UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

RAZLIČNI VIDIKI KIBER KRIMINALA IN NJEGOV RAZVOJ SKOZI ČAS

Ljubljana, september 2016 JERNEJ VODOPIVEC

IZJAVA O AVTORSTVU

Podpisani Jernej Vodopivec, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Različni vidiki kiber kriminala in njegov razvoj skozi čas, pripravljenega v sodelovanju s svetovalcem prof. dr. Tomažem Turkom

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 7. 9. 2016 Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Kibernetski kriminal postaja eno najpomembnejših in najbolj donosnih panog na področju organiziranega kriminala. Število kiber kriminalnih dejanj je v nekaterih državah že preseglo število tradicionalnih kriminalnih dejanj na letni ravni (Cyber Crime Assessment 2016, str. 6). Človekova odvisnost od digitalnih komunikacijskih poti in najrazličnejših storitev, ki uporabljajo sodobne komunikacijske poti, je namreč večja, kot je bila kadarkoli. Stalen dostop do informacij pridobljenih preko interneta je postal nepogrešljiv tako pri osebni kot tudi poslovni rabi (Verleur, 2015).

Na drugi strani je odvisnost od sodobnih digitalnih tehnologij v poslovnem svetu in industriji še toliko večja. Storitve, kot so npr. finančne transakcije v B2B segmentu, borzne storitve, infrastrukturne storitve; kot so upravljanje elektrarn in električnih omrežij, storitve v zdrastvenem sistemu ter mnoge druge storitve ne delujejo več brez internetnih povezav. Nevarnosti, ki jih prinaša tesna povezanost s kiber svetom, pa nas delajo občutljive in ranljive. Zaradi tega moramo ta tveganja upravljati in načrtovati poslovanje na način, da se tveganjem izognemo ali jih vsaj zmanjšamo.

Namen diplomskega dela je odgovoriti na raziskovalno vprašanje: kateri so različni vidiki kiber kriminala, kako se je kiber kriminal razvijal skozi čas in kaj nam bo prinesla prihodnost kiber kriminalcev? Uvodoma bom bralca popeljal skozi zgodovino odmevnejših dogodkov na področju kiber kriminala. Za lažje razumevanje razlik med posameznimi izrazi, ki nas lahko hitro zavedejo, bom v ločenem poglavju predstavil poglavitne pojme, ki se pojavljajo v povezavi s kiber kriminalom. Pogled v prihodnost pa bom gradil na razvoju pretklih dogodkov ter dogajanj v sedanjosti in s tem poskušal napovedati, kaj naj bi se dogajalo v prihodnjih letih.

Cilj diplomskega dela je raziskati finančne posledice na mikro in makro ravni, ki jih pusti za seboj kiber kriminal. Zanimalo me je katere metode uporabljajo podjetja, z namenom zmanjševanja stroškov in hkrati posledic kiber kriminalnih dejanj, ki so jih prizadela. Cilj diplomske naloge je razdeljen na:

- teoretični del ter
- praktični del.

V prvem delu se bom osredotočil na odmevnejše primere kiber kriminala po svetu ter predstavil posledice na stroškovni ravni, ki so jih ocenili avtorji člankov.

V drugem delu pa bom naredil analizo prodaje različnih varnostnih rešitev v neimenovanem podjetju ter s tem prikazal, kaj se dogaja na področju kiber kriminala v Republiki Sloveniji.

Pri diplomski nalogi bom uporabil znanje, ki sem ga pridobil skozi študij na Ekonomski fakulteti v Ljubljani ter izkušnje, ki sem jih pridobil z delom na področju varnostnih rešitev v informacijskem svetu. Teoretični del bo sestavljen iz preučevanja domače in tuje literature ter virov s področja kiber kriminala. Raziskovalni del naloge pa bo temeljil na analizi pridobljenih podatkov. Ugotovitve bom predstavil v obliki grafov, ki jih bom v nadaljevanju podrobneje obrazložil.

1 ČASOVNA PREMICA POMEMBNEJŠIH PRELOMNIC IN DOGODKOV

Razvoj dogodkov na področju kibernetske varnosti ter kibernetskih napadov sega dve oz. tri desetletja nazaj v prejšnje tisočletje. Kot eno izmed pomembnejših prelomnic v zgodovini razvoja kiber kriminala viri navajajo črva Morris, katerega avtor Robert Morris je bil prva oseba obsojena na podlagi t.i. Computer Fraud and Abuse act sprejetega v ZDA leta 1986 (Moore, 2010, str. 21).

Za prvi dogodek v kronološkem pregledu razvoja kibernetskega kriminala, ki obsega razvoj zlonamernega programja, kibernetskih napadov in pripravo zakonodaje in drugih dogodkov, sem izbral eno izmed prvih opredelitev in razčlenitev pojma računalniški virus. Cohen (1986, str. 5) v svoji doktorski disertaciji podrobno opredeli računalniški virus kot programje, ki lahko okuži ostale programe na način, da naredi, po možnosti razvito (angl. *evolve*), kopijo samega sebe. Ko je program enkrat okužen, se lahko ta računalniški virus širi po računalniškem sistemu ali omrežju, pri čemer uporablja avtorizacije vsakokratnega uporabnika z namenom, da okuži druge programe. Infekcija poteka na način, da se lahko vsak program, ki bo postal okužen, prav tako obnaša kot virus.

Povezetek bistvenih prelomnice iz sveta kiber kriminala od 80. let prejšnjega stoletja vse do danes je prikazan na časovni premici, ki se nahaja v prilogi št. 1 diplomskega dela.

V sedemdesetih in osemdesetih letih prejšnjega stoletja, kar obenem sovpada tudi z začetkom informacijske dobe, so se začele prve države že zavedati, da (domači) računalniki postajajo dosegljivi vse širši populaciji ljudi. To dejstvo je namreč, poleg vseh prednosti, ki jih je prineslo obdobje informatizacije, hkrati odprlo tudi povsem nova področja kriminalnih dejanj. Zaradi tega npr. Združene države Amerike (v nadaljevanju ZDA) leta 1986 že zakonsko opredelijo odgovornost in dejanja na področju zlorab v kibernetskem svetu s sprejemom zakonodaje na tem področju. Dve leti po tem ZDA tudi ustanovijo prvi *Computer Emergency Response Team* (v nadaljevanju CERT). Pojavijo se prvi računalniški virusi.

Devetdeseta leta prejšnjega stoletja so prinesla velik razmah računalniških virusov, črvov in drugih oblik zlonamernega programja. Pričele so izhajati prve revije na temo

kibernetske varnosti, prvič pa je bila organizirana tudi DEF CON konferenca, ki je ena izmed najbolj poznanih in obiskanih konferenc s področja vdiranja v tuje računalniške sisteme (v nadaljevanju hekanja) tudi danes.

Med leti 2000 in 2010 postaja kiber kriminal vse bolj donosno področje, zaradi česar postaja vse bolj zanimiv med tradicionalnimi kriminalci. V tem obdobju se tudi v Sloveniji zgodijo odmevnejši primeri kiber kriminala in posledično tudi prve aretacije, ki so nastale kot posledica teh dejanj. Zgodijo se prvi večji napadi porazdeljene ohromitve storitve (v nadaljevanju DDoS). Vse več podjetij, ki razvija in kodira programsko opremo, se zaveda problematike slabo spisane programske kode in začne uvajati dobro prakso in kontrolo pri kodiranju programske kode z namenom narediti le-to bolj varno.

V obdobju po letu 2010 vse do danes opazimo, da postaja kiber kriminal velik problem na svetovni ravni. Vse večje število držav se problema loteva strateško in tako problem opredeli v obliki strategije boja proti kiber kriminalu. Kiber kriminalci posegajo po povsem novih metodah kibernetskih napadov ter izpopolnjujejo obstoječe tehnike napadov. Pojavljajo se napadi na industrijske sisteme, zanimivo postaja področje napadov na internet stvari.

2 OPREDELITEV POJMOV

Informacijska varnost. Von Solms (1998, str. 98) opredeli namen informacijske varnosti kot zagotavljanje kontinuitete poslovanja in minimiziranja poslovne škode na način, da skušamo omejiti škodo oz. vpliv varnostnih incidentov.

Mednarodno uveljavljeni standard ISO/IEC 27002, katerega primarni namen je opredelitev dobre prakse informacijske varnosti, opredljuje informacijsko varnost kot ohranjanje zaupnosti, integrirete in razpoložljivosti informacij (angl. *Confidentiality, Integrity and Availability*; v nadaljevanju CIA trikotnik). Informacija ni nujno potrebna, da se nahaja le v elektronski obliki, temveč se po standardu ISO/IEC 27002 lahko pojavi tudi v drugih oblikah: zapis na papirju, shranjena elektronsko, poslana preko pošte ali elektronskih poti, prikazana na filmih, izrečena v pogovoru in podobno.

Zaradi neprestano spreminjajočega se okolja informacijske tehnologije (v nadaljevanju IT) pa nekateri avtorji poudarjajo, da je za natančnejšo opredelitev informacijske varnosti potebno razširiti CIA trikotnik. Da bi bolj ustrezno opredelili informacijsko varnost Whitman in Mattord (2011, str. 12) predlagata, da CIA trikotniku dodamo še naslednje elemente, ki jih moramo v sklopu informacijske varnosti nasloviti: natančnost, avtentičnost, uporabnost in posest. Res je, da že pojem v splošnem integritete zajema velikokrat avtentičnost na eni strani in neponovljivost na drugi strani. Menim pa, da je pravilno, da je avtentičnost izpostavljena kot ločena zahteva, saj natančneje definira

zahtevo po izvoru podatkov v primerjavi z integriteto. Pod integriteto bi lahko, morda povsem napačno, šteli tudi integriteto podatkov, ki niso avtentični.

Glede na omenjeno pridemo do zaključka, da informacijska varnost ni produkt ali samostojna tehnološka rešitev. Informacijska varnost je namreč dolgotrajen in kontinuiran proces, ki se v podjetju dolgotrajno razvija in se proces kot tak, nikoli ne konča (Mitnick in Simon, 2003, str. 13).

Kiber varnost. Kiber varnost zajema zaščito celotnega kiber prostora, kar vključuje poleg zaščite informacij tudi zaščito drugih sredstev, kot so npr. osebe, ki delujejo v kiber prostoru. Kiber varnost tako obsega tudi oprijemljiva (npr. državna strateška infrastruktura) in neoprijemljiva sredstva (družbene vrednote), ki jih osebe uporabljajo in so dosegljiva preko kiber prostora (von Solms in van Niekerk, 2013, str. 1).

Iz tega sledi, da kibernetske varnosti in informacijske varnosti ne moremo povsem enačiti. Če bi ju namreč lahko v celoti enačili, potem bi morali trditi, da za vsak incident na področju kibernetske varnostni velja, da je prišlo do kršitve zaupnosti, integritete ali razpoložljivosti informacij. Incidenti, ki kršijo enega ali več načel iz CIA trikotnika, so res pogosti tudi na področju kibernetske varnosti. A ključno je, da kibernetska varnost zajema tudi incidente, pri katerih ne prihaja do kršitve sestavnih elementov CIA trikotnika.

Za nazornejše razumevanje razlike med informacijsko varnostjo in kibernetsko varnostjo bom navedel dva dogodka na področju kibernetske varnosti, ki jih ne moremo šteti kot incidenta na področju informacijske varnosti:

- Kiber ustrahovanje: ustrahovanje se je z razvojem sodobnih tehnologij razširilo tudi na kibernetski prostor. Kiber ustrahovanje se pojavlja kot dejanje, ki povzroča zadrego, vnaša nadlegovanje in nasilje ter povzroča psihološke posledice (von Solms in van Niekerk, 2013, str. 3). Ker je v primeru kiber ustrahovanja tarča dotična oseba in ne informacijsko sredstvo, cilj pa povzročitev zadrege in nadlegovanje, ne moremo govoriti, da gre pri ustrahovanju za izgubo zaupnosti, integritete ali razpoložljivosti podatkov.
- Internet stvari (IoT) zajema množico raznovrstnih naprav, ki so priklopljene na internet: hladilniki, telefoni, luči, avtomobili, grelci, sistemi za upravljanje domov, televizije in mnoge druge. Preko zunanje krmilne enote lahko npr. posameznik danes upravlja že avto. Če pride do vdora oz. zlorabe sistema za upravljanje avtomobila, posledica tudi v tem primeru ne bo kršenje načel iz CIA trikotnika, lahko pa bo posledica npr. prometna nesreča z materialno škodo (How to summon a Tesla car using Apple Watch, 2016).

Kiber kriminal. Ko definiramo pojem kiber kriminal, moramo biti pozorni, da se ne omejimo le na kiber kriminalna dejanja, ki so usmerjena na odtujitev informacij, torej

incidentov na področju informacijske varnosti, ampak moramo definicijo postaviti širše. Vključiti moramo tudi incidente na področju kibernetske varnosti. Kiber kriminal je opredeljen kot kriminalna aktivnost, ki je izvršena preko računalnika oz. Interneta (Grant Thornton, 2015, str. 2). Zaradi širokega opredelitva pojma v številnih primerih težko ločimo med kriminalnimi dejanji, katerih cilj je zlonamerna akcija izvršena nad IT sredstvom, in dejanji, pri katerih je računalnik zgolj sredstvo uporabljeno v samem kriminalnem dejanju, cilj pa je neinformacijsko sredstvo. Primer slednjega bi bil, da terorist poišče na spletu objavljene informacije, kako izdelati sredstvo za množično uničevanje in te nato uporabi za izvedbo terorističnega napada.

Glede na namen samega kiber kriminalnega dejanja lahko ta razvrstimo v nekaj bistvenih skupin (Grant Thornton, 2015, str. 5):

- Kraja identitete, med katero štejemo spletne prevare, goljufije pri spletnih nakupih, preusmerjanje obiskovalcev na spletne strani s škodljivo vsebino, neusmerjeno ribarjenje in ribarjenje usmerjeno na dotičnega posameznika, ribarjenje preko uporabe glasovnih sporočil (tipično ribarjenje poteka preko e-pošte) ter nazadnje spletne kraje poslovnim subjektom.
- Kiber izsiljevanje, ki predstavlja napad na poslovne subjekte ali posameznike, z zahtevo po odkupnini, ki je tipično izražena kot nakazilo denarja ali pogosto tudi nakazilu sredstev v obliki kripto valute, nemalokrat pa se pojavi tudi kot grožnja razpoložljivosti storitev, kot je npr. napad na spletno trgovino s ciljem, da se onemogoči delovanje storitve.
- Industrijsko vohunjenje se tipično odraža kot nelegalno pridobivanje informacij o konkurenci npr., kakšno ceno bo oddalo konkurenčno podjetje na razpisu, pridobitev zaupnih informacij o postopkih, načrtih in izdelkih, ki zagotavljajo konkurenčno prednost ipd.

Kiber vohunjenje. Proces kraje zaupnih in tajnih informacij hranjenih v digitalni obliki na računalnikih ali IT omrežjih imenujemo kiber vohunjenje (Definition of cyber espionage, 2016). Nekateri pojem kiber vohunjenje razumejo širše, in sicer štejejo med ta proces tudi že samo pripravo omrežja na krajo (Ritchey, 2016).

Kiber terorizem. Avtorji niso enotni pri definiciji kiber terorizma, zato v literaturi najdemo več različnih definicij. Coleman (2003, str. 1), nekdanji zaposleni v Netscapeu, definira kiber terorizem kot naklepno izvajanje motečih aktivnosti nad računalniki in/ali računalniškimi omrežji z namenom povzročitve škode ali s sociološkimi, ideološkimi, verskimi, političnimi ali podobnimi cilji. Sem štejemo tudi morebitno ustrahovanje posameznika, ko se to izvaja z namenom doseči enega od prej omenjenih ciljev.

Kiber vojna. Točno definicijo kiber vojne je še predvsem zaradi zelo dinamičnega in spreminjajočega se načina izvajanja napadov težko natančno opredeliti. R. Shakarain, J.

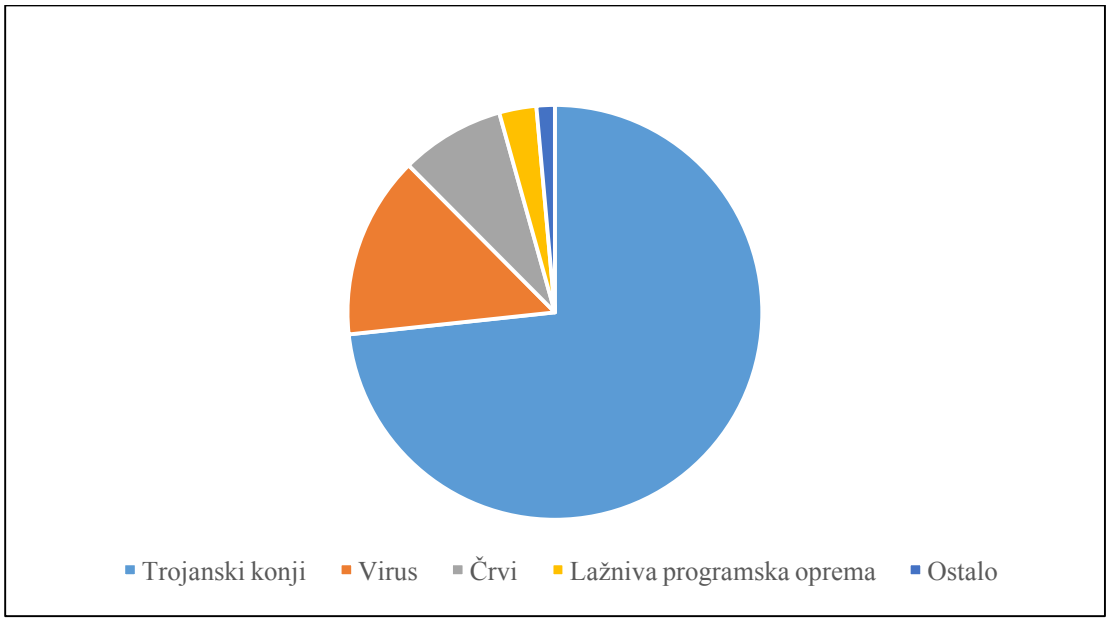
Shakarain in Ruef (2013, str. 2) so zato pri definiciji kiber vojne izhajali iz definicije vojne, kot jo je opredelil Clausewitz: vojna je razširitev politike z uporabo različnih sredstev. Iz te definicije vojne bi sklepali, da je kiber vojna razširitev politike v kiber prostoru z uporabo različnih sredstev. Ker pa bi pod takšno definicijo kiber vojne šteli npr. tudi vsak politično motiviran napad in zlorabo spletnega strežnika, bi bila ta preveč ohlapna. Kiber vojno zato Shakarain et al. (2013, str. 2-3) natančneje definirajo kot razširitev politike z ukrepi, ki so izvedeni v kibernetskem prostoru državnih ali nedržavnih akterjev. Ti bodisi predstavljajo resno grožnjo za varnost naroda ali se izvajajo kot odgovor na zaznane grožnje proti varnosti naroda.

Ranljivost. Ranljivost je lastnost sistema, ki ni del načrtovane funkcionalnosti, a jo je mogoče izkoristiti za nepooblaščen vdor ali okužbo sistema. Ranljivost se tipično nahaja v enem izmed treh gradnikov: programski opremi, strojni opremi ali računalniškemu omrežju. Kot primer dobre prakse krpanja ranljivosti v programski opremi bi navedel podjetje Microsoft Corporation (v nadaljevanju Microsoft). Podjetje je korenito spremenilo proces izdelave programske opreme z vidika izboljšanja kvalitete programske kode na eni strani in rednega izdajanja varnostnih popravkov za ranljivo programsko opremo na drugi strani (od oktobra 2003 dalje). Ta proces lahko zaznamo tudi vsi posamezniki, ki uporabljamo programsko opremo podjetja Microsoft. Na »patch Tuesday« dan se namreč naložijo popravki programske opreme na naš računalnik, posledično pa moramo ponavadi ponovno zagnati računalnik (Rouse, 2016). Splošni javnosti manj znani so napadi na strojno opremo, kot je npr. izkoriščanje ranljivosti centralnih procesnih enot (v nadaljevanju CPE), izkoriščanje ranljivosti v tiskalnikih ipd. Primer napada na CPE sta z vsemi podrobnosti in tehnikami napada opisala Wojtczuk in Rutkowska (2009), v katerem sta prikazala praktično izvedbo napada na t.i. System Management RAM. Primer uspešnega napada na tiskalnike je izkoriščanje ranljivosti v HP tiskalnikih, ki omogoča napadalcu, da zaobide varnostne mehanizme za ugotavljanje pravice do tiskanja, onemogoča delovanja tiskalnika in izvede ponatis predhodno natisnjenih dokumentov (Schwartz, 2016b). Zloraba ranljivosti v omrežnih napravah se pogostokrat odraža v prisluškovanju in prestrezanju komunikacij. Kot primer tovrstne ranljivosti navajam izkoriščanje ranljivosti v programski opremi usmerjevalnika svetovno uveljavljenega proizvajalca Juniper Networks, ki je bila javno objavljena januarja 2016 (Gross, 2016b). Ranljivost omogoča napadalcu dvoje: pridobitev popolnega dostopa do usmerjevalnika preko glavnega gesla (angl. *master password*) in prisluškovanje sejam, ki so potekale preko navideznih zasebnih omrežij (v nadaljevanju VPN).

Zlonamerno programje. Zlonamerno programje (angl. *malicious software*; v nadaljevanju malware) proizvajalec varnostnih rešitev Kaspersky Lab opredeli kot programsko opremo, katere namen je na različne načine okužiti legitimne računalnike in povzročitev škode na njih ali preko njih. Malware se lahko namesti na računalnik z ali brez vedenja lastnika računalnika.

Zlonamerno programje Rubenking (2016a) deli glede na aktivnost, ki jo izvaja ta koda, v naslednje skupine: oglaševalsko programje (angl. *adware*), organizirane trajne grožnje, stranska vrata (angl. *backdoor*), robote (angl. *bot*), ukane (angl. *exploit*), beležnike tipkanja (angl. *keylogger*), izsiljevalsko programje (angl. *ransomware*), korenske komplete (angl. *rootkit*), viruse, črve (angl. *worm*), strašilno programje (angl. *scareware*), vohunsko programje (angl. *spyware*) in trojanske konje (angl. *trojan*). Ciljne naprave so tipično osebni računalniki, prenosniki, strežniki, omrežna oprema in vse pogosteje tudi industrijski sistemi za oddaljen nadzor in upravljanje (v nadaljevanju SCADA sistemi).

Slika 1: Vrste zlonamernega programja



Vir: J. Jang-Jaccard in S. Nepal, A survey of emerging threats in cybersecurity, 2014, str. 975.

Razvoj malwarea se je skozi leta glede na namen razvil iz raziskovalnega namena (npr. črv Morris) v dobičkonosen posel. Programska koda, ki je sestavni del malwarea, postaja vse bolj napredna, učinkovita in kvalitetno napisana. Ustvarjanje tovrstne programske kode je postala panoga, kjer na trgu delujeta ponudba in povpraševanje, cilj razvijalcev pa je tako ustvarjanje dobička.

Računalniški črv. Računalniški črv je programje, katere primarni namen je širitev preko elektronskih medijev med računalniki (Rubenking, 2016b). Za širjenje je najpogosteje uporabljen medij računalniško omrežje. Širjenje lahko poteka bliskovito hitro. Sekundarna naloga črvov je, da ko se enkrat uspešno razširijo na novo žrtev, izvedejo prenos novega zlonamernega programja, kot je npr. računalniški trojanski konj.

Računaniški virus. Računalniški virus je glede na način širjenja zelo podoben računalniškemu črvu, saj je primarni namen obeh okužba čim večjega števila računalnikov.

Bistvena razlika med obema pa je v tem, da virus tipično naredi škodo na način, da pobriše ali poškoduje podatke oz. kako drugače poseže v delovanje računalnika, črv pa neposredne škode ne izvede (What is a computer virus?, 2016)

Trojanski konj. Računalniški trojanski konj je dobil ime po zgodbi iz grške mitologije, ko so Grki pod pretvezo darila boginji Ateni podarili pustili lesenega konja pred vrati Troje. V konju je bila skrita peščica vojakov, ki je kasneje znotraj obzidja odprla vrata grški vojski, da je ta lahko vkorakala v mesto. Računalniški trojanski konj je v zasnovi enak kot grški trojanski konj, saj se uporabniku predstavlja kot legitimna programska oprema. A ko jo uporabnik enkrat zažene na svojem računalniku, trojanski konj izvede zlonamerno aktivnost, kot je npr. vzpostavitev oddaljenega dostopa napadalcu in nadzor do zlorabljenega računanika (What is a Trojan Virus?, 2016).

Roboti. Roboti so zlonamerno programje, katere primarni namen je izvajanje avtomatiziranih aktivnosti na zahtevo upravljalca, ki sedi v oddaljenem nadzornem centru (angl. *Command & Control center*; v nadaljevanju C&C center). Omrežje, ki ga sestavljajo računalniki, ki so okuženi z roboti in so upravljani preko C&C centra, imenujemo *botnet* (Crimeware: Bots, 2016). Kiber kriminalci izkoriščajo okužene računalnike z roboti za izvajanje različnih kriminalnih aktivnosti, kot so npr. DDoS napadi, pošiljanje nezaželene in/ali okužene elektronske pošte in kraje podatkov o kreditnih karticah. Botnet omrežje samo po sebi ne izvaja napadov ali drugih kiber kriminalnih aktivnosti. Ima pa nalogo, da upravljalcu v C&C centru omogoča na zahtevo prenos zlonamernega programja za izvajanje zgoraj omenjenih aktivnosti.

