Kriminaliteta v informacijski družbi

Maja Dimc
Ministrstvo za obrambo RS
maja.dimc@mors.si

Povzetek

Z razvojem informacijsko-komunikacijskih tehnologij se je velik del našega delovanja premaknil v kibernetično okolje, ki je odprlo okno v popolnoma nov svet z neomejenimi možnostmi za delovanje na vseh področjih – od izmenjave informacij do izobraževanja, trgovanja ali druženja. Ob številnih pozitivnih vidikih je razvoj informacijsko-komunikacijskih tehnologij hkrati povzročil tudi razvoj novih oblik kriminalitete, ki niso omejene zgolj na internet, temveč vključujejo vsa kriminalna dejanja, izvedena z uporabo računalnika ali z njegovo pomočjo. Poleg tega je mogoče opaziti razlike v percepciji javnosti glede določenih kriminalnih dejanj na področju, na katerem je bilo kriminalno dejanje izvedeno (resnično vs. virtualno okolje). Zaradi večanja količine in raznolikosti računalniške kriminalitete je izobraževanje javnosti ter sodelovanje med zasebnim in javnim sektorjem tako na nacionalni kot na mednarodni ravni ključnega pomena.
Ključne besede: računalniška kriminaliteta, informacijska družba, kibernetična kriminaliteta, konvencija o kibernetski kriminaliteti.

Abstract

CRIME IN INFORMATION SOCIETY

With the development of information communication technologies, a large portion of our operations transferred to cyber-space, which opened a window to a whole new world with limitless possibilities for operation in many different fields from exchange of information, to education, commerce or establishing relationships. In addition to its numerous positive aspects, the development of information communication technologies contributed to the development of new forms of crime that are not merely limited to the Internet, but include all criminal activities performed with the use of a computer or are aided in its performance by the use of a computer. Additionally, we are noticing differences in the perception of general public related to particular criminal activities based on the area where a particular crime was performed (real vs. virtual environment). Due to the increasing number and variety of computer-related crimes, it is crucial to raise the awareness of general public and promote cooperation between private and public sector both on the national as well as the international level.
Key words: computer-related crime, information society, cyber-crime, Cyber Crime Convention.

1 UVOD

Vsaka ključna sprememba družbe kot celote nedvomno prinaša poleg pozitivnih tudi negativne posledice. Razvoj informacijske družbe, skupaj z razvojem interneta, je ključno vplival na način delovanja naše družbe kot celote. Z internetom in oblikovanjem tako imenovanega kibernetičnega prostora se je odprlo okno v popolnoma nov svet z neomejenimi možnostmi za poslovanje, izobraževanje, raziskave, druženje itd., hkrati pa se je oblikovalo tudi novo okolje za kriminalne dejavnosti, v katerem odpovejo ustaljene metode fizične zaščite. Računalniška kriminaliteta vključuje tako nove vrste kriminalitete, ki so se razvile z razvojem informacijske tehnologije, kakor tudi tradicionalne oblike kriminalitete, pri katerih se za njihovo izvedbo uporabijo prednosti, ki jih ponujajo informacijsko-komunikacijske tehnologije.

Med nove vrste kriminalitete med drugim uvrščamo vdore v sistem, onemogočanje storitev, uničenje ali spremembo podatkov. Pri tradicionalnih oblikah kriminalitete pa gre tako za prenos obstoječih oblik kaznivih dejanj, kot so kraja, nadlegovanje, grožnje v virtualnem okolju, kakor tudi za olajšanje same izvedbe kaznivega dejanja z uporabo informacijsko-komunikacijske tehnologije (npr. pranje denarja, otroška pornografija). Danes smo priča hitri rasti vseh oblik računalniške kriminalitete, zato so ključnega pomena odkrivanje, pregon ter predvsem preprečevanje. Kibernetični prostor je okolje, v katerem ne obstojajo fizične meje, zato delovanje na nacionalni ravni ne bo doseglo zadostnih rezultatov, učinkovito preprečevanje, zaščito, odkrivanje in pregon računalniške kriminalitete lahko zagotovi le mednarodno sodelovanje. Primerna in splošno znana definicija pojava ter jasno vzpostavljene sankcije igrajo pomembno vlogo pri odkrivanju in pregonu. V procesu preprečevanja pa je treba vzpostaviti primerne sisteme izobraževanja javnosti o različnih tipih računalniške kriminalitete in spodbujati sodelovanje med zasebnim in javnim sektorjem tako na nacionalni kot tudi na mednarodni ravni.

