UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

ZAKLJUČNA PROJEKTNA NALOGA

HELENA MAKSIMOVIĆ

KOPER, 2019

2019
ZAKLJUČNA PROJEKTNA NALOGA
HELENA MAKSIMOVIĆ

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

Zaključna projektna naloga

HEKERSTVO IN NJEGOV VPLIV NA PODJETJA

Helena Maksimović

Koper, 2019

Mentor: doc. dr. Uroš Godnov

POVZETEK

Hekerstvo se nanaša na dejavnosti, katerih cilj je ogroziti digitalne naprave kot so računalniki, mobilne naprave, omrežja ipd. Namen hekerstva ni vedno zlonameren a večina referenc danes označuje ta pojav kot neko nezakonito dejavnost, ki jo izvajajo kibernetski kriminalci oz. hekerji, katerih motivacija izhaja iz finančnega dobička, zbiranja informacij itn. Hekerji pa so ne nazadnje del kibernetskega (spletnega) kriminala, ki je v zadnjem času postal zelo velika grožnja tako podjetjem kot domačim uporabnikom interneta. Kibernetski kriminal je pravzaprav kot vsak drugi kriminal saj je delo kriminalcev ampak tistih, ki imajo tehnološke spretnosti in uporabljajo internet za doseganje svojih zlonamernih ciljev. Kot osnovo za razumevanje obravnavanega problema in tematike smo predstavili hekerstvo in hekerje ter spletni kriminal. Zaključna projektna naloga je deljena na dva dela in sicer v prvem delu smo preučili in teoretično predstavili kaj je hekerstvo in hekerji ter kaj sploh je spletni (kibernetski) kriminal in vrste le-tega. V drugem delu, pa smo s pomočjo intervjujev pridobili informacije kako se lahko domači uporabniki in podjetja zaščitijo pred hekerskimi napadi ter kako država poskrbi za podjetja in fizične osebe v primeru hekerskih napadov (zakonska ureditev tega področja).

Ključne besede: poslovna informatika, hekerji, hekerstvo, spletni kriminal, e-kriminal, heker, etični heker, varovanje podatkov.

SUMMARY

Hacking refers to activities aimed to jeopardize digital devices such as computers, mobile devices, networks, etc. The purpose of hacking is not always malicious, but most references today mark this phenomenon as an illegal activity carried out by cybercriminals so-called hackers, whose motivation derives from financial gain, collection of information, etc. Hackers are, however, part of the cybercrime, which has recently become a very serious threat to both businesses and home users of the Internet. Cybercrime is actually like any other crime because it is the work of criminals, but those who have technological skills and use the Internet to achieve their malicious goals. Hacking, hackers and cybercriminal were presented as the basis for understanding the problem and topic discussed. The final project assignment (thesis) is divided into two parts: in the first part we examined and theoretically presented what is hacking and hackers, and what is cybercrime and its types. In the second part, through interviews, we obtained information on how domestic users and businesses can be protected from hacking attacks and how the government provides for businesses and individuals in case of hacking attacks (legal regulation of this area).

Key words: business informatics, hackers, hacking, cybercriminal, e-crime, hacker, ethical hacker, data protection.

UDK: 004.056.53:330.526.33(043.2)

ZAHVALA

Mentorju doc. dr. Urošu Godnovu se iskreno zahvaljujem za vse strokovne nasvete ter pomoč pri izdelavi zaključne projektne naloge. Prav tako se mu zahvaljujem za vso podporo, motivacijo in spodbudne besede, ki mi jih je namenil tekom študija. In ne nazadnje se mu zahvaljujem, ker je tako na študijskem kot življenjskem področju enkraten mentor. Hvala!

Za izkazano podporo, spodbudo, potrpežljivost in ljubezen se zahvaljujem tudi svoji družini, ki me je v času študija spremljala ter več čas podpirala in bodrila. Zahvaljujem se jim, da so mi ves čas stali ob strani tako v dobrem in v slabem.

VSEBINA

PONAZORILA

KRAJŠAVE

DoS	zavrnitev storitve (angl. *denial of service*)
ECHELON	prvotno tajno vladno kodno ime kasneje program za nadzor, ki ga uporabljajo Združene države s pomočjo štirih drugih držav, ki so podpisale varnostni sporazum UKUSA
FBI	zvezni preiskovalni urad
HTML	označevalni jezik za izdelavo spletnih strani
IBM	International Business Machines Corporation
IT	informacijska tehnologija
MIT	Tehnološki inštitut Massachusettsa
SI-CERT	Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij
Svet ES	Svet mednarodnih svetovalcev za elektronsko poslovanje (angl. *International Council of Electronic Commerce Consultants*)
UNIX	omrežni, prenosljiv, večopravilni in večuporabniški operacijski sistem
URL	naslov spletnih strani v svetovnem spletu

1 UVOD

Živimo v času, ko se tako tehnologija kot način življenja stalno spreminjata. Tehnologija se iz dneva v dan vse bolj razvija in posledično postaja vse bolj napredna, rezultat tega pa je, da se naš način življenja prilagodi tem spremembam oziroma napredku. Pravzaprav pa se s tehnologijo srečamo že, ko se zbudimo, ko na mobilnem telefonu ugasnemo budilko, ali pa, ko stopimo iz hiše, npr. odklepanje avta z daljinskim ključem, plačevanje v trgovini s plačilno kartico, v šolah, na televiziji, računalnikih, mobilnih telefonih itd. Tako je torej skoraj vsak naš korak povezan s tehnologijo, ampak pojavljajo se vprašanja: »Ali je ta tehnologija postala preveč napredna za človeka? Ali tehnologija lahko škodi človeku ali pa nekemu podjetju? Ali je človek postal preveč odvisen od tehnologije?« Naše osebno življenje je postalo enostavno preveč odvisno od tehnologije, ki jo je ustvaril prav človek (Ramey 2012).

Tehnologija in tehnološki napredek sta s seboj prinesla kar nekaj sprememb tako v vsakdanjem življenju kot tudi na področju poslovanja podjetij. Razvoj interneta in tehnologije ni prispeval le k hitrejšemu pretoku informacij in krajšemu času delovnih procesov, ampak tudi na področju hekerstva in spletnega kriminala. Spremembe, ki jih je prinesla digitalna doba, so zagotovo dobre in so v dobro posamezniku kot tudi podjetjem. Poleg pozitivnih sprememb, ki jih je prinesel tehnološki napredek, pa je to vplivalo tudi na razvoj slabih oziroma zunanjih dejavnikov, kot je hekerstvo in spletni kriminal. Naredil nas je tudi bolj ranljive. Hekerji so v vseh teh spremembah našli »luknje« oziroma pomanjkljivosti, ki so jih lahko izkoristili v druge namene, kot npr. za vdor v sisteme, krajo denarja z osebnega računa, vdor v poštni račun ipd.

Rezultat razvoja in tehnološkega napredka pa niso samo prednosti za ljudi in podjetja, temveč so to tudi pomanjkljivosti, ki bi jim morali posvečati več pozornosti. Ena izmed teh je zagotovo varnost na spletu. Hekerji lahko ustvarijo različne viruse, ki lahko dostopajo do vaših osebnih podatkov na računalniku, kot so ime in priimek, naslov prebivališča, bančni podatki in druge informacije, ki so uporabljene na spletu. Do teh informacij lahko dostopajo »hudodelci«, ki jih nato uporabijo oziroma izkoristijo v druge namene, kot so npr. kraja denarja z bančnega računa, kraja identitete ipd., prav tako pa lahko uničijo tudi druge dragocene podatke, ki jih hranite na svojem računalniku (Edraw b. l.).

V današnjem tehnološko povezanem svetu in času se ljudje ne zavedajo nevarnosti, ki jim pretijo v virtualnem svetu. Čeprav večina meni, da so dobro informirani in so seznanjeni s to nevarnostjo, se v resnici ne zavedajo, kakšne posledice pravzaprav lahko prinese spletni kriminal. Spremembe v virtualnem svetu se dogajajo vsakodnevno, prav tako pa se razvijajo nove tehnologije, ki jim je težko slediti. A hekerstvo obstaja že nekaj časa, toda ne v taki obliki, kot ga poznamo danes. V 40-ih letih prejšnjega stoletja so kriptografi iz Bletchley parka uspeli dešifrirati Enigmo (električna naprava za šifriranje sporočil), ki so jo uporabljale nemške oborožene sile med 2. svetovno vojno. Lahko bi rekli, da pravzaprav ta dogodek predstavlja »rojstvo« hekerstva, čeprav v tistem času ni bil poimenovan tako. Besedi

»hekanje« in »hekerstvo« sta se prvič pojavili v tem smislu na Tehnološkem inštitutu v Massachusettsu (MIT) sredi petdesetih let, le nekaj minut pred sestankom inštituta Tech Model Railroad Club (IT PRO 2017).

Hekerstvo in spletni kriminal sta temi, za kateri ne obstaja veliko literature na spletu in v knjižnicah, prav tako pa je bilo na tem področju izvedenih zelo malo raziskav, zato smo se odločili v naši zaključni projektni nalogi raziskati prav ta dva pojava. Glavni problem, ki ga želimo obravnavati v naši zaključni projektni nalogi, je, kako se lahko posamezniki in podjetja zavarujejo pred hekerskimi napadi ter spletnim kriminalom. Spletni kriminal je postal v zadnjem času zelo pogost, še posebej med fizičnimi osebami, saj so prav te osebe bolj »ranljive«, ker niso dovolj poučene o spletnem kriminalu.

V tej nalogi se bomo osredotočili na »predstavitev« hekerstva in spletnega (kibernetskega kriminala) ter seznanitev tako posameznikov kot podjetij o nevernostih, ki jim pretijo na spletu, in o njegovih negativnih posledicah za poslovanje podjetij. Ker se z napredkom tehnologije in s stalnimi spremembami, ki se dogajajo na tem področju, stvari neprestano spreminjajo, želimo predstaviti, katere oblike hekerskih napadov obstajajo, kdo so tarče hekerjev, kako napadi vplivajo na podjetja in posameznike ter preventivne ukrepe proti tovrstnim napadom. Prav tako bomo teorijo podprli z nasveti slovenskih strokovnjakov s področja spletnega kriminala, ki jih bomo pridobili preko intervjujev. Predvsem želimo raziskati in pojasniti oziroma razložiti to tematiko, da bo razumljiva tudi najbolj preprostim uporabnikom spleta kot tudi podjetnikom, ki se srečujejo s tovrstnimi težavami med poslovanjem podjetja.

1.1 Opredelitev področja in raziskovalnega problema

Hekerstvo se nanaša na dejavnosti, ki si prizadevajo ogroziti digitalne naprave, kot so računalniki, tablični računalniki in celo vsa omrežja. Namen hekerstva ni vedno zlonameren. Dandanes večina referenc o hekerstvu in hekanju označuje ta dva pojava kot nezakonito dejavnost, ki jo izvajajo motivirani kibernetski kriminalci, ki so bodisi motivirani zaradi finančnega dobička, protesta, zbiranja informacij (angl. *»spying«*) ali pa celo samo za »zabavo« in izziv. Veliko jih meni, da so hekerji pravzaprav samouki ali pa lopovski programerji, ki so izurjeni v preoblikovanju računalniške strojne in programske opreme, ki nato to izkoristijo izven izvirnega razvijalčevega namena. Ampak to je ozek pogled, ki ne zajema širokega nabora razlogov, zakaj se nekdo ukvarja s hekanjem (Malwarebytes b. l.).

Število uporabnikov interneta se iz dneva v dan povečuje, kar je posledica vse bolj povezanega sveta. Svetovni splet zveni kot nek kompleksen, prostran pojav, ki je kot nek velik prostor, poln raznoraznih dokumentov, ki se imenujejo spletne strani. Čeprav je svetovni splet velik prostor, je ena izmed njegovih prednosti ta, da omogoča oziroma ustvarja svojim uporabnikom manjši kraj za življenje. Vendar pa se je s pojavom svetovnega spleta in

interneta pojavila tudi nova nevarnost za uporabnike interneta, ki veliko časa preživijo v »kibernetskem svetu«, in sicer je to kibernetski kriminal. Medtem ko se organi pregona poskušajo spoprijeti s to težavo, pa ta pravzaprav stalno narašča in mnogi ljudje so postali žrtve hekerjev, tatvine, kraje identitete ali zlonamerne programske opreme. Eden izmed najboljših načinov, da se izognete temu, da ste še ena izmed žrtev spletnega kriminala in zaščitite vaše osebne podatke, je uporaba nepremostljive varnosti, ki uporablja enoten sistem programske in strojne opreme za overjanje vseh informacij, ki so poslane preko interneta ali pa dostopne na internetu (Cross Domain Solution b. l.b).

Kljub temu, da živimo v času, ko postajamo vse bolj digitalni, je vprašanje, ali znamo oziroma kako dobro se znamo zaščititi pred nevarnostnimi, ki nam pretijo med brskanjem po spletu. Prihodnost prinaša vse več digitalizacije in s tem tudi številne prednosti za vse, obenem pa prinaša tudi tveganja digitalnega sveta. Težava je, da je digitalni svet manj oprijemljiv in je zato tudi težje opažen, kar pa daje ljudem lažen občutek varnosti (Leskovar 2017).

V zaključni projektni nalogi smo predstavili pojma hekerstvo in spletni kriminal. Podrobneje smo opisali načine kako se zavarovati pred tovrstnimi napadi, tako kot posameznik kot tudi kot podjetje. Nadalje smo v zaključni projektni nalogi večjo pozornost posvetili tudi nasvetom slovenskih strokovnjakov s področja spletnega kriminala, ki smo jih pridobili preko intervjujev.

1.2 Namen in cilji zaključne projektne naloge

Osnovni namen zaključne projektne naloge je raziskati, proučiti in predstaviti hekerstvo in spletni (kibernetski) kriminal ter seznaniti tako posameznike kot podjetja o nevarnostih, ki jim pretijo na spletu, in o njegovih negativnih posledicah na poslovanje podjetij. V teoretičnem delu naloge bomo podrobneje predstavili oba pojava – kaj sploh sta, v kakšnih oblikah se pojavljata in kdo so tarče hekerjev, kako napadi vplivajo na podjetja in na posameznika oziroma posledice, ki jih pustijo pri svojih vdorih na podjetja in njihovo poslovanje ter kako naj se zaščitijo pred tovrstnimi napadi. V raziskovalnem delu bomo s pomočjo intervjujev pridobili odgovore na naša zastavljena vprašanja, in tako dosegli postavljene cilje.

Namen zaključne projektne naloge je:
- raziskati, proučiti in opredeliti hekerstvo in kibernetski (spletni) kriminal,
- predstaviti delovanje hekerjev in kibernetskega kriminala ter njihov vpliv oziroma posledice, ki jih pustijo pri svojih vdorih na podjetja in njihovo poslovanje,
- prikazati, kako se lahko podjetja zavarujejo pred takimi vdori, še preden pride do njih.

V nalogi pa smo si zastavili naslednje cilje:

- predstaviti, kaj je hekerstvo in kdo so hekerji,
- predstaviti, kdo je »etični heker«,
- predstaviti kibernetski (spletni) kriminal,
- raziskati, proučiti in opredeliti posledice hekerskih napadov na podjetja,
- opredeliti in predstaviti metode preprečevanja spletnega kriminala ter zaščito pred njim.

1.3 Metode za doseganje ciljev

Pri pisanju zaključne projektne naloge smo uporabili različne metode. Pri teoretičnem delu naloge smo informacije pridobivali iz različne literature (članki, knjige, spletne strani ipd.), v empiričnem delu naloge pa smo namen in cilje zaključne projektne naloge raziskali s pomočjo intervjujev. Intervju smo izvedli v sodelovanju z dvema osebama. Z njimi smo skušali pridobiti informacije o tem, kako in na kakšen način se lahko posamezniki ter podjetja zavarujejo pred hekerskimi vdori, kako lahko posameznik varno brska po spletu, ali svetujejo usposabljanje tako za posameznike kot za podjetja, kako pravilno in varno brskati po spletu ter uporabljati internetne storitve.

