UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

KIBERNETSKI KRIMINAL IN NJEGOVI NEGATIVNI VPLIVI NA POSLOVANJE PODJETIJ

Ljubljana, september 2016 DANILO MILIĆ

IZJAVA O AVTORSTVU

Podpisani Danilo Milić, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Kibernetski kriminal in njegovi negativni vplivi na poslovanje podjetij, pripravljenega v sodelovanju s svetovalko dr. Borko Jerman Blažić Džonovo.

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 _____ Podpis študenta:_____

KAZALO

KAZALO SLIK

UVOD

Tehnološki napredek v računalniški tehnologiji nam je omogočil preprostejše življenje, vendar nas je naredil tudi bolj ranljive. Uporabljamo internet, računalnike, pametne telefone in z njimi delamo praktično vse. Shranjujemo podatke, informacije o kreditnih karticah, geslih, datotekah, pošiljamo razne datoteke, slike. Vse kar se nam zdi pomembno imamo nekje shranjeno, na osebnih računalnikih, prenosnih računalnikih, pametnih telefonih, tabličnih računalnikih. Mislimo, da je vse na varnem, dokler nam nekdo ne izprazni našega bančnega računa, vdre v naš elektronski poštni račun (v nadaljevanju e-poštni račun) ali pa ukrade dragocene poslovne skrivnosti iz našega podjetja. Hitra rast interneta in računalniške tehnologije v zadnjih nekaj letih je privedla do rasti novih oblik kriminala poimenovanega kibernetski kriminal. Kibernetski kriminal je nov pojav, ki ima velik vpliv tako na svetovno prebivalstvo kot tudi na svetovno gospodarstvo. Podjetja, ljudi, vlade spravlja v histerijo. Iz leta v leto se število žrtev kiberkriminala povečuje. Stroški, ki jih povzročajo kiberkriminalci podjetjem, so zelo veliki. Ljudje so še vedno slabo seznanjeni s temo kiberkriminalitete. Vlade, podjetja naredijo še vedno premalo, da bi se zaščitila pred kibernetskimi napadi.

V današnjem, tehnološko povezanem svetu ljudje ne vidijo nevarnosti, ki jim pretijo v virtualnem svetu. Čeprav večina ljudje meni, da so ustrezno seznanjeni s to temo, se v resnici še vedno ne zavedajo, kakšne posledice lahko povzročijo različni kibernetski napadi. Kibernetska kazniva dejanja ogrožajo prihodnost komuniciranja, zaupnosti in celovitosti podjetij, posameznikov. Ko ljudje pomislijo na računalniška kazniva dejanja, imajo v mislih osebo, ki sedi za računalnikom in prenaša nelegalne datoteke, kot so filmi, pesmi, vendar je to daleč od resnice. Kibernetski zločini so v resnici veliko bolj zapleteni in nevarni. Svet danes postaja vse manjši in hkrati vse bolj povezan, predvsem zaradi interneta. Na tisoče podjetij, organizacij in agencij, poleg milijone ljudi po vsem svetu, lahko navežejo stik prek računalnika, interneta ter komunicirajo. Prav preko računalnikov, interneta potekajo zločini, ki jih ljudje ne poznajo in se ne zavedajo, da sploh obstajajo.

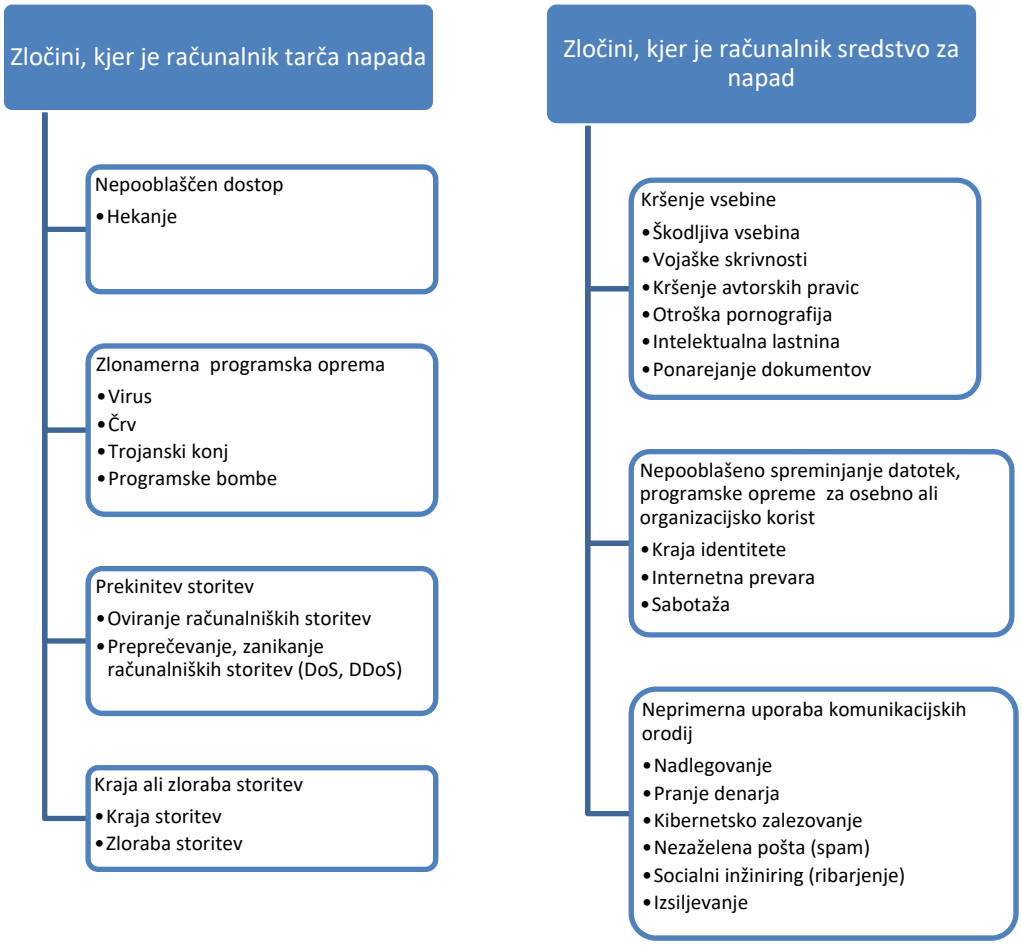
Zato sem se odločil napisati nalogo o kibernetskem kriminalu. Namen diplomske naloge je seznaniti tako podjetja, kot slehernega posameznika o nevarnostmi, ki jim pretijo v današnjem virtualno povezanem svetu in o njegovih negativnih vplivih na poslovanje podjetij. Poleg tega, na podlagi študij imam namen predstaviti kibernetski kriminal, kaj to sploh je, v kakšnih oblikah se pojavlja, kdo in kaj je tarča kiberkriminalcev, kakšne vplive imajo napadi na podjetja ter, kako naj se podjetja ubranijo pred raznimi kibernetskimi napadi. V nalogi imam namen podati oceno negativnih vplivov kibernetskega kriminala na poslovanje podjetij ter pripraviti poročila za zaščito pred kibernetskimi napadi.

1 KIBERNETSKI KRIMINAL

Število internetnih uporabnikov se vsako uro povečuje in posledica tega je, da svet postaja vedno bolj povezan. Svetovni splet zveni kot velik pojav, ampak presenetljivo ena izmed njegovih lastnosti je, da ustvarja manjši kraj za življenje njegovih uporabnikov. Vendar se je s

pojavom interneta pojavil tudi nov problem za koristnike interneta, ki se imenuje kibernetski kriminal. Medtem ko se organi pregona trudijo čim bolje spopasti s tem problemom, ta strmo raste in mnogi ljudje so postali žrtve hekanja, kraje osebnih podatkov, identitete in zlonamerne programske opreme. Eden izmed najboljših načinov, da ne bi postali žrtve kibernetskih kaznivih dejanj in zaščitili svoje občutljive podatke, je z uporabo neprebojnih varnosti, ki uporabljajo enotne sisteme programske in strojne opreme za preverjanje verodostojnosti vseh informacij na interneta. Tako poslanih, kot dostopnih. Vendar preden se dotaknemo te teme, moramo še kaj več izvedeti o kibernetskih kaznivih dejanjih (Cross Domain Solution, 2013). Vsako kaznivo dejanje, ki vključuje računalnike ter omrežja, internet se smatra kot kibernetski kriminal. Za vse, od goljufije, kraje denarja preko interneta, nezakonitega nalaganja glasbenih datotek, filmov pa do nezaželene elektronske pošte lahko rečemo, da je kibernetski kriminal. V nekaterih primerih so bili uporabljeni računalniki z namenom škodovanja, v drugih pa so bili računalniki tarča napada (Williams, 2014). Kot prikazuje Slika 1 obstaja veliko različnih vrst kibernetskega kriminala.

Slika 1: Vrste kibernetskega kriminala



Vir: A. Alkaabi & G. M. Mohay, Dealing with the problem of cybercrime, 2010, str. 7.

Ko je posameznika glavna tarča kibernetskega napada, računalnik smatramo kot sredstvo in ne kot cilj. Takšna vrsta napadov ne potrebuje nekega pretiranega strokovnega znanja ter

izkušenj. Izkoriščajo se predvsem človeške slabosti. Škoda, ki je povzročena je v veliki meri neopredmetena, psihološka. Takšne vrste zločinov obstajajo že več stoletij. Prevare, tatvine so obstajale že pred razvojem interneta, računalniške tehnologije. Z razvojem računalniške tehnologije so taka kazniva dejanja dobila orodje, ki poveča število potencialnih žrtev in ob enem je storilca kaznivega dejanje še težje izslediti in prijeti. Za razliko od zločinov, ki uporabljajo računalnik kot sredstvo, napadi ki imajo za tarčo napada druge računalnike, zahtevajo mnogo strokovnega, tehničnega znanja zato velikokrat takšne vrste napadov izvajajo izbrane skupine kiberkriminalcev. Z razvojem tehnologije se sočasno tudi razvijajo kazniva dejanja. Takšne vrste zločinov so relativno nov pojem, saj obstajajo le toliko časa, kot obstaja računalnik. To so razni računalniški virusi, škodljiva programska oprema (Aghatise, 2006).

