Lejla KARABAŠIĆ[1]

Kompjuterski ekonomski kriminal

Computer And Economical Crime

Sažetak

Osamdesetih godina svijet je iz ere industrije zakoračio u eru informacione i telekomunikacione tehnologije, a kratko nakon toga globalizacija mijenja svijet ekonomskog, političkog, pravnog i duhovnog života. Napredak informacionog društva, karakterisan razvojem kompjutera i na njima zasnovani mrežni sistemi, brza i promptna razmjena informacija i razvoj elektronskog poslovanja prati i transformacija klasičnih oblika kriminaliteta. Kao i drugi segmenti društva i kriminal se prilagođava novom dobu. Klasične, fizičke krađe postaju stvar prošlosti. Umjesto njih predmet napada ili sredstvo napada postaje kompjuter. Već 1981. godine Vijeće Evrope ukazuje na činjenicu da je kompjuterski kriminal po osnovu iznosa nezakonito stečene koristi izašao u sam vrh ljestvice kriminalnih djela, zajedno sa drogama i trgovinom oružjem.

Kompjuterski kriminal znači upotrebu kompjuterskih resursa za neautorizovane ili ilegalne radnje. On se može generalno podijeliti na dvije grupe kriminalnih djela: djela koja krše važeće etičke norme i vrijeđaju privatnost i dostojanstvo čovjeka i djela počinjena s ciljem ostvarenja imovinske koristi. Mada je članak posvećen kompjuterskom ekonomskom kriminalitetu, nedavni događaj terorističkih napada u USA su svakako iznijeli u prvi plan mogućnost korištenja kompjutera pri terorističkim akcijama, pojam kompjuterskog kriminaliteta se posmatra u sasvim drukčijem svjetlu, a posebno jačanje fizičke zaštite sistema i procjena eventualnih meta napada i načina i vjerovatnoća izvršenja. Mada je, uslijed neophodnosti što brže akcije, akcenat stavljen na intenziviranje metoda zaštite od ulaska u informacione sistema, u USA je uslijedio i val

[1] Asistent na Fakultetu kriminalističkih nauka u Sarajevu

ojačavanja ovlasti državnih sigurnosnih agencija, kroz izvršene promjene u zakonodavstvu, od proglašavanja i definiranja komjuterskog terorizma kao krivičnog djela do ovlaštenja FBI o nesmetanoj kontroli bilo kojeg kompjuterskog sistema, bez prethodnog sudskog naloga ili dokaza, što je prethodno bila praksa. Osnovna karakteristika ovog kriminaliteta, bez obzira o kojoj se grupi kriminalnih akata radi, je da je vrlo teško utvrditi i sankcionisati počinitelja, zbog:

- *anonimnosti počinitelja – zloupotrebe se dešavaju u virtualnom svijetu i veliki dio počinitelja zloupotreba uspješno ukloni tragove; i*
- *neprijavljivanje napada na kompjuterski sistem – preduzeća izbjegavaju prijaviti štete jer bi ta informacija ugrozila rejting preduzeća, i izazvala znatno veće štete.*

Uslijed ekspanzije kompjuterskog kriminala i imovinskih koristi koje on donosi, težište problematike danas se odnosi na povećanje sigurnosti sitema, zaštitu sistema i uspostavljanje pravno-kaznenog poretka, kroz dva osnovna pravca prevencije od kompjuterskog kriminala: mjera fizičke zaštite i sigurnosti sistema i izgradnja adekvatne pravne regulative.

Kriminal i kompjuterska tehnologija

Već početkom osamdesetih godina kompjuterski kriminalitet preuzima jedno od vodećih mjesta u okviru društveno štetnih i nezakonitih aktivnosti i postaje ozbiljna prijetnja zdravom ekonomskom privređivanju. Posljedice zloupotreba IS-a sa aspekta nezakonito stečene imovinske koristi stavljaju ovu vrstu kriminala u sam vrh akutnih krivičnih djela kao što su droga, prostitucija i nelegalna trgovina oružjem.

Godine 1981. Komitet ministara Vijeća Evrope donosi konvenciju o krivičnim djelima ekonomskog kriminala kojom obuhvata slijedeće povrede: djela pronevjere i zloupotrebe ekonomske situacije od strane multinacionalnih preduzeća; neosnovano osnivanje ili zloupotreba državnih ili međunarodnih donatorskih organizacija; *računarski kriminal (krađa podataka, manipulacija podacima, odavanje tajni);* osnivanje lažnih preduzeća; lažiranje bilansa stanja preduzeća i povrede zakona o računovodstvu; pronevjera u odnosu na ekonomsku situaciju i udruženi kapital preduzeća; kršenje sigurnosnih i zdravstvenih propisa od strane preduzeća; pronevjera na štetu kreditora; pronevjera na štetu korisnika; neravnopravna konkurencija; krađa novca ili preuveličavanje troškova od strane preduzeća na račun društva; povreda carinskih zakona; povreda zakona o novcu i valuti; povreda zakona o bankama i berzi; i povreda ekoloških zakona.

Stvarne posljedice kompjuterskog kriminaliteta, koji ujedno ima i najveću dinamiku razvoja, je teško odrediti. Prema mišljenju stručnjaka OECD-a čak 75-80% kompjuterskih zloupotreba nije prijavljeno. A nacionalni odred za kompjuterski kriminal FBI smatra da je manje od 10% svih kompjuterskih djela prijavljeno, a da 85-97% kompjuterskih kriminalaca hoda slobodno.