1.4 Predpostavke in omejitve

Zelo pomembno je, da so posamezniki in podjetniki seznanjeni z nevarnostmi, ki jim pretijo med brskanjem po spletu, kot tudi med poslovanjem njihovega podjetja. Hekerstvo in spletni (kibernetski) kriminal sta pojava, ki se zelo hitro spreminjata in »napredujeta«, zato je tudi toliko teže slediti vsem »novostim«, a vsekakor to ni izgovor, da se posamezniki in podjetja ne bi zavarovala pred tovrstnimi nevarnostmi že prej. V raziskovalnem delu naloge smo predpostavljali, da bodo intervjuvanci dobro poznali problematiko, ki smo jo obravnavali v zaključni projektni nalogi.

Omejitev v raziskovalnem delu zaključne projektne naloge je bila pomanjkanje literature na to temo.

2 HEKERSTVO

Hekerstvo je običajno tehnične narave – kot ustvarjanje »zlorab«, ki vnesejo zlonamerno programsko opremo, s pomočjo napada s pogonom, ki ne zahteva interakcije uporabnikov. Vendar pa lahko hekerji uporabijo tudi psihologijo, da uporabnika preusmerijo oziroma prepričajo h kliku na zlonamerno prilogo ali k posredovanju osebnih podatkov. Te taktike imenujemo »socialni inženiring«. Hekerstvo se je iz najstniške vragolije razvilo v poslovno rast v višini milijarde dolarjev, njegovi pripadniki so vzpostavili kriminalno infrastrukturo, ki razvija in prodaja orodja za hekerje na ključ za potencialne prevarante z manj prefinjenimi tehničnimi veščinami, znanimi kot »skriptni otroci« (Malwarebytes b. l.).

Motiv hekerjev je najbolj navdušujoč in tudi najbolj osvetljujoč dejavnik, ki na koncu določa celoten psihološki profil kibernetskega kriminalca – hekerja. Medtem ko imajo hekerji pogosto več kot en motiv za to, kar počnejo, nam lahko ti motivi povejo zelo pomembne razloge oziroma njihove »zakaj« za vdiranje in tudi, v kateri vrsti kibernetskega kriminala bodo verjetno sodelovali. Nekateri glavni motivi za različne vrste kibernetskega kriminala so naslednji: za zabavo/izziv, finančni, čustveni, ego, politični, verski, spolni impulzi/deviantno vedenje ipd. Prav tako so tam zunaj ljudje, ki enostavno samo želijo škodovati drugim in povzročati zmedo. Tam so fantje in dekleta, ki so pripravljena zlomiti ljudi, sposobni so spremeniti človekovo duševnost v matematični problem, nato pa ta problem tudi rešijo (Zamora 2018).

2.1 Definicija hekerstva

Hekerstvo se nanaša na dejavnosti, ki poskušajo ogroziti delovanje digitalnih naprav, kot npr. računalnike, pametne telefone, tablične računalnike in tudi celotna omrežja. Medtem ko namen hekerstva morda ni vedno v zlonamerne namene, je danes večina sklicevanj na hekerstvo in hekerje označena kot nezakonita dejavnost kibernetskih kriminalcev, ki so motivirani s finančnim dobičkom, protestom, zbiranjem informacij »spying« (vohunjenje) in celo tudi samo za zabavo in izziv. Mnogi menijo, da se beseda »heker« nanaša na nekega samouka ali lopova, ki je usposobljen za spreminjanje računalniške strojne ali programske opreme, tako da jih lahko uporablja na načine, ki niso izviren namen razvijalca. Toda to je ozek pogled, ki ne zajema širokega nabora razlogov, zakaj se nekdo »obrne« na hekanje (Malwarebytes b. l.).

Hekerstvo se na splošno nanaša na nepooblaščeno vdiranje v računalnik ali omrežje. Oseba, ki se ukvarja s hekerskimi dejavnostmi, je znana kot heker. Ta lahko spremeni sistemske varnostne funkcije, da doseže svoj cilj, ki se razlikuje od prvotnega namena sistema. Hekerstvo se prav tako lahko nanaša na ne-zlonamerne dejavnosti, ki običajno vključujejo nenavadne ali improvizirane spremembe opreme ali procesov (Techopedia b. l.b).

Pravzaprav vdiranje v računalniški sistem označujemo kot nadrejeni krovni izraz za dejavnost za večino, če ne vse, od škodljive programske opreme in zlonamerne kibernetske napade na računalniško javnost, podjetja in vlade. Poleg socialnega inženiringa in »malwerkanja« so skupne tehnike hekerstva tudi: roboti, ugrabitve brskalnikov, zavrnitev storitve (angl. *denial of service*, v nadaljevanju DoS), izsiljevalski programi/ransomware, rootkiti, trojanski virusi, virusi in črvi (Malwarebytes b. l.).

Nedavno se je »resnično hekanje« uporabljalo samo za dejavnosti, ki imajo dober namen, zlonamerni napadi na računalniška omrežja pa so bili uradno znani kot razpoke (angl. *cracking*), a večina ljudi danes tega ne razlikuje več. Zelo pogosto je, da se izraz »hekanje« uporablja za dejavnosti, ki so bile nekoč znane kot »cracking«. Hekerji gradijo, medtem ko »krekerji« (angl. *crackers*) razbijajo. To je osnovna razlika med hekanjem in razpokami v zvezi z računalniško varnostjo. Toda nadaljnje vprašanje, ki se pojavi, je: »Kaj je zgrajeno in kaj je vlomljeno?« Hekanje je vdiranje v računalniški sistem brez kakršnih koli pooblastil, bodisi je namen dober ali slab, medtem ko je krekanje (angl. *cracking*) pravzaprav ista praksa, čeprav s kaznivim namenom. Torej je osnovna razlika v tem, da heker uporablja svoje obsežno znanje o računalniški logiki in kodi, kreker pa išče »zadnja vrata« v programih in jih posledično tudi izkorišča. Hekerji vdirajo v varnostne sisteme z namenom, da preverijo luknje v njih in sodelujejo pri odpravljanju teh, medtem ko krekerji vdrejo v varnostni sistem zaradi kriminalnih in nezakonitih razlogov ali pa zaradi osebnih koristi (Kikonyogo 2018).

2.2 Vloga in pomen hekerstva

Kaj je pravzaprav tisto, kar žene hekerje, da počnejo to, kar počnejo? Roger A. Grimes (2018) pravi, da bodisi hekerji uporabljajo »računalniško izkoriščanje« ali pa zlonamerno programsko opremo je njihov cilj oziroma motiviranost vedno enaka. Razumeti, zakaj in kako hekerji počnejo, je ključ do vaše obrambe. Ne glede na grožnjo, ki preti vašemu računalniku, lahko ta pride do računalnika na dva načina – človeški nasprotnik ali zlonamerna programska oprema (»malware«). Človeški napadalci oziroma hekerji lahko uporabijo katero koli od več sto tisoč znanih računalniških potez in metodologij napadov za ogrožanje računalnika ali neke naprave. Ljudje naj bi, oziroma morajo izvajati rutinske popravke na svojem računalniku, številne naprave in programi pa »se trudijo«, da se samodejno posodabljajo, vendar obstaja veliko računalnikov, ki so dalj časa ranljivi in posledično postanejo bolj dovzetni za tovrstne napade, prav tako pa ostanejo ranljivi tudi po tem, ko so popravki za programe na voljo (Grimes 2018).

Kot smo v tem poglavju že omenili, so motivi hekerjev za izvajanje napadov finančni, sponzorirane kibernetske vojne, poslovno vohunjenje, haktivisti, kraja virov, za zabavo/izziv, finančni, čustveni, ego, politični, verski in spolno impulzivno/deviantno vedenje (Zamora 2018). Finančne kraje in nacionalni napadi so zlahka največji del kibernetskega kriminala. Pred desetletji je bil heker predstavljen kot nek povprečen posamezen mladostnik, ki je

deloval sam, poganjala pa ga je nezdrava hrana. Zanimalo jih je, kako se izkazati ter pokazati drugim, da lahko nekam vdrejo ali pa ustvarijo neko zanimivo zlonamerno programsko opremo, ampak le redko so povzročili neko resno škodo. Danes pa večina hekerjev pripada profesionalnim skupinam, ki so motivirane, da vzamejo nekaj vrednega in da povzročajo veliko škodo. Zlonamerna programska oprema, ki jo uporabljajo, je zasnovana tako, da je čim bolj prikrita in da pred odkritjem vzame toliko vrednosti, kot je le mogoče (Grimes 2018).

Ne glede na motivacijo hekerji ali njihova zlonamerna programska oprema običajno vdrejo v računalnik in izkoristijo računalniški sistem na enak način, kot že poprej, prav tako pa uporabljajo večinoma enake vrste izkoriščanja in metodologij vključno s socialnim inženiringom, nepokritimi programskimi in strojnimi ranljivostmi, napadi na nedoločen dan (angl. *zero-day attacks*), napadi brskalnikov, napadi gesel, prisluškovanje, DoS in fizični napadi. Seveda je ta seznam daljši, zato bomo v naslednjem poglavju predstavili najbolj pogoste oblike hekerskih napadov.

2.3 Hekerski napad (hekanje)

Izraz heker označuje več subkultur in skupnosti računalniških navdušencev. Danes se izraz heker največkrat povezuje z ljudmi, ki se ukvarjajo z vdori oziroma nepooblaščenimi dostopi v računalniška omrežja in zaobhajanju varnostnih sistemov iz razlogov, kot so zaslužek, pridobivanje informacij, iskanje pomanjkljivosti v teh sistemih ipd. Heker je torej človek, ki ima znanje na področju programiranja in omrežne tehnologije ter tudi številne druge spretnosti, ki jih uporablja za »vstop« v sisteme, podjetja, vlade in omrežja, kjer tudi povzroči škodo ali pa težave (Varga 2017). V računalniškem omrežju je hekerstvo tehnično prizadevanje za manipulacijo običajnega delovanja omrežnih povezav in povezanih sistemov. Heker je vsaka oseba, ki se ukvarja s hekanjem. Izraz hekanje se je v zgodovini nanašal na konstruktivno, pametno tehnično delo, ki ni bilo nujno povezano z računalniškimi sistemi. Danes sta hekerstvo in heker najpogosteje povezana z zlonamernimi napadi na omrežja in računalnike preko interneta. Dejansko hekanje se uporablja samo za tiste dejavnosti, ki imajo dobre namere, zlonamerni napadi na računalnike in računalniška omrežja pa se imenujejo »pokanje« (angl. *cracking)*, žal pa večina ljudi, ki nima tehničnega znanja, ne vidi razlike med njima. Ljudje brez tovrstnega znanja izraz hekanje velikokrat enačijo s pokanjem, v bistvu pa tovrstnega izraza ne poznajo (Mitchell 2019).

Vdori v računalniška omrežja se najpogosteje izvajajo s pomočjo skript ali drugih oblik programiranja. Ti posebej zasnovani programi običajno manipulirajo s podatki, ki »potujejo« preko omrežne povezave z namenom pridobivanja več informacij o tem, kako deluje ciljni sistem – tj. žrtvin sistem. Veliko takih vnaprej pripravljenih skript je objavljenih na internetu ter so dostopne vsem – običajno hekerjem na začetni ravni, ki so šele začeli s hekerstvom. Bolj izkušeni hekerji lahko proučujejo in prilagajajo te skripte, da bi razvili nove metode ter jih nato tudi uporabili. Nekaj zelo usposobljenih hekerjev dela za komercialna podjetja,

najemajo jih za zaščito, varovanje programske opreme in podatkov v podjetjih pred zunanjimi hekerji. Metode pokanja na omrežjih vključujejo ustvarjanje črvov, sprožanje napadov z zavrnitvijo storitve (DoS) in vzpostavitev nepooblaščenih povezav z oddaljenim dostopom do naprave. Zaščita omrežij in računalnikov, ki so nanj priključeni, pred zlonamerno programsko opremo, lažnim predstavljanjem (angl. *phishing)*, trojanskimi konji in nepooblaščenimi dostopi, je lahko tudi zaposlitev s polnim delovnim časom, ki je zelo pomembna. Učinkoviti hekerji morajo imeti kombinacijo tehničnih veščin in osebnostnih lastnostih, da bi bili njihovi napadi uspešni. Ena izmed veščin je sposobnost dela s številkami in znanje matematike, saj je bistvena za hekerje. Hekanje zelo pogosto zahteva razvrščanje velikih količin podatkov, kod in računalniških algoritmov. Dober spomin in logično sklepanje sta zelo pomembni veščini, saj hekerstvo vključuje zbiranje majhnih dejstev in podrobnosti, ki temeljijo na tem, kako računalniški sistemi delujejo. Prav ti podatki so bistvene sestavine dobrega napada. Ne nazadnje pa morajo biti hekerji tudi potrpežljivi. Napadi so pogosto kompleksni in zahtevajo veliko časa za načrtovanje ter izvedbo (Mitchell 2019).

Hekerstvo je v hollywoodskih filmih in televizijskih oddajah prikazano kot nekaj slabega, prikazano je drugače, kot dejansko je. Pravzaprav je to sistematičen, naporen proces, v katerem napadalec poskuša metodično najti računalniške sisteme, prepoznati njihove ranljive točke in jih nato tudi ogroziti, da pridobi dostop. Strokovnjaki so opredelili šest korakov, ki se običajno izvajajo v hekerskem procesu; ti vključujejo: odtis, skeniranje, oštevilčenje, penetracijo, napredovanje in brisanje sledi. V nadaljevanju bomo opisali vseh šest korakov, ki se izvajajo v hekerskem napadu (Nachenberg b. l.).

Prvi korak, ki ga pogosto uporabljajo hekerji, se imenuje *odtis* ali *izvidništvo* (angl. *footprinting*). Cilj tega koraka je zbrati informacije, ki so bistvene za napad, in tako omogočiti napadalcu, da pridobi popoln profil varnostne drže neke organizacije. V tej fazi lahko heker pridobi informacije, kot so lokacija podjetja, telefonske številke, imena zaposlenih, varnostni pravilniki, politike in tudi celotna postavitev ciljnega omrežja. Naštete informacije lahko hekerji pridobijo zelo preprosto, saj potrebujejo ali spletni brskalnik ali pa telefon. Žal pa so ljudje pogosto najšibkejši varnostni člen v organizaciji. Že samo en pameten telefonski klic oddelku za tehnično podporo lahko ogrozi varnost pomembnih podatkov in informacij podjetja, organizacije (Nachenberg b. l.).

Naslednji oziroma drugi korak, ki ga opravijo hekerji, je *skeniranje* (angl. *scanning*). Hekerji opravijo skeniranje, da bi dobili bolj podroben pogled na omrežje podjetja in da bi razumeli, kakšni računalniški sistemi in storitve se uporabljajo. V tej fazi heker določi, kateri sistemi na ciljnem omrežju so »živi« in dosegljivi preko interneta. Pogosto uporabljene tehnike skeniranja vključujejo preverjanje odzivnosti omrežja (angl. *ping sweep*) ter računalniških vmesnikov (angl. *port scan*). Preverjanje odzivnosti omrežja tako napadalcu omogoča, da lahko določi, kateri posamezni računalniki so delujoči in potencialne tarče za napad. Preverjanje računalniških vmesnikov oziroma skeniranje vrat pa se lahko uporabi za določitev

in ugotavljanje, kateri vmesniki so odprti na določenem računalniku in ali ima programsko opremo, ki upravlja ta vmesnik (Nachenberg b. l.).

Tretji korak se imenuje *oštevilčenje* (angl *ennumeration*) in je postopek identifikacije uporabniških računov in slabo zaščitenih računalniških virov. V tem koraku se heker poveže z računalniki v ciljnem omrežju in z drezanjem v te sisteme pridobiva čim več informacij. Medtem ko lahko fazo skeniranja primerjamo s trkanjem na vrata ali z obračanjem kljuke, da bi ugotovili, ali so vrata zaklenjena, se lahko oštevilčenje primerja z vstopom v pisarno in brskanjem po arhivskih omarah ali po predalnikih. Vsekakor je ta korak bolj vsiljiv (Nachenberg b. l.).