Kiberkriminalci lahko uporabljajo računalniško tehnologijo za dostop do osebnih podatkov, poslovnih skrivnosti ali pa uporabljajo internet za razkrivanje zaupnih podatkov ter za namene škodovanja. Kriminalci lahko uporabljajo računalnike za komunikacijo ter za shranjevanje podatkov oziroma dokumentov. Osebe, ki opravljajo takšne nezakonite dejavnosti, imenujemo hekerji. Kibernetski kriminal lahko z drugo besedo imenujemo tudi računalniški kriminal (Cybercrime, 2011). Ko so se računalniki in omrežja povezala leta 1990, so hekerji izvajali napade samo zato, da bi pridobivali informacije o sistemu, kako je vse povezano, kako vse deluje. Hekerji so tekmovali med seboj in posledično je bilo prizadeto veliko mrež, od vojske do podjetij, organizacij. Sprva hekerji niso predstavljali neke velike grožnje in so bili obravnavani kot nadloga, ne grožnja. Vendar s pojavom zlonamerne programske opreme so omrežja ter sistemi začeli postajati počasnejši. Z leti so hekerji začeli postajati vse bolj vešči in so začeli uporabljati svoja znanja in izkušnje za pridobivanje koristi z izkoriščanjem in negativnim obravnavanjem drugih. Danes kiberkriminalce ne poganja več ego ali pa želja po pridobitvi dodatnega, strokovnega znanja, ampak želja po koristi. Uporabljajo svoja znanja, da kradejo, zavajajo in izkoriščajo ljudi, ker vidijo lažjo pot do zaslužka. Kibernetski zločini so postala resnična grožnja in so precej drugačni od klasičnih zločinov (ropanje, kraje). Za razliko od klasičnih, kibernetski zločini ne potrebujejo fizične prisotnosti za izvedbo kriminalnega dejanja. Zločini so lahko organizirani z oddaljene lokacije in hekerjem ni treba skrbeti za organe pregona, ki delujejo v državi, kjer je bil zločin storjen. Isti sistem, ki je ljudem omogočil lažje elektronsko poslovanje in spletne transakcije, je sedaj postal tarča kiberkriminalcev (Cross Domain Solution, 2013).

Poznavanje dejstev in trendov ter rasti računalniškega kriminala je lahko ključnega pomena za preprečevanje kraje, tako osebnih podatkov kot tudi podatkov v javnem in zasebnem sektorju. Odgovornost pade na vsakega slehernega uporabnika interneta, da se zaščiti pred raznimi oblikami napada (National Crime Prevention Council, 2012).

2 VRSTE KIBERNETSKEGA KRIMINALA

Kot obliko kibernetskega kriminala lahko smatramo več nezakonitih dejavnosti. Na eni strani imamo kazniva dejanja, ki vključujejo temeljne kršitve pravne in fizične zasebnosti, kot so

napadi na integriteto podatkov v podatkovnih skladiščih in uporabo nelegalno pridobljenih podatkov, informacij za izsiljevanje podjetja ali posameznika. Kraja identitete postaja vedno večji problem. Na drugi strani pa imamo kazniva dejanja, ki vključujejo poskuse oviranja delovanja interneta. Sem lahko vključujemo nezaželeno pošto, hekanje, napade, ki ovirajo dostop do internetnih storitev (Dennis, 2016). Obstaja veliko vrst kibernetskega kriminala, najpogostejše bodo razložene v nadaljevanju.

2.1 Zlonamerna programska oprema

Pod zlonamerno programsko opremo (angl. *malware*) smatramo računalniške programe ali zlonamerne programe, kot so virusi, trojanci, vohuni, črvi itd. Zlonamerni program ponavadi okuži računalnik preko elektronske pošte, spletne strani ali preko strojene opreme. Škodljiva programska oprema se lahko uporablja za prevzem osebnih računalnikov, ki jih nato spremenijo v zombi računalnike in uporabljajo za pošiljanje nezaželene pošte ali pa za namene, prekinitve storitev spletnih strani. Poleg tega se oprema lahko uporablja za distribucijo pornografije in nelicenčne programske opreme. Lastniki okuženih računalnikov se zavedajo, da imajo težavo, ker je njihov računalnik občutno počasnejši ali pa, ker ne morejo odstraniti nekega nameščenega programa (Hosch, 2009).

Zlonamerni programi lahko okužijo računalnik ali drugo napravo na več načinov. Ponavadi se zgodi popolnoma naključno, pogosto krat s pomočjo nalaganja programske opreme, ki je skupaj v paketu z zlonamerno programsko opremo. Nekatere škodljive programe lahko napadalci naložijo na računalnik z izkoriščanjem varnostnih ranljivosti operacijskih sistemov ter programov. Zastarele različice spletnih brskalnikov in njihovi dodatki so tudi lahko tarča napadalcev. V večini primerov se zlonamerni programi naložijo na računalnik zaradi nepazljivosti uporabnikov, ker ne gledajo kaj prenašajo. V nekaterih primerih se računalniki okužijo z načeloma neškodljivimi datotekami, kot so slike, zvočne datoteke, filmi (Fisher, 2016).

Korenska orodja (angl. *rootkit*) so najhujša oblika zlonamerne programske opreme, ki okužijo korenski nivo trdega diska računalnika in jih je nemogoče odstraniti, razen če izbrišemo pogon v celoti. Značilno je, da osebni računalniki postanejo okuženi z orodjem, ko namestijo nekaj programske opreme, pridobljene preko interneta, predvsem avtorsko zaščitene programske opreme, ki je bila prenesena nezakonito. Okuženi računalnik je nato uporabljen za distribucijo spama in pornografije (Rootkit, 2016). Korenska orodja so skupina programov, ki so programirana, da ostanejo nezaznavna na računalnikih, ki imajo dostop do večjega sistema. Nato te programi brskajo po računalniških datotekah in iščejo razna gesla. V veliko primerih so programi uporabljeni za kontrolo in spremljanje obiskov spletnih mest (Abraham & Chengalur-Smith, 2010).

Računalniški virus je del programske kode, ki je bil zasnovan, da se naprej prepisuje v računalniške datoteke. Ustvarjen je z namenom uničevanja podatkov in programske kode. V večini primerov okuženi računalniki še naprej opravljajo svojo nalogo, vendar zraven še

izvajajo navodila virusa. Virus se lahko nato razširi na datoteke in programe drugih računalnikov preko drugih pomnilniških naprav, računalniških omrežjih, spletnih sistemov. Bolj škodljivi računalniški virusi lahko povzročijo velike težave večjim računalniškim sistemom. V nekaj minutah ali pa urah lahko uničijo dragocene podatke (Computer virus, 2016).

Vohunska programska oprema (angl. *spyware*) je vrsta računalniškega programa, ki je na skrivaj nameščena na računalnik osebe, z namenom razkrivanja osebnih podatkov lastnika, vključno s seznamom vseh obiskanih spletnih strani in gesel ter številk kreditnih kartic, preko interneta. Vohunski programi ponavadi najdejo pot do uporabnikovega računalnika preko nameščene programske opreme, kot so računalniške igre, sistemski pripomočki iz tretjih virov, ki so jim napadalci spremenili namembnost (Spyware, 2009).

Računalniški črv je računalniški program, ki je zasnovan tako, da se naprej prepisuje v druge računalnike. Za razliko od računalniškega virusa, ki okuži druge programe z namenom, da se prenaša naprej, so računalniški črvi popolnoma neodvisni od računalnika, ker ne potrebujejo gostitelja in se prenašajo po omrežju brez človeške pomoči (Computer worm, 2015).

Trojanec oziroma trojanski konj je zlonamerna programska oprema, ki je zamaskirana kot legitimno koristen program. Enkrat, ko je nameščen na uporabnikov računalnik, omogoča napadalcu oddaljen dostop do uporabnikovega računalnika in ga uporablja za razne škodljive in nezaželene dejavnosti. Predstavlja resno grožnjo za nič slutečega uporabnika. Oseba namesti trojansko aplikacijo, ponavadi preko e-pošte, spletne strani in tako omogoča dostop skozi zadnja vrata (angl. *backdoor*) napadalcu. Računalnik postane zombi, ki omogoči napadalcu, opravljanje vseh dejavnosti na računalniku, ki bi jih lahko opravljal uporabnik. Na tisoče takšnih programov je v obtoku in se uporabljajo za različne škodljive namene, od brisanja podatkov na trdem disku, iskanja podatkov, gesel, pošiljanja nezaželene pošte preko uporabnikovega elektronskega poštnega računa (Trojan, 2008).

2.2 Kraja identitete

Kibernetski kriminal vpliva tako na virtualno, kot realno entiteto, vendar vplivi so lahko drugačni. Ta fenomen je najbolj jasen v primeru kraje identitete. V Združenih državah Amerike (v nadaljevanju ZDA) posamezniki nimajo osebne izkaznice, ampak številko socialnega zavarovanja, ki je dolgo služila kot dejanska identifikacijska številka. Davki se zbirajo na podlagi številke socialnega zavarovanja in številne zasebne ustanove uporabljajo te številke za sledenje njihovih zaposlenih, študentov, bolnikov. Dostop do podatkov o socialni varnosti posameznika lahko ponudijo priložnost zbiranja podatkov o posamezniku ter posledično, krajo identitete. Tudi ukradeni podatki o kreditnih karticah se lahko uporabijo za rekonstrukcijo identitete posameznika. Ko kiberkriminalci kradejo podatke o kreditnih karticah od podjetja, povzročijo dva večja problema. Prvo dobijo digitalne informacije o posameznikih, ki jih lahko izkoristijo na več načinov. Na primer lahko uporabijo informacije o kreditnih karticah za povzročanje kreditnega dolga, ter s tem povzročajo veliko izgubo

podjetjem ali pa prodajo te informacije drugim osebam, ki imajo podobne namene. Drugi problem, ki ga lahko ustvarijo s krajo informacij, je ustvarjanje nove identitete, ponavadi za druge kriminalce. Osebe pridobijo ponarejene dokumente (potne liste, vozniška dovoljenja). V primeru ZDA lahko oseba s ponarejeno identiteto pridobi novo kartico socialnega zavarovanja in na podlagi te lahko odpira nove bančne račune ter pridobiva razne kredite, posojila. Prvotni imetnik bančnega računa se ne zaveda, kaj se dogaja z bančnim računom, dokler ga banka ne obvesti, da je dolg že velik. Šele po tem se ugotovi, da je bila oseba žrtev kraje identitete.