2 RAČUNALNIŠKA KRIMINALITETA

2.1 Definicija

Zaradi raznolikosti kriminalnih dejanj v povezavi z informacijskimi tehnologijami je potrebna široka de-

finicija pojava. Tako se najpogosteje pojavlja definicija računalniške kriminalitete kot kriminalnega dejanja, izvedenega z uporabo računalnika ali z njegovo pomočjo. Kibernetska kriminaliteta je označena kot zloraba računalniških sistemov z uporabo interneta. [1]

Pomembna značilnost računalniške kriminalitete je dejstvo, da lokacija pri izvedbi kriminalnega dejanja ne igra nobene vloge in so lahko takšna dejanja izvedena sočasno na različnih lokacijah z različnimi žrtvami, zaradi česar je še toliko teže odkriti kršitelje. Poleg tega dejstvo, da računalnik predstavlja neke vrste pregrado med storilcem in žrtvijo, daje takšni vrsti kriminalitete dodatno značilnost »neosebnosti«. Računalnik in internet kršiteljem tako dajeta še dodatno »ogrinjalo anonimnosti«.[2]

2.2 Tipi računalniške kriminalitete

Pojav računalniške kriminalitete je izredno širok; v grobem jo lahko delimo glede na vlogo, ki jo računalnik igra pri samem kriminalnem dejanju. Tako računalniško kriminaliteto delimo na štiri kategorije [3]:

- *računalnik kot tarča kriminalnega dejanja* – primeri takšnih kriminalnih dejanj vključujejo vdor v sistem, onemogočenje storitev, uničenje ali spremembo podatkov, vandalizem. Ključna razlika med vdorom v sistem ter uničenjem ali spremembo podatkov je v namenu kršitelja, kajti v primeru vdora kršitelj pregleduje in morebiti kopira zaupne podatke, pri čemer gre za krajo, vendar pa podatkov ne uniči;
- *računalnik kot orodje kriminalnega dejanja* – v tem primeru je računalnik uporabljen za doseganje nekega kriminalnega namena, kot na primer kraja, kraja storitve, prevara, grožnje, nadlegovanje;
- *računalnik kot pomoč pri kriminalnem dejanju* – primeri takšnih kriminalnih dejanj vključujejo pranje denarja, otroško pornografijo. Kriminalne organizacije uporabljajo računalnike kot pomoč pri svojem delovanju; odkritih je bilo nekaj kriminalnih združb na področju prostitucije, ki so uporabljale računalnik za vodenje podatkov o strankah in plačilih. Pojavlja se tudi uporaba računalnika kot pripomočka pri nasilnih kriminalnih dejanjih, storilci na primer uporabljajo internet za navezovanje stikov z žrtvami (pedofili, posiljevalci, morilci);
- *kriminalna dejanja, povezana s široko uporabo računalnikov* – primeri takšnih kriminalnih dejanj vključujejo krajo intelektualne lastnine, ponarejanje, krajo identitete itd. Prav na področju kraje intelektualne lastnine trčimo na problematiko spremembe percepcije zaradi razvoja informacijske tehnologije. Najbolj razširjen primer tega je piratstvo na področju programskih rešitev, glasbe in filmov, pri čemer se večina storilcev ne zaveda resnosti svojega dejanja.