Nezaželena elektronska pošta. Da dobi elektronsko sporočilo oznako nezaželene elektronske pošte (v nadaljevanju spam pošta) mora ta ustrezati hkrati dvema kriterijema: biti mora nezaželena (angl. *unwanted*) oz. nenaročena (angl. *unsolicited*) ter hkrati poslana večjemu številu prejemnikov. Nenaročena pomeni, da prejemnik ni izrecno dovolil pošiljatelju, da mu pošlje elektronsko sporočil (npr. prošnja za pripravo ponudbe). Masovno poslana pa pomeni, da mora biti sporočilo poslano kot del večjega števila sporočil, pri čemer imajo sporočila identično vsebino (npr. bilter ali okrožnica).

Pošiljanje spam pošte je dobičkonosen posel, saj lahko naročniki za nekaj sto dolarjev naročijo razpošiljanje spam sporočil na milijone elektronskih naslovov, ponudniki pošiljanja spam sporočil pa stroškov z izvedbo dodatne kampanijo nimajo skoraj nič (The Definition of Spam, 2016). Na črnem trgu tako nastopa večje število ponudnikov pošiljanja spam pošte, ki razpošljejo velike tovrstne pošte. Jang-Jaccard in Nepal (2014, str. 976) ocenjujeta, da je bilo samo v letu 2011 poslanih kar 3 bilijone spam sporočil.

Ribarjenje. Ribarjenje je proces, pri katerem je cilj pridobiti tajne oz. osebne informacije, kot so uporabniško ime, geslo, podatke o kreditni kartici, digitalno potrdilo in drugo (Jang-Jaccard & Nepal, 2014, str. 976). Prevara ribarjenja poteka tako, da žrtev prejme v svoje e-

predal sporočilo, ki naj bi bilo poslano od avtentične organizacije. V sporočilu se nahaja povezava do spletne strani, ki na prvi pogled izgleda zelo podobno kot izgleda zaupanja vredna spletna stran. Poneverjena spletna stran pa se od avtentične razlikuje v tem, da vsebuje elemente, s katerimi poskušajo zlikovci zavesti žrtev in priti do občutljivih informacij.

Tudi komitenti slovenskih bank so bili že večkrat tarča napadov ribarjenja. Ti napadi so bili še posebej intenzivni januarja leta 2015, zaradi česar je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljevanju SI-CERT) izdal posebno opozorilo glede nevarnosti za uporabnike (SI-CERT 2015-01 / Val phishing napadov na komitente slovenskih bank, 2016).

Okužba v mimohodu. Okužba v mimohodu (angl. *Drive-by downloads*) je način izvedbe okužbe računalnika, ki se zgodi ob obisku legitimne spletne strani (Zorabedian, 2016a). Napadalci posredno ali neposredno na povsem legitimno spletno stran namestijo malware, ki poskuša izkoristiti eno izmed ranljivosti v programski kodi spletnega spletnega brsnikalnika ali dodatka oz. razširitve za le-tega.

Porazdeljena ohromitev storitve. Porazdeljena ohromitev storitve (angl. *distributed denial of service*) je grožnja oz. napad, katere cilj je, kot ga definira Abliz (2011, str 3.), narediti sredstvo nerazpoložljivo. To predstavlja kršitev razpoložljivosti kot ene izmed treh ključnih točk CIA trikotnika. Gre za napad izveden preko elektronskih medijev tipično na javno dostopne storitve (npr. spletni strežnik), v obliki t.i. volumetričnega napada ali napada na omrežje, kot je npr. t.i. TCP-SYN flood napad, t.i. UDP-flood napad ipd. Najpogosteje se izvede napad preko zlorabljenih računalnikov, ki so upravljani preko C&C centra (Beal, 2016).

Socialni inženiring. Kot najboljšo opredelitev socialnega inženiringa Alen (2006, str. 4) izbere sposobnost in umetnot prepričati osebo, da naredi nekaj, kar mi želimo. Preko socialnega inženiringa torej želimo pretentati ljudi, da (nevede) prekršijo varnostne procedure, izdajo zaupno informacijo ali storijo nekaj, kar sicer ne bi storili (Rouse, 2016). Socialni inženiring tako ni neposredno izkoriščanje ranljivosti v programski kodi, je pa izkoriščanje ranljivosti v razmišljanju in naivnosti ljudi.

3 POSLOVNO TVEGANJE V KIBER PROSTORU

Podjetja ter tudi posamezniki se neprestano srečujemo s tveganjem, ne da bi se v določenih primerih tega sploh zavedali. Tveganje je del našega vsakdana in naša naloga je, da z njim čim bolj uspešno upravljamo. Upravljanje tveganja v podjetjih zagotavlja podjetju preko učinkovite analize tveganj prevzem kontrole nad svojo usodo.

Kaj sploh je tveganje in kako ga obravnavati, avtorji navajajo različno. Vsem pa je skupno, da tveganje predstavlja negotovost v prihodnosti. Whitman in Mattord (2011, str. 119) opredelita upravljanje tveganj kot proces identifikacije tveganj, kot ga predstavljajo ranljivosti, ki se nanašajo na sredstva in infrastrukture posamezne organizacije. Del procesa upravljanja tveganj pa so tudi postopki, ki znižujejo zaznana tveganja na sprejemljivo raven. Avtorja trdita tudi, da so vsi trije elementi CIA trikotnika bistveni dejavniki, ki morajo biti zagotovljeni za vzdržno dolgoročno konkurenčnost podjetja.

Tveganje delimo z vidika učinka glede na stanje negotovosti, ki ima lahko pozitiven ali negativen učinek. Na podlagi tega delimo tveganje na (HM Treasury, 2004, str. 9):

- pozitivno tveganje predstavlja priložnost in
- negativno tveganje predstavlja grožnjo.

Tveganje moramo zato obravnavati glede na verjetnost, da se bo dogodek zgodil in posledice, ki jih bo prinesel dogodek, če se bo dejansko tudi zgodil. Upravljanje tveganj pa definira podobno, kot sta ga definirala Whitman in Mattord (2011, str. 119), in sicer upravljanje tveganj zajema identifikacijo in oceno tveganj ter odziv glede na te.

Peltier (2005, str. 8) upravljanje tveganj opredeli kot celovit proces, preko katerega identificiramo, kontroliramo in minimiziramo amplitudo dogodkov, ki imajo nepoznano končno stanje. V praksi pomeni to cilj, ki odločevalcem v podjetju zagotavlja znižanje tveganja do sprejemljive stopnje. Takšno tveganje potem odločevalci tudi sprejmejo.

Glede na to, da se tveganje pojavlja na praktično vsakem koraku, mi pa želimo tveganja zmanjšati ali se jim v celoti izogniti, ugotovimo, da vseh tveganj ne bomo mogli zmanjšati na najnižjo možno raven. Nimamo namreč ne dovolj časa ne sredstev, da bi to lahko izvedli (HM Treasury, 2004, str. 9). Katera tveganja so za nas pomembnejša oz. katera tveganja bomo prednostno obravnavali, ker nas zavezujeta k temu zakonodaja in standardni, je zahteven proces, ki mu posvečamo posebno pozornost. Zagotovo pa je, da vseh tveganj ne bomo obravnavali enako in jim ne bomo posvečali enako časa in sredstev.

V nadaljevanju se bom osredotočil na poslovno tveganje na področju informacijske oz. kiber varnosti, ne bom pa obravnaval npr. naložbenega, finančnega, strateškega, operativnega kadrovskega ali drugega tveganja.

3.1 Upravljanje tveganj

Upravljanje tveganj sestavljajo štiri faze (Peltier, 2005, str. 8):

- analiza tveganj,
- ocena tveganj,

- zmanjševanje tveganj in
- ocena ranljivosti in ovrednotenje kontrol.

Analizo tveganj opredelita Whitman in Mattord (2011, str. 119) kot proces identifikacije tveganj in dokumentacije varnostne drže (angl. *posture*) informacijske tehnologije posamezne organizacije ter tveganj, katerim je izpostavljena. V procesu torej identificiramo vire, grožnje, ki so jim izpostavljeni, ranljivosti, ki bi jih grožnje lahko izkoristile, in vpliv groženj na sredstva oz. vire (Gaberšek, 2007, str. 31). Peltier (2005, str. 8) pa analizo tveganj opredeli kot tehniko, ki identificira in ovrednoti dejavnike, ki lahko ogrozijo uspešnost projekta oz. lahko vplivajo na dosego cilja, tipično določene stopnje varnosti oz. varnostne potrebe. Analiza tveganj nam pomaga tudi pri določitvi preventivnih ukrepov, ki zmanjšujejo verjetnost, da se bo dogodek zgodil. Po drugi strani pa zajema protiukrepe, ki jih moramo izvesti v primeru, da se nezaželen dogodek zgodi.

Ocena tveganj je naslednji korak po analizi tveganj v procesu upravljanja tveganj, pri katerem ocenimo verjetnost dogodka, ki bi povzročil (potencialno poslovno) škodo (Gaberšek, 2007, str. 31). V procesu moramo pripraviti ogrodje, preko katerega bomo ocenjevali posamezna tveganja, saj se vrste tveganj po strukturi lahko bistveno razlikujejo med seboj (HM Treasury, 2004, stran 19):

- Kvantitativna ocena tveganj, katere prvi poskusi se pojavijo že v sedemdesetih letih prejšnjega tisočletja (Tripton & Krause, 2004, str. 807).
- Kvalitativna ocena tveganj, ki pa ima v primerjavi s kvantitativno metodo ocene tveganj bistveno slabost: subjektivnost.

Whitman in Mattord (2011, str. 143) sta proces ocene tveganj povzela v štiri korake:

- določitev verjetnosti, da se bo zgodila zloraba ranljivosti,
- izračun relativne stopnje tveganja za posamezno sredstvo,
- pregled možnih kontrol ter
- dokumentiranje ugotovitev.

Zmanjševanje tveganj je sistematična metodologija, ki jo poslovodstvo uporablja za namen zmanjšanja organizacijskega tveganja (Peltier, 2005, str. 38).

V publikaciji The Orange Book Management of Risk: Principles and Concepts je zapisano, da zmanjševa tveganja vključuje (HM Treasury, 2004, str. 9):

- zmanjševanje tveganja (angl. risk mitigation / alleviation),
- sprejem tveganja (angl. risk acceptance / retention),
- prenos tveganja (angl. risk transfer) ali

- izogibanje tveganju s prekinitvijo aktivnosti in posledično izničitvijo tveganja (angl. risk avoidance).

Peltier (2005, str. 38) doda tem procesom še dva:

- planiranje tveganja (angl. risk planning) in
- omejitev tveganja (angl. *risk limitation*).

Za pomoč pri odločanju za vpeljavo korektivnega ukrepa za namene zmanjševanja tveganja si poomagamo z matriko stopenj tveganj.

Tabela 1: Matrika tveganj

		VPLIV		
		velik	**srednji**	**majhen**
VERJETNOST	**velika**	visoko	visoko	zmerno visoko
	srednja	visoko	zmerno visoko	zmerno majhno
	majhna	zmerno visoko	zmerno majhno	majho

Vir: T. R. Peltier, Information Security Risk Analysis, 2005, str. 26, tabela 2.4.

Na poglasi stopnje tveganja se odločimo, ali bomo korektivni ukrep vpeljali ali ne:

- visoko: korektivni ukrep moramo vpeljati;
- zmerno visoko: korektivni ukrep je priporočljivo vpeljati;
- zmerno nizko: spremljamo dogajanje;
- nizko: zaenkrat ni potrebno vpeljati korektivnega ukrepa.

Ocena ranljivosti in ovrednotenje kontrol je sistematičen pregled kritične infrastrukture in medsebojno povezanih sistemov, na katerih ta temelji, pregled informacij za določanje primernosti varnostnih ukrepov, identifikaciji varnostnih pomankljivosti, iskanju in ovrednotenju možnih alternativ in preverjanju skladnosti po že izvedeni implementaciji (Peltier, 2005, str. 8).

Glavni cilj procesa je identifikacija specifičnih ranljivosti in upravljanju ter odpravi le-teh v sprejemljivem časovnem okvirju na naslednji preko (Whitman & Mattord, 2011, str. 550):

- uporabi že dokumentiranih posptopkov za oceno ranljivosti,
- dokumentiranju informacij iz ozadja in že opravljenih testiranjih za odpravo ranljivosti,
- spremljanju ranljivosti,
- sporočanja informacij o ranljivostih,

- poročanja statusu o ranljivostih ter
- zagotavljanju vpletenosti vodstva podjetja, ki odloča o sprejemu tveganj.

3.2 Analiza vpliva na poslovanje

Analizo vpliva na poslovanje (angl. *business impact analysis*; v nadaljevanju BIA) kot prvo fazo v ciklu razvoja plana neprekinjenega poslovanja Whitman in Mattord (2011, str. 215) opredelita kot preiskavo in oceno vpliva, ki jo imajo lahko različni na organizacijo. BIA se začne, ko se konča proces ocene tveganj.

BIA za organizacijo preko podrobnega scenarija opredeli potencialni vpliv posameznega napada, ki ji preti. S tem organizaciji določi, kako se mora organizacija odzvati na napad, kako zmanjšati škodo, ki jo povzroči napad, kako okrevati glede na nastale učinke napada in kako povrniti normalno poslovanje. Kar pa BIA ne pojasnuje, je to, kakšen je konkreten postopek za vzpostavitev normalnega poslovanja.

BIA sredstva in procese obravnava z vidika kritičnosti, kot npr. to tudi navajata Whitman in Mattord (2011, str. 215). Ker pojem kritičnost sam po sebi ne opredeli vpliva dogodka na organizacijo dovolj natančno in njeno poslovanje, bi bila primernejša delitev glede na časovno odvisne in časovno neodvisne procese oz. sredstva. To delitev bom natančneje pojasnil na dveh hipotetičnih primerih v banki: e-bančništvu in marketinški akciji.

V banki pride do kratkega izpada električne energije. V kolikor v kratkem času banka ne vzpostavi električnega napajanja iz sekundarnega vira, tvega, da bo nastala velika poslovna škoda. Izpad električne energije je zato časovno odvisen proces.

Kot primer časovno neodvisnega procesa bom navedel marketinško akcijo, ki se pripravlja ravno v času izpada električne energije. Tudi daljši izpad električne energije ne predstavlja večjega tveganja z vidika izvedbe marketinške akcije, saj lahko brez večjih posledic odložijo izvajanje akcije na kasnejše obodbje. Izvedba uspešne marketinške akcije pa predstavlja tveganje za banko, saj ji le ta zagotavlja dolgoročni obstanek na trgu.

Z vidika področij v posamezni organizaciji, na katera vpliva nedelovanje oz. nerazpoložljivost sredstv, pa Peltier v sklopu BIA navaja naslednja področja: konkurečni zaostanek, neposredna izguba dobička, izguba zaupanja in ugleda v očeh javnosti, nizka morala, goljifije, napačne odločitve vodstva, moteno poslovanje, pravna odgovornost, izguba zasebnosti in varnostno tveganje (Peltier, 2005, str. 291).

Žnidar (2006, str. 55) ugotavlja, da se metoda BIA razlikuje od večine drugih metod, ki merijo vrednost IT v podjetju, po naslednjih značilnostih:

- Dobljeni rezultati ne kažejo na vrednost informatike v podjetju, temveč na obseg škode, ki nastane kot posledica nedelovanja IT v podjetju.
- Ker se ugotovljeni rezultati nanašajo na dan trenutek in se s časom lahko bistveno spremenijo, je potrebno BIA analizo ob večjih spremembah ponoviti.
- Zaradi načina pridobivanja rezultatov so le-ti praviloma zgolj delno natančni, saj BIA vsebuje zgolj približne ocene. Kljub temu so te za poslovodstvo zelo relevantne.

3.3 Neprekinjeno poslovanje

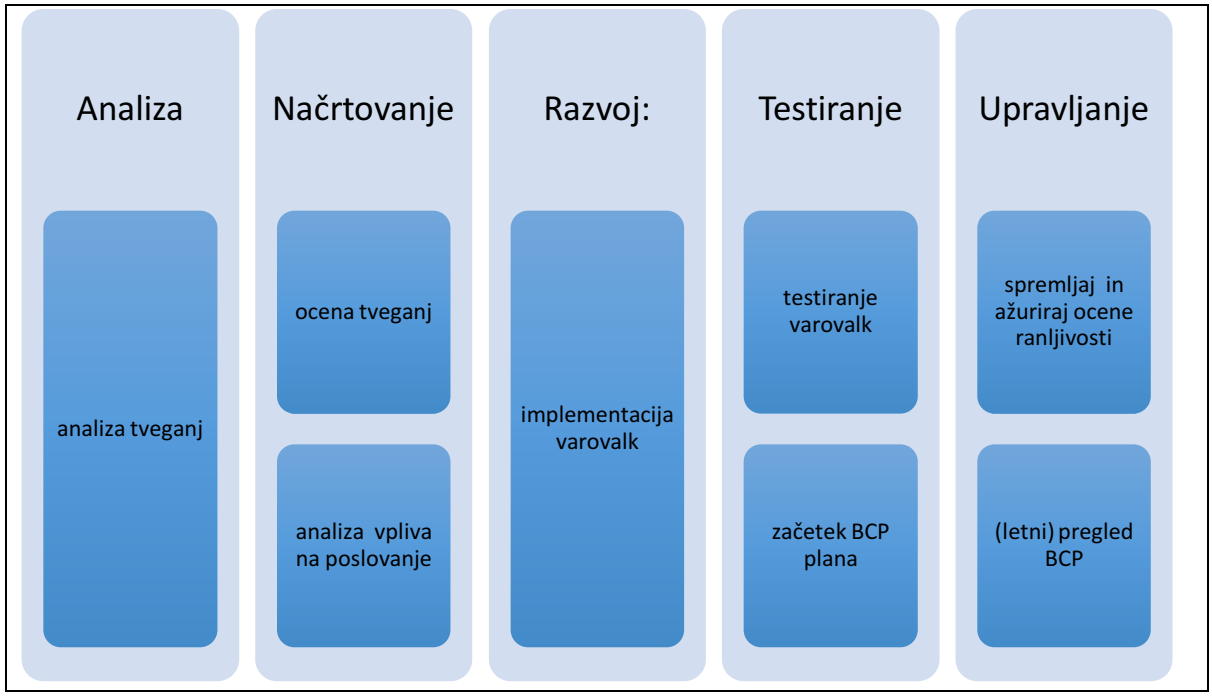
Eden izmed pomembnih ciljev uspešnega podjetja je izvajanje neprekinjenega poslovanja, saj le-to podjetju omogoča izvajanje poslovnih procesov predno se pripeti (varnostni) incident, v času trajanja samega incidenta in odpravi posledic, ko je incident končan.

Neprekinjeno poslovanje obsegajo tako procesi, postopki, odločitve in aktivnosti, ki jih podjetje izvaja v primeru motnje ali prekinitve delovanja. Za zagotovitev neprekinjenega poslovanja je potreba izdelava reaktivnih in proaktivnih načrtov, ki podjetju pomagajo pri izogibanju kriznih situacij in katastrof ter mu omogočajo pravočasno obnovo poslovanja. V kolikor do krizne situacije tudi pride, načrt neprekinjenega poslovanja podjetju omogoča hitro obnovo poslovanja (Continuity Central, 2016). Whitman in Mattord (2011, str. 215) pa ugotavljata, da npr. majhna podjetja ne potrebujejo plana neprekinjenega poslovanja ali ga ne izvajajo v enakem obsegu, kot ga izvajajo večja podjetja (npr. plan neprekinjenega poslovanja ne predvideva obnove poslovanja v nadomestni stavbi). Obenem ugotavljata tudi, da še posebej podjetja v proizvodni panogi in prodaji na drobno sploh nimajo možnosti vzpostavitve neprekinjenega poslovanja na nadomestni lokaciji. Vsaj na kratek rok so namreč vezana na poslovanje na fizični lokaciji.

Avtorji upravljanje neprekinjenega poslovanja razlagajo zelo podobno. Clanch (2004, str. 13) kot ključne korake pri izdelavi načrta neprekinjenega poslovanja navaja:

- **Analiza vpliva na poslovanje**, ki pove, kateri procesi in sredstva so izpostavljeni tveganju in kateri so kritični z vidika časovne komponente.
- **Analiza tveganja**, ki ugotovi ranljivosti in tveganja, ki jim je izpostavljeno podjetje.
- **Koncept obnove** opredeli strategijo za obnovo poslovanja.
- **Priprava načrta obnove** predpiše postopke in izdela načrt za obnovo poslovanja.
- **Testiranje postopka obnove** preverja ustreznost načrta ter postopkov.
- **Proces upravljanja sprememb, testiranja, izobraževanja in pregledovanja** je edini nepretrgan proces izmed procesov in spremlja delovanje neprekinjenega poslovanja, ko se ta prične izvajati.

Slika 2: Upravljanje procesa neprekinjenega poslovanja



Povzeto in prirejeno po T. R. Peltier, Information Security Risk Analysis, 2005, str. 9.

Peltier (2005, str. 9) pa upravljanje procesa neprekinjenega poslovanja deli na podobne faze, na katere jih deli tudi Clunch:

- **Analitika**: opredelitev tveganj.
- **Načrtovanje**: arhitektura, ki temelji na varnostnih zahtevah.
- **Razvoj**: pripravimo varnostne kontrole in varovalke.
- **Testiranje**: pred produkcijskim zagonom preverimo, ali nam varovalke in varnostne kontrole dejansko zmanjšujejo tveganje na sprejemljivo raven.
- **Upravljanje**: ko pride do sprememb ali posodobitev, ponovno preverimo varnostne kontrole in varovalke; preverbe delamo tudi planirano – periodično.

4 STROŠKI KIBER KRIMINALA

Število kiber kriminalnih dejanj je prič v letu 2015 preseglo število kriminalnih dejanj v Združenem kraljestvu (v nadaljevanju UK) ugotavlja National Crime Agency v poročilu izdanem 7. julija 2016 (Krebs, 2016). Poročilo navaja, da je bilo v letu 2015 izmed vseh prijavljenih kriminalnih dejanj v UK 36% kiber goljifij in 17% zlorab računalnikov, kar skupaj predstavlja 54% odstotkov (2,46 milijona) izmed vseh prijavljenih kriminalnih dejanj. Iz tega sledi, da je bilo vseh ostalih vrst kriminalnih dejanj manj kot polovica, natančneje 46%. Različnih žrtev kiber kriminalnih dejanj, ki so incident prijavile, je bilo skupaj 2,11 milijona.

Zaradi dovršenosti orodij za izvedbo kiber kriminalnega dejanja, zaradi razvitega črnega trga teh orodij, zaradi profesionalizma kiber kriminalcev in kiber kriminalnih organizacij, med žrtve kiber kriminalnih dejanj štejemo vse od posameznega prebivalca, manjša in velika podjetja, korporacije, (neprofitna) društa in mnoge druge. Velja rek, da "Ni več vprašanje, če boste postali žrtev zlorabe v kiber svetu, temveč je le še vprašanje, kdaj se bo to zgodilo" (It's not if but when a cyber security attack will happen, 2016).

Na podlagi študije, ki so jo opravili raziskovalci v Cambridgeu skupaj s sodelavci iz Nemčije in Nizozemske, ZDA in UK, Valley (2012, str. 10) deli stroške kiber kriminala v tri skupine:

- **Neposredni stroški**, med katere uvrščamo npr. odtujen denar iz bančnih računov, zlorabljenih bančnih in kreditnih kartic, stroški analize in forenzike, odvetniške storitve.
- **Stroški za zaščito**, ki delujejo preventivno in zmanjšujejo tveganja, npr. nakup in vpeljava naprednega sistema za detekcijo in preprečitev vdorov.
- **Posredni stroški**, ki jih ne moremo neposredno pripisati samemu dejanju, a nastanejo kasneje kot posledica tega dejanja, npr. prehod strank h konkurentom, izguba ugleda in zaupanja. Te stroške je velikokrat zelo težko oceniti in se lahko hitro zgodi, da vsebujejo subjektivno komponento.

4.1 Stroški kiber kriminala na makro ravni

Stroški kiber kriminala na makro (državni) ravni se po državah razlikuje. Irska npr. ocenjuje, da državi kiber kriminal povzroči letno 630 milijonov evrov stroškov (Conmy, 2014, str. 2). Kar 255 milijonov evrov stroškov od teh pa predstavljajo stroški, ki so bili nekoč posledica tradicionalnega kriminala.