Još je teže utvrditi stvarne razmjere šteta na nivou nacionalne ekonomije. Uprkos vrlo malom broju otkrivenih i prijavljenih djela, slijedeći podaci vrlo ilustrativno govore o razmjerama šteta prouzrokovanih zloupotrebom IS-a:

- Business Softver Aliance, udruženje svjetskih proizvođača softvera navodi slijedeće stope softverskog piratstva za 1996. godinu: Hrvatska 94%, Slovenija 91%, Mađarska 69%, Italija 55%, Kanada 42%, USA 40%. Softversko piratstvo je 1995. godine oštetilo softversku industriju za 13,1 milijardu US$.
- Britanski *Departement of Trade and Industry* navodi podatak da štete od kompjuterskog kriminala nanesene brtanskoj privredi iznose čak 2 milijarde funti godišnje.
- U USA štete od kompjuterskog kriminala iznose oko 63 mld US$ godišnje.
- Njemačka je 1996. godine registrirala 32.128 slučajeva ove vrste kriminala, 26.802 slučaja manipulacije bankomatima, 3.588 slučajeva kompjuterskih prevara, 198 slučajeva krivotvorenja kompjuterskih podataka, 282 slučajeva neovlaštene izmjene podataka i kompjuterske sabotaže.

Sa kriminološko-kriminalističkog aspekta još uvijek se vode sporovi o pojmu «kompjuterski kriminalitet».

Ipak, taj pojam prema prof. dr Šimundić Slavku[2] obuhvata zloupotrebu računala, kompjuterske prevare, delikte uz pomoć kompjutera, kriminalitet kroz automatsku obradu podataka i kriminalitet kroz elektronsku obradu podataka. Kompjuter se može pojaviti kao sredstvo izvršenja kompjuterskog krivičnog djela, a u drugom slučaju može biti objekat kriminalnog napada.

---

[2] Slavko Šimundić ISTRAŽIVANJE I SUZBIJANJE RAČUNALNOG KRIMINALITETA U HRVATSKOJ I SVIJETU, Zbornik radova pravnog fakulteta u Splitu, br.3-4, Split 1999

Prof. dr Dragan Roller[3] smatra da je razlikovanje kompjuterskog kriminaliteta u odnosu na druge vrste kriminaliteta vezano za specifičan način izvršenja pomoću kompjutera. Npr. kada se izvrši pljačka banke pomoću kompjutera, iako se radi o imovinskom deliktu riječ je ipak o kompjuterskom kriminalitetu.

U literaturi na engleskom jeziku u vezi sa definiranjem kompjuterskog kriminaliteta u upotrebi su pojmovi poput kompjuterski zločin (computer crime), kompjuterska zloupotreba (computer abuse), prevara i krađa uz pomoć kompjutera (fraud and theft by computer manipulation), kompjuterska sabotaža, špijunaža, nedopušten pristup kompjuteru, te zločin u vezi sa kompjuterom (computer related crime).

Granice definiranja kompjuterskog kriminala se svakodnevno pomjeraju uslijed razvoja i evolucije kompjuterske tehnologije. No, za utvrđivanje kompjuterskog kriminaliteta bitno je utvrditi one elemente koji ukazuju da je pomoću kompjutera izvšeno kazneno djelo. Specifičnost kompjuterskog kriminala se ogleda i u činjenici da počinilac ne mora biti na mjestu zločina da bi ga počinio, i da s druge strane za ovu vrstu kriminala ne postoje državne granične restrikcije. Sa pravnog aspekta postavlja se i pitanje jurisdikcije, odnosno nadležnosti za procesiranje slučaja, npr. ukoliko je prevara počinjena u Kaliforniji, a preko kompjuterskog sistema u NY, da li su za istragu nadležne državne vlast Kalifornije, NJ ili federalne vlasti SAD.

Prema C.Parkeru i T.Caseu[4]: «Kompjuterski kriminal se odnosi na upotrebu kompjuterskih resursa za neautorizovane ili ilegalne radnje. To su aktivnosti poput: krađa novca putem elekronskog preusmjeravanja fondova, upotreba kompjuterskih resursa za falsificiranje elektronskih podataka, kopiranje ili upotreba programa ili podataka bez autorizacije, ili ulazak u mrežu koji je nedozvoljen za tu osobu.»

Pojavni oblici kompjuterskih prevara

Bez obzira što je još uvijek najveći broj kompjuterskih šteta izazvan slučajnim i nehotičnim radnjama pri rukovanju i korištenju informacijskih sistema, svrsishodne i planirane akcije kompjuterskog kriminaliteta bilježe značajan porast. Tendencija koja posebno zabrinjava je porast

---

[3] Dragan Roller KRIMINALISTIČKA INFORMATIKA I KOMPJUTERSKI KRIMINALITET, Policija i sigurnost, br.6, Zagreb 1994

[4] Charles Parker&Thomas Case MANAGEMENT INFORMATION SYSTEMS, Strategy and action, Second edition

uvezanosti tzv. «kompjuterskih kriminalaca» sa organiziranom mafijom, te činjenica da savremeni kriminalci sve više koriste informatičku tehnologiju.

