.

Mnogo puta se govorilo i pisalo o programima koji se pretvaraju da su nešto što nisu. Najozloglašenija su lažna antivirusna rešenja - programi koji objavljuju poruke da je ciljani kompjuter zaražen, čak i ako nije. Ovi programi niti skeniraju niti čiste kompjutere, i ustvari su i pravljeni sa ciljem da ubede korisnike da su im kompjuteri izloženi opasnosti i preplaše ih dovoljno da kupe „antivirusni“ program. Ovakvi programi su često označeni kao 'scareware'. Kaspersky Lab ih je svrstala kao 'FraudTool' (prevarantsku alatku), podgrupu 'RiskWare' grupe.

[2] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.

1. Metodologija istraživačkog projekta

1.1. Uvodne napomene i obrazloženje rada

Projektni zadatak ima za cilj da definiše pojmove koji se koriste kada se govori o etici računarskom kriminalu i zaštiti. U ovom radu se pre svega sagleda odnos između etike računarskog kriminala i zaštite.

Rad se pored organizacionih bavi i tehnološkim aspektima informacionih sistema. Prikazana su tehnološka rešenja koja su trenutno aktuelna ali i ona koja će u bliskoj budućnosti biti preovlađujuća. Takođe, treba reći da je težište rada uglavnom okrenuto na bezbednost, a manje na potencijalne pretnje.

Projektni zadatak je izrađen korišćenjem teoretskih i praktičnih znanja iz domena savremene informacione tehnologije, a posebno je dat naglasak na računarski kriminal i zaštitu.

1.2. Predmet istraživanja

Predmet istraživanja bila je bezbendost informacionih sistema odnosno računarski krimina. Pored poglavlja koje se odnosi na informacione tehnologije , veći deo istraživanja posvećen je računarskom kriminalu i etici. Za obe vrste istrazivanja prikazani su prednosti i nedostaci kao i mogućnosti njihovog kombinovanja kako bi se od svake izvukle najbolje performanse, a smanjio uticaj slabosti koju svaka od njih poseduje. Može se sa sigurnošću reći da izbor protokola i tehnologija za razvoj informacionih sistema zavisi pre svega od organizacionih potreba kompanije, a takođe i od finansijskih sredstava sa kojima kompanija raspolaže. Evo nekih pitanja na koje su se tržili odgovori prilikom istraživanja:

- Šta je etika i čime se ona bavi

- Šta je računarski kriminal
- Istorija računarskog kriminala
- Tipovi i nastanak sayber kriminala
- Šta je softverska piraterija i zastupljenos softverske piraterije u svetu
- Šta su virusi istorija i nastanak virusa
- Antivirusne zaštite

1.3. Ciljevi i zadaci istraživanja

Ovaj rad je namenjen pre svega profesionalcima u oblasti savremenih informacionih tehnologija, kao i IT menadžerima koji treba da urade studiju izvodljivosti uvođenja zaštite informacionih sistema u neku kompaniju.

Cilj istraživanja bio da se kompanije koje prodaju računarsku opremu za zaštitu i koji su ujedno i sistem integratori nekih sigurnosnih rešenja potaknu na razmišljanje da postanu security provajderi odnosno kompanije koje nude security kao servis za veliki broj malih korisnika. Gotovo je nemoguće zamisliti da svaka od njih može da kreira sopstveni sistem za bezbednost pre svega zbog ograničenih finansijskih sredstava pa je ovakva inicijativa više nego korisna. Na ovaj način bi i kompanije koje deo svog poslovanja obavljaju preko Interneta, a koje nemaju velike budžete mogle sebi da priušte zaštitu pod povoljnim uslovima. Najvažnije je istaći da je ovakva inicijativa realno izvodljiva i da ne zahteva prevelika finansijska ulaganja.

1.4. Istraživačke hipoteze

Opšte hipoteze. Težište istraživanja je bilo na tome da se pokaže da na tržištu usluga u domenu informatike bezbednosti ne postoje kompanije koje sagledavaju zaštitu kao sveobuhvatan problem već to čine parcijalno favorizujući one segmente kojima se oni bave kao što su na prmer kriptografija, komercijalna hadverska rešenja ili softver koji se koristi za

zaštitu. Kompanije koje nude ovakva rešenja imaju zaposlene inžinjere koji su bez daljnjeg veoma stručni u svom poslu i veoma dobro poznaju Microsoft tehnologiju vezanu za zaštitu.

Da ne bude zabune, pronalaženje nedostataka u nekom informacionom sistemu je bitan segment zaštite ali ove kompanije se uglavnom zadržavaju na tome. Ukoliko neka od njih čak i ponudi neko resenje ono je neprecizno i nedefinisano i nikada se unapred ne zna koliko će da košta.

1.5. Metodi istraživanja i tok istraživaćkog procesa

Metodologija istraživanja svela se na korišćenje pre svega Interneta ali i na korišćenje ozbiljnih kljiga koje se bave oblastima organizacije zaštite i virtualnih privatnih mreža. Takođe informacije su dobijene i od eminentnih kompanija u ovoj oblasti, a koje u našoj zemlji imaju svoja predstavništva kao što su Cisco, SonicWall, Citrix ili Stonesoft, kao i pojedinaca koji su priznati eksperti u ovoj oblasti.

Na Internetu, a i u literaturi uopšte mnogo je manje informacija koje se tiču upravljanja zaštitom nego informacija o tehnologijama koje se za to koriste. Zbog toga je istraživanje bilo teže i kompleksnije ali i mnogo interesantnije. Svaka od informacija koja se nalazi u ovom radu proverena je obavezno na više mesta u literaturi da bi se dokazalo da je relevantna. Takođe informacije o ovoj oblasti teško su dostupne i trebalo je puno truda da se pronađu ljudi koji o organizaciji zaštite imaju znanje i iskustvo. U radu se nalaze stavovi i razmišljanja koja na potpuno nov način govore o nekim već poznatim pojmovima, tehnologijama ili daju kritički osvrt na njih. Ovakvi stavovi pozivaju na otvorenu polemiku koja bi pomogla još bolju implementaciju ovog rada u praksi. Ideja je da ovaj rad pomogne IT menadžerima, kao i drugim stručnjacima iz domena informacionih tehnologija da dobiju jasniju sliku o ovoj oblasti kao i da im se ukaže gde mogu da pronađu dodatne informacije koje su im potrebne. Neka praktična rešenja prikazana u ovom radu svako će im biti od koristi prilikom uvođenja zaštite informacionih sistema u njihovim organizacijama.

2. Etika, informacijska etika i moralne norme novih tehnologija

2.1. Etika

Reč etika potiče od grčke reči ethos - običaj i ethikos – moralan. Etika je nauka o moralu, nauka o proučavanju i procenjivanju moralnih vrednosti. To je filozofska disciplina, koja proučava moral, njegovo poreklo, ciljeve i smisao. Etike su nacionalni stereotipi koje jedno društvo i nacija propagiraju o sebi samom i veoma se razlikuju. Tako da ono što je etično za jednu naciju ne mora da bude i za drugu.

Etičke dilema je situacija do koje dolazi kada se čini da su dve ili više moralnih vrednosti jednako validne, a kontradiktorne, a od pojedinaca se zahtjeva da napravi najbolji mogući izbor.

2.1.1 Teorija dobrog ili vrednog

Za dobro, etika može uzeti bilo koju vrednost (ili više vrednosti) za koje se zalaže (npr. ljubav, mir u svetu, slobodna neutralna enciklopedija dostupna svima) a razloge za izbor određenih vrednosti skoro uvek argumentuje na određen način. Prihvatanje neke ili nekih određenih vrednosti za “dobre“ još ne obezbeđuje jednoznačno suđenje pri izboru ispravnih postupaka. Jedna etička teorija može dobro proglasiti npr. ličnu slobodu, a da i dalje nije u svim situacijama jasno kako treba pristupiti zato je potreban drugi deo etičkih teorija - koji određuje ispravno.

2.1.2 Teorija ispravnog

Zamislimo sad situaciju u kojoj bi se neka politička grupacija zalagala za smanjenje stepena slobode. Postavlja se pitanje, da li, u skladu sa poštovanjem lične slobode treba toj grupaciju dopustiti da nesmetano dela što može dovesti do njenog izbora na vlast što bi dovelo zapravo do suzbijanja ličnih sloboda, ili u skladu sa unapređivanjem lične slobode treba zabraniti rad takve grupacije zbog nepoželjnih posledica koje u protivnom mogu iskrsnuti, iako zabranom rada te grupacije kršimo pravo njenih članova na slobodno izražavanje, kao oblik lične slobode. Ovde stupa na scenu određenje ispravnog koje se odgovara na pitanje kako pojedinac ili grupa treba da postupe kada reaguju na dobro tj. vredno.[3]

2.2. Informacijska etika

U savremenom globalizovanom svetu nove tehnologije se razvijaju velikom brzinom, pa se kao najvažnije tehnologieje današnjice izdvajaju telekomunikacije, elektronika, kompjuteri, novi materijali, opelektrika, birotehnologija, energetsko inženjerstvo, informatizacija, sofistikacija i medikalizacija.

Telekomunikacije, omogućavaju sve veću povezanost među ljudima i to kao da oni fizički nisu blizu.

Elektronika, kao grana tehnike doživela je značajan uspon u vreme druge industrijske revolucije, što je nešto kasnije uslovilo pojavu i razvoj mikroelektronike. Nastanku mikroelektronike predhodilo je konstruisanje tranzistora.

Od pojave kompjutera, 1946. godine, pa sve do današnjih dana, razvijeno je nekoliko kvalitativno razlličitih generacija kompjutera. Sada je u poodmaklom razvoja već šesta generacija kompjutera zasnovana na bazi mikročipa.ta generacija mikročipa treba da ostvari

[3] www.wikipedija.org

prelazak sa obrade informacija na obradu znanja. To će biti moguće ostvaariti na nivou submikronskog procesora sačinjenog od bioloških materijala, odnosno biomolekla.

Sličan značaj ima i optoelektronika, kao tipična hibridna tehnologija. Zasniva se na novim optičkim materijalima koji omogućavaju integraciju raznih tehnologija, i to od starih elektromehaničkih tehnologija, preko robotičkih tehnologija, do komunikacionih i drugih tehnologija, stvarajući takozvanu optomatroniku u okviru koje se na optimalan način ostvaruje transformacija optičkih signala u elektronske i obratno. Taj spoj optike i elektronike posredstvom mehatronike u takozvanu optomatroniku, predstavljaće ključ sveukupnog budućeg tehnološkog razvoja. Posebno u razvoju laserske tehnologije.

Energija je osnov mogućih promena. Poseban značaj u tom smislu ima nuklearna energija.

Jedna os najznačajnijih tehnoligija današnjice nesumnjivo je robotika. Industrijski roboti, poljski roboti i inteligentni roboti. Industrijski roboti su fiksirane mašine koje su pripremljene da automatski izvršavaju različite poslove. Poljski roboti pripremljeni da rade u otvorenoj sredini, poseduju ssenzore koji im omogućavaju da se nesmetano kreću, da reaguju na prepreku i tome slično. Inteligentni roboti, kao treća generacija eksperimentalnih kopjuterizovanih mašina, dizajnirani su tako da koriste veštačku inteligenciju da bi rešavali određene probleme na način sličan ljudskom.

Digitalna ekonomija je zasnovana na digitalnim tehnologijama, što znači da sadrži digitalne komunikacione mreže, kao što su Internet, intranetovi i privatne mreže sa dodatom vrednošću, da sadrži rčunare, softver i druge među sobom povezane informacione tehnologije.

U užem smislu, pod informacionom tehnologijom se podrazumeva tehnološka strana informacionog sistema koja obuhvata hardver, baze podataka, softver, mreže i druge uređaje. U širem smislu pod informacionom tehnologijom sse podrazumeva skup više informacionih sistema, korisnika i menadžmenta celokupne organizacije.

U stvari, upotreba informacione tehnoligije pokreće značajna pitanja, tako da su etički problemi veoma važna prateća pojava digitljalne ekonomije, i to bez obzira da li se radi o nadgledanju.