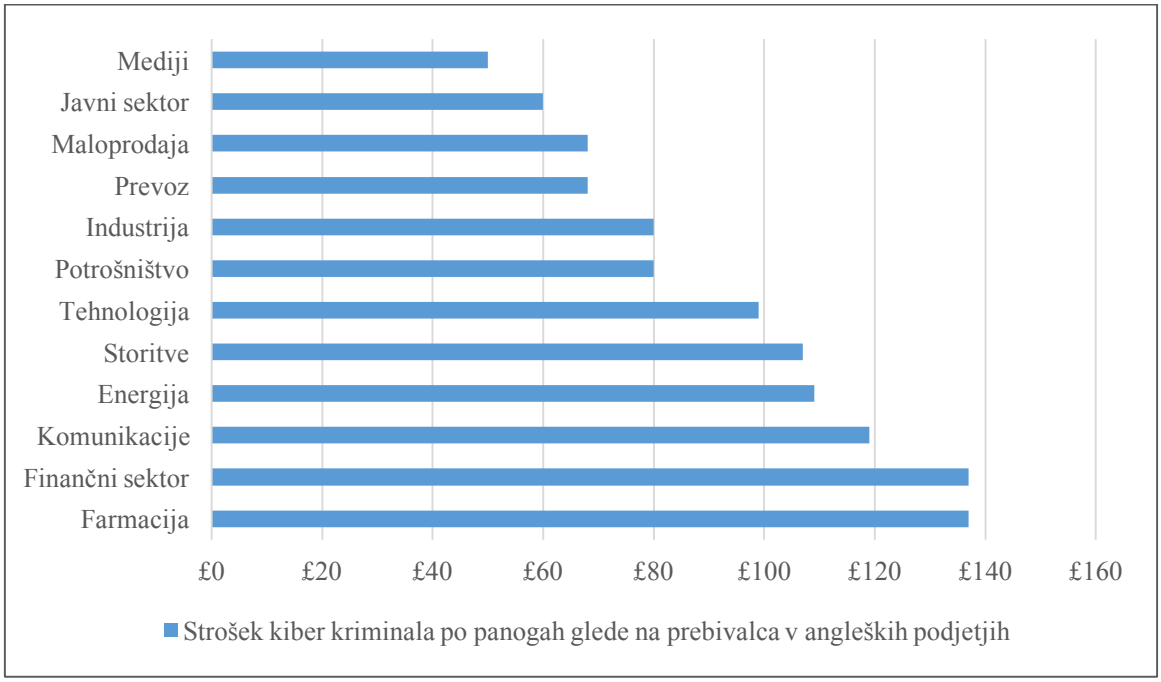
Kerner (2015, str. 1) navaja, da so se glede na rezultate študije stroškov kiber kriminala, ki jo letno pripravlja Ponemon Institute, povprečni stroški kiber kriminalih dejanj na letni ravni v ZDA med 2014 in 2015 povečali kar za 19%. Rast stroškov kiber kriminalnih dejanj pa je zaznati tudi v drugih državah.

Študija, ki jo je opravilo podjetje Detica v sodelovanju s Kabinetom za kiber varnost (angl. *Cabinet Office's Office of Cybersecurity and Information Assurance*), ocenjuje, da je kiber kriminal povzročil celotnemu gospodarstvu v UK v letu 2011 kar 27 milijard (Valley, 2012, str. 10).

Ponemon inštitut je opravil raziskavo v Angliji o stroških kiber kriminala glede na panogo. Stroški kiber kriminala so v študiji predstavljeni kot strošek glede na enega prebivalca Anglije na letni ravni.

Študija prikaže, da so stroški kiber kriminalnih dejanj največji v finančnem in farmacevtskem sektorju, sledijo pa jim stroški kiber kriminalnih dejanj na področju energetije in komunikacij.

Slika 3: Strošek kiber kriminala po panogah glede na prebivalca v angleških podjetjih



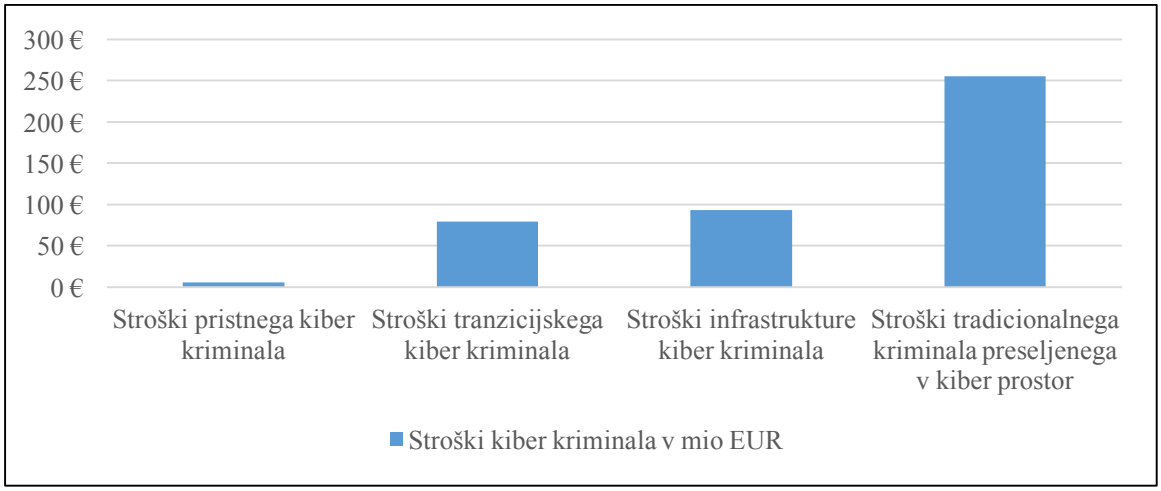
Vir: T. Caldwell, 2014, The true cost of being hacked, str. 10, tabela 5.

Analiza zajema stroške izražene v absolutni velikosti. Višina stroškov kiber kriminalnih dejanj v analizi je, kot je tudi v nekaterih drugih analizah, še predvsem tistih, ki so sponzorirane s strani proizvajalcev varnostnih rešitev, zelo visoka. Številni avtorji zato dvomijo o nepristranskosti tovrstnih analiz oz. v uporabljeno metodologijo. Kot primer navajam podatek iz ankete, ki jo je izvedel Computer Security Institute (www.gocsi.com), v katerem podaja nenavadno visok ocenjen strošek izgube prenosnega računalnika v višini 89.000 dolarjev (Cyber-Crime Losses, 2002, str. 1).

Center for Strategic and International Studies je leta 2014 opravil študijo stroškov, ki nastanejo kot posledica kiber kriminalnih dejanj na vetovni ravni. Poleg stroškov izraženih v denardni valuti ugotavlja tudi, da posledica kiber kriminalnih dejanj predstavlja tudi izgubo delovnih mest. Za Združene države Amerike (v nadaljevanju ZDA) ocenjuje, da jih kiber kriminal »stane« 200.000 delovnih mest. V Evropski uniji (v nadaljevanju EU) je ta številka manjša za četrtino in tako kiber kriminal »stane« EU 150.000 delovnih mest. V nadaljevanju študije avtorji ocenjujejo, da se bodo stroški kiber kriminala na globalni ravni povečevali, prvenstveno zaradi vse večjega števila podjetij, katerih poslovanje se seli ali povezuje v internet (Cyber Crime Costs More Than $400B Annually, 2014, str. 1).

Analiza stroškov kiber kriminalnih dejanj v letu 2013 na globalni ravni z vidika vrste kiber kriminalnih dejanj pokaže, da stroški pristnih kiber kriminalnih dejanj predstavljajo le 1,4 % vseh stroškov. Največji delež stroškov (58,9%) kiber kriminalnih dejanj analiza pripiše kiber kriminalnim dejanjem, ki izvirajo iz tradicionalnih kriminalnih dejanj in so se zgolj preselila v kiber prostor.

Slika 4: Stroški kiber kriminala v letu 2013



Povzeto po Grant Thornton, 2015, Cybercrime: Facing the challenges, str. 10, tabela 2.7.

4.2 Stroški kiber kriminala na mikro ravni

Stroške, ki nastanejo posameznemu podjetju v povezavi s kiber kriminalnimi dejanji, različni avtorji opredelijo podobno. Valley (2012, str. 10) je stroške kiber kriminala razdelil na podlagi primera zlorabe kreditne kartice:

- **Neposredni stroški** so v prvi vrsti finančne izgube, ki v tem primeru predstavljajo izgubo denarja žrtve, ki so ji zlorabili kreditno kartico. Tipično so ti stroški bolj objektivne narave.
- **Posredni stroški** predstavljajo dodatne stroške (dela), ki nastanejo banki kot posledica nezaupanja v elektronsko bančništvo zaradi česar več ljudi opravlja bančne storitve na bančnih okencih. Tipično so ti stroški bolj subjektivne narave.
- **Stroški obrambe**, ki predstavljajo stroški nakupa varnostnih rešitev in stroškov, ki nastanejo pri okrevanju.
- **Stroški družbe** predstavljajo vsoto vseh treh vrst stroškov.

Stroške kiber kriminala še nadalje razčlenimo na (Grant Thornton, 2015, str. 8):

- Med neposredne stroške uvrsti poleg finančnih izgub tudi stroške obveščanja in stroške intelektualne lastnine.

- Stroške obrambe opredeli kot denarni ekvivalent stroškov preprečitve, zaznavanja in eskalacije.
- Posredne stroške opredeli kot neoprijemljive stroške izgube poslovanja, ki so tipično večji v primerih, ko pride do izgube ali odtujitve podatkov. Mednje uvršča nižje prihodke zaradi izgube strank, povečanje aktivnosti za pridobivanje novih naročnikov, izgube ugleda in vpliva na dobro ime podjetja.

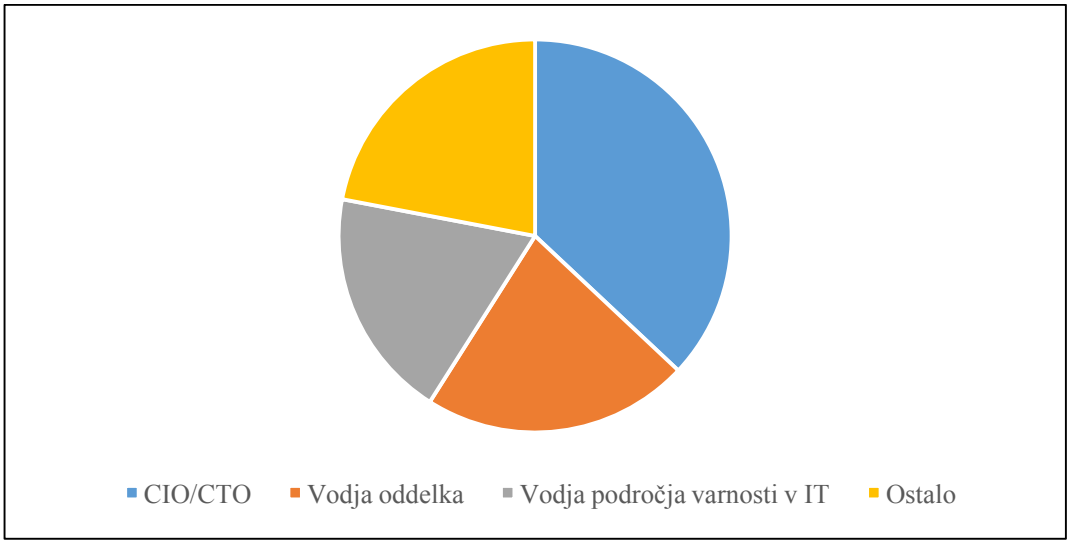
Savitz in Lewis (2012) sta v članku izdanem v reviji Forbes analizirala stroške kiber kriminala s področja DDoS napadov. Osredotočila sta se na analizo, kakšni stroški nastanejo podjetju v času med in po izvedenem DDoS napadu. Pri analizi sta upoštevala neposredne in posredne stroške, nista pa vključila stroškov obrambe, zaradi česar končna ocena stroškov ni popolna. Stroške nedelovanja storitve v času napada tako strnita v naslednje skupine:

- **Operativa**: koliko ljudi iz IT oddelka se bo ukvarjalo z incidentom koliko časa in koliko je njihov strošek dela.
- **Pomoč uporabnikom**: zaradi nedelovanja storitve bo povečano število klicev v klicni center. Koliko več bo potrebnih ljudi v klicnem centru izraženem glede na opravljene klice in stroške dela.
- **Obnovitev poslovanja**: koliko dela bo potrebnega za obnovo storitve izraženo kot npr. strošek dela zaposlenih, strošek zunanjih svetovalcev in izvajalcev itd.
- **Strošek nezmožnosti dela**, ki se bo odrazila kot izpad produktivnosti zaposlenih, ki niso mogli opravljati svojega dela.
- **Izgubljene stranke**: koliko strank in posledično prihodka bo podjetje izgubilo, ker bodo te prešle h konkurentom.
- **Kazni**: koliko stroškov bo nastalo z vidika odgovornosti, saj razpoložljivost storitve ne bo dosegala normativov iz pogodbe o določanju nivoja storitev (angl. *Service Level Agreement*). Kako visoka kazen bo doletela podjetje s strani države ali regulatorjev?
- **Izgubljen posel v prihodnosti**: koliko potencialnih novih strank ne bo sklenilo s podjetjem posla, ker mu ne bodo zaupale?
- **Izguba ugleda**: kolikšna bo za podjetje izguba ugleda z vidika prepoznavnosti in tržne znamke?

4.3 Paradoks deleža IT sredstev namenjenih za varnost

Kljub zavedanju porasta vdorov se številne organizacije še vedno ne zavedajo, da so lahko tudi sami žrtev kiber kriminalnega dejanja ali pa ne storijo dovolj, da bi se učinkovito zaščitili pred kiber kriminalnim dejanjem. Glede na lastne izkušnje bi kot enega najpogostejših izgovorov za tovrstno sprenevedanje izpostavil sprenevedanje, da je podjetje premajhno, nezanimivo ali nima dovolj vrednih informacij, da bi postalo žrtev kiber kriminalnega dejanja.

Slika 5: Nadzor nad sredstvi za IT varnost



Povzeto in prirejeno po M. Vizard, Inside the IT Security Budget Paradox, 2005, slide 2.

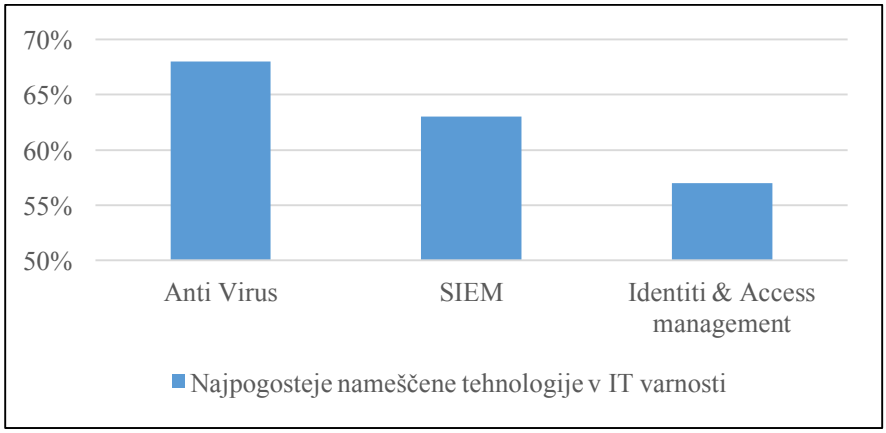
Podjetja posledično zaradi tovrstnih sprenevedanj ne namenjajo dovolj časa ali sredstev za zaščito pred kiber kriminalnimi dejanji oz. drugimi dejanji, ki bi imela za posledico izgubo podatkov, nedelovanje storitve ali podobno. Ta sredstva pogosto ohranjajo v istem obsegu ali pa jih celo zmanjšujejo. Temu pojavu pravi Channel Insider paradoks IT sredstev namenjenih za varnost. V sklopu analize pojava so anketirali 1.825 strokovnjakov iz IT in varnostnega področja (Vizard, 2005).

Razporejanje sredstev namenjenih za varnost IT je glede na podatke iz ankete v 37 % primerov v upravljanju direktorjev informatike oz. tehničnih direktorjev. Vodje področja IT varnosti, za katere bi pričakovali, da so najbolj kompetentne osebe v podjetju na tem področju in bi tako najbolje znali oceniti potrebna sredstva, pa imajo le v 19 % primerih ključno vlogo nad temi sredstvi.

Od vseh anketirancev jih je le 24 % odgovorilo, da je IT varnost ena izmed dveh ključnih strateških področij.

V povprečju delež sredstev namenjenih za varnost IT predstavlja le 8,2 % celotnega letnega IT proračuna. Zgolj 9,2 % sredstev namenjenih za varnost IT v povprečju podjetja vlagajo v nove varnostne tehnologije in rešitve. Preračunano na letno raven to pomeni, da v nove tehnologije na področju IT varnosti anketiranci vlagajo manj kot 1 % vseh IT sredstev. Tega problema se zaveda več kot polovica anketirancev, saj so odgovorili, da podjetja ne namenjanjo dovolj sredstev, da bi bili skladni z vsemi regulativami, standardni in zakoni, ki veljajo na področju IT varnosti.

Slika 6: Najpogostejše nameščene tehnologije v IT varnosti



Povzeto in prirejeno po M. Vizard, Inside the IT Security Budget Paradox, 2005, slide 15.

Presenetljivo visok odstotek anketirancev (84 %) pravi, da namenjajo sredstva v sisteme za preprečevanje vdorov (angl. *Intrusion Prevention System*; v nadaljevanju IPS), saj jih po drugi strani le 41 % verjame, da je IPS sistem ključen za zaščito sistema.

72 % odstokov anketirancev je odgovorilo, da že uporablja ali planira uporabljati sisteme za upravljanje identitet in dostopov (angl. *identity & access management*). Delež tistih, ki so odgovorili, da je naložba v tovrstne sistema ekonomsko učinkovita, je višji, kot je delež anketirancev glede učinkovitosti IPS sistemov. Ta znaša 57 % vseh anketirancev.

Slika 7: Zadovoljstvo z investicijami v IT varnost

Povzeto in prirejeno po M. Vizard, Inside the IT Security Budget Paradox, 2005, slide 14.

4.4 Zavarovanje kiber odgovornosti

Zaradi porasti stroškov, ki nastajajo ob reševanju problemov, se vse več podjetji ali lastnikov organizacij odloča za zavarovanje pred posledicami kiber kriminala. Zavarovanje

kiber odgovornosti (angl. *cyber insurance*) se osredotoča na e-poslovanje, in sicer: uporaba spleta, fizična ali elektronska hramba podatkov, obdelovanje podatkov, spletne transakcije in druge digitalne dejavnosti, katerih učinki zlorab se prenašajo na tretje osebe.

Večina zavarovalnih polic kiber zavarovanja ponuja kombinacijo zavarovanja odgovornosti pred zahtevki tretjih oseb in zavarovanje lastne škode. Zavarovanje odgovornosti – to pomeni, da zavarovalnica krije stroške pravne zaščite v primeru pravnih zahtevkov tretjih oseb in morebitno pravno priznano škodo tem tretjim osebam ter morebitne kazni in globe. Zavarovanje lastne škode pa krije stroške in škodo na strani podjetja – na primer upad prihodkov, morebitno odkupnino za podatke, forenzično preiskavo, obnovitev računalniških sistemom ali podatkov, PR-stroški ipd. (Tomšič, 2016).

Nastala škoda zaradi kiber kriminala pa ni edni razlog, zakaj se bo vse več podjetij odločalo za tovrstna zavarovanja. Po skoraj treh letih pogajanj sta Evropski parlament (na ravni odborov) in Evropski svet (na ravni veleposlanikov) decembra 2015 dosegla dogovor o novih pravilih o varstvu podatkov. Sprejeta je bila direktiva o varovanju informacij in omrežij ter zasebnosti podatkov. Uradni besedili uredbe in direktive sta bili po uradnem formalnem sprejetju 4. 5. 2016 objavljeni v Uradnem listu, veljati pa bosta začeli 25. 5. 2018 (Evropska direktiva 2016/680).

Direktiva gospodarskim družbam, ki upravljajo z osebnimi podatki, nalaga še večjo odgovornost za njihovo varstvo. Poslovni subjekti bodo morali pričeti z uvajanjem ustreznih mehanizmov za povečanje informacijske varnosti. V primeru vdora v sistem in morebitno zlorabo osebnih podatkov bodo morala podjetja seznaniti nadzorne organe v organizaciji in ustrezno ukrepati. V primeru neustreznega reševanja problema bodo podjetje in njegovi zakoniti zastopniki finančno kaznovani. Ocenjujem, da bo implementacija direktive Evropske komisije v zakonodaje držav članic EU pomembno vplivala na rast povpraševanja po zavarovanju kiber odgovornosti v prihodnjih letih.

5 STRATEGIJA KIBERNETSKE VARNOSTI (MAKROSTRATEGIJA)

Delovanje kiber kriminalcev postaja vse bolj organizirano, posamezniki in skupine se povezujejo v kriminalne združbe. Uspešno zoperstavljanje, zaščita in boj proti kiber kriminalu z vidika posameznika vse manj učinkovit.

Številne paradržavne in paravojaške skupine, kot je npr. na kitajskem People's Liberation Army enota 61398, so ustanovljene in financirane za namene kiber vojskovanja med državami. Naloge takšnih skupin niso zgolj obramba pred kiber napadi na državni ravni. Poleg obrambnih nalog izvajajo namreč tudi kiber napade, ki so večinoma politično motivirani (About ENISA, 2016).

Na nivoju EU je v boju proti kiber kriminalu bila leta 2004 ustanovljena agencija za omrežja in informacijsko varnost (European Union Agency for Network and Information Security), katere cilj je zaščita informacijske družbe. Naloge agencije se odražajo na treh področjih (About ENISA, 2016):

- Priprava priporočil za članice EU.
- Aktivnosti, ki so v podporo procesu priprave politike in implementacije le-te.
- Neposredna pomoč operativnim ekipam članicam EU, ki se tipično izvaja v obliki usposabljanj in drugih vrst treningov.

V prvih letih novega stoletja so prišle težnje, da North American Trading Organization (v nadaljevanju NATO) pripravi obrambno politiko v boju tudi s kiber terorizmom. NATO je tako v začetku leta 2008 pripravil prvo politiko za obrambo proti kiber terorizmu (Mahon, 2015, str. 21). Estonija je namreč v letu 2007 doživela obsežen kiber napad. Za napad naj bi bila odgovorna Rusija. V tem času so bila namreč velika nasprotovanja med Rusijo in Estonijo glede premestitve grobov vojakov iz Talina (Russia accused of unleashing cyberwar to disable Estonia, 2016).

NATO-va politika postavlja zaščito omrežij in infratrukture združenja članic je postala tako ena izmed prioritetnih nalog te organizacije. Implementacijo in upravljanje kiber varnostne politike prenese na posamezne države članice organizacije. Politika posameznih članic bo usmerjena v zaščito njihovih fizičnih in digitalnih sredstev (Mahon, 2015, str. 21).

Posamezne članice, ki same nimajo dovolj zadostnega znanja in sredstev, bo NATO aktivno pomagal pri pripravi strategije, preko katere bo takšna članica sprejela učinkovito politiko, ki bo lahko kljubovala kiber grožnjam. Ena pomembnejših nalog NATO kiber politike tako postaja izobraževanje in pomoč na državni ravni, da bodo države lahko implementirale robustno politiko.

Do leta 2012 je že več kot 50 držav pripravilo dokument na temo strategije boja proti kiber kriminalu (Klimmburg, 2012, str. 12). Anglija je 2011 kiber varnost že postavila na seznam top prioritet in se je zavezala, da bo v štirih letih za izvajanje državnega kiber varnostnega programa namenila preko 650 milijonov funtov (Cabinet Office, 2011, str. 8).

Republika Slovenija je 25. 2. 2016 sprejela Strategijo kibernetske varnosti Republike Slovenije. Dokument kot tak je začel nastajati že leto dni preje, prve aktivnosti za ureditev tega področja pa segajo vse do leta 2008. Cilj strategije je, da bo Republika Slovenija okrepila sistem zagotavljanja kibernetske varnosti, hkrati pa to področje tudi sistemsko uredila (Sporočilo za javnost Vlade RS, 2016).

Strategija ima jasno postavljeno vizijo, kaj želi v naslednjih petih letih doseči. Cilj je, da bi Slovenija vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. Ta cilj obsega osem podciljev (Strategija kibernetske varnosti, 2016):

- Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti.
- Varnost državljanov v kibernetskem prostoru.
- Kibernetska varnost v gospodarstvu.
- Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore.
- Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala.
- Razvoj obrambnih kibernetskih zmogljivosti.
- Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.
- Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.

V Sloveniji na državni ravni delujejo različne organizacije in projekte, ki vsak na svoj način prispevajo k izboljšanju informacijske varnosti:

- SI-CERT,
- Varni na internetu,
- Ceneter za varnejši internet,
- (v nastajanju) SIGOV-CERT in drugi.

SI-CERT je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT samostojno izvaja nacionalni program ozaveščanja Varni na internetu (O centru SI-CERT, 2016).

Center za varnejši internet, ki ga vodi konzorcij, sestavljen iz Fakultete za družbene vede Univerze v Ljubljani, Arnesa, Zveze prijateljev mladine Slovenije in Zavoda MISSS11 se izvajajo programi SAFE.SI12, Spletno oko in TOM telefon. Center za varnejši internet je dosegljiv preko spletne strani https://www.varninainternetu.si/.

Program SAFE.SI deluje kot nacionalna točka ozaveščanja otrok in najstnikov o varni rabi interneta in varni rabi mobilnih naprav. Dosegljiv je na enakem spletnem naslovu, kot je ime programa: http://www.safe.si. Program Spletno oko je prijavna spletna točka, ki

omogoča anonimno prijavo glede suma o gradivu, ki vsebuje spolnime zlorabe otrok in sovražni govora na spletu. Druga naloga programa pa je ozaveščanje o problematiki nezakonitih spletnih vsebin. Program TOM telefon je namenjen predvsem mlajši generaciji in svetuje o varni rabi interneta in mobilnih naprav.