Ob upoštevanju navedenih štirih kategorij se je treba zavedati, da določeno kriminalno dejanje le redko spada samo v enega od navedenih tipov, temveč je pogosto kombinacija dveh ali večih tipov. [4]

2.3 Storilci računalniškega kriminala

Poplava novih internetnih storitev skupaj s spremembami v razmišljanju javnosti, ki sedaj dokaj brez zadržkov sprejema novosti, sta pripomogla k uspehu računalniške kriminalitete. Internetne strani, namenjene mreženju, blogi, forumi ipd., se zanašajo na preproste tehnike izmenjave informacij (»downloadanje«, objavljanje itd.). Posamezniki so danes veliko bolj pripravljeni deliti osebne informacije kot kadar koli prej in stopnja zasebnosti se vse bolj znižuje; lahko bi rekli, da živimo v družbi nadzora, ki je veliko naprednejša od principa vizualnega nadzora Benthamovega Panoptikona. Nadzor v današnji informacijski družbi namreč ni več zgolj vizualen, temveč »prebiva« v okolju digitalnega signala. [5] Posledično narašča računalniška kriminaliteta na področju zlorabe osebnih podatkov.

Storilci na področju računalniške kriminalitete nimajo nekega tipičnega motiva in njihovi profili vključujejo različne tipe hekerjev, teroristov, nezadovoljnih zaposlenih, škodoželjnih partnerjev ali pa »navihanih« najstnikov. Kljub izredni raznolikosti lahko sklepamo, da morajo imeti nekatere osebnostne značilnosti, zaradi katerih se nagibajo v kriminalno smer. Ključne značilnosti vključujejo tehnično znanje na področju informacijsko-komunikacijske tehnologije, določeno stopnjo prezira do zakonodaje, nagnjenost k manipuliranju in tveganjem ter bujno domišljijo. [6]

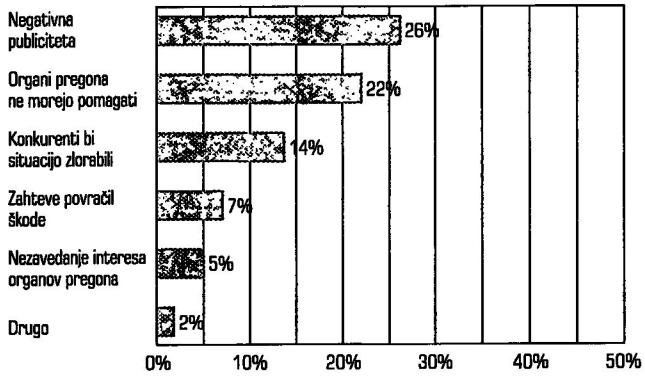
Posamezniki se odločajo za kršitve zakonodaje zaradi različnih razlogov; nekateri se odločajo za krajo zaradi golega preživetja, drugi se morda počutijo ogoljufane s strani sistema, tretji pa spet zgolj zaradi potrebe po zabavi. Poleg samega profiliranja storilcev je za namene odkrivanja in pregona ključnega pomena določanje potencialnih motivov, katere v grobem delimo na željo po zabavi, profit, maščevanje, socialne motivatorje, politične motive, seksualna nagnjenja

in psihična obolenja. Želja po zabavi kot motiv za izvedbo računalniške kriminalitete se nanaša predvsem na mlajšo generacijo, najstnike, ki v »hekanju« iščejo vzhičenje. Ta motiv gre v korak s socialnimi motivatorji, saj takšni najstniki po navadi delujejo v skupinah, v okviru katerih drug drugega spodbujajo oz. izzivajo, kar se odraža v vedno bolj drznih dejanjih. Medtem ko takšne storilce zanima samo vidik zabave, pa je profit najbolj razširjen motiv, pri katerem gre najpogosteje za tradicionalne oblike kriminalitete, ki so izvedene s pomočjo informacijsko-komunikacijske tehnologije (npr. kraja, poneverba). Pomembna motivatorja sta prav tako jeza in želja po maščevanju, v okviru česar gre najpogosteje za nezadovoljne zaposlene. V tem primeru gre za kazniva dejanja, kot so grožnje, izsiljevanja, napadi na sistem; po navadi v teh primerih ne gre za pazljivo načrtovana dejanja. Povsem drugače je v primerih računalniške kriminalitete, izvedene na podlagi določenih političnih prepričanj, pri katerih je izvedba natančno načrtovana in lahko vključuje samo širjenje propagande ali pa napade na delovanje institucij. [10]