Etika u menadžmentu informacione tehnologije, prema razmatranjima Roberta Davisona, razvila je etičke principe koji počivaju na ličnom moralnom izboru. U tom smislu

pominju se sledeći principi: „zlatno pravilo“, kategorički imperativ, „pravilo kllizave padine“, utilitarno pravilo i takozvano pravilo „nema besplatnog ručka“.[4]

„Zlatno pravilo svoje uporište nalazi u Bibliji i konfučijanskoj filozofiji. Ovo pravilo upućuje na pristup koji podrazumeva isti način ponašanja prema sebii prema drugima, pa u tom smislu je odlučivanje zasnovano na kategorijama dobra. Kategorički imperativ je preuzet od kanta, pa etičko pravilopodrazumeva ono ponašanje koje svima odgovara. „Pravilo klizave padine“ odnosi se na to da je nužno zaustaviti one ponovljene aktivnosti kje dovode do negativnoh posledica, da ne bi bilo prekasno. Utilitarni pravilo ukazuje da treba činiti one aktivnosti koje će najvećem broju ljudi doneti najviše dobra ili ukazuje na to da treba činiti one radnje koje će doneti najmanje štete ili će biti najjeftinije. Tkozvno pravilo „nema besplatnog ručka“ , ili „sve ima svoju cenu“ ustanovljava princip nadoknade korišćenja vlasniku.

Poseban značaj u ovomkompleksu složenih problema koje informaciona tehnologija sa sobom donosi je pravo intelektualne svojine. Informacijska etika koja se može odrediti kao skup etičkih principa odgovornog korišćenja informacionih sistema, treba da reguliše brojna pitanja i otkloni brojne probleme vezane za moralnu stranu u primeni novih tehnologija, a posebno onih koji se odnose na informacionu tehnologiju.

2.3. Etika i moralne norme novih tehnologija

Nema sumnje da nove tehnologije uvode nove pristupe neetickom ponašanju, ali to je vec poznata stvar. Naravno, jedna od najvecih briga jeste lakoca kojom se licne informacije mogu prikupljati i deliti preko interneta. Osnovna vrednost još uvek je privatnost. Upotreba weba u pirateriji muzike ili filmova, umesto klasicnih metoda presnimavanja, ne menja cinjenicu da neeticko postupanje obuhvata kradu intelektualne svojine. Kao što upotreba digitalne tehnologije za menjanje fotografije i dalje obuhvata pitanje iskrenosti i istine.

Prikljucivanjem racunara na Internet, odnosno na racunarsku mrežu realizovanu Internet tehnologijama, postoji realna opasnost da neko ko se takode nalazi u mreži kao uljez pristupi resursima našeg racunara, na primer podacima na disku koji predstavljaju poslovnu prepisku. Da li je, onda, naša kompanija sigurna ? Jedna od posledica narušavanja necije

[4] "Ethics for a new millennium" Dalai Lama XIV - Tenzin Gyatso

privatnosti može da bude i tzv. krada identiteta. Snabdeveni individualnim personalnim informacijama, kradljivci identiteta mogu da otvore racune u bankama, obavljaju kupovinu, a u zemljama u kojima su automatizovane servisne usluge za gradane, mogu da dobiju sertifikate o rodenju, pasoš, kredit i sl., a sve to u ime osobe o cijim podacima se radi. Lažnim identitetom kriminalac može da dobije pozajmicu u banci, kupi auto, stan, ode na putovanje i sl., i na taj nacin žrtvu može da optereti finansijski, a u nekim slucajevima da joj napravi i kriminalni dosije.

Dvosmerni mediji, elektronska pošta, pristup racunarskim bazama podataka i kupovina od kuce - sve su to mehanizmi koji omogucavaju prikupljanje informacija o pojedincima. Pošto se smatra da je informacija - roba koja ima ekonomsku vrednost, ona se cesto obraduje i prodaje marketinškim firmama. Tema dostupnosti privatnih podataka postala je mnogo šira od pitanja njihove puke komercijalne upotrebe nakon što je posle 11. septembra americki Kongres usvojio takozvani Patriotski Akt. Ovaj zakon državnim organima daje široka ovlaštenja da prisluškuju, prate i snimaju bilo koga osumnjicenog za ilegalne, ne samo teroristicke, aktivnosti u SAD-u. Tehnologije nadzora i prikupljanja informacija nisu vezana samo za navodne teroristicke aktivnosti, nego u rukama velikih kapitalistickih kompanija i država nalaze svoju primjenu i u sankcioniranju onih koji cine alternativu autorskim pravima (copyright) zašticenim podacima. Zakon koji sankcioniše slobodno deljenje podataka, a samim tim i anonimnost na Internetu, poznat je kao Digitalni milenijumski akt za autorska prava, a potpisala ga je demokratska administracija Billa Clintona 1998. godine. Ovaj zakon služi, recimo, Americkoj asocijaciji za zaštitu muzicara (www.riaa.com) da bez dokaza optužuje korisnike Interneta za nepropisnu razmjenu podataka. Što znaci da ovaj akt dopušta agencijama kao RIAA da prisile lokalne Internet provajdere (Internet Service Providers, ISP) da daju sve podatke o svojim korisnicima, ako RIAA to od njih zatraži, a bez predocavanja dokaza o aktivnosti subjekta ciji se podaci traže. Poslednji slucaj je zahtev RIAA-e bostonskom Univerzitetu da otkrije identitet studenta koji je bez dokaza optužen za razmenu muzickih fajlova, a u ciju je odbranu stala Americka unija za civilne slobode. Projekat "Internet pod nadzorom", koji prati stanje slobode na Internetu u više od 60 zemalja, otkrio je da su prava korisnika interneta i online novinara znatno ogranicena nakon 9. Septembra. "Demokratske zemlje postepeno oduzimaju slobode od svojih gradana" u ime vece nacionalne sigurnosti, uvodenjem zakona koji daju vladama proširena ovlašcenja da špijuniraju korisnike interneta i privode osumnjicene za terorizam. Sjedinjene Države i Francuska vode u donošenju antiteroristickih zakona. Medutim, autoritarni režimi sa svoje strane provode

sopstvene mere, pri cemu im nacionalna sigurnost služi kao izgovor za nove represalije protiv politickih disidenata i nezavisnih novinara i pisaca. Jednom diktatoru je upravo to i potrebno – dok se hvali borbom protiv terorizma, oci medunarodne zajednice nece videti da on u stvari hapsi cyber-disidente i cenzoriše web strane. U meduvremenu, sve je veci broj vlada koje koriste sofisticiranu tehnologiju da bi uskratile svojim gradanima pristup informacijama na internetu. Kina je instalirala specijalne filtere za internet koji ne dozvoljavaju korisnicima pretraživaca Google da dodu do informacija o kontraverznim temama, kao što su ljudska prava. U Uzbekistanu vlasti koriste "modifikovana ogledala" – lažnu verziju kontroverznih web-strana koje izgledaju kao da su original, ali u stvari sadrže izmenjene informacije. Medu svim zemljama koje su u izveštaju pracene, Kina je i dalje na prvom mjestu po hapšenjima korisnika interneta. Trenutno ih je šezdeset troje u zatvoru. Vijetnam je na drugom mjestu sa sedmoro zatvorenih cyber-disidenata, a za njim slede Maldivi sa troje.

Pojedinacni pristup Internetu stvorio je i zabrinutost, pravnu i eticku, u vezi s upotrebom sajberspejsa za neregulisano širenje pornografije i nekontrolisano širenje krade intelektualne svojine. Opasnost od neregulisanog web-a možda se najbolje ilustruje velikim izdavackim kucama, koje obicno pozelene od besa kad im neko spomene skracenicu MP3. Pošto se oko prodaje kompakt diskova vrte milioni dolara, muzicka industrija se podigla tražeci godinama nekoga koga bi tužili zbog zloupotrebe. Pronašli su žrtvu u autorima programa za razmenu datoteka Napster. Prvi put primenivši na Internetu revolucionaran distribuirani sistem deljenja datoteka, Napster je za manje od godinu dana stekao preko 20.000.000 vernih korisnika. Poznata americka grupa Metallica prva je podnela tužbu protiv autora ovog programa zbog kršenja autorskih prava, a zatim je usledila i tužba americkog Udruženja autora u muzickoj industriji (RIAA), prošlog decembra. Sudija Merilin Patel nedavno je, do daljeg, zabranila upotrebu programa Napster, uz objašnjenje da sudskim procesom samo stice još vecu popularnost i da bi do kraja sudenja dodatno oštetio muzicku industriju.

Neke od najproblematicnijih etickih dilema rezultat su integracije racunara i digitalne tehnologije. Digitalizacija je proces elektronskog konvertovanja slika, zvuka i teksta i njihovog cuvanja u obliku cifara koje se kasnije mogu dekodirati i vratiti u prvobitni proizvod ili neki njegov izmenjeni oblik. Pošto je "rekonstruisani" proizvod savršena kopija originala, bilo koju transformaciju originalnog sadržaja nemoguce je otkriti. Jedan program je raspršio snove o najsigurnijem digitalnom formatu današnjice. Grupa skandinavskih hakera je pre više od godinu dana "probila" zaštitu digitalnog video diska (DVD) i objavila na Internetu

besplatan program DeCSS koji je reprodukovao takve diskove pod Linuxom. Mnoge Internet lokacije ukljucile su ovaj program u svoje sadržaje - i ubrzo se našle na sudu. Mada su u njihovu odbranu stale brojne organizacije poput EFF (Electronic Frontier Foundation), sudenje je nedavno završeno, i to znatno nepovoljnije po slobodu govora na Internetu nego što je iko ocekivao. Ne samo da je zabranjena upotreba programa DeCSS, vec su i lokacije koje su ga prenosile kažnjene. Mnogi pravnici vide u ovoj odluci iste probleme kao i sa zloglasnim zakonom o pristojnosti u komunikacijama (Comunicatons Decency Act). Taj zakon je 1996. proglašen neustavnim u SAD, a zagovornici slobode govora na Internetu nadaju se da ce na slican nacin preobratiti sudsko rešenje i u ovom slucaju. Advokati filmske industrije najavili su cak i tužbe protiv Web lokacija koje su hipervezama usmeravale posetioce ka piratskim sadržajima. Evropski telekomunikacioni gigant British Telecom, otišao je korak dalje - zatražio je placanje autorskih prava na sve hiperveze.

2.4. Etičke dileme i nedoumice

Etičke dileme i nedoumice sa kojima se menadžeri u svojoj karijeri suasreću čine srž svakog menadžerskog posla. Područja u kojima najčešće dolazi do odstupanja od etičkih normi su: korupcija, industrijske krađe, špijunaža, konflikti interesa, zloupotreba medija, tajni dogovori, prevare. Korupcija uje veliki problem savremenoog sveta i jedan od najvećih izazova današnjice. U političkoj i pravnoj teoriji pod korupcijom se podrazumeva zloupotreba poverenog javnog ovlašćenja radi sticanja lične koristi ali i sukobi interesa i nepotizam kao prateće pojave.

Delatnosti koje su najpodložnije korupciji: javne nabavkke, prikupljanje javnih prihoda, imenovanja u sferi vlasti, donacije za političke kampanje kao i one pojave vezane za nepotizam, podmićivanje i prevare svih vrsta. Korupciju prati i mito koje se daje radi sticanja nečega što donosi korist.

Po preporukama Saveta OECD-a ukazuje se na moguća načela koja bi mogla postati polazna osnova za obezbeđivanje neophodnih sredstava za upravljanje etikom.Etički standardi za javne službenike treba da budu jasni, treba da čine polaznu osnovu za zakone i druge propise, zaposleni u javnim službama moraju bi8ti posvećeni vladavini prava. Proces

donošenja odluka treba da bude javan i treba da bude predmet nadzora javnosti, odnos između javnog i privatnog sektora treba da bude precizno definisan...

Korupciji se može suprostaviti na razne načine. Jedan od načina je i podizanje nivoa etičke svesti, definisanje novih moralnih standarda ponašanja i praktična provera čestitosti javnih službi. Najrazvijenijih zapadnih zemaljlja. Po njemu to jedan od najznačajnijih megatrendova sadašnjosti.