Področje kiber kriminala v Sloveniji obravnavajo glede na različne pristojnosti zlasti naslednji organi:

- Slovensko obveščevalno-varnostna agencija (SOVA),
- Policija,
- Ministrstvo za javno upravo (MJU) oz. v okviru MJU ga obravnava direktorat za informatiko,
- Ministrstvo za obrambo,
- Urad za informatiko in telekomunikacije in
- Uprava kriminalistične policije – oz. znotraj uprave Center za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala.

6 ANALIZA ODMEVNEJŠIH PRIMEROV KIBER KRIMINALA PRI NAS IN DRUGOD PO SVETU Z VIDIKA POLITIČNO-EKONOMSKE PERSPEKTIVE

Predstavil bom odmevnejše primere kiber kriminala pri nas in drugod po svetu z vidika politično-ekonomske perspektive, pri čemer se bom osredotočil na naslednja področja:

- politične, ekonomske ali verske motivacije;
- nastalih stroškov;
- ciljane populacije;
- razvoja vrste dejanja skozi zgodovino.

6.1 Prevare predplačila

Prevare predplačila (angl. *Advance-fee scam*) so se dogajale že v svetu kriminala, še predno so se torej pojavile v obliki kiber kriminalnih dejanj. Cilj tovrstnih prevar je pridobivanje žrtvinega zaupanja, preko katerega žrtev napeljejo, da vplača majhen znesek kot znesek za pokritje npr. administrativnih stroškov za pridobitev zapuščine v obliki osebnega avtomobila. Ko enkrat žrtev poplača namišljene administrativne stroške, se kriminalec ponavadi odzove z zahtevo po poplačilu še dodatnih nepredvidenih stroškov z novo obrazložitvijo, da so npr. nastali nepričakovni zapleti in zato za izvedbo postopka zapuščine potrebuje še nekaj dodatnega denarja. Cilj je torej popolnoma ekonomske narave, torej pridobitev denarja na kazniv način. Uspešnost prevar predplačila se kaže

predvsem na račun izkoriščanja zaupanja žrtev in na račun pohlepa žrtev, da bi v kratkem času prišli do premoženja.

Prevara predplačila je v svetu kiber kriminala uveljavilo kot "Nigerijsko pismo" ali "Prevara 419". "Nigerijsko pismo" je prevara, ki je dobila ime glede na velikokrat sklicevano državo Nigerijo v e-poštnih sporočilih. Ker pa v Nigeriji področje prevar, lažnih obljub in drugih podobnih kriminalnih dejanj obravnava člen št. 419 nigerijskega kazenskega zakonika, se je za tovrstna kiber kriminalna dejanja uveljavilo tudi ime "Prevara 419" (What Is The '419' Scam?, 2016). ,

Tehnike uporabljene v prevarah so se ves čas izpopolnjevale. Pomemben cilj je bil, da e-sporočila izgledajo čim bolj pristno. Kiber kriminalci so zato v e-sporočilih uporabili predvsem naslednje tehnike (What is a 419 (Advance-fee Fraud) Scam?, 2016):

- Prejemnik sporočila vidi, da je bilo sporočilo poslano samo njemu.
- Imena fiktivnih oseb in sorodnikov, ki naj bi zapustili večje vsote denarja denarja, so sestavljena pogosto iz npr. priimka prejemnika, da je žrtev zavedena, da gre morda res za nekoga, ki ga ne poznajo, a so z njim v sorodu.
- (S pomočjo storitve Google translate) prevejajo sporočila v materni jezik žrtve (Primeri spletnih goljufij, 2016).
- V sporočilih navajajo telefonske številke, kamor lahko potencialne žrtve pokličejo in preverijo avtentičnost poslanega sporočila.
- Za pridobivanje dodatnega zaupanja uporabijo ponarejene dokumente ali žige različnih vlad, držav in podjetij.

Posledice uspešno izvedene prevare imajo lahko večje izgube sredstev. Obravnavanih je veliko primerov, ko so žrtve izgubile vse svoje premoženje. Celo sposojale so si še denar od prijateljev in bank, predno so ugotovili, da so bili žrtev prevare.

Obramba pred tovrstnimi napadi ne zahteva najsodobnejših varnostnih rešitev. Bolj učinkovito je izobraževanje in osveščanje zaposlenih in nasploh javnosti, naj dvakrat premislijo o avtentičnosti in namenu sporočil, ki jim obljubljajo denar ali drugo vrsto nagrade. Neznancem ne pošiljamo denarja, osebnih podatkov, kreditnih kartic in drugih občutljivih informacij.

6.2 Maščevanje

Dejanje maščevanja lahko opredelimo kot povračilni ukrep, škodljivo dejanje storjeno proti osebi, skupini oseb, tudi organizaciji. Motivi za izvedbo dejanja iz maščevanja so različni glede na vsako dejanje, bi jih pa razvrstil v naslednje večje skupine: jeza, žalost, posmehovanje, prizadetost, zaničevanje, občutek zlorabe in drugi motivi.

Prvi poznan primer maščevanja kot kiber kriminalnega dejanja je izvršil Tim Lloyd. Ta je leta 1996 iz maščevanja izvedel sabotažo v podjetju Omega, v katerem je bil pred tem 11 let zaposlen kot oseba, ki je uživala ugled in spoštovanje sodelavcev in nadrejenih. Lloyd pa je imel v zadnjem letu, ko je še bil zaposlen v podjetju Omega, vse več nesoglasij z vodstvom podjetja, zato je sumil, da ga bodo odpustili. Ker se je želel delodajalcu maščevati, če bi ga dejansko tudi odpustil, je v informacijski sistem vgradil mehanizem za brisanje podatkov. Lloyda so kasneje v podjetju Omega odpustili in kmalu po njegovem odhodu iz podjetja je mehanizem nepovratno pobrisal celotno vsebino datotečnega strežnika. Takrat je podjetje Omega tudi ugotovilo, da se arhivske kopije podatkov niso izvajale tako, kot so pričakovali (Gaudin, 2000, str.1).

Vzrok: interno nesoglasje pripelje do odpovedi pogodbe o zaposlitvi. Ker je bil Lloyd ključna oseba v podjetju na področju IT, je nesporazumna (enostranska) prekinitev delovnega razmerja za podjetje povečala tveganje za podjetje z varostnega vidika, a se podjetje tega v danem momentu ni zavedalo. Želja po maščevanju je pripeljala do izgube podjetja v višini več kot 10 milijonov dolarjev. Največji delež te izgube je predstavljal posredni strošek izgube posla zaradi nezmožnosti dobave izdelkov. Poleg finančne izgube je bila posledica tega dejanja tudi izguba dela za cca. 80 zaposlenih. Lloyd je bil za dejanje obsojen in je prestal kazen v zaporu.

Kot drugi primer maščevanja, ki ima posledico kiber kriminalno dejanje, bom obravnaval dejanje Walterja Powella. Powell je bil pred izvedbo dejanja zaposlen v podjetju Baltimore Substance Abuse System kot vodja področja upravljalski informacijski sistem (angl. *Management Information Systems*). Leta 2009 je bil odpuščen in s tem je formalno izgubil dostop do sredstev podjetja (Bergen, 2011). A kljub temu je uspel več kot stokrat dostopati do sredstev IT podjetja s pomočjo gesel drugih uporabnikov, ki si jih je nepooblaščeno prisvojil (Herman, 2016). Želja po maščevanju ga je vodila k cilju škodovati ugledu podjetja in njegovih zaposlenih. V imenu nekdanjega nadrejenega (kaznivo dejanje zlorabe identitete) je npr. pošiljal poneverjeno e-pošto na različne e-poštne sezname v podjetju, tretjim osebam je npr. prepošiljal zaupne informacije podjetja itd. Direktorja podjetja Grega Warrena je postavil v neprijeten položaj, ko je v prezentaciji, ki jo je uporabil pri predstavitvi pred nadzornim odborom podjetja, zamenjal eno prosojnico z novo, na kateri je bila slike gole ženske. To so si ogledali vsi prisotni na velikem zaslonu diagonale velikosti 162 cm. Neposredni stroški, ki so nastali: 80.000 dolarjev za nakup varnostnih rešitev (Agnihotri, 2016).

6.3 SPAM

Pošiljanje nenaslovljene oz. nezaželene pošte je potekalo v obliki pošiljanja pošte v papirni obliki, še predno je to postalo problem v kiber prostoru. Pošiljanje spam elektronske pošte je v primerjavi s pošiljanjem tradicionalne pošte mnogo bolj razširjeno, saj so stroški pošiljanja nezaželene pošte preko elektronskih poti zanemarljivi.

Namena pošiljanja nezaželene e-pošte sta dva:

- Pošiljanje reklamnih sporočil; nezaželena pošta, ki ima soroden namen, poznamo tudi iz "papirnatega" sveta.
- Pošiljanje vsebine s škodljivo vsebino ali povezavo do le-te.

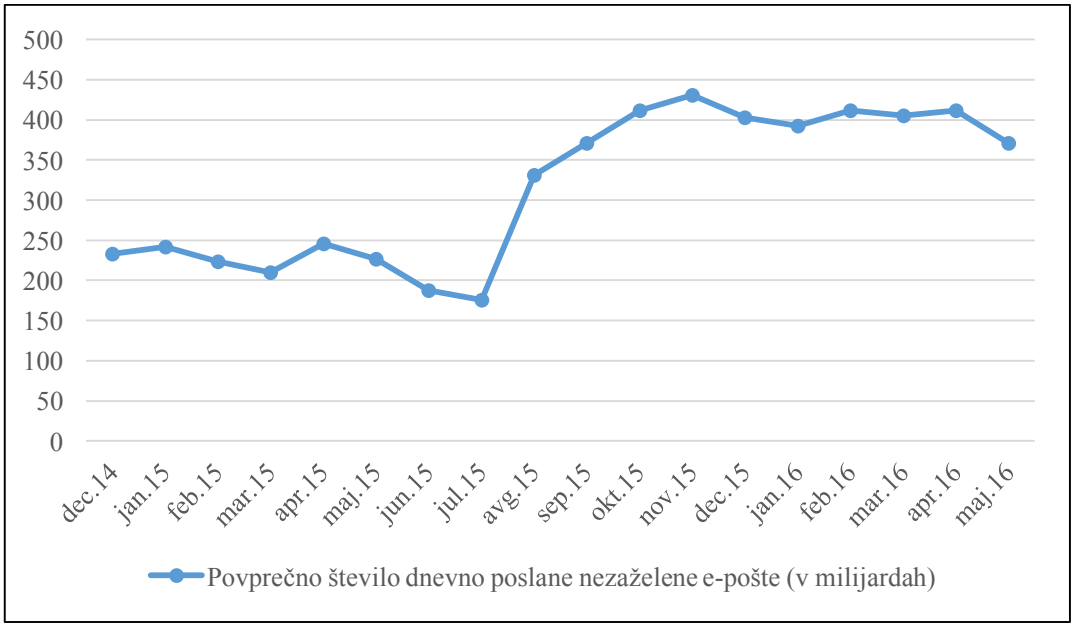
Pošiljanje reklamnih sporočil ne predstavlja dejanja, katerega cilj je povzročitev neposredne škode. Sicer z vidika prejemnika posredna škoda vseeno nastane, saj zaposleni porabijo čas za prebiranje in brisanje spam pošte, kar se na nivoju organizacije lahko odrazi kot izgubljene minute, ure ali dnevi. Kot posredni strošek lahko navedeno tudi npr. nakup varnostnih rešitev za detekcijo in preprečavanje dostave nezaželene e-pošte. BitDefender Labs ugotavlja, da so najpogostejše tematike spam sporočil od leta 2007 dalje naslednje (Penny Stocks and sexual enhancing drugs top spam topics for 2007, 2016): zdravila (vezano na težave v spolnosti), zdravila (vezano na izgubo prekomerne telesne teže), replike ur, hipoteke, ribarjenje, elektronika, potovanja, delnice, programska oprema, diploma, dovoljenja, zmenkarije ter ostale.

Pošiljanje sporočil s škodljivo vsebino ali povezave do le-te pa je kiber kriminalno dejanje. Sporočila vsebujejo škodljivo vsebino v obliki priponke (angl. *attachment*) ali pa povezavo do spletne strani, preko katere se na žrtvim računalnik namesti zlonamerno programje. Namen dejanja je najpogosteje prevzem oddaljenega nadzora in upravljanja računalnika in ga v naslednjem koraku uporabiti za izvedbo napada, kot je DDoS napad, krajo občutljivih podatkov, zakrivanje sledi itd.

Trg pošiljanja spam e-pošte oblikujeta ponudba in povpraševanje. Ponudniki storitve pošiljanja spam pošte računajo od 20 do 50 dolarjev za kampanijo, v kateri razpošljejo preko milijon sporočil (Madrigal, 2012). Do svoje smrti je Vardan Kushnir bil eden bolj znanih ponudnikov storitve pošiljanja spam sporočil. Internetne uporabnike je jezil s sporočili, kot so npr. "poceni seks" in drugo. Vardana so sicer pri njegovih 35 letih našli leta 2005 pretepenega do smrti. Smrt so preiskovali kot umor in obstaja verjetnost, da je smrt povezana s poslom pošiljanja spam sporočil. Vsaj uradno pa vzrok Kushnirjeve smrti ni bil dokazan (Leyden, 2016).

Trend pošiljanja nezaželenih sporočil preko zgodovine niha in je tesno povezan z dejanji razbijanja mrež kiber kriminalcev in zaprtjem oddaljenih C&C centrov. Takšen trend ugotavlja tudi Jaeson iz podjetja Cisco Systems, ki pa nadalje še ugotavlja, da se je v zadnjih nekaj letih količina nezaželene e-pošte na globalni ravni ponovno povečala (Schultz, 2016). Od sredine leta 2015 se je količina spam pošte poslane na globalni ravni občutno povečala in niha okoli 400 milijard poslanih spam sporočil dnevno.

Slika 8: Povprečno število dnevno poslane nezaželene pošte med leti 2014 in 2016



Vir: Global Spam Volume, 2016.

Zaradi naraščajoče problematike spam pošte je Evropska unija leta 2002 sprejela direktivo o zasebnosti in elektronskih komunikacijah, ki obravnava tudi pošiljanje nezaželene e-pošte. Direktivo so posamezne članice prenesle v svojo zakonodajo (ZEKom, 2007). Pristojen inšpektorat v Republiki Sloveniji za kršitve je tržni inšpektorat.

Z razvojem interneta in drugih modernih načinov komuniciranja so se razvile tudi druge poti za pošiljanje nezaželenih sporočil, kot sta npr. pošiljanje nezaželenih sporočil preko npr. socialnih omrežij, SMS sporočil in spletnih strani.

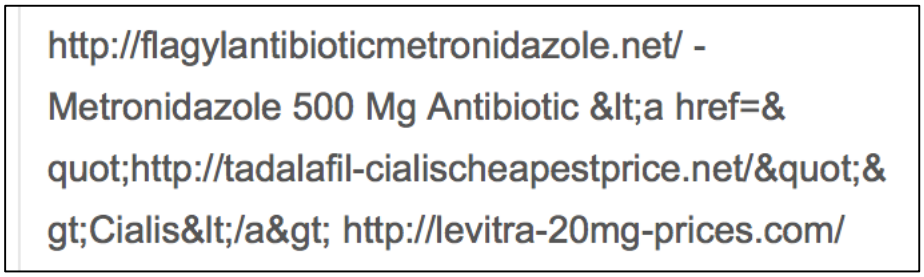
Sanford Wallace, ki se ga je prijel vzdevek "kralj spama", je med letoma 2008 in 2009 preko 500.000 zlorabljenih uporabniških računov na Facebooku poslal 27 milijonov spamerskih sporočil. S tem dejanjem se je Wallace tudi finančno okoristil, saj je prejemnike spam sporočil preusmeril na spletno stran in s tem na strani umetno povečal število obiskov. Tožilci so zanj zahtevali 16 let zaporna, a je v zaporu odsedel le dve leti in pol. Poleg tega, da je moral kazen prestati v zaporu, je moral še plačati visoko denarno kazen (Farivar, 2016).

Z razširjenostjo mobilne telefonije so se pojavila spam sporočila tudi na mobilnih telefonih. V večini primerov imajo ta sporočila reklamno vsebino ali pa gre za prevaro. Christensen (2016) navaja kot primer sms sporočila s prevaro vsebino, ki prejemnika sporočila obvesti, da je prejel plačilo preko PayPal sistema. Podrobne informacije o prejetem plačilu pa si prejemnik lahko ogleda s klikom na povezavo v sporočilu. Povezava ne vodi do prave Pay Pal spletne strani, temveč vodi do spletne strani, ki se pretvarja, da je

prava PayPal stran. Preko prevarantske spletne strani želijo kiber kriminalci pridobiti osebne podatke žrtve ter podatke o kreditni kartici.

Novejša tehnika spam sporočil so spam sporočila, ki se pojavljajo v komentarjih spletnih blogov in spletnih forumov. Takšna spam sporočila tipično nimajo veliko vsebine, vsebujejo pa povezavo do druge spletne strani (What Is Blog or Comment Spam and How Can I Fight It?, 2016). Kiber kriminalci v komentar zapišejo vsebino do tretje spletne strani z namenom, da obiskovalce foruma ali bloga napeljejo, da to spletno stran obiščejo. Na ta način umetno ustvarjajo promet na tretji spletni strani, s čimer se finančno nelegalno okoriščajo. Kiber kriminalci za objavo spam sporočil na blogih in forumih uporabljajo avtomatizirana orodja, ki izkoristijo slabo zaščitene, napačno skonfigurirane in neposodobljene sisteme za upravljanje z vsebinami. Primer spam sporočila, ki so ga kiber kriminalci skušali objaviti na blogu blog.meraki.si.

Slika 9: Primer spam sporočila v blogu



6.4 Socialni inženiring

Malcolm (2007, str. 4) socialni inženiring opredeli kot umetnost in znanost prepričati ljudi, da storijo tisto, kar ste si zaželeli.

Eden bolj poznanih primerov uspešne ukane preko socialnega inženiringa v zgodovini je primer trojanskega konja v času trojanske vojne. Ker Grki niso uspeli s silo vdreti v mesto Troja, so za dosego cilja uporabili tehnike socialnega inženiringa.

Uspešnost napada preko socialnega inženiringa je odvisna od priprave na samo dejanje napada. Pri postopku zbiranja informacij za pripravo napada Malcolm (2007, str. 6) navaja kot pogoste tehnike naslednje: pogled preko rame (npr. pridobitev PIN številke, ko jo žrtev vnaša v terminal), raziskovanje smeti (angl. *dumpster diving*), zbiranje informacij preko anketnih e-sporočil, ki obljubljajo npr. nagrado za izpolnjen vprašalnik (angl. *mail-outs*) in forenzična analiza (npr. starega računalnika, mobilnega telefona itd).

Načina za uspešno zaščito pred napadom izvedenim preko socialnega inženiringa ni. Človeškega faktorja ne bomo mogli odpraviti, saj na vsakega posameznika drugače

vplivajo kulturni, politični, ekonomski ali družbeni dejavniki. Lahko pa pomočjo uvedbe kontrol zmanjšamo tveganja, ki so povezana s socialnem inženiringom. Cisco priporoča naslednji pristop (Protect Against Social Engineering, 2016):

- Ustvarjanje varnostno zavedajoče se kulture, pri čemer mora podpora prihajati od vodstva navzdol.
- Izvajanje treningov za varnostno osveščanje.
- Uvedba varonstnih politik in procedur, kot so npr. upravljanje gesel, dvonivojska avtentikacija, fizična varnosti in druge.

Cilj uvedbe kontrol je, da posameznike usposobimo, da bodo znali v kritičnem trenutku razpoznati znake napada preko socialnega inženiringa in dejanje preprečiti.

Predstavil bom primer uspešno izvedenega kiber kriminalnega dejanja izvedenega v Sloveniji v letu 2012, pri katerem so kiber kriminalci uspešno vdrli v računalniški sistem Luke Koper. V koraku priprave na napad so pridobili informacije, katero podjetje vzdržuje IT okolje v Luki Koper. Nato so preko elektronskih sporočil in telefona kontaktirali z uslužbenci Luke Koper, ki so uporabljali elektronsko bančništvo. Lažno so se predstavili kot predstavniki podjetja, ki je vzdrežvalno računalniško okolje. S tem so izvršili prvo kriminalno dejanje – krajo identitete. Nato so uslužbence Luke Koper prepričali, da so na računalnike namestili zlonamerno programje, s pomočjo katerega so kiber kriminalcem omogočili dostop do informacijskega sistema, torej tudi do elektronskega bančništva. Nepooblaščeno so si prilastili več kot 100.000 eurov (Hekerji vdrli tudi v Luko Koper, 2016).

Schneier (2000, str. 266) v knjigi Skrivnosti in laži opisuje primer hekerja Anthonya Zboralskega iz Francije, ki je leta 1994 poklical v pisarno ameriške obveščevalne agencije (angl. *Federal Bureau of Investigation*; v nadaljevanju FBI) v Washingtonu in se predstavil kot FBI predstavnik zaposlen v ameriški ambasadi v Parizu. Uslužbenec FBI je Anthonyju posredoval podatke, kako se poveže v FBI telefonski konferenčni sistem. FBI je nato v obdobju sedmih mesecev naredil za 250.000 dolarjev škode.

6.5 Napadi na strateško in industrijsko infrastrukturo

Strateška infrastruktura zajema osnovna sredstva, ki jih uporablja prebivalstvo ali so namenjena za korist prebivalstva. Delimo jih na (Canada Strategic Infrastructure Fund Act; 2016):

- avtocestno ali železniško infrastrukturo,
- lokalno transportno infrastrukturo,
- turistično ali mestno razvojno infrastrukturo,

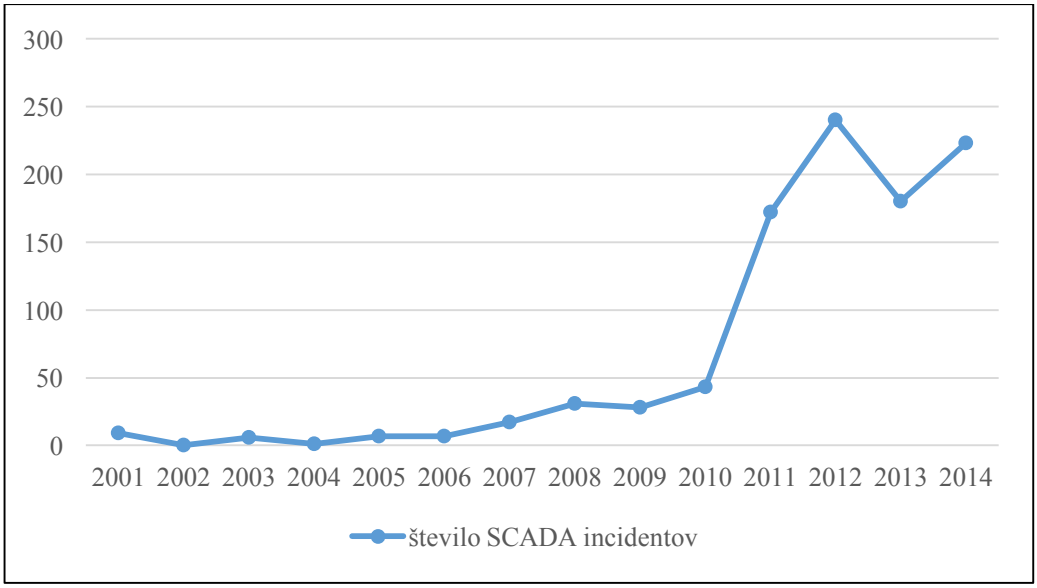
- komunalno infrastrukturo,
- elektro infrastrukturo,
- vodno infrastrukturo ali
- infrastrukturo, ki je predpisana z regulativo.

Posledice izpada ali motnje v delovanju strateške infrastrukture imajo večje ekonomske razsežnosti in negativno vplivajo na strateške cilje države, ogrožajo pa lahko tudi človekovo zdravje in življenje.

Upravljanje krmilnih enot v elektro in energetski industriji, upravljanje pametnih mest, upravljanje vodovodnih omrežij ter mnoge druge panoge na področju strateške infrastrukture uporabljajo sisteme, namenjne nadzorovanju in krmiljenju tehnološkega procesa z računalnikom (angl. *supervisory, control and data acquisition;* v nadaljevanju SCADA). Pri načrtovanju prvih SCADA sistemov varnost sistema ni bila ena izmed prioritetnih nalog oz. lastnosti sistema, zato so se v preteklosti vršili številni napadi na SCADA sisteme. Z razvojem SCADA sistemov se je povečevalo tudi število vdorov v te sisteme. Podoben trend pričakujemo tudi v prihodnje (Cherdantsev et al. 2016, str. 2).

Številni uspešno izvedeni vdori v preteklosti, visoko tveganje in možne posledice z velikimi razsežnosti so sicer razvijalce SCADA sistemov prisilile, da je varnost SCADA sistemov eden prioritetnih ciljev pri načrtovanju in razvoju le-teh. Ker se sodobni SCADA sistemi močno povezujejo v tradicionalno IT okolje, se za zmanjševanje tveganj uporabljajo tudi varovalke in zaščite, ki so tipično poznane v IT okolju in neposredne povezave s SCADA sistemi nimajo (npr. VPN, požarne pregrade, IDS/IPS sistemi ...).