Čeprav se kraja identitete dogaja skoraj v vsaki državi, imajo organi težave pri razkrivanju storilcev. Čeprav naj bi z uporabo interneta svet bil bolj povezan, v primeru organov pregona ni tako. Še vedno je premalo informacije o kibernetskem kriminalu ter njegovih statistikah. Interpol, mednarodna policijska agencija, še vedno ni dodalo nobene vrste kibernetskega kriminala vključno s krajo identitete v svojo letno statistiko kriminalnih dejavnosti. Kibernetski kriminal moramo dojemati kot mednarodni problem, saj s časom postaja vedno bolj problematična tema (Dennis, 2016). Kraja identitete je ena izmed najpogostejših vrst kibernetskega kriminala. Pojem kraje identitete se uporablja, kadar se neka oseba predstavlja z drugo identiteto z namenom ustvarjanja prevare ali pa finančne koristi. Ko se to stori preko interneta se to imenuje internetna kraja identitete. Najpogostejši viri za krajo podatkov o identiteti so državne spletne strani. Seveda so lahko vir tudi zasebne spletne strani, ki vsebujejo pomembne podatke, kot so podatki o kreditnih karticah, naslovi, elektronska pošta (Khanse, 2014). Na kratko povzamemo, za kaj lahko hekerji oz. kiberkriminalci uporabijo vaše nezakonito pridobljene podatke, infomacije (Australian Cybercrime Online Reporting Network, 2014):

- prevarajo vašo banko ali pa finančno institucijo, da jim omogočijo dostop do vašega denarja in drugih računov,
- odprejo nove bančne račune in ustvarijo velike dolgove, vse na vaše ime,
- prevzamejo nadzor nad vašimi računi, vključno s spreminjanjem naslova prejema bančnih izpiskov za vašo kreditno kartico ali pa za druge račune in tako preprečijo, da bi bili obveščeni o spremembah,
- sklenejo telefonske, internetne ali kakšne druge storitve na vaše ime,
- zahtevajo državne bonitete, pomoči, vračilo davkov na vaše ime,
- uporabljajo vaše ime za načrtovanje in izvajanje kriminalne dejavnosti, ter da vas predstavljajo in spravljajo v zadrego, na primer preko socialnih medijev.

Ni se težko izogniti kraji identitete. Vse kar moramo storite je, da bodimo previdni in imeti malo zdrave pameti, ko se ukvarjamo z ljudmi tako v virtualnem, kot realnem svetu. Ne odgovarjamo na elektronsko pošto, ki pravi, da smo zadeli na loteriji, v kateri sploh nismo sodelovali. Podjetja ne morejo dobiti našega elektronskega poštnega naslova (v nadaljevanju e-poštnega naslova) tako enostavno oziroma ga sploh ne morejo dobiti. Čeprav mogoče takšne prevare delujejo enostavne za razkrinkati, so ljudje še vedno naivni, posebej tisti, ki jim je denar pri srcu. Ni nikakršnih vdov, umirajočih ljudi, ki bi nujno potrebovali vašo

pomoč, za prenos denarja v nevladne organizacije v vaši državi. Družb, ki so pripravljene posoditi denar vsem ljudem po svetu, brez kakršnegakoli zavarovanja ni. Zato, če dobimo takšne vrste sporočilo, ga je najbolje takoj izbrisati. Priporočeno je, da se nakupuje samo preko zanesljivih, zaupanja vrednih spletnih strani. To nam, da vedeti ikona ključavnice zraven spletnega naslova, v orodni vrstici spletnega brskalnika. Seveda v današnjem obdobju interneta, se vsak dan pojavljajo nove spletne trgovine in moramo biti še posebej previdni preden nakupujemo. Pred nakupom prebrskamo še malo po internetu za dodatne informacije o spletni trgovini. Ne odgovarjamo neposredno na spletne ponudbe za delo, na primer moramo jim poslati svoj življenjepis, pa tudi če gre za zanesljiva podjetja. Danes lahko vsak ustanovi svoje podjetje in išče zaposlene. V tem primeru je tudi priporočeno poiskati dodatne informacije o podjetju oziroma, če nudijo delovno mesto. Če pa za vašo zaposlitev potrebujejo bančne podatke, je to že en znak, da gre za prevaro. Čeprav smo lahko iskalci zaposlitve je vseeno boljše, da naredimo še malo več raziskovanja, da se res prepričamo, da gre za legitimno podjetje. Bolje biti dodatno previden, kot pa preveč zaupljiv, ker se nam to lahko to v prihodnosti maščuje. Priporočljivo je, da preverjamo bančne izpise ter smo v stiku z bankami, da preprečimo krajo denarja z svojega bančnega računa oziroma, če se je kaznivo dejanje zgodilo, da čim prej ukrepamo. Pohlep in želja po hitro pridobljenemu denarju sta najpogostejša razloga, da ljudje postanejo žrtve prevar. Zato je priporočljivo, da nadzorujemo naše navdušenje nad možnostjo za lahek zaslužek. Preden kliknemo na povezavo, datoteko v elektronski pošti (v nadaljevanju e-pošta) ali pa sejo klepeta je bolje preveriti, če gre za zanesljivi vir (Khanse, 2014).

2.3 Nezaželena elektronska pošta

Nezažalena elektronska pošta (angl. *spam*) je elektronska nezaželena, nenaročena pošta, poslana po e-pošti, telefonskih sporočilih, brez privolitve prejemnika. Tovrstna sporočila ponujajo razne nagrade, poceni izdelke, obljube o lahko pridobljenem denarju. Včasih moramo za včlanitev plačati vstopnino, poklicati ali pa poslati tekstovno sporočilo na telefonsko številko, ki nam zaračuna poslano sporočilo (Australian Cybercrime Online Reporting Network, 2014). Pojav e-pošte je ustvaril enega izmed najpogostejših oblik kibernetskega kriminala, spama ali drugače povedano nenaročenih izdelkov in storitev. Strokovnjaki ocenjujejo, da približno 50 % vse elektronske pošte, ki kroži po internetu, nezaželene. Pošiljanje nezaželene pošte je zločin proti vsem uporabnikom interneta, saj nezaželena pošta ovira tako shranjevalne kot omrežne zmogljivosti ponudnikov internetnih storitev. Ob tem so pa lahko sporočila še vsiljiva in žaljiva. Kljub številnim poskusom, da bi z zakonodajo izkoreninili nezaželeno pošto, še vedno ni jasno, kako bi tovrstene napade mogoče bilo odpraviti brez kršitve svobode govora v današnjem demokratičnem svetu.

Za razliko od reklamnih oglasov, kjer vsak oglas nekaj stane, nezaželena pošta je za storilce praktično brezplačna, saj plačajo isto, če pošljejo 10 sporočil ali pa 10 milijonov sporočil. Še ena težava, ki se pojavi je, kako ustaviti pošiljatelje nezaželene pošte, saj spamerji pošiljajo pošto preko osebnih računalnikov, drugih ljudi, ki se sploh ne zavedajo, da je njihov računalnik uporabljen za zlonamerne namene. Ponavadi okužijo številne naprave, ki so

povezane z internetom, z virusoma ali drugače povedano trojancem in si tako pridobijo tajni nadzor. Okužene naprave imenujemo zombi računalniki in celotno omrežja takih računalnikov, ki jih je na tisoče, lahko storilci aktivirajo in preplavijo internet s spam pošto ali pa da sprožijo napade z namenom oviranja storitev. Medtem ko je spam pošta neškodljiva, saj nagovarja kupca k nakupu legalnega blaga, so napadi z namenom oviranja storitev uporabljeni za izsiljevanje lastnikov spletnih strani. Strokovnjaki menijo, da ena četrtina vseh zombi računalnikov prihaja iz ZDA in da te računalniki predstavljajo izvor ene tretjine nezaželene pošte (Dennis, 2015). Nezaželena pošta se je v zadnjih letih razširila v vse oblike digitalnega komuniciranja. Povečanje baze uporabnikov socialnih omrežij, kot so Facebook, Twitter, YouTube so odprle nove možnosti za pošiljatelje nezaželene elektronske pošte. Zakonodaja omogoča svobodno pošiljanje nezaželene pošte in s pojavom socialnih medijev, napadalci to s pridom izkoriščajo. E-poštni naslovi in spletni iskalniki so bili v preteklosti glavna tarča, kiberkriminalcev in boj proti nezaželeni pošti je bil usmerjen v te dve platformi. Socialna omrežja so po naravi precej drugačna od včasih glavnih tarč in imajo drugačno oblike nezaželene pošte in hekerji uporabljajo različne tehnike napadov. Poleg tega se z nenehnim in hitrim razvijanjem socialni medijev, sama nezaželene pošte razvijaja tako hitro in predstavlja veliko grožnjo skupnosti. Čeprav je nezaželena pošta na socialnih medijih relativno nov pojem, je prišlo do številni napadov in z razvojem socialnih platform bo takšnih napadov samo še več. Nezaželena pošta je neizogibna skoraj v vseh oblikah spletnih komunikacij in ovirajo produktivnost medijev, v katerih se prikazujejo. Sprejeti so bili različni ukrepi za povečanje robustnosti različni elektronskih medijev pred številnimi poštnimi napadi, vendar zaradi mladosti socialnih medijev niso še dovolj uspešni (Manajit, Sukomal, Rahul, & Ravindranath, 2016).