Četrti korak se imenuje *penetracija* (angl. *penetration*). V tem koraku napadalci (hekerji) poskušajo pridobiti nadzor nad enim ali več sistemi v ciljnem omrežju oziroma omrežju organizacije. Ko npr. napadalec med postopkom oštevilčenja (enumeracije) pridobi seznam zaposlenih in njihovih uporabniških imen, lahko velikokrat pridobi geslo enega ali več zaposlenih ter tako pridobi bolj obsežen dostop do tega uporabniškega računa. Ko heker ugotovi, da ciljni računalnik izvaja staro ali hroščasto (angl. *buggy*) programsko opremo, ki ni pravilno nastavljena, lahko heker poskusi prav s to programsko opremo izkoristiti že znane elemente ranljivosti (slabosti) in tako pridobiti nadzor nad sistemom (Nachenberg b. l.).

Predzadnji, peti korak se imenuje *napredovanje* (angl. *advance*). V tej bolj napredni fazi heker uporablja računalnike ali pa račune, v katere je že vdrl v koraku penetracije, zato da bi izvedel dodatne napade na ciljnem omrežju. Na primer: heker lahko izvede dodaten vdor v še bolj občutljive skrbniške račune, namesti skrite (angl. *backdoor*) programe ali pa trojanske konje in namesti omrežne »vohune« (angl. *sniffers*) za zbiranje dodatnih informacij, kot so gesla iz podatkov, ki potujejo po omrežju (Nachenberg b. l.).

Zadnji korak se imenuje *brisanje sledi* (angl. *covering tracks*). V tej končni fazi hekanja napadalec odpravlja vse zapise ali dnevnike, ki kažejo na njegovo zlonamerno dejavnost. Z brisanjem datotek dnevnika (angl. *log files*), onemogočanjem revizije (ki bi sicer lahko opozorila skrbnika na zlonamerne dejavnosti) in prikrivanjem hekerskih datotek, ki jih je uvedel heker, lahko prikrije svoje sledi in se izogne odkritju. Končno heker lahko namesti korenski komplet (angl. *root kit*) – serijo programov, ki nadomestijo obstoječo programsko opremo in s tem tako prikrije svoje sledi in nato zbira nove informacije (Nachenberg b. l.).

2.4 Vrste hekerjev

V hekerskih skupnostih obstajajo tudi subtilne razredne razlike, s katerimi splošna javnost ni seznanjena. Obstajajo hekerji, ki vdirajo v sisteme in jih ne nujno uničujejo; pravzaprav imajo dober namen. Ti ljudje so hekerji z belim klobukom (angl. *white-hat hackers*) ali »dobri hekerji«. White-hat oziroma etični hekerji so tisti posamezniki, ki delujejo znotraj organizacije in vdirajo v sisteme ter opozarjajo na varnostne napake. Njihove namere niso nujno opustošenje, temveč opravljanje javne službe. Poznamo pa tudi nekaj znanih dobronamernih hekerjev (Collins 2018):

- Tim Berners-Lee – najbolj znan po tem, da je izumil svetovni splet, html in sistem URL;
- Vinton Cerf – znan kot »oče interneta«, bil je zelo koristen pri ustvarjanju interneta in spleta, kot ga poznamo danes;
- Dan Kaminsky – zelo spoštovan strokovnjak za varnost, najbolj znan po svoji vlogi pri odkrivanju škandala z zaščito pred kopiranjem Sony BMG;
- Ken Thompson – je soustvaril UNIX, operacijski sistem in programski jezik C;
- Donald Knuth – eden najbolj vplivnih ljudi na področju računalniškega programiranja in teoretičnega računalništva;
- Larry Wall – ustanovitelj PERL-a, programskega jezika na visoki ravni, ki se lahko uporablja za najrazličnejše naloge.

Na drugi strani pa obstajajo hekerji s črnim klobukom (angl. *black-hat hackers*), katerih namen je zlonameren. Zelo znani zlonamerni hekerji so (Collins 2018):

- »Anonymous« – široko povezana skupina hekerjev z vsega sveta, ki se preko različnih internetnih socialnih medijev in forumov povezujejo. Najbolj znani so po svojih prizadevanjih za spodbujanje civilne neposlušnosti in/ali nemirov zaradi obrekovanja in uničevanja različnih spletnih strani, DoS in spletnega objavljanja osebnih podatkov.
- Jonathan James – zloglasni heker, ki je vdrl v agencijo za zmanjšanje obrambne grožnje in krajo programske kode;
- Adrian Limo – znan po tem, da je v mrežah organizacij na visoki ravni, vključno z Yahoojem, New York Timesom in Microsoftom, prodrl v varnostne pomanjkljivosti;
- Kevin Mitnick – obsojen po dveh letih in pol izogibanja oblastem zaradi več kriminalnih računalniških zločinov ter vdora v telefonski sistem FBI-ja, medtem ko ga je agencija lovila. Po odsluženi kazni v zveznem zaporu zaradi svojih dejanj je Mitnick ustanovil podjetje za kibernetsko varnost, da bi podjetjem in organizacijam pomagal ohranjati njihovo omrežje varno.

Medtem ko večina hekerskih napadov, za katere slišimo v novicah, prihaja od ljudi, ki imajo zlonamerne namene, pa obstaja tudi veliko neverjetno nadarjenih in predanih ljudi, ki uporabljajo svoje hekerske spretnosti za večje dobro. Zelo pomembno je razumeti razliko.

2.5 Etični heker

Zelo pogosto slišimo novice glede hekerjev, od anonimnih do ponarejenih novic ter do napadov zavrnitve storitev in kršitev podatkov. Zdi se, da »slabi fantje« vedno povzročijo opustošenje. In tako tudi je – slabi fantje povzročajo vse vrste škod, od nadležnih (spam) do uničujočih (kibernetski napadi, ki kradejo osebne podatke). Toda prav tako obstajajo »dobri fantje« z enakimi veščinami, imenujemo jih etični hekerji. Toda kdo sploh so etični hekerji? Kar nekaj definicij opisuje, kdo oziroma kaj so etični hekerji, zato je to včasih tudi izjemno težko na kratko povedati. Če nekako povzamemo, etični hekerji počnejo enake stvari kot neetični hekerji, vendar na legalen in etičen način, na koncu pa za svoje delo dobijo plačilo. Poleg vsega tega dela etični hekerji tudi izvajajo varnostne preglede, penetracijske teste ali varnostne analize z vednostjo naročnika v nadzorovanem okolju. Delovnik etičnega hekerja nikoli ni enak, temveč je zelo raznolik, saj so tudi projekti, v katerih sodeluje, različni. Slovenski etični heker Milan Gabor[1] (po Varni na internetu 2014) pravi, da je glede na statistiko izvajanja glavne dejavnosti etičnih hekerjev dejanskega etičnega hekanja približno 30 odstotkov celotnega projekta. Preostali čas pa porabijo za pripravo kakovostnega poročila o odkritih ranljivostih ter pripravo prezentacije. Ne nazadnje je zelo pomembno, da etični heker natančno pozna različne tehnologije in da je iznajdljiv (Varni na internetu 2014). Etični heker (znan tudi kot »white hat«) je tako vrhunski strokovnjak za varnost, ki zna najti in izkoristiti ranljivosti in slabosti v različnih sistemih – tako kot zlonamerni hekerji (»black hat«). Kot smo že omenili, oba hekerja uporabljata enaka znanja, vendar etični heker uporablja te veščine na zakonit način (Manikandan 2013).

Poleg preizkušanja so etični hekerji povezani tudi z drugimi odgovornostmi. Glavna ideja je, da replicira zlonamernega hekerja na delu in namesto izkoriščanja ranljivosti za zlonamerne namene pravzaprav poišče obrambne ukrepe, s katerimi bi zaščitil sistem. Etični heker lahko uporabi vse ali pa le nekatere od teh strategij za vdor v sistem: skeniranje vrat in iskanje ranljivosti, pregledovanje namestitvenih popravkov in testiranje, da jih ni mogoče izkoristiti, ter ukvarjanje s koncepti socialnega inženiringa, kot je »brskanje po smeteh« (angl. *dumpster diving*) za gesla, grafikone, opombe ali kar koli, kar bi vsebovalo ključno informacijo, ki jo je kasneje moč uporabiti za ustvarjanje napada. Etični hekerji lahko tudi uporabljajo druge tehnike socialnega inženiringa, kot so deskanje po ramenih (angl. *shoulder surfing*), da bi pridobili dostop do ključnih informacij, ali pa igra na karto prijaznosti, da ukane zaposlene, da izdajo svoja gesla. Seveda se bo etični heker poskušal izogniti sistemom za odkrivanje vdorov (angl. *intrusion detection systems*), sistemom za preprečevanje vdorov (angl. *intrusion prevention systems*) in požarnim zidovom. Prav tako lahko izvohajo omrežja, se izogibajo in razbijajo brezžična šifriranja ter ugrabijo spletne strežnike in spletne aplikacije, ne nazadnje pa se lahko ukvarjajo tudi z vprašanji, povezanimi s krajo in zlorabo prenosnika. Ugotavljanje, kako dobro se organizacija oziroma podjetje odzove na te in druge taktike,

[1] Primarni vir ni naveden.

pomaga etičnemu hekerju ugotoviti moč varnostne politike in varnostne infrastrukture organizacije. Etični heker poskuša tudi izvesti enake vrste napadov, kot jih izvajajo zlonamerni hekerji, in preko tega poskuša pomagati organizacijam okrepiti svojo obrambo (Manikandan 2013).

In kdo bi moral biti etični heker? Nekateri trdijo, da dobronamerni hekerji ne obstajajo in da so vsi »white hat« hekerji pravzaprav zlonamerni, ki so samo obrnili nov list v svoji karieri. Tako kot pri vsakem poklicu je strast za industrijo eden ključnih vidikov uspeha. To, skupaj z dobrim poznavanjem mrežnega povezovanja in programiranja, pomaga strokovnjakom uspeti na etičnem hekerskem področju. Za strokovnjake varnosti, forenzične analitike, analitike vdora in, kar je najpomembnejše, ljudi, ki si želijo vstopiti na ta področja, je certifikat CEH V9 najboljša izbira. Številna IT podjetja so ta certifikat označila kot obvezno kvalifikacijo za delovna mesta, ki so povezana z varnostjo, kar pripelje do tega, da morajo vsi strokovnjaki s tega področja imeti pridobljen ta certifikat. Vsak strokovnjak, ki pridobi certifikat CEH V9, poglobi svoje znanje o trojanskih konjih, zakulisnih vratih (angl. *backdoors*) in o protiukrepih, prav tako pa je tudi bolj izkušen v razumevanju sistemov za odkrivanje vdorov, požarnih zidov in brezžičnega vdora ipd. (Manikandan 2013).

Podjetja in vladne organizacije, ki se resno ukvarjajo z varnostjo omrežja, najemajo etične hekerje in preizkuševalce penetracij, da bi pomagali preiskati in izboljšati njihova omrežja, aplikacije in druge računalniške sisteme s končnim ciljem preprečevanja kraje podatkov in goljufij. In kako je videti trg dela za etične hekerje? Pravzaprav zelo dobro, saj trg informacijske tehnologije neprestano raste kljub trenutnim gospodarskim »pretresom« (Geier 2012). Raziskovalni podjetji IDC in Gartner sta poročali, da je svetovna poraba IT v letu 2017 porasla za 3,3 odstotka, v letu 2018 pa naj bi se po njihovih ocenah ter napovedih povečala za 4,3 odstotka. V prihodnjih letih bo svetovna poraba za IKT rasla predvsem zaradi uvajanja novih tehnologij, kot so internet stvari (IoT), robotika, obogatena (angl. *augmented reality*) in navidezna resničnost (angl. *virtual reality*), kognitivno računalništvo ter umetna inteligenca (angl. *artificial intelligence*) (IRT3000 2018).

Zaposlovanje etičnih hekerjev

Rast IT varnosti in etičnih hekerjev je posledica tehnološkega napredka in vse večjega števila groženj v računalniškem svetu. Banke so glavne tarče, zato so vedno izpostavljene kibernetskim grožnjam. Zaščita pred kibernetskimi napadi zahteva velik delež sredstev bank, tj. 24 milijard dolarjev, ki jih na svetovni ravni letno porabijo za varnostno tehnologijo (Gonsalves 2012). Poleg bank so tudi druge organizacije, bodisi majhne, srednje velike ali pa velike, nenehno izpostavljene kibernetskim napadom oziroma so njihove žrtve. Svet informatike se premika proti oblaku (angl. *cloud*), kjer sta virtualizacija in IT zunanje izvajanje (angl. *outsourcing*) glavni trend. Od nastanka računalništva v oblaku je bilo varnosti posvečeno veliko skrbi. Da bi izkoristili prednosti oblaka in virtualizacije brez povzročanja

škode varnosti, morajo podjetja najeti etične hekerje. Glavni izziv, s katerim se danes soočajo podjetja, je hitro rastoči kibernetski svet in kompleksnost varnostnih zahtev. Takšne taktike se razvijajo iz dneva v dan in samo strokovnjaki s tega področja lahko premagajo ta izziv. Etični hekerji so zato v današnjem poslovnem svetu zelo iskani (Chandana 2013).

Zakaj zaposliti etične hekerje v svoji organizaciji? Etični hekerji znajo »zgraditi« računalniške sisteme, ki preprečujejo dostop hekerjev in ščitijo sistem in njegove informacije pred zlonamernimi napadi. Prav tako urejajo ustrezne preventivne ukrepe, da bi se izognili zunanjim kršitvam varnosti. Najemajo jih tudi za varovanje informacij o uporabnikih ali strankah, ki so na voljo v poslovnih transakcijah in obiskih, ter za redno preverjanje omrežij in ustvarjanje zavesti o varnosti na vseh ravneh delovanja podjetja. Zelo veliko znanih podjetij, kot sta Apple in IBM, je najelo etične hekerje. V konkretnem primeru je Apple najel dva varnostna raziskovalca, ki sta prej delala na področju virusov, ki so ciljali na računalnike Mac. Eden izmed raziskovalcev je tudi razvil protivirusnega hibrida virus-črv, imenovanega Thunderstrike 2, ki je bil namenjen računalnikom Mac. Toda namesto da bi uporabila svoje ugotovitve ter jih prodala najvišjemu ponudniku, sta raziskovalca raje obvestila Apple o njegovi ranljivosti, kar je bilo od takrat naprej v celoti onemogočeno (Leswing 2016).

Stroški testiranja varnosti se razlikujejo glede na podjetje. Podjetja, ki imajo veliko podatkovno bazo uporabnikov, bi morala plačati zajetne stroške, medtem ko bi manjša podjetja plačevala manj sredstev za varnost informacij. Naloge, kot so preverjanje požarnih zidov, strežnikov, naslovov IP, so visoko finančno ovrednotene, vendar je ta naložba upravičena v primerjavi z izgubo, ki bi jo povzročili kibernetski napadi. Za zaščito sistemov lahko podjetja torej najamejo etično podjetje ali agencijo ali pa najamejo etične hekerje. Seveda je ta odločitev odvisna od različnih dejavnikov, npr. mala podjetja si ne morejo privoščiti, da bi drugim agentom dovolila, da vdrejo v sisteme od zunaj, zato zaradi varnosti raje zaposlijo lastne etične hekerje, medtem ko drugi raje najamejo etična hekerska podjetja, da ščitijo njihov sistem in omrežja. V obeh primerih morajo etični hekerji s stranko oziroma podjetjem, za katerega bodo delali, podpisati pravni sporazum. Danes zaposlovanje etičnih hekerjev ni več stvar izbire, ampak je za podjetje nekaj nujnega oziroma obveznega. Svet ES izvaja program certificiranega etičnega hekerja, s katerim kvalificirajo poklicne hekerje. Iz očitnih razlogov je po certifikatu CEH veliko povpraševanje v podjetjih po vsem svetu (Chandana 2013).

3 KIBERNETSKI (SPLETNI) KRIMINAL

Kibernetski kriminal oziroma spletni kriminal je zelo velika grožnja, večja kot kadar koli prej, saj je vedno več ljudi povezanih z internetom prek prenosnih računalnikov, pametnih telefonov in tabličnih računalnikov. Kibernetski kriminal je pravzaprav eden od najbolj dobičkonosnih načinov, kako zaslužiti denar v kriminalnem svetu. Obstaja več različic kibernetskih kaznivih dejanj, ki jih lahko razdelimo v dve kategoriji: enkratni zločin (npr. namestitev virusa, ki krade vaše osebne podatke) in kazniva dejanja (npr. spletno ustrahovanje, izsiljevanje, distribucija otroške pornografije, organizacija terorističnih napadov ipd.). Kibernetski kriminal je torej kot vsak drug kriminal, saj je delo kriminalcev, ampak tistih kriminalcev, ki imajo tehnološke spretnosti in uporabljajo internet za doseganje svojih zlonamernih ciljev. Kibernetski kriminalci uporabljajo svoj raznolik nabor spretnosti za dostop do bančnih računov, krajo identitet, izsiljevanje, goljufije, zalezovanje in nadlegovanje, ali pa za uporabo ogroženega računalnika kot dela naprednega botneta za izvedbo DDoS (angl. *distributed denial of* service) napadov na večje organizacije (Avast b. l.).