Slika 10: Število SCADA incidentov med leti 2001 in 2014



Vir: Resources for the Ethical SCADA Hacker, 2016.

Prvi zabeležen primer kiber kriminala na strateško infrastrukturo se je zgodil leta 1982, ko je bil izveden napad na transibirski plinovod, čigar posledica je bila eksplozija. Za napad so Rusi obtožili ZDA (Carr, 2016). Nekateri drugi viri sicer temo oporekajo in trdijo, da eksplozija ni bila posledica kiber kriminalnega dejanja, temveč je nastala kot posledica napake inženirja, ki je opravljal vzdrževalna dela na plinovodu (Carr, 2016).

V januarju 2003 se je črv uspešno razširil v nuklerarno eletrarno v Ohiu in za kar 5 ur onesposobil varnostni nadzorni sistem (Poulsen, 2016). Virus Sobig je onesposobil železniško signalizacijo na Floridi (Computer Virus Brings Down Train Signals, 2016). V obeh primerih vdora je bila uporabljeno standardno, ne posebej prilagojeno zlonamerno programje, kot je bilo npr. uporabljeno leta 2009 pri napadu na iranske jedrske centrifuge. In že samo standardna zlonamerno programje bi lahko imelo uničujoče posledice za tamkajšnje prebivalstvo.

Prelomnica v kiber kriminalnem svetu je leta 2009 postal Stuxnet, ki ga lahko označimo kot prvo orožje v kiber svetu (Zetter, 2016). Stuxnet je izjemno napredno zlonamerno programje, mnogo bolj dovršena, kot je bila do takrat ta poznana. Stuxnet se ni obnašal kot ostali virusi in črvi, katerih naloga je čim hitrejše širjenje, temveč se je prožil le v točno določeni kombinaciji strojne in programske opreme. Celo točno določena verzija programske opreme je bila pogoj, da se je Stuxnet izvršil. Sprožil se je namreč le v primeru, da je bila na računalniku nameščena točno določena Siemensova oprema za krmiljenje jedrskih centrifug, s katero je bil upravljan točno določen krmilnik. Ta kombinacija pa je ustrezala konfiguraciji, ki so jo uporabljali v iranskih jedrskih centrifugah. Škodljivost Stuxneta se ni kazala v uničevanju dokumentov, zbiranju bančnih podatkov ipd., temveč je Stuxnet opravljal točno določen namen: prikrito manipulacijo z opremo za upravljanje centrifug. Preko npr. uravnavanja pritiska je povročal okvare na opremi in prikrito upočasnjeval proces bogatenja urana. Tradicionalni malware temelji na izrabi ponavadi le ene še neznane ranljivosti (angl. *Zero day exploit*), Stuxnet pa je za širjenje uporabljal kar štiri še neznane ranljivosti v Microsoft Windows operacijskem sistemu (Matrosov, Rodoinov, Harley & Malcho, str. 7). Noben antivirusni program zato Stuxneta ni zaznal. Cilj avtorjev napada je bil najverjetneje povsem politično motiviran, saj je bil Iran v konfliktu z zahodnim svetom glede lastnega jedrskega programa. Kot avtorje Stuxneta večina virov navaja sodelovanje ZDA in Izraela na državni ravni, čeprav vsaj javno ni bil avtor nikoli identificiran.

Kot primer napada na SCADA sisteme v Evropi bom omenil vdor v nemško podjetje iz železarske panoge, ki se je kot tak začel odvijati s pomočjo socialnega inženiringa. Napadalci so pridobili uporabniška imena in gesla, s katerimi so kasneje vdrli v informacijski sistem in med drugim izvedli sabotažo na sistemu za upravljanje peči. Posledica sabotaže je bila, da peči niso mogli ugasniti, kar je povzročilo precejšnje motnje v celotnem sistemu in povzročilo veliko škode (Check Point 2015 security report, str. 24).

Z vidika razsežosti in medsebojne odvisnosti različnih organizacij, podjetji in državne infrastrukture je dober primer napad na vladne spletne strežnike v Kanadi v letu 2011. Tega samega po sebi niti ne bi uvrstil v poglavje napadov na strateško infrastrukturo. A prav zaradi obsega posledic, ki jih je imel napad, ga uvrščam v to poglavje. Kiber napad je povzročil, da so bile nekaj časa nedostopne spletne strani vladnih agencij in drugih nekaterih državnih institucij, saj so varnostni inženirji preventivno prekinili internetno povezavo do napadenih organizacij. Posledice so bile močno ohromljene ekonomske, poslovne, finančne, politične in celo socialne aktivnosti v celotni državi, saj podjetja niso mogla priti do potrebnih finančnih informacij, ki jih potrebuejo pri dnevnem poslovanju. Napad, ki sam po sebi ne bi imel večjih posrednih stroškov, je posredno na državni ravni povzročil precejšnjo finančno škodo (Mahon, 2015, str. 20). Motiv naj bi bil politično motiviran, in sicer naj bi Kitajska poskušala priti do zaupnih finančnih informacij kanadske vlade. Predstavnik Zunanjega ministrstva Kitajske Ma Zhaoxu se je odzval na obtožbe in povedal, da so te brez kakršnekoli podlage in da Kitajska ne stoji za napadom (Cyber-attack hits Canadian government computers, 2016).

Strateška infrastruktura pa ni nujno samo industrijska infrastruktura. Med strateško infrastukturo lahko štejemo tudi vojaško infrastrukturo, kot je npr. več milijard vredna protiraketna zaščita, ki jo gradi NATO. Posledice kibernetskega vdora v sistem za upravljanje protibalističnih raket bi lahko imele uničujoče posledice na svetovni ravni.

6.6 Ribarjenje

Ribarjenje (angl. *phising*) lahko uvrstimo v eno izmed tehnik socialnega inženiringa. Metode izvedbe kiber kriminalnega dejanja namreč temeljijo na pridobivanju zaupanja žrtve, da berejo avtentična sporočila, ki so jih jim poslale legitimne organizacije. Tehnike ribarjenja so se skozi čas razvijale in izpopolnjevale.

Prva znani primeri ribarjenja v kiber prostoru so bila izvedena konec prejšnjega stoletja, ko je imel ponudnik internetnih storitev America Online (v nadaljevanju AOL) v ZDA izrazit monopol. Kiber kriminalci so se izdajali kot uslužbenci AOL in pošiljali različnim uporabnikom AOL storitev e-pošto, v kateri so jih pozvali, da za potrebe potrditve uporabniškega računa upoponovno vnesejo podatke kreditnih kartic in druge osebne podatke (Rekouche, 2011, str. 2).

Najpogostejši cilj ribarjenja je bil skozi zgodovimo pridobivanje osebnih in zaupnih informacij preko e-pošte in spletnih strani (History of Phishing, 2016), pri čemer so bile v napadih največkrat posnemane spletne banke.

Prvi napadi ribarjenja so bili storjeni precej amatersko, besedilo je vsebovalo veliko slovničnih napak itd. Sčasoma so napadi postali vse inovativnejši, popolnejši in bolj

organizirani. Kiber kriminalci so se zato soočali predvsem z dvema problemoma (Ramzan, 2016):

- Kako oblikovati sporočila in spletne strani, da bodo izgledala čim bolj pristna. Kako zakriti povezave v sporočilih, da žrtev ne bo zaznala, da ne bo preusmerjena na legitimno stran.
- Kako zaobiti vse bolj napredne in učinkovite varnostne rešitve, ki zaznavanjo poneverjena elektronska sporočila in poneverjene spletne strani.

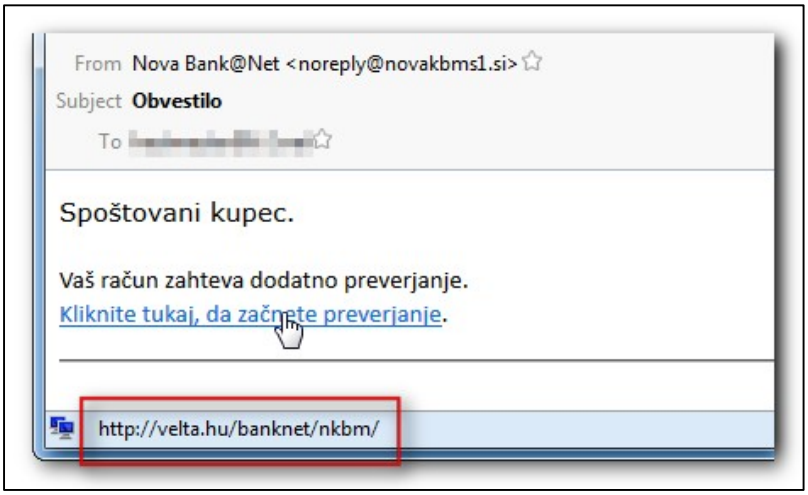
Grožnja, ki jo predstavlja uspešno izveden napad ribarjenja, je za podjetja in posameznike precejšnja. Posledica napada ribarjenja ima lahko velike neposredne stroške za žrtve napada, ki se pogosto odrazijo kot posledica odtujitev (večje) količine denarja. Kadar so žrtve ribarjenja zaposleni v podjetju, podjetju nastane škoda v obliki neposrednih stroškov in posledično najverjetneje tudi v obliki posrednih stroškov. Podjetja se, sicer takrat že prepozno, da bi kiber kriminalno dejanje preprečili, odločijo za uvedbo ustreze opreme za detekcijo napada ribarjenja, uvedbo dvofaktorske avtentikacije itd.

Zlonamerno programje, katerega namen je izvedba napada ribarjenja, je postalo dosegljivo širši množici oseb. Na črnem trgu kupite orodje za ribarjenje preko e-pošte ali najamete zlorabljen spletni strežnik, ki ga uporabite za ribarjenje preko spleta ipd. (History of Phishing, 2016).

V Sloveniji so bile tarča napada ribarjenja že številne banke. Eden večjih napadov ribarjenja se je zgodil v začetku leta 2015, ko je večje število oseb prejelo sporočila v svoj e-poštni nabiralnik, v katerih so jih poskusila preusmeti na lažna spletna mesta. Ta spletna mesta so posnemala obliko spletnih mest slovenskih bank, uporabnike pa so skušala prepričati, da v ustrezna polja vpišejo podatke za dostop do e-bančništva. Tarče napada so bili komitenti Nove ljubljanske banke, Nove kreditne banke Maribor (NKBM), Probanke, SKB banke, Probanke, Abanke in Unicredit banke.

Elektronska sporočila so bila napisana v slovenskem jeziku, bila so kratka in vsebovala so poziv uporabnikom, naj obiščejo spletno mesto banke. Slika 11 prikazuje dejanski primer ribarjenja, ki je bil usmerjen na slovensko banko Nova KBM.

Slika 11: Primer ribarjenja Nova KBM



Vir: Val phishing napadov na komitente slovenskih bank, 2016.

To sporočilo predstavlja sicer zelo slabo narejen primer sporočila ribarjenja že zaradi naslednjih dejstev: vsebinsko slabo oblikovano neprofesionalno sporočilo, "kupec" vas banka ne naslavlja, pošiljateljev e-naslov ne prihaja iz prave domene banke, povezava, ki je obkrožena z rdečo, pa vas vodi na spletno stran na madžarski domeni itd.

6.7 Politično motivirani napadi

Napadi organizirani ali motivirani s strani različnih vlad in držav niso dandanes nobena redkost. Številne države že imajo oblikovane (paravojaške) oddelke ali celotne organizacije, katerih primarni namen je bolj proti kiber terorizmu in kiber vojskovanju.

Sicer vsaj uradno praviloma ne obstaja neposredna vpletenost držav v tovrstne specializirane skupine, ki izvajajo politično motivirane kiber napade. A kljub temu za številne organizacije obstajajo dokazi in indici, da so ustanovljene ali vsaj financirane s strani posameznih držav. Skupini, ki sta tesno povezani z vladami v državah, sta gotovo "Iranian Cyber Army" in kitajska enota 61398. Kitajsko enoto povezujejo z napadom na npr. časnik New York Times (Hello, Unit 61398, 2016), iransko kiber vojsko pa povezujejo z npr. napadom na Twitter (Iranian cyber army' hits Twitter, 2016) in Baidu (Baidu hacked by 'Iranian cyber army', 2016) v letu 2009. Prav napad na Baidu pa se je razvil v pravo kiber vojno med skupinami v Iranu in na Kitajskem (Woollacott, 2016).

Enoto 61398 povezujejo tudi s serijo napadov na velikana Google v letu 2009 in začetku 2010. Mcafee je poimenoval te napade Operacija Avrora (Schmuger, 2016). Razsežnost napada je bila velika, saj je bilo napadenih kar 34 različnih podjetjih. ZDA se je formalno odzvala glede napada in zahtevala od Kitajske uradno pojasnilo. Nekaj dni kasneje je prišla na dan novica, da so vdrli v tiste uporabniške račune uporabnikov Gmaila, ki se borijo za

človekove pravice (Zetter, 2016). David W. Aucsmith je kasneje razkril, da so bili v napadu ciljani uporabniški računi, za katere so že predhodno imeli sodno odredbo za prisluškovanje in gre najverjetneje za protiobveščevalno dejanje (Schwartz, 2016a).

Leta 2011 so kiber kriminalci izvedli uspešen vdor v informacijski sistem overovitelja digitalnih potrdil DigiNotar. Vdor je omogočil dostop do 300.000 iranskih uporabniških računov Gmail storitve za kratek čas. Izraelski Mossad in ameriška CIA sta zapisala, da bi za napadom lahko stala iranska vlada (Iran authorities could be behind cyber attack against Mossad and CIA, experts say, 2016). Kakšne so bile posledice vdora, je težko oceniti, saj uradno ni bilo nikoli potrjeno, koliko podatkov iz zlorabljenih uporabniških računov je bilo dejansko odnešenih. Je pa imel dogodek pomembnejših vpliv za bankrota DigiNotarja kasneje v tem letu (Caldwell, 2014, str. 10).

Naprednega računalniškega trojanskega konja Gauss je Kaspersky Lab odkril v letu 2012 (Storm, 2016). Cilj Gaussa je kraja občutljivih bančnih podaktov. V prvih nekaj mesecih od odkritja Gaussa je bilo največ okužb zaznanih v Libanonu, skupaj v svetu pa jih je bilo zaznanih okoli 2.500 okužb. Kaspersky Lab je zaradi podobnosti med Gaussom, Flameom in Stuxnetom špekuliral, če morda Gaussa uporabljajo vlade za financiranje kiber vojskovanja, a naj bi bilo to malo verjetno (Gauss: Nation-state cyber-surveillance meets banking Trojan, 2016).

Veliko medijsko pozornost je požel vdor v IT okolje milanskega podjetja Hacking Team (Komu vse je Hacking Team dobavljal policijske trojance? 2016), ki se ukvarja z razvojem napredne programske opreme za izvajanje kiber napadov, kot so trojanski konji, korenski kompleti, roboti in druga programska oprema. Zaradi uspešnega vdora v informacijski sistem podjetja Hacking Team se je podjetja prijel vzdevek "Hacked team". Kiber kriminalci so objavili interne dokumente podjetja Hacking team, ki so med drugim vsebovali tudi različne poslovne skrivnosti ter izvorno kodo programske opreme. Analiza dokumentov je pokazala, da so bile stranke podjetja Hacking Team npr. policija in druge varnostno-obveščevalne službe tako iz razvitih držav (npr. ZDA in Avstralija) kot tudi iz držav tretjega sveta (npr. Sudan, Etiopija itd.). Republike Slovenije glede na vsebino javno objavljenih dokumentov ni bilo med državami, ki so kupile opremo podjetja Hacking Team. Uradni motiv za nakup tovrstne opreme držav je sicer preprečevanje in reševanje kiber kriminalnih dejanj. V številnih virih pa se postavlja vprašanje, da je motiv s strani različnih vlad za nakup te programske opreme v nadzoru novinarjev, aktivistov in političnnih nasprotnikov (Hack Back, 2016).

Trend nadzora in vpliva s strani države se le povečuje. Dogodki, kot so npr. teroristična dejanja, bodo vplivali na stopnjevanje povečevanja nadzora države nad prebivalci. To pa bo pomembno vplivalo na našo zasebnost (Schneier, 2016, str. 20).

6.8 Kraja kreditnih kartic in drugih finančnih sredstev

Kraja bančnih kartic, denarja, kreditnih kartic, podatkov za e-bančništvo in drugih finančnih sredstev so eni izmed najpogostejših ciljev kiber kriminalcev. Številno zlonamerno programje opravlja izključno en cilj: krajo zaupnih (finančnih) informacij, s katerimi si kasneje kriminalci protipravno prisvojijo denar žrtve kiber kriminalnega dejanja. Tehnike napadov kiber kriminalcev se neprestano razvijajo, tudi z razvojem in uvedbo novih bančnih e-poti.

Eno največjih botnet omrežij je bilo Mariprosa, v katerem je bilo v C&C center povezanih več kot 12 milijonov zlorabljenih osebnih, vladnih in univerzitethnih računalnikov (t. i. zombie računalnikov). Z združenimi močmi so španska policija Guardia Civil, FBI, podjetje Panda Security in Defense Inteligence leta 2010 uspešno ugasnila Mariprosa botnet omrežje. Sledile so aretacije v Španiji in drugod po svetu, pa tudi v Sloveniji in drugih državah bivše Jugoslavije (Botnet, 2016). Ocenjujejo, da so preko računalnikov, ki so tvorili Mariprosa botnet omrežje, naredili za kar 850 milijonov dolarjev škode (Cluley, 2016). Avtor programske kode je državljan Republike Slovenije z vzdevkom Iserdo. Modularno zasnovano škodljivo kodo za upravljanje računalnikov na daljavo je sprogramiral sprva za hobi. Kasneje je programsko kodo dopolnil še s funkcionalnostjo, da se ta samostjono širi iz okuženega računalnika na še neokužene računalnike. Za upravljanje botnet omrežja, ki je temeljil na tej programski kodi, je izdelal še enostaven uporabniški vmesnik. Ta je bil tako enostaven, da so ga lahko uprobljali tudi programiranja nevešči uporabniki. Na črnem trgu je izdelek prodajal med 500 in 2.000 ameriškimi dolarji (Botnet, 2016).

Z razvojem bančnih kartic nove generacije v zadnjih nekaj letih, ki za avtorizacijo majhnih zneskov ne potrebujejo več vpisa PIN kode, potrebna je le bližina kartice v območju POS terminala, je v porasti kraja manjših vsot denarja (angl. *petty crime*). Pri NLB lahko nakup do 15 eurov opravimo npr. povsem brez vnosa PIN kode (Brezstično plačevanje s plačilnimi karticami, 2016). V Angliji ocenjujejo, da so v letu 2015 oškodovali cca. 4.000 oseb, pri čemer je bilo odtujenih 19 milijonov funtov. Tipična žrtev, ki so si jo kiber kriminalci izbrali, je bila starejša ženska, stara več kot 80 let. Porast tovrstnih zlorab je še posebej izrazita od septembra 2015 dalje, ko so banke dvignile zgornjo meja zneska za brezstično plačevanje iz 20 na 30 funtov (Morley, 2016).

Leta 2012 je bil na hekerski konferenci Defcon v ZDA predstavljen primer, kako z uporabo pametnega telefona prekopirati kartico za brezstično plačevanje in s kopijo kartice nato plačevati v trgovinah. Postopek ni tehnično enostaven, a je bil dokazano izvedljiv (Greenberg, 2016).

V začetku leta 2016 je v javnost prišla novica o zlorabi globalnega finančnega sistema Society for Worldwide Interbank Financial Telecommunication (v nadaljevanju SWIFT).

SWIFT zagotavlja storitev medbančne izmenjave finančnih sporočil (naročil) na svetovni ravni (SWIFT Society for the Worldwide Interbank Financial Telecommunication, 2016). Vdor v sistem je bil skrbno načrtovan že vsaj leto dni nazaj, tako iz tehničnega vidika kot tudi z organizacijskega in postopkovnega vidika. V incidentu je bilo februarja 2016 Bangladeške centralne banke odtujenih kar 81 milijonov dolarjev, a so kasneje večino denarja nakazali nazaj na prvotne račune (Finkle, 2016).

Da pa kiber kriminalcev niso zanimive le valute različnih držav, temveč tudi digitalne valute, dokazujejo napadi na borze popularne digitalne valute Bitcoin. Konec leta 2014 in v začetku 2015 so odtujili 18.866 Bitcoinov iz borze Bitstamp, ki je sicer prva mednarodno priznana bitcoin borza (Higgins, 2016). Licenco ji je podelila Luxemburška vlada (Bitstamp to Become the First Nationally Licensed Bitcoin Exchange and Launches BTC/EUR Trading/, 2016). Napadalci so se napada lotili zelo temeljito, saj so dodobra preučili osebnosti posameznih ključnih oseb v Bitstampu in nato izvedli napad tudi s pomočjo socialnega inženiringa. Bitcoine so napadalci uspeli odtujiti takoj po novem letu 2015, ko so iz t. i. vroče denarnice (angl. *hot wallet*) odtujili bitcoine v protivrednosti cca. 5 milijonov ameriških dolarjev. Zaradi vdora borza Bitstamp nekaj dni ni delovala, saj so jo selili na novo opremo, primer pa je medtem raziskovalo več varnostnih strokovnjakov in uradni organi pregona. Zaradi zamenjave in nadgradnje varnostne in druge IT opreme pa so nastali tudi znatni posredni stroški.

6.9 (Porazdeljena) ohromitev storitve

Napade ohromitve storitve (angl. *Denial of Service*; v nadaljevanju DoS) je že v koncu osemdesetih let prejšnjega stoletja, ko je internetni klepet (angl. *Internet Relay Chat*) postajal vse bolj razširjeno orodje za druženje in komuniciranje, so uporabljali za izvajanje napada na posameznike, ki so prišli v konflikt s kom, ki je imel hitrejši dostop do interneta. Preko protokola za nadzor naprav Internet Control Message protokola (na kratko ICMP) so s poplavo (angl. *flood*) poslanih večjih paketov povsem zasičili žrtvino internetno povezavo, da je postala neuporabna za običajno delo. Ker je bila v tistem času bila velika večina uporabnikov povezanih preko počasnih modemskih povezav, le malo ljudi pa je imelo na voljo hitre širokopasovne povezave, je lahko že ena oseba iz samo svojega računalnika izvedla DoS napad.

Z razvojem interneta in kiber kriminala so napadi onemogočanja postali vse bolj učinkovitejši. Kiber kriminalci so postali vse naprednejši in uspešnost napadov ohromitve storitve so povečali tako, da so preko večje množice računalnikov napadli žrtve, kar predstavlja porazdeljen napad ohromitve storitve oz. DDoS. Za DDoS napade pogosto uporabijo računalnike povezane v botnet omrežja, kar jim hkrati pomaga tudi zakriti sledi, kje in kdo je izvor napada.

Motivi za DoS in DDoS napade so povsem različni, pri čemer bi izpostavil tri bolj pogoste:

- **Verski**. Primer je "Project Chanology", v katerem je skupina anonimni (anlg. *Anonimous*) izvedla DDoS napad na scientološko cerkev zaradi nestrinjanja s pogledi, kasneje pa so cerkev zasuli še s faks sporočili, telefonskimi klici itd. (Singel, 2016).
- **Politični**. Primer: oktobra 2015 se je zgodil DDoS napad na Tajske vladne spletne strani, za katerega špekulirajo, da je v ozadju izražanje nestrinjanje z nekaterimi vladnimi plani (Thai government websites hit by denial-of-service attack, 2016).
- **Ekonomski**. Primer: v začetku 2013 se je zgodil DDoS napad na strežnike start-up porjetje Noblego v Nemčiji, ki je popolnoma odrezal spletne strani in trgovine za 36 ur; sum za organizacijo napada je padel na konkurenco, ki ji je bil Noblego s popolnoma novim tržnim pristopom trn v peti (Weverbergh, 2016).

Razvoj orodij in pristopov za izvedbo DDoS napadov se je ves čas razvijal. Podjetje Imperva Incapsula je npr. v 2015 oporozilo na zaznan DDoS napad, ki je bil izveden iz botnet omrežja, v katerega niso bili vključeni računalniki, temveč so ga izvajale zlorabljene omrežne naprave – usmerjevalniki namenjeni za domačo uporabo in male pisarne (Gayer, Atias and Zeifman, 2016).

Orodja za izvedbo DDoS napadov so postajale vse bolj dostope širši, manj tehnično izobraženi populaciji. Na (črnem) trgu je možno že od nekaj deseet dolarjev in več najeti DDoS orodje kot storitev.

