2015

DIPLOMSKA NALOGA

NEJC FURLAN

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

DIPLOMSKA NALOGA

NEJC FURLAN

KOPER, 2015

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

Diplomska naloga

KRAJA IDENTITETE NA SPLETU

Nejc Furlan

Koper, 2015

Mentor: izr. prof. dr. Viktorija Florjančič

POVZETEK

V diplomski nalogi je predstavljen računalniški kriminal, njegova prisotnost, temeljni pojmi in značilnosti. Najbolj izpostavljena veja računalniškega kriminala je kraja spletne identitete, ki je vse bolj prisotna in razširjena v svetu in pri nas. Empirični del naloge zajema raziskavo uporabe protivirusne programske opreme, zavedanja nevarnosti na internetu, stopnjo razširjenosti kraje spletne identitete, in odzivanje ob ugotovitvi spletne zlorabe. Raziskava, ki je bila opravljena med 120–imi uporabniki interneta iz Notranjsko-kraške regije, je pokazala, da anketiranci poznajo protivirusno programsko opremo in jo tudi uporabljajo, da se zavedajo nevarnosti na internetu ter da so že bili deležni kraje spletne identitete.

Ključne besede: računalniški kriminal, kraja spletne identitete, informacijski sistem, nevarnosti interneta, protivirusna programska oprema.

SUMMARY

The Diploma thesis presents computer crime, its populartiy, basic terms and features. The most exposed branch of computer crime is theft internet identity, which is become more actively involved and expanded in the world as in our country. The empirical part of the work includes research of use antivirus software, awareness of the threats on the Internet, prevalence rates internet identity theft, and forwarding at conclusion of the Internet spoof. Analysis which have carried between 120 users of web from Notranjsko-kraške showed that respondents are familiar antivirus software and it also used to be aware of the threats on the Internet, and that present of minimally rate internet identity theft.

Keywords: computer crime, theft web identity, computer system, threats of internet, Antivirus Software.

UDK: 343.525:004.738.5(043.2)

ZAHVALA

Zahvaljujem se izr. prof. dr. Viktoriji Florjančič, za strokovno vodenje pri pripravi diplomske naloge in vse nasvete, komentarje ter spodbude. Zahvaljujem se tudi vsem povabljenim anketirancem, ki so rešili anketo, saj je ta raziskovalni del moje diplomske naloge.

VSEBINA

SLIKE

PREGLEDNICE

1 UVOD

Iz dneva v dan poslušamo, gledamo, razpravljamo in komentiramo dogodke o računalniških prevarah, zato smo se odločili delno raziskati in se dotakniti te problematike v našem okolju.

1.1 Opredelitev problema in teoretičnih izhodišč

Internet je svetovno omrežje računalniških omrežij. Imenujemo ga tudi omrežje omrežji, ki je sestavljeno iz več deset tisoč omrežji, v katera je povezano več milijonov računalnikov s skoraj celega sveta. Internet tako postaja nek nov informacijski prostor, ki nam omogoča dostop do velikega števila podatkov. V omrežju so dostopne različne zvrsti informacij, od komercialnih, akademskih do državnih in seveda tudi osebnih (Grubelnik b. l.).

Razvoj tehnologije in računalnikov ter opravljanje storitev preko njih je človeštvu omogočilo lagodnost, a je s tem prineslo tudi nekatere pomanjkljivosti. Z razvojem računalniške tehnologije se je povečala uporaba interneta, kar dokazujejo tudi podatki Statističnega urada RS (SURS). Po podatkih SURS (2013) je v prvem četrtletju 2013 v Sloveniji imelo dostop do interneta 76 % gospodinjstev, kar je za 2 odstotni točki več kot v prvem četrtletju 2012. S širjenjem uporabe interneta se pojavljajo tudi težave, kot sta računalniški kriminal in kraja identitete.

Računalniški kriminal je oblika kriminalitete, pri kateri prihaja do vdiranja v računalniške mreže in baze podatkov, pa tudi do denarnih transakcij, ki jim je izredno težko slediti. Prav ta oblika ima v prihodnosti največ možnosti za razvoj organiziranega kriminala in je tudi zakonsko najslabše opredeljena. Računalniki postajajo za organizacije organiziranega kriminala čedalje pomembnejše orodje za uspešno vodenje nelegalnih poslov ter za varovanje podatkov pred zakonom (Dobovšek 1997, 53).

Podatkov o tem v kakšni meri je računalniški kriminal razširjen, žal nismo našli, znani pa so podatki o računalniškem kriminalu po svetu, ki pa so presenetljivi. Letno naj bi bilo 556 milijonov žrtev spletnega kriminala, kar pomeni da se vsak dan s spletnim kriminalom sreča vsaj 1,5 milijona ljudi, to pa pomeni, da je ogroženih več kot 232,4 milijonov identitet (Go-Gulf 2013). Vse bolj priljubljeni Facebook ima dnevno ogroženih več kot 600 tisoč uporabniških računov. Zanimiv je tudi podatek, da je 1 od 10 vprašanih uporabnikov Facebooka postal žrtev goljufij ali lažnih povezav na socialnih omrežjih (Go-Gulf 2013).

Poseben problem na področju računalniške kriminalitete predstavlja kraja identitete. Kraja identitete je pojav, v katerem druga oseba nepooblaščeno prevzame naše identifikatorje (ime, priimek, naslov, EMŠO, številko računa, itd.) in se izdaja za nas. Tako lahko druga oseba zavaja druge in v našem imenu počne karkoli (npr. naroči in plača drag proizvod na internetu).

Tako kot ima kraja identitete pomen v realnem okolju jo ima tudi v spletnem okolju, vendar je veliko bolj nevarna, saj je nadzor in preverjanje le-te, otežen oziroma velikokrat tudi onemogočen. Preverjanje identitete v spletnem okolju zahteva samo določene segmente osebnih podatkov, kar v primerjavi s tradicionalnim preverjanjem identitete, ki poteka z predložitvijo osebnega dokumenta, na katerem je slika, predstavlja veliko večje tveganje in predstavlja večje razsežnosti škode, ki prizadenejo žrtev.

Ena izmed pomanjkljivosti uporabe tehnologije, interneta in internetnih orodij je tudi ta, da svetu odkrivamo svoje zasebno življenje. Tradicionalne načine identifikacije z osebnim dokumentom danes nadomeščajo uporabniška imena, gesla in digitalna potrdila, ali tako imenovani elektronski certifikati. Vse to pa lahko zlonamerneži z različnimi prijemi, kot so vdori v računalnik, okužbe z virusi, vohljanjem in pa tudi osebno nepazljivostjo, pridobijo in našo identiteto izkoristijo v zle namene oziroma v njim ljube interese. Pri takih dejanjih lahko trpi naš ugled, zaupne informacije ali celo naše stanje na bančnem računu (SI-CERT b. l.).

1.2 Namen in cilji diplomskega dela

V Sloveniji je preiskovanje računalniškega kriminala v rasti, saj smo šele leta 2005 sprejeli zakon, ki določa tovrstna kazniva dejanja. Zaradi pomanjkanja informacij in nepoznavanja tega pojava nas zanima, kako je pojav razširjen v Sloveniji. Predvsem zato, ker je v Sloveniji vsak dan vse več uporabnikov internetnih storitev, s tem pa so le-ti iz dneva v dan izpostavljeni takšnim in drugačnim internetnim zlorabam. Cilji diplomskega dela oziroma raziskave so sledeči:

- opredeliti osnovne pojme s področja spletnega kriminala,
- prikazati razširjenost spletnega kriminala, pri čemer se bomo osredotočili predvsem na področje kraje identitete,
- raziskati problem spletnega kriminala in predstaviti rezultate raziskave.

Z raziskavo, ki jo bomo opravili s pomočjo ankete, želimo potrditi/zavreči naslednje trditve:

- več kot polovica anketirancev, uporabnikov interneta, se ne zaveda nevarnosti računalniškega kriminala,
- več kot 50 % anketirancev je že bilo žrtev kraje identitete na spletu,
- več kot 60 % anketirancev ne ve, v kolikšni meri je kraja identitete (kot pojav računalniškega kriminala) razširjena po svetu,
- več kot 70 % anketirancev uporablja socialna omrežja, in se pri tem, ko objavlja svoje podatke (slike, letnice, naslove, itd.), ne zaveda nevarnosti zlorabe njihove identitete,
- več kot pol anketirancev v primeru zlonamernega napada na svoj računalnik ne pozna ustreznih načinov posredovanja problema ustanovam.

1.3 Predvidene metode za doseganje ciljev pri obravnavanju problema

Pri izdelavi diplomske naloge se bomo najprej posvetili študiju domače in tuje literature, kjer bomo dobili teoretično znanje. S pomočjo deskriptivne oziroma opisne metode, bomo opisali in opredelili določene pojme in pojave.

Nato se bomo lotili zbiranja podatkov in ugotavljanja obstoječega stanja, za kar bomo, kot instrument raziskovanja, uporabil anketo. Anketa v elektronski obliki, bo zajemala vprašanja zaprtega in odprtega tipa. Anketirali bomo ljudi stare od 15 do 60 let, anketirancev pa bo približno 150. Vzorec bo naključni. Anketirancem bomo, prek elektronske pošte, poslali vabila za izpolnitev ankete. Kljub temu, da bo seznam povabljenih anketirancev znan, bo anketa anonimna, saj zbranih podatkov ne bomo povezovali z imeni anketirancev. Zbrane podatke bomo obdelali s pomočjo programa Microsoft Excel, pri tem pa uporabili metode opisne statistike. Rezultate bomo prikazali grafično, opisno in tabelarično.

1.4 Predvidene predpostavke in omejitve pri obravnavanju problema

Predpostavljamo, da:

- anketiranci vse bolj uporabljajo internetne storitve in vse bolj zaupajo ponudnikom internetnih storitev,
- je vse več anketirancev že bila žrtev spletnega kriminala – kraje identitete,
- anketiranci v primeru kraje spletne identitete ne znajo pravilno reagirati in posredovati problema za to pooblaščenim organom,
- bodo anketiranci vprašanja razumeli in na vprašanja odgovarjali vestno ter bodo odgovori anketirancev odražala njihova realna mnenja.

Ker ima identiteta več pomenov določanja več različnih stvari, bomo v nalogi raziskovali le osebno identiteto, ki določa osebo.

Informacije zbrane s pomočjo ankete bodo imele omejeno veljavnost, saj se bomo osredotočili samo na stike, prijatelje in znance avtorja naloge, kar pomeni, da vzorec ne bo reprezentativen. Rezultatov raziskave tako ne bomo mogli posplošiti na slovensko populacijo.

2 KRAJA IDENTITETE NA SPLETU

S širjenjem spletnih storitev in rastjo računalniškega kriminala se povečuje tudi t. i. kraja identitete na spletu. To je, kot ugotavlja Turban idr. (2013), najhujša in najbolj razširjenja oblika računalniškega kriminala. Napad na posameznika za pridobitev številke zavarovanja (v ZDA) in številke kreditne kartice niso nič novega. Storilci kaznivih dejanj, ki so za pridobitev teh informacij kradli denarnice in torbice so v časih elektronike in tehnologije po obsegu škode manj nevarni od nepridipravov, ki svoja kriminalna dejanja opravijo preko spleta. Kraja spletne identitete in s tem povezanih podatkov obsega veliko večjo povzročeno škodo, kajti po spletu se podatki hitro širijo in tako postanejo dostopni javnosti. Prizadeti pa niso samo posamezniki, temveč tudi podjetja. Turban idr. (2013) trdi, da spletna kraja identitete podjetjem povzroči tudi veliko posredne škode, na primer izgubo ugleda in dobrega imena. Odkritje incidentov v podjetju pa lahko ogrozi celo obstoj podjetja.

2.1 Opredelitev osnovnih pojmov

Zaradi specifičnosti teme diplomske naloge in lažjega razumevanja nadaljnjega besedila, smo v nadaljevanju opredelili osnovne pojme.

2.1.1 Identiteta in kraja identitete

Identiteta je ujemanje bistvenih osebnih podatkov z resničnimi oziroma generičnim dejstvi v različnih primerih (Merriam-Webster b. l.). Kazenski zakonik (KZ-1-UPB2, 143. člen) krajo identitete opredeli kot kaznivo dejanje, pri katerem storilec, brez podlage v zakonu ali brez osebne privolitve posameznika, pridobi določene ključne osebne podatke, kot na primer EMŠO in davčno številko. Škodljive posledice tega kaznivega dejanja ne obsegajo zgolj pridobitve premoženjske koristi, ampak tudi druge koristi, kot npr. vstop v določene prostore. Za osebo, katere identiteta je bila ukradena ima takšno dejanje lahko neslutene posledice, saj se jo lahko okrivi za dejanja, ki jih sama ni storila. Kraja identitete predstavlja poseg v informacijsko zasebnost in varstvo osebnih podatkov. Žrtve kraj identitete lahko doživijo posledice, ki so primerljive s posledicami drugih nasilnih kaznivih dejanj in se nanašajo na življenje ter telo ali premoženje.

Kraja identitete ne pomeni samo premoženjskega oškodovanja (npr. izpraznjene bančnega računa ali prodajo vrednostnih papirjev), ampak tudi poseg v osebnost žrtve. Poznani so primeri, ko je bila posameznikom odvzeta prostost zaradi suma storitve kaznivega dejanja zaradi kraje biometričnih osebnih podatkov, npr. prstnega odtisa (Informacijski pooblaščenec RS b. l.).

2.1.2 Vdiralec

Storilca kaznivega dejanja kraje spletne identitete označimo z besedo vdiralec (angl. Hacker). Laudon (2012, 298) vdiralca opredeli kot osebo, ki pridobi nepooblaščen nadzor nad računalniškim omrežjem in sistemom z namenom pridobitve finančne koristi, kriminalnega dejanja ali osebnega zadovoljstva. Vdiralec se v praksi označuje tudi z besedo »kreker« (angl. Cracker), ki opredeli vdiralca, ki v sistem vdira s kriminalnim namenom. V medijih se ta dva termina uporabljata kot sopomenki. Vdiralci si nepooblaščen dostop do informacijskega sistema priskrbijo z iskanjem varnostnih pomanjkljivosti v sistemih.

2.1.3 Vdiranje

Vdiranje je vrsta kaznivega dejanja, pri katerem pride do vloma v računalnike posameznika ali organizacije, tako da je mogoče dostopati do njihovih osebnih in poslovno občutljivih podatkov (Cross Domain Solutions b. l.). Vdiranje (angl. Hacking) v računalnike O'Brien (2011) opredeli z obsesivno rabo računalnika ali s pridobitvijo nepooblaščenega nadzora nad računalniškim omrežjem.

Vdiranje je izraz, ki se večinoma uporablja za »kompleksno mešanico legalnih in nelegalnih aktivnosti, od legitimnega kreativnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov«; pogostoma pa se ga dojema, kot sofisticirano nelegalno dejavnost (Kovačič 2006, 87).

V Sloveniji vdiranje v informacijske sisteme velja za kaznivo dejanje in je za takšno dejanje, po Kazenskem zakoniku (KZ-1-UPB2, 221. člen), zagrožena kazen do dveh let zapora. V primeru povzročene večje škode je storilcu zagrožena kazen od treh mesecev do pet let zapora.