Zaščita pred kibernetskim kriminalom je lahko zamudna, a vendar se vedno obrestuje. Že samo izvajanje varnega brskanja lahko prepreči tovrstne napade, na primer izogibanje nenavadnim prenosom in nezanesljivim spletnim mestom je razumna rešitev za kibernetski kriminal. Vsekakor pa moramo biti zelo previdni pri uporabi svojih splošnih podatkov ter osebnih podatkov, še posebej pa takrat, ko se prijavljamo v spletne strani, saj je »izvajanje varnosti« lahko le prednost za nas in smo tako samo korak pred spletnimi kriminalci. Najboljša stvar, ki jo kot posameznik lahko storimo, je, da se zaščitimo s pomočjo močnega protivirusnega programa. Ne nazadnje je zelo pomembno, da se ljudje ozaveščajo v tej smeri in spremljajo »obveščevalne centre«, ki vsakodnevno opozarjajo na spletne goljufije in nevarnosti, ki smo jim izpostavljeni na spletu. V Sloveniji imamo nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljevanju SI-CERT), ki je prav s tem namenom ustvaril projekt »Varni na internetu«. Projekt je namenjen širši slovenski javnosti in prav tako malim podjetjem. Njihov cilj je dvigniti stopnjo zavedanja ciljnih javnosti o različnih nevarnostih, ki smo jim izpostavljeni na spletu, informiranju o varni uporabi spletne banke, informiranju o različnih oblikah spletnih prevar in ponuditi praktične rešitve, kako se zavarovati, in še veliko več (Varni na internetu b. l.). Ne nazadnje je pomembno tudi, da ljudje uporabijo »zdravo kmečko pamet«, saj, če prejmemo elektronsko pošto z obvestilom, da smo zadeli dobitek na lotu, čeprav ga nismo igrali, zelo verjetno nekaj ni v redu. Ali pa, da nam je nek daljni sorodnik zapustil veliko vsoto denarja. Ta dva primera sta le dva izmed mnogih, na katere ljudje nasedemo, zato je še toliko bolj pomembno, da se informiramo in smo na tekočem o tovrstnih napadih.

3.1 Opredelitev spletnega kriminala

Hekanje, zlonamerna programska oprema (angl. *malware*), botneti, temačni del interneta (angl. *darknet*), kibernetski kriminal kot storitev – vse te besede in besedne zveze, ki so komaj obstajale pred desetimi leti, so zdaj del našega vsakdanjega jezika, saj kriminalci uporabljajo nove tehnologije, da se zoperstavijo vladam, podjetjem in posameznikom. Ti zločini ne poznajo nobenih meja, fizičnih ali virtualnih, povzročajo pa resno škodo in predstavljajo resnično grožnjo žrtvam po vsem svetu. »Čisti kibernetski kriminal« se nanaša na kazniva dejanja zoper računalniške in informacijske sisteme, kjer je cilj pridobiti nepooblaščen dostop do naprave ali zavrniti oziroma preprečiti dostop zakonitemu uporabniku. Ta vrsta kriminala napreduje neverjetno hitro. Policija mora slediti vsem tem novim tehnologijam, razumeti možnosti, ki jih ustvarjajo za kriminalce, ter vedeti, kako jih je mogoče uporabiti kot orodje za boj proti kibernetskemu kriminalu (Interpol b. l.).

Kibernetski kriminal je opredeljen kot kaznivo dejanje, kjer je računalnik predmet kaznivega dejanja ali pa se uporablja kot orodje za izvedbo kaznivega dejanja. Kibernetski kriminalci lahko uporabljajo napravo za dostop do osebnih podatkov uporabnika, zaupnih poslovnih informacij, vladnih informacij ali celo onemogočijo delovanje naprave. Del kibernetskega kriminala je tudi prodaja ali pridobivanje navedenih informacij na spletu. Kibernetski kriminal delimo v dve kategoriji (Panda Security 2018):

- *kazniva dejanja, ki se nanašajo na omrežja ali naprave* – gre za viruse, zlonamerne programske naprave ter DoS napade,
- *kazniva dejanja, ki z uporabo naprav sodelujejo v kriminalnih dejavnostih* – tukaj gre za ribarjenje (angl. *phishing*), spletno zalezovanje (angl. *cyberstalking*) ter krajo identitete.

Kibernetski kriminal spada v tri glavne kategorije: posameznik, lastnina in vlada. Vrste uporabljenih metod in stopnje težavnosti se razlikujejo glede na kategorijo. Na kratko bomo predstavili te tri glavne kategorije (Panda Security 2018):

- *Lastnina* je podobna resničnemu primeru kaznivega dejanja – npr. posedovanje bančne ali kreditne kartice posameznika. Tako kot v resničnem svetu, kjer lahko zločinci kradejo in ropajo, se lahko tudi v spletnem svetu zločinci zatekajo h kraji in ropanju. Hekerji lahko ukradejo bančne podatke posameznika, da pridobijo dostop do njegovih sredstev, opravijo nakupe na spletu ali pa izvajajo prevare (angl. *phishing scams*) z lažnim predstavljanjem, s čimer spodbudijo ljudi, da posredujejo svoje podatke. Poleg tega lahko uporabijo tudi zlonamerno programsko opremo za dostop do spletnega mesta organizacije ali povzročijo motnje v sistemih organizacije. Prav tako lahko zlonamerna programska oprema poškoduje tudi programsko in strojno opremo in tako kot vandali škodujejo nepremičninam v svetu brez povezave.
- *Posameznik.* Ta kategorija kibernetskega kriminala vključuje le eno osebo, ki distribuira zlonamerne ali nezakonite informacije na spletu. To lahko vključuje spletno zasledovanje (angl. *cyberstalking*), distribucijo pornografije in trgovino z ljudmi. Danes organi pregona

zelo resno obravnavajo to kategorijo kibernetskega kriminala in na mednarodni ravni združujejo moči, da dosežejo in aretirajo storilce.

– *Vlada.* Ta kategorija je najmanj običajna za kibernetski kriminal, a je vendar najresnejše kaznivo dejanje. Zločin proti vladi je znan tudi kot kibernetski terorizem. Vladni kibernetski kriminal vključuje hekanje vladnih spletnih strani, vojaških spletnih strani ali pa distribucijo propagande. Ti kriminalci so pogosto teroristi ali pa sovražne vlade drugih narodov. Če bo ta kategorija postala uspešna, lahko povzroči paniko med civilnim prebivalstvom.

3.2 Vloga in pomen spletnega kriminala

V današnjem času kriminalce, ki so del spletnih zločinov, ne motivira oziroma jih ne spodbuja njihov ego ali pa strokovno znanje. Namesto tega si želijo svoje znanje uporabiti za hitro pridobivanje koristi. Svoje strokovno znanje uporabljajo za krajo, zavajanje ter izkoriščanje ljudi, saj z lahkoto zaslužijo denar, ne da bi morali opraviti pošten delovni dan v službi. Kibernetski zločini so v današnjem času postali resna grožnja in se precej razlikujejo od kaznivih dejanj »stare šole«, kot so ulični rop, kraja ... Za razliko od teh kaznivih dejanj se lahko kibernetski zločini izvedejo enostransko ter tako ne zahtevajo fizične prisotnosti storilcev kaznivih dejanj. Tako so lahko kazniva dejanja storjena iz neke oddaljene lokacije, kriminalcem pa posledično ni treba skrbeti za organe kazenskega pregona v državi, kjer storijo kaznivo dejanje. Kibernetski kriminalci zdaj izkoriščajo iste sisteme, ki ljudem omogočajo lažje izvajanje elektronskega trgovanja in spletnih transakcij (Cross Domain Solution b. l.a).

3.3 Vrste spletnega kriminala

Ker se uporaba interneta vsakodnevno povečuje, se posledično tudi svet bolj povezuje. Svetovni splet (angl. *world wide* web) zveni kot velik pojav, vendar je presenetljivo ena od njegovih prednosti »zbliževanje sveta«, kar pomeni manjši kraj za življenje svojih uporabnikov. Vendar pa je svetovnemu spletu uspelo ustvariti tudi težavo za ljudi, ki preživijo dolge ure pri brskanju po »spletnem svetu« – spletni kriminal. Čeprav se organi kazenskega pregona poskušajo spopasti s temi težavami, je teh vedno več in mnogi ljudje so postali žrtve hekanja, kraje, kraje identitete in zlonamerne programske opreme. Eden najboljših načinov, da se izognete temu, da bi postali žrtev kibernetskih zločinov in da zaščitite vaše občutljive informacije, je uporaba »neprebojne varnosti«, ki uporablja enoten sistem programske in strojne opreme za overjanje vseh informacij, ki so poslane ali dostopne prek interneta (Cross Domain Solution b. l.a). Kot prikazuje slika 1, pa obstaja kar nekaj vrst kibernetskega kriminala, kjer je tarča napada lahko računalnik ali pa je računalnik uporabljen kot sredstvo za napad.

Slika 1: Vrste kibernetskega (spletnega) kriminala

Vir: Alkaabi idr. 2010.

Ker obstaja veliko vrst kibernetskega kriminala, bomo najprej opisali manj pogoste nato pa bolj pogoste vrste kriminala, ki jih bomo prav tako podrobneje razložili. Med manj pogostejše vrste kibernetskega kriminala spadajo (Panda Security 2018):

- *Botneti* (angl. *botnets*). Gre za omrežja iz kompromitiranih računalnikov, ki jih nadzorujejo oddaljeni hekerji. Prav ti hekerji nato pošiljajo neželeno pošto (angl. *spam*) ali pa preko teh botnetov napadajo druge računalnike. Botneti se lahko uporabijo tudi kot zlonamerna programska oprema in tako opravljajo zlonamerne naloge.
- *Spletno zalezovanje/nadlegovanje* (angl. cyberstalking) je vrsta kibernetskega kriminala, ki vključuje spletno nadlegovanje, kjer je uporabnik izpostavljen množici spletnih sporočil in elektronskih poštnih sporočil. Običajno spletni (kibernetski) kriminalci raje uporabljajo socialna omrežja, spletne strani in iskalnike, da bi ustrahovali uporabnika ter tako povzročili strah. Običajno spletni zalezovalci poznajo svojo žrtev ter povzročijo, da se oseba boji ali skrbi za svojo varnost.
- *PUPs ali potencialno neželeni programi* (angl. *potentially unwanted programs*) so manj nevarni od drugih kibernetskih kaznivih dejanj, vendar so vrsta zlonamerne programske opreme. Ti programi v žrtvinem sistemu odstranijo potrebno programsko opremo, vključno z iskalniki in vnaprej naloženimi aplikacijami. Vključujejo lahko vohunsko programsko opremo (angl. *spyware*) ali oglasno programsko opremo (angl. *adware*), zato je dobro namestiti protivirusno programsko opremo, da se izognete zlonamernemu prenosu.
- *Prepovedane/nezakonite vsebine* vključujejo kriminalce, ki delijo in distribuirajo neprimerne vsebine, ki se lahko štejejo za zelo zaskrbljujoče in žaljive. Žaljiva vsebina lahko vsebuje, vendar ni omejena na, spolno aktivnost med odraslimi, videoposnetke z intenzivnim nasiljem in videoposnetke o kriminalnih dejanjih. Nezakonita vsebina vključuje gradiva, ki zagovarjajo dejanja, povezana s terorizmom, in material za izkoriščanje otrok. Ta vrsta vsebine obstaja tako na vsakodnevnem internetu kot na temnem spletu ter anonimni mreži.
- *Spletne prevare* (angl. *online scams*) so po navadi v obliki oglasov ali neželenih elektronskih poštnih sporočil, ki vključujejo obljube o nagradah ali ponudbe nerealnih zneskov denarja. Spletne prevare vključujejo vabljive ponudbe, ki so »preveč dobre, da bi bile resnične«, in če žrtev klikne nanje, lahko povzroči, da se vmeša zlonamerna programska oprema, ki ogrozi informacije.
- *Izkoriščevalska oprema/kompleti* (angl. *exploit kits*) potrebuje ranljivost – napako v kodi programske opreme, da bi pridobila nadzor nad računalnikom uporabnika. To so vnaprej pripravljena orodja, ki jih spletni kriminalci lahko kupijo prek spleta in jih nato uporabijo proti vsakomur, ki ima računalnik. Ti kompleti za izkoriščanje so redno nadgrajeni kot običajno programska oprema in so na voljo na temnih spletnih forumih.

3.3.1 Najpogostejše oblike spletnega kriminala

Čeprav obstaja veliko oblik spletnega kriminala, to še ne pomeni, da so manj pogostejši tudi manj nevarni. Uporabniki interneta in računalnikov se ne zavedajo, koliko težav in nevšečnosti lahko prinese kakršen koli spletni kriminal, bodisi manj pogost ali bolj pogost. Med bolj pogoste oblike spletnega kriminala spadajo DDoS napadi, kraja identitete, socialni inženiring, internetno ribarjenje, zlonamerna programska oprema ter nezaželena elektronska pošta. V nadaljevanju bomo vsako obliko posebej razložili.

Napad za zavrnitev storitve (angl. *denial of service*) je katera koli vrsta napada, kjer napadalci (hekerji) poskušajo preprečiti dostop legitimnih uporabnikov do storitve. V takem napadu napadalec običajno pošlje pretirana sporočila, v katerih zahteva, da omrežje ali strežnik potrdi zahteve, ki imajo neveljavne povratne naslove. Omrežje ali strežnik tako ne more najti povratnega naslova napadalca pri pošiljanju odobritve overjanja, zaradi česar strežnik počaka, preden zapre povezavo. Ko strežnik zapre povezavo, napadalec pošlje več sporočil o pristnosti z neveljavnimi povratnimi naslovi. Zato se postopke preverjanja pristnosti in čakanja na strežnik začne znova, pri čemer bo omrežje ali strežnik zaseden. Takšen napad se lahko izvede na več načinov; med osnovne vrste napadov DoS spadajo (Tehnopedia b. l.d):

- poplavljanje omrežja za preprečevanje zakonitega omrežnega prometa,
- prekinitev povezav med dvema strojema za preprečitev dostopa do storitve,
- preprečevanje dostopa določenega posameznika do storitve,
- prekinitev storitve za določen sistem ali posameznika,
- prekinitev stanja informacij, kot je ponastavitev sej TCP (transportni sloj).

Druga različica DoS napada je »smurf« napad, ki vključuje elektronsko pošto s samodejnimi odgovori. Če nekdo pošlje na stotine elektronskih sporočil s ponarejenim povratnim elektronskim naslovom na stotine ljudem v neki organizaciji s samodejnim odzivnikom v njegovi elektronski pošti, prvotno poslana sporočila potencirajo v tisoče poslanih sporočil na lažen naslov elektronske pošte. Če ta lažni naslov elektronske pošte dejansko pripada nekomu, lahko ta napad preobremeni elektronsko pošto. Prav tako pa DoS napadi povzročijo veliko težav, kot so: neučinkovite storitve, dostopnost storitev, prekinitev omrežnega prometa in motnje povezave (Techopedia b. l.a).

Kraja identitete (angl. *identity theft*). Spletni kriminal vpliva tako na virtualno kot na resnično telo, vendar so učinki na vsakega različno. Kot primer lahko izpostavimo Združene države Amerike, kjer posamezniki nimajo uradnega osebnega dokumenta oziroma izkaznice, temveč številko socialnega zavarovanja, ki služi kot identifikacijska številka. Davki se zbirajo na podlagi številke socialnega zavarovanja vsakega državljana, številne zasebne ustanove pa to številko uporabljajo za spremljanje svojih zaposlenih, študentov ali pa bolnikov. Dostop do te številke omogoča zbiranje vseh dokumentov, povezanih z državljanstvom te osebe. Tudi ukradene podatke o kreditni kartici lahko uporabijo za rekonstrukcijo identitete posameznika.