2.4 Socialni inženiring

Socialni inženiring je postal resna grožnja virtualnim skupnostim in je učinkovito sredstvo za napad na informacijske sisteme. Storitve, ki jih današnji zaposleni uporabljajo, so odlična podlaga za napade tega tipa. Naraščajoči trend prinašanja svojih naprav (angl. *BYOD-bring your own device*) in uporaba spletnih komunikacijskih orodij v zasebnem in službenem okolju samo še poslabša položaj. Zmanjšanje osebnih interakcij v kombinaciji z mnogimi orodji za komunikacijo (e-pošta, Dropbox, Skype) ustvarjajo nove možnosti za napade tipa socialnega inženiringa. Napadi na podjetje, kot je New York Times ter agencijo RSA so pokazali, da so napadi ribarjenja s kopjem učinkoviti in ustvarjajo naprednejše oblike socialnega inženiringa. Napadi so postali nevarno orožje, ki jih pogosto uporabljajo tehnološko napredne grožnje. Socialni inženiring je umetnost pridobivanja uporabnikov, da ogrozijo informacijske sisteme. Namesto tehničnih napadov na sisteme socialni inženirji ciljajo na ljudi, ki imajo dostop do informacij, z njimi manipulirajo in jih prisilijo v razkritje zaupnih informacij, ali pa celo prepričajo, da opravijo zlonamerno napade. Tehniško zaščitniški ukrepi so ponavadi neučinkoviti proti takšni vrsti napada. Napadi socialnega inženiringa so večplastni in vključujejo psihološke, socialne in tehnične vidike, ki se uporabljajo v različnih fazah dejanskega napada (Krombholz, Hobel, Huber, & Weippl, 2014). Poznamo več oblik, tehnik socialnega inženiringa. Če napadalcu uspe vdreti v e-poštni račun posameznika, imajo dostop

do kontaktov te osebe, ampak ker večina ljudi uporablja eno geslo povsod, imajo napadalci tudi dostop do posameznikovih kontaktov, ki jih ima na socialnih omrežjih. Ko imajo napadalci e-poštni račun pod kontrolo, začnejo pošiljati elektronska sporočila (v nadaljevanju e-sporočila) vsem kontaktom. Sporočila lahko vsebujejo razne dokumente, slike, ki vsebujejo zlonamerno programsko opremo ter razna sporočila o tem, da je prvotni lastnik e-poštnega računa v težavah. Ena od tehnik socialnega inženiringa je ribarjenje. Za to tehniko je značilno, da napadalec pošlje e-poštno ali pa telefonsko sporočilo, ki naj bi prihajalo od legalnega, zakonitega podjetja, banke, šole, itd. Ker je ta tehnika socialnega inženiringa najbolj priljubljena, jo bom pozneje v zaključni nalogi še podrobnejše opisal. Ena izmed tehnik socialnega inženiringa je tudi scenarij vab. Takšne oblike vidimo predvsem na spletnih mestih, ki ponujajo prenos nečesa, ponavadi najnovejših filmov ali glasbe. Vendar pa jih vidimo tudi na socialnih omrežjih, zlonamernih spletnih straneh in celo, kot rezultat iskanja. Napadalci prikažejo spletno stran, ki imajo izjemne ponudbe, po nizkih cenah. Ljudje, ki nasedejo na vabe, so okuženi z zlonamerno programsko opremo, ki lahko izkoristi tako žrtve, kot njihove kontakte. Žrtve ponavadi izgubijo denar, ne da bi izdelke prejeli in če so dovolj nepazljivi in plačajo s čekom, lahko najdejo svoj bančni račun prazen (Webroot, 2011).

Poleg omenjenih, standardnih tehnik socialnega inženiringa postaja vse bolj popularna strašilna tehnika (angl. *scareware*). Napadalec prevara žrtev, da je njegov, njen računalnik okužen z zlonamerno programsko opremo ali pa, da je prenesel nezakonito vsebino. Napadalec nato ponudi žrtvi rešitev, ki bo popravila lažne težave, v resnici pa je žrtev napeljana v namestitev programa, ki je v resnici, zlonamerna programska oprema napadalca (Rouse, 2016). V napadu napadalec ustvarja pojavna okna, ki so podobna opozorilnim oknom operacijskega sistema. Takšna prevarantska okna prevarajo uporabnika, da si prenese zlonamerni program in popravi domnevne napake. Program lahko vključuje klik funkcijo, ki preusmeri uporabnika na napadalčevo spletno stran ali pa sproži prenos zlonamernega programa, če uporabnik poskuša zapreti pojavno okno. »Rešilni« program prisilni uporabnika tudi v odstranitev legitimnega protivirusnega programa. Če se pojavi sumljivo pojavno okno, je priporočeno, da uporabnik preko upravitelja opravil (angl. *task manager*) prekine postopek brskalnika. Program okuži uporabnike in njihove računalnike po elektronski pošti, v obliko oglasov, kjer naj bi programi, ki uporabnikov računalnik očistijo zlonamerne programske opreme. Ampak takšni programi prikažejo navidezne težave, ki naj bi jih imel računalnik (Scareware, 2011).

2.4.1 Ribarjenje

Ribarjenje (angl. *phising*) je poskus nezakonite pridobitve občutljivih informacij, ko to uporabniška imena, gesla, podatki o kreditnih karticah z namenom izkoriščanja uporabnikov. Kiberkriminalci se predstavljajo kot zaupanja vredne entitete. Ribarske prevare so običajno ponarejena e-poštna sporočila, ki naj bi bila poslala zakonita podjetja, organizacije, kot so univerze, banke, ponudniki internetnih storitev. Sporočila nas ponavadi usmerjajo na sleparske spletne strani, kjer nas prosijo, da vnesemo svoje osebne podatke, od ime ter priimka pa vse do številke bančne kartice. Te informacije se potem uporabljajo za krajo

identitete. Ena od vrst poskusov ribarjenja je prejem e-poštnega sporočila, ki navaja da ste prejeli sporočilo zaradi goljufivih aktivnosti na vašem računu ter da »kliknete tukaj«, da preverijo vaše podatke. Od takih vrst napadov niso zaščiteni uporabniki mobilnih telefonov, saj storilci pošiljajo iste tipe sporočil tudi na mobilne telefone (Indiana University, 2016).

Kibernetsko ribarjenje je populareno pri kiberkriminalicih, saj je preprostejše ukaniti nekoga, da klikne na zlonamerno povezavo za vstop na navidezno legitimno spletno stran, kot pa poskušati prebiti obrambo računalnika z raznimi napadi, kot je na primer napad s surovo silo (angl. *brut force*). Čeprav so nekatere e-pošte slabo napisane in jasno ponarejene, prefinjeni kiberkriminalci vse bolj uporabljajo tehnike profesionalnih tržnikov, za čim bolj učinkovite tipe sporočil, ki bi pritegnile pozornost uporabnikov elektronske pošte. Na primer, gledajo katera podjetja na Facebooku so najbolj všečkana. Ribarske kampanje so pogosto zgrajene okoli večjih dogodkov, praznikih, obletnicah ali pa izkoriščajo trenutne medijske zgodbe. Da bi tovrstna sporočila, bila videti kar se da resnična, v sporočila »ribiči« vključujejo logotipe in podatke družbe, podjetja, organizacije (Rouse, 2015).

V zaključni nalogi bom opisal dve vrsti ribarjenja, ribarjenje s kopjem (angl. *spear phising*) ter kitolov (angl. *whaling*). Ribarjenje s kopjem je poskus goljufije preko e-poštnega sporočila, ki cilja na posebne organizacije z namenom pridobitve dostopa do zaupnih podatkov. Takšne vrste napadov ne delajo naključni hekerji, ampak tisti, ki hočejo pridobiti finančno korist, poslovne skrivnosti ali pa celo vojaške informacije. Kot pri sporočilih, ki se uporabljajo pri navadnem ribarjenju tudi sporočila pri ribarjenjem s kopjem prihajajo od zanesljivega vira, ampak s to razliko, da naj bi sporočila prihajala od zaposlenih, sodelavcev, nadrejenih v lastnem podjetju. Večina ljudi je nezaupljivih, do nepričakovanih zahtev za zaupne informacije ter ne bodo razkrivali osebnih podatkov in klikali na povezave v sporočilu, razen če so prepričani, da je vir resničen, zanesljiv. Uspeh ribarjenja s kopjem je odvisen od treh stvari. Prvič se napadalci morajo predstaviti kot znan in zaupanja vreden posameznik, drugič morajo v sporočilo vključiti podatke, informacije, ki bodo potrdile resničnost posameznika, tretjič pa podati logičen zahtevek za pridobitev informacij (Rouse, 2011).

Pri kitolovu so tako kot pri ribarjenju s kopjem tarča prevare zaposleni v podjetju s to razliko, da storilci ciljajo na »velike ribe« v podjetjih, od managerjev pa vse do direktorjev. Tako kot pri vsaki ribarski prevari gre tudi tukaj za e-poštna sporočila, ki naj bi bila legitimna ter potrebovala čimprejšnji odziv. Sporočila pri kitolovskih prevarah so zamaskirana kot kritična poslovna sporočila, poslana od zakonitih poslovnih organov. Vsebina sporočila je oblikovana tako, da so prilagojena delovanju zgornjemu managementu in vzbujajo neko skrb za celotno podjetje. V ZDA je veliko direktorjev, dobilo sporočilo od Zveznega preiskovalnega urada (angl. *Federal Bureau of Investigation*), kjer so morali managerji klikniti na povezavo, da so si lahko prenesli posebno programsko opremo, ki jim je omogočala ogled sodnega poziva. In na žalost še vedno veliko managerjev nasede na takšne prevare. V tem primeru je bilo napadenih okoli 20.000 direktorjev različnih podjetij in od tega jih je 2.000 kliknilo na povezavo. V resnici je bila škodljiva programska oprema, iskalnik ključev (angl. *key logger*),

ki na skrivaj snema gesla, ki jih vnašajo direktorji. Ta gesla so nato kiberkriminalci uporabili za kraje podatkov, informacij, denarja. V tem primeru prevare so bila oškodovana vsa podjetja, katerih direktorji, so kliknili na povezavo (Gil, 2016).

