Kriminalističke teme
Časopis za kriminalistiku, kriminologiju i sigurnosne studije
Godište XV, Broj 3-4, 2015. str. 53-70
ISSN 1512-5505

GENEZA RAČUNALNOG KRIMINALITETA

Stručni članak

GENESIS OF COMPUTER CRIMINALITY

Professional paper

Siniša FRANJIĆ

Sažetak

Inspiracija za rad i problem(i) koji se radom oslovljava(ju): Računalni kriminalitet kao niz društveno neprihvatljivih ponašanja

Ciljevi rada (naučni i/ili društveni): Djelotvorno suzbijanje**.** Potaknuti svijest o štetnosti.

Metodologija/Dizajn: Pregled postojeće literature. Pregled internetskih izvora.

Ograničenja istraživanja/rada: Ne postoje.

Rezultati/Nalazi: Pojava velikog broja kaznenih djela iz područja računalnog kriminala.

Generalni zaključak: Osamdesetih godina i devedesetih godina XX. stoljeća došlo je do naglog razvoja suvremenih računalnih tehnologija. Pojava interneta je donijela niz korisnih informacija na svim životnim područjima.

Opravdanost istraživanja/rada: Suzbijanje računalnog kriminaliteta kao velike negativne društvene pojave

Ključne riječi

Internet, Konvencija o kibernetičkom kriminalu, Zakon o izmjenanama i dopunama Kaznenog zakona, računalni kriminalitet, Kazneno djelo

Abstract

Reason(s) for writing and research problem(s): Computer crime as a number of socially unacceptable behavior

Aims of the paper (scientific and/or social): Effective suppression. To encourage awareness of the harmfulness.

Methodology/Design: Overview of existing literature. Overview of Internet sources.

Research/paper limitations: Do not exist.

Results/Findings: The emergence of a large number of criminal acts in the field of computer crime.

General conclusion: In the eightieth and the Ninetieth years of XX. century was became to abrupt development of modern computer technologies. Then was became to appearrance of internet which be bring many advantageous information to the peoples in all life areas.

Research/paper validity: Combating computer crime as a major negative social phenomena.

Keywords:

Internet, Convention on Cybercrime, Law of exchanges and amendment of Criminal law, Computer Criminality, Criminal act

Uvodna razmatranja

Ljudski talent, inteligencija i obrazovanje dolaze do izražaja kroz komunikaciju s drugim ljudima (Šimundić i Franjić, 2009, str. 17). Ta je komunikacija počela napredovati od sredine XV. stoljeća uporabom raznovrsnih i sve savršenijih tehničkih pomagala koji se smatraju temeljem svjetske informacijske revolucije. Za razliku od informacijske, informatička revolucija obuhvaća ona tehnološka rješenja koja se ostvaruju korištenjem modernih informatičkih i komunikacijskih postrojenja, strojeva, različitih uređaja i mreža kojima se unose, obrađuju i pohranjuju podaci, prenose slike, glas, zvuk i signali u digitalnom obliku.

Današnje moderno doba suvremenih digitalnih i računalnih tehnologija svakim danom sve više napreduje i, na zadovoljstvo mnogobrojnih korisnika diljem svijeta, ta moderna tehnologija svakim danom postaje sve dostupnija i jednostavnija za uporabu. To bi značilo da razdoblje od devedesetih godina XX. stoljeća, kada je došlo do nagle ekspanzije tih modernih tehnologija, do danas slobodno možemo nazvati razdobljem znanstveno-tehnološke revolucije koja će se i u budućnosti nastaviti razvijati. Središnje mjesto u tom procesu ima čip (Sićušni komadić kristala poluvodiča, ponajviše silicija, na koji se utiskuje sklop ili niz sklopova koji čine elektronički integrirani krug. Na njegovoj površini od nekoliko milimetara utiskuju se tisuće i tisuće tranzistora, kondenzatora i niz drugih elektroničkih elemenata), odnosno mikroprocesor (Skup nekoliko povezanih čipova koji djeluju kao samostalno računalo). Svjetska znanstvena javnost u današnje vrijeme velike nade ulaže u pronalaženje biočipa koji bi imao djelovanje poput ljudskog mozga. Biočip bi postao izvrsna podloga za razvoj umjetne inteligencije, robotizacije, digitalne komunikacije itd.

Današnja tehnološka razina omogućuje povezivanje sustava računala u mreže, ali i njihovo globalno povezivanje u jedinstveni komunikacijsko-informacijski sustav – internet. Internet je vrlo brzo postao plodno tlo za zlouporabu, odnosno plodno tlo za razvoj i širenje računalnog kriminaliteta. Tehnološki razvoj interneta omogućio je mnoštvo zlouporaba zbog nepostojeće ili nedostatne pravne regulative iz područja računalnog kriminaliteta.

Uz pojam interneta usko je vezan pojam informacijski sustav. Informacijski sustav je skup jasno definiranih pravila, praktičnog iskustva i metoda rada kod kojih ljudi ili grupe ljudi trebaju raditi na unošenju datih podataka u računalo, koji će obraditi informaciju tako da pruži sve specifikacije, što će omogućiti pojedincima da se odluče u konkretnim situacijama.

Svakodnevnim povećanjem broja nazočnih na internetu, svijet sve više postaje globalno informacijsko selo. Ukidaju se prostorna, regionalna, etnička i druga ograničenja i tako je svijet postao globalna zajednica, a internet – informacijska superprometnica! Internet je tako postao tehnološki, socijalni, ekonomski, medijski, politički pa, između ostalih, i pravni fenomen. Budući da na današnjem stupnju razvoja trenutačno nije moguće postići apsolutnu sigurnost informacijskog sustava, potrebno je pružiti apsolutnu i djelotvornu zaštitu ako dođe do zlouporabe. To je moguće postići jedino koordinacijom država koje čine globalno selo.