2.1.4 Spletni terorizem

Založnik (2007) spletni terorizem opredeli kot zlitje terorizma in spletnega prostora. To so nezakoniti napadi ali grožnje na računalnike, mreže in podatke, ki so shranjeni v njih, ki so izvedeni z namenom ustrahovanja ali pritiska na vlado za podpiranje določenih političnih ali družbenih ciljev. Spletni terorizem se razlikuje od drugih oblik računalniških zlorab, kot so vdiralstvo, gospodarsko vohunstvo, internetne goljufije in podobna kazniva dejanja, saj je glavni cilj spletnega terorizma uničenje večje omrežne infrastrukture določene države ali večje državne korporacije. Pojem spletnega terorizma se je začel pojavljati zadnja leta, predvsem v ZDA (prav tam). Pri tem so ključna vprašanja ali spletni terorizem sploh obstaja; ali res obstaja grožnja napadov preko interneta, ki lahko ogrozijo življenja in kako se obvarovati pred njimi.

2.2 Načini kraje identitete na spletu

Laudon (2012, 293) ugotavlja, da so lahko informacijski sistemi, brez zaščitne programske opreme, v nekaj sekundah onemogočeni in za vrnitev v normalno delovanje potrebujejo kar nekaj dni. Ena izmed zlorab je tudi kraja spletne identitete. Informacijski pooblaščenec RS (b. l.) pri kraji identitete loči več vrst napadov, in sicer napad glede na pooblaščenost napadalca – napad lahko izvaja pooblaščena ali nepooblaščena oseba, ter glede na to, ali so podatki ukradeni iz podatkovne zbirke ali med pretokom po omrežju neposredno. Podatki se lahko ukradejo tudi pri pretvorbi dokumentov iz analogne v digitalno obliko (preslikovanje dokumentov). Kraja spletne identitete se lahko izvede zaradi finančnih razlogov ali prevzema identitete v vsakdanjem življenju. Pri tem poznamo tehnične in ne-tehnične metode napada, oziroma kraja identitete.

Internet je v primerjavi z notranjimi omrežji (doma in v podjetjih) še posebej ranljiv zaradi svoje obsežnosti uporabe in možnosti uporabe vsakogar. Tega se je potrebno zavedati pri povezovanju informacijskega sistema podjetja v omrežje interneta (Laudon 2012, 294). Računalniki s stalno povezavo v internetno omrežje so bolj podvrženi napadom iz zunanjosti, posebno, če uporabljajo stalne internetne naslove, katere je lahko prepoznati in identificirati. Takšni stalni ali fiksni internetni naslovi so tudi stalne tarče vdiralcev. Telefonske storitve temelječe na internetnem omrežju so v primerjavi s telefonskim omrežjem bolj ranljive, če le te ne potekajo na zaščitenem privatnem omrežju. Telefonija preko internetnega protokola (angl. Voice over Internet Protocol VoIP), ki deluje preko javnega nezaščitenega omrežja je prav tako lahka tarča, saj lahko komunikacijo kdorkoli in kadarkoli prisluškuje. Ranljivost se je povečala tudi z uporabo e-pošte, hitrih sporočil in izmenjavo datotek prek P2P omrežij. Elektronska pošta lahko vsebuje tudi datoteke z zlonamerno programsko kodo, ki omogoča nepooblaščen dostop do prodajnih skrivnosti, finančnih podatkov ali drugih občutljivih informacij podjetja. Storitev hitrih sporočil delujejo brez zaščitnega sloja tekstovnih sporočil, zato je vsebina hitrih sporočil lahko odkrita in posredovana tujcem tudi med samimi prenosom preko javnega internetnega omrežja. Ilegalno deljene datoteke preko P2P omrežij, prav tako lahko vsebujejo zlonamerno programsko kodo in na tak način prevzamejo informacije o posamezniku ali organizaciji, ki so lahko posredovane neznancem. Nova tehnologija je prinesla nove internetne storitve, s tem pa tudi nove možnosti za nelegalno početje.

Uporaba brezžičnega interneta s pomočjo usmerjevalnikov se širi zaradi potrebe po mobilnosti (pametni telefoni, tablice, itd.). Kljub vsem prednostim (nepotrebni kabli, enostavna povezava, itd.), ki jih prinaša brezžično omrežje je le to tudi zelo ranljivo. Še posebej na udaru so brezžična omrežja na javnih mestih (knjižnice, letališča, bari, itd.) saj v večini primerov takšna omrežja niso varovana z varnostnim ključem in se v njih lahko poveže vsakdo. Laudon (2012, 295) trdi da tudi domača in zasebna brezžična omrežja varovana z varnostnimi ključi niso povsem varna, saj jih lahko danes vdiralci z malo strojne in programske opreme »preberejo« in ugotovijo varnostni ključ. S tem pa se lahko začne spremljanje internetnega prometa ali kot temu pravimo internetno prisluškovanje. V ta namen se je skozi leta razvijal tudi varnostni standard in sicer WEP, WPA, WPA2, ki je trenutno tudi v uporabi, saj podpira standard 802.11i in ima polno podporo v algoritmu AES-CCMP, kar pomeni, da se od prejšnjih dveh razlikuje v tem, da ga je težje »prebrati« in tako dobiti nepooblaščen dostop do računalnika in mobilne naprave.

2.2.1 Računalniški virusi in črvi

Laudon (2012, 296) poudarja da gre pri računalniški virusih in črvih za računalniške programe, ki vsebujejo del škodljive kode. Le-ta se prilepi na različne programske ali podatkovne datoteke, in tam »živi« dokler uporabnik ne odpre oziroma uporabi te datoteke. Ko uporabnik program oziroma datoteko uporabi se virusi aktivirajo ter okužijo še ostale dele sistema, največkrat brez vednosti in dovoljenja uporabnika (Informacijski pooblaščenec RS b. l.).

Virusi so lahko prisotni v večini računalniških datotek. Tako jih lahko dobimo v navodilih, elektronskih sporočilih, slikah, računalniških igrah, itd. Nekateri virusi so lahko zelo škodljivi in uničujoči, saj strojno opremo računalnika obremenijo do take mere, da se s časoma uniči oziroma pokvari. Virusi se prenašajo iz računalnika na računalnik s pomočjo človeških dejanj v obliki pošiljanja e-pošte ali kopiranja okuženih datotek.

Novejše oblike napadov so črvi. Črvi se od virusov razlikujejo v tem da lahko delujejo samostojno in za svoje delo ne potrebujejo datotek ali drugih računalniških programov, prav tako pa so tudi neodvisni od vedenja uporabnikov. Ravno to je glavni razlog, zakaj se črvi širijo hitreje od virusov. Črvi prav tako uničujejo datoteke in programe, lahko privedejo do prekinitve in celo do zaustavitve delovanja računalnika ali računalniškega omrežja. Tako črvi kakor virusi s seboj nosijo slab programski zapis (angl. Payload), kar jim omogoča popoln nadzor nad okuženim računalnikom in napadalcu omogočijo brisanje in urejanje datotek, krajo osebnih podatkov in tudi krajo spletne identitete.

Laudon (2012, 297) navaja, da se črvi in virusi najpogosteje širijo prek interneta z datotekami, preneseno programsko opremo, priponkami e-pošte, itd. Virusi pridejo oziroma vdrejo v računalniški sistem iz okuženih trdih diskov in okuženih informacijsko-telekomunikacijskih naprav (npr. pametni telefoni, tablični računalniki, itd.). Z vse pogostejšo rabo mobilnih naprav, se zlonamerna programska oprema širi tudi na mobilne naprave, na katerih se njihova škodljiva koda širi s pomočjo e-pošte, tekstovnih sporočil (SMS), Bluethooth-a in prenesenih datotek s spleta prek brezžičnega (Wi-Fi) ali mobilnega omrežja. Trenutno je poznanih približno 200 virusov in črvov ki so namenjeni mobilnim napravam. To so t. i.: Cabir, Commwarrior, Frontal.A, Ikee.B. Frontal, itd. Ti virusi lahko namestijo poškodovano datoteko, ki povzroči okvaro in prepreči ponovni zagon mobilne naprave, ali pa omogočijo napadalcu prevzem nadzora nad mobilno napravo.

Nova vrsta spletnih aplikacij za dostop do spletnih dnevnikov, wikijev, družabnih omrežij (Facebook, Twitter, MySpace, itd.) so uporabnikom olajšale stike in delo na daljavo, zlonamernežem pa odprle nov kanal za širjenje zlonamerne in/ali vohunske (angl. Spyware) programske opreme.

Informacijski pooblaščenec RS (b. l.) navaja, da se vsak teden pojavi okrog 500 novih virusov in črvov, pri čemer postajajo njihovi avtorji vse bolj inovativni in iznajdljivi. Večinoma se takšna škodljiva koda pojavlja v obliki neželenih elektronskih sporočil (angl. Spam), zato moramo biti pri odpiranju tovrstnih elektronskih sporočil še posebej previdni.

2.2.2 Vohunska programska oprema

Vohunska programska oprema (angl. Spyware) je ena izmed oblik škodljivih programskih kod. Laudon (2012, 298) ugotavlja, da mnogi uporabniki to vrsto programske opreme zaznajo kot nadležne programe, čeprav je ta vrste programska oprema še kako nevarna, saj lahko napadalec žrtvi ukrade določene podatke ali celo spletno identiteto. Laudon (2012, 298) tako opisuje primer programa za beleženje pritiska tipk na tipkovnici (angl. Keylogger). Ta program beleži vse pritiske tipk na tipkovnici in pridobljene podatke pošilja napadalcu. Napadalec na takšen način pridobi gesla, ki jih uporabnik vtipka pri prijavi v svoj e-poštni nabiralnik, e-banko, na družabna omrežja, itd. Napadalec lahko neposredno pridobi tudi številke ali PIN kode kreditnih kartic ter ostale podatke, ki jih uporabnik uporablja pri prijavi. Tovrstni programi se v računalnik, kot to ugotavlja Informacijski pooblaščenec RS (b. l.), naselijo med običajnim brskanjem po spletu, pri čimer za okužbo računalnika izkoristijo varnostne pomanjkljivosti spletnih brskalnikov (Mozilla, Interenet Explorer, Opera …). Drug način naselitve teh programom je možen v obliki brezplačnih programov, ohranjevalnikov zaslona, raznih orodnih vrstic (angl. Toolbar) in P2P programov (Lime Wire) za deljenje datotek.

2.2.3 Spletno ribarjenje in socialni inženiring

Informacijski pooblaščenec RS (b. l.) spletno ribarjenje (angl. phishing) opredeli kot sestavljenko iz besed geslo (password) in spletno ribarjenje (fishing). Pri spletnem ribarjenju gre za nelegalen način zavajanja uporabnikov z lažnimi spletnimi stranmi in elektronskimi sporočili, s čemer želijo zlonamerneži od uporabnikov izvabiti njihove osebne podatke, kot so: uporabniška imena in gesla, številke kreditnih kartic, digitalna potrdila in ostale osebne podatke. V ta namen zlonamerneži (Turban idr. 2013, 125) uporabljajo lažno spletno stran, ki je na videz identična kot prava spletna stran, nato pa od uporabnikov, z lažno e-pošto, poskušajo izvedeti osebne podatke, tudi številko bančnega računa in/ali številko osebnega zavarovanja. Spletno ribarjenje je tako lahko dobičkonosen posel zlonamernežev. Za svoje početje zlonamerneži uporabljajo internet in privatna omrežja s pomočjo katerih zlorabijo veliko število osebnih računalnikov. Od tu dalje se začne vohunjenje za njihovimi uporabniki. To naredijo tako, da uporabnike začnejo zasipati z nezaželeno e-pošto (angl. Spaming). Kasneje jim uničijo poslovanje ali jim ukradejo identiteto. Spletno ribarjenje je po podatkih, ki jih navaja Kocmur (2004) v zadnjih 10 letnih največjo škodo naredilo maja 2004. Nemški uporabniki spleta so takrat dobili povabilo, naj obiščejo navidezno spletno stran Volksbank in Raiffeisenbank ter vanjo vpišejo pomembne bančne podatke. Naivnežem, ki so nasedli, so tatovi kasneje izpraznili bančni račun. Tudi britanska enota računalniških kriminalistov je prejela skupino dvanajstih ljudi, ki so s podobnim načinom napadli britanske bančne račune in v Rusijo prenesli več sto tisoč britanskih funtov.

Forum za informacijsko varnost (securityforum.org) in organizacija za samopomoč, ki vključuje sto organizacij, sta sestavila seznam najbolj pogostih informacijskih napak in ugotovila, da je devet od desetih največjih incidentov rezultat treh dejavnikov:

- Sistemske napake in/ali človeške napake in/ali nepazljivosti.
- Okvare na sistemu.
- Nerazumevanje učinkov dodajanja neskladne programske opreme na že obstoječi sistem.

Socialni inženiring izkorišča obnašanje ljudi oziroma uporabnikov v določenih situacijah (npr. pod pritiskom). Zlonamerneži pri tem uporabljajo dognanja psihologije, saj imajo znanje za prevzemanje identitete drugih in tako lahko hitro pridejo do želenih osebnih podatkov. V strokovnih krogih je poznan računalniški vdiralec Kevin Mittnick, ki je slovel ravno po zmožnostih pridobivanja podatkov od ljudi (Informacijski pooblaščenec RS b. l.). Zlonamernežem, ki se poslužujejo socialnega inženiringa so v veliko pomoč socialna omrežja, saj tam uporabniki prostovoljno objavljajo številne svoje osebne podatke, ki napadalcem olajšajo napade. S takim obnašanjem na socialnih omrežjih uporabniki zlonamernežem sami olajšajo napade in s tem postanejo žrtve zlonamernih napadov.

2.2.4 Trojanski konji

Trojanski konj (angl. Trojan horse) je ena izmed oblik računalniških virusov, vendar z drugačnim načinom delovanja, čeprav sam po sebi ni virus, saj se ne ponavlja (Laudon 2012, 298). Ima pa veliko moč in lahko na računalniškem sistemu naredi veliko škode. Zlonamerneži ga velikokrat uporabijo za okužbo informacijskega sistema z virusom ali katerokoli drugo zlonamerno programsko kodo. Izraz trojanski konj izhaja iz antične Grčije, saj so takrat Grki uporabljali velikega lesenega konja, kjer so bili skriti vojaki. Z njim so prebili obzidje mesta, kjer se je leseni konj odprl in vojaki so lahko nadaljevali boje znotraj obzidja. Na podoben način deluje tudi računalniški trojanski konj, saj pomaga zlonamernežem prodreti skozi požarni zid računalnika. Za požarnim zidom se aktivira in okuži računalnik z eno izmed oblik zlonamerne programske opreme.

2.2.5 SQL vrinjeni napadi

Pri tej vrsti napadov, gre za vrivanje stavkov v izvorno kodo programa z namenom pridobitve dostopa do baze podatkov. Pri tem zlonamerneži uporabljajo t. i. »luknje v sistemu«. Svoje napade vršijo tako, da v programski zapis vrinejo svoje zapise, ki oslabijo določen program in jim na tak način dopustijo upravljanje baze podatkov. Z vrinjenim SQL napadom lahko napadalec pride do zaupnih podatkov (Strošar 2008). Po ugotovitvah Laudona (2012, 298) SQL vrinjeni napadi izkoristijo slabe kode v spletnih aplikacijah in uvedejo zlonamerne kode v sisteme in omrežja podjetja. V današnjem času so SQL vrinjeni napadi ena večjih groženj informacijskemu sistemu, oziroma bazi podatkov.