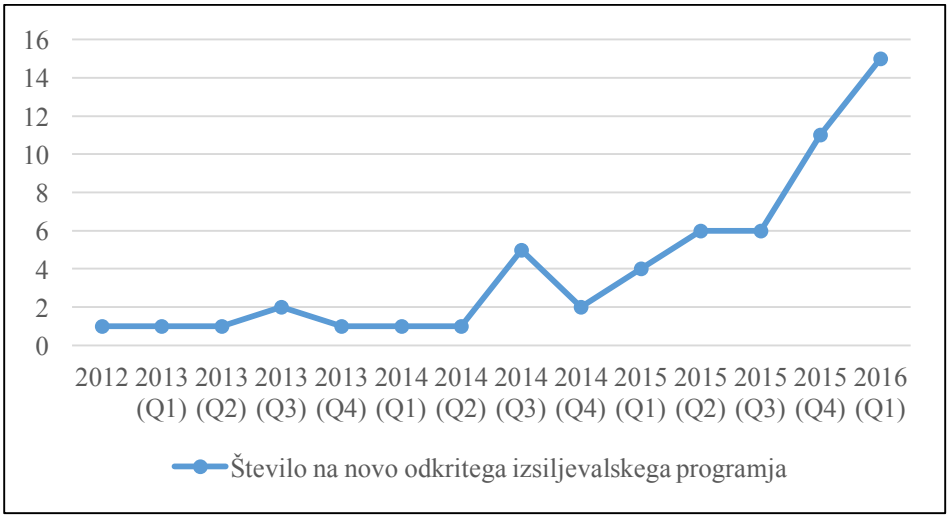
Primer ponudnika takšne storitve je organizacija Lizard Squad, ki je ponujala DDoS orodje v obliki programja kot storitve (angl. *software as a service - SaaS*). Za le nekaj deset dolarjev mesečno so ponujali najem orodja za izvedbo DDoS napada z imenom "stresser" (Parrish, 2016). Plačila so sprejemali preko bitcoinov. Ta vrsta plačila jim je zagotavlja nesledljivost pred uradnimi organi pregona. Nekateri drugi ponudniki DDoS storitve pa sprejemajo plačila tudi preko PayPal storitve.

Vsekakor pa je zanimiv pristop organizacije Lizzard Squad k marketingu. Da so promovirali DDoS storitev "Stresser", so uspešno napadli infrastrukturo podjetji Sony in Microsoft, ki omogočata spletno igranje igric preko njihovih konzol. In to ravno v času božiča, ko je bila igralna mrzlica na višku. Seveda je to povzročilo veliko negodovanja na strani uporabnikov (Turton, 2016).

6.10 Izsiljevalsko programje

Izsiljevalsko programje se je prvič pojavilo v letu 2005, ko je takrat trojanski konj GPcoder šifriral uporabniške datoteke in v zameno za plačilo od 100 do 200 ameriških dolarjev ponujal odklep šifriranih datotek (PGPCoder, 2016). Ker je bila zasnova PGPcoderja slabo narejena, je to omogočilo enostavno povračilo originalnih datotek brez plačila odkupnine.

Slika 12: Prikaz na novih odkritih oblik izsiljavalskega programja v letih 2012 do 2016



Vir: Internet Security Threat Report, 2016, str. 59.

Med leti 2013 in 2014 so prihajale nove vrste izsiljevalskega programja v dokaj počasi, v enem tromesečju je bilo zaznanih med 2 in 6 novih inačic. V zadnjem tromesečju leta 2015 je število novo odkritega izsiljevalskega programja začelo skokovito naraščati z rastjo med 150 in 200 % na posamezno tromesečje. Kako razširjeni so napadi z izsiljevalskim programjem lahko sklepamo iz ocene, da v Mehiki delež tovrstnih napadov predstavlja kar 80 % celotnega kiber kriminala, v Indiji pa je ta delež cca. 60 % (Cyber H., 2013, str. 1).

Cisco v letnem varnostnem poročilu za leto 2016 ocenjuje, da Angler, ki je eden bolj razširjenih primerov izsiljevalskega programja, letno kiber kriminalcem ustvari prihodek v višini preko 30 milijonov ameriških dolarjev (Cisco ASR 2016, str. 13).

Slika 13: Primer grožnje z izsiljevanjem, ki ga dobi uprorabnik

Vir: Ransomware: Cyber criminals have locked your computer but should you pay up, 2016.

Prve različice izsiljevalskega programja so se širile predvsem po domačih računalnikih. Žrtve so sicer bila tudi različne organizacije, pri čemer je bilo v napadu uporabljeno enako, ne posebej prilagojeno izsiljevalsko programje. V zadnjem letu je zaznati porast usmerjenih napadov na različne organizacije in podjetja, pri katerih je bilo izsiljevalsko programje prilagojeno.

Npr. februarja 2016 je delovanje bolnišnice v Los Angelesu ohromil uspešno izveden napad. Bolnišnične datoteke je izsiljevalsko programje zašifriralo in tako zdravnikom in drugemo bolnišničnemu osebju onemogočilo dostop do zdravstvenih datotek, rentgenskih slik, slik iz CT ter drugih dokumentov (Kadal & Kovacik, 2016). Kiber kriminalci so zahtevali plačilo 9.000 bitcoinov, kar je februarja 2016 znašalo cca. 3,4 milijone ameriških dolarjev. Posledica napada: premestitev bolnikov v drugo bolnišnico in plačilo odkupnine v višini 17.000 ameriških dolarjev (Mogg, 2016).

Pri razvoju izsiljevalskega programja so kiber kriminalci izpopolnili še dve pomembnejši tehniki: dodali so časovno komponento in dopolnili programsko kodo, da brez plačila odkupnine ni možno odšifrirati datotek.

- Časovna komponenta: z namenom, da žrtve čim preje plačajo odkupnino in se ne odločajo predolgo, kakšni so alternativni scenariji za pridobitev zašifrirane vsebine, izsiljevalsko programje opozarja uporabnika, da ima le-ta omejen čas (npr. 36 ur), da plača nižji znesek odkupnine. Po preteku tega časa se znesek odkupnine poveča (npr. podvoji).
- Koda sodobnega izsiljevalskega programja je precej bolj dovršena, praktično ne obstaja možnost, da bi lahko brez plačila odkupnine dešifrirali datoteke. To trditev potrdi tudi npr. FBI, ki pravi, da so nove različice CryptoWalla (ena od različic izsiljevalskega programja) tako dovršene, da vam praktično ne preostane drugega, kot da plačate odkupnino (Zorabedian, 2016b).

7 PRODAJA VARNOSTNIH REŠITEV PROIZVAJALCA ABC V PODJETJU RRC

Predstavil bom analizo prodaje varnostnih rešitev podjetja ABC, ki ga zastopa v Sloveniji distributer RRC BT d. o. o. (v nadaljevanju RRC), kjer sem zaposlen. ABC je fiktivno ime podjetja za namen diplomskega dela, saj točen naziv proizvajalca zaradi varovanja poslovnih skrivnosti v diplomskem delu ne navajam. ABC je svetovno uveljavljen proizvajalec rešitev na področju informacijskih tehnologij in omrežnih rešitev in kot tak eden vodilnih v tej panogi. Glede na različne raziskave, kot jih je objavil tudi npr. IDC, lahko povzamemo, da je imelo podjetje ABC v obdobju, za katerega sem naredil analizo podatkov, prevladujoč tržni delež na področju požarnih pregrad/navideznih privatnih omrežij, rešitev za enotno upravljanje groženj (angl. *unified threat management*), sistemih

za zaznavanje in preprečevanje vdorov in samostojnih rešitev za navidezna privatna omrežja.

Po dogovoru z delodajalcem in podjetjem ABC bom predstavil ugotovitve pridobljene z analizo prodaje izključno z vidika gibanja deležev v obdobju med leti 2005 in 2012. Podrobnejši (absolutni) podatki, ki sem jih pridobil v podjetju RRC, in novejši podatki so zaupne narave in poslovna skrivnost, zato jih v diplomskem delu ne bom navajal.

Metodologija, ki sem jo uporabil, je bila sledeča: iz ERP sistema podjetja RRC sem pridobil podatke o vseh prodanih artiklih proizvajalca ABC, vključno s prodajnimi cenami po posameznih strankah za celotno obdobje med 2005 do 2012. Vsaka vrstica v izvoženi XLS tabeli, ki sem jo pripravil s pomočjo posebej za ta namen lastno pripravljene SQL poizvedbe, je vsebovala naslednje podatke:

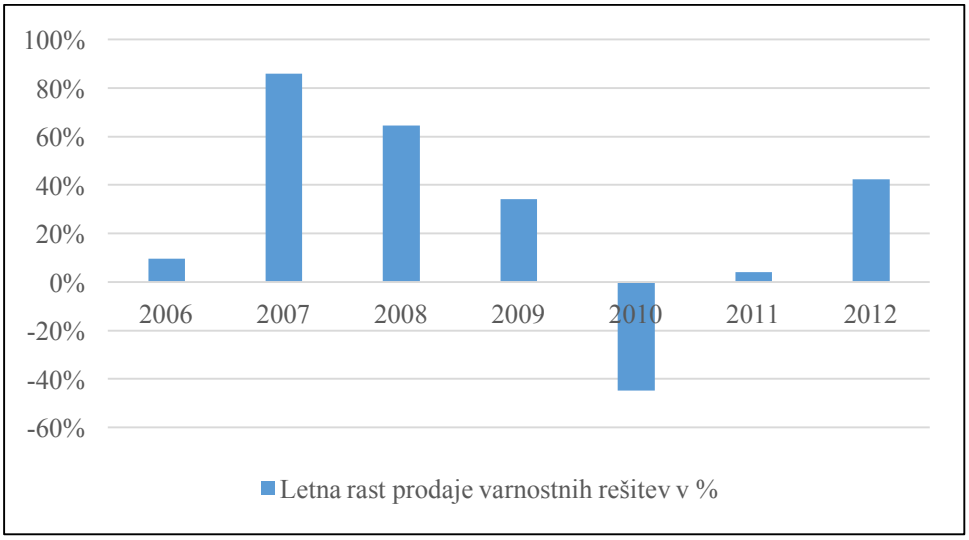
- kodo izdelka,
- datum prodaje izdelka,
- prodajno ceno na kos,
- prodano količino izdelkov in
- ime partnerja.

Glede na strukturo same baze ERP sistema sem moral SQL poizvedbo prilagoditi na način, da sem izključil vse knjižbe, ki so se nanašala na interna skladišča.

Eden večjih izzivov pri analizi podatkov je predstavljalo to, da v ERP sistemu, ki ga sicer podjetje RRC ne uporablja več, artikli niso bili opremljeni z atributom, v katero funkcionalno skupino spadajo. Namreč asortiman produktov proizvajalca ABC je izredno širok in vanj uvrščamo: rešitve za omrežja v podjetjih (tako za lokalna omrežja, prostrana omrežja kot tudi za brezžična omrežja in omrežja za ponudnike storitev), varnostne rešitve, rešitve za podatkovne centre, rešitve za sodelovanje ter mnoge druge. V Excelu sem moral tako spisati prilagojene funkcije, ki so glede na koren šifre posameznega izdelka opremile izdelek z informacijo, v katero funkcionalno skupino spada posamezni prodani izdelek. Le tako, ko sem imel podatek, ali sodi prodan izdelek v skupino varnostnih rešitev ali v katerokoli drugo skupino, sem lahko nadaljeval z analizo.

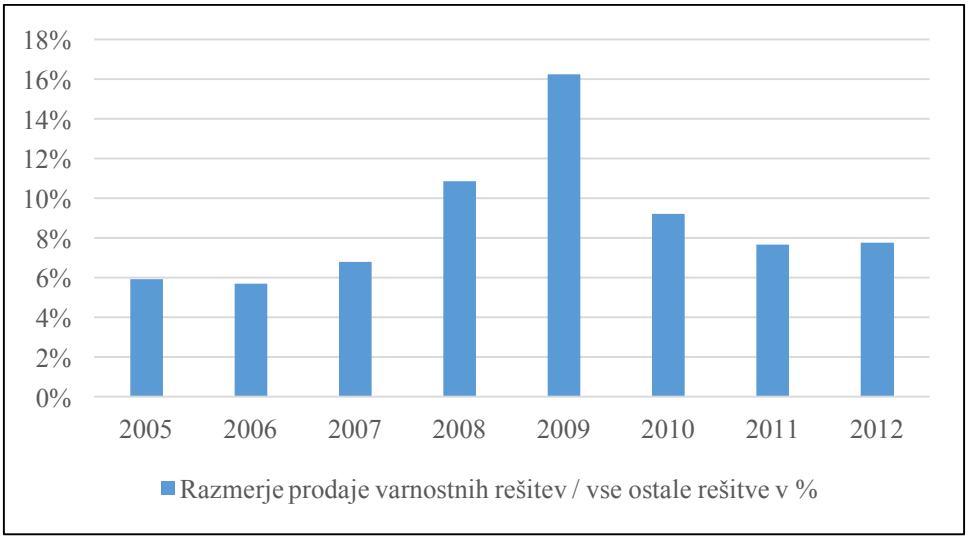
Podatki, ki so bili v ERP sistemu zabeleženi kot poslovni dogodek, ki se je zgodil pred 1. 1. 2008, so bili izraženi še v valuti slovenski tolar. Vrednost izraženo v tolarjih sem preračunal v evre tako, da sem uporabil menjalni tečaj določen z uredbo sveta ES (Zamenjava tolarjev v evre, 2016).

Slika 14: Rast prodaje varnostnih rešitev v Sloveniji med leti 2006 in 2012



Prodaja varnostnih rešitev v letu 2006 je bila točno takšna, kot bi jo opisali v učbeniku: za uspešen razvoj v podjetju je potrebna stalna rast prodaje ali dobička nekaj procentov letno. V letih 2007 in 2008 je rast prodaje glede na preteklo leto občutno poskočila. Sprva je bilo to kar malce presenetljivo, a ko sem iskal vzroke takne nepričakovane rasti, sem ugotovil, da je leta 2007 ABC prevzelo tehnološko zelo inovativno in v svetu priznano podjetje, ki se je specializirano ukvarjalo z razvojem rešitev za zaščito vsebine (angl. *content security*). Prav razširitev portfolija s produktoma za zaščito spletnega prometa in elektronske pošte je bistveno vplivala na skokovito rast prodaje varnostnih rešitev v podjetju RRC. V letu 2009 je bila rast prodaje varnostnih rešitev še vedno precej visoka, a je začela upadati glede na pretekli dve leti. Pozitivni dejavniki na rast prodaje varnostnih rešitev bi gotovo lahko pripisali tudi prevzemu novega podjetja v letu 2009, ki se je specializiralo tudi za razvoj rešitev za zaščito vsebine, ki pa se v celoti upravlja iz oblaka. Manjši negativni vpliv na rast oz. upad prodaje varnostih rešitev pa lahko pripišemo gotovo recesiji, ki je takrat že dosegla tudi Slovenijo. Prav globalna recesija je najverjetneje največji dejavnik za drastičen upad prodaje varnostnih rešitev v letu 2010. Gospodarstvo je v letu 2011 začelo počasi okrevati od prvega sunka recesije in v letu 2012 je bila ponovno zaznana rast prodaje varnostnih rešitev. ABC je proti koncu leta kupil še inovativno podjetje, ki je proizvajalo omrežne rešitve (stikala, varnostne naprave in brezžične dostopne točke), ki so v celoti upravljane preko oblaka. A prodaja varnostnih naprav tega podjetja ni imela vpliva na rast prodaje varnostnih rešitev ABC v RRC v letu 2012.

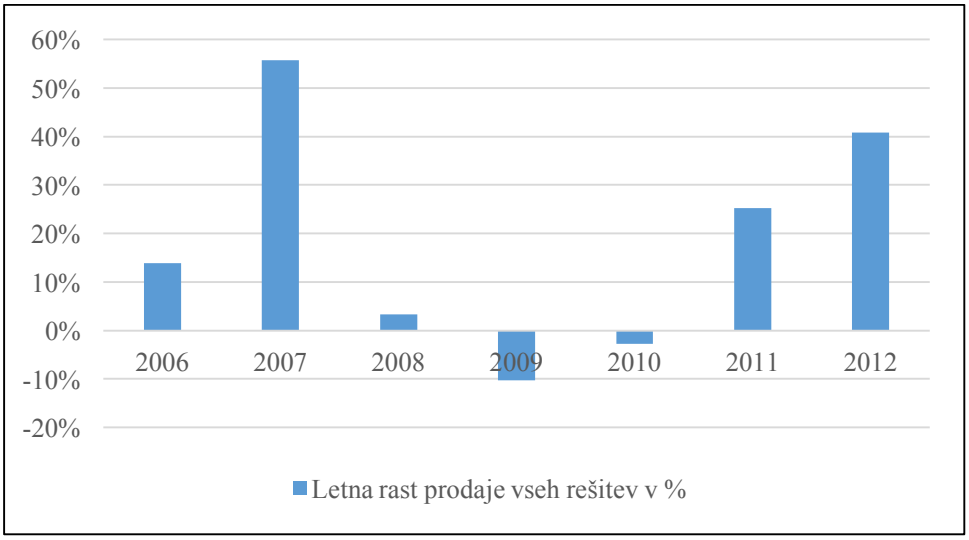
Slika 15: Prodaja varnostnih rešitev glede na ostale rešitve med leti 2005 in 2012



Iz grafa, ki prikazuje razmerje prodaje ABC varnostnih rešitev v podjetju RRC v primerjavi z vsemi ostalimi tehnologijami, ki jih ponuja ABC in jih je RRC. Analiza je narejena po posameznih letih v obdobju med 2005 in 2012. Ugotavljam, da je razmerje skozi vsa leta bilo približno enako in se je gibalo na višini 6 do 8 %. Zelo izstopajoči sta izjemi v letih 2008 in 2009, kar ne sovpada povsem z bistveno povečano rastjo prodaje varnostnih rešitev v letih 2007 in 2008, kar sem ugotovil v predhodni analizi. Ko sem poskusil najti vzrok tega nekako "porušenega" razmerja, ga nisem našel, vse do momenta, ko sem naredil naslednjo raziskavo, in sicer analizo rasti prodaje vseh ABC rešitev v podjetju RRC v enakem obravnavanem obdobju. Ali je globalna recesija vplivala na upad prodaje ostale opreme, pri čemer je to bilo vsaj v letu 2009 mnogo usodno za varnostne rešitve, ne morem potrditi.

Zadnji graf prikazuje rast oz. upad prodaje vseh rešitev proizvajalca ABC v podjetju RRC glede na preteklo leto za obdobja med leti 2005 do 2012. Tudi tokrat ugotavljam, da je bilo leto 2006 zelo stabilno. Leta 2007 je bilo izredno uspešno, saj je prodaja na letni ravni zrastla za več kot 50 %. Glede na to, da sem v predhodnih analizih odkril, da je razmerje prodanih varnostnih rešitev proizvajalca ABC tudi izredno poskočila v tem letu, a razmerje prodanih varnostnih in vseh ostalih rešitev je ostalo približno enako kot v drugih letih, ugotavljam, da je v letu 2007 močno poskočila tudi prodaja tudi drugih rešitev iz ABC portfelja. Leta 2008 je prodaja le malenkost narastla na letni ravni. V letih 2009 in 2010 pa se pozna vpliv mednarodne gospodarske krize. Kar pa ugotavljam, je to, kar je sicer morda kar malce pričakovano, da so podjetja zmanjšala oz. začasno odložila nenujne investicije. To se odrazi v rahlem padcu celoletnega prometa v tem letu. Kar pa je bolj skrb zbujajoče, pa je to, da so, kot kaže, zaradi gospodarske krize bila podjetja bolj zadržana pri investicijah v varnostne rešitve, saj so te v primerjavi s predhodnimi leti upadle bolj kot so upadle investicije v drugo vrsto opreme. Rezultati analize namreč prikazujejo ravno to.

Slika 16: Letna rast prodaje vseh varnostnih rešitev med leti 2006 in 2012



8 KAJ NAS ČAKA V PRIHODNJE

Napovedati, kaj se bo dogajalo v prihodnje, vsebuje vedno elemente negotovosti. V nadaljevanju poglavja bom tako na podlagi preteklih dogodkov, podatkov, ki sem jih poznal predno sem se lotil izdelave diplomske naloge in podatkov, ki sem jih pridobil v času izdelave diplomskega naloge, z določeno mero negotovosti napovedal, kaj se bo po mojem videnju dogajalo na področju kiber kriminala v prihodnjih letih.

Napadi na SCADA sisteme se bodo še povečevali, čeprav se zadnja leta varnostna problematika na tem področju izboljšuje. A ker imajo posledice uspešnih kiber napadov na tovrstne cilje lahko velike razsežnosti, tako ekonomske, medijske in tudi politične, menim, da se trend napadov ne bo zmanjšal.

Številne raziskave (npr. Cisco ASR 2016, str. 30), pa tudi analize omrežnega, ki sem jih opravil pri svojem delu, kažejo na to, da vedno več spletnega prometa poteka preko šifriranih povezav, pri čemer je protokol Hypertext Transfer Protocol (HTTP) šifriran z uporabo protokola Secure Sockets Layer (SSL) ali Transport Layer Security (TLS). Slednji je v zadnjem letu v velikem delu izrinil SSL, saj ima le ta številne znane pomanjkljivosti. Delež šifriranega spletnega prometa predstavlja tipično med 30 % in 70 % celotnega spletnega prometa, odvisno od posamezne organizacije.

Težava, ki jo šifrirane povezave predstavljajo varnostnim inženirjem, je ta, da varnostne rešitve brez dodatnega posega nimajo vpogleda v šifriran promet in posledično ne morejo preprečiti poskusa vdora, pregledati vsebine in ugotoviti skladnost le-te z varnostno politiko podjetja. Obstajajo sicer že tehnologije, ki omogočijo vpogled v šifirane povezave,

a pogosto obstajajo organizacijske ali pravne omejitve, da jih organizacije še ne uporabljajo.

Napovedujem, da bo delež šifriranih povezav v prihodnje še naraščal vse do splošne uvedbe nove različice protokola za izmenjavo hiperteksta ter grafičnih, zvočnih in drugih večpredstavnostnih vsebin na spletu verzije 2 (angl. *Hypertext Transfer Protocol Version 2)*, ko bodo povezave bile le še šifrirane.

Število napadov na zdravstvene institucije se bodo povečevalo. Posledice kiber napada na bolnišnico, kot se je že zgodil z uporabo izsiljevalskega programja, predstavljajo bolnišnicam visoko tveganje. To se odraža predvsem kot odtujitev in razkritju zaupnih in osebnih informacij, nerazpoložljivosti informacij, kot so npr. zdravstvene datoteke, brez katerih zdravljenje ljudi ni možno, medijski in politični pritisk ipd.

Napadi na storitve v oblaku se bodo stopnjevali tako v kvalitativnem kot tudi v kvantitativnem smislu. Trend v IT je namreč, da se vse več storitev podjetij seli iz lastnih podatkovih centrov v oblačno računalništvo, kiber kriminalci pa kot tarče tipično izbirajo storitve in naprave, kjer je večje število naprav, podatkov in uporabnikov. Vzporednico bi gotovo lahko poiskali pri razvoju malwarea: dokler je imel Microsoft Windows operacijski sistem močno prevladujoč delež med operacijskimi sistemi nameščenih na računalnikih, je večina malwarea izkoriščala ranljivosti prav v teh sistemih. Ko pa je npr. Applov operacijski sistem Mac OS X začel pridobivati tržni delež na tem področju, je tudi bilo zaznati porast v številu malwarea, usmerjenega v zlorabo ranljivosti v Mac OS X operacijskem sistemu.

Število DDoS napadov se bo še povečalo. Samo v zadnjih dveh letih se je število teh napadov povečalo za kar 62 %. Število DDoS napadov že danes predstavlja eno najpogostejših oblik kiber kriminalnih dejanj. Napovedujem, da še predvsem zaradi tveganja, ki ga predstavlja ohromitev poslovanja zaradi DDoS napada, bo tovrstna oblika kiber kriminala bila pogosto uporabljena tudi v prihodnje.

Izsiljevanja s pomočjo izsiljevalskega programja strmo naraščajo. Glede na donosnost te vrste kiber kriminala z ekonomskega vidika, kot sem to predstavil v diplomskem delu na primeru Angler-ja, glede na to, se bo trend teh napadov naslednjih nekaj let le še stopnjeval. Prepričan sem, da bo v porastu tudi delež specializirano usmerjenih kiber napadov z izsiljevalskim programjem na zdravstvene in finančne institucije ter strateško infrastrukturo.

Kiber napadi na manjša in srednja velika podjetja se bodo stopnjevala. Tovrstna podjetja imajo manj sredstev na letni ravni kot velika podjetja, ki jih namenjajo za varnost IT. Zaradi tega so bolj ranljivi v kiber prostoru in bolj pritegnejo kiber kriminalce, katerim je cilj, da si prisvojijo denarna sredstva.

Porast napadov in škodljive kode na mobilnih napravah, še predvsem na Android platfomi. Zakaj? Kot prvi razlog bi navedel dejstvo, da se število vseh mobilnih naprav na globalni ravni še vedno povečuje, Android pa na trgu mobilnih naprav obenem pridobiva tržni delež. Kot drugi pomembni razlog pa bi izpostavil dejstvo, da je Android platforma prisotna na napravah številnih proizvajalcev, pri čemer le peščica teh skrbi za dolgoročno podporo za programsko opremo in varnostne popravke na svojih napravah. Iz tega sledi, da imajo Android uporabniki pogosto uporabljajo zastarelo programsko opremo, ki vsebuje poleg neznanih tudi znane ranljivosti.