Problematika računalnog kriminaliteta jest problematika čija je pojavnost sve učestalija u modernom društvu. Računalni kriminalitet nastaje i razvija se na isti način u svim dijelovima svijeta. O njemu se javno piše i govori, a rezultati njegova sprječavanja praktički su zanemarivi. Danas to više nije tako jer je sve više država koje u vlastitim nacionalnim zakonodavstvima imaju opisana kaznena djela koja proizlaze iz uporabe modernih informacijsko-računalnih tehnologija. Republika Hrvatska je kroz Zakon o izmjenama i dopunama Kaznenog zakona iz 2004. [1] propisala niz kaznenih djela opisanih u Konvenciji o kibernetičkom kriminalu (Convention on Cybercrime).

Zaštita privatnosti

Uporaba moderne informacijske tehnologije omogućava prikupljanje i obradu velike količine različitih podataka iz najrazličitijih područja ljudskih djelatnosti (Šimundić i Franjić, 2009, str. 19). Pojava interneta u velikoj je mjeri otvorila mogućnost pristupa takvim informacijama. Golema količina podataka, a neke od baza podataka sadržavale su i najintimnije osobne podatke, postala je dostupna diljem svijeta, a o zaštiti od zlouporaba nije se vodilo računa. Iz ovoga proizlazi da se pod pitanjem zaštite podataka uglavnom misli na zaštitu privatnosti. Budući da je ovdje riječ o temeljnom pravu čovjeka i građanina na slobodno raspolaganje i odlučivanje o svojim osobnim podacima koje se nalazi u Ustavu [2], početkom sedamdesetih godina XX. stoljeća započeo je rad na pravnom reguliranju zaštite podataka pohranjenih u različitim informacijskim sustavima. Osnovan je tzv. Youngerov odbor koji je proučavao pitanja privatnosti i pitanja njezine zaštite. Ustanovio je sljedeća opća načela za rad s takvim bazama podataka:

- svaki podatak može se koristiti samo za posebnu namjenu i ne može se bez odgovarajuće dozvole koristiti za druge svrhe
- pristup treba biti omogućen samo ovlaštenim osobama koje ih koriste za svrhu za koju su prvobitno prikupljeni
- količina podataka mora odgovarati namjeni
- u sustavima koji obrađuju podatke u statističke svrhe, rad mora biti organiziran tako da su podaci za identifikaciju odvojeni od ostalih
- uspostaviti načine informiranja da bi svaka osoba čiji se podaci nalaze u sustavu mogla saznati informacije koje se na nju odnose
- treba se unaprijed odrediti stupanj sigurnosti sustava, kao i mjere zaštite od zlouporabe ili pogrešne uporabe
- uspostaviti sustav tehničke kontrole koji će olakšati otkrivanje kršenja sigurnosti
- potrebno je odrediti i vremensko razdoblje nakon kojega se podaci više neće moći čuvati

[1] Zakon o izmjenama i dopunama Kaznenog zakona Republike Hrvatske, *Narodne novine, Službeni list RH*, 105/2004.

[2] Ustav Republike Hrvatske, *Narodne novine, Službeni list RH*, 56/90.; 135/97.; 8/98.; 113/2000.; 124/2000.; 28/2001.; 41/2001.; 55/2001.; 76/2010.; 85/2010.: 05/2014.

- podaci moraju biti točni, potrebno je utvrditi načine za ispravljanje netočnosti kao i otkrivanje zastarjelih podataka
- voditi posebno računa o kodiranju vrijednosnih sudova kako ne bi došlo do njihove izmjene
- za radnike izraditi poseban kodeks profesionalne etike

Nakon što su ustanovljena ova načela, sastavljen je niz međunarodnih studija, a kao rezultat tih studija, javljaju se zakoni o zaštiti podataka. Neke su zemlje išle tako daleko pa su mijenjale vlastite Ustave u svrhu zaštite podataka. Tim je zakonima osigurana otvorenost sustava i određenost njihove opće namjene, ali i mogućnost svakog pojednica da utvrdi nalaze li se u informacijskim sustavima podaci o njemu te pravo pojedinca na kontrolu takvih podataka.

Zaštita intelektualnog vlasništva

Zaštita intelektualnog vlasništva predstavlja veliki problem koji se javlja tijekom osamdesetih godina XX. stoljeća. Zaštita intelektualnog vlasništva usmjerena je, prije svega, na programe i topologiju čipova. Zaštita intelektualnog vlasništa ima za cilj stati na kraj softverskom piratstvu jer upravo zbog piratstva država, zajedno s autorima softwarea, gubi znatne prihode koje bi ostvarila legalnom prodajom.

U praksi se primjenjuju neka postojeća pravna rješenja budući da se piratstvo ne može podvesti pod krađu zbog toga što su programi nematerijalni i ne mogu se podvesti pod pojam stvari bez obzira na medij (Šimundić i Franjić, 2009, str. 21). Pravna zaštita u tom smislu može se ostvariti uz pomoć nekoga od prava intelektualnog vlasništva, a to su najčešće autorsko pravo i pravo industrijskog vlasništva. Praksa je pokazala da je najpogodnja vrsta zaštite ona koja proizlazi iz autorskog prava zbog toga što autorsko pravo ima međunarodni karakter i zaštitu kroz neke konvencije.

Zaštita intelektualnog vlasništva može se ostvariti i kroz patentnopravnu zaštitu, ugovornu zaštitu i zaštitu poslovne tajne. Patentnopravna zaštita pokazala se manjkavom zbog skupoće, dugog trajanja i same prirode. Cilj joj je da štiti izum koji predstavlja neko novo tehničko postignuće što ne mora biti slučaj s programima. Manjkavost ugovorne zaštite i zaštite poslovne tajne očituje se u tome što nema apsolutni karakter, jer ne djeluje prema trećim osobama.