Pod kompjuterskim zloupotrebama koje se definiraju kao kompjuterski kriminal u ekonomskoj sferi, smatraju se akcije zloupotrebe informacionih sistema s ciljem ostvarenja imovinske koristi. Generalno, kompjuterski kriminalitet se manifestira kroz:

- *Neovlašteno korištenje sredstava komunikacije radi pristupa udaljenim kompjuterskim sistemima;*
- *Neovlašten pristup kompjuterskim sistemima;*
- *Krađa, izmjena, brisanje, i/ili kopiranje podataka;*
- *Softversko piratstvo (kopiranje i korištenje tuđih autorkih programa);*
- *Korištenje resursa kompjuterskog sistema za sosptvene potrebe od strane osoba ovlaštenih da se njima koriste (krađa vremena ili krađa usluga);*
- *Izrada i širenje malicioznih programa s ciljem prouzrokovanja materijalne štete; i*
- *Fizičko onesposobljavanje kompjuterskih sistema ili sistema telekomunikacija (sabotaža) s ciljem prouzrokovanja materijalne štete.*

C.Parker i T.Case navode preciznu definiciju pojavnih oblika kompjuterskog kriminala:

1. *Prevare sa podacima* putem neautorizovane modifikacije podataka pohranjenih u kompjuterskom sistemu (eng. data diddling). (npr. falsificiranje diploma; usmjeravanje isporuke robe na drugu destinaciju; brisanje kazni iz policijskog registra itd.)
2. *Tehnika trojanskog konja* je blok kriminalnog kompjuterskog koda koji omogućava ulazak u sistem jer je nosilac autorizovanog programa koji obavlja neautorizovana djela, kao što je transfer novca sa računa.
3. *Tehnika salame* funkcioniše pod pretpostavkom da ukoliko se izuzmu manje sume novca sa računa koji se ne provjeravaju strožije, i prebace na jedinstven račun, nakon izvjesnog vremena na računu će se skupiti znatnija sredstva. S obzirom da banke ne vrše detaljniju provjeru svakog računa, sa poravnanjem, u koje ulazi i račun na koji se transferira novac, ne može se utvrditi nikakva nepravilnost.
4. *Rutine stražnjih vrata* (eng. trapdoor routines) su rutine koje se koriste pri razvoju programa. One omogućavaju autorima da uđu u različite dijelove sistema da bi vidjeli da li program korektno funkcionira. Mada se zamke trebaju ukloniti prije puštanja programa u upotrebu, dešava se da nisu. Kriminalci koriste ove zamke za ulazak u sistem.

5. *Superzap programi* mogu probiti kontrolni sistem ukoliko postoji greška ili nefunkcioniranje na određenom dijelu sistema. Superzapovi su obično dozvoljeni samo nekolicini uposlenih, i ukoliko ih koristi neautorizovano lice može doći do zloupotreba.
6. *Logička bomba* je tehnika koja prouzrokuje da dijelovi sistema postanu neoperativni ili da pogrešno operiraju nakon izvršenja zadane procedure. Većinom se ovom tehnikom služe sami programeri koji su npr. pod prijetnjom otkaza i uništavaju određene podatke ili stopiraju i modificiraju procese.
7. *Kompjuterski virus* je termin koji se koristi za opis logičke bombe u kojoj komad neautorizovanog koda djeluje kao parazit koji se uvlači u program tokom operacije kopiranja. Kao njihovi biološki primjerci, virusi se reproduciraju i šire, komande reproduciranja su ugrađene u virus kopiranja. Virusi mogu prouzrokovati zanačajne organizacione probleme. Prvi otkriveni slučaj je student informatike R.Morris koji je 1988. godine ubacio virus u mrežu koju koristi preko 6.000 korisnika, blokirajući njihove aplikacije. Ovaj američki student je prva osoba koja je optužena za ovu vrstu kompjuterskog kriminala. Efekti ubacivanja virusa u kompjuterske mreže su ogromni i rezultiraju velikim gubitkom produktivnosti.
8. *Tehnike traženja po smeću* su tehnike putem kojim se pretraživanjem izbrisanih fajlova pronalaze informacije koje se koriste u kriminalne svrhe.
9. *Propuštanje* (eng. Leakage) je tehnika kojima se podaci, programi ili kompjuterski izvori koji su pod šifrom propuste bez autorizacije. Ovom se tehnikom može postići da podaci izađu iz organizacije na vrlo sofisticiran način, koji neće biti otkriven.
10. *Tehnika prisluškivanja* daje mogućnost da se prate transmisije namijenjene drugom korisniku. Mete ovih tehnika su zaštićene ulazne šifre i brojevi računa.
11. *Prisluškivanje putem žice* je tehnika postavljanja specijalnog transmisionog uređaja kojim se mijenja tok podataka. Npr. ukoliko se postave žica ili kabel ilegalno na mrežu može se postići niz ilegalnih djela: špijuniranje, krađa programa, mijenjanje podataka, itd. Posebno pogodni za ovu vrstu prisluškivanja su sateliti.
12. *Softversko piratstvo* se odnosi na neautorizovano kopiranje ili upotrebu programa. Najopasniji oblik je komercijalna nelegalna proizvodnja softverskih programa.
13. *Hakiranje* - Ranije je engleski termin "hacker" korišten za imenovanje komjuterskih eksperata koji rješavaju najsloženije probleme. Danas ovaj termin ima znatno negativnije značenje i obilježava upadanje u komjuterski sistem iz igre ili izazova. Ova vrsta kompjuterskog

kriminala ima najveći publicitet, ali i relativno malo učesće u cjelokupnim aktima kompjuterskog kriminaliteta.