Ko spletni kriminalci kradejo podatke o kreditnih karticah podjetij, ima to lahko dva različna učinka (Dennis 2019):

- pridobijo digitalne informacije o posameznikih, ki so lahko koristne na več načinov; npr. uporabijo podatke kreditnih kartic ter povzročijo visoke račune, ki nato »pripeljejo« podjetja, ki izdajajo kreditne kartice, do velikih izgub, ali pa informacije prodajo drugim, ki jih lahko uporabijo na podoben način;
- uporabijo lahko posamezna imena in številke kreditnih kartic, da bi ustvarili nove identitete za druge storilce kaznivih dejanj; npr. kriminalec lahko vzpostavi stik z banko, izdajateljico ukradene kreditne kartice, ter spremeni poštni naslov na računu, prav tako pa lahko kriminalec pridobi nov potni list ali vozniško dovoljenje s svojo sliko, a vendar z imenom žrtve, z vozniškim dovoljenjem pa kriminalci zlahka pridobijo novo kartico socialnega zavarovanja, kar pripelje do tega, da lahko odprejo tudi nov bančni račun in prejemajo posojila, žrtev pa se posledic zave šele takrat, ko ga banka obvesti o velikih dolgovih. Ne nazadnje pa lahko kriminalec uživa tudi ugodnosti države.

Socialni inženiring (angl. *social engineering*) je »umetnost« pridobivanja dostopa do zgradb, sistemov ali podatkov z izkoriščanjem človeške psihologije in ne z razpadom ali uporabo tehničnih tehnik hekanja. Na primer: namesto, da bi poskušal najti ranljivost programske opreme, socialni inženir lahko pokliče zaposlenega v nekem podjetju in se predstavi kot oseba, ki podpira informacijsko tehnologijo (IT oddelek) in poskuša zaposlenega napeljati na to, da razkrije svoje geslo (Hulme in Goodchild 2017). Pri socialnem inženiringu gre za to, da kriminalci vzpostavijo neposreden stik s posamezniki bodisi po telefonu ali po elektronski pošti. Želijo si pridobiti zaupanje posameznika in velikokrat se predstavijo kot zaposleni v službi za stranke, s čimer pridobijo zaupanje ter posledično tudi informacije, ki jih potrebujejo. Večinoma gre za gesla, informacijo o podjetju, kjer posameznik dela, ali pa bančne informacije. Velikokrat ciljajo na tiste posameznike, ki imajo dostop do informacij, in nato psihološko manipulirajo z njimi, kar pripelje do tega, da oseba razkrije zaupne informacije ali celo izvede zlonameren napad. Obstaja več vrst socialnega inženiringa (Hulme in Goodchild 2017):

- preko telefona – socialni inženir lahko pokliče in se predstavi oziroma pretvarja, da je sodelavec ali zaupanja vreden zunanji organ, kot je revizor ali pa organ kazenskega pregona;
- v pisarni – s taktiko »lepljenja« (angl. *tailgating*) lahko socialni inženir pridobi dostop do podjetja. »Ali lahko pridržiš vrata zame? Nimam ključa/kartice za dostop,« je le eden izmed trikov, kako lahko vstopijo v podjetje; enako velja za zadrževanje v prostorih, kjer zaposleni kadijo in kamor hodijo na odmore, kar lahko pripelje do tega, da mnogi ljudje preprosto ne preverijo, ali imajo res dovoljenje, da so tam;
- na spletu – socialni inženirji imajo takšna orodja, s katerimi gredo na mesta, kot so LinkedIn ali pa Facebook, in najdejo uporabnike, ki so zaposleni v podjetju, in nato zberejo veliko podrobnih informacij, ki jih lahko uporabijo za nadaljnji napad.

Ribarjenje (angl. *phishing*) je kraja podatkov, ki storilcu omogoči dostop do spletnih storitev v imenu žrtve, v skrajnem primeru pa tudi omogoči krajo denarja. Običajno storilci skušajo z elektronskim sporočilom žrtev zvabiti na lažno stran banke ali pa spletne storitve, običajno pod pretvezo, da se mora zaradi preverjanja podatkov ali nekih dodatnih ugodnosti prijaviti in »preveriti podatke«. Če na tej lažni strani (»phishing«) žrtev vpiše geslo za dostop, se ta posreduje storilcu. Gre za nezakonito pridobivanje informacij, kot so uporabniška imena, gesla, podatki o bančnem računu in kreditnih karticah, z namenom izkoriščanja žrtve oziroma uporabnikov (SI-CERT b. l.a).

Zlonamerna programska oprema (angl. *malware*) je splošen izraz za viruse, črve, trojanske konje in druge škodljive računalniške programe, ki jih hekerji uporabljajo za uničevanje in dostop do občutljivih informacij. Nanaša se na katero koli opremo, ki povzroči škodo enemu računalniku, strežniku ali računalniškemu omrežju. Obstaja več različnih načinov kategorizacije zlonamerne programske opreme. Prvi je, kako se širi zlonamerna programska oprema in kaj počne, ko uspešno okuži računalnik žrtve. Pri prvi kategorizaciji obstajajo trije različni načini, s katerimi lahko omenjena oprema okuži ciljne računalnike (Fruhlinger 2019):

- črv (angl. *worm*) je samostojen kos zlonamerne programske opreme, ki se reproducira in širi od računalnika do računalnika;
- virus je del računalniške kode, ki se vstavi v kodo drugega samostojnega programa, nato pa prisili ta program, da sprejme zlonamerno dejanje in se širi;
- trojanski konj je program, ki pa se ne more reproducirati, temveč se pretvarja, da je nekaj, kar uporabnik želi, in tako pretenta žrtev v aktivacijo programa, da lahko naredi svojo škodo in se širi.

Pri drugi kategorizaciji pa je prisotna široka »paleta« možnih tehnik napadov, ki jih zlonamerna programska oprema lahko uporabi (Fruhlinger 2019):

- vohunska programska oprema (angl. *spyware*) se uporablja za zbiranje podatkov o sumljivem uporabniku, torej »vohuni« med uporabo računalnika in podatkov, ki jih posameznik pošilja in prejema. Keylogger je posebna vrsta vohunske programske opreme, ki beleži vse pritiske na tipke, ki jih uporabnik ustvari – odlično za krajo gesel;
- korenska orodja (angl. *rootkit*) so programi ali zbirka programskih orodij, ki okužijo koren trdega diska računalnika in posledično jih je nemogoče odstraniti, razen če izbrišemo vse podatke in programe na pogonu;
- oglasna programska oprema (angl. *adware*) prisili spletni brskalnik, da se preusmeri na spletne oglase, ki si pogosto prizadevajo prenesti še več zlonamerne programske opreme;
- izsiljevalska orodja (angl. *ransomware*) šifrirajo datoteke trdega diska in nato zahtevajo plačilo, običajno v bitcoinih v zameno za ključ za dešifriranje, brez tega ključa za dešifriranje pa je matematično nemogoče, da bi žrtev ponovno pridobila dostop do svojih datotek.

Nezaželena pošta (angl. *spam*) se nanaša na uporabo sistemov za elektronsko pošiljanje sporočil, za pošiljanje nepodpisanih ali neželenih sporočil v razsutem stanju. Težava pri ustavljanju neželene pošte je v tem, da je ekonomika tega zelo prepričljiva. Medtem ko bi se večina strinjala, da je pošiljanje tovrstne pošte neetično, je strošek dostave sporočila prek neželene pošte skoraj ničen. Če se odzove le majhen delček tarč, je lahko neželena oglaševalska akcija uspešna (Techopedia b. l.c). V splošnem lahko za »spam« sporočilo štejemo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Velikokrat gre tudi za goljufije, ki prevarantom enostavno uspejo (SI-CERT b. l.b).

3.4 Najpogostejše tarče spletnega kriminala

Kibernetski kriminal je grozljiv, grozen za informacijsko dobo, v kateri živimo. Ne samo, da kibernetski kriminalci delujejo nekaznovano, temveč jim tudi sploh ni pomembno, koga bodo prizadeli. Kljub temu je kibernetski kriminal vseeno eden najpomembnejših podjetij na temnem spletu. V letu 2017 je več podjetij doživelo kibernetske napade in ogrožene so bile ogromne količine kritičnih podatkov. Dejstvo je, da so velika podjetja v ZDA, kot so Verizon, Yahoo, Uber, Whole Foods in drugi le nekatere izmed žrtev teh zločinov. Ker so takšna podjetja po navadi tarče takih napadov, bi lahko pomislili, da so mala in srednje velika podjetja izvzeta iz spletnega kriminala, a žal ni tako. V današnjem svetu ni vprašanje, »ali« boste napadeni, temveč »kdaj« boste napadeni in ali ste pripravljeni na napad, da ga bodisi v celoti preprečite ali pa preživite. Spletni kriminal narašča po vsem svetu in prizadene vse industrije z denarjem za odtekanje. Dandanes nobeno podjetje nima imunitete pred spletnim kriminalom (Menzheres 2018).

V zadnjem času je bilo veliko malih podjetij zaskrbljenih zaradi spletnega kriminala. Po mnogih opazovanjih je jasno, da večja podjetja dobijo večji medijski odziv, ko so napadena, kot pa manjša podjetja. Pravzaprav imajo hekerji zelo radi mala in srednje velika podjetja, ker imajo, za razliko od večjih podjetij, bistveno manj moči za zaščito končnih točk in ustavitev napada. V nekaterih manjših podjetjih menijo, da jih bo nameščena protivirusna programska oprema na vseh strojih na delovnem mestu zaščitila, vendar je v današnjem poslovnem okolju treba storiti veliko več, kot npr. zaščita pošte, napredna varnost končne točke, ki jo lahko uveljavlja umetna inteligenca, online in praktično usposabljanje, dvojno preverjanje pristnosti in upravljanja gesel ter zaščiteni oblaki in internetni prehodi. Še ena izmed pogostejših tarč spletnega kriminala je zdravstvena industrija, saj je vredna milijarde dolarjev in ima posledično najbolj bogate podatke na svetu. Hekerji jo imajo radi, saj vsebuje medicinske datoteke in najintimnejše podrobnosti o življenju osebe, zato so zdravstvene datoteke najbolj zaupne celo po zakonu. Prav tako so na udaru tudi odvetniške družbe, saj imajo najpametnejše ljudi na planetu, a kibernetska varnost običajno ni njihova »najmočnejša obleka«. Hekerjem so odvetniške družbe glavni cilj predvsem zaradi narave podatkov in informacij, ki jih zbirajo,

shranjujejo in uporabljajo. Osebni računalniki in mobilni telefoni so postali vse močnejši za brezhibno obravnavo aplikacij, a so vseeno še zmeraj med glavnimi tarčami hekerjev. In ne nazadnje so prav tako finančne institucije ena izmed najpogostejših tarč spletnega kriminala, saj delajo z denarjem. Ker pa je v zadnjem času kripto valuta izredno dragocena, bodo hekerji še naprej ciljali na spletne denarnice, na podružnice in izmenjave denarja. Ta vrsta valute jim najbolj ustreza, saj je splošno znano, da večine kripto valut ni mogoče izslediti. Ko torej hekerju uspe obiti varnostne protokole in pride do kovancev, ni več upanja, da bi lahko obnovili denar, ki je bil v denarnici (Menzheres 2018).

4 VPLIV HEKERSTVA IN SPLETNEGA KRIMINALA NA POSLOVANJE PODJETIJ

Spletni kriminal in hekerstvo sta postala hitro rastoča industrija, ki iz dneva v dan raste, poleg tega pa je tudi ta »industrija« zelo donosna. Ocenjuje se, da bo spletni kriminal v povprečju na leto stal približno šest milijard dolarjev vse do leta 2021. Ta številka je zagotovo ogromna in si je večina ljudi ne predstavlja, toda bolj zaskrbljujoče je, kaj to pomeni za sodobna podjetja. Vsepovsod podjetja povečujejo svoje proračune za kibernetsko varnost, da bi zmanjšali katastrofalne stroške, ki bi jih lahko prinesle morebitne zlorabe podatkov (angl. *data breach*). Ko proučujemo stranske učinke kibernetskega napada, obeti za podjetja postanejo na koncu zelo slabi. Nekatera podjetja si nikoli v celoti ne opomorejo od zlorabe in napadov, prav tako pa lahko pride do nekaterih katastrofalnih posledic. Čeprav lahko s proaktivno varnostno držo in preventivnimi ukrepi »ublažimo« napade, to še ne pomeni, da se zloraba ne more zgoditi. Podjetja v nekaterih panogah so bolj izpostavljena tovrstnim napadom, kar vedo tudi delničarji, ko pa pride do zlorabe oziroma napada, lahko sledi strm padec zaznane vrednosti podjetja. Negativni mediji in njihovi članki lahko poganjajo misel skupine »prodaj zdaj« in ko se vlak začne premikati, ga je zelo težko obdržati na tirnicah. To še posebej velja za manjša podjetja, ki nimajo korporativne infrastrukture ali pa prepoznavnosti blagovne znamke, da bi ob napadu ohranili stvari na površju. Investitorji in delničarji želijo, da je njihov vložen denar v varnih podjetjih, za katere sklepajo, da jim je mogoče zaupati. Preprosta logika nam pove, da je slab pritisk medijev na zlorabe podatkov enak javnemu nezaupanju, vsaj kratkoročno. Če je ta kratkotrajni udarec dovolj velik oziroma močan, lahko podjetje dolgoročno oslabi (Eubanks 2017).

4.1 Rezultati spletnega kriminala

Spletni kriminal je »nedavni dodatek« k seznamu kaznivih dejanj, ki nas zadevajo neposredno ali posredno. Kriminal na splošno slabo vpliva na podjetja ne glede na vrsto kriminala. Spletni kriminal je lahko vsakršno kaznivo dejanje, ki sega od hekanja (vohunskega) do bolj resnih dejanj, ki lahko škodujejo intelektualni lastnini (uničevanje spletnih strani) (Herselman in Warren 2004).

Zlorabe podatkov se in se bodo dogajale tako dolgo, dokler podjetja ohranjajo evidence in hranijo zasebne in občutljive podatke. Vendar pa so se v zadnjem desetletju povečali število podatkov, tehnološki napredek in digitalizacija shranjevanja podatkov, kar kaže na močno povečanje števila kršitev pri ravnanju s podatki. Od leta 2005 naprej so se zgodile vse največje kršitve podatkov v zgodovini, velikost in obseg teh kršitev pa se iz dneva v dan povečuje (Clickatell 2017). V nadaljevanju bomo preučili nekatere od teh kršitev in njihove učinke na podjetja (Pribanic 2018):

- *Omadeževan ugled*. Spletni kriminal lahko v veliki meri vpliva na poslovanje podjetij s tem, da škoduje ugledu in dobremu imenu podjetja, kar zavira rast blagovne znamke

oziroma vodi k propadu. Zelo pomembno je, da se zavedamo, da informacije, ki jih objavimo na spletu, ostanejo tam večno in jih je zelo težko izbrisati, kar privede do tega, da je zelo pomembno zaščititi podatke o strankah in podjetju pred kibernetskimi kriminalci. Kršitev podatkov je škodljiva za podjetja, saj ne samo, da uničuje zaupanje strank, ampak tudi povzroča to, da javnost dojema podjetje kot slabo opremljeno in preprosto za napad.

– *Škoda intelektualne lastnine*. Vpliv spletnega kriminala ni škodljiv le za ugled podjetja, ampak lahko škoduje tudi intelektualni lastnini podjetja. Če bi podjetje utrpelo kibernetski napad, pri katerem bi napadalci ukradi zamisli podjetja, tržne kampanje ali pa načrte za širitev poslovanja, bi podjetje izgubilo konkurenčno prednost, ki jo je nekoč imelo pred drugimi podjetji na trgu. Heker, ki bi ukradel te ideje in načrte, bi jih zlahka izpostavil ali pa prodal konkurentom in tako bi ideje postale neuporabne, to pa bi za podjetje pomenilo izgubo dragocenega časa in dela, ki so ga posvetili tem idejam in načrtom. Ne samo, da bi razkritje teh idej stalo zaposlene veliko časa, ki so ga vložili vanje, ampak bi to lahko škodovalo tudi rasti poslovanja in dobičku, ki bi ga podjetje pridobilo, če njihovi podatki ne bi bili kršeni.