U visokorazvijenim zemljama sveta ima preko 90% finansijskog kapitala i 98% svih otkrića. U nerazvijenim u kojima živi 80%svetskog stanovništva ostvaruje se 12%industrijske proizvodnje između 17-18% izvoza, 16-20% društvenog proizvoda, dok za isplatu dugova odlazi 30% njihovog društvenog priozvoda a u većini zemalja i ukupan nacionalni dohodak. Najnerazvijenijim zemljama bi trebalo 350 godina da dostignu stepen razvoja kao u razvijenim zemljama.

„nova ekonomija“ karakteriše je intelektualni kapital, savremena informaciona i komunikaciona tehnologija.

Intelektualni kapital obuhvata ukupnost svih vrsta znanja i sposobnosti kao što su veštine, iskustvo, samopouzdanje, odgovornost, motivisanost...

2.5. Uticaj poslovne etike na poslovnu komunikaciju

Komunikacija se ostvaruje na osnovu informacija koje jedan od učesnika u komunikacionom procesu upućuje drugom ili ostalim učesnicima. Informisanje može biti: namerno i ne namerno.

Znakovi se dele na: prirodne i veštačke (arbitrarne). Prirodni znak se javlja kao spontani izraz određenih emocionalnih stanja a tumači se od onoga ko zapaža. Veštački znakovi su skupine glasova ili linija i oblika radi označavanja određenih pojava koje čovek konstruiše.

Signali su znakovi koji izazivaju nečiju pažnju. Simboli oni označavaju stvari i pojave.

PODELA Ljudska komunikacija se može podeliti na: simboličku (koja počiva na znakovima kojima se prenose razne vrste namerno upućenih poruka), signalnu (koja pretstavlja izvor informacija o stanju i osobinama za pojedinca koji te signale uočava.

- Komunikacija može biti: verbalna-uvek simbolička i neverbalna - obično signalna
- Komunikacija može biti: glasovna i neglasovna
- Komunikacija može biti: posredna i neposredna
- Komunikacija može biti: jednosmerna i uzajamna
- Komunikacija može biti: interpersonalna i intrapersonalna
- Pregovaranje je veoma važan proces komunikacije.
- Kulturni identitet svakog naroda čine kultura i tradicija.

Multikulturalizam uvažavanje postojanja različitih kultura. Faktorikoji ga definišu: entitet, rasa, pol, fizička sposobnost, seksualna orijentisanost, starost. Jedna od najvažnijih i osnovnih karakteristika japanske kulture je egalitarizam a amerike autoritarnost.

2.6. Etičke norme

Hosmer pravi razliku između etičkih pravila i kodeksa. Etičkim kodeksima se uspostavlja viši moralni nivo u organizaciji definišu se vrednosti i na njima zasnovana ponašanja. Oni nisu večni i podložni su promenama.

Etička pravila obuhvataju zahteve da se ponaša na određeni način, ona se ne odnose samo na očekivanja, predloge ili molbe ona imaju i određene prinude.

U SAD-u postoje dva argumenta koja govore da etici nema mesta u internacionalnom bizniisu: prvi je da se moralna shvatanjlja u raznim zemljama međusobom razlikuju pa se iz tih razloga nemože govoriti o univerzalnom moralu. Drugi se tiče prakse u kojoj korporacije nekih zemalja ne slede nikakva moralna pravila.

Ričard Di Džordž se suprostavio ovakvim stavovima tvrdeći da se mogu ustanoviti univerzalna moralna pravila koja će važiti za sve zemlje sveta. On navodi pet osnovnih moralnih normi i tri dodatna principa.

- moralni minimum-da se ne nanosi namerno neposredno zlo, taj minimum moraju svi da ispoštuju.
- multinacionalne kompanije u manje razvijenim zemljama moraju imati u vidu nesumnjive razlike između zemlje koja izvozi i zemlje koja uvozi.
- poštovanje ljudskih prava radnika u zemlji domaćinu
- unapređenje i razvoj pravednih pozadinskih institucija unutar zemlje kao i na internacionalnom nivou
- zahteva od multinacionalne korporacije da poštuje zakone zemlje domaćina njenu kulturu i lokalne vrednosti.

Ovim opštim normama mogu se dodati i specifične norme ili pravila ponašanja koja važe za posebne privredne grane.

2.7. Neetičko ponašanje u elektronskom poslovanju

Nema sumnje da nove tehnologije uvode nove pristupe neetičkom ponašanju, ali to je već poznata stvar. Naravno, jedna od najvećih briga jeste lakoća kojom se lične informacije mogu prikupljati i deliti preko Interneta. Osnovna vrednost još uvek je privatnost. Upotreba web-a u pirateriji muzike ili filmova, umesto klasičnih metoda presnimavanja, ne menja činjenicu da neetičko postupanje obuhvata krađu intelektualne svojine. Kao što upotreba digitalne tehnologije za menjanje fotografije i dalje obuhvata pitanje iskrenosti i istine.

Priključivanjem računara na Internet, odnosno na računarsku mrežu realizovanu Internet tehnologijama, postoji realna opasnost da neko ko se takođe nalazi u mreži kao uljez pristupi i resursima našeg računara, na primer, podacima na disku koji predstavljaju poslovnu prepisku. Da li je onda naša kompanija sigurna?

Pojavni oblici kompjuterskog kriminala su: protivpravno korišćenje usluga i neovlašćeno pribavljanje informacija, kompjuterske krađe, kompjuterske prevare, kompjuterske sabotaže i kompjuterski terorizam i kriminal vezan za kompjuterske mreže.[5]

[5] "Ethics for a new millennium" Dalai Lama XIV - Tenzin Gyatso

2.8. Porjeklo i pojam morala

Moral je nastao u ljudskom društvu, još u prvobitnoj zajednici. Tokom svoje evolucije čovek je najpre živeo u malim grupama gde je bilo potrebno uskladiti svoje potrebe sa šptrebama drugih. Na osnovu iznalaženja rešenja za to, formirana su pravila ljudskog ponašanja i nastala je filozofska disciplina – etika.

Moral je objektivna društvena pojava koja je određena skupom pravila ili normi koja regulišu ponašanje članova jedne društvene zajednice, ali i navikama ponašanja. Procenjivanje morala ili moralni sud se donosi na osnovu postupaka, rasuđivanja, ponašanja ili uopšte karaktera nekog čoveka. U skladu sa tim i sa složenom komunikacijom koja se odvija u društvu, ljudi formiraju svoje ličnosti, usmeravaju svoju motivaciju i delovanje, vrednuju i sude i sebi i drugima.

Osnovna karakterističnost moralnih normi je njihova obaveznost, koja je dvostruka, što znači da je moral obavezujući i društveno i individualno, za razliku od pravne i običajne obaveznosti koja je isključivo društvena. Takođe, kao bitna karakteristika morala, navodi se i trenutačnost, bezuslovnost, nametnutost i sl. Prema tumačenju hristovih učenja, „moralnost je dobrota prema slabijima“. Niče je definisao moralnost kao „smelost jačih“, a Platon kao „stvaralačku harmoniju celine“.

3. Računarski kriminal

3.1. Pojam i definicija računarskog kriminala

Računarski kriminal je opšti pojam koji obuhvata krivična dela koja se vrše posredstvom računarskog sistema ili mreže, u računarskom sistemu ili mreži, ili protiv računarskog sistema ili mreže. U principu on uključuje bilo koje krivično delo koje se vrši u digitalnom ambijentu.“

Pored definicije formulisane od strane UN i druge međunarodne organizacije i pojedinci bavili su se definisanjem pojma računarskog kriminala. Iz toga se najbolje može zaključiti koliki se značaj pridaje izučavanju ove vrste kriminala širom sveta.

Definicija usvojena od strane OECD glasi: „Kriminal povezan sa računarom je svako ilegalno, neetičko ili neovlašćeno ponašanje koje uključuje automatsku obradu podataka ili prenos podataka“.

U teoriji krivičnog prava mogu se naći i mnogobrojne definicije računarskog kriminala formulisane od strane pojedinaca. U tu grupu definicija spadaju pojmovna određenja računarskog kriminala Dona Parkera, Avgusta Bekvaja, Bogo Brvara, Đorđa Ignjatovića i Slobodana R. Petrovića.

U svetu se koriste mnogi termini koji označavaju ovu pojavu – computer abuse, computer fraud, crime by computer, tehnokriminal ili računarski kriminal. Računarski kriminal je protivpravna povreda imovine kod koje se računarski podaci s predumišljajem mijenjaj u (manipulacija računara), razaraju (računarska sabotaža), do njih se neovlašteno dolazi iz koristi (računarska špijunaža) ili se koriste zajedno sa hardverom (krađa vremena). [6]

1. [6] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.

Kao sveobuhvatnu funkcionalnu definiciju, mogli bismo da prihvatimo onu koja računarski kriminal definiše kao radnju koja se preduzima uz upotrebu računara i drugih sredstava informacionih tehnologija, a koja je usmjerena na:

- neovlašćeni pristup zaštićenom računaru
- neovlašćeno presretanje elektronskih podataka koji su upućeni sa računara ili ka drugom računaru
- uništavanje, izmenu i brisanje elektronskih podataka
- ometanje ili onemogućavanje funkcionisanja računarskog sistema putem oštećenja, brisanja, mjenjanja ili umetanja elektronskih podataka
- distribuciju nedozvoljenih sadržaja
- stvaranje i širenje virusa i malicioznog softvera.
- U odnosu na činjenicu da li se računar, sistem ili mreža koriste kao sredstvo za izvršenje dela ili su objekat na kome se delo izvršava, ponekad se koriste različiti izrazi da bi se definisala kriminalna delatnost koja se vrši upotrebom računara:
- klasičan računarski kriminal kod koga je računar ili računarski sistem sredstvo izvršenja ili objekat napada;
- Internet kriminal kod koga je zloupotreba mreže određujući faktor (posjedovanje i distribucija dječije pornografije, raspirivanje nacionalne i rasne mržnje, neovlašćena distribucija autorskih djela i predmeta intelektualne svojine);
- e-kriminal koji se vezuje za zloupotrebu komunikacionih uređaj i uređaja za skladištenje elektronskih podataka

Iz Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala: visokotehnološki kriminal predstavlja „vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom i elektronskom obliku.“ [7]

Razvoj informacionih tehnologija ima uticaj na mnoge profesije. Ministarstvo unutrašnjih poslova koristi specijalizovane baze podataka u kojima se skladište podaci o građanima, motornim vozilima, prekršsjima, zločinima, kriminalcima i sl.i na zahtev se putem

[7] Computer Crime and Intellectual Property Section

različitih upaita nad bazom podataka dobija pravovremene informacije u mnogim kompleksinm slučajevima.

Kao i kod upotrebe oružja ljudi koriste računare kao podršku u svom mposlu, ali vrlo često i za kršenje zakona. Računari su moćni alati u rukama kriminalaca, a računarski kriminal je rapidno rastući problem. Danas je raćunar u mnogim situacijama kod kriminalaca zamjenio klasično oružje. Računarski kriminal se često definiše kao bilo koji zločin učinjem zahvaljujući znanju ili korištenjem računarske tehnologije.

Niko ne zna pravi obim računarskog kriminala. Mnogi računarski zločini prođu neopaženi. Oni koji se otkriju, često prođu neprijavljeni zato što se kompanije plaše da mogu izgubiti više zbog negativnog publiciteta nego od stvarnog zločina.

Većinu računarskih zločina počine insajderi kompanije (zaposleni unutar kompanije), a njih ne prijavljuju vlastima, čak i kada su uhvaćeni na delu. Ovakvu vrstu zločina običnjo počine referenti, blagarjnici, programeri, operatori na računarima i rukovodioci koji nemaju izraženu tehničku genijalnost. Organizovani kriminal je odavno prešao na računarsku tehnologiju. Eksplozivni razvoj interneta i servisa za trgovanje i plaćanje putem interneta postali su meta računarskog kriminala, kako internet veze, tako i računarski sistemi koji su povezani na internet.