Kompjuterski kriminal i internet

Internet je telekomunikaciona mreža internacionalnog karaktera koja nudi slobodan pristup širokoj publici. Mreža ima vrlo veliku brzinu, i omogućava prevazilaženje fizičkih i vremenskih barijera uz minimalne troškove. Internet je najveća kompjuterska mreža koja je sačinjena od stotina hiljada regionalnih i državnih mreža.

Internet je suštinski promijenio ulogu informacionih sistema u poslovanju i svakodnevnom životu. Niz ekonomista zastupa tezu da se pronalaskom Interneta svijet ekonomije dijeli na dvije ere: prije i poslije Interneta.

Internet nema vlasnika niti menadžmenta. Postoje samo pravila ponašanja, koja određuju način pristupa mreži.

Internet je zasnovan na ideji i projektu razvijenim od strane US Defence Department's Advanced Research Projects Agency–ARPA, kompjuterskoj mreži koja je razvijena 1969. godine s ciljem omogućavanja razmjene podataka i kreiranja elektronske pošte. 80-tih godina ARPANET-u se priključuje NASA, 1986. godine se u mrežu uvezuje National Science Foundation – NSF. Priključenjem američke univerzitetske mreže na ARPANET može se reći da je rođen Internet. 1993. godine nastaje World Wide Web, organizacijska struktura Interneta koja je i danas dominantna. WWW standardizuje mrežu uvodeći komunikacijski protokol HTTP i standardni format dokumenta HTML, koji omogućavaju korisnicima da na jednostavan i brz način pristupe drugim umreženim kompjuterima i ostvare komunikaciju s njima.

Klijent-server tehnologija je ključ Interneta. Ona omogućava ponudu proizvoda i elektronsko poslovanje umreženim preduzećima.

Danas je Internet mreža za koju se procjenjuje da ima više od 30 miliona korisnika u preko 195 zemalja svijeta.

Osnovne alatke Interneta[5] su:

1. *E-mail* je najupotrebljavanija funkcija koja omogućava razmjenu poruka. Popularnost duguje vrlo niskim troškovima (lokalni

---

[5] Kenneth C. Laudon & Jane P. Laudon INFORMATION SYSTEMS AND INTERNET, 4th Edition, The Dryden Press, USA

telefonski razgovor), velikoj brzini razmjene, mogućnosti slanja velikih dokumenata i grafika, mogućnosti pokrivanja istom porukom neograničenog broja korisnika.

2. *LISTSERVs* je alatka koja omogućava javni forum. Svakodnevno se vode rasprave o bilo kojem subjektu, i jednostavnim prijavljivanjem ova alatka omogućava primanje svih diskusija na E-mail korisnika, kao i promptno slanje sopstvenih poruka svim članicama grupe.
3. *Chatting* je alatka neposredne komunikacije koja omogućava živi, interaktivan razgovor putem Interneta.
4. *Telnet* omogućava pristup matičnom kompjuteru bez obzira gdje se korisnik nalazi. Pomoću ove alatke se može pristupiti sopstvenim fajlovima sa bilo kog mjesta, kao i kompjuterima koji su otvoreni za javnost.
5. *File Transfer Protocol, Gophers* i druge alatke koje omogućavaju pristup informacijama. FTP omogućava pristup bilo kom drugom kompjuteru u svijetu koji je na Internetu i koji omogućava FTP pristup. Pomoću ove alatke se može pristupiti informacijama koje nude univerziteti, vlade, preduzeća itd.
6. *World Wide Web* omogućava korisnicima interaktivnu razmjenu informativnih prezentacija, kombiniranjem teksta, zvuka, grafike i videa.

Rast Interneta i ekspanzija elektronskog poslovanja je upravo proporcionalna razvoju kompjuterskog kriminaliteta. Tačan broj napada se ne može odrediti, jer ogroman broj preduzeća (banke, finansijske institucije) ne želi prijaviti zloupotrebe zbog održavanja profesionalnog rejtinga. Međutim, prema određenim izvorima pretpostavlja se da je 98,5% preduzeća bilo žrtva kriminalnog napada.

Ciljevi napada prema D.Dragičeviću su[6]:

1. *Korisničke lozinke* koje omogućavaju pristup sistemu.
2. *Podaci i informacije* koji su pohranjeni u memoriji kompjutera ili su na mreži. Cilj može biti uvid, izmjena ili brisanje podataka.
3. *Datoteke* s brojevima kreditnih kartica i kartica za identifikaciju i pristup sistemu. Omogućavaju ilegalno kupovanje roba ili usluga, te krađu putem transfera novca na željeni račun.
4. *Kompjuterski programi* su cilj napada sa namjerom kopiranja i daljnje neovlaštene distribucije.
5. *Web stranice i News grupe* se napadaju s ciljem promjene sadržaja. Iako ne donose konkretnu imovinsku korist, i izgledaju bezazleno,

---

[6] Dražen Dragičević KOMPJUTORSKI KRIMINALITET I INFORMACIJSKI SUSTAVI, Informator, Zagreb, 1999

ovi napadi mogu ugroziti povjerenje u prezentirane informacije i poslužiti za malicioznu propagandu.