4.2 Preprečitev spletnega kriminala

V današnjem času vedno več uspešnih podjetij, tako domačih kot svetovnih, izkorišča to, kar jim internet ponuja. Spletni trgovci in druge spletne storitve računajo na to, da jim bo internet prinesel uspeh. Prav tako se vse več tradicionalnih podjetij povezuje z internetom, saj je to nekaj, kar potrošniki ne samo pričakujejo, ampak celo zahtevajo. Tako so podjetja povečala svoja prizadevanja, da izkoristijo vse, kar ponuja internet. Vendar pogosto pozabljajo na enega od najpomembnejših vidikov prisotnosti na spletu. V večini primerov pozabijo skrbeti za varnost na internetu ter tako postanejo lahka tarča spletnega (digitalnega) izsiljevanja (Gary 2016). Kot smo v prejšnjih poglavjih že omenili, gre za napade s posebnimi vrstami zlonamernih programov, ki se imenujejo »ransomware«. Ti programi tako zaklenejo okužen računalnik oziroma več računalnikov v nekem podjetju ter za odklepanje zahtevajo odkupnino. Težava pri vsem tem je, da za te vrste virusov ne obstajajo »zdravila«. Edino, kar lahko storimo, je to, da se predhodno zaščitimo ter tako zmanjšamo možnost takih napadov.

Ključ za zaustavitev kibernetskih kriminalcev je spoznati, kako dejansko delujejo. Če vemo, kako bo napadalec izvedel svoj napad, lahko postavimo obrambo, ki ga bo zaustavila. V nadaljevanju bomo našteli metode, ki jih uporabljajo spletni kriminalci, ter kako jim napade preprečiti (Gary 2016):

– *Elektronska pošta.* Nevarnost zlonamerne programske opreme in spletnega kriminala prek elektronske pošte ni nova. Ves čas se ljudi ozavešča, da naj ne odpirajo nobene elektronske pošte, ki prihaja iz neznanega vira, ter da ne smejo klikniti povezav v elektronskih poštnih sporočilih. Kibernetski kriminalci bodo še naprej uporabljali

elektronska poštna sporočila v te namene, zato je naloga podjetja, da se prepriča, da počnejo vse, kar je v njihovi moči, da je elektronska pošta varna. Programska oprema za šifriranje elektronske pošte lahko doda raven zaščite, zaradi katere kriminalci »gledajo« drugje. Programska oprema za preprečevanje zlonamerne programske opreme (angl. *anti-malware software*) za izboljšanje kibernetske varnosti s pomočjo sistema za zaznavanje preprečevanja vdorov lahko pomaga zagotoviti, da prejeta zlonamerna elektronska pošta ne povzroča škode podjetju.

- *Neprestano usposabljanje/ozaveščanje.* Zaposlene v podjetju je treba naučiti, kako ustvariti močna gesla in kako jih redno spreminjati. Zaposleni morajo razumeti nevarnosti elektronske pošte in morajo vedeti, kako lahko varno uporabljajo internet. Naučiti jih je treba, da pred odhodom iz službe preverijo, ali so njihovi računalniki zaklenjeni in zaščiteni z geslom. Vsi zaposleni v podjetju morajo biti usposobljeni za kibernetsko varnost, prav tako jih je treba spremljati, da bi si podjetje zagotovilo, da sledijo varnostnim politikam, uporabljajo prava orodja in da ne ogrožajo poslovanja z odpiranjem luknjic za prepletanje kibernetskih zločincev. Če kateri izmed zaposlenih ponavlja napake, je treba opraviti več usposabljanj.
- *Uporaba zaščite pred zlonamerno programsko opremo*. Na voljo je veliko programov za zaščito pred zlonamerno programsko opremo; prilagojeni so poslovnim namenom. Programska oprema je eno najučinkovitejših orodij, ki jih mora podjetje imeti, da ustavijo spletni kriminal, preden se zgodi. Programska oprema ni popolna, saj je možno, da kibernetski kriminalci najdejo pot okoli nje, vendar to ni največja težava, ki bi jo podjetje lahko imelo. Da bi podjetje uporabljalo programsko opremo, se mora prepričati, da zaposleni vedo, kako jo uporabljati. Programska oprema mora biti vedno posodobljena, uporabljati jo je treba na vseh računalnikih v podjetju ter ne nazadnje mora biti vedno vključena.

4.3 Zaščita podjetij pred hekerskim vdorom

V malih podjetjih velikokrat menijo, da niso primarna tarča kibernetskim kriminalcem, vendar pa lahko ta predpostavka povzroči veliko napako, če podjetje ni sprejelo ustreznih varnostnih ukrepov za varovanje podatkov podjetja. Dejstvo je, da vedno več kriminalcev cilja na manjša podjetja, in sicer preprosto zato, ker niso izvedli oziroma uvedli ustreznih zaščitnih ukrepov, da bi svoje poslovanje zaščitili pred morebitnimi kibernetskimi napadi. Tako mala kot velika podjetja morajo izvesti naslednjih osem korakov, da bi preprečili tovrstne napade (Manning 2015):

- *Ustanovitev notranje politike* – zelo pomembno je, da so vodilne službe ter informacijska služba na tekočem z najnovejšimi prevarami, ki se odvijajo, prav tako pa se tega morajo zavedati tudi vsi zaposleni.
- *Učiti se iz napak drugih* – zelo velikokrat se piše o različnih kibernetskih vdorih in razkritjih zasebnih podatkov, kar privede do precejšnjih finančnih izgub. Tako se druga

podjetja lahko naučijo na napakah drugih in »pridobijo« iztočnice za sprejemanje bolj ozaveščenih odločitev o podobnih vprašanjih v zvezi s spletnimi vdori.

- *Posodabljanje računalnikov* – je ena izmed najpreprostejših strategij, ki jo lahko podjetje uporabi. Podjetje mora biti pozorno na vsa obvestila o posodobitvah operacijskih sistemov, protivirusni programski opremi, spletnih brskalnikih in požarnih zidovih. Zanemarjanje katerega koli od teh obvestil pušča razpoke v obrambnem sistemu podjetja, zato je pomembno vzdrževati posodbljenost celotnega omrežja.
- *Uporaba storitev v oblaku* – mnoga podjetja prihranijo čas in denar z uporabo storitev v oblaku za obravnavanje potreb svojih aplikacij in shranjevanje podatkov. Uporaba te storitve je velikokrat malim podjetjem velik finančni zalogaj, vendar pa lahko z uporabo oblaka podjetje dobi enako raven računalniške obdelave podatkov za minimalno mesečno naročnino.
- *Vedeti, česa ne storiti* – dodajanje požarnih zidov in filtrov na platformo, ki je že negotova, je v bistvu enako, kot pritrjevanje ključavnice na zaslonska vrata. Sčasoma bodo kibernetski kriminalci našli ranljivost, zato mora podjetje odkriti, kje so glavne težave, in potem tudi najeti strokovnjaka, ki bo težavo popravil. To je edini način, da podjetje zagotovi, da bo sistem ostal varen.
- *Povečanje ozaveščenosti zaposlenih* – je ena izmed najbolj stroškovno učinkovitih metod za preprečevanje spletnega kriminala. Pomembno je razumeti, da se kibernetski napadi pojavijo takrat, ko imajo hekerji dostop do prenosnega računalnika nekega zaposlenega. Zato je pomembno, da podjetje izvaja usposabljanje na področju zasebnosti.
- *Ustvarjanje močnih gesel ter njihovo posodabljanje* – veliko varnostnih strokovnjakov meni, da nikoli ne smemo uporabljati istega gesla za vse svoje račune. S tem samo »privabljamo« hekerje, da nam ukradejo naše osebne podatke. Zaposleni morajo poskusiti ustvariti gesla, ki združujejo številke, simbole in druge znake, prav tako pa je treba gesla spreminjati vsakih nekaj mesecev.
- *Najem strokovnjaka za varnost* – eden izmed najboljših načinov, da podjetje odkrije, ali so v infrastrukturi kakršne koli luknje ali varnostna tveganja, je, da najame varnostnega svetovalca. Čeprav to mogoče zveni kot dodaten in nepotreben strošek, je dejansko neprecenljiva storitev, ki lahko podjetju pomaga prihraniti kar nekaj denarja in frustracij, ki bi jih prizadele v primeru napada. Prav tako velika podjetja, kot je npr. Facebook, ustvarijo programe, ki nagrajujejo tiste, ki raziskujejo varnost spletne strani. To so pravzaprav etični hekerji, ki pomagajo videti, kje se lahko v podjetju skrivajo varnostna tveganja.

5 EMPIRIČNI DEL – RAZISKAVA O VARNEM NAČINU »BRSKANJA NA SPLETU« ZA FIZIČNE OSEBE TER NAČINI ZAŠČIT PRAVNIH OSEB OZIROMA PODJETIJ

V empiričnem delu zaključne projektne naloge smo s pomočjo slovenskih strokovnjakov s področja informatike raziskali, proučili in opredelili, kako varno brskati na spletu.

Prav tako smo izvedli kvalitativno raziskavo v obliki polstrukturiranega intervjuja. Prvi intervju smo izvedli z generalnim direktorjem direktorata informacijske družbe na Ministrstvu za javno upravo, gospodom dr. Urošem Svetetom, drugi intervju pa z vodjo nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, Arnes Gorazdom Božičem.

5.1 Intervju z generalnim direktorjem direktorata za informacijsko družbo na Ministrstvu za javno upravo

V prvem delu smo izvedli kvalitativno raziskavo v obliki polstrukturiranega intervjuja. Intervju z generalnim direktorjem direktorata za informacijsko družbo na Ministrstvu za javno upravo je potekal v torek, 11. junija 2019, v Ljubljani. S pomočjo njegovih odgovorov smo želeli raziskati in pridobiti čim več informacij s področja spletnega kriminala na ravni države, in sicer o tem, kako država poskrbi za podjetja ter fizične osebe v primeru hekerskih napadov. Prav tako smo želeli ugotoviti, kako je to področje zakonsko urejeno oziroma ali obstaja kazenski zakonik, ki pokriva to področje v primeru tovrstnih napadov.

Za začetek smo želeli, da nam dr. Svete pove, ali so državni organi tarče hekerjev v Sloveniji in, če so, ali so kateri organi bolj dovzetni za takšne napade. Dr. Svete nam je povedal naslednje:

> Seveda, ni nobenega dvoma, da so tudi državni organi tarča kibernetskih napadov, pri čemer je treba vedeti eno zadevo – sama identifikacija napadov, torej pri ogromno napadov se lahko zgodi, da ostanejo nezapisljivi oziroma se jih ne detektira, in če nimajo nekega konkretnega učinka oziroma se ti napadi ne razvijejo v nek večji incident, se praktično ne štejejo v nobeno statistiko. V državni upravi imamo več omrežij, med katerimi so nekatera popolnoma zaprta, druga so hibridna, tretja pa povezana v internet in temu ustrezno se število napadov lahko ocenjuje, kje je teh napadov največ, zagotovo pa je največ tistih, ki prihajajo iz zunanjega sveta, torej tista omrežja, ki so odprta v internet. Opažamo tudi porast groženj, ki se odvijajo preko mobilnih telefonov, saj se mobilni telefoni v Sloveniji uporabljajo kriptirani, ampak v zelo omejenem obsegu, tudi v državni upravi in je pravzaprav na ta način najlažje priti preko socialnega inženiringa oziroma neke druge prevare do točk, ki jih hekerji ciljajo.

Skozi pogovor smo želeli ugotoviti, ali je tako v Sloveniji kot v Evropi gospodarsko vohunjenje pogosto in kaj bi gospodarstvo kot tako lahko naredilo, da se izogne tovrstnim napadom. Dr. Svete nam je povedal, da je brez dvoma gospodarsko vohunjenje prisotno tako med posameznimi podjetji kot tudi med posameznimi državami. Takšnih primerov je javno

znanih ogromno, kot primer lahko izpostavimo sistem Echelon, ki se je v hladni vojni uporabljal za nadzorovanje določenih držav, ki so bile znotraj zavezništva v NATO ali pa v Evropski uniji. Še eden izmed takih primerov je očitanje gospodarskega vohunjenja med Nemčijo in Kitajsko. Takih primerov je ogromno in dejstvo je, da se to dogaja. Povedal nam je tudi, da so se nekatera podjetja lotila svoje informacijske varnosti že v 70-ih letih prejšnjega stoletja, kot na primer Boeing, ki je kot prvi uvedel termin »informacijsko vojskovanje« še preden so ta termin uvedle v uporabo države, oborožene sile itd. Boeing je to v notranjem komuniciranju uporabljal že v začetku 80-ih let, poleg tega pa lahko podjetja s pomočjo tehničnih ukrepov izboljšajo svojo informacijsko varnost, kot npr. varne sobe (faradeyeva kletka), tihe sobe (angl. *silent room*), kjer ni nobene možnosti komuniciranja. Vse več podjetij se zgleduje po ukrepih obveščevalnih služb; torej, da morajo vsi, ki vstopijo v stavbo, pustiti elektronske naprave pri recepciji. Prav tako se vse več izvajajo penetracijski testi, za kar podjetja plačujejo tako imenovane etične hekerje. Prav tako podjetja vse več pozornosti namenjajo izobraževanju zaposlenih na tem področju, saj so ugotovili, da je največja težava notranji napad.

Dr. Svetetu smo nato zastavili vprašanje, ali v Sloveniji obstaja organizacija oziroma organ na državni ravni, ki obvešča tako »domače uporabnike« ter podjetja o napadih ter jim svetuje, kako se zavarovati. Povedal nam je, da v Sloveniji v skladu z zakonom o informacijski varnosti, ki je bil sprejet maja 2018, obstaja nacionalni CSIRT. Zelo pomembno je, da ne zamešamo kratice s SI-CERT, ki je oddelek oziroma en del na Arnesu in je od 1. januarja 2019 nacionalni CSIRT (angl. *computer security incident response team*). Pri tem centru se prijavljajo incidenti sicer še prostovoljno ter jih potem obravnavajo in nato preko svojih kanalov obveščajo in izdajajo opozorila posameznikom in podjetjem. Na državni ravni pa obstaja tako imenovani CSIRT državnih organov, ki je tudi aktualen od 1. januarja 2019, to vlogo pa opravlja sektor za informacijsko varnost znotraj direktorata za informatiko na Ministrstvu za javno upravo in tam je pravzaprav SOC (angl. *security operating center*) za državno upravo. Poleg tega imajo določene institucije svoje varnostne operacijske centre, kot npr. policija, SOVA, vojska in druge.

Na vprašanje, ali v Sloveniji obstaja zakonski pravilnik, s katerim bi kaznovali hekerja, če bi ga »ujeli na delu«, nam je dr. Svete povedal, da obstaja kazenski zakonik, v katerem lahko najdemo določene člene, ki se tičejo kriminala kot takega ter nepooblaščenih vstopov v informacijski sistem, ki se štejejo kot kaznivo dejanje v kazenskem zakoniku.

Pri naslednjem vprašanju, ali so se na slovensko vlado že obrnile večje glasbene in filmske založbe v primerih kraje filmov, ki so bili namenjeni za presojo morebitne nagrade in ali je Slovenija zaostrila zakonodajo na tem področju, nam je povedal, da na direktoratu za informacijsko družbo takih primerov niso imeli ter da je to »stvar« Ministrstva za kulturo ter SAZAS-a.

Nato smo dr. Sveteta vprašali, koliko je že bilo pozivov, da bi Slovenija omejila dostop do določenih strani, kot je to poskusila v primeru udba.net (ko so žvižgači objavili določene podatke, ki niso bili po godu vplivnežem). Povedal nam je naslednje:

> Pozivov je bilo že kar nekaj, a vprašanje, ki se pojavi tukaj, je, koliko jih je bilo realiziranih. Slovenija lahko z inšpekcijo naloži operaterjem, da omejijo dostop do neke spletne strani, kot v primeru udba.net, druga možnost pa je, da določeni lastniki platform sami blokirajo določene vsebine, ki so dostopne za Slovenijo; recimo kot uporabniki Googla imamo drugačen Youtube, kot je npr. v Belgiji ali pa v Združenih državah Amerike, v nekaterih primerih pa te platforme v državi celo ni. Število takšnih poskusov oziroma idej je upadlo, še posebej zato, ker se je P2P (angl. *peer-to-peer*) komunikacija precej razširila, da bi danes praktično, če bi prišlo do neke take odločitve, zelo težko dosegli svoje.