Najnoviji izvještaji sačinjeni od kompanije ArcSight su alarmantno pokazali da kompanije godišnje gube oko 3.8 milijardi dolara, direktno od računarskog kriminala. Istraživanje je izvedeno nad 45 kompanija tokom perioda od četiri sedmice, a za isti period je zabilježeno više od 50 uspešnih računarskih napada na svaku od njih. Najčešće mete napada hakerskih grupa su krađe podataka o radnom osoblju, korisnicima, brojevi kreditnih kartica, brojevi socijalnog osiguranja i slične privatne informacije.

Prisutan je i određen broj krađa poslovnih tajni, kao što je slučaj sa jednom američkom kompanijom, koju su hakeri novčano ucijenili pod prijetnjom da će podatke prodati konkurenciji. Oko 90% navedenog iznosa se odnosi na trošak borbe sprečavanja upada hakera i implementacije sistema zaštite, a kada se uračunaju štete i gubitak povjerenja korisnika jasno je da se radi o još većim sumama novca.

Izveštaj dalje pokazuje da je većina napada izvršena tako što se kod instalira od strane vanjskog hakera na računare u kompaniji. U 19% napada štetni kod je aktiviran kada je osoblje pristupilo određenim web stranicama, a 9% od slučajnih instalacija nenamjernim klikanjem na linkove u e-mailovima, iskačućim prozorima i slično.

3.2. Istorija računarskog kriminala

Prvi evidentirani slučaj računarskog kriminaliteta pojavio se 1958. Godine, dok je prvi slućaj gonjenja na federalnom nivou SAD bio izmena bankarskih zapisa u Mineapolisu 1966. godine, a prvi slučaj zabeležen u Nordijskim zemljama, i verovatno Evropi, bila je jedna tipična softverska krađa, koja se desila u Finskoj, februara 1968. godine. Na prostoru bivše SFRJ prvi slučaj računarskog kriminala zabeležen je 1983. Godine, kada su radnici SUP-a Pula uhapsili radnike Istarske banke u Puli i radnika filijale Zagrebačke banke u Puli, zbog osnovane sumlje da su prva dvojica radeći kao operateri uz pomoć trećeg bivšeg rukovodioca, izveli finansisku malverzaciju uz pomoć računara pokušavši tako da izvođenjem niza programa na računaru, nezakonito izvrše bespravni upis kamata na koji način su nameravali sebi pribaviti protivpravnu imovinsku korist oštetivši banku za iznos od 10 130 353,50 tadašnjih SFRJ dinara. [8]

3.3. Karakteristike kompijuterskog (računarskog) kriminaliteta

Kompjuterski (računarski) kriminalitet se pre svega karakteriše velikom dinamikom i izuzetnim bogatstvom svojih pojamnih formi i vidova ispoljavanja. To je i razumljivo jer se radi o novoj tehnologiji sa velikom mogućnosti i primenom u skoro svim oblastim društvenog,privrednog pa i ličnog života te su i mogućnosti za zloupotrebu kompjutera svakim danom sve veće. Pored novih pojavnih oblika ranije već poznatog kriminaliteta koje pod uticajem kompjutera menja svoj tradicionalni način i modus ispoljavanja,sada se javljaju i novi, znatno opasnijij oblici kriminalnog ponašanja koji do sada nisu bili poznati u kriminalističkoj praksi , a koji ne poznaju granice izmedju država pa i izmedju kontinenata.

Štetne posledice kompjuterskog kriminaliteta su izuzetno velike. One se mogu ispoljti i u nastupanju imovinske štete za pravno ili fizičko lice (ponekad i za celu državu), u gubitku

[8] www.wikipedija.org

poslovnog ugleda, gubitku poverenja u sigurnost i istinitost kompjuterskog poslovanja i uopšte kompjuterskih informacija,opasnosti od zloupotrebe po slobode i prava čoveka uopšte na razne načine i u raznim oblicima. I sami učinioci krivičnih dela u vezi sa zloupotrebom kompjutera predstavljaju posebnu često specifičnu kategoriju ljudi. Ovde se najčešće radi o nedelikventnim, nenasilnim, socijalno prilagodljivim pojedincima.

To su po pravilu lica koja ipak moraju da poseduju posebna stručna i praktična znanja i veštine u domenu visoke informatičke, računarske i kompjuterske tehnologije i kojima su ovakva tehnološka sredstva dostupna. Ova se krivična dela vrše prikriveno, često bez neke vidljive i bliske prostorne povezanosti učinioca dela i žrtve (oštećenog). Najčešće se teško otkrivaju a još teže dokazuju, a dugo vremena ostaju praktično neotkriveni sve dok oštećeni ne pretrpi neku štetu koja je vidljiva u sistemu računarskih informacija. To je kriminalitet koji brzo menja forme i oblike ispoljavanja,granice medju državama kao i vrstu oštećenog.

Tako je Interpol još 1980. godine konstatovao sledeće : "Danas u savremenom svetu postoji još jedan veliki usavršeni front koji je prisutan u svetskim razmerama.Veliki kriminalitet, organizacije kriminalaca sve više se orijentišu na akcije pljački u kojima je objekt kompjuter. Elektronika se zloupotrebljava. Ne beleži se pad klasičnih pljački ali se iz godine u godinu povećava nova vrsta kriminaliteta u kome se elektronika koristi kao sredstvo da se kriminalci domognu milionskih svota novca.[9]

Savremena informaciona i kompjuterska tehnologija unela je nove i drastične promene u sve sfere društvenog života. Te promene su pored pozitivnih i korisnih novina donele i niz problema vezanih za pojavu i širenje kompjuterskog kriminaliteta različitih oblika, formi i vidova ispoljavanja. Sve te promene se mogu svesti na sledeće :

- nove forme vrednosti,
- koncentracija podataka,
- novi ambijent delovanja,
- nove metode i tehnike delovanja,
- sužavanje vremenske skale delovanja,
- širenje geografskog prostora delovanja,
- pokretljivost,
- stabilnost rizika

[9] Aleksić Ž. Milosavljević Z. *Leksikon kriminalistike,* Beograd, 1993.

3.4. Krađa preko računara

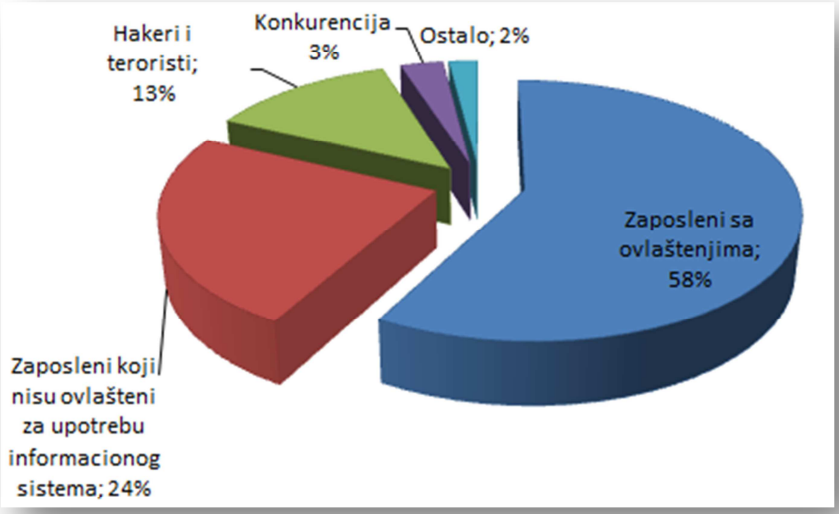
Krađa je najčešći oblik računarskog zločina. Računari se koriste za krađu novca, robe, informacija i računarskih resursa. Neke vrste računarskih zločina su toliko česte da su ovi zločini dobili svoja imena. Česta studentska prevara koristi proces koji se naziva spoofing (obmana) za krađu lozinki. Tipičan obmanjivač pokreće program koji na nekom računaru u labaratoriji imitira ekran za logovanje. Kada student – žrtva otkuca ID i lozinku, program reaguje npr. Porukom o grešci a lozinka se pamti. Računari mogu biti sredstvo, objekat i posrednik za izvršenje krivičnog dela.

Ponekad lopovi koriste računare i drugi alat da ukradu kompletan identitet. Sakupljanjem ličnih podataka: brojeva kreditnih kartica, brojeva vozačkih dozvola, brojeva socijalnog osiguranja i drugih podataka- lopov moze efikasno da se izdaje kao neko drugi, čak i da počini zločin u ime te osobe. Jedan od dobro poznatih problema danas je npr. uništavanje nepotrebnih CD-ova na kojima može biti zaostalih važnih informacija. Vrlo često oni se ne uništavaju, već se jednostavno bacaju.[10]

3.5. Računarske prevare

Računarske prevare se vrše u namjeri pribavljanja za sebe ili drugog protivpravne imovinske koristi, s tim što se kod njih u zabludu ne dovodi neko lice kao kod obične prevare. Ta zabluda se odnosi na kompjuter u koji se unose netačni podaci, ili se propušta unošenje tačnih podataka, ili se na bilo koji drugi način računar koristi za vršenje prevare. Računarske prevare predstavljaju najrasprostranjeniji oblik računarskog kriminaliteta. Osnovna karakteristika prevara je njihova teritorijalna rasprostranjenost. Kompjuterski prevaranti koriste prednost činjenice da prevara preko interneta ne zahteva pristup do nekog sistema za splatu, kao što to zahtjeva svaka druga vrsta prevara.

1. [10] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.



Slika 1: prikazuje zastupljenost računarskih prevara

Svako 44 sekunde neko postane žrtva računarskog kriminaliteta pošto se odluči da kupi robusa čijim se mogućnostima upozna preko interneta. Otkriveno je preko 1400 sumnjivih sajtovasamo u oblasti zdravlja što je rezultiralo podizanjem tužbi protiv nekih kompanija. Najčešći proizvodi su pilule koje omogućavaju svojim korisnicima da piju piva koliko žele, a da se neugoje, tečnost koja masnoću iz tkiva tokom spavanja pretvara u mišiće, magneti protiv nesanice i sl. U periodu od juna do avgusta 1994. u osamnest upada, Vladimir Levin iz Petrograda, izvukao je preko 10 miliona dolara iz sistema Citybank. Naredne godine je uhapšen u Londonu, 1997 je izručen američkim vlastima, a u avgustu 1997.g. je osuđen na 36 mjeseci zatvora i kaznu od 250.000 dolara. Kevin Mitnik u SAD je uhapšen i osuđen 1995. g. za falsifikovanje 20.000 brojeva kreditnih kartica. Čak su i pet gospođa starijih od 50 godina, službenici Zavoda za penzije u Francuskoj, prebacile na svoje račune 6 miliona franaka kao penzije za osobe koje su već odavno umrle.

3.6. Računarska etika

Računarska etika (engleski computer ethich) je skup pravila za pravilno ponašanje svetu računara. Korištenje računara danas je u porastu zbog toga je neophodno uvesti pravila i načine ponašanja u svetu računara. Računarska etika brine o provođenju tih pravila. Ona uči ljude kako da pravilno upotrebljavaju računar. Sa povećanom upotrebom računara raste i broj pravila koje nameće računraska etika. To nam pomaže da povećamo privatnost u upotrebi računara da ih zaštitimo od virusa i pogrešne upotrebe softvera.

Postojanje računarske etike povezano je sa pojavom i razvojem kompijutera. Mnogi ljudi misle da pojava računara može biti štetna za društvo, ne gledajući pozitivne strane postojanja računara. Tie je rekao da će mnoge poslove koji ljudi rade preuzeti da rade računari. Računarska etika nameće mnogo pravila za ljude da razumeju stvarni doprinos kompijutera današnjici. Pravila koja definiše računarska etika pokazuju nam kako da pravilno koristimo računar i ne činimo greške u poslu.

Računarska etika počinje da se uvodi u osnovne škole sa ciljem da se djeca pravilno informišu o upotrebi računara i njihovom doprinosu. Računarska etika uči nas kako da upravljamo rizicima i povećamo sigurnost. Računarski korisnici treba da imaju na umu da računari rade po strogim pravilima softverskih programa koji su kreirani od strane ljudi i oni su zamisao ljudi.[11]

[11] www.wikipedija.org

4. Sajber (cyber) kriminal

Računarski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje računarske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se računar upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica. Računarski kriminalitet je takođe protivpravna povreda imovine kod koje se računarski podaci sa predumišljajem menjaju (manipulacija računara), razaraju (računarska sabotaza), ili se koriste zajedno sa hardverom (krađa vremena).