Internet

Internet je globalni informacijsko-komunikacijski sustav koji povezuje i spaja mreže pojedinih zemalja i organizacija, te tako omogućava korisnicima računala diljem svijeta da putem svojih lokalnih mreža i telefonskih veza komuniciraju, razmjenjuju informacije i koriste druge usluge (Dragičević, 2004, str. 28). Razvoj interneta počinje 1969. godine kada je pokrenut projekt Arpanet s ciljem stvaranja pouzdane mreže koja će moći funkcionirati i kada jedan njezin dio nije u funkciji zbog napada ili tehničke neispravnosti (Šimundić i Franjić, 2009, str. 21). U tu svrhu započet je razvoj mrežnog protokola koji bi omogućio da se komunikacija preko mreže automatski preusmjerava mimoilazeći

mjesto gdje je problem nastao i tako spriječi dobivanje informacija bez obzira na novonastale probleme. Internet je omogućio razmjenu i dostupnost informacija lakšom nego ikada prije, a vremenom je profilirao pet osnovnih funkcija :

- prikupljanje, pohranjivanje i obradu informacija, jednostavniju i bržu razmjenu podataka i programa
- veliki prostor oglašavanja
- rasprostranjen e-mail
- interaktivna neposredna komunikacija između korisnika, telekonferencija i internet telefonija
- obavljanje najrazličitijih poslovnih aktivnosti

Prvotna namjena interneta nije bila komercijalna niti je bila usmjerena prema onome što danas predstavlja. Nije se usmjeravala dovoljna pozornost prema sigurnosti, pa su protokoli bili, uglavnom, usmjereni prema djelotvornosti, fleksibilnosti i otvorenosti sustava.

Razvoj interneta prati rast broja i učestalosti napada. Točan, ali i približan broj napada ne može se utvrditi. Kada su u pitanju veliki informacijski sustavi, tendencija je prešućivanje napada zbog tajnosti podataka ili straha od gubitka korisnika. Današnje procjene kažu da se štete nastale računalnim kriminalitetom nalaze odmah iza šteta nastalih trgovinom drogom i trgovinom oružjem. Razvojem interneta raste i broj potencijalnih počinitelja. Sve veće tehničko znanje i sve sofisticiranija oprema omogućuju stvaranje naprednih softverskih alata namijenjenih lakšem i bržem napadanju. Najčešći razlog tomu jest dostpunost izvornih kodova programa koji počiniteljima omogućavaju uvid u samu strukturu programa i njegove slabosti koje se mogu iskoristiti. Do napada dolazi usljed:

- neovlaštenog pristupa
- neovlaštenog mijenjanja podataka
- neovlaštenog brisanja podataka
- presnimavanja malicioznih programa (virusa, crva itd.)
- uporabe tuđeg računala za pristup drugom sustavu
- stvaranja uvjeta za nastanak štete na sustavu
- krađe, oštećenja, uništenja hardverske osnovice, medija itd.

Sve ovo bi bilo besmisleno kada se počinitelj ne bi mogao povući, ne ostavljajući nikakve dokaze o svome neovlaštenom pristupu. Anonimnost je jedan od temelja računalnog kriminaliteta i osnovni razlog zašto ga je teško sprječavati i suzbijati. Napadači će nastojati ukloniti podatke o svom pristupu, a u kojoj će im mjeri to biti moguće, ovisit će o njihovim vlastitim sposobnostima, ali i sposobnostima sustava koji je bio meta njihova napada.

Računalni kriminalitet

Uz razvoj računalne tehnologije, razvija se, na žalost, i njezina zlouporaba, odnosno zlouporaba podataka i informacija obrađenih suvremenim informacijskim tehnologijama (Šimundić i Franjić, 2009, str. 29). Zlouporaba računala usko je povezana s računalnim kriminalitetom. Masovnost ove pojave poprimila je goleme razmjere, a izravne štete su nesagledive. Masovna uporaba računala u najrazličitijim prilikama, uz sve veće korištenje telekomunikacijske opreme od sve većeg broja korisnika, omogućuje da sve veći broj nestručnih i neovlaštenih osoba (hackera) uzrokuje nesagledive posljedice. Računalni kriminalitet je u stalnom porastu, a zakonodavna regulativa prema računalnim prijestupnicima je vrlo blaga. O tome govore činjenice koje kažu da se otkriva samo 1 % računalnog kriminaliteta; 14 % otkrivenih slučajeva bude prijavljeno nadležnim vlastima; od 2000 slučajeva samo jedan bude izveden pred sud. Zaštita podataka i informacija od neovlaštenog korištenja nije izmišljena samo zbog osiguranja tajnosti podataka, već da se sustav suvremene obrade podataka ne pretvori u svoju suprotnost. Sustav zaštite stalno valja preispitivati i dograđivati, jer se neprestano pojavljuju nove metode zaštite, a razvoj informacijske tehnologije omogućuje da se stariji sustavi zaštite učine ranjivim, nedostatnim, pa čak i bezvrijednim.