Profiliranje kriminalcev je ključnega pomena za proces pregona. V okviru raziskav na tem področju se informacije primarno pridobijo prek posameznikov, ki so bili prijeti, so pod nadzorom ali pa so pripravljeni sodelovati. Ti posamezniki sicer predstavljajo le majhen del storilcev na področju računalniške kriminalitete, kljub temu pa se profiliranje izvede na podlagi pridobljenih informacij, statistik in primerjalne analize. [6]

2.4 Razlogi, zakaj organizacije ne prijavijo vdora v sistem

Čeprav velja splošno prepričanje, da so kršitelji na področju računalniške kriminalitete v glavnem mladostniki, pa so raziskave pokazale precejšnje zvišanje števila kriminalnih dejanj s strani odraslih, pogosto strokovnjakov na področju informacijsko-komunikacijskih tehnologij. Kar 70 do 80 odstotkov primerov nelegalnega dostopa je izvedenih s strani zaposlenih v podjetju. Zanimivo je dejstvo, da podjetja prijavijo le 5 do 10 odstotkov takšnih primerov; v večini primerov kršitelje odpustijo, pri čemer je velika verjetnost, da bodo ti svoje nelegalne dejavnosti ponovili v drugem okolju. Razlogov za takšno odločitev je več, primarno pa podjetja ocenjujejo, da bo javno priznanje takšnega incidenta negativno vplivalo na sloves in poslovanje podjetja. [7]



CSI 2007 Computer Crime and Security Survey 2007: 196 anketirancev
Vir: Computer Security Institute

Slika 1: **Razlogi, zakaj organizacije ne prijavijo incidentov vdora v sistem [8]**

Javno priznanje preboja varnostnih sistemov organizacije bi povzročilo nezaupanje v organizacijo na vseh ravneh, kar bi se odražalo tako na vrednostnem trgu, kakor tudi v odnosu strank, ki bi se zaradi tega nagibale k »varnejšim« konkurentom. Poleg tega bi lahko prišlo do zahtev glede povračil morebitne škode strankam ali investitorjem. V času po incidentu je organizacija še bolj ranljiva in javno priznanje bi hkrati pomenilo javno priznanje slabosti na področju varnosti informacijskega sistema, kar bi privabilo nadaljnje poskuse napadov. Dodatni razlog za prikrivanje takšnih incidentov je nedvomno pomanjkanje zaupanja organizacij in splošne javnosti v uspešnost organov pregona na področju odkrivanja storilcev računalniškega kriminala. [8]

2.5 Kako delujejo napadi na sistem

Pri napadu na sistem govorimo o dveh glavnih tehnikah, in sicer dostavi (delivery) in proženju/implementaciji (deployment). Prvi korak nedvomno predstavlja dostava zlonamernega programa, ki ji nato sledi njegovo proženje. Za dostave storilci uporabljajo različne metode, od katerih se najbolj široko uporablja nezaželena (»spam«) pošta in pa inficirane spletne strani (zlonameren program se naloži med obiskom spletne strani). Idealen scenarij za storilce predstavlja žrtev, pri kateri lahko zlonameren program nemudoma naložijo. Naslednji korak predstavlja zagotovitev čim daljše življenjske dobe zlonamernega programa, za kar storilci uporabljajo različne strategije. Primarno se posvetijo temu, da bi zlonameren program čim bolje prikrili, kar dosežejo z onemogočanjem sistemskih obvestil, onemogočanjem opozoril antivirusnih programov, onemogočanjem ažuriranja antivirusnih

programov ipd. Poleg tega sodobnejši zlonamerni programi zagotavljajo svoj obstoj in »lastništvo« nad sistemom z uničevanjem drugih morebitnih zlonamernih programov. [9]

Seznam najbolj nevarnih in najbolj varnih domen v letu 2008 (Vir: RIS, http://www.ris.org):

Najbolj nevarne	Najbolj varne
Hong Kong (hk)	Finska (fi)
Kitajska (cn)	Japonska (jp)
Filippini (ph)	Norveška (no)
Romunija (ro)	Slovenia (si)
Rusija (ru)	Kolumbija (co)