6. *Onemogućavanje korištenja kompjuterskog sistema* se vrši s ciljem blokiranja rada matičnog kompjutera, najčešće slanjem crva ili ogromne količine poruka matičnom sistemu, koji dovodi do toga da on postaje neoperativan za izvjesno vijeme. Može prouzrokovati ogromne finansijske štete preduzeću.
7. *Materijalno-tehnički resursi informacionih sistema* su cilj kod «klasičnih» krađa, kada počinilac ima mogućnost konkretne krađe, posebno prenosivih kompjutera. Mada je ova vrsta kriminalnog napada zastarjela, još uvijek je prisutna.

Napadi i zloupotrebe kompjuterskih umreženih sistema mogu biti slučajni i planirani. Bez obzira o kojoj vrsti napade se radi, najveću poteškoću predstavlja činjenica da napadači vrlo profesionalno uklanjaju tragove. Jedna od osnovnih karakteristika kompjuterskog kriminaliteta je anonimnost.

Sigurnost sistema i sredstva zaštite

Teroristički napad 11.septembra na World Trade Center i Pentagon su dali sasvim drukčije svjetlo na pojam kompjuterske zaštite. Mada su napadi izvedeni probijanjem sistema fizičke zaštite, sveobuhvatna anti-teroristička akcija koja je poduzeta odmah nakon, iznosi u jedan od prvih planova eventualne napade na informacione sisteme i probijanje zaštitnih barijera kompjuterskih sistema.

Odmah nakon događaja 11. septembra FBI je izdao naređenje da se pojača kompjuterska zaštita. Institucije i kompanije su imale za zadatak procijeniti nivo zaštite i potencijalne slabosti sistema, s ciljem što efikasnije reakcije na eventualni teroristički napad. Državna administracija USA inicira po prvi put akciju dvosmjerne razmjene informacija između privatnog i državnog sektora na području zaštite kompjuterskih sistema, procjenjujući da bi eventualni kompjuterski teroristički napad imao za cilj paraliziranje društva i unošenje panike i haosa (od napada na sisteme snabdijevanja strujom, vodom, komunikacije, saobraćaj, do ometanja i paraliziranja ekonomskih tokova Amerike). Mada je težište akcija na području ojačavanja fizičke zaštite sistema od napada, američka administracija je poduzela hitnu akciju i na planu mijenjanja pravne regulative kompjuterskog kriminaliteta. Novi zakon USA potpisan od strane predsjednika Busha, zvani USA Patriot Act, po prvi put definira kompjuterski terorizam kao krivično djelo, te ovlašćuje FBI da po svojoj sopstvenoj procjeni i bez sudskog naloga i dokaza o

kriminalnoj aktivnosti, ima pravo ulaska u bilo koji kompjuterski sistem i instaliranja kontroverznog kompjuterskog programa praćenja. «Ako je ranije FBI bila iza svakog poštanskog sandučeta, danas je ona iza svakog kompjutera»[7] izajvio je predsjednik Centra za Demokraciju i tehnologiju Jerry Berman, smatrajući da ova odluka ugrožava zaštitu privatnosti građana.

11. septembar 2001. godine će svakako promijeniti način sagledavanja kompjuterskih zloupotreba, i sigurno izazvati znatno obuhvatnije izučavanje ove problematike i efikasnije strategije prevencije. Kakve odgovore daje dosadašnja teorija o sigurnosti informacionih sistema i koji su načini zaštite?

Informacioni sistem je izložen opasnosti od niza faktora, koji mogu ugroziti tehničku, programsku i/ili informacijsku bazu sistema. Sigurnost, odnosno propusnost sistema je osnova nastanka kompjuterskog kriminaliteta. Prijetnje sistemu mogu dolaziti od ljudi, stvari i događaja unutar sistema i iz njegove okoline. Njihovo djelovanje se može u nekim slučajevima predvidjeti, i na osnovu toga izgraditi adekvatan sistem zaštite. Međutim, još uvijek nije moguće obezbijediti apsolutnu sigurnost sistema. Već krajem osamdesetih godina zabilježen je značajan porast ulaganja američkih tvrtki u povećenje sigurnosti svojih informacionih sistema.

J.M. Caroll[8] razlikuje fizičku, komunikacijsku i sistemsku sigurnost. Autor navodi i niz zaštitnih mehanizama za svaki nivo sigurnosti, i ističe posebne mjere koje svoju primjenu nalaze u svakodnevnoj upotrebi informacionih sistema, a osiguravaju relativno visok stepen zaštite od zloupotreba: mjere fizičke zaštite; provjera pristupa; pravilno postavljanje i zaštita lozinki; kriptografske metode; kerberos metoda; metoda vatrenih zidova; digitalni potpis; digitalni vremenski biljeg; steganografija; izdvajanje; sigurnosne kopije; zaštita od virusa; nadzor rada i korištenja kompjuterskog i mrežnog sistema.

Prema C.Parkeru i T.Caseu sigurnost se odnosi na za zaštitu hardvera, softvera, podataka, procedura i ljudi - u smislu izmjena, uništavanja ili neautorizovane upotrebe.