Trebalo je da prođe niz godina od pojave prvih oblika kompjuterskog kriminala do njegovog definisanja i taman su nastale neke srodne definicije kada se pojavljuje novi fenomen – sajber (cyber) kriminal.

Sajber kriminal (engl. Cyber crime) predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivčnog dela, gde se kompjuter ili računarska mreža upotrebljavaju kao sredstvo ili cilj izvršenja. Kompjuteri i kompjuterska tehnologija se mogu zloupotrebljavati na razne načine, a sam kriminalitet koji se realizuje pomoću kompjutera može imati oblik bilo kog od tradicionalnih vidova kriminaliteta, kao sto su krađe, utaje, pronevere, dok se podaci koji se neovlašćeno pribavljaju zloupotrebominformacionih sistema mogu na razne načine koristiti za sticanje protivpravne koristi. Može se konstatovati da je sajber kriminal takav oblik kriminalnog ponašanja kod koga je sajber okruženje u kome se kompjuterske mreže pojavljuju kao sredstvo, cilj, dokaz ili okruženje izvršenja krivčnog dela. Pri tome se pod sajber prostorom, podrazumeva ili vrsta “zajednice” sačinjene od mreže kompjutera u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova ili “prostor koji kreiraju kompjuterske mreže”. Termin sajber prostor prvi je upotrebio Vilijam Gibson u naučno-fantastičnoj noveli Neuromanser (engl. Neuromancer) 1984. godine.[12]

[12] Aleksić Ž. Milosavljević Z. *Leksikon kriminalistike,* Beograd, 1993.

4.1. Tipovi (cyber) sajber kriminala

Postoje dve sub kategorije ovog kriminala:

- Cyber kriminal u užem smislu - kao svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju;
- Cyber kriminal u širem smislu - kao svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža.

Konkretni oblici ovog kriminaliteta su:

- Neautorizovani pristup računarskom sistemu ili mreži kršenjem mera sigurnosti (haking);
- Oštećenje kompjuterskih podataka ili programa;
- Kompjuterske sabotaže;
- Neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama;
- 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 dela cyber kriminala u širem smislu najčešće se pojavljuju:
- Kompjuterski falsifikati
- Kompjuterske krađe

- Tehničke manipulacije uređajima ili elektronskim komponentama uređaja
- 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 dela podržana računarima. Ova dela obuhvataju "rasturanje" materijala ili samo njihovo posedovanje pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbegavanje pravde.

U ova dela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih prava, prodaja zabranjene robe (oružja, kradene robe, lekova) ili pružanje nedozvoljenih usluga (kockanje, prostitucija). Najviše pažnje u ovoj grupi dela privlači dečija pornografija i distribucija raznih materijala Internetom.

- Evropska konvencija o cyber kriminalu predviđa 4 grupe dela:
- Dela 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, pasvorda;
- Dela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;
- Dela vezana za sadržaje – dečija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupni iraspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka;
- Dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskim sistemima**.**
- U Enciklopediji cyber kriminala navodi se da FBI i Nacionalni centar za kriminal belih kragni SAD (National White Collar Crime Center) otkrivaju i prate sledeće oblike:
- Upade u kompjuterske mreže
- Industrijsku špijunažu
- Softversku pirateriju
- Dečiju pornografiju

- Bombardovanje elektronskom poštom
- "njuškanje" pasvorda
- "prerušavanje" jednog računara da elektronski "liči" na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama
- Krađu kreditnih kartica[13]

4.2. Razvoj (cyber) sajber kriminala

Ideja o posebnoj kategoriji kompjuterskog kriminala nastaje otprilike u isto vreme kada su računari postali više mejnstrim. Već šezdesetih godina bilo je izveštaja o kompjuterskim manipulacijama, kompjuterskim sabotažama, špijunažama i nelegalnim korišćenjima računarskih sistema. Dok su sedamdesetih godina viđeni prvi ozbiljni tretmani kompjuterskog kriminala, relativno ograničena uloga računara u svakodnevnom životu usmerila je ove prekršaje na krađe i prevare vezane za telekomunikacione usluge i prenos elektronskih sredstava. U narednim decenijama, sa povećanjem umreženih i personalnih računara transformiše se kompjuterski kriminal i stvara se potreba za specifičnim zakonima vezanim za ovu vrstu kriminala. Evolucija takvog zakonodavstva sledi uzastopne trendove na polju informacionih sistema i zabrinutost za zloupotrebu računarskih sistema. Greškom u programu koja je nazvana "Internet crv" 1988.godine oboreno je 6.000 računara. Iste godine uhapšen je Robert Moris (SAD) i osuđen je na 400 sati dobrotvornog rada i 10.000 dolara. Problemi neovlašćenog pristupa privatnim informacijama skrenuli su pažnju na mogućnost korišćenja računara u svrhe privrednog kriminala. Tako je u periodu od juna do avgusta 1994. u osamnaest upada Vladimir Levin iz Petrograda izvukao preko 10 miliona dolara iz sistema Sitibank (engl. *Citybank*). Naredne godine je uhapšen u Londonu, 1997. je izručen američkim vlastima, a u avgustu iste godine je osuđen na 36 meseci zatvora i kaznu od 250.000 dolara. Kevin Mitnik u SAD je uhapšen i osuđen 1995. godine za falsifikovanje 20.000 brojeva kreditnih kartica. Sa povećanom upotrebom personalnih računara povećala se i briga

[13] Attorney General Report, Cyberstalking: A New Challenge for Law Enforcement and Industry – www.usdoj.gov/ criminal/ cyber crime

za zaštitom od neovlašćenog pristupa računarskim podacima. Sve veća umreženost je uveličala tu brigu i dovela do novih problema, poput napada na udaljene računare i mreže, i dala život delima kao što su povrede autorskih prava, distribucija dečije pornografije i dr. Brz tehnološki razvoj se nastavlja i stvara nove izazove. Sve veća prisutnost na internetu i mrežama izlaže računare novim opasnostima od spoljnih napada, prenos ilegalnih sadržaja, DoS (engl. *Denial of Service*) napada i širenje malvera. Razvoj telekomunikacija i računarstva transformisao je mobilne uređaje u minijaturne umrežene računare sa velikim potencijalom za kriminal.

4.3. Sajber kriminal u Srbiji

Mnogi smatraju da je Srbija tehnološki zaostala zemlja, ali prema visokotehnološkom kriminalu, nalazi se u svetskom vrhu, po podacima američkih službi, na trećem mestu u svetu po prevarama putem Interneta. Prema rečima zamenika tužioca Drugog opštinskog tužilaštva u Beogradu Branka Stamenkovića, kod nas se pojavljuju svi oblici visokotehnološkog kriminala, najraširenija je piraterija, ali ima i računarske sabotaže, prevare, zloupotreba platnih kartica, neovlašćeno korišćenje podataka, pedofilije itd. Zakon o organizaciji i nadleznosti državnih organa za borbu protiv visokotehnoloskog kriminala stupio je na snagu 26. jula 2005. godine, kao odgovor države na visokotehnološki kriminal, i "njim se uređuje obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena ovim zakonom". Pored definisanja šta je visokotehnološki kriminal i oblasti delovanja ovog zakona, za postupanje u predmetima krivičnih dela ovog zakona određeno je Okružno javno tužilaštvo u Beogradu za teritoriju Republike Srbije, i u okviru njega organizuje se posebno odeljenje za borbu protiv visokotehnološkog kriminala. Radom ovog odeljenja rukovodi poseban tužilac koga postavlja republički javni tužilac, pri čemu prednost u izboru imaju javni tužioci i zamenici javnih tužioca koji poseduju znanje iz oblasti informatičkih tehnologija. Posebni tužilac se postavlja na četiri godine sa mogućnošću reizbora.

Ugrožavanje sigurnosti	21 0osoba
Maloletnička pornografija	39 Osoba
Piraterija	11 Osoba
Računarska prevara	21 Osoba
Piratski emiteri	46 Osoba

Slika broj 2: prikazuje broj krivičnih postupaka pokrenutih u 2011 godini

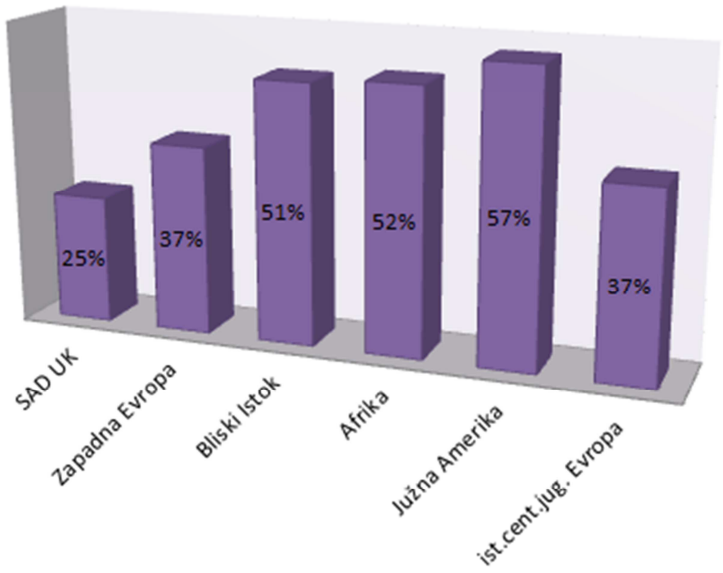
U našem pravu kompjuterska krivična dela, uvedena su Krivičnom zakonom Srbije iz 1998. godine, koja su u Glavi 27 predviđena kao "krivična dela protiv računarskih podataka" (čl. 298-304). U posebnom odeljku, Krivični zakon definiše izraze koji se koriste u zakonu, i u okviru toga daje zakonske definicije koje se odnose na kompjuterska krivična dela. Osnovni pojmovi su: računarski podatak, računarska mreža, računarski program, računarski virus, isprava, pokretna stvar.[14]

[14] www.pretraga.com

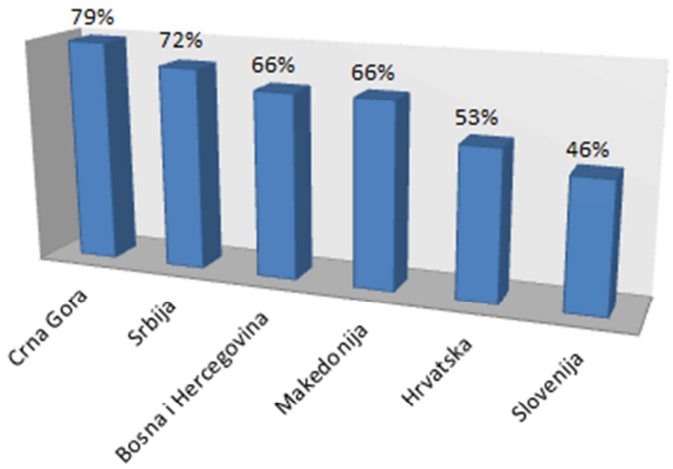
5. Softverska piraterija i virusi

5.1. Softverska piraterija

Softverska piraterija je neovlašćeno kopiranje ili distribucija softvera zaštićenog autorskim pravom. Milioni računarskih korisnika prave kopije programa koje ne poseduju legalno i dobijene kopije distribuira rodbini, prijateljima itd. Iz razloga što samo mali broj softverskih kompanija koristi fizičke metode za zaštitu od kopiranja, kao što je hadverski ključ za zaštitu, kopiranje softvera je jednostavno kao i umnožavanje audio diskova fotokopiranje poglavlja knjiga. Na nesreću, mnogi ljudi nisu svesni da kopiranje softvera, snimanje muzike i knjiga može da prekrši zakone koji štite intelektualnu svojinu.