2.2.6 Oglaševalska vohunska programska oprema

Laudon (2012, 298) oglaševalsko vohunsko programsko opremo opredeli kot eno izmed oblik vohunske programske opreme, ki sicer ni tako nevarna kot ostala tovrstna programska oprema, je pa za uporabnike nadležna. Oglaševalska vohunska programska oprema se v računalnik v obliki programov naseli naskrivaj. Ti programi nato spremljajo uporabnika pri spletnem brskanju in zgodovino spletnega brskanja nato posredujejo podjetjem, ki to izrabijo v korist oglaševanja. Čez čas uporabnik v svoj e-poštni nabiralnik dobi oglase z vsebino, ki bi ga lahko najbolj zanimali.

2.2.7 Prevare in vohljanje

Vdiralci skušajo svoje prave identitete, največkrat s pomočjo prevar, ali zavajajočimi predstavami samih sebe, skriti. Skrivanje lahko poteka na različne načine. Eden izmed načinov je uporaba lažnega e-poštnega naslova. Druge vrste prevar vključujejo preusmerjanje spletnih strani, ki so na oko identične pravim vendar so v resnici »lažne«. S preusmerjanjem vdiralci pridobijo občutljive informacije o strankah, ki prek lažne strani izvedejo naročilo (Laudon 2012, 299).

Vohljanje (angl. Sniffing) je način za »prisluškovanje« podatkom, ki se prenašajo preko omrežja. Vdiralci uporabljajo tudi ta način za pridobitev zaupnih informacij o uporabnikih spleta. Vohljanje lahko povzroči zelo veliko škodo in ga je velikokrat težko prepoznati ter odkriti (Laudon 2012, 299).

2.2.8 Napad na naslove spletnih mest

Napad na naslove spletnih mest (angl. DDos attack) Laudon (2012) opredeljuje kot poplavo več tisočih lažnih sporočil in prošenj na strežnike, kar privede do sesutja omrežja. Omrežje zaradi prevelikega števila zahtev obremeni strežnik do take mere, da strežnik ne more več procesirati vseh zahtevkov, kar onemogoči dostop do spletne strani. Pri prodajnih spletnih straneh, lahko takšen napad privede da stranke ne morejo naročiti blaga. Takšni napadi na prodajne spletne strani prodajalcem povzročijo izpad prometa in neposredno manjši dobiček. Takšni napadi so nevarni predvsem za manjša in srednje velika podjetja, ki imajo svoja omrežja manj zaščitena kot velike korporacije.

Napadalci na naslove spletnih mest za svoje napade uporabljajo okužene računalnike imenovane »zombi« računalnik. Ti »zombi« računalniki so računalniki (v verigi jih je lahko tudi več sto tisoč), ki so jih zlonamerneži že prej okužili. Preko njih zlonamerneži nadaljujejo svoje početje. Tako preprečijo odkritje naslova prvotnega računalnika iz katerega je bil napad storjen. Laudon (2012) podaja različne ocene teh »zombi« računalnikov. Na svetu naj bi bilo med 6 in 24 milijonov »zombi« računalnikov. Ti podatki se iz dneva v dan spreminjajo saj napadalci po storjenem napadu, v to verigo povežejo nove računalnike, ostale pa medtem uporabniki, zaradi slabšega delovanja ali kakšnih drugih razlogov, očistijo. Laudon (2012) poudarja, da se je največji takšen napad (angl. Botnet attack) zgodil leta 2010. Imenovan je »Mariposa botnet«, začel pa se je v Španiji in se kasneje razširili po vsem svetu. Mariposa naj bi okužila in nadzorovala 12,7 milijonov računalnikov z namenom kraje številk kreditnih kartic in gesel elektronskega bančništva. Takrat se je okužilo več kot 1.000 podjetji, 40 glavnih bank in veliko število vladnih organizaciji, ki pa za okužbo kar nekaj časa sploh niso vedele.

2.3 Razširjenost kraje identitete na spletu

Rezultati, ki jih je slovenski nacionalni center za posredovanje pri omrežnih incidentih (SI-CERT) zbral, kažejo na to, da se spletne prevare in s tem povezana kraja spletne identitete, povečujejo in širijo. Po podatkih (SI-CERT b. l.) so v letu 2011 zabeležili 261 prijav spletnih goljufij in kraje identitete, kar je za 92 % več kot v letu 2010. Glede na to, da je to področje najslabše zakonsko opredeljeno, in je za kriminalne organizacije računalnik postal pomembno orodje, ima spletni kriminal v prihodnosti največje možnosti za razvoj, s tem pa tudi kraja identitete na spletu.

V ZDA je, po podatkih Harellove in Langtona (2013), v letu 2013 bilo žrtev kraje identitete kar 7 % prebivalcev starih 16 ali več let. Največ (37 %) kraj identitete se je zgodilo v povezavi s krajo podatkov obstoječih bank in krajo bančnih računov (40 %), 14 % žrtev kraje identitete je na spletu izgubila 1 dolar ali več. Od teh žrtev je le polovica utrpela izgube v višini manjši od 100 dolarjev.

Harellova in Langton (2013) poročata, da naj bi več kot polovica žrtev uspela rešiti vse probleme v povezavi s krajo spletne identitete v dnevu ali manj. Slaba tretjina teh žrtev (29 %) je za reševanje teh problemov potrebovala mesec ali več, 36 % žrtev kraje identitete pa naj bi, kot posledico kraje spletne identitete, imela zmerno ali hudo duševno stisko. Neposredne in posredne izgube zaradi kraje identitete pa naj bi v letu 2012 znašale približno 24,7 milijard dolarjev.

Iz vseh teh podatkov je razvidno, da je kraja spletne identitete v svetu veliko bolj prisotna kot pri nas. Posledice takšnih incidentov so hude in žrtve lahko prizadenejo materialno in duševno.

2.4 Značilnosti storilcev

Z računalniškim kriminalom se ukvarjajo ljudje različnih profilov in družbenih statusov oziroma skupin. Pred nekaj desetletji so izraz vdiralec in vdiranje poznali le strokovnjaki s področja računalništva. Ta izraz je prvi uporabil Joseph Weizenbaum leta 1976. Danes ta termin opisuje posameznika z veliko tehničnega in intelektualnega znanja, katerega izkorišča za napad na računalniške sisteme, kar vdiralce uvršča na področje računalniškega kriminala. Ljudje so ta dva izraza spoznali skozi medije, ki so stvari precej posplošili in vse vrste računalniških zlonamernežev poimenovali vdiralci oziroma »hekerji«. V praksi in teoriji temu ni tako, kajti biti vdiralec je tudi način oziroma slog življenja, ne pa samo želja po zastrahovanju, okoriščanju, itd. Vdiralec je bil v 70. letih prejšnjega stoletja termin, ki se je po ugotovitvah Yarja (2006) uporabljaj za nekoga, ki je močno tehnično usposobljen za razvoj kreativnih in učinkovitih rešitev računalniških problemov. Siciliano (2011), glede na to kaj storilci počnejo in na kakšen način izvajajo svoja dejanja, loči »slabe« in »dobre« vdiralce:

- *Beli klobuki:* to so »dobri« vdiralci, ki delajo v korist podjetji in države, saj z vdori testirajo in razvijajo nove metodologije, kako zaščiti in obvarovati informacijski sistem družbe, podjetja, države, itd.
- *Črni klobuki:* v večini gre za t. i. »slabe« vdiralce, za katere se v praksi uporablja tudi izraz »hekerji«. To so vdiralci, ki vdirajo v mrežne in računalniške sisteme ter izdelujejo raznovrstne računalniške viruse. Črni klobuki so še vedno bolje tehnološko podkovani kot beli klobuki. Največkrat so pri svojem delu uspešni, zaradi tega, ker izvedejo nov napad po najnižji stopnji odpora, bodisi zaradi človeške napake, lenobe ali malomarnosti. Motivacija za to vrsto vdiralcev je plačilo.
- *Skriptni posnemovalci:* to je poniževalni izraz za »črne klobuke«, saj so ti vdiralci slabše tehnološko podkovani in si za svoje »umazano« delo izposodijo že ustvarjene programe, ki jih kasneje uporabijo za napad na omrežja in spletne strani, v upanju da ne bi pustili sledi za seboj.
- *Vdiralci aktivisti:* nekateri vdiralci so motivirani s strani politike ali religije, in se svojim tarčam želijo maščevati s kršitvami ali pa jih samo nadlegovati, za zabavo in osebno zadovoljstvo.
- *Sponzorirani vdiralci:* vlade po vsem svetu si prizadevajo, da bi bili njihovi vojaški cilji, dobro pozicijonirani na spletu. Sponzorirani vdiralci imajo neomejen čas in sredstva za politično in drugo usmeritev civilistov, podjetji in ostalih vlad.
- *Vdiralec vohun:* podjetja najamejo vdiralce, da bi prišli do računalnikov svoje konkurence. Od tam pa naj bi jim ukradli poslovne skrivnosti, lahko od zunaj ali pa z zaposlitvijo v podjetju pod pretvezo. Vdiralec vohun deluje podobno kot vdiralec aktivist, vendar je njegova prioriteta zadovoljstvo stranke in pošteno plačilo.
- *Spletni teroristi:* ti vdiralci so na splošno motivirani s strani verskih in političnih prepričanj, poskušajo ustvariti vsesplošni strah in kaos z namenom motenja kritičnih infrastruktur. Spletni teroristi so daleč najbolj nevarni. S širokim spletom znanj in ciljev. Njihova motivacija je širjenje strahu in terorja.

Belih klobukov oziroma vdiralcev z dobrimi nameni je proti ostalim vdiralcem, ki imajo slabe namene zelo malo. Izpostaviti moramo tudi različne poglede na vdiralce. V javnosti se pojavljajo različna mnenja na to temo. Po različnih teorijah in mnenjih nam je najbolj racionalna trditev, da niso vsi vdiralci slabi in da niso vsi kriminalci dobri. Nekateri vdiralci delujejo tako, da javnost osveščajo in se v njihovem imenu borijo proti nepravičnemu svetu. Takšen primer je spletna stran wikileaks.org. To je neprofitna medijska organizacija, ki širi informacije, ki so nedostopne oziroma tajne za širšo javnost (WikiLeaks). Te informacije največkrat prihajajo iz verodostojnih, vendar anonimnih virov. Prav Julian Assange, ki je idejni vodja ter tiskovni predstavnik WikiLeaksa je bivši računalniški vdiralec in programer.

Eden izmed problemov pri odkrivanju in zmanjševanju računalniške kriminalitete je v tem, da t. i. računalniški vdiralci težijo k najnaprednejši tehnologiji in imajo zelo močan motiv. To se kaže da vsako noviteto na področju računalniške varnosti, predvsem pa tisto ki velja za najbolj učinkovito, skušajo uničiti in vdreti v sistem. To pomeni, da so vdiralci vse bolj vztrajni, prizadevni, vedno bolj iznajdljivi in še bolj dosledni pri svojem delu (Yar 2006). Problemi se kažejo tudi v sodelovanju velikih računalniških korporacij z vdiralci, saj velike korporacije običajno, za razvijanje novih programskih rešitev, vdiralce plačujejo. S takim ravnanjem informacije niso več zaupne in so hitro posredovane javnosti. To pa vdiralcem omogoča, da so vedno korak pred kriminalisti, velike korporacije pa veliko lažje opravijo svoje napade, saj so jim programske rešitve dobro poznane. Vdiralci na ta račun lahko delajo »čisto« brez vsakršnih sledi, tako jim je kriminalno dejanje težko dokazljivo. Po forumih (Ahemmahem, b. l.) se širijo neuradne informacije, da naj bi velika korporacija, ki izdeluje računalniške igre Electronic Arts plačala vdiralcem, da ti ne izdajo »cracka[1] « za FIFO 14 v prvih mesecih njenega izida. To pa zato, da bi v tem času bilo prodanih veliko število računalniških iger FIFA 14, s tem pa bi si Electornic Arts zagotovil dodaten zaslužek in si še povečal dobro ime (Ahemahem b. l.). Vsi takšni prihodki vdiralcem omogočajo posodabljanje in nakup najnovejše tehnologije, medtem ko se v kriminalistične oddelke ki preiskujejo računalniški kriminal ne nameni velike pozornosti niti finančnih sredstev.

Tomšič (2015) ugotavlja, da motivi vdiralcev v 21. stoletju niso nič bolj drugačni od motivov pred desetletji. Glede na motive se jih da razvrstiti v tri skupine; tiste, ki delajo za lastno korist, tisti ki propagirajo politično ideologijo in širijo zavest o svobodi govora (t. i. hektivisti), in na tiste z uničevalnimi nagnjenji, katere ženeta maščevalnost in/ali želja po povzročanju kaosa.

Završnik (2005) opredelili motive vdiralcev po naslednjih postavkah:

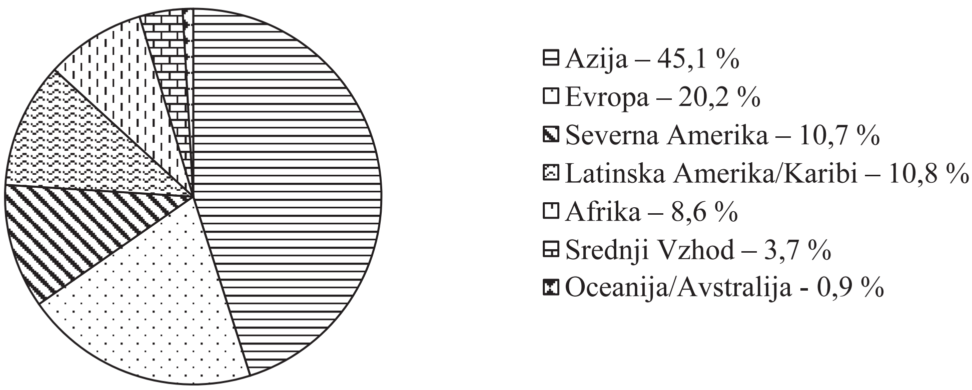
- *Intelektualni izziv:* vdiralci večinoma želijo svoje tehnično znanje razširiti in se podajo v vdiranje iz radovednosti in želje po učenju ter pridobivanju novega tehničnega znanja.
- *Ugled:* vdiralci si želijo ugleda in spoštovanja v družbi, tako da poskušajo izvesti vedno težje tehnično izvedljive stvari.
- *Kolekcija:* pri tem motivu gre za zbiranje čim več uspešnih napadov na žrtve, s tem se povečuje vdiralska zbirka žrtev.
- *Pohlep:* gre za vdiralce, katerim je glavni cilj dobiček in finančno okoriščanje na račun drugih, primer: kraja spletne identitete žrtve, za pretvezo pri dvigu z žrtvinega bančnega računa.
- *Informacije:* ta motiv zajema pridobivanje zaupnih informacij in/ali podatkov, ki so tako ali drugače cenjene v družbi, nekateri ljudje so za zaupne informacije pripravljeni odšteti veliko denarja.
- *Maščevanje:* ta motiv je najbolj prisoten v organizaciji, ker zaposleni iz maščevanja nepooblaščeno dostopajo do podatkov zaupne narave in jih posredujejo ali tržijo drugim konkurenčnim organizacijam, gre lahko za zelo nevarno početje, saj je pri tem večinoma prisotna jeza, ki ne pozna meja.

[1] crack = ilegalna programska koda, ki spremeni programsko opremo tako, da ima vse avtorske pravice, največkrat se to uporablja pri računalniških igrah (kršene so avtorske pravice).