Ovdje posebno treba istaknuti da se ulažu golemi napori na suzbijanju svih oblika računalnog kriminaliteta kako u Republici Hrvatskoj tako i u svijetu. Europska unija, odnosno Vijeće Europe, 2001. godine je usvojilo Konvenciju o kibernetičkom kriminalu koju su potpisale države članice, ali, što je posebno zanimljivo, i države nečlanice Vijeća Europe. Konvencija o kibernetičkom kriminalu (zaključno s 20. prosinca 2014. godine potpisale su je sljedeće države članice Vijeća Europe: Albanija, Andora, Armenija, Austrija, Azerbejdžan, Belgija, Bosna i Hercegovina, Bugarska, Hrvatska, Cipar, Češka Republika, Danska, Estonija, Finska, Francuska, Njemačka, Grčka, Gruzija, Mađarska, Island, Irska, Italija, Latvija, Lihtenštajn, Litva, Luksemburg, Malta, Moldavija, Monako, Crna Gora, Nizozemska, Norveška, Poljska, Portugal, Rumunjska, Srbija, Slovačka, Slovenija, Španjolska, Švedska, Švicarska, Makedonija, Ukrajina, Turska, Velika Britanija i sljedeće države nečlanice Vijeća Europe: Kanada, Japan, Južnoafrička Republika i Sjedinjene Američke Države. Od država nečlanica Vijeća Europe, Konvenciju su ratificirale Australija, Dominikanska Republika, Japan, Mauricijus, Panama i Sjedinjene Američke Države), usvojena je na konferenciji Vijeća Europe u Budimpešti. Republika Hrvatska potpisala ju je 23. studenog 2001., a ratificirala 03. srpnja 2002. Konvencija o kibernetičkom kriminalu objavljena je u Narodnim novinama (NN – MU 9/2002.) u engleskom izvorniku i u prijevodu na hrvatski jezik. U njezinoj Preambuli, između ostalog, stoji da Konvencija o kibernetičkom kriminalu ima za cilj vođenje zajedničke kaznene politike usmjerene na zaštitu društva od kibernetičkog kriminala. Dodatni protokol Konvencije o kibernetičkom kriminalu (Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenofobic nature commited through computer systems) odnosi se na progon čina rasne i ksenofobične prirode počinjenih računalnim sustavima. Dodatni protokol Konvencije o kibernetičkom kriminalu (zaključno s 20. prosinca 2014., potpisale su ga sljedeće države članice Vijeća Europe: Albanija, Andora, Armenija, Austrija, Belgija, Bosna i Hercegovina, Hrvatska, Cipar, Češka Republika, Danska, Estonija, Finska, Francuska, Njemačka, Grčka, Island, Italija, Latvija, Lihtenštajn, Litva, Luksemburg, Malta, Moldavija, Crna Gora, Nizozemska, Norveška, Poljska, Portugal, Rumun-

jska, Srbija, Slovenija, Španjolska, Švedska, Švicarska, Makedonija, Ukrajina te Kanada i Južnoafrička Republika kao države nečlanice Vijeća Europe), usvojen je na konferenciji Vijeća Europe u Strasbourgu 28. siječnja 2003. Republika Hrvatska potpisala je Dodatni protokol Konvencije 26. ožujka 2003. Odredbe Konvencije o kibernetičkom kriminalu i odredbe njezina Dodatnog protokola ugrađene su u Kazneni zakon Republike Hrvatske [3] koji je bio u primjeni do 31. prosinca 2012., ali i u Kazneni zakon Republike Hrvatske [4] koji je u primjeni od 01. siječnja 2013.

Pojam računalnog kriminaliteta

Računalni kriminalitet je svako kazneno djelo počinjeno posredstvom posebnog znanja ili stručnog korištenja računalne tehnologije (Šimundić i Franjić, 2009, str. 31). Praksa kaže da je kaznenih djela počinjenih posredstvom posebnog znanja sve manje, a da ih je sve više počinjenih izravnom ili neizravnom uporabom računalne tehnologije. Stručnost se ne smatra važnim elementom zbog jednostavnosti i dostupnosti računalne tehnologije.

Kriminalitet je ukupnost kriminalnog ponašanja na određenom prostoru kroz određeno vrijeme. Sukladno tome, računalni kriminalitet bi se mogao definirati kao ukupnost kriminalnih djela na nekom području izvršenih kroz određeno vrijeme na računalnom sustavu ili uz njegovu pomoć.

Računalni kriminalitet se može definirati i kao ukupnost kaznenih djela, na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na uporabu, cjelovitost i dostupnost hardverske, softverske i podatkovne osnovice sustava ili tajnost podataka (Dragičević, 2004, str. 113).

Nastanak računalnog kriminaliteta

Nastanak računalnog kriminaliteta treba tražiti u telekomunikacijskom kriminalitetu iz šezdesetih godina XX. stoljeća kada se pojavljuju tzv. phreakeri. Phreakeri su osobe koje rabe različite metode kako bi besplatno koristile telefonske usluge (Šimundić i Franjić, 2009, str. 32). Otkrivši načine zlouporabe tadašnje telekomunikacijske tehnologije, nije im trebalo dugo da tako stečeno znanje primjene na područje informacijske tehnologije. Mnogi phreakeri tako postaju hackeri što dovodi i do brisanja granice između telekomunikacijskog i računalnog kriminaliteta.

Razvoj računalnog kriminaliteta

Prvi računalni sustavi koristili su se u znanstvene i vojne svrhe, a tek potom za poslovanje gospodarskih subjekata (Šimundić i Franjić, 2009, str. 33). Budući da su ti prvi sustavi bili zatvoreni, prve su zlouporabe bile ograničene na ovlaštene korisnike

3 Kazneni zakon, Narodne novine, Službeni list RH, 110/97.; 27.98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.; 143/2012.

4 Kazneni zakon, Narodne novine, Službeni list RH, 125/2011.; 144/2012.

koji su manipulirali financijskim podacima sa svrhom stjecanja protupravne imovinske koristi. Razvojem modema sedamdesetih, stvaraju se preduvjeti za pristup udaljenim računalima, a osamdesetih godina XX. stoljeća sve se više širi softversko piratstvo što proizvođačima nanosi velike gubitke. Razvojem interneta računalni kriminalitet dobiva globalne razmjere. Na žalost, u novije vrijeme su i terorističke organizacije počele svoje ideološke programe prezentirati putem interneta svojim simpatizerima. Internet je tako sa svojom prirodom masovnog medija postao prostor u kojemu se odvijaju javne, ali i konspirativne djelatnosti legalnih i nelegalnih skupina ljudi.

Glavne značajke računalnog kriminaliteta

Glavne značajke računalnog kriminaliteta čine društvena opasnost i štetnost te tamna brojka (Šimundić i Franjić, 2009, str. 43).

Društvena opasnost i štetnost računalnog kriminaliteta

Među pravnim teoretičarima nema jedinstvenog stajališta u svezi obujma šteta, pa se sumnja u vjerodostojnost i opravdanost mnogih provedenih istraživanja. Problem čine neodređenost pojma računalnog kriminaliteta i nemogućnost uspostavljanja jedinstvene metodologije pri prikupljanju i obradi podataka, ali i činjenice o malome broju otkrivenih i prijavljenih djela.