2.6 Preprečevanje, preiskovanje in pregon

Preiskovanje in pregon večine primerov računalniškega kriminala sta problematična zaradi dejstva, da običajno takšnih incidentov ni mogoče obravnavati samo v okviru pristojnosti ene države. Mednarodno sodelovanje in predvsem enoten pristop k preiskovanju in pregonu te vrste kriminalitete je tako edina mogoča pot k uspehu. Konvencija o kibernetski kriminaliteti,[1] ki jo je leta 2001 sprejel Svet Evrope, predstavlja temelj evropskega sodelovanja na področju računalniške kriminalitete. Dodatni protokol h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v računalniških sistemih, je bil sprejet leta 2003. Večina evropskih držav je ratificirala konvencijo in dodatni protokol leta 2004; v tem letu je konvencijo ratificirala tudi Slovenija ter izvedla zahtevane zakonodajne spremembe. Primarni cilj konvencije je poenotenje državnih zakonodaj na področju računalniške kriminalitete, vzpostavitev enotnega pristopa k pregonu računalniške kriminalitete in vzpostavitev učinkovitega mednarodnega sodelovanja. Konvencija in dodatni protokol predstavljata močno podlago za vzpostavitev skupnih dejavnosti preprečevanja in pregona na področju računalniške kriminalitete v okviru držav podpisnic in vzpostavljata skupno ogrodje za mednarodne dejavnosti na področju boja proti računalniški kriminaliteti.

Kljub tehnični naravi računalniške kriminalitete preprečevanje in preiskovanje potekata na enak način kot pri drugih oblikah kriminalitete in vključujeta procese zaščite, odkritja, preiskovanja in pregona. Organizacije poskušajo svoje sisteme in podatke zaščititi z uporabo varnostnih tehnik, kot so gesla, požarni zidovi, sistemi za odkrivanje vdora ipd. Uradna preiskava se začne s prijavo incidenta, temu sledi iskanje dokazov. Za uspešno preiskovanje je treba vključiti strokovnjake s poznavanjem zakonodaje in postopkov pregona ter precejšnjim tehničnim znanjem na področju računalniške opreme in forenzičnih računalniških rešitev. Ključni del preiskave je torej zbiranje in preverjanje elektronskih dokazov z uporabo forenzičnih orodij in tehnik za področje računalniške kriminalitete. Primerno zbrani dokazi vodijo v pregon storilca kaznivega dejanja. [7]

Preiskovanje in pregon primerov računalniškega kriminala ni omejeno na posamezno državo, temveč se lahko razteza prek več držav, pri čemer naletimo na problematiko pristojnosti, kar kritično otežuje uspeh preiskovanja in pregona. Najboljša obramba je v tem primeru nedvomno preventiva, ki vključuje izboljšanje prakse na področju zagotavljanja informacijske varnosti – tako na strani posameznikov kot tudi organizacij. Izobraževanje javnosti glede pojavnih oblik računalniške kriminalitete, preventivnih in zaščitnih tehnik je izrednega pomena, saj se storilci okoristijo predvsem na račun nevednih žrtev.

Uspešno preprečevanje računalniške kriminalitete je mogoče doseči le z vzpostavitvijo visoke stopnje zavesti o problematiki računalniške kriminalitete v splošni javnosti, v javnem in zasebnem sektorju, ter z izmenjavo informacij in s sodelovanjem na regionalni, nacionalni in internacionalni ravni. Politika, pravne in sodne prakse na nacionalni ravni se morajo prilagajati obstoječim mednarodnim pravnim okvirom ter zagotoviti primerne sankcije za storilce kaznivih dejanj na področju računalniške kriminalitete, ki morajo vključevati tudi odvzem prostosti. Prav tako je pomembno vzpostaviti sodelovanje med državami in nuditi pomoč manj razvitim državam pri oblikovanju učinkovitih sistemov preprečevanja in odzivanja na incidente računalniškega kriminala.