3 RAZŠIRJENOST SPLETNEGA KRIMINALA

Z naraščanjem števila uporabnikov spleta narašča tudi število kriminalnih dejanj na spletu. Pojavljajo se novi napadalci in bolj ali manj posledično tudi nove žrtve spletnega kriminala. Internet in uporaba spleta je postala vse prej nuja kot luksuz. Primerjava podatkov spletnega portala RIS (2008) s podatki spletnega portala IWS (2013) kažejo na to, da se število uporabnikov interneta hitro povečuje. Tako je po podatkih Rabe interneta v Sloveniji (2008) v prvem četrtletju 2008 znašala ocena števila uporabnikov interneta v svetu 1.407.724.920 in je takrat predstavljala (21 %) vsega prebivalstva. Po podatkih Internet World Stats (2013) pa znaša ta ocena 2.802.478.934 in predstavlja (39 %) celotnega svetovnega prebivalstva. Iz prej predstavljenih podatkov lahko sklepamo, da ima že skoraj cel svet internet. Izjema so nedostopni kraji ali kraji, kjer so prisotni kakršnihkoli drugi okoljski in družbeno-ekonomski dejavniki v regiji.

Slika 1: Struktura uporabnikov interneta po svetovnih področjih za 1. polletje 2013



Vir: Internet World Stats 2013.

Po podatkih Eurostata (2015) ima v EU (28 držav članic) dostop do interneta od doma 96 % gospodinjstev.

3.1 Računalniški kriminal kot globalni problem

Vdiralci so vse bolj inovativni in učinkoviti, kar potrjujejo tudi ugotovitve Tomšiča (2015), ki pravi, da v letu 2014 skoraj, da ni bilo meseca brez vdiralskega napada. Pomembno razliko med vdiralci danes in vdiralci v 90. letih prejšnjega stoletja Tomšič (2015) vidi predvsem v učinkovitosti metod in dostopa do znanja in orodij. Danes lahko do orodij dostopi vsakdo, medtem ko so si ta orodja, pred desetletji, lahko privoščile le največje in najbogatejše internetne kriminalne združbe. Računalniški vdiralci so napadali od trgovskih gigantov eBay, Target in Home Depot do strežnikov Evropske centralne banke in ameriške banke JP Morgan Chase in celo Googlove storitve spletne pošte (Gmail).

Vdiralci so posegli tudi v zasebna življenja javnih oseb (afera The Fappening). Hollywoodskim zvezdnicam in uporabnicami Snapchata naj bi odtujili in javno objavili na tisoče razgaljenih slik. Najbolj odmeven vdor, je po navedbah Tomšiča (2015), ko so vdiralci z vdorom v strežnike filmskega studia Sony Pictures Entertainment povzročili škodo v višini 95-ih milijonov ameriških dolarjev.

Internetni kriminal je vse bolj razširjen, zaradi česar povzroča vse več škode, kar naj bi po ugotovitvah Tomšiča (2015) potrdila študija ameriškega inštituta Ponemon Institute. Tako naj bi po podatkih te študije, ameriške gospodarske organizacije internetni kriminal stal 10,5 milijona evrov (prav tam). Trgovski giganti naj bi v povprečju imeli 7,2 milijona evrov škode, podjetja iz tehnološkega sektorja pa dobrih 12 milijonov evrov škode. Bussines Insider vidi razlago za nastanek tako velike finančne škode v tem, da so se vsa podjetja iz razvitega sveta, ki poslujejo preko spleta začela prepozno zavedati nevarnosti interneta in njegovih storitev. Podjetja naj bi se vse preveč osredotočala na druge grožnje: konkurenco, regulatorje, gospodarsko krizo, ipd. Organizacije za analizo podatkov s področja informacijske tehnologije po besedah Tomšiča (2015) napovedujejo, da bodo v letu 2015 organizacije namenile več denarja za zavarovanja.

Tomšič (2015) poudarja, da so vdiralcem še vedno glavna tarča računalniško slabo podkovani posamezniki, ki vdiralcem z naivnimi in nepremišljenim obnašanjem na spletu (klikanje na povezave sumljivega porekla) olajšajo delo. Tako se, na primer, da si uporabniki, med ogledovanjem internetne pornografije, namestijo predvajalnik za ogled vsebin, v resnici pa gre za trojanskega konja, črva ali zadnja vrata, ki vdiralcem omogočijo dostop do uporabnikovega računalnika in/ali pametne prenosne naprave.

Med žrtvami vdiralcev se vsako leto znajde 556 milijonov uporabnikov spleta, podjetji in javnih organizaciji (Tomšič 2015). Vsak dan naj bi vdiralci napadli več kot 1,5 milijona računalnikov, vsako sekundo pa dobrih 17 računalnikov in informacijskih sistemov. Vsako leto v javnost uidejo osebni podatki o več kot 230 milijonih spletnih uporabnikov. Facebook naj bi vsak dan doživel 600 tisoč vdorov v uporabniške račune. Po teh podatkih 1 od 10 oseb priznava, da je že postala žrtev prevar na družbenih omrežjih. Krajo podatkov med odhodom iz podjetja naj bi izvajalo 59 % bivših uslužbencev. Največ vdiralskih napadov pa naj bi bilo izvedenih iz naslednjih držav: Rusija, Tajvan, Nemčija, Ukrajina, ZDA, Romunija in Kitajska (Tomšič 2015).

3.1.1 Opredelitev računalniškega kriminala

Računalniški kriminal je po O'Brienu (2011, 534) opredeljen z nepooblaščeno uporabo, dostopom, spreminjanjem ali uničenjem strojne in programske opreme, podatkov ter omrežnih virov. Med računalniški kriminal spada tudi nepooblaščena objava podatkov, nepooblaščeno kopiranje programske opreme, omejitev dostopa končnemu uporabniku do njegovih lastnih podatkov, strojne in programske opreme ter omrežnih virov. Prav tako je računalniški kriminal nepooblaščena uporaba tujih omrežnih virov za pridobitev materialnih in nematerialnih dobrin.

O'Brien (2011, 534) računalniški kriminal povezuje tudi s krajo denarja oziroma finančnih sredstev. V večini primerov gre za »notranja delovna mesta«, ki omogočajo nepooblaščen vstop v omrežje. S tem pa goljufivo spreminjanje zbirke podatkov. V večini primerov so finančne izgube veliko večje, kot se o njih dejansko poroča. Veliko podjetji, ki so bili žrtve računalniškega kriminala tega ne prijavijo, saj se bojijo padca vrednosti svojih delnic na borzah. Znano dejstvo je, da je nekaj britanskih bank, vključno z The Bank of London vdiralcem plačalo več kot pol milijona dolarjev, za skrivanje informacij o tem da so bile žrtve internetnih vdorov.

Laudon (2012, 145) računalniški kriminal interpretira, kot skupek nedovoljenih dejanj z uporabo računalnika ali proti računalniškemu sistemu. Predmet kaznivega dejanja so v takih primerih lahko računalniki ali informacijski sistemi (uničenje računalniškega sistema ali centra podjetja). Pri tem gre lahko tudi za kraje računalniških seznamov z nedovoljenim oziroma nezakonitimi dostopom do računalniškega sistema.

Obstaja veliko vrst računalniškega kriminala. V Sloveniji, na podlagi KZ-1-UPB2, ločimo naslednja kazniva dejanja:
- zloraba osebnih podatkov (143. člen),
- kršitev materialnih avtorskih pravic na internetu (148. člen)
- napad na informacijski sistem (221. člen),
- zloraba informacijskega sistema (237. člen),
- izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem (306. člen).

Računalniškemu kriminalu posvečamo veliko pozornosti, saj je z njim lahko povzročena velika škoda. Zaradi vse večjih možnosti izvedbe računalniškega kriminala, ga nekateri opredeljujejo kot kriminal prihodnosti. Z internetom je danes povezan že skoraj ves svet. Prek njega uporabniki koristijo spletne storitve in različna komunikacijska orodja. Množična uporaba spleta je storilcem omogočila izvrševanje nekaterih kaznivih dejanj. Žrtve niso samo posamezni uporabniki spleta, temveč tudi organizacije in svetovne korporacije. Problem računalniškega kriminala je z vidika preiskovalcev v tem, da je večina dokazov v elektronski obliki in da jih je moč izbrisati in spreminjati, tako da določeni dokazi sploh ne obstajajo. Preiskovalci se srečujejo tudi z drugimi problemi, kot so naprednejša tehnologija in boljše računalniško znanje kriminalcev. Le-ti so pogosto korak pred preiskovalci.

Slovenija je podpisnica *Konvencije o kibernetski kriminaliteti* oziroma »*Budimpeštanske konvencije*«. »To je mednarodni pravni akt, ki sodobno kibernetsko kriminaliteto obravnava z vidika priporočil, ki naj jih podpisnice upoštevajo pri oblikovanju in reformi svojega notranjega prava« (Rupnik 2003). Konvencija v svojem 20. členu opredeli pravno podlago za prestrezanje prometnih podatkov v realnem času, v 21. členu pa temelje za prestrezanje vsebinskih podatkov oziroma internetnega prometa. Zakon o elektronsko posredovani komunikaciji ima prav tako podlago v prej omenjeni konvenciji in v 107. členu opredeljuje pravno razmerje operaterja do njegove strojne opreme in pravi, da mora operater (fizična ali pravna oseba) na svoje stroške zagotoviti ustrezno opremo v svojem omrežju in primerne vmesnike, ki v njegovem omrežju omogočajo zakonito prestrezanje komunikacij. Prestrezanje internetnega prometa je sporno kot ugotavlja Kovačič (2006) iz dveh razlogov: učinkovitosti nadzora in iz vidika človekovih pravic. Postavlja pa se tudi vprašanje glede učinkovitosti in uporabnosti nadzora, kdaj bi sploh lahko policija uporabila prestrezanje internetnega prometa in ali ima pri tem kakšne tehnične omejitve.

Na preiskovanja računalniškega kriminala vpliva (Podjed 2008, 15):

- kompleksnost tehnologije,
- nezadostna usposobljenost preiskovalcev,
- žrtve v večini primerov ne poskrbijo za določeno stopnjo zaščite in druge varnostne ukrepe (posodabljanje programske opreme) saj se ne počutijo ogrožene.

Šket (2009, 11) razlikuje politični in ekonomski internetni kriminal. V skupino političnega kriminala uvrščamo naslednje:

- internetno vohunjenje (angl. Cyber spionage),
- računalniško sabotažo,
- vdiralstvo v sistem in
- internetni terorizem (npr. navodila za izdelavo eksplozivnih teles).

Ekonomski internetni kriminal je povezan s pridobitvijo finančnih sredstev. V to skupino uvrščamo:

- internetne goljufije pri trgovanju (angl. Consumer fraud),
- vdiralstvo,
- krajo internetnega časa in storitev,
- črne kopije, piratstvo (angl. Softwarepiracy)
- industrijsko vohunjenje (angl. Industrial spionage),
- žaljenje preko interneta (angl. Libel),
- otroško pornografijo (angl. Child pornography),
- pranje denarja,
- neupravičeno prilaščanje intelektualne lastnine (angl. Copyright infrigment),
- zlorabo elektronske pošte (pošiljanje kriptirane vsebine za organizirani kriminal),
- neupravičeno pridobitev tujih gesel (angl. Password sniffing),
- preprečevanje strežbe (angl. Denial of service),
- napeljevanje h kaznivim dejanjem in podajanje navodil preko interneta za izvajanje le-teh (nasilje, rasizem, nacizem, izdelava bomb ter pridelava drog).

Poznamo tudi dejanja, ki nimajo vseh značilnosti kaznivih dejanj, kot na primer:

- zanikanje (angl. Repudiation) pošiljanja oziroma prejemanja,
- nadlegovanje (angl. Harassment) npr. bombardiranje poštnih strežnikov,
- izguba zaupnosti (angl. Lost of Confidentiality),
- izguba integritete (angl. Alteration),
- zloraba programske opreme, npr. zadnja vrata (angl. Backdoor),
- trojanski konji, črvi (angl. Trojan Horses, Worm),
- maskiranje v zakonite uporabnike, oponašanje (angl. Spoofing).

Med neškodljiva, vendar nadležna dejanja, sodijo:

- prvo aprilske šale in potegavščine,
- besedni napadi (angl. Flamming) in
- neželena e-pošta.

Po Konvenciji Sveta Evrope o kibernetski kriminaliteti (Rupnik 2003) v računalniško kriminaliteto uvrščamo:

a) *Protipravni dostop (angl. Illegal Access)*: gre za nepooblaščen dostop do računalniškega sistema na podlagi pridobljenega uporabniškega imena in gesla.
b) *Protipravno prestrezanje (angl. Illegal Interception):* v tem primeru se izvaja nepooblaščeno prestrezanje podatkov, ki se vrši v računalniškem sistemu, bodisi iz sistema ali v sistem, lahko prav tako na podlagi pridobljenega uporabniškega imena in gesla ali pa s programsko opremo za prisluškovanje.
c) *Motenje podatkov (angl. Data interference)*: izvajanje določenih procesov, ki motijo pretok podatkov v omrežju, velikokrat zaradi programske opreme za prisluškovanje.
d) *Motenje sistemov (angl. System interference):* podobno izvajanje procesov, ki motijo oziroma upočasnjujejo delovanje sistemov, velikokrat se pojavljata t. i. modri zaslon (angl. blue screen).
e) *Zloraba naprav (angl. Misuse of Devices):* v takih primerih gre za fizično odtujitev tehnoloških naprav (npr. pametni telefoni, tablice, prenosni računalniki, itd.).
f) *Računalniško ponarejanje (angl. Computer-Related Forgery):* z določeno programsko in strojno opremo je možno na računalniških sistemih ponarediti od dokumentov (npr. os. izkaznice, potnega lista, servisne knjižice za avtomobile, itd.) do denarja, itd.
g) *Računalniške goljufije (angl. Computer-Related Fraud):* s tem pojmom povezujemo vse goljufije, ki se pojavijo v svetu računalništva in tehnologije, največkrat je prisotna e-pošta, ki od uporabnika želi na goljufiv način (prijatelj v stiski - pošlji denar) priti do finančnih sredstev.
h) *Kazniva dejanja, povezana z otroško pornografijo:* to zajema vse od posedovanja, do proizvajanja otroške pornografije.

i) *Kazniva dejanja, povezana s kršitvijo avtorskih in sorodnih avtorskih pravic:* največkrat je v povezavi s tem na udaru programska oprema, saj jo pirati največkrat in najpogosteje ponaredijo oziroma skopirajo, s tem so razvijalska podjetja oškodovana za dobiček od prodaje.

3.1.2 Razširjenost računalniškega kriminala

Medtem ko se nekatera kazniva dejanja iz leta v leto povečujejo, se delež drugih kaznivih dejanj zmanjšuje (Preglednica 1).

Preglednica 1: Kazniva dejanja po vrsti kaznivega dejanja

Kazniva dejanja računalniške kriminalitete	Št. kaznivih dejanj		Število ovadenih osumljencev	
	2012	2013	2012	2013
Zloraba osebnih podatkov	3	2	2	3
Zloraba informacijskega sistema	12	8	4	3
Kršitev materialnih avtorskih pravic	2	6	3	13
Napad na informacijski sistem	131	226	45	125
Izdelava in pridobivanje orožja ali pripomočkov za napad na informacijski sistem	3	2	3	1
Skupaj	151	244	57	145

Vir: MNZ Policija (2014).