2.5 Hekanje

Heker je oseba, ki nepooblaščeno vstopa v računalniški sistem. Z vdorom v sistem lahko povzroči veliko škode. Večina hekerjev vdira v sisteme, ker jim to predstavlja neki izziv, ampak vseeno moramo biti previdni, saj nekateri hekerji vdirajo v sisteme, da bi pridobili neko finančno korist. Samostojni osebni računalniki so običajno varni, saj ni neke povezave, po kateri bi lahko hekerji vdrli. Računalniki, ki pa so del omrežja ali pa tisti z zunanjimi povezavami, kot so na primer modemi, so tarča napadov. Mnogi hekerji ne nameravajo povzročiti škode ali pa ukrasti podatke, samo uživajo v vdoru v sistem. Vendar v nekaterih primerih je lahko namen hekerjev, goljufija, kraja podatkov ali pa poškodovanje in brisanje podatkov z namenom škodovanja podjetju. Mogoče je težko verjeti, vendar je večina napadov izvedena s strani zaposlenih, ki imajo neko zamero do podjetja ali pa hočejo na hitro priti do denarja. Seznanjeni so z vsemi gesli in uporabniškimi podatki, imeni, zaradi česa je preprosto vdreti v sistem (Teach ICT, 2009).

V računalniškem omrežju se za hekanje smatra vsak tehnični napor manipuliranja normalnega delovanja omrežnih povezav in povezanih sistemov. Izraz hekanje je nekoč pomenilo konstruktivno, pametno tehnično delo, ki ni bilo nujno v zvezi z računalniškimi sistemi. Danes pa so hekerji najpogosteje povezani z zlonamernimi programskimi napadi na internetu in drugih omrežjih. Zlonamerni napadi na računalniška omrežja se imenujejo pokanje (angl. *cracking*), medtem ko se hekanje navezuje samo na dejavnosti, ki imajo dobre namene. Večina ne tehničnih ljudi ne vidi razlike med njima. Zunaj akademskih krogov izraz hekanje pogosto enačijo s pokanjem, ubistvu ljudje sploh ne poznajo tovrstnega izraza. Vdori v računalniška omrežja velikokrat potekajo preko skript ali drugih oblik omrežnega programiranja. Ti programi manipulirajo s prehodom podatkov preko omrežja, z namenom pridobivanja informacij o tem, kako ciljni sistem deluje. Veliko vnaprej pripravljenih skript je objavljeno na internetu, za vsakogar, ponavadi za hekerje, ki so šele začeli s hekanjem. Bolj izučeni hekerji lahko te skripte preučijo in spremenijo te skripte ter jih uporabijo za razvoj novih metod. Nekaj visoko usposobljenih hekerjev dela za komercialna podjetja z namenom varovanja programske opreme in podatkov od zunanjih hekerjev. Tehnike pokanja na omrežjih vključujejo črve, napade z namenom zavrnitve storitve ali pa vzpostavljanje nepooblaščenih povezav za oddaljene dostope do naprav. Učinkovito hekanje zahteva kombinacijo tehničnih veščin in osebnostnih lastnosti. Sposobnost dela s številkami in dobro znanje matematike, hekanje pogosto zahteva razvrščanje velike količine podatkov, kode in računalniških algoritmov. Dober spomin in logično sklepanje sta nujno potrebni veščini hekerja, saj morajo sestavljati dejstva ter podatke, ki temeljijo na tem kako računalniški sistem dela in so ključna sestavina dobrega napada. Potrebna je tudi velika mera potrpežljivosti, saj vdori so zelo zapleti in zahtevajo veliko časa (Mitchell, 2009). Hekanje lahko smatramo kot sistematično, naporen proces, v katerem napadalec poskuša najti

računalniški sistem, ugotoviti njegove ranljivosti in na podlagi teh ranljivosti pridobiti dostop. Strokovnjaki so opredelili šest korakov, ki si sledijo v procesu hekanja.

Prvi korak se imenuje odtis (angl. *footprinting*). Cilj je zbrati informacije, ki so bistvene za napad in omogočajo napadalcu pridobiti popoln profil organizacije. V tej fazi lahko heker pridobi informacije o lokaciji podjetja, telefonskih številkah in imenih zaposlenih, varnostnih politikah ter ciljnem omrežju. Te informacije pridobijo zelo lahko, saj potrebujejo samo spletni brskalnik ter telefon. Na žalost so ljudje še zmeraj najšibkejši varnostni člen v družbi. Pameten telefonski klic na oddelek za tehnično pomoč lahko ogrozi varnost pomembnih informacij.

Drugi korak, ki sledi v procesu hekanja, se imenuje skeniranje (angl. *scanning*). Hekerji opravijo skeniranje, da bi dobili podrobnejši pregled nad omrežjem družbe in da bi razumeli, kateri računalniški sistemi in storitve so v uporabi. V tej fazi se ugotavlja, kateri sistemi so dosegljivi preko interneta. Najbolj pogoste tehnike skeniranja sta preverjanje odzivnost omrežja (angl. *network ping sweep*) ter preverjanje računalniških vmesnikov (angl. *port scan*) Preverjanje odzivnosti omrežja omogoča napadalcem, da določijo, kateri računalniki so v omrežju in potencialne tarče za napad. Preverjanje računalniških vmesnikov se uporablja za ugotavljanje, kateri vmesniki so povezani z določenim računalnikom.

Tretji korak imenujemo številčenje (angl. *enumeration*). Tretja faza je postopek ugotavljanja uporabniških računov ter slabo zaščitenih računalniških virov. V tem koraku se heker poveže z računalniki v ciljnem omrežju in brska po sistemu s ciljem pridobitve čim večje količine podatkov. Medtem ko lahko fazo skeniranja primerjamo kot trkanje po vratih, da preverimo, ali so vrata odprta, lahko številčenje primerjamo kot vstop v pisarno ter brskanje po omarah in predalih.

Četrti korak hekanja se imenuje penetracija (angl. *penetration*). V tej fazi napadalec skuša pridobiti nadzor nad enim ali več sistemov v omrežju. Na primer, ko je napadalec v fazi enumeracije pridobil seznam zaposlenih, lahko velikokrat ugane geslo enega ali več zaposlenih ter pridobi širši dostop do računa zaposlenega. Druga možnost je, da ko napadalec ugotovi, da ciljni računalnik deluje na zastareli in hroščasti programski opremi, ki ima napačne nastavitve. Heker lahko izkoristi znane šibke točke programske opreme in pridobi nadzor nad sistemom.

Peti korak napada je napredovanje (angl. *advance*). V tej fazi napadalec uporablja računalnike, sisteme, v katere je vdrl v koraku penetracije za dodatne napade na ciljnem omrežju. Na primer napadalec lahko vdre v bolj občutljive administratorske račune, namesti skrite (angl. *backdoor*) programe ali trojanske konje in namesti omrežne »vohače« za dodatno zbiranje informacij podatkov, ki potujejo skozi omrežje.

Zadnja faza se imenuje brisanje sledi (angl. *covering tracks*). V tej končni fazi hekerji odpravljajo vse zapise, ki dokazujejo na njegovo škodljivo dejavnost. Z brisanjem datotek,

onemogočanjem revizije sistema (skrbi za opozarjanje skrbnika v primeru zlonamerne dejavnosti) in skrivanjem datotek ki so mu omogočile vdor, lahko heker zabriše svoje sledi in se izogne odkritju. Heker lahko lahko namesti korenski komplet programov, ki nadomestijo obstoječe sisteme programske opreme in s tem izbrišejo svoje sledi in zbirajo nove informacije (Nachenberg, 2005).

2.6 Napadi za zavrnitev storitev dobavitelja vsebin ali dostopa do interneta

Ena od najbolj pogostih oblik kibernetskih groženj je zavrnitev storitve (angl. *denial of service,* v nadaljevanju DoS), ki že, ko samo ime pove, naredi spletno stran ali pa druge spletne storitve nedosegljive za uporabnika. DoS napadi potekajo v različnih oblikah. Nekateri so neposredno usmerjeni v osnovno strežniško infrastrukturo, medtem ko nekateri izkoriščajo ranljivosti v aplikacijah in komunikacijskih protokolih. Za razliko od drugih vrst virtualnih napadov, ki so začeti zato, da bi pridobili koristne informacije, DoS napadi ne temeljijo na kršenju uporabnikove zasebnosti. S takimi napadi hočejo kiberkriminalci narediti spletne strani in strežnike nedosegljive za uporabnike. V nekaterih primerih se napadi za zavrnitev storitev uporabljajo, kot dimna zavesa za druge zlonamerne dejavnosti in za sesutje varnostnih naprav, požarnih zidov. Uspešen DoS napad je zelo opazen dogodek, ki vpliva na celotno bazo uporabnikov in lahko traja več dni, tednov celo mesece ter lahko je zelo vseuničujoč za katerokoli spletno organizacijo (Incapsula, 2011).

DoS napade je mogoče izvršiti na več načinov. Osnovne vrste DoS napadov vključujejo, poplave omrežij z namenom preprečevanja omrežnega prometa, motenje povezave med dvema napravama, strojema, s čimer uporabnikom interneta preprečujejo dostop do internetnih storitev. Poleg neposrednega napada na omrežne naprave, se uporablja smurf napad. Takšen napad vsebuje e-pošto s samodejnim odgovorom. Napadalec pošlje številna e-poštna sporočila različnim ljudem in za povratni e-mail naslov, navede e-poštne naslove zaposlenih v organizaciji. S tako obliko napada se lahko osredotočijo na posameznika in mu preplavijo e-poštni račun. DoS napadi lahko povzročijo naslednje težave: neučinkovite spletne storitve, nedostopne spletne storitve, motnje spletnega prometa v omrežju, motnje povezave (Denial of Service Attack, 2011).