Internet stvari (angl. *Internet of Things;* v nadaljevanju IoT) je eno najhitreje rastočih področij. V današnjem času je vedno več naprav poveznanih v internet, kot so npr. kamere, otroške igrače, avtomobili, hladilniki in mnoge druge. V raziskavi Deloitte ocenjuje, da je bilo v letu 2015 v internet povezanih že več kot 2,8 milijard IoT naprav (Lee, Stewart, Culgar-Pop, 2015, str. 6). Eden pomembnejših dejavnikov rasti število napadov na IoT področju bo v prihodnje razlog, da razvijalci varnostni pri razvoju IoT naprav ne posvetijo dovolj časa in sredstev, temveč se osredotočajo predvsem na cilje, kot so uporabnost ter hiter razvoj in plasiranje na trg. Drugi dejavnik, ki bo vplival na porast napadov, pa je to, da nekatere IoT naprave upravljanjo oz. dostopajo do velike količine podatkov, ki so zanimive za kiber kriminalce. Posledice napadov na IoT naprave bodo morda neškodljive, kot če bi npr. sosed za zabave ponagajal sosedu in mu odpeljal avto iz garaže, kar bi mu npr. omogočilo šibko nastavljeno geslo za brezžično povezavo do avtomobila. Posledice kiber kriminalnih dejanj na IoT naprave bodo imele seveda materialno ali ekonomsko škodo, morda bodo celo ogrozila človeška življenja. Bomo morda že kmalu doživeli napad in prevzem upravljanja na vlak ali letalo?

Večje število kazni in višje kazni bodo za podjetja, ki ne bodo ustrezno zavarovala osebnih in drugih podatkov, saj se tudi na nivoju Evropske unije odvijajo spremembe zakonodaje na področju odgovornosti in nalog. Ena od direktiv, ki bo pomembno prispevala k temu, je direktiva o varovanju informacij in omrežij ter zasebnosti podatkov.

Kiber kriminalci bodo še naprej izpopolnjevali tehnike napadov in povezovali v organizirane kiber kriminalne združbe. Malware se bo še izpopolnjeval. Organi pregona bodo vse težje odkrili preganjali kiber kriminalce, saj bodo ti bolj previdni in bodo izpopolnjevali tehnike za zakrivanja sledi.

Zlonamerno oglaševanje (angl. *malvertising*) je tehnika za razširjanje malwarea preko spletnih oglasov, ki se je začel širita v zadnjih nekaj mesecih. Ker je oglaševanje na internetnih straneh že vrsto let zelo razširjeno in uspešno tržno orodje, pri čemer je oglaševanje edini ali pa najpomembnejši del financiranja za številne spletne strani, bo to gotovo vplivalo na to, da se bo stopnjevala rast zlonamernega oglaševanja.

Manjša in srednje velika podjetja bodo predvsem zaradi bolj omejenih finančnih in drugih sredstev zaščito pred kiber napadi prepustila v upravljanje podjetjem specializiranim na tem področju. Ocenjujem, da se bodo zaradi tega oblikovala podjetja, ki bodo strankam nudila storitev varnostni IT kot storitve.

SKLEP

Skozi diplomsko nalogo sem predstavil, kakšna so bila prva kiber kriminala dejanja in kako se je ta razvijal skozi zgodovino vse do danes. Ugotovil sem, da je kiber kriminal med nami prisoten že nekaj desetletij. Kar nekaj metod kiber kriminalcev, ki jih danes uporabljajo v kiber prostoru, izvirajo iz tradicionalnega kriminala, ki je ohranil metode in se preselil v digitalni svet. Vzporednice med kiber in tradicionalnim kriminalom lahko potegnemo še iz časa antičnih Grkov, srednjega veka in tudi novejše zgodovine. Ugotavljam, da se je področje kiber kriminala skozi zgodovino spreminjalo predvsem na sledečih področjih:

- Kiber kriminalci so postajali vse bolj organizirani, oblikovale so se kriminalne organizacije, ki delujejo v kiber prostoru.
- Malware je postajo vse naprednejši, hkrati pa tudi dostopnejši širši množici posameznikov, saj ni več na voljo le zelo omejenem številu posameznikov na črnem trgu. Uporaba malwarea je postala enostavnejša, prilagojena za uporabo tudi manj tehnično veščim uporabnikov.
- Kiber napadi postajajo vse pogostješi, vse težje jih je zaznati, njihovi vplivi in posledice pa so vedno večji.
- Problema kiber kriminala se zaveda vse več majhnih in velikih podjetij, a se pogosto ukrepi za zaščito in obrambo pred kiber napadi ne nahajajo na dovolj visokem mestu na lestvici prioritet podjetij, da bi bila zaščita bolj učinkovita in število uspešnih napadov manjše.
- Tudi glede na raziskavo, ki sem jo opravil glede na gibanje prodaje varnostnih rešitev podjetja ABC v Sloveniji, pridem do enakih zaključkov: kiber varnost še ni ena izmed višje uvrščenih prioritet.
- Države se zavedajo naraščajočega problema kiber kriminala in vedo, da brez strateškega pristopa in povezanosti vseh vpletenih boj proti kiber kriminalu ne bo bil uspešen. Zaradi tega se oblikuje na evropski in državni ravni strategija za boj proti kiber kriminalu.

Za zaključek bi predlagal nekaj priporočil, kako se lahko podjetja zaščitijo in omejijo tveganja pri kiber napadih:

- Zloraba privilegijev je še vedno eden bolj pogosto uporabljenih načinov za izvedbo vdorov. Organizacije morajo slediti principu najmanjšega privilegija (angl. *least*

privilege). Močna gesla, dvofaktorska avtentikacija uporabnika morajo biti zajeta v varnostni politiki.

- Plan neprekinjenega poslovanja je eden ključnih dejavnikov za zaščito pred kiber napadom in omejevanju posledic škode, ki nastane po kiber kriminalnem dejanju.
- Arhiviranje podatkov mora biti skrbno načrtovano glede na opravljeno analizo tveganj in analizo vpliva na poslovanje. Mariskateremu podjetju, tudi v Sloveniji, bi dobro načrtovan in tudi izvajan postopek arhiviranja podatkov omejil škodo, ki je nastala z vdorom izsiljevalskega programja v njihovo informacijsko okolje.
- Izobraževanje in osveščanje zaposlenih na področju kiber varnosti mora biti oblikovano kot trajen proces in ne kot enkratno dejanje.
- Organizirana trajna grožnja (angl. *advanced persistent threat*), katera po raziskavah v naslednjih 6 mesecih ne bo prizanesla 71 % anketirancev (Eddy, 2015, str. 1), bo velik problem tudi v prihodnje. Proizvajalci varnostnih rešitev skušajo čim bolj ažurno slediti tovrstnim grožnjam pri izdelavi učinkovitih varnostnih rešitev. Priporočljivo je redno spremljati razvoj in različne pristope rešitev proizvajalcev varnostnih rešitev.
- Redne posodobitve programske opreme, še predvsem z varnostnimi popravki, so nuja. Kljub številnim uspešnim vdorom na račun uporabe zastarele programske opreme še vedno preveč organizacij ne izvaja tovrstnih posodobitev. Posodabljanje programske opreme z namenom odprave ranljivosti v tej je namreč eden izmed najcenejši in bolj učinkovitih načinov za vzdrževanje varne infrastukture. Proizvajalci programske opreme namreč največkrat izdajajo varnostne popravke povsem brezplačno.
- Uporaba, upravljanje in nameščanje neodobrene programske opreme na računalnikih naj bo v podjetjih omejena oz. prepovedana. Zaposleni z uporabo poljubne, neodobrene programske opreme s strani podjetja in s (prekomernim) brskanjem po internetu predstavljajo varnostno tveganje za podjetje in tako ogrožajo sredstva IT, podatke in integriteto podjetja kot celoto. V praksi se je tudi izkazalo, da uporaba neavtorizirane s strani podjetja programske opreme pogosto vodi hkrati tudi v uporabo nelicenčne programske opreme. To še dodatno poveča tveganje podjetja, da to ne bo poslovalo skladno z veljavno zakonodajo oz. bo s tem storjeno kaznivo dejanje.
- Prinesite svojo napravo (angl. *Bring Your Own Device*) je pristop, ki je prisoten v večini podjetij. Podjetja naj tehnično in organizacijsko podprejo ta pristop, da bodo imela možnost upravljati in nadzorovati pretok in hrambo informacij.
- Tradicionalni sistemi za zaščito pred vdori, antivirusni programi in druga varnostna oprema ni postala nepotrebna in neučinkovita. Kljub spreminjanju tehnik kiber kriminalcev, uporabe novih orodij za izvedbo napadov, iskanje novih vrst ranljivosti itd. ta orodja še vedno pomembno vplivajo na kiber varnost. Vzporednico bi lahko potegnili s cepivi pri ljudeh: davica in podobne bolezni se v razvitem svetu praktično ne pojavljalo več. A z ukinitvijo obveznih cepiv proti tem boleznim bi močno povečali tveganje, da bi se te bolezni ponovno razširile v razvitem svetu.

Ključnega pomena za vsako organizacijo pa je, da se ta zaveda, da za uspešno zaščito proti kiber napadom ne bo zadostovala le ena rešitev, ki jo bodo kupili v trgovini (angl. *of the*

shelf). Potrebna je temeljita analiza, priprava lastne strategije, zagotovitev finančnih in drugih sredstev ter zadostna razpoložljivost človeškega kadra, da bo boj proti naraščajočemu kiber kriminalu učinkovit.

LITERATURA IN VIRI

1. *2012 Cyber Attacks Timeline Master Index*. Najdeno 6. septembra na spletnem naslovu http://www.hackmageddon.com/2012-cyber-attacks-timeline-master-index/
2. Abliz, M. (2011, Marec). Internet Denial of Service Attacks and Defense Mechanisms. *University of Pittsburgh Technical Report*, 1-50.
3. *About ENISA*. Najdeno 6. Maja 2016 na spletnem naslovu: https://www.enisa.europa.eu/about-enisa
4. Agnihotri, M. (2015, 12. oktober). *5 True Stories That Prove You Shouldn't Piss Off The IT Guy*. Najdeno 18. maja 2016 na spletnem naslovu https://www.linkedin.com/pulse/5-true-stories-prove-you-shouldnt-piss-off-guy-mayur-agnihotri?redirectFromSplash=true
5. Alen, M. (2006). *Social Engineering: A Means To Violate A Computer System*, SANS institute.
6. Arthur, C. (2010, 3. marec). *Alleged controllers of 'Mariposa' botnet arrested in Spain*. Najdeno 6. septembra 2016 na spletnem naslovu https://www.theguardian.com/technology/2010/mar/03/mariposa-botnet-spain
7. *Baidu hacked by 'Iranian cyber army'*. Najdeno 14. maja 2016 na spletnem naslovu http://news.bbc.co.uk/2/hi/8453718.stm
8. Beal, V. (b.l.). *DDoS attack - Distributed Denial of Service*. Najdeno 2. junija 2016 na spletnem naslovu http://www.webopedia.com/TERM/D/DDoS_attack.html
9. Bergen, J. (2011, 23. junij). *Baltimore IT guy sentenced for hacking boss's PowerPoint with porn*. Najdeno 1. junija 2016 na spletnem naslovu http://www.geek.com/news/baltimore-it-guy-sentenced-for-hacking-bosss-powerpoint-with-porn-1394821/
10. *Bitstamp to Become the First Nationally Licensed Bitcoin Exchange and Launches BTC/EUR Trading*. Najdeno 22. maja 2016 na spletnem naslovu https://www.bitstamp.net/article/bitstamp-first-nationally-licensed-btc-exchange/
11. *Brezstično plačevanje s plačilnimi karticami*. Najdeno 20. maja 2016 na spletnem naslovu https://www.nlb.si/brezsticno
12. Cabinet Office (2011, november). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. London: Crown copyright.
13. Caldwell, T. (2014, junij). The true cost of being hacked. *Computer Fraud & Security*. Najdeno 14. julija 2016 na spletnem naslovu http://www.sciencedirect.com/science/journal/13613723/2014/6
14. *Canada Strategic Infrastructure Fund Act*. Najdeno 14. junija 2016 na spletnem naslovu http://laws-lois.justice.gc.ca/eng/acts/c-10.3/fulltext.html
15. Carr, J. (2012, 7. junij). *The Myth of the CIA and the Trans-Siberian Pipeline Explosion*. Najdeno 6. septembra 2016 na spletnem naslovu http://jeffreycarr.blogspot.si/2012/06/myth-of-cia-and-trans-siberian-pipeline.html
16. Check Point (2015, 16. junij). *Check Point 2015 security report*. Najdeno 5. avgusta 2016 na spletnem naslovu http://blog.checkpoint.com/2015/06/16/check-

point-2015-security-report-paints-a-picture-of-the-threat-landscape-and-its-not-pretty/
17. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016, februar). A review of cyber security risk assessment methods for SCADA systems. *Computers & security (56)*, 1–27.
18. Christensen, B. (2016, 20. april). *'You've Just Sent a Payment' PayPal SMS Phishing Scam*. Najdeno 15. junija 2016 na spletnem naslovu http://www.hoax-slayer.net/youve-just-sent-a-payment-paypal-sms-phishing-scam/
19. Cisco Systems, Inc. (2016, Januar). *Cisco 2016 Annual Security Report.* San Jose: Cisco Systems, Inc.
20. Clanch, C. (2004). Management Update: Best Practices in Business Continuity and Disaster Recovery. *Gartner Research*.
21. Cluley, G. (2011, 26. april). *Memories of the Chernobyl virus*. Najdeno 6. septembra 2016 na spletnem naslovu https://nakedsecurity.sophos.com/2011/04/26/memories-of-the-chernobyl-virus/
22. Cluley, G. (2012, 13. december). *Suspected gang behind the $850 million Butterfly botnet arrested*. Najdeno 15. maja 2016 na spletnem naslovu https://nakedsecurity.sophos.com/2012/12/13/butterfly-botnet-arrests/
23. Cohen, F. (1986). *Computer Viruses* (Phd dissertation). Faculty of the Graduate School, University of Southern California.
24. Coleman, K. (2003, 11. oktober). Cyber Terrorism. *Directions Magazine*. Najdeno 5. junij 2016 na spletnem naslovu http://www.directionsmag.com/entry/cyber-terrorism/123840
25. *Computer Virus Brings Down Train Signals*. Najdeno 1. junija 2016 na spletnem naslovu http://www.informationweek.com/computer-virus-brings-down-train-signals/d/d-id/1020446?
26. *Computer Virus Timeline*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.infoplease.com/ipa/A0872842.html
27. Condon, R. (2009, 20. november). *Conficker worm update: How does Conficker spread?* Najdeno 6. septembra 2016 na spletnem naslovu http://www.computerweekly.com/news/1375088/Conficker-worm-update-How-does-Conficker-spread
28. Conmy, S. (2014, 3. april). *Cybercrime costs Irish economy €630m a year*. Najdeno 1. julija 2016 na spletnem naslovu http://www.digitaltimes.ie/cybercrime-costs-irish-economy-e630m-a-year/
29. *Continuity Central*. Najdeno 30. aprila 2016 na spletnem naslovu http://www.continuitycentral.com/
30. *Crimeware: Bots*. Najdeno 26. maja 2016 na spletnem naslovu http://us.norton.com/cybercrime-bots
31. *Cyber Banking Fraud*. Najdeno 6. septembra 2016 na spletnem naslovu https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud

32. *Cyber Crime Costs More Than $400B Annually*. Najdeno 6. avgusta 2016 na spletnem naslovu http://www.arma.org/r1/news/newswire/2014/06/25/cybercrime-costs-more-than-$400b-annually
33. *Cyber Threats History: The Internet Expansion (1990s)*. Najdeno 6. septembra 2016 na spletnem naslovu http://tremblinguterus.blogspot.si/2013/01/cyber-threats-history-internet.html
34. *Cyber-attack hits Canadian government computers*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.bbc.com/news/world-us-canada-12498254
35. *Def Con 1 Archive*. Najdeno 30. marca 2016 na spletnem naslovu https://www.defcon.org/html/links/dc-archives/dc-1-archive.html
36. Definition of cyber espionage (b.l.). V *Financial Times Lexicon*. Najdeno 3. junija 2016 na spletni strani http://lexicon.ft.com/Term?term=cyber-espionage.
37. *Dragonfly: Western Energy Companies Under Sabotage Threat*. Najdeno 19. aprila 2016 na spletnem naslovu http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
38. Esposito, R. (2006, 1. november). *Hackers Penetrate Water System Computers*. Najdeno 14. aprila 2016 na spletnem naslovu http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html
39. Evrospka direktiva o varovanju informacij in omrežij ter zasebnosti podatkov. *Uradni list EU* 2016/680.
40. Fadilpašić, S. (2015, 26. Februar). *The true cost of Target's 2013 cyber attack*. Najdeno 6. 9. 2016 na spletnem naslovu http://www.itproportal.com/2015/02/26/target-reveals-true-cost-2013-cyber-attack/
41. Farivar, C. (2016, 15. junij). *"Spam King," who defied nearly $1B in default judgments, sentenced to 2.5 years*. Najdeno 18. junija 2016 na spletnem naslovu http://arstechnica.com/tech-policy/2016/06/spam-king-who-defied-nearly-1b-in-default-judgments-sentenced-to-2-5-years/
42. Finkle, J. (2016, 26. april). *Exclusive: SWIFT warns customers of multiple cyber fraud cases*. Najdeno 1. maja 2016 na spletnem naslovu http://www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI
43. Gaberšek, S. (2007). *Ekonomika naložb v informacijsko varnost*. Ljubljana: Ekonomska fakulteta.
44. Gaudin, S. (2000). Case Study of inside Sabotage: The Tim Lloyd Case. *Computer Security Journal*, *16*(3), 1-8.
45. *Gauss: Nation-state cyber-surveillance meets banking Trojan*. Najdeno 18. junija 2016 na spletnem naslov: https://securelist.com/blog/incidents/33854/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/
46. Gayer, O., Atias, R., & Zeifman, I. (2015, 12. maj). *Lax Security Opens the Door for Mass-Scale Abuse of SOHO Routers*. Najdeno 6. maja 2016 na spletnem naslovu https://www.incapsula.com/blog/ddos-botnet-soho-router.html

47. Global Spam volume (b.l.). Najdeno 15. junija 2016 na spletnem naslovu https://www.senderbase.org/static/spam/#tab=1
48. *Gmail ups security after Chinese attack*. Najdeno 17. aprila 2016 na spletnem naslovu https://www.theguardian.com/technology/2010/jan/13/gmail-increases-security-chinese-attack
49. Grant Thornton (2015). *Cybercrime: Facing the challenges*. Dublin: Grant Thornton.
50. Greenberg, A. (2012, 27. julij). *Hacker Demos Android App That Can Wirelessly Steal And Use Credit Cards' Data*. Najdeno 14. junija 2016 na spletnem naslovu http://www.forbes.com/sites/andygreenberg/2012/07/27/hacker-demos-android-app-that-can-read-and-use-a-credit-card-thats-still-in-your-wallet/#22f0032813a8
51. Gross, D. (2011, 15. avgust). *'Mafiaboy' breaks silence, paints 'portrait of a hacker'*. Najdeno 6. septembra 2016a na spletnem naslovu http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/
52. Gross, G. (2016, 11. januar). *Juniper ScreenOS Backdoor Eavesdropping*. Najdeno 1. junija 2016 na spletnem naslovu https://www.alienvault.com/blogs/security-essentials/juniper-screenos-backdoor-eavesdropping
53. *Hack Back*. Najdeno 20. maja 2016 na spletnem naslovu http://pastebin.com/raw/0SNSvyjJ
54. *Hekerji vdrli tudi v Luko Koper*. Najdeno 10. junija 2016 na spletnem naslovu http://www.zurnal24.si/vdrli-tudi-v-luko-koper-clanek-153149)
55. *Hello, Unit 61398*. Najdeno 14. junija 2016 na spletnem naslovu http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks
56. Herman, P. (2010, 9. september). *Baltimore IT guy sentenced for hacking boss's PowerPoint with porn*. Najdeno 1. junija 2016 na spletnem naslovu www.baltimoresun.com/bs-mtblog-2010-09-employee_charged_with_hacking-story.html
57. Higgins, S. (2015, 1. julij). *Details of $5 Million Bitstamp Hack Revealed*. Najdeno 22. maja 2016 na spletnem naslovu http://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/
58. *History of Phishing*. Najdeno 12. junija 2016 na spletnem naslovu http://www.phishing.org/history-of-phishing/
59. HM Treasury (2004, oktober). *The Orange Book Management of Risk: Principles and Concepts*. London: HM Treasury.
60. *How To Remove The Happy99 Worm*. Najdeno 6. septembra 2016 na spletnem naslovu http://thestarman.pcministry.com/avt/happy99.html
61. *How to summon a Tesla car using Apple Watch*. Najdeno 1. junija 2016 na spletnem naslovu http://www.telegraph.co.uk/motoring/12144080/How-to-summon-a-Tesla-car-using-Apple-Watch.html
62. *Interni nadzor potrdil ugotovitve podcrto.si: policija se ni pravilno odzvala na opozorila o varnostnih ranljivostih Tetre*. Najdeno 19. aprila 2016 na spletnem

naslovu https://podcrto.si/interni-nadzor-potrdil-ugotovitve-podcrto-si-policija-se-ni-pravilno-odzvala-na-opozorila-o-varnostnih-ranljivostih-tetre/
63. *Iran authorities could be behind cyber attack against Mossad and CIA, experts say*. Najdeno 20. maja 2016 na spletnem naslovu http://www.haaretz.com/news/diplomacy-defense/iran-authorities-could-be-behind-cyber-attack-against-mossad-and-cia-experts-say-1.382853
64. *Iranian cyber army' hits Twitter*. Najdeno 14. maja 2016 na spletnem naslovu http://news.bbc.co.uk/2/hi/technology/8420233.stm
65. *It's not if but when a cyber security attack will happen*. Najdeno 20. julija 2016 na spletnem naslovu http://www.companydirectors.com.au/director-resource-centre/publications/the-boardroom-report/back-volumes/volume-11-2013/volume-11-issue-4/its-not-if-but-when-a-cyber-security-attack-will-happen
66. Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*, 973–993.
67. Kadal, J. & Kovacik, R. (2016, 18. februar). *Hollywood Hospital 'Victim of Cyber Attack*. Najdeno 23. maja 2016 na spletnem naslovu http://www.nbclosangeles.com/news/local/Hollywood-Hospital-Victim-of-Cyber-Attack-368574071.html
68. Kerner, S. M. (2015). Average Cost of Cyber-crime in the U.S. Rises to $15 Million. *QuinStreet, Inc*.
69. Klimmburg, A. (2012). *National cyber security Framework Manual*. Tallinn: NATO CCD COE Publication.
70. *Komu vse je Hacking Team dobavljal policijske trojance*. Najdeno 2. junija 2016 na spletnem naslovu https://slo-tech.com/novice/t647512
71. Krebs, B. (2016, 16. julij). *Cybercrime Overtakes Traditional Crime in UK*. Najdeno 20. julija 2016 na spletnem naslovu http://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk/
72. Laroux (b.l.). V *Virus Encyclopedia*. Najdeno 31. marca 2016 na spletni strani http://virus.wikidot.com/laroux
73. Lee, P, Stewart, D., & Culgar-Pop, C. (2015). *Technology, Media & Telecommunications Predictions 2015*. London: The Creative Studio at Deloitte.
74. Leyden, J. (2005, 26. julij). *Russian spammer murdered*. Najdeno na dne 31. maja 2016 na spletnem naslovu http://www.theregister.co.uk/2005/07/26/russian_spammer_killed/
75. *Macro Virus Protection in the Microsoft Office Line, Part One*. Najdeno 31. marca 2016 na spletnem naslovu http://www.symantec.com/connect/articles/macro-virus-protection-microsoft-office-line-part-one
76. Madrigal, A. (2012, 7. avgust). *All the Spammers in the World May Only Make $200 Million a Year*. Najdeno 15. maja 2016 na spletnem naslovu http://www.theatlantic.com/technology/archive/2012/08/all-the-spammers-in-the-world-may-only-make-200-million-a-year/260814/

77. Mahon, T. (2015). Cyber - the 21th Century Threat. *Monch Publishing Group MT*, 5/2015, 20-23.
78. Malcolm, A. (2007). *Social engineering - a means to violate a computer system*. SANS Institute.
79. Matrosov, A., Rodoinov, E., Harley, D., & Malcho, J. (b.l.). *Stuxnet Under the Microscope, Revision 1.31*. ESET spol. s r.o.
80. *Melissa virus*. Najdeno 6. septembra 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/Melissa-virus
81. Mitnick, D. K., & Simon, L. W. (2003). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
82. Mogg, T. (2016, 18. februar). *Hollywood hospital pays $17,000 to ransomware hackers*. Najdeno 12. junija 2016 na spletnem naslovu http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/
83. *Mondo 2000 History Project*. Najdeno 6. septembra 2016 na spletnem naslovu https://archive.org/details/mondohistory&tab=about
84. Moore, R. (2010). *Cybercrime: Investigating High-Technology Computer Crime*. Routledge.
85. Morley, K. (2016, 21. januar). *Tap-and-go card boom leaves elderly at greater risk of 'family fraud'*. Najdeno 1. junija 2016 na spletnem naslovu http://www.telegraph.co.uk/finance/personalfinance/borrowing/creditcards/12113814/Tap-and-go-card-boom-leaves-elderly-at-greater-risk-of-family-fraud.html
86. National Crime Agency and Strategic Cyber Group (2016). *Cyber Crime Assessment 2016*. Najdeno 20. julija 2016 na spletnem naslovu http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
87. *O centru SI-CERT*. Najdeno 12. julija 2016 na spletnem naslovu https://www.cert.si/si/o-centru/
88. Parrish, K. (2014, 30. december). *Lizard Squad Offering Its DDoS Tool For Monthly Fee.* Najdeno 20. aprila 2016 na spletnem naslovu http://www.tomshardware.com/news/lizard-squad-ddos-toolset-subscription,28280.html
89. *Patch Tuesday*. Najdeno 2. junija 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/Patch-Tuesday
90. Peltier, T. R. (2005). *Information Security Risk Analysis*. Auerbach Publications.
91. *Penny Stocks and sexual enhancing drugs top spam topics for 2007*. Najdeno 2. julija 2016 na spletnem naslovu http://pressreleases.responsesource.com/news/33138/penny-stocks-and-sexual-enhancing-drugs-top-spam-topics-for-2007/
92. Poulsen, K. (2003, 19. avgust). *Slammer worm crashed Ohio nuke plant network*. Najdeno 14. junija 2016 na spletnem naslovu http://www.securityfocus.com/news/6767