Iz preglednice 1 je razvidno, da je največ kaznivih dejanj povezanih z napadom na informacijskih sistem. Ta kazniva dejanja zajemajo predvsem vdore v informacijske sisteme.

Po virih Policije (MNZ 2014) je za napad na informacijski sistem največkrat kriv človek, ki s svojo nepazljivostjo pogosto olajša delo storilcem kaznih dejanj.

V nalogi se ukvarjamo s krajo spletne identitete, ki je v KZ-1-UPB2, 143. člen opredeljena kot zloraba osebnih podatkov, napad na informacijski sistem in zloraba informacijskega sistema.

Pri zlorabi osebnih podatkov gre lahko za javno objavljanje teh podatkov, zlorabo osebnih podatkov, ki se nahajajo v bazi podatkov, itd. To dejanje se lahko kaznuje z denarno kaznijo ali pa celo z zaporom do 5 let, če gre za uradno osebo, ki zlorabi svoj položaj (KZ-1-UPB2, 143. člen).

Napad na informacijski sistem se lahko kaznuje z zaporom do enega leta v primeru, ko kdo neupravičeno vstopi ali vdre v informacijski sistem. Osebo, ki podatke iz informacijskega sistema neupravičeno uporabi, preslika, spremeni, prenese, neupravičeno vnese kakšen podatek, ovira delovanje in prenos podatkov, pa se lahko kaznuje z zaporom do dveh let (KZ-1-UPB2, 221. člen).

Zloraba informacijskega sistema v gospodarskem poslovanju ter na ta način pridobitev protipravne premoženjske koristi ali povzročitev premoženjske škode drugemu, se lahko kaznuje z zaporno kaznijo do treh let. V primeru ko je iz tega naslova pridobljena večja protipravna premoženjska korist ali je drugemu povzročena večja premoženjska škoda se storilca kaznivega dejanja lahko kaznuje z zaporom do petih let (KZ-1-UPB2, 237. člen).

Premiki na področju varnosti na internetu se kažejo v podpisu Kodeksa ravnanja izvajalcev javnih elektronskih komunikacijskih storitev za zaščito uporabnikov. Kodeks, ki so ga podpisali mobilni operaterji in internetni ponudniki, je bil pripravljen in urejen z namenom izboljšanja zaščite pred morebitnimi internetnimi nevarnostmi. Te bi lahko škodovale uporabnikovemu telesnemu, duševnemu ali moralnemu razvoju, ali pa bi uporabnikom škodovale v finančnem smislu (omogočanje primernih in dobrih razmer za razvoj uporabnosti z nudenjem podpore uporabnikom, staršem mladostnikov in drugim skrbnikom). Druga opredelitev tega kodeksa pa je, zagotavljanje varnejše rabe mobilnih naprav, še posebej pri otrocih in mladostnikih do 18. leta in starejših, ki zaradi pomanjkanja znanja slabše poznajo kibernetske nevarnosti.

Tokratni kodeks je nadgradnja že obstoječega Samoregulacijskega kodeksa ravnanja operaterjev mobilnih javnih elektronskih komunikacijskih storitev, ki je bil podpisan leta 2009 s strani predstavnikov Združenja za informatiko in telekomunikacije pri GZS ter mobilnimi operaterji. Kodeks je v skladu z veljavno evropsko in nacionalno zakonodajo in je namenjen varnejši rabi mobilnih naprav med mladostniki (RIS 2013).

Policija in ostali pristojni organi opozarjajo predvsem na preventivo oziroma primerno zaščito informacijskega sistema.

3.1.3 Možnosti zaščite pred računalniškim kriminalom

Informacijski sistemi so danes vedno bolj ogroženi, kljub novim posodobitvam, popravkom, aplikacijam, itd. Računalniški kriminalci so še vedno korak pred vso zaščitno opremo, pa čeprav se ta hitro in uspešno razvija. Programska oprema za zaščito informacijskih sistemov je v današnjih časih skoraj obvezen sestavni del informacijskih sistemov. V nadaljevanju bomo predstavili nekaj zaščitne programske opreme.

Šifriranje podatkov

Šifriranje podatkov (angl. Encryption of data) je po ugotovitvah O'Briena (2011, 548) postalo pomembno orodje za zaščito podatkov in drugih omrežnih virov, ki sodelujejo v internetnem omrežju. Šifriranje deluje na posebnem matematičnem algoritmu ali ključu za pretvorbo digitalnih podatkov z umeščeno kodo pred pošiljanjem in za dekodiranje teh podatkov ko so prejeti. To v praksi pomeni, da se npr. e-pošta pred pošiljanjem šifrira s ključem, ki se posreduje pooblaščenemu naslovniku. Naslovnik prejetega šifriranega e-poštnega sporočila mora sporočilo dešifrirati, za kar potrebuje ustrezen ključ. Na tak način se zaščiti e-pošta v primeru, da bi prišla na napačen e-poštni predal ali pa v primeru da bi bila prestrežena s strani vdiralcev. Programska oprema za šifriranje podatkov se po besedah O'Briena (2011, 548) prodaja posamezno ali v paketih z drugimi podobnimi programi. Ostaja veliko programov namenjenih za šifriranje, vsi pa uporabljajo standarda RSA (RSA Data Security) in PGP (Preety Good Privacy). Nekateri programi so prosto dostopni na spletu. Programska oprema kot je Novell NetWare in Lotus Notes deluje na platformi standarda RSA.

Požarni zid

Požarni zid (angl. Firewall) Laudon (2012, 314) opredeli kot programsko opremo, ki nepooblaščenim osebam preprečuje dostop do zasebnih omrežij. Gre za kombinacijo strojne in programske opreme, ki nadzoruje odhodni in dohodni prometni tok v omrežju. Programska oprema je nameščena med notranjim in zunanjim omrežjem kot je to internet. Požarni zid deluje kot vratar, ki pred dostopom do omrežja pregleduje dovolilnice vsakega uporabnika. Na tak način identificira naslove IP, imena, aplikacije in ostale druge lastnosti dohodnega prometa. Vse te zbrane informacije preveri in reagira v skladu s pravili, katere je namestil in modificiral skrbnik (uporabnik) omrežja. Če se katera izmed lastnosti ne ujema, požarni zid to zazna in uporabniku prepreči dostop do omrežja. Obstajajo različne tehnologije požarnih zidov, vključno s statističnim paketnim filtriranjem omrežnega prometa, naprednim pregledom, prevajanjem internetnih naslovov, uporabo pooblaščenega filtriranja, itd. V praksi se te tehnologije uporabljajo v kombinaciji za zagotavljanje požarnega varstva.

Paketno filtriranje preiskuje izbrana polja v glavah podatkovnih paketov, ki se pretakajo nazaj in naprej med zaupanja vrednim omrežjem in internetom ter pregleduje posamezne pakete v izolaciji. Ta vrsta varnostne tehnologije lahko »spregleda« veliko vrst internetnih napadov (Laudon 2012, 315).

Tehnologija »*statistični pregled*« zagotavlja dodatno varnost s preverjanjem in ugotavljanjem ali so paketi del stalnega prometa med oddajnikom in sprejemnikom. Tehnologija določa tabele stanja za sledenje informacijam različnih paketov. Paketi so odobreni ali zavrnjeni na podlagi tega, ali so del stalnega komuniciranja in, ali pa so poskušali vzpostaviti legitimno povezavo (Laudon 2012, 315).

Prevod internetnega naslova (NAT) požarni zid uporabi, ko sta prvi dve tehnologij polno zasedeni. Ta vrsta tehnologije gostiteljskemu računalniku omogoči spremenjeni internetni naslov (IP), tako da vohljaški programi, ki delujejo zunaj območja požarnega zidu, dobijo napačen internetni naslov in zavedejo napadalca (Laudon 2012, 315).

Proxy filtriranje prefiltrira vsebino prijavnih paketov v internetnem prometu. Tehnologija deluje tako, da pakete ki so izven požarnega zidu ustavi in skrbnika sistema obvesti, da želijo v sistem vstopiti zunanji podatki. Na podlagi informacij, ki jih proxy strežnik ponudi pooblaščencu, se le-ta odloči ali bo dovolil vstop zunanjih podatkov v sistem. To pomeni, da se za vsako komunikacijo, ki poteka v smeri od zunaj na noter in obratno, ter komunikacijo znotraj organizacije vedno zahteva pooblastilo skrbnika sistema (Laudon 2012, 315).

Za vzpostavitev dobrega in uspešnega požarnega zidu, Laudon (2012, 315) ugotavlja, da mora skrbnik sistema dosledno ohranjati in prilagajati pravilo za identifikacijo ljudi, aplikaciji in naslovov, ki so bodisi dovoljeni bodisi zavrnjeni. Požarni zid lahko s svojim delovanjem napadalcu oteži delo, ne pa popolnoma prepreči napad na omrežje in informacijski sistem, zato ga je potrebno obravnavati kot enega od elementov splošnega varnostnega načrta.

Sistem za odkrivanje vdorov

Ponudniki varnostnih storitev poleg požarnih zidov ponujajo orodja in storitve za odkrivanje vdorov, zaščito pred sumljivim zunanjim internetnim prometom ter poskusi dostopa do datotek in baz podatkov. Takšne vrste zaščite v večini primerov namestijo na t. i. »vroče točke«, kjer nenehno poteka preverjanje, odkrivanje in odvračanje vsiljivcev oziroma sumljivega internetnega prometa. V primeru da sistem odkrije sumljiv in nenavaden zunanji internetni promet, generira alarm. Pregledovanje programske opreme temelji na znanih metodah računalniških napadov, kot so slaba gesla in preverjanju če so bile pomembne datoteke spremenjene ali odstranjene (prav tam).

Sistem ob zaznavi sumljivih dogodkov pošlje opozorilo o vandalizmu nad računalniškim sistemom ali o napakah na skrbniškemu sistemu. Sistem za odkrivanje vdorov se lahko prilagodi tako, da v primeru nedovoljenega ali sumljivega internetnega prometa zaustavi delovanje občutljivega dela omrežja (Laudon 2012, 316).

Protivirusna in protivohunska programska oprema

Splošni varnostni načrt za posameznike ali podjetja mora vključevati protivirusno zaščito za vsak računalnik. Protivirusna zaščita je zasnovana tako, da pregleda prisotnost računalniških virusov na računalniškem sistemu in na pogonih. V večini primerov lahko sam protivirusni program odstrani najdeni virus, če je bil virus poznan že pred pisanjem tega protivirusnega programa. Za učinkovitost protivirusnega programa, mora skrbnik sistema poskrbeti, da se protivirusni program stalno posodablja, saj to zagotavlja, da baza podatkov o virusih vsebuje vse do tedaj znane viruse. Protivirusni izdelki so na voljo za različne vrste mobilnih in ročnih naprav (pametni mobilni telefoni, tablice, pametne ure, itd.), strežnikov, delovnih postaj in namiznih računalnikov.

Vodilni prodajalci protivirusne zaščite so: McAfee, Symantec, Trend, Micro, itd., ki so svoje programe okrepili še z protivohunskimi programi, kot so: Ad-Aware, Spybot Serch & Destroy, Spyware Doctor, itd. Prodajalci programskih rešitev za računalniške sisteme so za potrebe organizacij in zmanjšanje stroškov z zaščitno programsko opremo uvedli enotno zaščitno upravljanje sistema. Tako so v program uvedli paket, ki zajema več varnostnih rešitev: požarni zid, sistem za odkrivanje vdorov ter protivirusno in protivohunsko zaščito. S tem so zaščitno programsko opremo naredili finančno in uporabniško dostopnejšo za vse vrste podjetji in omrežij (Laudon 2012, 316).

Poleg vse zaščitne programske opreme, pa si moramo za učinkovitejše zavarovanje informacijskega sistema predvsem v organizacijah oziroma podjetjih ustvariti še obrambno strategijo.

3.1.4 Obrambna strategija podjetja

Cilj vseh uporabnikov spleta, posameznikov in podjetij, je zaščita pred računalniškimi kriminalom. Zato vsi uporabniki težijo k zaščiti informacijskega sistema, še posebej podatkov, programske opreme, strojne opreme in omrežji (Turban idr. 2013).

Preden se uporabniki spleta odločijo za zaščito morajo, kot to ugotavlja Turban idr. (2013), razumeti in poznati postopke poslovanja, ki dajejo temelje prilagojeni obrambni strategiji. Strategija obrambe in nadzora temelji na uporabi določenih prijemov in ukrepov. V nadaljevanju bomo predstavili glavne cilje obrambne strategije (Turban idr. 2013).

Preprečevanje in odvračanje

Pravilno zasnovane kontrole lahko preprečijo pojavljanje napak, odvračajo kriminalce od napadov na informacijske sistem in še bolje, preprečijo dostop nepooblaščenim ljudem. To so najbolj zaželene kontrolne aktivnosti.

Odkrivanje

Tudi na področju računalniškega kriminala je preventiva boljša od kurative. Odkrivanje lahko naredimo v večini primerov z uporabo posebne diagnostične programske opreme ob minimalnih stroških in s tem preprečimo škodo, ki bi lahko nastala zaradi na primer vdora v informacijski sistem. Običajno je povzročena škoda višja od stroškov diagnostične opreme.

Omejitev škode

Pri strategiji omejitve stroškov gre za zmanjšanje oziroma omejitev škode, potem ko je do okvare oziroma napada že prišlo. Ta proces drugače imenujemo tudi nadzorovanje škode. To lahko dosežemo s sistemom, ki je odporen na napake in lahko deluje v nestabilnih okoliščinah dokler se sistem ponovno ne obnovi. V primeru, da takšnega sistema nimamo, moramo nemudoma začeti obnovitveni postopek sistema, ne glede na višino stroškov, saj si uporabniki želijo svoj polno delujoči informacijski sistem kakor hitro je to mogoče.

Obnovitev

Načrt za obnovitev predvideva načine, kako popraviti poškodovani informacijski sistem v najkrajšem možnem času. Pogosto zamenjamo okvarjene dele, kar je sicer najhitrejši način obnovitve, ni pa nujno tudi najugodnejša možnost.

Posodobitve

S posodobitvami programske opreme in gonilnikov strojne opreme odpravimo ponavljanje istih napak in preprečimo ponovni vdor v sistem.

Osveščenost in skladnost

Vsi člani organizacije morajo biti osveščeni o nevarnostih in morajo ravnati v skladu s pravili in predpisi o varnosti.

3.2 Spletni terorizem in haktivizem

Računalniški terorizem (angl. Cyberterrorism) predstavlja grožnjo računalniškim sistemom organizacij ali vlade (O'Brien 2011, 537). Filozofija tega gibanja je pridobitev pomembnih informacij za napad na internetno infrastrukturo določene države ali večje svetovno znane organizacije. Na ameriški nacionalni konferenci za zakonodajo (NCSL), leta 2006, je bila oblikovana širša opredelitev računalniškega terorizma: »To je uporaba informacijske tehnologije s strani terorističnih skupin ali posameznikov, da bi dosegli svoje cilje. Za organiziranje in izvajanje svojih ciljev uporabljajo informacijsko tehnologijo, napadajo mreže računalniških sistemov, telekomunikacijsko infrastrukturo ter si izmenjujejo informacije in ustvarjajo grožnje v elektronski obliki.« Računalniški terorizem s svojimi aktivnostmi vpliva na zaslužke podjetij, ki poslujejo preko spleta, lahko pa tudi resno oslabi celotno gospodarstvo, saj podjetjem in državnim organom onemogoči dostop do ključnih virov, s tem pa se poveča dovzetnost za vojaški napad.