Velike razlike med navadnimi DoS napadi in napadi za porazdeljene zavrnitve storitev (angl. *distributed denial of service,* v nadaljevanju DDoS) ni. Pri DoS napadih se uporablja en računalnik in en priključek za preplavitev internetnega strežnika s paketi (TCP/UDP). Cilj takega napad je preobremeniti pasovno širino ciljnega strežnika in drugih virov. Tako bo strežnik nedostopen drugim in spletna stran bo blokirana. V večini pogledov je DDoS napad podoben DoS napadu, vendar je rezultat napada, precej drugačen. Namesto enega računalnika in ene internetne povezave, DDoS napadi vsebujejo veliko računalnikov in veliko povezav. Računalniki, ki so vključeni v tak napad, so pogosto razporejeni po celem svetu in so sestavni del večje celote imenovane botneti. Botneti ali zombiji so računalniki, ki so bili napadeni, v večini primerov z virusom in so upravljeni z neke oddaljene lokacije. Takšni računalniki so nato uporabljeni za ustvaritev velikega prometnega toka, ki je potreben za DDoS napad. Z

večino botnetov hekerji trgujejo in si jih izmenjavajo med seboj, tako da je lahko tak sistem računalnikov pod nadzorom več kiberkriminalcev, ki imajo vsak svoj namen. Nekateri napadalci lahko uporabljajo botnete kot spam-releje, drugi, da delujejo kot internetne strani z zlonamerno programsko kodo, tretji za gostitev phising napadov ali pa za že zgoraj omenjene DDoS napade. Glavna razlika med DDoS in DoS napadi je torej, da bo ciljni strežnik preobremenjen s tisoče zahtevkov, saj bo napaden z več računalnikov. Zato je veliko težje za spletni strežnik, da vzdrži DDoS napad v nasprotju s preprostejšim DoS napadom (Monsum, 2014). Celotni proces DDoS napada je razdeljena na tri faze. V prvi fazi napadalec določi tarčo napada na podlagi nekih svojih razlogov (politična, finančna korist, osebno sovraštvo). Seveda napadi so tudi odvisno od stopnje varnosti cilja napada ter količine zbranih informacij s strani napadalca. V drugi fazi sproži proces skeniranja ranljivosti, da določi vse nezavarovane sisteme. Ti sistemi so nato napadeni, ogroženi s strani botnetov oziroma zombijev. Napadalec usmerja promet skozi mrežo računalnikov z namenov zakrivanja svojih sledi. V zadnji fazi se sprožijo ukazi za napad skozi različne botnete z uporabo različnih omrežnih kanalov. Računalniki nato preplavijo žrtev napada in ovirajo storitve tako dolgo, kot napadalec želi (Karanpreet, Paramvir, & Krishan, 2015).

DDoS napadi hitro postajajo najbolj razširjena vrsta kibernetskih napadov in število takih napadov hitro narašča. Napadi postajajo vse bolj krajši, vendar se pošilja vse več paketov na sekundo in število prijavljenih napadov strmo narašča. V zadnjem četrtletju leta 2015 je bilo v povprečju 4,5 napadov vsak dan. Večje število napadov lahko pripišemo tudi ogromni rasti in uspehu omrežnih operaterjev, ki so s povečanjem števila vstopnih točk in znatnim povečanjem pasovne širine omogočili bolj škodljive, moteče DDoS napade. Nove grožnje DDoS metod so nam pokazale, da so sedanje strategije za zmanjšanje takih napadov prepočasne, predrage za vzdrževanje in ne dovolj prilagodljive za posamezne napade. Jasno je, da morajo biti strategije posodobljene in v koraku s časom (Larson, 2016). Povečanje števila DDoS napadov je dokaz, da veliko število programske opreme zastarele, saj je zelo preprosto celo za nekvalificirane hekerje, da ogrozijo številne naprave. Čeprav programsko opremo podjetje redno posodabljajo, so njihovi računalniki izpostavljeni napadalcem, ki hočejo sprožiti DoS ali pa DDoS napad (Dennis, 2016). Ampak kljub temu da strategije in ukrepi niso dovolj uspešni jih je potrebno še naprej razvijati in poskušati preprečiti, da bi takšni napadi vplivali na delovanje interneta.

DDoS obrambni sistem je sestavljen iz treh faz: preprečevanje, odkrivanje in filtriranje ter identifikacije in sledenje. Prva faza se ukvarja predvsem z zmanjšanjem verjetnosti napada, bodisi s krepitvijo varnosti različnih sistemov z nadgradnjami, posodobitvami ali pa s stalnim spremljanjem omrežnega prometa. Sicer se ne moremo zaščititi pred škodo takih napadov, ker ima internet številne ranljive sisteme, katerih bi jih moralo biti čim manj, ampak z večanjem števila uporabnikov interneta, je vse več. Ko se začne napad, je pomembno, da se zmanjša učinek v čim krajšem času. Učinkovitost te druge faze je odvisna od sposobnosti sistema za odkrivanje, da izloči napadalčeve pakete. Tretja faza je identifikacija vira napada in poti, povezav, po katerih se napad odvija. Proces identifikacije se opravlja že med napadom in tudi, ko je napad konec. S takim sledenjem lahko odkrijejo napadalce in katere poti so uporabili. S

tem lahko tudi zmanjšajo verjetnost prihodnjih napadov (Karanpreet, Paramvir, & Krishan, 2015).

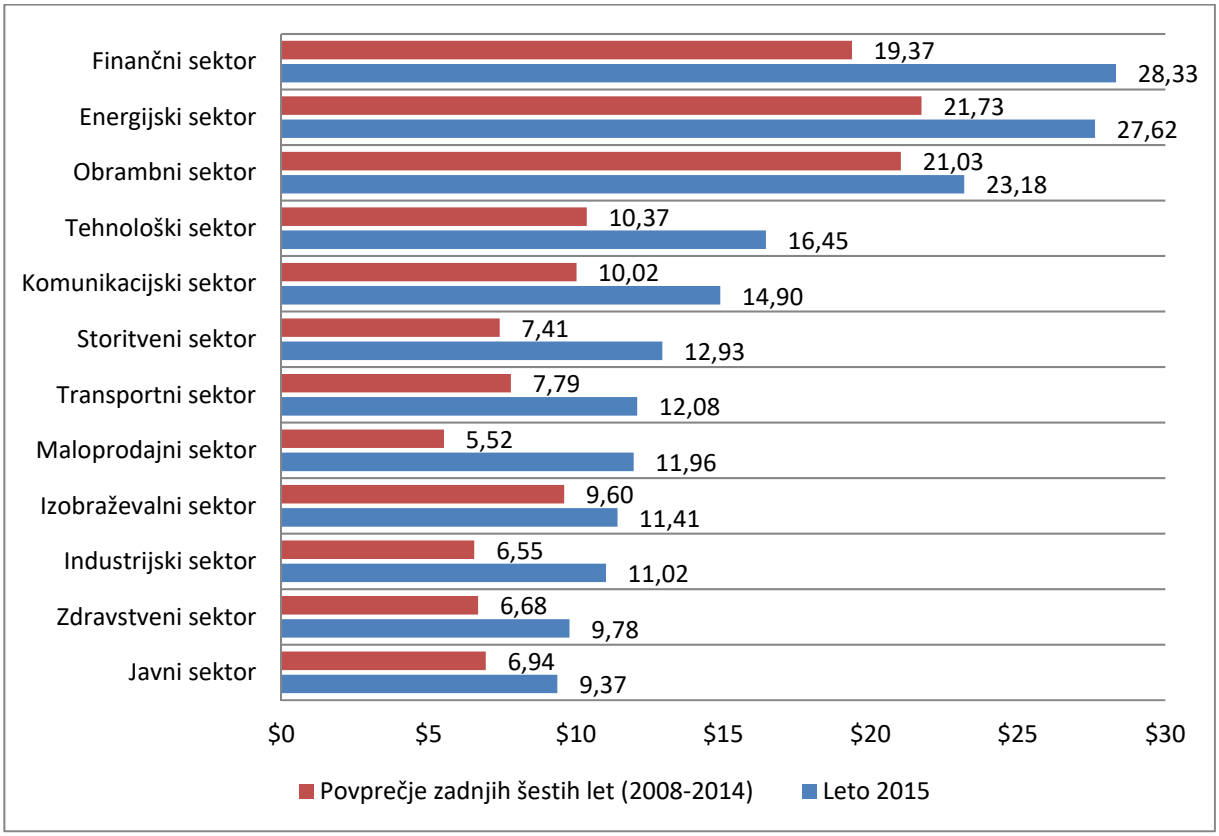
3 VPLIV KIBERNETSKEGA KRIMINALA NA GOSPODARSTVO IN NA POSLOVANJE PODJETIJ

Kiberkriminaliteta je v zadnjem času postala rastoča industrija. Donosi so veliki, tveganja so nizka. Ocenjeno je, da so letni stroški, ki jih povzroči kiberkriminal svetovnemu gospodarstvu, okoli 400 milijard ameriških dolarjev. Sicer je to približek, ker v resnici nihče ne more izračunati in oceniti kolikšen je ta strošek. Ocena od 400 milijard je najbolj optimistična, saj nekateri izvedenci trdijo, da je ta številka mnogo večja, okoli 570 milijard ali pa manjša okoli 375 milijard (McAfee, 2014). Glavni razlog, zakaj se ocene tako razlikujejo, je, da podjetja, ki so žrtve napada molčijo. Nekatere institucije so redkobesedne, ko pride do govora o kraji podatkov iz strahu, da bi pritegnili pozornosti nase. Če vzamemo v račun optimistično vrednost (400 milijard ameriških dolarjev), je to še zmeraj vrednost, ki presega tržno vrednost podjetij, kot sta Microsoft, Exxon ter je tik za petami giganta Appla. Če smo zelo konservativni in vzamemo najmanjšo številko stroška za realen podatek, je ta številka večja kot nacionalni dohodek večine svetovnih držav. Če povemo drugače, lahko štejemo spletni kriminal kot 23. največja gospodarstvo na svetu in premaga državi, kot sta Avstrija ter Iran. Če bi vzeli kiberkriminal, kot industrijo v ZDA bi bila ta večja kot ena izmed njihovih največjih industrij, nafte ter plina. V zadnjih petih letih se je mediana stroškov spletnega kriminala povečala za skoraj 200 %. Kiberkriminal ne postaja samo večji, temveč tudi vse pogostejši ter obsežnejši. Ne povzročijo samo finančne škode podjetjem, ampak tudi vplivajo na sloves podjetja. Čeprav je tema spletnega kriminala razširjena med podjetji, podjetja naredijo še vedno premalo, kar se kaže v vse večjem številu napadov na podjetja, organizacije (Warren, Favole, Haber, & Hamilton, 2016).