Še eno izmed vprašanj, ki smo ga zastavili dr. Svetetu, se je glasilo: »Koliko je bilo do sedaj žrtev med podjetji pri tako imenovanih nigerijskih prevarah in ali so še vedno žrtve tudi podjetja?« Povedal nam je, da točnega podatka nima, ampak da je edina baza podatkov, ki obstaja, baza SI-CERT-a, ki je tudi javna. V letnih poročilih lahko najdemo število obravnavanih incidentov in klasficiranih glede na posamezno vrsto incidenta. Izpostavil je tudi problem, da mnoga podjetja ne priznajo, da so bila napadena, saj če priznajo, da so bila napadena in zahtevajo pomoč, s tem pokažejo, da so šibka, kar lahko vpliva na njihov tržni položaj. Poleg tega nastaja vse več varnostnih operacijskih centrov v podjetjih. V Sloveniji lahko izpostavimo kot primer podjetja, ki ima svoj varnostni operacijski center Telekom Slovenije, ampak oni sami vodijo svojo statistiko, ki pa ni javna, saj je to poslovna skrivnost. Prav tako nam je zaupal, da je Slovenija implementirala NIS (angl. *network information security*) direktivo (EC 2019), ki sicer ni slovenska iznajdba. To direktivo je Slovenija sprejela v letu 2016 na ravni Evropske unije in nato v letu 2018 (v zakonu) to tudi implementirala. Ta direktiva omenja tako imenovane izvajalce bistvenih storitev. V letu 2019 bodo določili izvajalce bistvenih storitev, stvar je trenutno v fazi sprejemanja podzakonskih aktov in ko bodo enkrat določeni, to je zdravstvo, okolje, energija, prehrana, oskrba z vodo, torej vsi razen operaterjev, saj so ti zavezani po drugem zakonu – po zakonu o elektronskih komunikacijah. Vsi sklopi teh podjetij bodo zavezani, da bodo poročali nacionalnemu CSIRT-u tako, da bodo vsekakor morali poročati o napadih in prav tako bodo pod nadzorom inšpekcije (država bo preverjala, ali imajo neko varnostno politiko, standarde itd.).

Na zadnje vprašanje, ali vlada pomaga slovenskim žrtvam kraje identitete, ki so zadnje čase pogoste, in ali obstajajo kakšna priporočila o tem, kakšen je postopek v takem primeru, nam je dr. Svete povedal:

> Slovenija zaenkrat še nima elektronske identitete, država še ne izdaja elektronske identitete, bo pa to storila v kratkem oziroma delamo na tem tukaj na direktoratu; gre za zakon o elektronski identifikaciji, ki naj bi bil sprejet v roku enega leta in država bo nato predvidoma na osebni izkaznici izdala e-identiteto na nekem čipu na izkaznici. V tem primeru bo država morala zagotoviti zaščito in ukrepe, če se to zlorabi. Do takrat pa za to jamčijo izdajatelji certifikatov, kot

npr. Nova Ljubljanska banka, Halcom, Sigenca, Pošta Slovenije in drugi. Pri izsiljevalskih virusih pa pomaga SI-CERT z nasveti, kako se pogajati s hekerji, kakšne so tehnike pogajanj in podobno.

5.2 Intervju s predstavnikom SI-CERT, Arnes

V drugem delu empiričnega dela zaključne projektne naloge smo izvedli kvalitativno raziskavo v obliki polstrukturiranega intervjuja s predstavnikom oziroma vodjo slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, Arnes, Gorazdom Božičem. Intervju je potekal v četrtek, 13. junija 2019, v Ljubljani. S pomočjo njegovih odgovorov smo želeli raziskati in pridobiti čim več informacij na temo hekerstva in spletnega kriminala ter kako ta vplivata tako na posameznika kot na podjetja.

Najprej smo g. Božiča vprašali, katere vrste hekerskih napadov so najbolj pogoste v Sloveniji in tudi na splošno ter, ali obstaja določen »tip« napadov in ali meni, da za tem stoji nek tehten razlog. Odgovoril nam je:

> Na splošno bi rekel, da je veliko podtikanja škodljive kode, se pravi raznoraznih virusov, njihova funkcija je po navadi kraja podatkov, gre za tako imenovane »key loggerje«, ki beležijo gesla za dostop do raznoraznih storitev na spletu, kot je e-bančništvo. Potem lahko tudi kradejo certifikate in jih tudi prekopirajo. Veliko je »phishing« napadov, kjer gre zopet za krajo pristopnih podatkov. Že dve leti pa opažamo razširjene napade na podjetja s tako imenovano »direktorsko prevaro«, kjer gre za socialni inženiring. Pri tej vrsti napada storilci pridobijo podatke s spleta o tem, kdo je direktor podjetja, računovodja podjetja in potem v imenu direktorja pošljejo račun v računovodstvo, da nakažejo neko vsoto na drug račun. Bolj kompleksni napadi pa so vrivanje v poslovno komunikacijo (angl. *man-in-the-email*), kjer gre za vdor v poštni predal podjetja v Sloveniji ali pa tujega partnerja. Storilci potem spremljajo pošto, bodisi jo preusmerijo oziroma dodajo preusmeritev kopije na svoje poštne predale in tako spremljajo poslovno komunikacijo. V pravem trenutku, npr. ko pride do nakupa oziroma prodajnega procesa, pa goljufi vskočijo v ta proces z opozorilom, da se je spremenil transakcijski račun, na katerega mora podjetje nakazati denar. Tukaj gre seveda za velika oškodovanja. V lanskem letu je znašalo posamično oškodovanje 170 tisoč evrov. Tukaj so tarče predvsem mala in srednje velika podjetja, in sicer zato, ker morajo biti fleksibilna in se morajo v hipu »obrniti« in zagrabiti posel takoj, večja podjetja pa imajo bolj kompliciranе računovodske procese in sisteme odobritve nakazil. Javni sektor je tukaj popolnoma imun zaradi zakona o javnem naročanju, ker velike količine denarja ni mogoče kar preprosto vplačati na nek račun.

Nato smo g. Božiča vprašali, ali obstaja podatek, kdaj je bil izveden prvi hekerski napad v Sloveniji, in ali meni, da je od takrat število napadov naraslo ter so napadi postali še toliko bolj nevarni za uporabnike. Povedal nam je, da so prvo prijavo incidenta na internetu v Sloveniji obravnavali leta 1995, verjetno pa so se hekerski napadi takrat že dogajali. To so bili začetki komercialnega interneta; v veliki meri je bil takrat v uporabi še v akademski sferi, sredi devetdesetih let pa se je začela komercializacija in širitev interneta med podjetji in domačimi uporabniki. Zagotovo pa njihova statistika kaže porast prijav, kar lahko vidimo v

letnih poročilih, kjer najdemo tudi grafe rasti. Kar se hekerjev tiče, nam je povedal, da so ustvarili tudi dokumentarni film, ki se imenuje Hekerji.si, govori pa o razvoju hekerske skupnosti v Sloveniji in gre skozi štiri poglavja oziroma faze; prvo poglavje je hekanje kot raziskovanje, poskušanje, kaj se da narediti, pa vse do tega, kako poznamo hekerstvo danes, ko je v ozadju vedno neka finančna korist. Vsekakor pa so tudi napadi od leta 1995 postali bolj zapleteni in vse pogosteje so tarče hekerjev uporabniki, saj smo vedno bolj prepredeni z internetom in smo zato tudi večja tarča. Narašča pa je tudi socialni inženiring, kjer gre za »hekanje možganov« – na psihološki ravni človeka, saj ga je ceneje izvesti, saj je za tehnični hekerski napad treba najeti strokovnjake, ki ga bodo znali izvesti, medtem pa socialni inženiring lahko izvedejo tudi tisti ljudje, ki so nagnjeni k temu, da znajo manipulirati z ljudmi.

Na vprašanje, katere so bolj pogoste tarče hekerjev v Sloveniji (domači uporabniki ali podjetja), nam je g. Božič povedal, da se tu pojavi vprašanje, koliko imamo vpogleda in kaj se dejansko dogaja v velikih podjetjih. Res je, da imajo takšna podjetja močne IT-ekipe, prav tako pa vidijo, da se nekatera podjetja, kot so banke, zagotovo zavedajo pomena informacijske varnosti, saj z bančnim sektorjem tudi sodelujejo in vidijo, da so poskusi napadov nanje in na komitente bank itn. Bančni sektor je tisti, ki je med prvimi posloval na internetu in se zaveda nevarnosti, ki jim pretijo, zato imajo že sami po sebi polno predpisov v zvezi z rabo interneta in za skladnost z raznimi standardi; ne nazadnje se zavedajo informacijske varnosti ter vedo, da morajo ščititi poslovne skrivnosti podjetja (npr. Krka, Petrol ipd.). V srednje velikih podjetjih pa je tega zavedanja žal manj v primerjavi z večjimi podjetji, ki skrbijo za informacijsko varnost, saj je zanje to pravzaprav strošek. Pri domačih uporabnikih obstaja nek »profil« napadov, in sicer na družbenih omrežjih, pri spletnem nakupovanju, brskanjem po novicah in zabavnih vsebinah, kjer lahko z generičnimi nasveti zmanjšamo tveganja na internetu.

Skozi pogovor smo želeli ugotoviti tudi, ali hekerji, ki izvajajo napade, prihajajo iz Slovenije ali iz tujine in ali je mogoče slediti izvoru napada. Gospod Božič nam je povedal naslednje:

> Oboje. Več je napadov iz tujine prvič zato, ker smo majhna država. Res je tudi, da je razvoj nekega hekanja v smislu izvajanja kriminalnih dejanj povezano tudi s stanjem v družbi, se pravi da mora biti klima ugodna za razvoj nekega »hekerskega podzemlja« oziroma kriminala, povezanega s hekanjem. Slovenija ni najbolj ugodna za razvoj takega kriminala, kar je pravzaprav dobro, saj gre za kriminalno dejavnost, v Sloveniji pa imamo dokaj stabilno družbo, kjer še zmeraj ni velikih socialnih problemov. V primerjavi z vzhodno Evropo (predvsem Ruska federacija) pa se tam takega kriminala dogaja veliko. Sledenje izvoru napada pa je odvisno od primera; včasih ga lahko izsledimo, saj vemo, da goljufije prihajajo iz podsaharske Afrike, torej socialni inženiring in raznorazna izsiljevanja, napadi z izsiljevalskimi virusi in drugo škodljivo programsko kodo dostikrat izvirajo iz vzhodne Evrope, torej Ruske federacije in njene okolice, in v posamičnem primeru, odvisno od tega, kako dobro se storilec skrije, ga lahko včasih najdemo, včasih pa ne, saj se dobri hekerji znajo dobro skriti.

Še eno izmed vprašanj, ki smo ga zastavili g. Božiču, je bilo, ali meni, da v je v Sloveniji v primerjavi s tujino manj hekerskih napadov in če je tako, ali za to obstaja kakšen razlog. Povedal je, da tukaj ni geografskih mej in da je Slovenija izpostavljena prav toliko kot druge države. Dodatno vprašanje je, ali imamo na državni ravni dovolj dobro zastavljeno odzivanje na incidente in neko koordinacijo, vizijo, kaj želimo s kibernetsko varnostjo doseči. Zaupal nam je, da je to področje, kjer v Sloveniji »šepamo« tako kot na drugih področjih v državi.

Na vprašanje, ali se domači uporabniki in podjetja velikokrat obrnejo na njihov center v primeru hekerskih napadov, je g. Božič odgovoril, da v letošnjem letu pričakujejo, da bodo obravnavali okoli tri tisoč incidentov. Prijav je več, ampak jih porazdelijo, saj potem istovrstne prijave obravnavajo kot en incident, tako da pričakujejo tudi čez štiri tisoč letnih prijav, prošenj za pomoč. Prav tako se število prijav iz leta v leto povečuje.

Nato smo g. Božiču zastavili vprašanje, kako obveščajo slovensko javnost o nedavnih napadih in ali to vpliva na »razgledanost« ljudi o tej tematiki. Povedal nam je naslednje:

> Sigurno. Leta 2011 smo začeli z nacionalnim programom ozaveščanja varninainternetu.si, kjer z jasnimi navodili in opisi groženj in tveganj poskušamo to področje čim bolj približati vsem uporabnikom in podati zelo jasna navodila, kako zmanjšati ta tveganja. Javnost obveščamo preko družbenih omrežij, včasih na tiskovnih konferencah, mediji nam tudi na družbenih omrežjih sledijo in potem tudi odreagirajo, sicer odvisno od tega, kaj objavimo, in potem presodijo, ali je to zanimivo za širšo javnost. Sem pa zelo zadovoljen, da smo tako dobro razvili sodelovanje z mediji, da v bistvu ni treba vsakič sklicati tiskovne konference, ampak lahko na Twitterju in Facebooku objavimo in vemo, da bodo medijske hiše to opazile in bo naslednji dan to v časopisih in zvečer pri poročilih.

Nato smo g. Božiča vprašali, kako bi svetoval tako ljudem kot podjetjem, da se zavarujejo pred nevarnostmi na spletu. Povedal je, da naj predvsem poiščejo strokovno pomoč, saj pri majhnih podjetjih še vedno opažajo pristop k IT-rešitvam, da saj nekdo ima nekega znanca, ki študira računalništvo in potem bo on naredil neko aplikacijo. Pove nam, da to ni profesionalen pristop, saj se kasneje lahko pojavijo težave, saj ima taka aplikacija lahko neke luknje, skozi katere bo napadalec namestil neke »zoprne stvari« in bo strežnik podjetja začel »metati ven« spam pošto, kar lahko privede tudi do vrivanja v poslovno komunikacijo. IT je stvar, ki se je moramo lotiti na strokovno ustrezen način in predvsem pri malih podjetjih to še zmeraj ni na zadostni ravni. Za uporabnike svetujejo, naj bodo previdni pri prejemanju ponudb, sledijo naj navodilom operacijskega sistema in nadgrajujejo protivirusno zaščito ipd., prav tako pa naj uporabijo »zdravo pamet« in pomislijo, zakaj nam nekdo zdaj ponuja loterijske zadetke, če pa nismo vplačali nobene srečke, vsekakor pa svetuje, naj delamo varnostne kopije računalnika. G. Božič nam je še povedal, da možnost, da bi se domači uporabniki popolnoma izognili vsem hekerskim dejavnostim, na žalost ne obstaja, razen če bi se popolnoma odklopil od interneta.

Na zadnje vprašanje, ali so etični hekerji pogosti v slovenskih podjetjih in ali meni, da so pomemben del organizacij, nam je g. Božič povedal naslednje:

> Pri etičnem hekanju je vedno problem definicija, saj se vsem zdi, kaj naj bi bil etični heker, ampak ni nekega slovarskega zapisa. Mislim, da so pomemben del, saj se hekerji, ki raziskujejo, zavedajo, zakaj to delajo, in poznajo mejo, ki je ne smejo prestopiti. Znotraj strokovne javnosti – torej tisti, ki se ukvarjajo z informacijsko varnostjo – jih najemajo, izven tega pa pojem ni znan in ne vidijo potrebe po takem kadru.

6 SKLEP

V današnjem času, ko se dogajajo velike spremembe tako na tehnološkem področju kot v življenju, je težko slediti vsem »inovacijam«, pa čeprav hekerstvo in spletni kriminal nista novost, se pa nenehno izboljšujeta in postajata tako ljudem kot podjetjem vse bolj nevarna. Zelo pomembno je, da se ljudje in podjetja zavedajo, da tehnologija napreduje zelo hitro, ter se začnejo tudi informirati o tem, saj lahko v nasprotnem primeru to pripelje do nasprotnega učinka. Prav tako je zelo pomembno vedeti, kaj je hekerstvo in kaj spletni kriminal, in sicer se hekerstvo nanaša na dejavnosti hekerjev, ki poskušajo ogroziti delovanje digitalnih naprav, kot so računalniki, pametni telefoni ipd., spletni kriminal pa je kot vsak drug kriminal, saj je to delo kriminalcev, ki imajo tehnološke spretnosti in z uporabo interneta dosežejo svoje zlonamerne cilje. Poznamo ga v dveh oblikah, in sicer kot enkraten zločin – namestitev virusa, ki krade osebne podatke iz računalnika, ter kot kaznivo dejanje – spletno ustrahovanje, izsiljevanje itd.