Tamna brojka računalnog kriminaliteta

Problem tamne brojke jedan je od gorućih problema s kojima se susreću svi koji se bave ovom problematikom zbog toga što ista onemogućava potpuni uvid u sam problem. Odnosi se na pojam koji se u kriminologiji odnosi na broj realiziranih kažnjivih ponašanja za koja se ne zna zato što nisu otkrivena, a ne zato što počinitelj nije poznat. Osnovni uzroci tome jesu:

- globalni karakter djela koji ne poznaje granice
- teškoće u otkrivanju, gonjenju i dokazivanju (počinitelj ne mora biti na mjestu zločina, ne mora čak ništa ni raditi za vrijeme činjenja kaznenog djela)
- kaznena djela iz područja računalnog kriminaliteta mogu se prikriti na razne načine, a i dokazi se mogu ukloniti
- podaci se nalaze u digitalnom obliku što znači da su podložni mijenjanju i brisanju bez ostavljanja tragova o počinitelju i njegovoj aktivnosti
- počinitelj često raspolaže stručnim znanjem koje omogućava zaobilaženje sigurnosnih mjera
- žrtve ne prijavljuju napade zbog straha od gubitka povjerenja korisnika
- metode i sredstva napada teško je uočiti čak i profesionalcima
- objektivne i subjektivne slabosti (slabosti programa, protokola, sustava, nepažnja i neobrazovanost korisnika itd.)

Sve je popraćeno nezainteresiranošću te neodgovarajućom i nedostatnom reakcijom društva, što je dovelo do nedostatne pravne zaštite na tom području.

Fenomenologija računalnog kriminaliteta

Na osnovi izvješća OECD-a pod nazivom *„Computer-Related Crime: Analysis of Legal Policy"* iz 1986. godine, sačinjen je prijedlog koji sadrži minimalnu listu zlouporaba koje bi članice trebale uzeti u obzir prigodom reforme kaznenog zakonodavstva s ciljem suzbijanja i sankcioniranja računalnog kriminaliteta (Šimundić i Franjić, 2009, str. 44). Lista obuhvaća:

- unos, izmjenu, brisanje/onemogućavanje uporabe podataka/programa svjesno napravljenih s ciljem da učine ilegalni transfer sredstava ili nekih drugih vrijednosti
- unos, uzmjenu, brisanje/onemogućavanje uporabe podataka/programa svjesno napravljenih s namjerom da izvrše krivotvorenje
- unos, izmjenu, brisanje/onemogućavanje uporabe podataka/programa ili drugo ometanje rada s ciljem da onemogući funkcioniranje računalnog, odnosno telekomunikacijskog sustava
- povrede prava vlasnika zaštićenog programa
- pristup/onemogućavanje pristupa računalnom/telekomunikacijskom sustavu svjesno napravljenom i bez odobrenja ovlaštenika, kršenjem sigurnosnih mjera ili nekom drugom nepoštenom i štetnom radnjom

Po uzoru na OECD, Vijeće Europe je 1989. godine usvojilo Preporuku 89/9 kojom se članicama preporuča da prilikom reforme zakonodavstva uzmu u obzir minimalnu listu djela koja treba sankcionirati. Za ovu je listu postignuta suglasnost. Lista djela obuhvaća:

- Računalne prijevare
- Računalno krivotvorenje
- Oštećenje podataka/programa
- Računalne sabotaže
- Neovlašteni pristup
- Neovlašteno prisluškivanje
- Neovlaštenu reprodukciju zaštićenih programa
- Neovlaštenu reprodukciju topologije poluvodičkih proizvoda

Uz minimalnu, postoji i opcijska lista djela oko koje nije postignuta suglasnost, ali koje se mogu usvojiti prema željama članica. Tu listu čine:

- Izmjena podataka/programa
- Računalna špijunaža
- Neovlaštena uporaba računala
- Neovlaštena uporaba zaštićenog programa

U konačnici, to bi značilo da su se danas isprofilirale tri skupine računalnih zlouporaba i to:

- **Zlouporabe na računalu** – gdje sustav, odnosno njegovi resursi predstavljaju objekt zlouporabe

- **Zlouporabe pomoću računala** – računalo je samo pomoćno sredstvo za neku zlouporabu
- **Zlouporabe počinjene računalom** – realiziraju se na samom računalu

Metode manipuliranja računalima

Računala se mogu pojaviti kao objekt napada ili kao sredstvo napada (Šimundić, 2007, 398 – 400). Najčešće vrste napada su:

Neovlašteni pristup računalnom sustavu (hacking)

Upad u računalni sustav ne mora nužno sadržavati elemente kaznnog djela. Naprimjer, upad u njega se može dogoditi slučajno i iz čiste znatiželje. Teško je prihvatiti da bi netko povjerovao provalniku da je cilj njegova ulaza u tuđi stan samo razgledavanje.

Zaraza sustava virusima

Zaraza virusima predstavlja veliki problem današnjice. Od nje strahuju mnogi koji imaju otvorene sustave. Virusima obično zovemo manje programe koji imaju zadaću izvršiti određenu manipulaciju na računalnom sustavu. U početku su ih stvarali dokoni programeri. No, nisu ih stvarali samo dokoni programeri. Virusi se najčešće šire kada se koristi neautorizirani (piratski) software, ali i u drugim situacijama u kojima se koriste magnetni mediji (najčešće diskete) koji su bili u doticaju s drugim kompatibilnim sustavima ili su putem telekomunikacijskih veza došli u doticaj s drugim sustavima.

Manipuliranje podacima

Manipuliranje podacima u računalnom sustavu moguće je prilikom prikupljanja i unosa podataka u sustav, a moguće je i kasnije. Cilj takve manipulacije obično je stjecanje protupravne imovinske koristi. Naprimjer, povećanjem (ispravkom) stanja bankovnog računa, neovlaštenim ažuriranjem dugovanja, dobivanjem krivotvorenih dokumenata kojima se ostvaruje neko pravo itd.