Vlade in podjetja podcenjujejo kibernetski kriminal in kakšno škodo povzroča ter kako hitro lahko tveganje naraste. Strošek kiberkriminalitete vključuje milijone oseb, ki so jim bili ukradeni osebni podatki. 40 milijonom ljudi v ZDA je bilo žrtev kiberkriminalcev, 54 milijonov v Turčiji, 16 milijonov v Nemčiji, 20 milijonov na Kitajskem. Po nekaterih ocenah je skupaj več, kot 800 milijonov posameznikov v letu 2013 bilo tarča kiberkriminala. Samo stroški napadov na posameznike, bi lahko znašali okoli 160 milijard dolarjev na leto. Sicer hekerji imajo še vedno težave pri preoblikovanju ukradenih podatkov v nekakšno finančno korist. Ampak številke, ki se vrtijo okoli te teme nakazujejo, da je kiberkriminaliteta ušla izpod nadzora. V razvitih državah ima kibernetska kriminaliteta resne posledice za zaposlene. Vplivi kiberkriminalitete odvračajo zaposlene od delovnih mestih, ki ustvarjajo največjo dodano vrednost. Celo majhne spremembe v bruto domačem proizvodu lahko vplivajo na zaposlovanje. Študije so pokazale, da bi samo v ZDA izgube zaradi kiberkriminalitete, lahko zahtevale 200.000, v Evropski uniji pa 150.000 delovnih mest. Skoraj dve tretjini napadov je usmerjenih na mala in srednje velika podjetja. Majhna podjetja so vse pogostejša tarča, saj lahko napadalcem predstavljajo zadnja vrata (angl. *backdoor*) v večja podjetja, z bolj vzdržljivimi sistemi (McAfee, 2014). Podatki kažejo, da se je 63 % malih podjetij in 60 %

srednje velik podjetij soočilo z zlonamerno programsko opremo v zadnjih 12 mesecih. To vključuje viruse, črve, trojance. Poleg tega jih je 60 % doživelo napade z nezaželeno pošto, 44 % ribarske napade ter 24 % DoS napade. Tudi kibernetsko vohunjenje predstavlja težavo, saj je eno izmed petih srednje velikih podjetij, tarča takšnega napad. Majhna podjetja so pogosto bolj ranljiva kot velika podjetja, ker imajo premalo strokovnega znanja o informacijski tehnologiji (v nadaljevanju IT). Veliko malih podjetij, zlasti najmanjših meni, da nimajo dovolj časa ali pa sredstev za vlaganje v ustrezne varnostne sisteme ter njihovo vzdrževanje, nadgradnjo. Medtem ko polovica velikih podjetij uporablja licenčne varnostne programe, 70 % anketirancev iz malih in 58 % iz srednjih podjetij verjame, da nelicenčni izdelki, zagotavljajo potrebno stopnjo zaščite. Med tistimi, ki pa vlagajo v dodatno varnost, je včasih težko razumeti, kaj vse rešitve, ki so na voljo, ponujajo in tako imajo lahko podjetja luknje v varnostnem sistemu, ker v resnici rešitev, ki so jo izbrali ni ustrezna (Emm, 2013). Iz Slika 2 je razvidno, da pri vseh panogah, sektorjih se stroški kibernetskega kriminala povečujejo. Povprečni letni strošek spletnega kriminala se razlikuje glede na segment industrije. Stroški kriminala so se znatno povečali v zadnjih sedmih letih, najbolj to velja za finančni sektor (povečali skoraj za 9 milijonov ameriških dolarjev).

*Slika 2: Povprečni strošek kiberkriminala, glede na sektor delovanja (v milijonih ameriških dolarjev)**



Legenda:* rezultati anket, ki jih je opravil Ponemon Institut v sodelovanju s 300 podjetji iz sedmih držav

Vir : Ponemon Institut, 2015 Cost of Cyber Crime Study: United States, 2015, str. 11.

Ne glede na velikost ali področje delovanja vsa podjetja morajo biti pripravljena, da bodo bili tarča kibernetskega kriminala. Prepogosto vodilni v podjetjih misljo, da so tarče napada samo velike blagovne znamke, banke, trgovine. V resnici se hekerji osredotočajo na podjetja z najšibkejšo varnostjo, ne glede na njihovo velikost. Verjetnost napada na podjetje je tudi odvisna od narave poslovanja podjetja ter v katerem sektorju deluje. Na primer finančna institucija ima velike količine osebnih podatkov o strankah in kraja teh bi predstavljala nepopisno denarno škodo. Vdori v tehnološka in farmacevtska podjetja lahko razkrijejo dragocene skrivnosti intelektualne lastnine. S pojavom spletnega kriminala se je pojavila tudi nova dejavnost, spletno zavarovanje, ki postaja vse bolj dobičkonosen posel. Za sektorje, ki obravnavajo velike količine podatkov, kot so na primer zdravstvo, prodaja ali pa tiste sektorje, ki se veliko zanašajo na digitalizirane tehnološke procese, kot so na primer telekomunikacije, obstaja velika verjetnost, da se spletno zavarujejo (McAfee, 2015). Kraja informacijskih baz in namerna motnja spletnih procesov sta največji težavi s katerima se podjetja ukvarjajo, ko je govora o kibernetskem kriminalu. Skoraj dve tretjini podjetij v vseh sektorjih in regijah so opisali kibernapade, kot »pomembno vprašanje, ki ima lahko velike posledice«. Preprečevalci napadov imajo velike težave v boju s kiberkriminalom. Skoraj 80 % uslužbencev, ki skrbijo za tehnološko plat podjetja, pravi, da ne morejo držati koraka z vse bolj izpopolnjenimi napadalci. Velike institucije ne poznajo dejstev in procesov, ki bi jim pomagali najti odgovor glede kibernetske varnosti. Od 60 podjetij iz celega sveta, ki je sodelovalo pri raziskavi jih je 60 % šele v fazi razvoja varnostnega sistema. Čeprav bi lahko rekli, da je v raziskavi sodelovalo malo število podjetij, če bi vzeli večje število podjetij rezultati ne bi bili bistveno drugačni, mogoče še slabši. V večini podjetij vodilni menijo, da je vzpostavljanje učinkovitega anti-kriminalnega sistema prevelika naložba in lahko bi rekli, da s tem poklanjajo denar napadalcem. Količina denarja, ki ga bi vložili v preventivne ukrepe je veliko manjša kot količina denarja, ki bo potrebnega za vzpostavitev normalnega delovanja po kibernetskem napadu (Chinn, Kaplan, & Weinberg, 2014).

Uvedba varnostnega sistema ima velik vpliv na podjetje. Ugotovitve kažejo, da podjetja, ki so bila tarča napadalce in uporabljajo obveščevalne varnostne sisteme, prihranijo približno 2 milijona ameriških dolarjev, v primerjavi s tistimi, ki učinkovitega varnostnega sistema nimajo. Podjetja, ki zaposlujejo strokovno varnostno osebje, lahko zmanjša stroške kibernetskih kaznivih dejanj v povprečju za 1,5 milijona ameriških dolarjev (Fougere, 2016). Vendar dober varnostni sistem ima lahko negativne učinke na poslovanje. Kontrole, ki je potrebne za zaščito proti kibernetskem kriminalu že imajo negativne efekte, na primer zmanjša se operativna produktivnost zaposlenih, zaradi kontrole izmenjave podatkov. Obstaja več scenarijev, kako bi se lahko kiber-varnostno okolje razvilo v bližnji prihodnosti. Vendar, če se bodo napadalci bolj razvijali, bili uspešnejši od branilcev, se bo proces digitalizacije razvijal občutno počasneje. V tem primeru lahko relativno majhno število uničujočih napadov zmanjša zaupanje v gospodarstvo, zaradi česar bodo vlade uvajale nove predpise in podjetja začela upočasnjevati hitrost tehnoloških inovacij. Takšen črni scenarij bi imel katastrofalne posledice na svetovno gospodarstvo. V bližnji prihodnosti bi lahko podjetja izgubila okoli 3 bilijone ameriških dolarjev, zaradi različnih ukrepov, ki bi jih podjetja sprejela. Sprejeti ukrepi bi imeli negativne vplive na produktivnost ter rast podjetij (Chinn, Kaplan, &

Weinberg, 2014). S stalnim povečevanjem odvisnosti gospodarstev od interneta, so ta vedno bolj izpostavljena grožnjam kiberkriminalcev. Delnice se prodajajo preko interneta, bančne transakcije so opravljene preko interneta, nakupi so opravljeni s kreditnimi karticami preko interneta. Vsi napadi, primeri goljufij v teh transakcijah vplivajo na finančno stanje prizadetih podjetij ter s tem na gospodarstvo (Saini, Shankar Rao, & Panda, 2012). Manipulacija tržne vrednosti delnice je področje razvoja kibernetske kriminalitete. Z vdorom v omrežje gospodarske družbe ali v omrežje njihovih odvetnikov ali računovodij, kiberkriminalci lahko pridobijo notranje informacije o prevzemih in načrtih o združitvi, prihodkovnih poročilih ter drugih podatkov, ki vplivajo na ceno neke družbe (McAfee, 2014). Takšne motnje lahko imajo velik vpliv na mednarodne finančne trge in predstavljajo resno skrb. Sodobno gospodarstvo se razteza skozi več držav in časovnih pasov. Takšna soodvisnost svetovnega gospodarskega sistema, pomeni, da motnje v eni svetovni regiji, občutijo tudi druge svetovne regije. Vsaka motnja teh sistemov pošiljala udarne valove zunanjemu trgu, ki niso vir problema. Produktivnost je v nevarnosti. Napadi v obliki zlonamerne programske opreme bodo onemogočali normalno delovanje. Stroji opravljajo svoje storitve počasneje, strežniki so nedostopni, omrežja so preobremenjena, itd. Takšni primeri napadov vplivajo na splošno produktivnost posameznika in organizacije. Vplivajo tudi na odnose s stranko, ker ta lahko to vidi, kot negativni vidik organizacije. Poleg tega lahko, zaskrbljenost porabnikov, strank zaradi možnosti potencialne goljufije, negativno vpliva na podjetja, ki ponuja svoje storitve preko interneta. Jasno je, da je velik del elektronskih poslovnih prihodkov izgubljen, zaradi oklevanja, dvoma ter skrbi glede nakupa (Saini, Shankar Rao, & Panda, 2012).