3 SKLEP

Sodobne informacijsko-komunikacijske tehnologije se vključujejo v vsa področja našega življenja in delovanja. Kibernetski prostor je postal sodobno okolje poslovanja, izobraževanja, mreženja in razvila se je

[1] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

nova vrsta kriminalitete. Računalniška kriminaliteta vključuje nove vrste kriminalitete (vdor v sistem, onemogočenje storitev itd.), ki so se razvile skupaj z razvojem informacijsko-komunikacijskih tehnologij, ter tradicionalne oblike kriminalitete (izsiljevanje, prevare itd.), pri katerih se za izvedbo uporabijo prednosti informacijsko- komunikacijskih tehnologij. Ena izmed največjih prednosti, ki jih je prinesel razvoj interneta – virtualni globalni trg –, hkrati predstavlja eno največjih težav pri odkrivanju storilcev računalniških kriminalnih dejanj.

Finančne izgube kot posledica računalniškega kriminala so ocenjene na stotine milijonov in celo milijard dolarjev, zato je uspešno preprečevanje, preiskovanje in pregon računalniške kriminalitete vedno večjega pomena. Zakonodaja na tem področju se posveča problematiki obeh navedenih vrst računalniške kriminalitete, vendar pa samo aktivnosti na ravni pregona ne zadostujejo, preventiva in zaščita igrata ključno vlogo. Zaradi internacionalne narave računalniške kriminalitete je treba vzpostaviti skupna vodila za delovanje na nacionalni in mednarodni ravni, kar poskuša doseči Konvencija o kibernetski kriminaliteti, ki predstavlja temeljni dokument na tem področju. Konvencija z opredelitvijo smernic poskuša zagotoviti konsistentnost zakonodajnih in regulativnih okvirov držav podpisnic.

Uspešna strategija boja proti računalniški kriminaliteti torej zahteva sodelovanje (svetovne) družbe kot celote s stalnim izobraževanjem o preventivi in zaščiti. Samo povečanje zavedanja pomena informacijske varnosti in problematike računalniške kriminalitete med posamezniki ter zasebnim in javnim sektorjem bo zagotovilo uspešno prevencijo. Zagotoviti je treba sodelovanje organizacij na nacionalni in internacionalni ravni, skupna pravila delovanja ter sistem najboljše prakse, s katerim bi zagotovili uniformne odzive na incidente računalniškega kriminala vseh vrst.

4 VIRI IN LITERATURA

[1] Britz, Marjie T. (2004). Computer Forensics and Cyber Crime, Prentice Hall, New Jersey, str. 4–5.

[2] Chantler, N. (1996). Profile of a computer hacker. Florida: Infowar.

[3] Tayor, Robert W. et al. (2006). Digital crime and digital terrorism, Prentice Hall, New Jersey, str. 4–15.

[4] Carter, E. (2002). Examining Cybercrime: Its Forms and Its Perpetrators. http://www.univd.edu.ua/_projects/ezloch_kor/docs/eng/37.doc

[5] Kovačič, M. (2003). Zasebnost na internetu. Ljubljana: Mirovni inštitut, Inštitut za sodobne mirovne in politične študije, Zbirka Politike.

[6] Rogers, M. K. (2001). A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study. University of Manitoba, Department of Psychology, August 2001.

[7] GAO-07-705 - Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. U.S. Government Accountability Office, July 23, 2007. http://www.gao.gov/htext/d07705.html.

[8] Richardson, R. CSI Computer Crime and Security Survey 2007. http://i.cmpnet.com/v2.goc.si.com/pdf/CSISurvey2007.pdf.

[9] Kaspersky, E. (2008). The Cybercrime Ecosystem. http://www.kasperskyusa.com/partners/pdf/The_Cybercrime_Ecosystem.pdf.

[10] Cybercrime. Piercing the darkness. http://library.thinkquest.org/04oct/00460/characteristics.html.

Maja Dimc je diplomirala na Roosevelt University v Chicagu iz politologije in informatike ter magistrirala na Fakulteti za družbene vede Univerze v Ljubljani, smer politologija – ameriške in svetovne študije. V okviru Ministrstva za obrambo RS deluje v Uradu za informatiko in komunikacije, na Fakulteti za management Univerze na Primorskem pa kot predavateljica sodeluje pri predmetu poslovna informatika. Raziskovalno se ukvarja s področjem preventive, preiskovanja in pregona računalniške kriminalitete.