Trojanski konj

Umetanje seta programskih instrukcija pomoću drugih programa metodom tzv. Trojanskog konja, predstavlja oblik manipulacije računala kod kojeg se nedozvoljeni, odnosno prikriveni dio instrukcija umeće u neki od programa koji se izvode na sustavu. Neki virusi se šire istom metodom.

Nedozvoljena uporaba programskih alata

Prigodom kreiranja sustava sigurnosti treba biti pažljiv jer je moguće da se uz pomoć tzv. pomoćnih alata, odnosno univerzalnih programskih alata izvrše preinake na inače zaštićenim podacima, odnosno datotekama. Ako se, naprimjer, na IBM osobnom računalu drži kompletna verzija DOS ili OS/s operativnog sustava, nepozvana osoba svašta može napraviti na tom sustavu.

Unošenje logičke (programske) bombe

Poput Trojanskog konja, u sustav se može unijeti program koji se aktivira tek kad se ispune određeni uvjeti. Takav program uništava, odnosno briše sve datoteke u sustavu kad se pojavi ime programera na otkaznoj listi.

Sjeckanje ili Tehnika salame

Program koji obavlja obradu može se izraditi tako da, naprimjer, sve iznose zaokružuje na niže, a da razliku stavlja na poseban račun ili da se sa svakog računa skine neznatan iznos, za koji se pretpostavlja da se komintenti banke ili ustanove neće buniti, i upisuje se na poseban račun itd.

Strvinarenje (scavengening)

Strvinarenje je oblik neovlaštenog prikupljanja podataka zaostalih na računalu ili nakon računalne obrade. Strvinarenje kao pojam nastao je kada su se informacije o sustavu skupljale iz odbačenih materijala po kantama za smeće.

Prisluškivanje sustava

Jedan od načina kako se može doći do podataka koji se nalaze na sustavu jest prisluškivanje. Dovoljno je snimiti zvuk pisača u radu pa da se kasnijom obradom dođe do teksta koji je otisnut pisačem. Prisluškivanje se može izvesti i na svim komunikacijskim linijama koje su povezane sa sustavom. Stoga je pri zaštiti potrebno da se podaci šifriraju, odnosno demoduliraju uz pomoć posebnih uređaja i algoritama.

Prerušavanja tj. ulaženje u sustav pomoću ukradene šifre

U sustav se može ući pomoću odgovarajućih kartica, lažnih iskaznica i sličnih dokumenta koji su ukradeni ili kopirani zbog nepažnje ili nepromišljenosti djelatnika koji rade na sustavu. Takvi upadi su opasni zato što se ponekad ne zna ni vrijeme kada su izvršeni ni način na koji je izvršen upad u sustav.

Crv

Računalni program koji se sam nakon pokretanja programa umnožava na računalu ili na mreži s ciljem iskorištavanja resursa sustava u tolikoj mjeri da ovaj ne može normalno funkcionirati.

Ostali načini upada u sustav

U sustav se može ući i drugim načinima i uporabom raznih metoda. Jedna od metoda je tzv. asinhroni napad kod kojeg se u sustavu multiprogramiranja zaustavlja program (u djeliću sekunde) koji se napada i tako se ulazi u sustav njegovih podataka.

Ostale aktivnosti potaknute razvojem interneta

Devedesetih godina pojavljuju se pravne reforme koje se protežu i na druga područja koja su razultat razvoja interneta (Dragičević, 2004, str. 110):

- zaštita baza podataka, njihova sadržaja na internetu i autorskih prava
- globalni karakter računalnog kriminaliteta dovodi do toga da se postupanje prema počiniteljima uskladi diljem svijeta
- širenje nezakonitih i štetnih sadržaja potaknuli su pitanje odgovornosti ne samo onih koji to čine već i onih koji pružaju usluge i oni koji bi ih trebali nadzirati
- ostvarivanje sigurnosti elektroničkog poslovanja
- uloga informacije i pitanje njezine zaštite doveli su do stvaranja sigurnosnih mjera zbog sigurnosti informacijskih sustava i nesmetane komunikacije njegovih korisnika

Otkrivanje računalnog kriminaliteta

Otkrivanje računalnog kriminaliteta zahtijeva specijalne strategije istrage te dobru obučenost i istreniranost osoblja (Šimundić i Franjić, 2009, str. 74). FBI, naprimjer, rabi timski pristup u razrješavanju pojedinačnih slučajeva. Stvorena je CASIAT skupina stručnjaka koja obavlja analizu računalnog kriminaliteta i razvija profil računalnih kriminalaca sa svrhom da pomogne istražiteljima. U borbi protiv računalnog kriminaliteta valja utvrditi niz sigurnosnih mjera kao što su:

- usporedbe podataka kod sudionika transakcija
- ovjera isprava unositelja podataka
- ručna i instrumentalna kontrola pribavljača podataka
- ovjera rezultata rada računala i testiranje integriteta računala
- analiza spisa itd.

Sve ovo ukazuje na činjenicu da istraživanjima računalnog kriminaliteta, kao i zaštiti podataka i informacija, treba posvetiti punu pozornost iz razloga što se primjena računala i računalnih, osnosno informacijskih sustava sve više širi, a sve je manje dostupna izravna kontrola podataka.

Mnoge zemlje osnivaju specijalne policijske postrojbe za borbu protiv računalnog kriminaliteta i veliku pozornost posvećuju edukaciji i permanentnom školovanju tih jedinica i ostalog policijskog osoblja za borbu protiv te vrste kriminala.