93. *President Bush Signs Homeland Security Act*. Najdeno 6. septembra 2016 na spletnem naslovu https://georgewbush-whitehouse.archives.gov/news/releases/2002/11/20021125-6.html
94. *Primeri spletnih goljufij*. Najdeno 1. julija 2016 na spletnem naslovu https://www.cert.si/si/varnostne-groznje/spletne-goljufije/primeri
95. *Protect Against Social Engineering*. Najdeno 25. junija 2016 na spletnem naslovu http://www.cisco.com/c/en/us/about/security-center/protect-against-social-engineering.html
96. Ramirez, J. (2010, 9. marec). *The History of Computer Hacking*. Najdeno 30. marca 2016 na spletnem naslovu http://europe.newsweek.com/history-computer-hacking-69449?rm=eu
97. Ramzan, Z. (2007, 10. avgust). *A Brief History of Phishing: Part I*. Najdeno 21. maja 2016 na spletnem naslovu http://www.symantec.com/connect/blogs/brief-history-phishing-part-i
98. *Ransomware: Cyber criminals have locked your computer but should you pay up*. Najdeno 21. maja 2016 na spletnem naslovu http://www.ibtimes.co.uk/ransomware-cyber-criminals-have-locked-your-computer-should-you-pay-1544446
99. Rekouche, K. (2011). Early Phishing. *Computer Science*.
100. *Resources for the Ethical SCADA Hacker*. Najdeno 12. maja 2016 na spletnem naslovu https://scadahacker.com/resources.html.
101. Riley, C. (2015, 20. julij). *Hackers threaten to release names from adultery website*. Najdeno 22. aprila 2016 na spletnem naslovu http://money.cnn.com/2015/07/20/technology/ashley-madison-hack/
102. Riley, M., & Robertson, J. (2014). *JPMorgan Hackers Said to Probe 13 Financial Firms*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.bloomberg.com/news/articles/2014-10-09/jpmorgan-hackers-said-to-probe-13-financial-firms
103. Ritchey, D. (2014, 1. avgust). *Special Report: Cyber Risk and Special Security*. Najdeno 15. avgusta 2016 na spletnem naslovu http://www.securitymagazine.com/articles/85679-special-report-cyber-risk-and-security
104. Rouse, M. (b.l.). *Definition social engineering*. Najdeno 20. maja 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/social-engineering
105. Rubenking, J. N. (2014, 15. februar). *A guide to the different kinds of malware*. Najdeno 3. avgusta 2016a na spletnem naslovu http://www.itproportal.com/2014/02/15/a-guide-to-the-different-kinds-of-malware/
106. Rubenking, J. N. (2014, 26. marec). *Know Your Malware*. Najdeno 20. junija 2016b na spletnem naslovu https://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/

107. *Russia accused of unleashing cyberwar to disable Estonia*. Najdeno 6. septembra 2016 na spletnem naslovu https://www.theguardian.com/world/2007/may/17/topstories3.russia.
108. Savitz, E., & Lewis, J. (2012, 5. avgust). *Figuring DDoS Attack Risks Into IT Security Budgets*. Najdeno dne 21. marca 2016 na spletnem naslovu http://web.b.ebscohost.com/ehost/delivery?sid=0e52213c-246f
109. Schmuger, C. (2010, 14. januar). *More Details on "Operation Aurora"*. Najdeno 20. maja 2016 na spletnem naslovu https://blogs.mcafee.com/mcafee-labs/more-details-on-operation-aurora/
110. Schneier, B. (2000). *Secrets & Lies. Digital Security in a Networked World (*15th ed.*)*. John Wiley & Sons.
111. Schneier, B. (2005, 17. november). *Sony's DRM Rootkit: The Real Story*. Najdeno 6. septembra 2016 na spletnem naslovu https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html
112. Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
113. Schultz, J. (2014, 2. maj). *Spam Hits Three Year High-Water Mark*. Najdeno 1. junija 2016 na spletnem naslovu http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark
114. Schwartz, M. (2013, 21. maj). *Google Aurora Hack Was Chinese Counterespionage Operation.* Najdeno 1. junija 2016a na spletnem naslovu http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060
115. Schwartz, M. (2013, 23. januar). *Security Flaws Leave Networked Printers Open To Attack*. Najdeno 1. junija 2016b na spletnem naslovu http://www.networkcomputing.com/government/security-flaws-leave-networked-printers-open-attack/1607103194
116. Shakarain, R., Shakarain, J., & Reuf, A. (2011). *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (1th ed.). Elseview.
117. *SI-CERT 2015-01 / Val phishing napadov na komitente slovenskih bank*. Najdeno 2. junija 2016 na spletnem naslovu https://www.cert.si/si-cert-2015-01/
118. Singel, R. (2008, 23. januar). *War Breaks Out Between Hackers and Scientology — There Can Be Only One*. Najdeno 6. septembra 2016 na spletnem naslovu https://www.wired.com/2008/01/anonymous-attac/
119. *Slovenski portal varni na internetu*. Najdeno 12. aprila 2016 na spletnem naslovu www.varninainternetu.si.
120. Storm, D. (2012. 9. avgust). *Gauss malware: Nation-state cyber-espionage banking Trojan related to Flame, Stuxnet*. Najdeno 20. maja 2016 na spletnem naslovu http://www.computerworld.com/article/2597456/security0/gauss-malware--nation-state-cyber-espionage-banking-trojan-related-to-flame--stuxnet.html
121. *Strategija kibernetske varnosti*. Najdeno 18. avgust 2016 na spletnem naslovu https://www.cert.si/strategija-kibernetske-varnosti-slovenije/

122. *SWIFT Society for the Worldwide Interbank Financial Telecommunication*. Najdeno 22. maja 2016 na spletnem naslovu http://searchcio.techtarget.com/definition/SWIFT
123. *Symantec (2016). 2016 Internet Security Threat Report*. Najdeno 1. junija 2016 na spletnem naslovu https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
124. *Škulj naredil samomor*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.24ur.com/novice/slovenija/skulj-naredil-samomor.html
125. *Thai government websites hit by denial-of-service attack*. Najdeno 22. aprila 2016 na spletnem naslovu www.bbc.com/news/world-asia-34409343
126. *The History Of Hacking – Timeline Of Hacking Techniques*. Najdeno 6. septembra 2016 na spletnem naslovu https://tbgsecurity.com/the-history-of-hacking-timeline-of-hacking-techniques-infographic/
127. *The Panama Papers*. Najdeno 6. septembra 2016 na spletnem naslovu https://www.occrp.org/en/panamapapers/
128. *Timeline of Computer Viruses*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.mapcon.com/timeline-of-computer-viruses
129. Tomšič, M. (2016, 10. marec). *Kako se lahko podjetja zaščitijo pred hekerskimi vdori ali nerodnostjo zapolsenih*. Najdeno 20. maja 2016 na spletnem naslovu http://siol.net/digisvet/novice/kako-se-lahko-podjetja-zascitijo-pred-hekerskimi-vdori-ali-nerodnostjo-zaposlenih-406832
130. Tripton, H., & Krause, M. (2004). *Information Security Management Handbook* (5th ed.). Auerbach Publications.
131. Turton, W. (2014, 30. december). *Lizard Squad's Xbox Live, PSN attacks were a 'marketing scheme' for new DDoS service*. Najdeno 20. aprila 2016 na spletnem naslovu http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/
132. Umbach, F. (2013, 9. maj). City Electricity Supplies Held to Ransom by Cyber Hackers. *Geopolitical Information Service*. Najdeno 21. marca 2016 na spletni strani http://web.b.ebscohost.com/ehost/delivery?sid=f7f39d09-ac8f-4
133. Urad vlade Republike Slovenije za komuniciranje. (2016). Sporočilo za javnost Vlade RS. Najdeno 15. julija 2016 na spletnem naslovu http://www.vlada.si/fileadmin/dokumenti/si/Sporocila_za_javnost/2016/sevl76-16.pdf
134. Valley, H. (2012, 18. junij). How much does cyber crime cost. *Business Jornal*, str. 10.
135. Verleur, J. (2015, 30. marec). *The Top 5 Ecommerce Trends You Should Look Out For*. Najdeno 18. junija 2016 na spletnem naslovu https://www.entrepreneur.com/article/244085
136. Vičič, D. (2015, 6. januar). *Slovenska bitcoin borza tarča hekerjev, ukradenih štiri milijone evrov*. Najdeno 19. aprila 2016 na spletnem naslovu

http://www.mladina.si/163325/slovenska-bitcoin-borza-tarca-hekerjev-ukradenih-stiri-milijone-evrov/
137. *Virus Profile: Ghostballs*. Najdeno 6. septembra 2016 na spletnem naslovu https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=498
138. *Viruses that can cost you*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.symantec.com/region/reg_eu/resources/virus_cost.html
139. Vizard, M. (2015). *Inside the IT Security Budget Paradox*. Najdeno 20. maja 2016 na spletnem naslovu http://www.channelinsider.com/security/slideshows/inside-the-it-security-budget-paradox.html
140. Von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security, 6*(5), 224-225.
141. Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & security, 38*, 97-102.
142. Weverbergh, R. (b.l.). *The German startup wars: now it's DDoS attacks AND black hat SEO attacks*. Najdeno 20. aprila 2016 na spletnem naslovu http://www.whiteboardmag.com/the-german-startups-wars-now-its-ddos-attacks-and-black-hat-seo-attacks/
143. *What is a 419 (Advance-fee Fraud) Scam?* Najdeno 12. junija 2016 na spletnem naslovu http://whatismyipaddress.com/419-scam
144. *What is a computer virus?* Najdeno 2. junija 2016 na spletnem naslovu https://www.microsoft.com/en-us/safety/pc-security/virus-whatis.aspx
145. *What is a Trojan Virus?* Najdeno 26. maja 2016 na spletnem naslovu https://usa.kaspersky.com/internet-security-center/threats/trojans#.V2VUkGaLlPM
146. *What is Antivirus Software?* Najdeno 6. septembra 2016 na spletnem naslovu https://antivirus.comodo.com/what-is-antivirus-software.php
147. *What Is Blog or Comment Spam and How Can I Fight It?* Najdeno 2. julija 2016 na spletnem naslovu http://www.webspam.org/what-is-blog-or-comment-spam-and-how-can-i-fight-it/
148. *What Is The '419' Scam*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.419eater.com/html/419faq.htm
149. *What is WikiLeaks*. Najdeno 6. septembra 2016 na spletnem naslovu https://wikileaks.org/What-is-Wikileaks.html
150. Whitman, E. M., & Mattord, J. H. (2011). *Principles of Information Security* (4th ed.). Course Technology, Cengage Learning.
151. Wojtczuk, R., & Rutwoska, J. (2009). Attacking SMM Memory via Intel® CPU Cache Poisoning. *Invisiblethingslab.* Najdeno 13. julija 2016 na spletnem naslovu http://invisiblethingslab.com/resources/misc09/smm_cache_fun.pdf
152. Woollacott, E. (2010, 12. januar). *Baidu: Hacking war breaks out between Iran and China*. Najdeno 6. septembra 2016 na spletnem naslovu http://www.tgdaily.com/security-features/45454-hacking-war-breaks-out-between-iran-and-china

153. Zakon o elektronskih komunikacijah. *Uradni list RS* št. 13/2007-UPB1, 102/07–ZDRad, 110/09, 33/11, 109/12–ZEKom-1.
154. *Zamenjava tolarjev v evre*. Najdeno 18. junija 2016 na spletnem naslovu https://www.bsi.si/orodja/preracun-tolarja.asp?MapaId=1279
155. Zetter, K. (2014, 14. januar). *Google Hack Attack Was Ultra Sophisticated, New Details Show*. Najdeno 25. maja 2016 na spletnem naslovu https://www.wired.com/2010/01/operation-aurora/
156. Zetter, K. (2014, 3. november). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Najdeno 25. maja 2016 na spletnem naslovu https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
157. Zorabedian, J. (2014, 26. marec). *How malware works: Anatomy of a drive-by download web attack*. Najdeno 20. aprila 2016a na spletnem naslovu https://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/
158. Zorabedian, J. (2015, 28. oktober). *Did the FBI really say "pay up" for ransomware? Here's what to do…* Najdeno 20. aprila 2016b na spletnem naslovu https://nakedsecurity.sophos.com/2015/10/28/did-the-fbi-really-say-pay-up-for-ransomware-heres-what-to-do/
159. Žnidar, B. (2006). *Vloga informatike pri zagotavljanju neprekinjenega poslovanja v slovenskih podjetjih* (diplomsko delo). Ljubljana: Ekonomska fakulteta.

PRILOGA

Priloga: Časovna premica odmevnejših dogodkov v svetu kiber kriminala

LETO	DOGODEK
1986	• Ameriški kongres sprejme Computer Fraud and Abuse Act, ki kriminalizira vdore v računalniške sisteme in tako daje pravno podlago pregonu kriminalcev.
1987	• Lehigh je eden prvih virusov, ki jih poznamo v zgodivini računalništva. Okužil je command.com in se širil preko disket. • Prvi antivirusni program, ki ga je naredil avtor Bernd Fix (What is Antivirus Software?, 2016).
1988	• Eden prvih internetnih črvov Morris – namen naj bi bil zgolj pritegniti medijsko pozornost, realni rezultat pa ohromitev delovanja velikega števila računalnikov. Avtor R. T. Morris je bil obsojen na osnovi CFAA (Ramirez, 2016) • Ustanovljen prvi CERT (Computer Emergency Response Team).
1989	• Ghostball je prvi multipartitni virus, kar pomeni, da se je širil in okuževal sisteme na različne načine (Virus Profile: Ghostballs, 2016). • Pojavijo se prve revije na temo računalništva, tehnologije, hekanja, kot je npr. Mondo 2000 (Mondo 2000 History Project, 2016).
1990	• Prvi polimorfni virus (spreminja svojo obliko), znan pod imenom Chameleon: avtorja M. Washburn in R. Burger (Timeline of Computer Viruses, 2016)
1992	• Michelangelo pusti pečat avtorja: svojo škodljivo dejavnost izvede 6. marca, kar sovpada z rojstnim dnevom avtorja (Timeline of Computer Viruses, 2016).
1993	• Prva DEF CON konferenca (Def Con 1 Archive, 2016).
1994	• Goljufija sistema »Green Card Lottery«, kjer prevaranti posredniki zaračunavajo storitev, ki je sama po sebi popolnoma brezplačna.
1995	• Prvi Word macro virus, ki se je uspel masovno razširiti. (Poneserči) so ga na CD-jih razmnoževale tudi velike korporacije, ki jim je okužil vsebino zgoščenk (Macro Virus Protection in the Microsoft Office Line, Part One, 2016).
1996	• T. Lloyd sabotira glavni strežnik. Posledica: 2 mio $ neposrednih stroškov, 10 mio $ oportunitehnih strškov zaradi manjše prodaje. 41 mesecev zapora (Gaudin, 2000, str. 1). • Laroux - prvi virus, ki okuži Microsoft Excel dokumente, virus Baza okuži Windows 95 operacijske sisteme, Linux operacijski sistemi pa so dobili svoj virus z imenom Staog (Laroux, 2016).

1997	• Virusi so dobili novo nalogo: poškodovati strojno opremo. CIH, znan tudi pod imenom Chernobyl, je v nekaterih primerih namreč povsem onesposobil računalnik za delo s prepisom BIOS-a (Cluley, 2016). • 15-letni Hrvat vdre v računalnike v U.S. Air Force bazi v Guamu (Cyber Threats History: The Internet Expansion (1990s), 2016).
1998	• Melissa črv izrablja pomankljivost v MS Wordu. Marsikateri vir ocenjuje, da je naredil največ škode doslej (Melissa virus, 2016). • Yahoo! iskalnik so pretentali, da je strašil uporabnike, da se bo sprožila »logična bomba«, če Kevin Mitnick (eden najbolj poznanih hekerjev) ne bo izpuščen iz zapora. Gre seveda za prevaro (Cyber Threats History: The Internet Expansion (1990s), 2016).
1999	• »Happy New Year« je vsem žrtvam zaželel virus Happy99, ki se je razpošiljal preko e-pošte (How To Remove The Happy99 Worm, 2016).
2000	• ILOVEYOU virus, znan tudi pod imenom Love Letter, ki je bil eden največjih in najbolj odmevnih primerov zlonamerne programske kode nasploh. Eden prvih, ki uporablja socialni inženiring za širjenje (Computer Virus Timeline, 2016). • MafiaBoy, kot se je poimenoval takrat 15 let stari deček, je z DoS napadom popolnoma ohromil delovanje velikanov Yahoo, eBay, CNN in mnoge druge (Gross, 2016a).
2001	• Virus Anna Kournikova, ki je ciljal (predvsem) na moški del populacije in je že dobro izrabljal socialni inženiring za razširjanje, je obljubljal slike omenjene lepotice, a je bil na koncu le zlonamerna programska koda (Computer Virus Timeline, 2016).
2002	• Microsoft je pričel izvajati interne treninge na področju varnosti in uvedel kontrolo kvalitete programske. • Ameriški predsednik Bush ustanovi Department of Homeland Security, ki bo med drugim odgovoren za varnost državne kritične IT infrastrukture (President Bush Signs Homeland Security Act, 2016).
2003	• Robert Škulj spiše program za zaščito varnostne luknje v NLB spletni banki, sistemu KLIK, in ga skuša prodati banki. Robert kasneje napove, da bo tožil državo in NLB za 200 mio tolarjev, a zgodba ne dobi epiloga, saj ga 8. 8. 2003 ga najdejo mrtvega v stanovanju (Škulj naredil samomor, 2016). • Formirana skupina Anonymous, ki deluje anonimno, a sinhrono organizirano sprva bolj za zabavo, kasneje izvaja odmevne napade na politične in druge organizacije. • Črv slammer, ki je neverjetno majhen, v 10 minutah okuži več kot 75.000 računalnikov in upočasni delovanje interneta na globalni ravni

	(Timeline of Computer Viruses, 2016). • Sobig črv, ki sicer v osnovi ni bil načrtovan, da ohromi strateško infrastrukturo, je zaradi svojega agresivnega delovanja precej ohromil in povročil številne preglavice in zastoje v železniškem prometu, preobremenjenost mednarodnih internetnih povezav ipd. (Viruses that can cost you, 2016).
2004	• Razširjenost črvov MyDoom, Bagle in Netsky, ki so se širili preko e-pošte, je vodila k precejšnjemu izboljšanju programske opreme za zaznavanje nezaželenih sporočil.
2005	• Neslavni škandal Sonyja, ki je uporabnikom igralnih konzol na več načinov namestil korenski komplet brez njihovega vedenja, te tudi odstraniti niso mogli. Antivirusni programi je niso zaznali. Ta je zbirala različne informacije o uporabnikih in jih pošiljala Sony-ju ter odprla različne ranljivosti v samem sistemu (Schneier, 2016).
2006	• Wikileaks ustanovi Julian Assange z namenom objavljanja zaupnih in tajnih dokumentov (What is WikiLeaks?, 2016). • Hakerji vdrejo v sistem za filtriranje vode v Harrisburgu in namestijo zlonamerno programsko kodo. Primer preiskuje FBI (Esposito, 2006). • Prvi primer kiberkriminala na področju internetne telefonije v ZDA.
2007	• Zeus trojanski konj uporabljen predvsem z namenom kraje bančnih podatkov, s katerimi so si zlikovci iz Vzhodne Evrope nelegalno prilastili cca. 70 milijonov USD (Cyber Banking Fraud, 2016).
2008	• Mariprosa, ki ga sestavlja v omrežje povezanih preko 1 milijona računalnikov (500-100 največjih podjetij), izvaja DDoS in druga kriminalna dejanja . Sledijo aretacije, v katerih je bil aretiran in kasneje obsojen tudi Slovenec (Arthur, 2016).
2009	• Koobface črv izrablja socialne medije (npr. Facebook in MySpace) in druge popularne spletne strani in storitve (npr. Gmail, Skype ...), za širitev in zbiranje informacij (Timeline of Computer Viruses, 2016). • Črv Conflicker prizadane milijone računalnikov, tudi najbolj strogo varovane. Zanimiv je vektor napada, ki izrablja poti, ki bi jih morali vestni varnostni inženirji že zdavnaj sanirati (Condon, 2016).
2010	• Stuxnet, katerega avtorji so domnevno ekipa (vladno motiviranih) ljudi iz ZDA in Izraela z namenom prikrito oslabiti iranske jedrske centrifuge (Timeline of Computer Viruses, 2016). • Napad na Gmail z namenom pridobitve nepooblaščenega dostopa do uporabniških računov kitajskih aktivistov za človeške pravice. Izvor napada: Kitajska (Gmail ups security after Chinese attack, 2016).
2011	• RSA, eden največjih proizvajalcev IT varnostnih rešitev, je bil uspešno napaden. Posledica: visoki stroški zamenjave generatorjev enkratnih

	gesel (preko 30.000 strank oz. 40 mio žetonov), izguba ugleda in zaupanja. • Napad na Sony Playstation Network, ki je prizadel kar 77 mio. uporabniških računov in povzročil nedelovanje storitve za kar 23 dni (The History Of Hacking – Timeline Of Hacking Techniques, 2016). • Vdor v Youtubeov račun, kjer so napadalci preko otroškega kanala serije Sezamova ulica kar 22 minut predvajali pornografijo.
2012	• Vdor v računalnik Luke Koper (Hekerji vdrli tudi v Luko Koper, 2016). • Prikaz ranljivosti policijskega radijskega omrežja, poznanega pod imenom TETRA, razkrije velike pomanjkljivosti sistema. Ker sistem TETRA uporablja med drugim tudi vojaška policija, ki izvaja protidiverzantsko in protiteroristično zaščito v vojaških objektih ter varuje objekte in okolje, ki so posebnega pomena za obrambo države (Interni nadzor potrdil ugotovitve podcrto.si: policija se ni pravilno odzvala na opozorila o varnostnih ranljivostih Tetre, 2016). • Saudi Aramco, ki dobavlja 10 % svetovne zaloge nafte, postane žrtev napada. V le nekaj urah postanejo v celoti odrezani od sodobnih komunikacijskih poti in so prisiljeni uporabljati tipkarske stroje in fakse. Nastanejo enormni stroški saniranja posledic, oportunitetni stroški izgubljenih poslov (nafto so v svoji državi npr. začeli deliti celo brezplačno itd.) (2012 Cyber Attacks Timeline Master Index, 2016).
2013	• Dragonfly napade preko kiberspijonaže različne tarče zahodnega sveta. Najbolj je na udaru energetski sektor, ki ga sabotaža najbolj prizadane (Dragonfly: Western Energy Companies Under Sabotage Threat, 2016). • Napad na Pintrest, Facebook in Twitter, pri čemer so bili odtujeni podatki o uporbnikih: e-naslovi, gesla itd. • Napad na Target v času nakupovalne mrzlice, ki so ga sicer zaznali, a niso ukrepali. Odtujitev podatkov o več kot 40 mio. kreditnih karticah. Dodatni stroški nastali tudi zaradi tožb jeznih strank (Fadilpašić, 2016). • Prvič zaznana zlonamerna programska koda, ki zašifrira vsebino lokalnega diska in zahteva odkupnino za pridobitev dešifrirnega ključa, znana pod imenom ransomware (Internet Security Threat Report, 2016, str. 59). • Logo na Twitterjevem računu podjetja Burger King zamenja logo konkurenčnega podjetja McDonald.
2014	• Napad na bitcoin borze. Odmeven primer je zelo dovršen, premišljen in uspešno izveden napad na eno najuspešnejših borz Bitstamp, katere avtorji so Slovenci (Vičič, 2016). • Napad na JPMorgan Chase & Co prizadane preko 76 mio. gospodinjstev in preko 7 mio. podjetij (Riley in Robertson, 2016).

	• Virus Backoff krade podatke iz kreditnih kartic preko prodajnih terminalov (POS) sistemov.
2015	• Napad na največjo spletno posredovalnico za zmenke s sloganom »Life is short. Have an affair.«. Odtujitev občutljivih osebnih podatkov (imena ter priimki, e-naslovi, spolne fantazije, številke kreditnih kartic ...). Motiv za napad: zahteva za takojšnjo zaprtje strani, saj kljub plačilu 19 $ posameznika za trajno brisanje osebnih podatkov tega ni storil. Posledice: tudi ločitve v zakonskih zvezah (Riley, 2016).
2016	• Anonimni vir pošlje nemškemu časopisu podatke o poslovanju panamskega podjetja Mossack Fonseca, ki jih poznamo pod imenom »Panamski dokumenti«. Razkrivajo davčne prevare in utaje najrazličnejših posameznihov in podjetij (The Panama Papers, 2016).