---

[7] Christopher Schmitt, Joellen Perry WORLD WIDE WEAPON, USNews and World Report, 5/11/2001, br.131, USA

[8] J.M.Caroll COMPUTER SECURITY, Butterworth-Heinemann, Boston, 1996

Ranije, problem se odnosio samo na centralizirane sisteme, koji su bili meta eventualnih napada, međutim razvoj komunikacijskih mreža povećava problem sigurnosti jer su ljudi naučili kako da uđu u centralizirane sisteme sa različitih lokacija. U nekoliko posljednjih godina razvoj mikrokompjuterski baziranog procesiranja dovodi do distribucije podataka koji imaju vrlo malu ili nikakvu zaštitu. Zatim, međuorganizacijski sistemi rezultiraju upotrebom tuđeg kompjuterskog sistema, nad kojim matična firma nema više kontrolu.

Niz kontrola validacije koje se mogu ugraditi u personalni komjuter danas mogu pružiti relativnu zaštitu privatnosti. Međutim, kada se govori o kompjuterskoj sigurnosti, ona podrazumijeva širu problematiku sigurnosti i zaštite. Najbitnije tačke ovog problema su zaštita od kriminala, prirodnih katastrofa, i opasnosti od pada hardvera i softvera.

Odgovornost za sigurnost se dijeli na dvije oblasti:
- dizajn sigurnosnih procedura (što je zadatak sistemskih analizatora i dizajnera), i
- svakodnevno izvršavanje procedura sigurnosti (što je zadatak službenika koji je odgovoran za održavanje kompjutera u okviru kompanije).

Nemoguće je garantirati potpunu sigurnost sistema. Ipak, moguće je zaštititi preduzeće od gubljenja podataka koje je prouzrokovano problemom nedovoljne sigurnosti.

Organizacije koriste niz metoda za zaštitu od kompjuterskih kriminalnih djela. Postoje dvije osnovne solucije za prevencije: uspostavljanje zaštitnog sistema ili minimiziranje rizika za kriminalne akte od strane zaposlenih.

Izbor metode zaštite sistema ovisi od samog sistema i važnosti podataka pohranjenih u sistemu. Nijedna metoda zaštite ne pruža stoprocentnu sigurnost sistema. Međutim, optimalnom kombinacijom i svakodnevnom primjenom izabranih metoda moguće je smanjiti opasnost od zloupotreba na vrlo visok nivo.

Pri zboru adekvatnih mjera zaštite autor Dražen Dragičević[9] ističe da je najveći broj pogreški rezultat ljudskih slabosti, bez obzira da li su posljedica neznanja, nemara, nedovoljne pažnje ili namjernih radnji. Isti autor navodi i najčešće uzroke greški pri zaštiti informacionih sistema:

---

[9] Dr. Dražen Dragičević KOMPJUTORSKI KRIMINALITET I INFORMACIONI SUSTAVI, Informator, Zagreb, 1999

- Nizak stupanj informacijskog obrazovanja korisnika usluga IS-a;
- Pogrešan izbor lozinki i krivo postavljanje privilegija;
- Greške u vlastitom ili tuđem softveru i protokolima;
- Pogrešne implementacije softvera i protokola;
- Pogrešne konfiguracije kompjuterskog sistema ili kompjuterske mreže;
- Korištenje manjkavih i zastarjelih metoda fizičke zaštite;
- Nedostatak odgovarajućeg nadzora sistema;
- Nekompatibilnost hardvera i softvera;
- Nepostojanje ili neprovođenje sigurnosne politike;
- Nedostatak ulaganja u zaštitu i sigurnost IS-a.

Pravni aspekti zaštite IS-a

Pravna regulativa zaštite informacionih sistema od sve češćih zloupotreba, započinje šezdesetih godina, ubrzo nakon objavljivanja u javnosti prvih slučajeva zloupotreba i njihovih posljedica. Pravna regulativa se prvo javlja u najrazvijenijim zemljama, u kojima je i upotreba, a time i stepen zloupotreba IS-a najviši. Aktivnost na domaćem terenu je praćena i snažnom akcijom na međunarodnom nivou, od strane međunarodnih i regionalnih organizacija i udruženja, čija je zasluga da su akcije pravne zaštite sprovođene istovremeno i u relativnoj mjeri ujednačeno.

Mjere pravne zaštite i regulative se mogu podijeliti na četiri osnovne oblasti:

1. *zaštita baza podataka s podacima građana* (zaštita privatnosti);
2. *zaštita od kompjuterskih zloupotreba na području privređivanja*;
3. *zaštita intelektualnog vlasništva* (topografije poluvodičkih proizvoda – čipova i kompjuterskih programa); i
4. *zaštita drugih prava i interesa* čija je povreda u neposrednoj vezi sa korištenjem informatičke i komunikacione tehnologije, te promjena do kojih je došlo uslijed razvoja Interneta.

S obzirom na predmet ovog rada, fokus je dat na kazneno-pravnu regulaciju kompjuterskog kriminaliteta koji se javlja u sferi privređivanja, i koji je motiviran imovinskom korišću.

Mada većina zemalja ima zakone kojima se sankcionišu krivična dijela počinjena kompjuterskom tehnologijom, vrlo malo ovih slučajeva završi na sudu. Većina kriminala tretiranog na sudu su djela počinjena od strane zaposlenih u kompaniji. Velika većina krivičnih dijela ove vrste se ne prijavljuje, jer bi kompanija imala negativnih posljedica ukoliko bi javnost

saznala da je njen kompjuterski sistem nesiguran. S obzirom da je nemoguće utvrditi stvarni obim kompjuterskog kriminala, vrlo je teško procijeniti koliki su troškovi koje kompanije snose uslijed ove vrste kriminala. Prema istraživanjima u USA, više od polovine kompanija je izjavilo da su imali finansijske gubitke zbog upada u njihov kompjuterski sistem, u visini izmedju 50.000$ i 500.000$. Na vrhu ljestvice su banke i kompanije iz oblasti telekomunikacija.