Slika broj 3: prikazuje stopu softverske piraterije u Svetu



Slika broj 4. prikazuje stopu softverske piraterije u okruženju

Organizacije softverske industrije sarađuju sa bezbednosnim službama za suzbijanje piraterije. Istovremeno oni sponzorišu obrazovne programe da bi korisnici računara postali svesni da je piraterija krađa, zato što zakoni ne mogu da funkcijonišu bez razumevanja i podrške građana.

Ukupna vrednost zakonskog softvera u Srbiji procenjuje se na oko 71 milion evra godišnje, a nezakonitog na 73 miliona evra. Prema Majkrosoftu Srbija, smanjenjem stope piraterije od 10 odsto u Srbiji donelo bi još 20 miliona evra državnom budžetu godišnje i stvorilo 10.000 radnih mesta.

Softverska piraterija je ključno pitanje u pogledu razvoja domaćeg IT sektora, koji se ubraja u najbrže rastuće i najprofitabilnije sektore“, rekao je Miloš Blagojević, menadžer Majkrosofta za poslovni razvoj.

Poreska uprava u Ministarstvu finansija Srbije osnovala je odeljenje za rešavanje pitanja softverske piraterije u Srbiji. Prve inspekcije obavljene su u periodu od 16. maja do 31. oktobra u 161 kompaniji koja plaća porez. Rezultati su pokazali da 42 odsto kompanija koristi zakoniti softver, 57 odsto nezakoniti, a jedan odsto krši licencna prava.[15]

1. [15] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.

5.2. Virusi

Profesor Fred Kohen sa univerziteta u Sinansitiju smatra se prvom osobom koja je 1983. godine uvela reč „virus“ u rečnik računarske terminologije. On je, u svojoj tezi, postavio opštu definiciju virusa, 1984. godine: ˝Definišemo kompjuterski ˝virus˝ kao program koji ˝inficira˝ ostale programe modifikujući ih da uključuju njegovu naprednu kopiju. Sa inficiranog područja, virus se može širiti kroz kompjuterski sistem i mrežu koristeći autorizaciju svakog korisnika, koristeći ih da inficira njihove programe. Svaki program koji se inficira se takođe ponaša kao virus, i stoga, infekcija raste˝.

Kao i većina softverskog koda, virus je obično napravljen za određeni operativni sistem. Virusi za Windows osvajaju samo diskove sa Windows-om, virusi za Macintosh osvajaju samo Macintonsh diskove, itd. Postoje izuzeci: Makro virusi kače sebe na dolumenta koja sadrže makroe – usađene programe za automatizovanje zadataka. Makro virusi mogu da se šire preko računarskih platformi ako su dokumenta napravljena i širena korišćenjem među platformskih aplikacija – najčešće Microsoft Office aplikacija. Makro virusi mogu da se šire preko e-mail priloga bezazlenog izgleda.

Poslednjih nekoliko godina, virusi su se razvili od malih programa koji zadirkuju internetsku poubliku do jakih destruktivnih napadača na kompjutere,zapravo sve ono što se pohranjuje u njima bilo da je u pitanju kompjuter privatnog lica ili poslovnog korisnika. Pri tome je povećana programska složenost virusa kao i sam način upada u kompjuter. Firme koje se bave antivirusnim programima očekuju da se taj trend nastavi.

Računarski virusi su programi pisani sa namerom da poremete rad računara. Nazvani su tako jer imaju sposobnost razmnožavanja. Oni sami sebe iskopiraju na više mesta na disku ili disketi, najčešče na kraju programa koji se trenutno izvršava, čime se taj program produžava. Virus tako na neki način mora da se prikači za domaćina i to tako da kada se izvrši domaćin izvrši se i virus. Ovde je i razlika između virusa i crva, pošto crvima ne trebaju domaćini.

5.3. Nastanak virusa

Istorija kompjuterskih virusa seže do početka druge polovine prošlog veka. U to vreme ozbiljniji računari su bili divovski uređaji čije dimenzije su iskazivane u metrima i tonama, smešteni u zasebne klimatizovane prostorije u blizini kojih se obično nalazilo energetsko postrojenje koje je obezbeđivalo potrebno napajanje.

Korisnici su im pristupali putem terminala, a računarski resursi bili su večno oskudni te bi ih sistem administratori po određenim kriterijumima raspodeljivali među korisnicima, odnosno njihovim aplikacijama. Sa kompjuterskog stanovišta u davna vremena nastali su preci današnjih virusa. Bili su to programi koje su dovitljiviji korisnici pisali obično kako bi neovlašćeno nabavili sistemske resurse svojim aplikacijama, a neretko i da bi se našalili sa kolegama.

Pravi procvat i masovnu pojavu virusi doživljavaju širenjem PC-a po kancelarijama i domaćinstvima, a potom razvojem Interneta, čime je stvorena ogromna baza korisnika - kako potencijalnih žrtava, tako i onih zlonamernih.

5.4. Trojanski konj

Trojanskim konjem se u računarskom žargonu označavaju zloćudni programi, koji su "maskirani" kao korisni ili se proširuju "prikačeni" na druge korisne programe. "Trojanci" obično vrše, neželjene akcije u računaru i to u "pozadini" i prikriveno. Najčešća od tih neželjenih akcija je otkrivanje korisničkih lozinki, bankovnih podataka i drugih poverljivih informacija "prisluškivanjem" razmjene podataka ili jednostavno čitanjem tih datoteka, i javljanje istih "vlasniku" trojanskog konja.

Jedna vrsta trojanskog konja – logička bomba je programirana da napdne kao reakcija na određen događaj ili redosled događaja. Na primjer programer može da ugradi logičku bombu koja je projektovana tako da uništi fajlove sa podacima ako se programer ikada pojavi na spisku optuženih u fajlu personalne službe kompanije. Logička bomba može da se aktivira kada se uloguje određeni korisnik, unese specijalna šifra u polje baze podataka ili korisnik

izvrši određen redosled radnji. Ako se logička bomba aktivira događajem povezanim sa časovnikom, ona se zove tempirana bomba. Dobro je poznat virus sa logičkom bombom, koji je programiran da uništi PC fajlove sa podacima na Mikelanđelov rođendan.

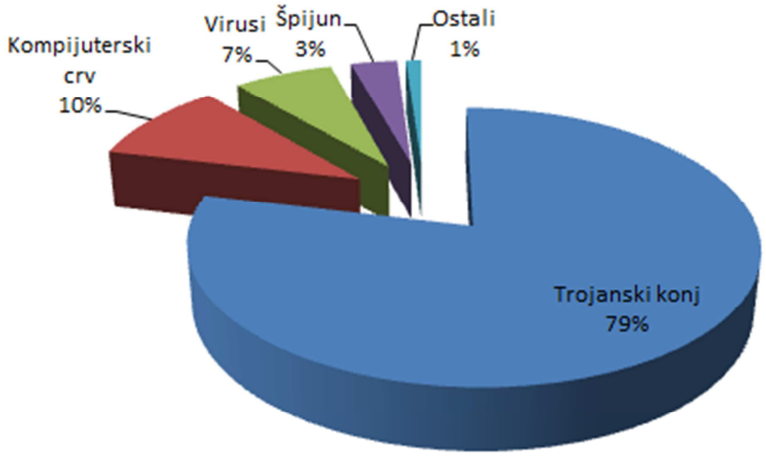
Trojanski konji mogu da prouzrokuju ozbiljne probleme u računarskim sistemima svih veličina. Da stvar bude gora mnogi trojanski konji prenose softverske viruse.

Poznati trojanski konji su:

- Back Orifice
- Netbus
- SubSeve

Trojanci su postavili novi rekord u svojoj kategoriji i time dokazali da su i dalje omiljeno sredstvo sajber kriminalaca za krađu podataka, koji u ukupnom broju malvera učestvuju sa čak 80%. U 2011. godini Trojanci su činili 73% svih malvera. Kompjuterski crvi i virusi su zamenili prošlogodišnje pozicije te su tako crvi sada na drugom mestu sa 9,3%, a virusi na trećem sa 6,43%.[16]

2. [16] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.



Slika broj 4: prikazuje statistiku zastupljenosti virusa u 2011 godini

5.5. Crv

Računarski crvi su računarski programi koji umnožavaju sami sebe. Pri tome koriste računarske mreže da bi se kopirali na druge računare, često bez uticaja čoveka. Za razliku od virusa, svojim delovanjem ne moraju inficirati druge programe. Mogu stići i kao fajl u mejlu te im pristup računaru omogućuju propusti u operativnim sistemima i aplikacijama. Crvi otežavaju rad mreže, a mogu oštetiti podatke i smanjiti sigurnost računara.

Prvi poznati crv napravio je student Cornell-a u okviru eksperimenta, 1988. godine. Crv je slučajno pušten na internet i blokirao je 6000 računara širom SAD. U leto 2001, godine pojavio se crv nazvan Code Red. Ovaj crv nije napadao PC računare. Njegova meta su bili internet servisi koji rade pod Microsoft serverima. Vlada SAD i Microsoft su poslali upozorenje o crvu i napravili besplatne softverske zakrpe radi zaštite servera.

Crvi se sastoje od samokopirajućeg koda koji omogućava razmnožavanje i širenje crva i tereta (payload), a teret može biti:

- Nepostojeći/nefunkcionalan – Najčešći slučaj kod većine crva je upravo ovaj, kada ne postoji kod osim koda za širenje ili u njemu postoji nekakva greška pa nije funkcionalan.

- Daljinska kontrola – Otvara backdoor na žrtvinom računaru.
- Spam relays – Deo crva Sobig kreira mail relay koji spameri mogu koristiti da bi slali neželjenu elektronsku poštu. Većina Internet provajdera ima sigurnosne mehanizme koji blokiraju spam sa poznatih IP adresa, ali kod zaraze ovim crvom spam dolazi sa svih strana i nemoguće je na taj način kontrolisati njegovo širenje.
- HTML-proksi – Još jedna osobina crva Sobig je distribucija HTML-proksija. Preusmeravajući veb zahteve preko mnogo proksija veb stranice sa zabranjenim sadržajem dobijaju na vremenu jer provajderima treba puno vremena da otkriju na kojoj se adresi veb stranica fizički nalazi. Ovo se koristi za razne nelegalne aktivnosti, uključujući prevare sa upisivanjem finansijskih podataka ili brojeva kartica.
- Internet DOS – Još jedan čest teret je Internet DOS (Denial of Service) napad. Code Red, Yaha i još mnogo crva sadrže DOS alate, koji su ili upereni protiv određene stranice ili se mogu uperiti protiv bilo koga ako autor crva to poželi. Kada crv zarazi 100.000 ili više računara zombija moguće je nedostupnom učiniti bilo koju stranicu, pa čak i celi DNS sistem.
- Skupljači podataka – Većina ljudi na računaru na kojem rade imaju osetljive podatke poput poslovnih tajni, nacrta novih uređaja, finansijskih izveštaja, itd. Crv može pretražiti disk računara u potrazi za tim podacima i zatim ih poslati na pre određeno mesto.
- Brisači podataka – Postoji mnogo virusa, sadrže kod za brisanje podataka nakon određenog vremena. Budući da se crvi mogu širiti mnogo brže, mogli bi da počnu da brišu podatke odmah nakon infekcije.
- Fizička šteta – Većina današnjih računara podržava nadogradnju pokretačkog softvera, pa tako i računari imaju BIOS čip koji je moguće flešovati direktno iz Vindousa. Ukoliko se u flašu čip upišu pogrešni podaci računar više neće moći da se pokrene.

Crvi i virusi su kreirani za prenos payloada na računar. Payload je kreiran za provođenje specifičnih funkcija kao što su brisanje ili promena podataka, instalisanje softvera na računar i kreiranje stražnjih vrata koja napadač može kasnije upotrebiti da bi dobio neovlašćen pristup računaru. Internet crvi i virusi stvaraju probleme inficiranim računarima, ali crvi mogu napraviti veću štetu zbog mrežnog prometa koji generišu prilikom širenja Internetom. Npr. crv SQL Slammer u januaru 2003. godine je na vrhuncu brzine širenja udvostručavao broj zaraženih računara svakih 8,5 sekundi.