Internetne teroristične organizacije naj bi po trditvah Vidica (2011) v evropskem prostoru imele svoje spletne strani z radikalno islamistično propagando. Preiskovalcem največ težav povzroča jezik, ki naj bi bil v večini arabski, pa še v različnih narečjih, tako bi potrebovali več različnih prevajalcev. Na takšnih spletnih straneh naj bi se pojavljali podatki za izvajanje nalog islamističnih ekstremistov v različnih državah. Pogosto so na teh spletnih straneh prisotni tudi pozivi za različne donacije muslimanom v evropskih državah in forumi, kjer se izražajo mnenja muslimanov živečih v Evropi. Takšne spletne strani naj bi se pojavljale nekje od sredine 90. let prejšnjega stoletja, od takrat pa naj bi tudi teroristične organizacije začele uporabljati internet in njegove storitve. S pomočjo spleta naj bi po ugotovitvah Vidica (2011) teroristične organizacije objavljale zelo obširno literaturo islamističnih ideologov, strokovnjakov in učiteljev. Takšna literatura naj bi propagirala predvsem povezavo med teologijo in nasiljem. Tako opisujejo tudi načine za izdelavo improviziranih eksplozivnih sredstev ali izognitve morebitnemu nadzoru varnostnih služb. Na straneh se pojavlja tudi pisni, avdio in video material, ki javnost obvešča o džihadističnih bojih v Afganistanu in Iraku.

Internet in njegove storitve naj bi teroristom olajšala komunikacijo, načrtovanje napadov in pripravljalna dejanja. Velik problem se pojavlja s sledljivostjo in preiskovanjem spletnega terorizma. Internetno okolje prepleteno z različnimi vrstami tehnoloških tehnik uporabnikom oziroma teroristom omogoča visoko stopnjo diskretnosti (Vidic 2011, 40). Zaskrbljujoče je predvsem dejstvo, da se preko internetnih storitev informacije zelo hitro širijo. To lahko privede tudi do zelo hitre širitve terorističnih organizacij. Privrženci oziroma simpatizerji teroristični organizacij se na tak način lahko hitro in enostavno včlanijo na internetne strani, kjer pridobijo vse potrebne informacije in napotke za izvršitev terorističnih dejanj. Internet je, kot smo že omenili, prisoten povsod po svetu, zato lahko teroristične organizacije, organizirajo preko interneta teroristično dejanje kjerkoli. Iz tega vidika je internetni terorizem globalni problem, ki ga je težko omejiti.

3.3 Posledice spletnega kriminala

Splet je med uporabniki znan po tem, da jim daje občutek anonimnosti. Mislijo namreč, da jih nihče ne vidi in da so popolnoma skriti pred drugimi uporabniki spleta. Po ugotovitvah O'Briena (2011, 547) temu ni tako, kajti pravi, da je splet zelo odprt in so osebni podatki zelo dobro vidni. Splet, e-pošta, klepetalnice, itd. so na spletu na široko odprta in nezavarovana območja, ki nimajo elektronskih mej in so brez trdnih pravil o tem kaj je osebni podatek in kaj je to zasebnost. Informacije o spletnih uporabnikih so samodejno in legitimno ujete vsakič, ko uporabnik obišče določeno spletno stran. Obisk se zapiše v t. i. »piškotek«, ki je shranjen na trdem disku. Lastnik spletnih mest ali spletnih revizijskih storitev, kot je to npr. DoubleClick, lahko podatke in evidence shranjene v piškotkih prodajajo drugim strankam, kot so spletne trgovine, ki na podlagi teh podatkov oblikujejo privlačen oglas in ga uporabniku pošljejo na e-poštni naslov.

O'Brien (2011, 547) opozarja, da te podatke prestrežejo t. i. vdiralci in iz takih piškotkov pridobijo uporabniška imena in gesla do določenih spletnih strani. V primerih, ko gre za spletne strani podobne Paypalu je lahko uporabnik tudi finančno oškodovan. Uporabniki spleta lahko določene podatke in svojo zasebnost tudi zaščitijo. Obstajajo različni načini, kot je npr. šifriranje e-pošte. Drugi preprosti način je, da se uporabnik spleta ne odloči za sprejem

»piškotkov«, tako se njegovi podatki ne shranijo v »piškotke« in uporabnik ostane anonimen. V Sloveniji se je 15. 6. 2013 začela izvajati nova zakonodaja, ki ureja uporabo piškotkov. Zakonodaja je bila spremenjena na podlagi direktive o zasebnosti v elektronskih komunikacijah 2002/58/ES s strani EU. V tej direktivi je bil spremenjen člen, ki se nanaša na »piškotke in podobne tehnologije«. Spremembo direktive je prinesla spremenjena Direktiva 136/2009. V slovensko zakonodajo so jo prenesli kot »Zakon o elektronskih komunikacijah (ZEKom-1). V 157. členu »piškotki« predstavlja pravno osnovo, na podlagi katere morajo slovenski lastniki spletnih strani poskrbeti za zasebnost obiskovalcev spleta. Člen lastnikom spletnih strani nalaga upoštevanje določil Zakona o varstvu osebnih podatkov, hkrati pa dodeljuje in nalaga inšpekcijski nadzor Uradu informacijskega pooblaščenca. V primeru kršitev zakon predvideva sankcije v višini od 200 do 20.000 EUR. Informacijski pooblaščenec lahko določi globo v najnižjem znesku 1.000 EUR za pravne osebe in 200 EUR za odgovorno fizično osebo, višjo kazen pa lahko določi le sodišče (Piskotki.net b. l.).

Kot smo omenili, se s širjenjem uporabe interneta povečuje tudi število potencialnih žrtev. Žrtve so lahko pravne in fizične osebe, ali pa celo državna uprava, ki svojim uporabnikom odpira vedno več možnosti za urejanje uradnih zadev preko spleta: e-dohodnina, točka eVem, spletni portal AJPES, itd.

Države so tako začele uvajati različne programe osveščanja ljudi o nevarnostih rabe interneta. Tako je v Sloveniji, od leta 2011, prisoten nacionalni program osveščanja o informacijskih varnosti imenovan Varni na internetu, ki z izobraževalnim programom[2] skuša dvigniti zavedanje o spletnih nevarnostih. Program poteka pod okriljem SI-CERTa (Planet Siol 2012).

Ker je spletni kriminal vse bolj pereč problem in hitro rastoč problem, so države počasi začele izvajati določne ukrepe in sprejemati zakone povezane z računalniškim kriminalom. V Sloveniji imamo tako možnost prijave incidenta kar prek spletnega obrazca, preko katerega lahko oškodovanci prijavijo omrežni incident – vdor, goljufijo, krajo identitete, itd. Gre za nacionalno prijavno točko, kjer oškodovancem in tudi drugim spletnim uporabnikom pomagajo brezplačno (Planet Siol 2012).

Z že omenjenimi virusi ali »poštnimi« napadi (angl. spaming) na sisteme napadalci običajno ne povzročijo le finančne škode, temveč tudi zmešnjavo in izgubo podatkov ter zastoje pri delu. Več finančne škode povzročijo posamezniki ali kriminalne združbe z goljufijami, kot npr. lažna prodaja blaga in s krajo bančnih kartic.

Po navedbah Založnikove (2007, 4) do računalniškega kriminala v obliki spletnega terorizma še ni prišlo. (Založnik 2007, 5) ugotavlja tudi, da je splet izgubil prvotni smisel javnega prostora, saj je zaradi vse večjih napadov vdiralcev aktivistov v ospredje prišlo spletno poslovanje in ne izmenjava podatkov, znanja in razprav, kot je bilo sprva mišljeno. Splet je

[2] Http://www.varninainternetu.si.

tako postal interesni prostor za korporacije. Glavna zakonodaja, ki ščiti računalniške sisteme pred terorizmom, je tudi zakonodaja, ki zajema kršitve nižjega reda, kar pomeni, da so v tem zakonu zajeti tudi računalniški nepridipravi, ki pa niso nujno tudi računalniški teroristi.

Najbolj na udaru v spletnem prostoru so informacije. Posledice kraje spletnih informacij lahko le posredno vplivajo na naše fizično zdravje. Računalniki sami po sebi nimajo dovolj nadzora nad fizičnimi procesi brez aktivnega človeškega faktorja, da bi lahko povzročili takšno obliko in razsežnost škode, kot jo lahko povzroči klasični terorizem. Direktne posledice kriminalnih dejanj na spletu pa so v ekonomski škodi (Pollit 1997, po Založnik 2007, 4). Spletno okolje je neprestano podvrženo spletnemu kriminalu, tako je pred nekaj leti t. i. ILOVEYOU virus povzročil škodo več kot deset tisočim uporabnikom, stroški pa so bili ocenjeni na več bilijonov dolarjev. Prav tako je napad na spletne strani podjetji Yahoo, CNN, eBay, itd., ki se je zgodil februarja leta 2000 povzročil za nekaj več bilijonov škode. Neposredno se je zaradi napada zmanjšalo zaupanje drugih podjetji in posameznikov v e-trgovanje (Denning 2000, po Založnik 2007, 5). Vse to je privedlo do zmanjševanja vlaganja v ta podjetja, kar je posledično privedlo do padca cen delnic prej omenjenih podjetji.

4 RAZISKAVA KRAJE SPLETNE IDENTITETE

Naša naloga je zajemala tudi raziskavo. Tako smo v empiričnemu delu predstavili rezultate naše raziskave, ter dokončno potrdili ali ovrgli hipoteze.

4.1 Potek raziskave in predstavitev vzorca raziskave

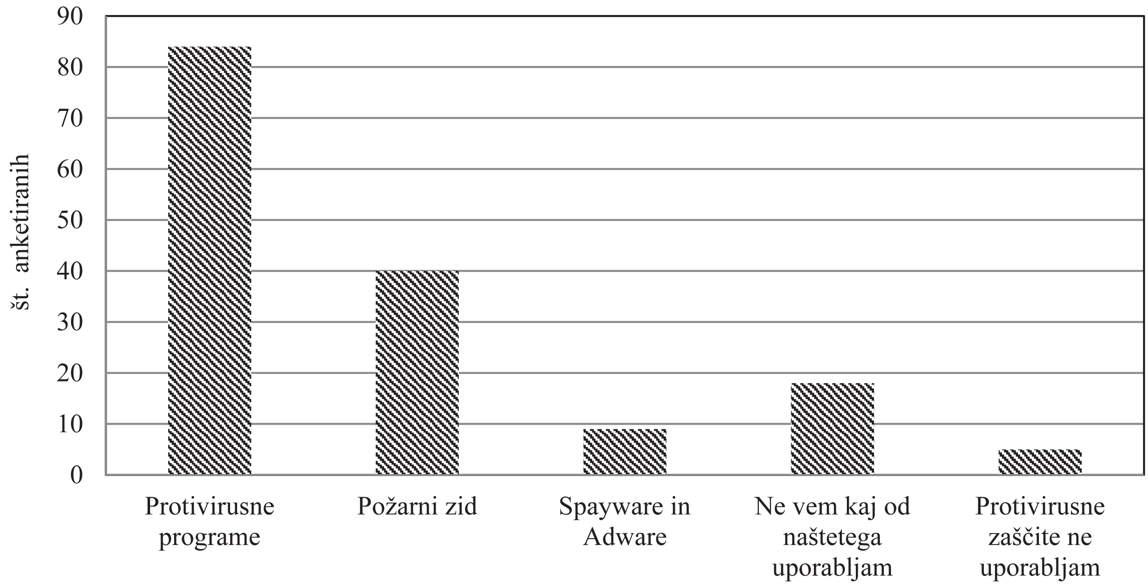
Raziskavo o poznavanju in zavedanju nevarnostih pri uporabi interneta smo naredili s pomočjo spletne ankete, narejeno s spletnim orodjem mojaanketa.si. Anketiranje je potekalo januarja 2014. Povezavo do ankete smo, s povabilom za izpolnitev ankete, poslali prijateljem in znancem preko e-pošte. Na 157 poslanih povabil se je odzvalo 120 anketirancev (76,4 % odziv). Vse prejete ankete so bile polno izpolnjene.

Med anketiranci je bilo 55 % moških. Čeprav smo v anketo vključili posameznike med 17 in 65 letom, je povprečna starost anketirancev le 22,5 leta. Anketiranci so iz različnih krajev Slovenije, prevladujejo pa kraji iz Notranjsko–kraške regije. Stopnja izobrazbe anketiranih je različna, od II. do VIII/1. stopnje.

4.2 Predstavitev rezultatov raziskave

Najprej smo anketirance vprašali, kateri operacijski sistem uporabljajo, saj so določeni operacijski sistemi manj dovzetni za spletne napade, kot so virusi, vdori v računalniški sistem, itd. Največ anketirancev (95 %) uporablja operacijski sistem Microsoft Windows, ki je tudi najbolj ranljiv, manjši del (4,8 %) pa operacijski sistem Mac OS. Le en anketiranec uporablja odprtokodni operacijski sistem Linux.

Želeli smo ugotoviti, kako anketiranci zaščitijo svoje osebne računalnike pred spletnimi napadi. Dobra polovica anketirancev (53,8 %) uporablja protivirusne programe, ki so najpogostejši način zaščite pred spletnimi napadi. Anketiranci uporabljajo npr. Eset NOD32 Antivirus, AVG, Kaspersky Anti-Virus, BitDefender Antivirus, kar je tudi najpogosteje oglaševana programska oprema proti spletnim napadom. Pri tem vprašanju je bilo ponujenih več možnih odgovorov, saj se uporabniki računalnikov, pred spletnimi napadi, lahko zaščitijo na več načinov. Poleg protivirusnih programov jih 25,6 % uporablja požarni zid, nekateri anketiranci tudi v kombinaciji s protivirusnim programom (Slika 2).

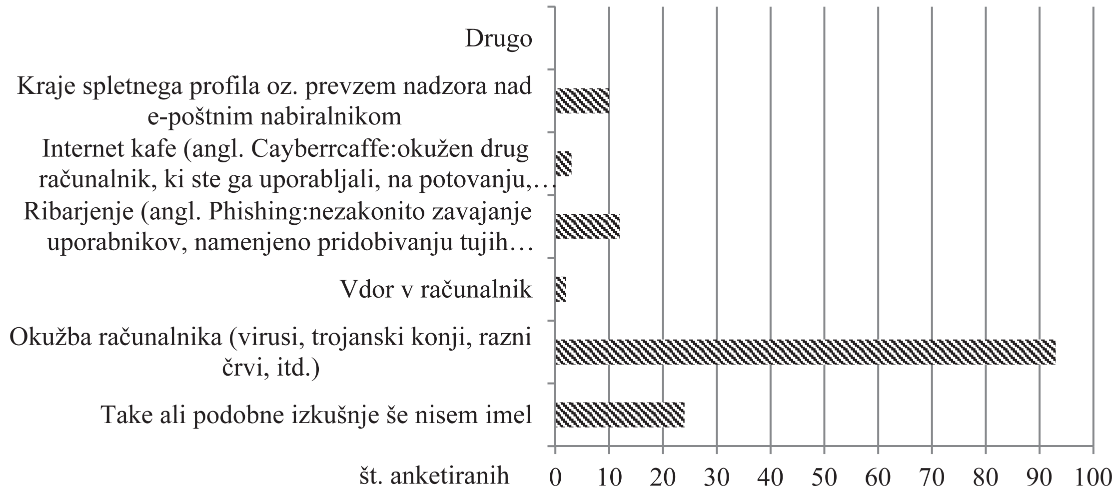


Slika 2: Uporaba zaščitne programske opreme

Nadalje smo želeli izvedeti, kako močno se anketiranci zavedajo nevarnosti, ki so jim izpostavljeni z dejavnostjo na internetu, na primer z objavo osebnih podatkov, slik, javnimi potrditvami udeleževanja na različnih dogodkih, objavo »spornih ali žaljivih« stavkov, itd. Na 5-stopenjski Likertovi lestvici (ocena je 5 je pomenila, da se anketiranci zelo zavedajo spletnih nevarnosti, ocena 1 pa je pomenila, da se jih sploh ne zavedajo) so anketiranci ocenjevali zavedanje o nevarnostih. Nevarnosti se zelo zaveda 28,3 %, medtem ko se nevarnosti ne zaveda 0,8 % anketirancev, kar kaže na to, da sledijo medijem, ki obveščajo o novih računalniških prevarah, prisotnih na internetu. Anketiranci so zavedanje o nevarnostih, ki jim pretijo pri uporabi interneta, ocenili s povprečno oceno 3,9.