Prvi val pravne regulatuve se odnosio na zaštitu privatnosti građana. Ali vrlo brzo je postalo jasno da ovaj nivo pravne regulacije nije dovoljan, uslijed sve veće ekspanzije zloupotreba kompjuterskih sistema koji nisu imali za cilj narušavanje privatnih podataka, već ostvarenje imovinske koristi.

Prvi zakoni koji sankcionišu ekonomski kriminal počinjen upotrebom kompjutera su donešeni u SAD 1978. godine, u Italiji 1979., Australiji 1981., Velikoj Britaniji 1984., SAD – na saveznom nivou 1985., u Kanadi i Danskoj 1986., Saveznoj Republici Njemačkoj i Švedskoj 1986., u Austriji, Japanu i Norveškoj 1988., Francuskoj i Grčkoj 1990., Finskoj 1992., Nizozemskoj 1993., Luxemburgu 1994., Švicarskoj 1995., Španiji i Maleziji 1997.

Kazneno-pravno sankcionisanje kompjuterskog kriminaliteta je zbog kompleksnosti materije vjerovatno najlakše prezentirati prema počinjenim kriminalnim djelima. Skupine kriminalnih akata koje su pravno definirane su slijedeće:

1. Neovlašten pristup kompjuterskom sistemu;
2. Kompjuterska špijunaža i prisluškivanje;
3. Kompjutersko krivotvorenje; i
4. Kompjuterska prevara.

Nacionalna zakonodavstva kao sankciju za počinjeni kompjuterski kriminal predviđaju kombinaciju zatvorskih i novčanih kazni, a kao ključno oružje u borbi protiv ove vrste kriminaliteta predviđa se i povrat nelegalno stečene imovinske koristi (navedeno i u Rezoluciji UN-a br. 45/121 iz 1990. godine).

Međunarodna aktivnost na planu pravne regulative kompjuterskog kriminaliteta se manifestira u rezolucijama, konvencijama i aktima UN-a, OECD-a, Vijeća Evrope, EZ, te niza međunarodnih udruženja poput Interpola, Međunarodnog udruženja za kazneno pravo - AIDP itd. Akcije navedenih institucija su vrlo često paralelene sa akcijama na državnom

nivou. Od posebnog su značaja akcije koje imaju za cilj ujednačavanje državnih regulativa sa međunarodnim propisima i standardima.

Organizacija za ekonomsku saradnju i razvoj - OECD je već 1983. godine formirala komisiju za harmonizaciju kazneno-pravnih rješenja u sferi ekonomskog kriminaliteta. Komisija je 1986. godine objavila izvještaj Kompjuterski kriminal: analiza pravne politike (Computer-Related Crime:Analysis of Legal Policy) u kome je prezentirana analiza postojećih pravnih rješenja, te prijedlozi za harmonizaciju nacionalnih zakonodavstava. U materijalu je predložena i lista minimalnih zloupotreba:

- kompjuterska prevara;
- kompjutersko krivotvorenje;
- mijenjanje ili brisanje kompjuterskih programa i/ili podataka;
- zaštita autorskih prava na kompjuterskim programima;
- prisluškivanje komunikacija; i
- na drugi način ometanje rada kompjuterskih ili telekomunikacionih sistema.

Vijeće Evrope osniva posebnu komisiju za kompjuterski kriminal 1985. godine, koja rezultira 1989. godine Preporukom br. R(89)/9 u kome su sadržane smjernice akcija za zemlje članice, i u kojoj je proširena lista akata kompjuterskog kriminala. Proširena lista sadrži pored kriminalnih akata navedenih u listi OECD-a i slijedeće akte:

- oštećivanje kompjuterskih podataka i/ili programa;
- kompjuterska sabotaža;
- neovlašten pristup kompjuterskom sistemu;
- neovlaštena reprodukcija zaštićenog kompjuterskog programa;
- neovlaštena reprodukcija topografije.

Komisija Vijeća Evrope je pored nove minimalne liste, koja je obavezujuća za članice, dala i prijedlog liste kriminalnih akata koja su rezultat prakse i iskustava u pojedinim zemljama članicama, tzv. opcijska lista koja se preporučuje ali nije obavezujuća:

- izmjena kompjuterskih podataka i/ili programa;
- kompjuterska špijunaža;
- neovlašteno korištenje kompjutera; i
- neovlašteno korištenje zaštićenog kompjuterskog programa.

OECD publikuje 1992. godine Preporuku koja se odnosi na minimum sigurnosnih mjera koje treba poduzeti s ciljem zaštite informacionih sistema, te kazneno-pravna rješenja sankcionisanja zloupotreba.