Najbolja zaštita od virusa i crva je antivirusni softver. Taj softver može da spreči instaliranje virusa, a može i da otkrije, izoluje i ukloni crve i viruse sa računara koji su se

provukli kroz odbrambene mehanizme. Ali, može da zaštiti od poznatih virusa, a od onih za koje se ne zna (novih virusa) teže je se zaštititi. Metode zaštite su i zaštitni zidovi (firewall), neotvaranje neobičnih poruka e-pošte i redovno ažuriranje softvera.

5.6. Špijun

Špijun (engl. Spyware) je široka kategorija štetnog softvera sa namenom da delimično presreće ili preuzima kontrolu nad računarom bez znanja ili dozvole korisnika. Iako sam naziv sugeriše da je reč o programima koji nadgledaju rad korisnika, ovaj naziv danas označava široku paletu programa koji iskorišćavaju korisnički računar za sticanje koristi za neku treću osobu.

Špijun se razlikuje od virusa i od crva u tome što se obično ne razmnožava. Kao mnogi novi virusi, špijun je stvoren da iskorišćava zaražene računare radi komercijalne dobiti. Tipične taktike su prikazivanje iskačućih oglasa, krađa ličnih podataka (uključujući i finansijske podatke kao što su brojevi kreditnih kartica i lozinke), praćenje aktivnosti na internetu za marketinške svrhe ili preusmeravanje HTTP zahteva na oglasne stranice. U nekim slučajevima, špijun se koristi za proveravanje pridržavanja uslova licence za korišćenje programa.[17]

Zaraza se u najvećem broju slučajeva događa prilikom otvaranja stranica s nelegalnim ili pornografskim sadržajem.

3. [17] Veinović M. Milosavljević M. Gruber G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.

6. Zaštita računara i zaštita podataka

U današnjem elektronskom svetu, postoje dve napasti koje svakog korisnika računara pre ili kasnije "stignu" – SPAM poruke i virusi – programi napisani samo sa jednim ciljem – da vam na posredan ili neposredan način nanesu štetu. Pri tom ću termin "virusi" koristiti široko: to su svi programi koji vam na neki način smetaju – ili šalju poštu u vaše ime sa ciljem da zaraze i vaše sagovornike, ili izbacuju dosadne reklame dok surfujete Mrežom (tzv. Adware programi) ili javljaju svojim tvorcima vaše poverljive podatke i/ili navike (tzv. Spyware programi).

Razvoj svakog korisnika računara prolazi kroz nekoliko jasno odvojenih faza: nabavka računara, instalacija svakog mogućeg programa ili igre, upoznavanje mogućnosti same sprave i pronalaženje pravog mesta za novu igračku ili alat, u zavisnosti za šta će se računar primarno koristiti. Posle toga dolazi faza razumnog korišćenja, kada se pravi selekcija i kada se pravi željeno radno okruženje. U ovoj fazi dolazi do stvaranja dokumenata ili drugih objekata (pošta, slike, crteži) koji nose i određenu vrednost za korisnika, bilo materijalnu, bilo neku drugu. U ovoj fazi treba poraditi na promenama navika kada je korišćenje računara u pitanju. Najvažnija navika, najvažnija rutina koju treba da steknete pre nego li vaš računar postane ozbiljan alat za vas je: Da li ste skoro napravili kopije vaših važnih podataka? Vaš adresar, vaša pošta, dokumenta, crteži, stvari koje su nastale kao rezultat vašeg rada? Najjednostavniji način, najjevtiniji način za zaštitu vaših podataka je upravo redovno kopiranje na neki drugi medijum.[18]

[18] www.wikipedija.org

6.1. Bezbednost – smanjenje rizika

Sa porastom računarskog kriminala, računarska bezbednost je postala važna briga za administratore sistema i računarske korisnike. Bezbednost se odnosi na zaštiti računarskih sistema i informacija protiv neželjenog pristupa, oštećenja, modifikacije ili uništavanja. Računari imaju dvije unutrešnje karakteristike koje ih ostavljaju otvorenim za napade ili greške u radu:

- Računar radi tačno ono za šta je programiran, uključujući otkrivanje poverljivih informacija. svaki sistem koji može da se programira može da se i reprogramira.
- Svaki računar može da uradi samo ono za šta je programiran. On ne može da zaštiti samog sebe od otkazivanja ili namernih napada osim ako su takvi događaji posebno pretpostavljeni, obrađeni i odbijeni odgovarajućim programiranjem.

Vlasnici i administratori računara koriste različite bezbednosne tehnike da zaštite svoj sistem, obuhvatajući svakodnevne jednostavne fizičke blokade i ograničenja do naprednih tehnika koje koriste kriptološke sisteme (šifrovanje) i biometrijske podatke.

6.2. Antivirusna zaštita

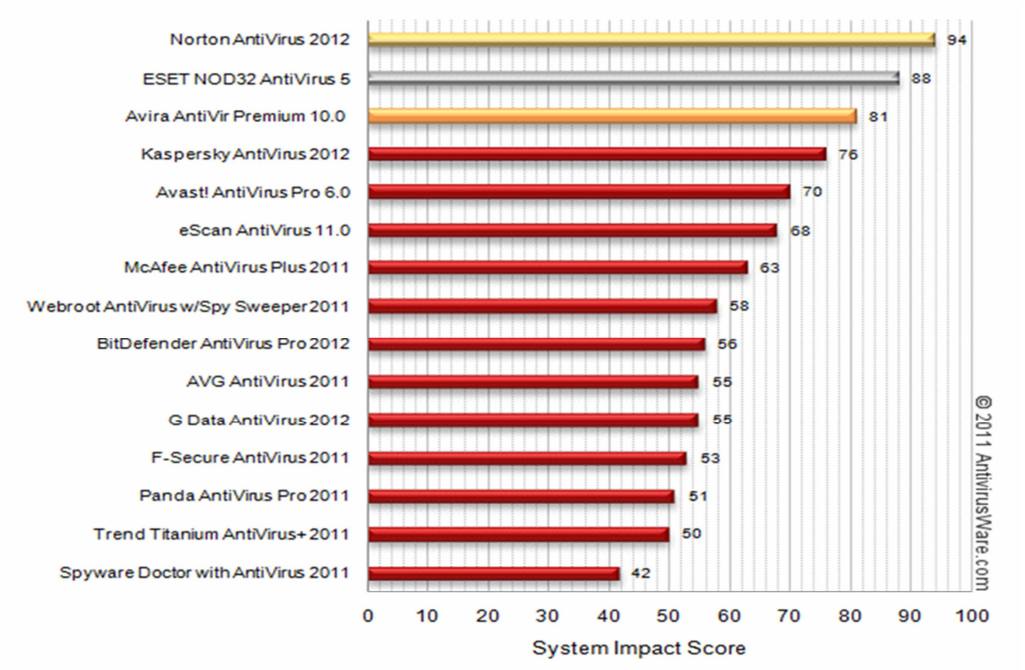
Antivirusni softver ili antivirus je računarski softver koji se koristi za zaštitu, identifikaciju i uklanjanje računarskih virusa, kao i sveg drugog softvera koji može da ošteti ili nanese štetu računarskom softveru, a jednim imenom se naziva malver.

Za razliku od prvobitnih antivirus softvera koji su bili bazirani isključivo na tretiranju računarskih virusa, moderni antivirus softver se dizajnira tako da sistem štiti od što većeg broja različitih mogućih malvera, kao što su crvi, fišing napadi, bekdor, rutkit, trojanci...

Prvo poznato uklanjanje jednog računarskog virusa izvršeno je 1987. godine softverom Bernt Fiks, a radilo se o jednom od prvih poznatih virusa — Viena virusu.

Savremeni virusi mogu da se raširе brže od virusa od pre par godina iz nekoliko razloga. Prenos podataka na internetu se neprekidno ubrzava, a samim tim se ubrzava i prenošenje virusa. Web strane, makroi i druge tehnologije daju autorima virusa nova mjesta za skrivanje štetnih programa. Pored toga, povećana standardizacija Microsoft aplikacija i operativnih sistema olakšala je širenje virusa.

Antivirusni programi (poznati kao AV softver) su projektovani da traže viruse, obavjeste korisnika kada ih nađu i uklone ih sa zaraženog diska ili fajla. Većina antivirusnih programa neprekidno nadgleda aktivnost sistema, prateći i izvještavajući o sumljivim radnjama nalik virusima. Međutim ne postoji antivirusni program koji može da otkrije sve viruse. I ovi programi, sa pojavom novih virusa, moraju stalno da se poboljšavaju. Većina antivirusnih programa može automatski da preuzme novi programski kod sa web-a.



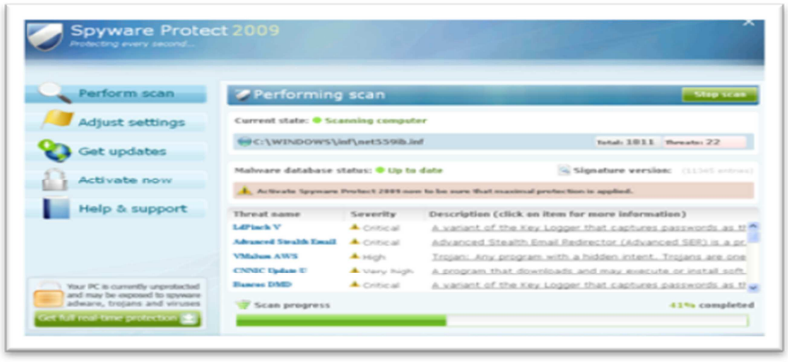
Slika broj 5: Prikazuje podelu antivirusnih programa po kvalitetu 2011/12 godini

Međutim ponekad je softverskim kućama potrebno nekoliko dana da razviju i distribuiraju zakrpe za novi viruse. Za to vrjeme destruktivni virusi mogu da načine veliku štetu. Borba protiv virusa, kao i razvijanje novih virusa se neprestano razvija. Većina korisnika je naučila da ne otvara nedefinisane e-mail priloge, a prodavci softvera su počeli da

modifikuju e-mail aplikacije da bi sprečili ovu vrstu napda. Međutim, crv nazvan BubleBoy demontirao je da sistem može da se zarazo email-om čak i ako mail nije otvoren. Neki virusi su čak razvijeni da zaraze HTML kod ma Web stranama ili HTML e-mail porukama. HTML virusi ne mogu (trenutno) da zaraze računar kada se pregleda zaražena Web strana. Zaraženi HTML kod mora da se preuzme download-uje na računar.

6.3. Lažni antivirusi

Mnogo puta se pisalo o programima koji se pretvaraju da su nešto što nisu. Najozloglašenija su lažna antivirusna rešenja - programi koji objavljuju poruke da je ciljani kompjuter zaražen, čak i ako nije. Ovi programi niti skeniraju niti čiste kompjutere, i ustvari su i pravljeni sa ciljem da ubede korisnike da su im kompjuteri izloženi opasnosti i preplaše ih dovoljno da kupe „antivirusni“ program. Ovakvi programi su često označeni kao 'scareware'. Kaspersky Lab ih je svrstala kao 'FraudTool' (prevarantsku alatku), podgrupu 'RiskWare' grupe.



Slika broj 6: Prikazuje izgled lažnog antivirusnog programa

Ovakvi programi su veoma široko rasprostranjeni a cyber-kriminalci ih sve više koriste. Dok je Kaspersky Lab otkrio oko 3.000 lažnih antivirusnih programa u prvoj polovini 2008. godine, više od 20.000 uzoraka je identifikovano u prvoj polovini 2009. godine.

Kao prvo, kako lažni antivirusni programi završavaju na ciljanom kompjuteru? Oni se šire korišćenjem istih metoda kojima se šire i drugi štetni programi: na primer, Trojan-Downloader može tajno da download-uje ovakve programe, ili ranjivosti na

kompromitovanim/zaraženim sajtovima mogu biti iskorišćene za izvođenje 'drive-by download. Međutim, ovakve programe download-uju korisnici, cyber-kriminalci koriste namenske (Hoax) programe ili reklame da bi prevarili korisnike da upravo urade ovakav download.

Hoax progami su još jedna vrsta prevarantskog softvera: oni su stvoreni sa namerom da ubede korisnike da im je potreban download čudesno delotvornog antivirusnog rešenja, a glavna funkcija im je instaliranje lažnog antivirusnog rešenja na ciljanom kompjuteru čak i ako korisnik odbije ponudu.