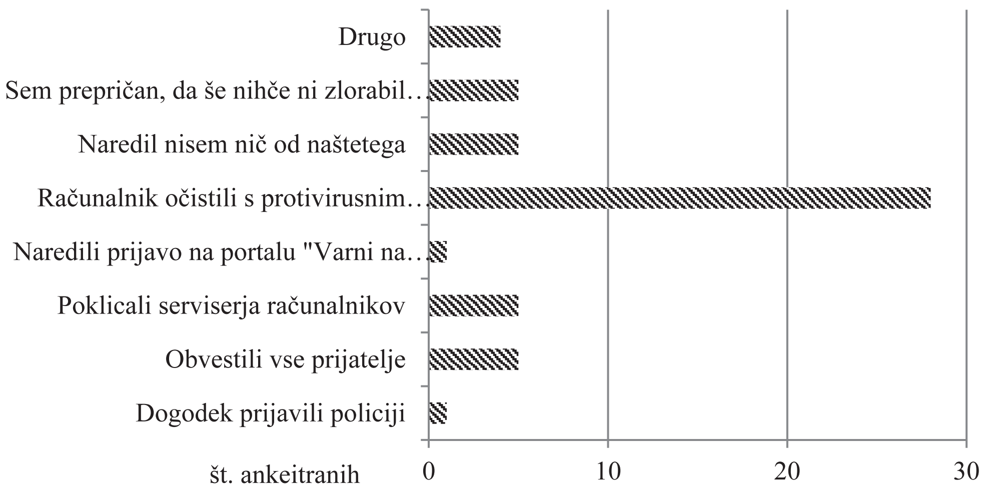
Za potrditev ali zavrnitev hipoteze smo morali izvedeti, kako močno anketiranci verjamejo spletnim aplikacijam, kot je e-nakupovanje, socialna omrežja, elektronska pošta, itd. E-storitvam sploh ne zaupa 6,7 % anketirancev, 2,5 % vprašanih pa jim zelo zaupa. Rezultati so najverjetneje odraz izkušenj anketirancev, ki so jih imeli pri uporabi spletnih storitev, zato je odvisno za katero storitev gre, oziroma za katero spletno trgovino, socialno omrežje, elektronsko pošto, itd. Povprečna ocena je v tem primeru nižja in znaša 2,8. Ocena kaže na to, da anketiranci glede varovanja osebnih podatkov in varnosti niso pretirano zaupljivi do prej omenjenih spletnih storitev.

Zanimalo nas je tudi, ali so anketiranci že imeli izkušnjo s spletnim napadom in, če so jo imeli, za katero obliko spletnega napada je šlo. Med anketiranci se jih je največ srečalo z virusnimi okužbami računalnika, saj jih je na to vprašanja odgovorilo (77,5 %). Težav povezanih s spletnim napadom ni imelo 16,6 % vprašanih. Vse ostale podrobnosti so razvidne iz slike 3. Anketiranci so lahko izbrali več možnosti.



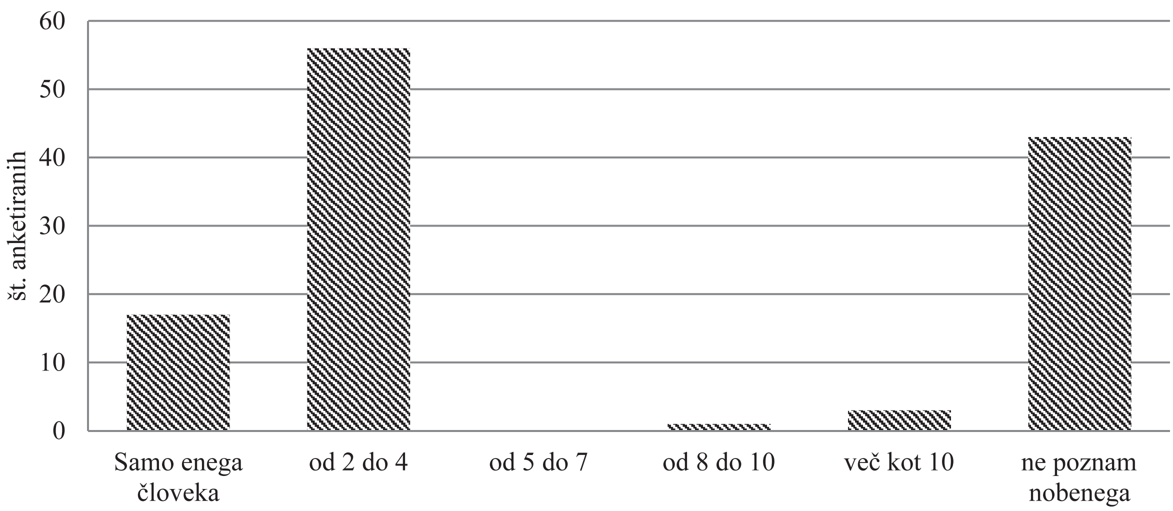
Slika 3: Vrste spletnih napadov, ki so jih zaznali anketiranci

Iz slike 3 je razvidno, da se je 32,5 % anketiranih že srečalo s spletnim napadom. Predvidevali smo, da so se anketiranci že srečali s spletnimi napadi, zato nas je zanimalo, kako so se odzvali na napad kraje spletne identitete. Pri odzivu na spoznanje, da so žrtev zlorabe, so anketiranci lahko izbirali med več možnostmi, saj se je na spletni napad možno odzvati na več načinov. Tako so anketiranci, v primeru okužbe z virusi, svoj računalnik najpogosteje očistili s protivirusnim programom (Slika 4). Le po 1 anketiranec je dogodek prijavil policiji, ali pa na portalu »Varni na internetu«.



Slika 4 : Odziv anketirancev ob spoznanju, da so bili žrtev spletne kraje identitete

Z anketo smo med drugim želeli preveriti tudi, kako pogosta je kraja identitete. Več kot polovica anketirancev (67,5 %) še ni bila žrtev kraje spletne identitete, zato nas je zanimalo, ali poznajo koga, ki je že bil žrtev. Rezultate prikazujemo na sliki 5.



Slika 5: Število poznanih, ki so že bili žrtev spletne kraje identitete

V nadaljevanju nas je zanimalo, kako so anketiranci seznanjeni z razširjenostjo kraje spletne identitete po svetu. Dobra desetina anketirancev (12,5 %) meni, da kraja identitete lahko ogrozi do 10 % uporabnikov interneta, medtem ko jih 45,9 % meni, da je pojav bolj razširjen in je ogroženih nad 10 do 40 % vseh uporabnikov interneta. Ostali anketiranci (35,8 %) so menili, da je ta pojav razširjen med 40 in 60 % uporabnikov interneta. Le 5,8 % anketirancev meni, da je kraja identitete na internetu razširjena med 60 in 100 % uporabnikov interneta.

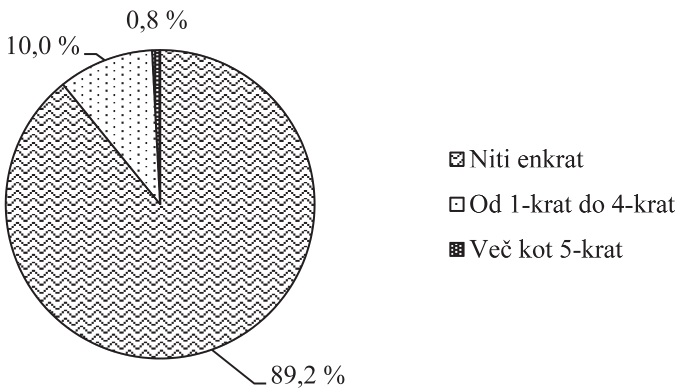
Anketiranci so svojo seznanjenost, oziroma osveščenost z nevarnostmi na internetu ocenjevali na 5-stopenjski Likertovi lestvici, kjer je ocena 1 pomenila zelo nizko osveščenost, ocena 5 pa zelo visoko osveščenost. Povprečna ocena tega vprašanja znaša 3,6.

V zadnjem času se je razširil virus po imenu Ukash (Slika 6). Pravzaprav gre za spletno prevaro, ki uporabniku pod pretvezo, da gre za kaznivo dejanje, zaklene računalnik in od uporabnika zahteva plačilo globe. Iz tega razloga smo želeli raziskati, ali so se anketiranci že srečali s takšnim primerom.

Slika 6: Primer virusa Ukash

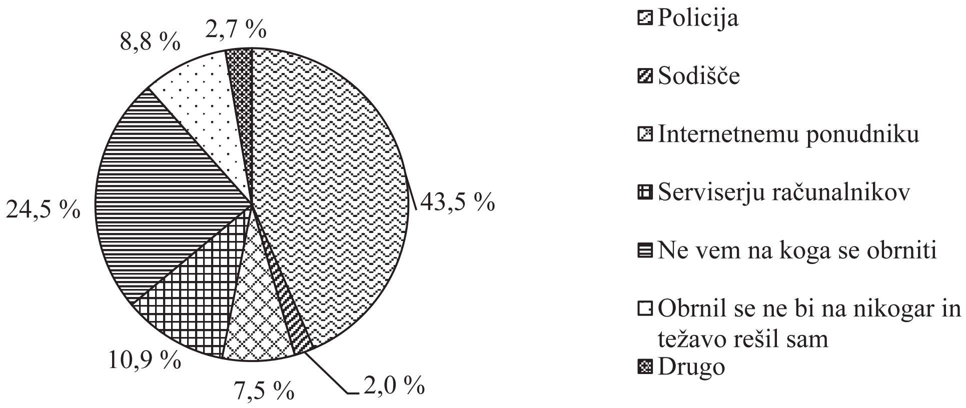
Vir: Krofeksecurity 2013.

Kot je razvidno iz slike 7 se 89,2 % anketirancev še ni srečala z omenjenim virusom. Ostale podrobnosti so razvidne iz slike 7.



Slika 7: Srečanje s sliko računalniškega virusa

Z zadnjim vprašanjem smo želeli izvedeti, na katero ustanovo bi se anketiranci obrnili v primeru, če bi bili žrtev kraje spletne identitete. Skoraj polovica anketirancev (43,5 %) bi krajo spletne identitete prijavila policiji. Skoraj četrtina anketirancev (24, 5 %) pa ne ve, na koga bi se lahko obrnila. Vse ostale podrobnosti so razvidne iz slike 8.



Slika 8: Posredovanje računalniškega incidenta odgovornim ustanovam

4.3 Ugotovitve raziskave

V začetku naloge smo si zastavili trditve, ki smo jih želeli preveriti na vzorcu anketirancev.

Hipoteza 1 – Več kot polovica anketirancev, uporabnikov interneta, se ne zaveda nevarnosti računalniškega kriminala.

Predvidevali smo, da se uporabniki interneta ne zavedajo nevarnosti računalniškega kriminala, kar je pokazala tudi raziskava. Povprečna ocena 3,6 je najbrž posledica, da mediji opozarjajo na računalnišk prevare oziroma goljufije. Oceno 4 je izbralo 17,3 %, oceno 5 pa 8,1 % anketiranih. Na podlagi teh ugotovitev lahko hipotezo ovržemo.

Hipoteza 2 – Več kot 50 % anketirancev je že bilo žrtev kraje identitete na spletu.

Glede na to, da je 1,4 % anketiranih bilo žrtev vdora v računalnik in da je 6,9% anketiranih imelo ukraden profil na eni izmed storitev spleta (Facebook, Gmail, itd.), lahko predvidevamo, da je bilo manj kot 50 % anketiranih že žrtev kraje identitete na spletu. Na podlagi dobljenih podatkov te hipoteze ne moremo potrditi.

Hipoteza 3 – Več kot 60 % anketirancev ne ve, v kolikšni meri je kraja identitete razširjena po svetu.

Dobljeni rezultati so pokazali, da 94,2 % anketiranih misli, da je ta pojav razširjen do 60 % vseh uporabnikov interneta, vendar se o tem motijo. Razširjenost kraje spletne identitete se v svetu giblje med 60 % in 100 % vseh uporabnikov interneta. Na podlagi teh podatkov hipotezo sprejmemo.

Hipoteza 4 – več kot 70 % anketirancev uporablja socialna omrežja, in se pri tem, ko objavlja svoje podatke (slike, letnice, naslove, itd.), ne zaveda nevarnosti zlorabe njihove identitete

Dobljena povprečna ocena je 3,9. Nevarnosti se tako zaveda več kot 80 % anketirancev, zato tudi te hipoteze ne moremo sprejeti.

Hipoteza 5 – več kot pol anketirancev v primeru zlonamernega napada na svoj računalnik ne pozna ustreznih načinov posredovanja problema ustanovam.

Raziskava je pokazala, da bi 43,5 % anketiranih v primeru ugotovitve zlonamernega napada na njihov računalnik o tem obvestilo policijo. Smotrne reakcije ne bi izbralo 24,5 % anketiranih, ostalih 32 % bi izbralo dobro ali deloma dobro reakcijo. Na podlagi vseh ugotovitev, moramo hipotezo ovreči.

5 SKLEP

Z diplomskim delom smo predstavili in raziskali področje računalniškega kriminala. Osredotočili smo se predvsem na vse bolj aktualen in prisoten problem t. i. krajo spletne identitete. Kraja identitete je nepooblaščeno prevzemanje osebnih podatkov druge osebe, v primeru, ko se to zgodi preko internetnih storitev (npr. Facebook), gre v takem primeru za krajo spletne identitete. Ljudi, ki nepooblaščeno prevzemajo oziroma kradejo identitete preko internetnih storitev in računalniških sistemov imenujemo vdiralci (angl. Hackers). Vdiralci lahko delujejo posamezno, ali pa so organizirani v skupine. V večini primerov gre za združbe, saj so le te bolj učinkovite in pri svojih dejanjih bolj uspešne. Vdiralci lahko s svojim početjem povzročijo veliko škode na gospodarskem področju, pa tudi na ugledu. Posamezniki, poleg finančnih, pogosto utrpijo tudi psihične posledice. Proti vdiralcem deluje policija (kriminalistični oddelek za računalniški kriminal), tožilstvo in druge pristojne organizacije (varninainternetu.si).