Pored navedenih primjera rješavanja ove problematike u okviru organizacija koje uključuju samo određeni broj zemalja, globalna akcija na svjetskom nivou se vodi pod okriljem UN. 1990. godine na VIII Kongresu UN-a o prevenciji kriminala i tretmanu počinitelja, donesena je Rezolucija br. 45/121 koja poziva članice da intenziviraju napore u prevenciji i sankcionisanje kompjuterskog kriminala i ističe slijedeće:

- Modernizacija nacionalnih kaznenih zakona i postupaka;
- Unapređenje kompjuterske sigurnosti i preventivnih mjera;
- Primjena mjera koja će objasniti javnosti, tijelima pravosuđa i organima gonjenja značaj i težinu akata kompjuterskog kriminala, te značaj prevencije;
- Obrazovne mjere za suce, službenike i službe odgovorne za prevenciju i procesiranje kompjuterskog kriminala;
- Propaganda pravila etike pri korištenju kompjutera; i
- Primjena politike za žrtve kompjuterskog kriminala i oduzimanje ilegalno stečene imovinske koristi, te poticanje žrtvi da prijavljuju takva kriminalna djela.

Abstract

During eighties the world made a step from the era of industry into the era of information and telecommunication technology, and shortly after that globalization changes the world of economical, political, legal and spiritual life. The progress of information society, is being characterized by the development of computers and their networks , fast and timely exchange of information and development of electronic business exchange is being followed by transformation of classical models of criminal. As others segments of society, criminal is being adopted to the new age. Classical, physical thefts are in the past now. Instead of them the subject of attack or the means of attack becomes a computer. Already in 1981. the Council of Europe brings out the fact that a computer criminal on the basis of illegally achieved interest came on the first place of criminal acts, together with narcotics and arms trade.

Computer criminal means the use of computer resources for non authorised or illegal works. It could be generally shared on two groups of criminal acts: acts that break present ethical norms and offend privacy and dignity of man and acts committed with the aim of achieving material interest. Even though the article is dedicated to the computer economical criminal, recant events of terrorist attacks in the USA have surely brought into light

possibility of using computers in terrorist actions, the notion of computer criminal is being viewed in different perspective, and especially strengthening of physical protection of system and assessments of eventual targets of attacks and ways and possibilities of implementations. For the purposes of prompt action the accent now is on the intensive methods of protection from entries into information system, but in the USA we have a process of strengthening of power of state security agencies, through changes in legal procedure. Computer terrorism is being defined as a criminal act and the authority of FBI is being expanded to freely control any kind of computer system, without previous warrant or prove, which was previously necessary condition. Basic characteristic of this criminal, regardless which group of criminal acts is in question, is the difficulty to find and sanction perpetrators, because of :
-Anonymity of perpetrators – misuse takes place in virtual world and a huge part of perpetrators successfully cleanses traces; and
-Lack of registering of this kind of crime-firms avoid to report damages since that information could jeopardize firm reputation and cause more damage. Due to expansion of computer criminal and material interest it brings, emphasis of this issue today is given to the increase of security system, protection of system and the establishment of legal-sanctioning praxis, through two basic direction of prevention from the computer crime: measures of physical protection and development of relevant legal regulations.

IX BIBLIOGRAFIJA

1. Kenneth C. Laudon & Jane P. Laudon MANAGEMENT INFORMATION SYSTEMS – Oraganization and Technology, 4th Edition, Prentice Hall, NJ, USA
2. Charles Parker & Thomas Case MANAGEMENT INFORMATION SYSTEM Strategy and action, Second edition
3. Kenneth C. Laudon & Jane P. Laudon INFORMATION SYSTEMS AND INTERNET, 4th Edition, The Dryden Press, USA
4. United Nation Manual on the prevention and control of computer-related crime
5. CD ROM Information USA, Office of International Information Programs, October 1999

6. Dražen Dragičević KOMPJUTORSKI KRIMINALITET I INFORMACIJSKI SUSTAVI, Informator, Zagreb, 1999
7. Velimir Srića i saradnici MENADŽERSKA INFORMATIKA, Mepconsult, Zagreb 1999
8. David Mann & Mike Sutton KRIMINALITET NA INTERNETU, Izbor iz članaka stranih časopisa, br.4, Zagreb 1999
9. Dragan Roller KRIMINALISTIČKA INFORMATIKA I KOMPJUTERSKI KRIMINALITET, Policija i sigurnost, br.6, Zagreb 1994
10. Slavko Šimundić ISTRAŽIVANJE I SUZBIJANJE RAČUNALNOG KRIMINALITETA U HRVATSKOJ I SVIJETU, Zbornik radova pravnog fakulteta u Splitu, br.3-4, Split 1999
11. Slavko Šimundić i Miroslav Baća METODOLOGIJA ISTRAŽIVANJA RAČUNALNOG KRIMINALITETA, Zbornik radova pravnog fakulteta u Splitu, br.1-2, Split 1999
12. Ira Sager, John Carey, Jim Kerstetter PREPARING FOR CYBER ASSAULT, Business Week, 22/10/2001, br. 3754, USA
13. Eileen Colokin, Alorie Gilbert, George Hulme, Marianne McGee, John Randleman IT SECURITY AND LAW, Information Week, 26/11/2001, br. 865, USA
14. Christopher Schmitt, Joellen Perry WORLD WIDE WEAPON, USNews and World Report, 5/11/2001, br.131, USA
15. Dan Verton SECURITY EXPERTS: Users are the weakest link, Computerworld, 26/11/2001, br. 48, Volume 35, USA
16. George F. Will NOW, WEAPONS OF MASS DISRUPTION, Newsweek, 29/10/2001, br. 18, Volume 138, USA