U suzbijanju raznih vrsta kriminala, policija najčešće rabi računalo. U ovome trenutku, policija rabi računalo i za provjeru drugih računala, te za kontrolu onih koji ih zlorabe. No, ovdje svakako treba istaknuti da su policijske patrole radio vezama povezane s policijskim postajama i na raspolaganju im stoje sve baze podataka s kojima policijska postaja trenutačno raspolaže. U svakoj područnoj policijskoj postaji nalazi se po jedan terminal spojen s državnim centrom za Automatsku obradu podataka Ministarstva un-

utarnjih poslova Republike Hrvatske. Terminali omogućuju dostupnost mase podataka policijskim službenicima na terenu.

Kaznenopravni aspekti računalnog kriminaliteta

Najčešći pojavni oblici računalnih zlouporaba su (Šimundić i Franjić, 2009, str. 37-40):

Neovlašteni pristup računalnom sustavu (hacking)

Neovlašteni pristup računalnom sustavu su radnje kojima je cilj zaobilaženje provjere pristupa sustavu i omogućavanje počinitelju da se pod krinkom ovlaštenog služi uslugama i resursima sustava. Posljedica napada je povreda tajnosti, dostupnosti podataka i programa, ali i dostupnosti usluga.

Počinitelji su osobe kojima je omogućen pristup sustavu pri čemu se koriste terminalima drugih zaposlenika ili su to osobe koje putem modema pristupaju sustavu. Dijele se na unutarnje i vanjske počinitelje.

Unutarnji počinitelji pristup ostvaruju, uglavnom, nepažnjom drugih zaposlenika dok se vanjski počinitelji koriste raznim metodama kako bi došli do lozinki za pristup sustavu.

Počinitelji vode računa da djela koja počine putem tuđih računalnih sustava ili uporabom kloniranih mobitela ostanu neotkrivena kako bi zameli svoj trag i onemogućili druge koji tragaju za njima.

Računalna špijunaža

Računalnu špijunažu čine manipulacije gdje je cilj neovlašteno pribavljanje tajnih podataka i informacija pohranjenih u sustavima ili prijenosu putem telekomunikacijskih kanala. Prodajom tako stečenih informacija nastoji se steći protupravna imovinska korist.

Kao počinitelji javljaju se osobe koje na takav način žele onemogućiti konkurenciju i doći do informacija koje će moći koristiti u svom radu. To su osobe s visokim stupnjem obrazovanja u informatičkoj i telekomunikacijskoj tehnologiji. Ponekad rade sami, a ponekad po narudžbi. Kada slučajno dođu do informacija, sami ih nude na tržištu.

Vanjski subjekti nastoje neopaženo pristupiti sustavu uz zaobilaženje postojećih mjera fizičke zaštite. Profesionalci koji na raspolaganju imaju razna sredstva, koriste se svim slabostima sustava kako bi došli do cilja.

Računalna sabotaža

Računalnu sabotažu čine aktivnosti koje imaju za cilj onemogućavanje normalnog rada sustava ili sprječavanje njegove uporabe, odnosno uporabe njegovih resursa. Tu spada brisanje, mijenjanje, oštećivanje podataka, oštećivanje programa s namjerom da se onemogući njegova daljnja uporaba i funkcioniranje. Računalna sabotaža posebno je opasna kada se dogodi upad u gospodarske sustave, vojna i sva druga infrastrukturna postrojenja.

Počinitelji su osobe s većim tehničkim znanjem koje koriste sofisticirana sredstva i metode. Najčešći počinitelji su hackeri, teroristi, kriminalci motivirani koristoljubljem koji to čine zbog osvete, političkih i drugih uvjerenja.

Riječ je o fizičkoj aktivnosti koja dovodi do daljnjeg onesposobljavanja ili otežavanja uporabe računala.

Računalna prijevara

Odnosi se na razne vrste manipuliranja podacima zbog stjecanja protupravne imovinske koristi. Do manipuliranja dolazi prigodom unosa, obrade, pohranjivanja, ali i razmjene podataka unutar pojedinoga informacijskog sustava ili unutar razmjene informacija na internetu. Lako se izvodi, a teško otkriva, jer počinitelji rabe tuđe osobne podatke.

Počinitelji su, uglavnom, zaposlenici pravnih osoba ovlašteni za pristup računalnom sustavu.

Unutarnji počinitelji u odsutnosti svojih nemarnih kolega rabe njihove terminale, a često je riječ i o bivšim zaposlenicima koji iz osvete (uglavnom zbog gubitka posla) tako postupaju.

Računalno krivotvorenje

Postoje dvije vrste manipulacija. U prvoj se računalo rabi za krivotvorenje tuđih postojećih dokumenata u digitalnom obliku, a u drugoj se računalo rabi kako bi se kreirali takvi dokumenti i izvršilo krivotvorenje.

Počinitelji imaju veće znanje i rabe sofisticiraniju legalnu i nelegalnu opremu koja danas više nije presudan element jer tehnologija svakim danom postaje sve jeftinija. Uz relativno male izdatke, ostvaruju se vjerni rezultati.

Ovlašten ili neovlašten pristup sustavu na kojem se nalaze takve isprave omogućava izmjenu postojećih podataka ili kopiranje nove isprave. Rabe se skeneri za prijenos na računalo, programi kojima se mijenja njihov sadržaj i oblik te pisači kojima se ispisuju na papir.

Softversko piratstvo

Softversko piratstvo čine neovlašteno reproduciranje i uporaba zaštićenih programa i to je jedan od najrasprostranjenijih oblika računalnog kriminaliteta. Digitalni oblik omogućuje jednostavnu i brzu reprodukciju, te razmjenu programa čemu je svoj doprinos dala i nedostatna pravna regulativa.

Počinitelja ima jako puno jer za ovaj oblik računalnog kriminaliteta nije potrebno posebno znanje ni posebna oprema.

Potrebno je malo tehničko znanje, a tome je svoj doprinos dao razvoj modema, ali i razvoj interneta.