Hoax programi bivaju download-ovani na ciljane kompjutere bilo korišćenjem backdoor-a, bilo iskorišćavanjem ranjivosti na web sajtu. Čim se takav program instalira, pojavljuje se upozorenje o navodnom postojanju višestrukih grešaka, oštećenom registru ili se pak pojavljuje navodna poruka da su vam ukradeni poverljivi podaci.

6.4. Ograničenje fizičkog pristupa

Jedan od načina za smanjenje rizika od bezbednosnih proboja je osiguranje da samo ovlašćeno osoblje ima pristup računarskoj opremi. U zavisnosti od sistema bezbednosti pristup računaru može biti odobren na osnovu:

- Posedovanja dokumenata ili uređaja: ključ ID kartica sa fotografijom ili smart kartica koja sadrži digitalno šifrovanu identifikaciju u ugrađenom čipu;
- Poznavanja i pamćenja- lozinka, ID broja, kombinacija ili deo lične istorije, kao što je npr djevojačko prezime majke;
- Način vršenja neke radnje- potpis, brzina kucanja;
- Biometrijskih podataka: glas, otisak prsta, skeniranje mrježnjače, skeniranje osobina lica ili druga mjerenja pojedinih tjelesnih karakteristika.

Većina ovoh bezbednosnih kontrola mogu da se kompromituju, zato većina sistema koriste kombinaciju kontrola. Na primer, od zaposelenog može da se zahteva da pokaže bedž, otključa vrata ključem i otkuca lozinku za korišćenje zaštićenog računara.

6.4.1. Lozinke

Lozinke (paswords) su najčešći alati koji se koriste za ograničenje pristupa računarskim rsursima. Lozinke su efektivne pod uslovom da su pažljivo izabrane. Većina korisnika računara bira lozinke koje je lako pogoditi: imena pratnera, dece ili kućnih ljubmaca, reči vezane za poslove ili hobije ili uzastopne karaktere na tastaturama. Mnogi bezbednosni sistemi odbijaju da omoguće korisnicima izbir bilo koje govorne reči ili imena kao lozinku tako da hakeri ne mogu koristiti softverske rečnike za njihovo sistematsko pogađanje. Čak i najbolje lozinke treba često menjati.

Softver za kontrolu pristupa ne treba da tretira sve korisnike na isti način. Mnogi sistemi korite lozinke da ograniče korisnike tako da oni mogu da otvore samo fajlove vezane ze njihov posao. U dosta slučajeva korisnicima je dato pravo pristupa samo za čitanje fajlova tako da mogu da ih vide ali ne mogu da ih menjaju.

7. Zloupotrebe i prevare primenom novih tehnologija

Nove tehnologije pružaju velike mogućnosti za različite vrste zloupotreba i prevara, najviše iz razloga što mehanizmi zaštite poslovanja na internetu još uvek nisu dovoljno razvijeni. Danas mnogi prevaranti koriste Internet za različite vrste zloupotreba i prevara. Prema istraživanju američkog udruženja za zaštitu potrošača (NLC) , čak 98% ispitanih je reklo da su bar jednom dobili e-mail u kojem su im bile ponuđene finansijske usluge ili neobični poslovni predlozi.

Prevare čini skup aktivnosti koje karakterišu obmana, lažno predstavljanje, prikrivanje činjenica, manipulacija, izgubljeno poverenje i slično. Ova kategorija je poznata i pod nazivom "kriminal bele kragne". Osnovno obeležje ovog dela je dovođenje nekog u zabludu da bi se time pribavila protivpravna imovinska korist. U suštini se svode na lažno prikazivanje činjenica ili prećutkivanje činjenica. Automatizacijom klasičnih i nastajanjem novih metoda ovaj vid zloupotreba dobija i na kvalitetu i na kvantitetu.[19]

Jedan od najrasprostranjenijih oblika krivičnih dela prevare koji se vrši uz pomoć računara je prevara poznata kao „Nigerijska prevara“, ili prevara poznata pod nazivom „prevara 419“, pojavila se ranih 80-tih godina, sa naglim ekonomskim razvojem Republike Nigerije, koji se zasnivao na upotrebi naftnih resursa. U toku prve decenije 21-og veka „prevara 419“ postala je veoma popularan način izvršenja krivičnih dela prevare u Africi, Aziji i Istočnoj Evropi, a u posljednje vreme i u Sjevernoj Americi, Zapadnoj Evropi (uglavnom Velikoj Britaniji) i Australiji.

Dobila je naziv po članu broj 419 Nigerijskog krivičnog zakona (koji je deo poglavlja 38) pod nazivom „Pribavljanje imovine pomoću prevarnih radnji: Prevara“, koji definiše ovo krivično delo (Chawki, 2009:2). Američko društvo za dijalektiku je utvrdilo da se izraz „prevara 419“ koristi od 1992. godine. „Nigerijska prevara“ je metoda vršenja krivičnog dela prevare uz pomoć računara i najčešće počinje pismom ili elektronskom porukom koja je tako osmišljena da izgleda kao da je namjerno

[19] Aleksić Ž. Milosavljević Z. *Leksikon kriminalistike,* Beograd, 1993.

poslata primaocu poruke. Radnja izvršenja „Nigerijske prevare“ uglavnom počinje ubjeđivanjem „žrtve“ prevare da učestvuje u podjeli određenih novčanih fondova ako unapred uplati određeni novčani iznos koji je, u najvećem broju slučajeva, neuporedivo manji od onog iznosa koji bi trebalo da dobije kao korist od tog fonda (Smith et al., 1999:1).

- Vreme svetske krize pokazalo se kao odlično vreme za Internet prevare. Cyber kriminalci postali su sofisticiraniji i tehnološki napredniji, pa prema izvještaju specijalizovane kompanije za online bezbjednost Actimize, predstavljeno je deset najčešćih načina za prevare putem Interneta:

- Prevare na društvenim mrežama - kriminalci hakuju (neovlašćeno preuzmu, " uđu") na nalog korisnika na nekoj od online društvenih mreža, kao što su Facebook, Twitter, MySpace ili Bebo i šalju poruke prijateljima i članovima porodice da su u nevolji i da je potrebno odmah da se pošalje novac na neku adresu.

- "Kladioničarska" prevara-žrtva dobija rezultat fudbalske utakmice putem elektronske pošte. Trik je u tome što većina korisnika koja prima ovakve poruke dobija netačne rezultate, ali ipak manji procenat korisnika dobija i tačne rezultate. - Prevare "uštede novca" - savršene za periode ekonomskih kriza, ove prevare putem Interneta, telefona ili pošte uključuju veliki broj finansijskih pomoći i ponuda za konsolidaciju kredita i kredita za nekretnine, sniženje kamatne stope, i sl., uz obavezu korisnika da uplati određeni iznos.

- "Crna" prevara - uglavnom se viđa u Aziji, nije tako česta na Zapadu. Naime, prevaranti obično pozivaju ili šalju e-mail starijoj osobi navodeći da je njihovo djete stradalo u saobraćajnoj nesreći i da je potrebno hitno da uplate određeni novčani iznos.

- Ponuda koju ne možete odbiti - korisnicima Interneta nude se čekovi, najčešće ukradeni kao nagrada za kupovinu nekog proizvoda. Takođe, traži se od kupaca da uplati depozit na neki račun, uz neku proviziju koju zadržava žrtva prevare. Međutim, ček se ubrzo stornira, dok kriminalci uzimaju depozit.

- Neautorizovana kompanija (e-processor) za naplatu - korisnicima se šalju zahtevi za "ponovnim upisom korisničkih informacija o broju platne kartice", u okviru čega su stranice identične stranicama nekih poznatih kompanija, kao što su eBay, Amazon i sl., samo je adresa potpuno različita.

- Telefonska prevara - prevarant poziva korisnika i informiše ga da je došlo do problema sa sigurnošću u okviru njegovog naloga. Zatim putem konferencijske veze kriminalac poziva banku, čiji predstavnik traži sigurnosne informacije (lozinku i tajno pitanje, ili PIN code). Žrtva odgovara na pitanja o tajnim podacima i na taj način i prevarant dolazi do neophodnih informacija da pokrade novac sa računa.

E-mail sa "trojancima" - kada korisnik u okviru e-maila klikne na link, ili otvori prilog poruke, ukoliko nema efikasnu Internet zaštitu, zaraziće se trojancem, zloćudnim programerskim kodom koji će sa računara pokrasti sve tajne podatke i šifre. [20]

[20] www.netnovinar.org

Zaključak

Reč etika potiče od grčke reči ethos - običaj i ethikos – moralan. Etika je nauka o moralu, nauka o proučavanju i procenjivanju moralnih vrednosti. To je filozofska disciplina, koja proučava moral, njegovo poreklo, ciljeve i smisao.

Etičke dilema je situacija do koje dolazi kada se čini da su dve ili više moralnih vrednosti jednako validne, a kontradiktorne, a od pojedinaca se zahtjeva da napravi najbolji mogući izbor.

U savremenom globalizovanom svetu nove tehnologije se razvijaju velikom brzinom, pa se kao najvažnije tehnologieje današnjice izdvajaju telekomunikacije, elektronika, kompjuteri, novi materijali, opelektrika, birotehnologija, energetsko inženjerstvo, informatizacija, sofistikacija i medikalizacija.

Prikljucivanjem racunara na Internet, odnosno na racunarsku mrežu realizovanu Internet tehnologijama, postoji realna opasnost da neko ko se takode nalazi u mreži kao uljez pristupi resursima našeg racunara, na primer podacima na disku koji predstavljaju poslovnu prepisku. Da li je, onda, naša kompanija sigurna ? Jedna od posledica narušavanja necije privatnosti može da bude i tzv. krada identiteta.

Računari imaju rastuću ulogu u borbi protiv kriminala, istovremeno, bezbednosne službe se suočavaju sa povećanjem računarskog kriminala. Većina računarskih zločina prođu neopaženi a dosta onih koji su otkriveni često prođu neprijavljeni.

Zbog porasta računarskog kriminala i drugih rizika, organizacije su razvile brojne bezbednosne tehnike da zaštite svoje sisteme i podatke. Međutim ti alati postaju manje efikasni u doba personalnih računara i mreža. Lozine, šifrovanje, postavljanje zaštite i softver za kontrolu se koriste da zaštite poverljive podatke u različitim organizacijama. Bezbednosne mreže služe da zaštite našu privatnost i druga individualna prava. Ali, povremeno, bezbednosne procedure prete tim pravima. Ustupci između računarske bezbednosti i slobode podižu važna pravna i etička pitanja.

Jedan od vidova borbe protiv računarskog kriminala je stalna edukacija kroz česte treninge koji obezbeđuju uspešnost u otkrivanju krivičnih dela, dokaze i samih počinoca.

Edukacija u tom smislu mora biti na nivou saradnje sa predstavnicima zemalja koje imaju zavidne uspehe u borbi protiv računarskog kriminala i na internacionalnom nivou.

Računarskim sistemima ne predstavljaju samo pretnju ljudi, njima takođe prete softverski bagovi i hardverski kvarovi. U modernim vojnim aplikacijama, bezbednost i pouzdanost su kritične. Kako se brzina, snaga i kompletnost oružanih sistema povećava, mnogi se plaše da su ljudi istisnuti iz procesa donošenja odluka.

Literatura

1. www.wikipedija.org
2. www.pretraga.com
3. www.netnovinar.org
4. Aleksić Ž. Milosavljević Z. *Leksikon kriminalistike,* Beograd, 1993.
5. Veinović M. Milosavljević M. Grubor G. *Informatika,* Univerzitet Singidunum, Beograd, 2009.
6. Computer Crime and Intellectual Property Section (CCIPS),www.cybercrime.gov/Osowski_TangSent.htm, Novembar, 2001..
7. "Ethics for a new millennium" Dalai Lama XIV - Tenzin Gyatso
8. Attorney General Report, Cyberstalking: A New Challenge for Law Enforcement and Industry – www.usdoj.gov/ criminal/ cyber crime