Zavedanje nevarnosti in izkušnje s krajo spletne identitete smo raziskali s pomočjo spletne ankete. Anketa je bila polno izpolnjena pri 120 anketirancih, v večini primerov so bili to naši prijatelji in znanci. Povabilo za izpolnitev ankete smo jim poslali preko e-pošte. Raziskava je pokazala, da so anketiranci zelo dobro osveščeni o vseh internetnih oziroma spletnih nevarnostih, se jih zavedajo in poskrbijo za varnost svojih računalniških sistemov (slika 2 in slika 5). S slike 3 je razvidno, da je 83,3 % anketirancev že imelo izkušnjo z enimi izmed spletnih napadov. Glede na to, da so anketiranci zelo dobro osveščeni o spletnih nevarnostnih, smo pričakovali, da bodo v večini vedeli, v kolikšni meri je kraja spletne identitete razširjena v svetu, vendar je na to vprašanje pravilno odgovorilo le 5,8 % anketiranih. Uporaba družabnih omrežjih je vse večja, s tem pa se pojavlja vse več objav, katerih vsebina je osebne narave (npr. slike, letnice rojstva, potrditev udeležbe na dogodkih, itd.). Zanimalo nas je v kolikšni meri se anketiranci zavedajo nevarnostni kraje spletne identitete, ki so ji izpostavljeni s takšnim načinom obnašanjem na družabnih omrežjih. Podatki, ki smo jih dobili na to vprašanje so pokazali, da se naši anketiranci zelo zavedajo teh nevarnosti, saj je povprečna ocena zavedanja, na 5-stopenjski lestvici, 3,9. Kajti na veliko javnih mestih je moč opaziti takšne ali drugačne letake, zgibanke, plakate, itd. za pomoč odvisnikom, nasilju v družini, itd. S slike 8 je razvidno, da večina anketirancev ve na katero pristojno ustanovo naj se obrne v primeru računalniške prevare.

Med pisanjem diplomskega dela smo ugotovili, da bi za omejevanje in preprečevanje računalniškega kriminala lahko naredili še veliko. Predvsem lahko veliko naredimo sami, saj s svojim ravnanjem zlonamernežem pogosto olajšamo delo. Po drugi strani bi radi opozorili na predvidene kazni za storilce, ki so zelo mile, posebno, če gledamo na to, da z zlonamernim dejanjem nekomu, ki je bil žrtev kraje identitete na spletu, lahko uničimo življenje. Čeprav se o preventivi v medijih veliko govori in piše, pa pogrešamo poudarek o tem, kako in kaj narediti v primerih , ko smo žrtev računalniškega kriminalnega dejanja.

Po našem mnenju bi tudi storilci bili manj aktivni, če jim uporabniki ne bi dajali povoda za njihovo početje. To pomeni, da sami uporabniki z določenimi aktivnostmi spodbudimo vdiralce oziroma hekerje. Vdiralci, katerim motiv je intelektualni izziv, bodo vlagali več energije v zrušitev neke varnostne programske opreme, ki velja za najbolj učinkovito na tržišču. Tudi hranjenje zaupnih podatkov na serverjih podjetji dajejo vdiralcem povod, saj jih take vrste podatki zanimajo. To pomeni, da vdiralcem katerim glavni motiv je ekonomske narave, bodo hoteli priti do finančnih podatkov klientov banke, saj bi jim lahko na takšen način izpraznili račune. Naslednje področje je povezano s kaznimi in sicer se izboljšave nanašajo na sam zakon. Premalo je zakonov, ki opredeljujejo varovanje osebnih podatkov na spletu oziroma internetu. Na določenih spletni straneh predvsem so to spletne trgovine, morajo uporabniki vnesti toliko osebnih podatkov, kot da bi bili pred policijskim preiskovalcem, tako bi lahko zakon določal kateri osebni podatki so lahko zahtevani s takšnih strani in katere ne.

Z upoštevanjem vseh naštetih izboljšav in njihovim sodelovanje ter povezovanjem med seboj, bi se lahko za preprečevanje računalniškega kriminala storilo veliko. Vendar pa je najbolje da vsak uporabnik interneta in njegovih storitev sam pri sebi razjasni kako se mora obnašati na spletu. Kajti največkrat smo si uporabniki sami krivi za neljube dogodke povezne z računalniškim kriminalom, saj se preveč izpostavljamo in delujemo predvsem naivno in nespametno.

LITERATURA IN VIRI

Ahemahem. B.l. *Why is The Fifa 14 Crack Taking Time?* Http://www.ahemahem.com/fifa-14 crack-will-take-time-buy-original-game-instead/693/ (27. 10. 2014).

Cross Domain Solutions. *Cyber Crime*. Http://www.crossdomainsolutions.com/cyber-crime/ (12. 3. 2015).

Dobovšek, Bojan. 1997. *Organizirani kriminal*. Ljubljana: Založba Unigraf.

Eurostat. 2015. *Households - devices to access the internet*. http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do;jsessionid=ZfpCbbJf ZjGs4PblkvGzoIGVoUObWK5jUKmP6r0_nwLeImX3ctNg!-1585438010

Go-Gulf. 2013. *Cyber Crime Statistic and Trends.* Http://www.go-gulf.com/blog/cyber-crime/ (18.10.2014).

Grubelnik, Vladimir. B. l. *Astronomija na internetu.* Http://lizika.pfmb.uni-mb.si/~vlado/astro/astro/astro.pdf (25. 10. 2014).

Harrell, Erika in Lynn Langton. 2013. *Victims of Identity Theft 2012*.. Http://www.bjs.gov/content/pub/pdf/vit12.pdf (23. 10. 2014).

Informacijski pooblaščenec RS. B. l. *Smernice za preprečevanje kraje identitete*. Https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_kraja_identitete.pdf (1. 10. 2014).

IWS (Internet World Stats). 2013. *Internet Usage Statistics.* Http://www.internetworldstats.com/stats.htm (5. 6. 2014).

Kazenski zakonik (KZ-1-UPB2). *Uradni list RS*, št. 50/2012.

Kocmur, Helena. 2004. *Računalniški kriminal postal svetovni problem*. Delo. Ljubljana.

Kovačič, Matej. 2006. *Kiberkriminal v Sloveniji*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Kroferksecurtiy. 2013. *Odstranitev virusa Ukash.* Http://www.krofeksecurity.com/novice/odstranitev-virusa-ukash/ (11. 5. 2014).

Laudon, Kenneth C. 2012. *Management Information System: Managing the Digital Firm.* 12. izdaja. London: Pearson Prentice Hall.

Merriam-Webster. B. l. *Identity*. Http://www.merriam-webster.com/dictionary/identity (21. 3. 2015)

MNZ Policija. 2014. *Poročilo o delu policije v letu 2013.* Ljubljana: Ministrstvo za notranje zadeve.

O'Brien, James A. 2011. *Managment Information System.* 10. izdaja. New York: McGraw-Hill/Irwin.

Piskotki.net. B. l. *Zakonodaja o piškotkih.* Http://piskotki.net/zakonodaja-o-piskotkih/

Planet Siol.net. 2012. *V letu 2011 skoraj podvojitev števila spletnih goljufij in kraje identitet.* Http://www.siol.net/novice/tehnologija/racunalnistvo/2012/02/spletne_goljufije_in_kraje _idenidenid.aspx (6. 5. 2014).

Podjed, Dejan. 2008. *Računalniški kriminal*. Magistrsko delo, Univerza v Ljubljani, Fakulteta za pravo.

RIS (Raba interneta v Sloveniji). 2008. *Ocena število uporabnikov interneta – 4. preglednica*. Http://www.ris.org/index.php?fl=0&id=1183 (6. 5. 2014).

RIS (Raba interneta v Sloveniji). 2013. *Podpis kodeksa ravnanja izvajalcev javnih elektronskih komunikacijskih storitev za zaščito uporabnikov*. Http://www.ris.org/db/26/12530/Novice/Dan_varne_rabe_interneta_slovenski_mobilni_operatoper_in_internetni_ponudniki_podpisali_kodeks_za_zascito_uporabnikov/?&p1=276&p2=285&p3=1318&p4=1319 (20.10.2014).

Rupnik, Andrej. 2003. *Konvencija o kibernetski kriminaliteti.* Http://uploadi.www.ris.org/editor/1216115785Konvencija%20o%20kibernetski%20kriminalitkri%20Andrej%20Rupnik.PDF (30. 9. 2014).

SI-CERT. B. l. *Kraja identitete.* Https://www.cert.si/si/varnostne-groznje/kraja-identitete/ (1. 10. 2013).

Siciliano, Robert. 2011. *7 Types of Hacker Motivations. McAfee Blog Central.* Https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations (5. 5. 2014).

Strošar, Edi. 2008. *Vrivanje SQL od A do Ž. Monitor.* Http://www. monitor.si/clanek/vrivanje-sql-od-a-do-z/123404/ (20. 10. 2014).

SURS. 2013. *Uporaba interneta v gospodinjstvih in pri posameznikih, Slovenija, 2013 - končni podatki.* Http://www.stat.si/novica_prikazi.aspx?id=5795 (18. 10. 2014).

Šket, Ines. 2009. *Psihološke implikacije kiberprostora ter interakcije med storilci in žrtvami*. Diplomsko delo, Univerza v Mariboru, Fakulteta za varnostne vede.

Tomšič, Matic. 2015. *Kako dolgo še, preden hekerji zavladajo spletu (in svetu)?* Http://www.siol.net/novice/tehnologija/racunalnistvo/2015/01/2015_leto_hekerskih_napadov_hekerji.aspx (6. 1. 2015).

Turban, Efraim, Gregory Wood in Linda Volonino. 2013. *Information Technology for Management.* 9. izdaja. New Jersey: Aptara.

Vidic, Matjaž. 2011. *Ekstremizmi na internetu*. Magistrsko delo, Univerza v Ljubljani, Fakulteta za družbene vede.

Yar, Majid. 2006. *Cybercrime And Society*. London: SAGE Publications.

Zakon o elektronskih komunikacijah (ZEKom-1). *Uradni list RS*, št. 109/2012.

Založnik, Pika. 2007. *Konstrukcija kiberterorizma*. Http://www.memefest.org/works/699-13f898e12/konstrukcija_kiberterorizma.pdf (6. 5. 2014)

Završnik, Aleš. 2005. Kibernetična kriminaliteta: (kiber)kriminološke in (kiber)viktimiološke posebnosti »informacijske avtoceste«. Revija za kriminalistiko in kriminologijo 3 (56): 248-264.

PRILOGA

Priloga 1 Spletni vprašalnik

SPLETNI VPRAŠALNIK

Raziskava o kraji spletne identitete.

Pozdravljeni!
V svoji diplomski nalogi bi rad raziskal krajo identitete na spletu. Za pripravo naloge potrebujem vašo pomoč. Prosim, da si vzamete 5 minut časa in odgovorite na anonimno anketo. Podatki zbrani z anketo bodo uporabljeni le za potrebe diplomske naloge.
Hvala za vašo pomoč.

1. Kateri operacijski sistem imate nameščen na vašem osebnem računalniku? (možnih je več odgovorov)

- ☐ MS-DOS
- ☐ Windows (95/98/NT/2000/XP/Vista/7/8 ali katerokoli drugo različico)
- ☐ Unix (katerakoli različica)
- ☐ Linux (katerakoli različica)
- ☐ Mac OS (katerakoli različica)
- ☐ Računalnika ne uporabljam
- ☐ Drugo

2. Katero protivirusno zaščito uporabljate? (možnih je več odgovorov)

- ☐ Protivirusne programe
- ☐ Požarni zid
- ☐ Spayware in Adware
- ☐ Ne vem kaj od naštetega uporabljam
- ☐ Protivirusne zaščite ne uporabljam
- ☐ Drugo

3. Kako močno se zavedate nevarnosti, ki prežijo na internetu, z objavo vaših osebnih podatkov, slik, potrditev udeleževanja raznih prireditev, objavo »spornih ali žaljivih« stavkov, itd.?

	1	2	3	4	5	
Se ne zavedate	☐	☐	☐	☐	☐	Zelo se zavedate

4. Kako močno ste seznanjeni z vsemi nevarnostmi, ki prežijo na internetu (virusi, kraja profilov, kraja elektronski potrdil, vdori v e-pošto, itd.)?

	1	2	3	4	5	
Sploh niste seznanjeni	☐	☐	☐	☐	☐	Zelo ste seznanjeni

5. Kako močno zaupate internetnim trgovinam, socialnim omrežjem, ponudnikom elektronskih poštnih predalov, itd.?

	1	2	3	4	5	
Sploh jim ne zaupate	☐	☐	☐	☐	☐	Popolnoma jim zaupate

6. S katero vrsto zlorabe oziroma napada na vaš računalnik ste imeli izkušnjo? (možnih je več odgovorov)

☐ Take ali podobne izkušnje še nisem imel

☐ Okužba računalnika (virusi, trojanski konji, razni črvi, itd.)

☐ Vdor v računalnik

☐ Ribarjenje (angl. Phishing:nezakonito zavajanje uporabnikov, namenjeno pridobivanju tujih osebnih podatkov)

☐ Internet cafe (angl. Cayberrcaffe:okužen drug računalnik, ki ste ga uporabljali, na potovanju, šoli, v kavarni, itd.)

☐ Kraje spletnega profila oziroma prevzem nadzora nad e-poštnim nabiralnikom

☐ Drugo

7. Kolikokrat ste se srečali z takšno ali podobno sliko pri uporabi računalnika oziroma interneta?

☐ Niti enkrat

☐ Od 1-krat do 4-krat

☐ Več kot 5-krat

8. Kaj ste naredili, takrat ko ste izvedeli, da ste bili žrtev kraje spletne identitete oziroma zlorabe vaših podatkov? (možnih je več odgovorov)

- ☐ Dogodek prijavili policiji
- ☐ Obvestili vse prijatelje
- ☐ Poklicali serviserja računalnikov
- ☐ Naredili prijavo na portalu "Varni na internetu"
- ☐ Računalnik očistili s protivirusnim programom
- ☐ Naredil nisem nič od naštetega
- ☐ Sem prepričan, da še nihče ni zlorabil mojih podatkov, saj imam dobro zaščiten računalnik in vem kaj počenem
- ☐ Nisem še opazil, da bi kdo zlorabil moje podatke
- ☐ Drugo

9. Koliko ljudi poznate, ki so bili žrtev takšne ali drugačne spletne prevare oziroma kraje osebnih podatkov?

- ☐ Samo enega človeka
- ☐ od 2 do 4
- ☐ od 5 do 7
- ☐ od 8 do 10
- ☐ več kot 10
- ☐ ne poznam nobenega

10. Kaj mislite o tem, v kolikšni meri je spletna kraja identitete razširjena v svetu?

- ☐ do 10% vseh uporabnikov interneta
- ☐ od 10% do 40% vseh uporabnikov interneta
- ☐ od 40% do 60% vseh uporabnikov interneta
- ☐ od 60% do 100% vseh uporabnikov interneta

11. V primeru, da bi bili žrtev kraje spletne identitete na koga bi se obrnili? (možnih je več odgovorov)

- ☐ Policijo
- ☐ Sodišče
- ☐ Internetnega ponudnika
- ☐ Serviserja računalnikov
- ☐ Ne vem na koga se je potrebno obrniti
- ☐ Obrnil se nebi na nikogar, in težavo rešil sam

☐ Drugo ☐

Zahvaljujem se vam za sodelovanje v anketi.