Štetni i protuzakoniti sadržaji

Riječ je o djelima koja se uz pomoć moderne informacijske tehnologije reproduciraju, proizvode i distribuiraju, a sadrže različite nemoralne i protuzakonite sadržaje u digitalnom obliku. Najčešće se radi o dječjoj pornografiji, sadističkim, neonacističkim, šovinističkim i drugim sličnim sadržajima. Širenju je posebno doprinio razvoj modema, interneta i ostalih telekomunikacijskih sadržaja.

Počinitelji se mogu svrstati u četiri kategorije:

- oni koji to čine iz materijalnih pobuda
- oni koji se rukovode nekakvim ideološkim ciljevima
- psihički poremećene osobe
- profesionalni kriminalci

Razvoj tehnologije omogućio je da se na malom prostoru pohrane velike količine podataka u svim oblicima. Time su stvoreni uvjeti da se relativno jeftino i brzo materijali prenesu i distribuiraju.

Raširenost kaznenih djela iz ovog područja također je vrlo velika, a kazne za počinitelje su gotovo zanemarive.

Etiologija računalnog kriminaliteta

Uzroci pojavnosti računalnog kriminaliteta dijele se u dvije skupine (Šimundić i Franjić, 2009, str. 34-36):

Objektivni kriminogeni čimbenici

Objektivne čimbenike koji su doveli do pojave i rasprostranjenosti računalnog kriminaliteta treba tražiti u specifičnostima same tehnologije, razvoju, širenju, društvu itd. To su:

- računalni kriminalitet u neposrednoj vezi sa stupnjem postignutog razvoja
- kriminalitet urbanih sredina, ne znači da ga nema i u drugim sredinama
- globalni kriminalitet
- jedna od najviših stopa rasta, odlikuje ga tzv. Tamna brojka
- posljedica je slabosti – ljudskih i tehničkih koje onemogućavaju djelotvornu borbu
- teško ga je suzbijati i zaustaviti
- podaci u digitalnom obliku otežavaju zaštitu
- ogromna količina podataka i informacija
- može dovesti do najštetnijih posljedica za pojedinca i društvo
- kriminalitet XXI. stoljeća

Subjektivni kriminogeni čimbenici

Odnose se, uglavnom, na osobne čimbenike koji izazivaju takvo djelovanje za koje se slobodno može reći da su posljedice modernog doba. To su:

- *Otuđenost* – Posljedica suvremenog načina života, komunicira se sve manje uz izravan kontakt, a sve više putem modernih tehnologija
- *Frustracija* – Količina informacija oko nas je ogromna, neki ljudi ne mogu se oduprijeti informacijskom stresu, jer se svi podaci moraju obraditi i odabrati oni valjani, odnosno na kojima će se bazirati odluke koje mogu dovesti do agresivnosti i raznih drugih reakcija
- *Psihička oboljenja* – Posljedica nekontrolirane i dugotrajne uporabe interneta rezultira socijalnim, poslovnim ili financijskim problemima
- *Motivacija* – Brzina kojom se može izvršiti zlouporaba s velikih udaljenosti uz anonimnost i mogućnost brzog i lakog bogaćenja
- *Stavovi i shvaćanja* – Razlozima sve češće postaju ideološki stavovi

Zaključak

Moderna informacijsko-računalna tehnologija svakim danom sve više napreduje i razvija se. Sukladno tome, nažalost, svakim danom sve više napreduju njezine zlouporabe koje mogu izazvati kaos kako na sustavu nekoga, naprimjer, gospodarskog subjekta, tako i na osobnom računalu bilo kojega običnog čovjeka. Zbog toga je potrebno, koliko je god to moguće, otkrivati i prijavljivati nadležnim tijelima sve oblike računalnog kriminaliteta. Nadležna tijela bi trebala u što kraćem roku poduzeti sve što mogu kako bi se u najkraćem mogućem vremenu primjereno kaznili počinitelji takvih kaznenih djela. Ako kazna bude primjerena, za ponadati se je da će u osuđenog počinitelja proraditi savjest i da ta i slična kaznena djela više neće činiti. Presude iz područja računalnog kriminaliteta trebale bi se javno objavljivati kako bi se na taj način upozorilo javnost da kaznena djela iz područja računalnog kriminaliteta spadaju u red društveno neprihvatljivih ponašanja. Tako bi se mogli spriječili potencijalni novi hakeri koji se namjeravaju baviti ovim protuzakonitim djelatnostima. Kaznena djela iz područja računalnog kriminaliteta neupućenima možda izgledaju bezazleno, no, ona to nipošto nisu, jer mogu izazvati goleme probleme bez obzira pojave li se u nekom informacijskom sustavu ili u osobnom računalu.

Literatura:

- Dragičević, D. (2004.*). Kompjutorski kriminalitet i informacijski sustavi*. Zagreb: IBS.
- Kazneni zakon, *Narodne novine, Službeni list RH*, 110/97.; 27.98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.; 143/2012.
- Kazneni zakon, *Narodne novine, Službeni list RH*, 125/2011.; 144/2012.
- Šimundić, S. (2007). *Pravna informatika*. Split: Pravni fakultet Sveučilišta u Splitu.
- Šimundić, S. i Franjić, S. (2009). Računalni kriminalitet. Split: Sveučilište u Splitu – Pravni fakultet.
- Ustav Republike Hrvatske, *Narodne novine, Službeni list RH*, 56/90.; 135/97.; 8/98.; 113/2000.; 124/2000.; 28/2001.; 41/2001.; 55/2001.; 76/2010.; 85/2010.; 05/2014.
- Zakon o izmjenama i dopunama Kaznenog zakona, *Narodne novine, Službeni list RH*, 105/2004.

Biografija

Siniša Franjić rođen je u Osijeku, Republika Hrvatska, gdje je završio osnovno i srednje školovanje, a diplomirao je na Pravnom fakultetu Sveučilišta u Splitu. Napisao je (u koautorstvu) sveučilišni udžbenik „Računalni kriminalitet“ i nekoliko znanstvenih radova iz tog područja. Trenutačno radi kao asistent na Elektrotehničkom fakultetu u Osijeku.

sinisa.franjic@gmail.com.