Z izvedenima kvalitativnima raziskavama v obliki intervjuja z generalnim direktorjem direktorata informacijske družbe na Ministrstvu za javno upravo, gospodom dr. Urošem Svetetom, ter z vodjo slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, Arnes, gospodom Urošem Božičem, smo prišli do nekaj ključnih ugotovitev, kako pride do varnosti na spletu ter kako se zavarovati, tako kot domač uporabnik interneta kot podjetje. Vsekakor smo vsi uporabniki interneta tarče hekerjev in njihovih napadov in ne nazadnje je tudi država ena izmed tarč hekerjev. Ugotovili smo, da je največ tistih napadov, ki pridejo iz zunanjega sveta, torej iz tistih omrežij, ki so odprta v internet, poleg tega pa narašča tudi število groženj, ki potekajo preko mobilnih telefonov, saj ti v Sloveniji niso kriptirani in na ta način je najlažje priti preko socialnega inženiringa in drugih prevar do točk, ki jih hekerji ciljajo. Vsekakor pa je problem tudi to, da podjetja v primeru napada tega ne priznajo in tudi ne govorijo o tem, saj bi s tem pokazala, da potrebujejo pomoč in so pravzaprav šibka, to pa bi lahko vplivalo na njihov tržni položaj. Ne samo podjetja, tudi domači uporabniki interneta raje molčijo o hekerskih napadih, namesto da bi ta incident prijavili na SI-CERT, kjer bi jim pomagali ter prav tako obvestili širšo javnost. Čeprav je veliko takih, ki raje molčijo, pa druga podjetja izobražujejo svoje zaposlene na tem področju, saj se zavedajo, da je največja težava pravzaprav notranji napad. Pomembno je, da se ljudje in podjetja zavedajo, da imamo v Sloveniji v skladu z zakonom o informacijski varnosti (Ur. l. RS, št. 30/2018), ki je bil sprejet maja 2018, nacionalni CSIRT, kjer lahko prijavimo incidente in se tudi obrnemo po pomoč, na državni ravni pa imamo tako imenovani CSIRT državnih organov, ki je aktualen od 1. januarja 2019, to vlogo pa opravlja sektor za informacijsko varnost direktorata za informatiko na Ministrstvu za javno upravo.

Pri drugem intervjuju z gospodom Božičem smo izvedeli, da je bila prva obravnavana prijava incidenta v Sloveniji leta 1995, od takrat pa so napadi postali bolj sofisticirani in vse pogosteje so tarče hekerjev uporabniki interneta, saj smo vedno bolj prepredeni z njim in tako

tudi bolj izpostavljeni. Zagotovo se je število napadov od prve prijave incidenta povečalo, v zadnjem času pa narašča tudi socialni inženiring, kjer gre za »hekanje možganov« – na psihološki ravni človeka, saj ga je tudi ceneje izvesti. Najpogostejše vrste hekerskih napadov so podtikanje škodljive kode (virusi), »phishing« napadi, kjer gre za krajo podatkov, ter socialni inženiring, kjer je, kot že omenjeno, zadnji dve leti opazna rast števila napadov na podjetja s tako imenovano »direktorsko prevaro«. Pri podjetjih so tarče predvsem mala in srednje velika podjetja, saj morajo biti fleksibilna in se »v hipu obrniti« in zagrabiti posel, prav tako pa je v srednje velikih podjetjih zavedanje o informacijski varnosti manjše v primerjavi z večjimi podjetji, ki zanjo skrbijo, saj za mala in srednje velika podjetja to predstavlja nesorazmeren strošek. Vsekakor večina napadov prihaja iz tujine, saj smo majhna država, vemo, da goljufije prihajajo iz podsaharske Afrike (socialni inženiring, izsiljevanja ipd.), napadi z izsiljevalskimi virusi in drugo škodljivo programsko kodo pa izvirajo iz vzhodne Evrope, Ruske federacije in njene okolice.

Zelo spodbudno pa je, da se zavedanje o tveganjih na internetu širi ter da tako država kot nacionalni odzivni center delajo na tem. Od leta 2011 je SI-CERT začel z nacionalnim programom ozaveščanja »varninainternetu.si«, kjer z jasnimi navodili in opisi groženj in tveganj poskušajo vsem uporabnikom interneta to področje čim bolj približati. Javnost obveščajo preko družbenih omrežij, tiskovnih konferenc, prav tako pa s pomočjo medijev. Podjetjem svetujejo, naj predvsem poiščejo strokovno pomoč pri informacijski varnosti in naj se ne zanašajo na znance, ki so zaključili študij računalništva, saj to ni profesionalen pristop k reševanju težav, saj se kasneje lahko pojavijo še številne druge težave. Uporabnikom pa svetujejo, naj bodo pri brskanju po spletu ter pri prejemanju ponudb previdni in naj sledijo navodilom operacijskega sistema na računalniku ter tako nadgrajujejo protivirusno zaščito in delajo varnostne kopije podatkov na računalniku. Ne nazadnje moramo vsi uporabiti »zdravo pamet« in premisliti, zakaj nam nekdo ponuja loterijske zadetke, če pa nismo vplačali nobene srečke. Možnost, da bi se tako domači uporabniki in podjetja popolnoma izognili vsem hekerskim dejavnostim, pa na žalost ne obstaja, razen če bi se popolnoma izključili z interneta.

LITERATURA

Kikonyogo, Albert Douglas. 2018. *Hacking vs cracking: what is the difference?* Https://www.dignited.com/31529/hacking-vs-cracking-difference/ (4. junij 2018).

Alkaabi, Ali, George Mohay, Aarian McCullagh in Nicholas Chantler. 2010. *Dealing with the problem of cybercrime*. Https://doi.org/10.1007/978-3-642-19513-6_1 (18. maj 2018).

Avast. B. l. *Cybercrime – what it is and how to defend against it*. Https://www.avast.com/c-cybercrime (20. maj 2019).

Chandana. 2013. *Why businesses need ethical hackers?* Https://www.simplilearn.com/ethical-hackers-for-businesses-article (16. december 2013).

Clickatell. 2017. *Cybercrime and its effect on businesses*. Https://www.clickatell.com/articles/information-security/cybercrime-effect-businesses/ (28. marec 2017).

Collins, Jerri. 2018. *Hackers: what do they do?* Https://www.lifewire.com/hackers-good-or-bad-3481592 (24. november 2018).

Cross Domain Solution. B. l.a. *Cyber crime*. Http://www.crossdomainsolutions.com/cyber-crime/ (21. maj 2019).

Cross Domain Solution. B. l.b. *Cyber crime – types & preventive measures*. Http://www.crossdomainsolutions.com/cyber-crime/ (8. april 2019).

Dennis, Michael Aaron. 2019. *Cybercrime – identity theft and invasion of privacy*. Https://www.britannica.com/topic/cybercrime (20. februar 2019).

EC – European Commission. 2019. *The directive on security of network and information systems (NIS directive)*. Https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (15. 7. 2019).

Edraw. B. l. *Advantages and disadvantages of the Internet*. Https://www.edrawsoft.com/internet-use.php (13. marec 2019).

Eubanks, Nick. 2017. *The true cost of cybercrime for businesses*. Https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/ (13. julij 2017).

Fruhlinger, Josh. 2019. *What is malware? How to prevent, detect and recover from it*. Https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html (17. maj 2019).

Gary, Sheza. 2016. Cyber *crime prevention tips for a successful business*. Https://www.colocationamerica.com/blog/cyber-crime-tips-for-businesses (5. november 2016).

Geier, Eric. 2012. *How to become an ethical hacker.* Https://www.pcworld.com/article/250045/how_to_become_an_ethical_hacker.html (15. februar 2012).

Gonsalves, Antone. 2012. *Largest banks under constant cyberattack, feds say*. Https://www.csoonline.com/article/2132452/largest-banks-under-constant-cyberattack--feds-say.html (2. november 2012).

Grimes, Roger A. 2018. *What hackers do: their motivations and their malware*. Https://www.computerworld.com.au/article/635805/what-hackers-do-their-motivations-their-malware/ (5. april 2018).

Herselman, Marlien in Warren, Matthew. 2004. Cyber crime influencing businesses in South Africa. *Journal of Issues in Informing Science and Information Technology* 1: 253–266.

Hulme, George V. in Joan Goodchild. 2017. *What is social engineering?* Https://www.csoonline.com/article/2124681/what-is-social-engineering.html (3. avgust 2017).

Interpol. B. l. *Cybercrime*. Https://www.interpol.int/en/Crimes/Cybercrime (21. maj 2019).

IRT3000. 2018. *V znamenju novih tehnologij*. Https://www.irt3000.si/novice/2018030506341844/V-znamenju-novih-tehnologij/ (5. marec 2018).

IT PRO. 2017. *The history of hacking*. Https://www.itpro.co.uk/go/30179 (22. december 2017).

Leskovar, Robert. 2017. *Ali se znamo zaščiti pred hekerji in škodljivimi programi (virusi)?* Http://www.saop.si/poslovne-informacije/novice/aktualno-1120/ali-se-znamo-zasciti-pred-hekerji-in-skodljivimi-programi-virusi/ (21. junij 2017).

Leswing, Kif. 2016. *Apple hired the hackers who created the first Mac firmware virus*. Https://www.businessinsider.com/apple-hired-the-hackers-who-created-the-first-mac-firmware-virus-2016-2 (3. februar 2016).

Malwarebytes. B. l. *Hacker – what is hacking and how to protect yourself*. Https://www.malwarebytes.com/hacker/ (28. april 2019).

Manikandan, Jayanthi. 2013. *Who's an ethical hacker?* Https://www.simplilearn.com/roles-of-ethical-hacker-article (8. avgust 2013).

Manning, Katrina. 2015. *8 ways businesses can prevent cyber attacks*. Https://www.business2community.com/cybersecurity/8-ways-businesses-can-prevent-cyber-attacks-01251164 (15. junij 2015).

Menzheres, Alexander. 2018. *Top targets for cyber criminals in 2018*. Https://blog.eteam.io/targets-for-cyber-criminals-2018/ (22. marec 2018).

Mitchell, Bradley. 2019. *What is network hacking and why is it a bad thing?* Https://www.lifewire.com/definition-of-hacking-817991 (7. januar 2019).

Nachenberg, Carey. B. l. *Hacking*. Https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/hacking (8. maj 2019).

Panda Security. 2018. *Types of cybercrime*. Https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/ (20. avgust 2018).

Pribanic, Emily. 2018. *Impact of cybercrime on business*. Https://www.techfunnel.com/information-technology/impact-of-cybercrime-on-business/ (25. maj 2018).

Ramey, Karehka. 2012. *Technological advancements and their effects on humanity*. Https://www.useoftechnology.com/technological-advancements-effects-humanity/ (12. november 2012).

SI-CERT. B. l.a. *Phishing*. Https://www.cert.si/si/varnostne-groznje/phishing/ (24. maj 2019).

SI-CERT. B. l.b. *Spam*. Https://www.cert.si/si/varnostne-groznje/spam/ (24. maj 2019).

Techopedia. B. l.a. *What is a denial-of-service attack (DoS)? Definition from Techopedia*. Https://www.techopedia.com/definition/24841/denial-of-service-attack-dos (23. maj 2019).

Techopedia. B. l.b. *What is hacking? Definition from Techopedia*. Https://www.techopedia.com/definition/26361/hacking (28. april 2019).

Techopedia. B. l.c. *What is spam?* Https://www.techopedia.com/definition/1716/spam (24. maj 2019).

Tehnopedia. B. l.d. *Denial-of-Service Attack (DoS).* Https://www.techopedia.com/definition/24841/denial-of-service-attack-dos (23. maj 2019).

Varga, Miran. 2017. *Dobri in slabi fantje*. Https://www.monitor.si/clanek/dobri-in-slabifantje/180477/ (13. junij 2017).

Varni na internetu. 2014. *Etično hekanje.* Https://www.varninainternetu.si/kdo-so-eticni-hekerji/ (18. april 2014).

Varni na internetu. B. l. *Cilji projekta*. Https://www.varninainternetu.si/cilji-projekta/ (4. junij 2019).

Zakon o informacijski varnosti (ZInfV). *Uradni list RS*, št. 30/2018.

Zamora, Wendy. 2018. *Under the hoodie: why money, power, and ego drive hackers to cybercrime*. Https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/ (15. avgust 2018).

PRILOGE

Priloga 1 Vprašanja za intervju z generalnim direktorjem direktorata informacijske družbe na Ministrstvu za javno upravo, dr. Urošem Svetetom

Priloga 2 Vprašanja za intervju s predstavnikom, vodjo slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, Arnes, gospodom Gorazdom Božičem

Vprašanja za intervju z generalnim direktorjem direktorata informacijske družbe na Ministrstvu za javno upravo, dr. Urošem Svetetom

1. Ali so državni organi tarče hekerjev v Sloveniji? Če, da ali so kateri organi bolj dovzetni za te napade?
2. Menite, da je tako v Sloveniji kot Evropi gospodarsko vohunjenje pogosto? Kaj bi gospodarstvo kot tako lahko naredilo, da se izogne takim napadom?
3. Ali obstaja organizacija ali pa organ na državni ravni, ki obvešča tako »domače uporabnike« ter podjetja o napadih ter jim svetuje kako se zavarovati?
4. Ali v Sloveniji obstaja zakonski pravilnik s katerim bi kaznovali hekerja v primeru, da bi ga »ujeli«?
5. Ali so se na slovensko vlado že obrnile večje glasbene in filmske založbe v primerih kraje filmov, ki so bili namenjeni za presojo morebitne nagrade? Ali je oziroma bo Slovenija zaostrila zakonodajo na tem področju?
6. Koliko je bilo že pozivov, da bi Slovenija omejila dostop do določenih strani, kot je to poskusila v primeru udba.net, ko so npr. žvižgači objavili določene podatke, ki niso bili po godu vplivnežev?
7. Koliko je bilo do sedaj žrtev med podjetji pri tako imenovanih nigerijskih prevarah? Včasih so Nigerijci pošiljali klasično pošto podjetjem, danes sicer ciljajo predvsem fizične osebe, zanima pa me, ali so še vedno žrtve tudi podjetja?
8. Ali vlada pomaga slovenskim žrtvam kraje identitete, ki so zadnje čase kar pogoste? Obstajajo kakšna priporočila, kakšen je postopek v tem primeru?

Vprašanja za intervju s predstavnikom, vodjo Slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, Arnes, gospodom Gorazdom Božičem

1. Katere vrste hekerskih napadov so najbolj pogoste v Sloveniji in na splošno? Če obstaja določen »tip« ali menite, da za tem stoji nek tehten razlog?
2. Ali obstaja podatek, kdaj se je izvedel prvi hekerski napad v Sloveniji? Menite, da je od takrat število napadov naraslo ter, da so napadi postali še toliko bolj »nevarni« za uporabnike?
3. Katere so bolj pogoste tarče hekerjev v Sloveniji, »domači uporabniki« ali podjetja?
4. Ali hekerji, ki izvajajo napade prihajajo iz tujine ali Slovenije? Ali je možno pravzaprav slediti od kod izvajajo napade?
5. V primerjavi z tujino ali menite, da je v Sloveniji manj hekerskih napadov? Če da ali obstaja nek razlog?
6. Ali se »domači uporabniki« in podjetja velikokrat obrnejo na vaš center v primeru hekerskih napadov?
7. Kako oziroma ali obveščate slovensko javnost o nedavnih napadih in ali to vpliva na »razgledanost« ljudi o tej tematiki?
8. Kako bi svetovali tako ljudem kot podjetjem, da se zavarujejo pred nevarnostmi na spletu?
9. Ali obstaja možnost, da bi se »domači uporabniki« popolnoma izognil vsem hekerskim dejavnostim? Če, da kako?
10. Ali so etični hekerji pogosti v slovenskih podjetjih? Menite, da so pomemben del organizacij?