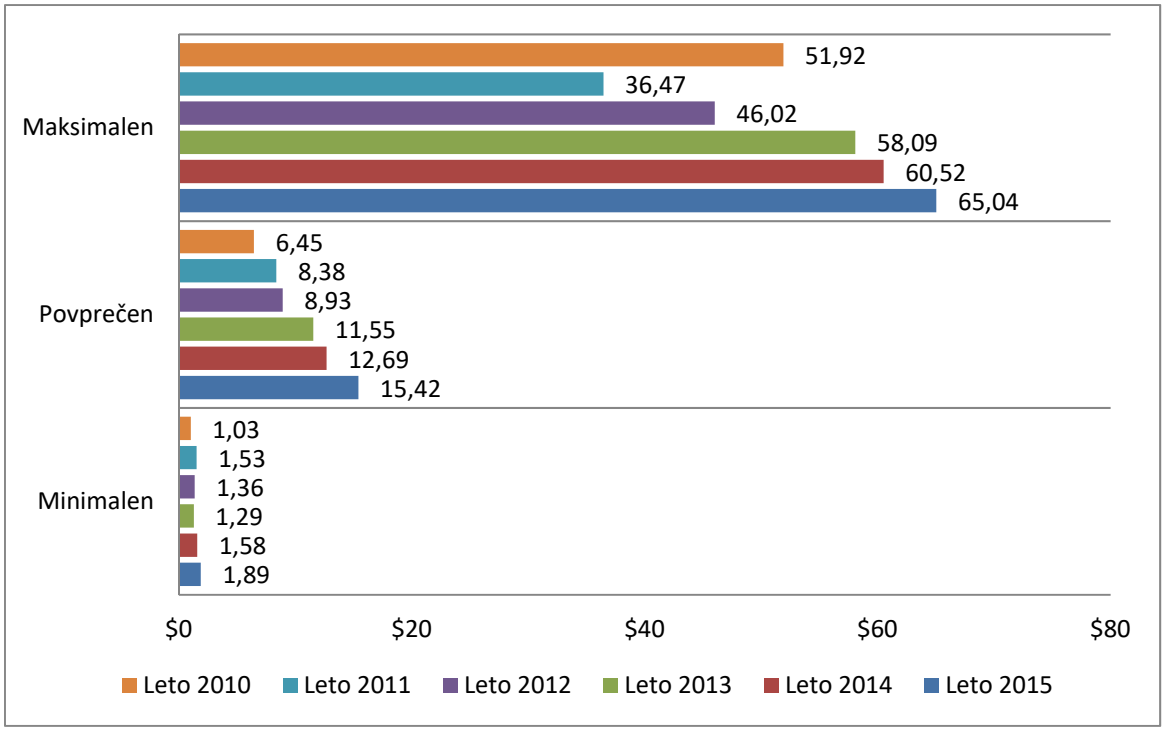
Povrnitev podjetja v stanje, ki je bilo pred kibernetskim napadom je pogosto dražje kot sam napad. Stroški okrevanja podjetij naraščajo. Medtem ko vemo, da napadalci ne bodo mogli ovrednotiti vsega kar ukradejo, se podjetja morajo obnašati, kot da imajo vsi ukradeni podatki, informacije neko monetarno vrednost. Ena od študij stroškov kibernetske kriminalitete za Italijo je pokazala, da medtem, ko je bilo dejanske izgube v višini 875 milijonov ameriških dolarjev, so oportunitetni stroški ter stroški okrevanja dosegli vrednost 8,5 milijard ameriških dolarjev (McAfee, 2014). Organizacije, ki so postale žrtve napada, bodo bile soočene s stroški na več področjih. Administrativni in obnovitveni ukrepi, vključno z obnovitvijo poslovanja organizacije, bodo predstavljali velik strošek za podjetje. Te stroške lahko dejansko imenujemo oportunitetni stroški, ker bi lahko organizacija uporabljala resurse za vsakdanje dejavnosti, ampak jih mora preusmeriti v obravnavanje napada. Podjetja se lahko soočijo tudi z izgubo intelektualne lastnine, kot so patentirane informacije, avtorsko gradivo, poslovne skrivnosti, seznami strank. Kazni, ki so lahko pravne ali zakonske (na primer kršitev varstva podatkov), izravnalna plačila za stranke (za neprijetnosti) ali pogodbena nadomestila (zaradi zamud), lahko predstavljajo velik finančni zalogaj za podjetje. Podjetja se soočijo z izgubo lastnine, ki lahko izhaja iz izgube zalog (fizične ali digitalne) ali zaradi nezmožnosti zagotavljanja storitev, lahko pa tudi zaradi kraje financ ali pa finančni prevar. Izguba ugleda, dobrega imena, tržne vrednosti cene delnic, zaupanja strank in poslovnih partnerjev, so stvari na katere organizacija ne bo mogla vplivati. Varnostne dejavnosti, ki lahko vključujejo preiskovanje napada, podpiranje varnostnih organov pri preiskovanju, omogočanje varnostnih kopij datotek in vzpostavljanje okrepljenih varnostnih

ukrepov za preprečevanje ponovitve napada so neizbežne dejavnosti, s katerimi se morajo podjetja soočiti (Boyes, 2013).

Podjetja imajo lahko zaradi kibernetskih napadov, velike izgube. Organizacije, ki so sodelovale pri raziskavi (100 podjetij), so utrpele izgube v višini več kot 5 milijonov ameriških dolarjev, od tega je skoraj tretjina poročala, da je dejanska izguba presegala 100 milijonov ameriških dolarjev. Največja težava, s katero so se soočila podjetja je bila izguba ugleda. 56 % podjetij, ki pravi, da še nikoli niso bili žrtve napadov, so lahko bili dejansko napadeni, ne da bi to sploh vedeli. Hekerji so lahko v omrežju organizacije, dolgo časa, ne da bi podjetje to odkrilo. Napadalci izvedejo napade, ki prekrivajo njihove dejanske namene. Na primer napadalec izvede DoS napad, ki je zelo moteč ter ga je lahko zaznati, z namenov prekrivanja dejanskega napada. Običajno v takem scenariju napadalec napade sistem, ki mu ne predstavlja neke vrednosti in v ozadju pridobiva podatke, ki ga dejansko zanimajo (PwC, 2016).

Slika 3 prikazuje skupni letnih strošek kibernetskega kriminala v letu 2015, ki se giblje od nizkih 1,89 do visokih 65 milijonov dolarjev. Povprečni letni strošek znaša 15,4 milijonov dolarjev in se je glede na preteklo leto povečal za 2,7 milijona dolarjev oziroma 19 %. Strošek kibernetskega kriminala se je v obdobju šestih let povečal za 82 %.

*Slika 3: Strošek kiberkriminala skozi leta (v milijonih ameriških dolarjev)**



Legenda:* rezultati anket, ki jih je opravil Ponemon Institut v sodelovanju s 300 podjetji iz sedmih držav

Vir : Ponemon Institut, 2015 Cost of Cyber Crime Study: United States, 2015, str. 6.

Obstaja seveda veliko rešitev na katera se podjetja obrnejo, da bi zaščitila svoja digitalna sredstva. Mnogi managerji še vedno verjamejo, da prodajalci programske opreme, sprejmejo vse potrebne ukrepe, da bo njihova programska oprema varna. In medtem, ko večina ponudnikov opravi veliko testiranj, imajo njihovi programi pomanjkljivosti, ki omogočajo kiberkriminalcem dostop do celotne infrastrukture vsake organizacije. Z množico programske opreme, ki se uporablja v organizacijah danes, vključno s službenimi telefoni, prenosnimi računalniki, ki se uporabljajo tako profesionalno kot zasebno, imajo napadalci različne možnosti za napad. Trend prinašanja svojih naprav v delovno okolje je v porastu. Kar 95 % organizacij sedaj dovoli zaposlenim uporabo lastnih naprav na delovno mesto. Čeprav so zaposleni bolj fleksibilni, to lahko predstavlja veliko nevarnost. Nevarnosti ne predstavljajo naprave same, ampak tudi njihovi programi, aplikacije. Ker veliko uporabnikov ne posodablja programske opreme na svojih računalnikih, IT oddelek ne ve kje je luknja, ki bi jo bilo potrebno zakrpati. Za zaščito končnih točk, ki so povezane s tehnološko infrastrukturo organizacije, je nujno potrebno opredeliti ranljivo programsko opremo in jo pokrpati, posodobiti. Posodobitev lahko odpravi številne napade. Razni programski obliži vsebujejo varnostne posodobitve, ki so zelo dobrodošle. Večina posameznikov in malih podjetij meni, da je preveč zamudno in preveč zapleteno posodabljanje programske opreme. Posodabljanje programske opreme jim ni v interesu.

Pomanjkljiva varnost končnih sistemov predstavlja največjo varnostno grožnjo podjetjem. Ranljiva programska oprema na teh končnih točkah je najbolj priljubljena tarča hekerjev in glede na to, da ljudem ni v interesu posodabljanje programov, bodo napadi na zastarelo programsko opremo, postali vse večja težava. Napadalci najpogosteje napadajo programe ponudnikov Adobe ter Microsofta (Office, Internet Explorer), ker te ponujajo nedodelane izdelke, ki potrebujejo veliko posodobitev (Eriksen-Jensen, 2013). Čeprav je vedno večje število napadov na mobilne telefone z uporabo zlonamerne programske opreme, so te še vedno v poskusni fazi in imajo majhen vpliv na uporabnike. Število mobilnih uporabnikov se strmo povečuje, vendar število napadov narašča zelo počasneje. Vrednost podatkov, pridobljenih iz pametnih telefonov je majhna. Pametni telefoni ne igrajo pomembne vloge, pri napadih na podjetje, ali pač? Napadalci napadajo mobilne telefone, da ugotovijo, kam, v kateri oblak se podatki shranjujejo. Večina mobilnih telefonov ima aplikacije, ki shranjujejo podatke v neki oddaljen oblak in dokler napadalec ne pridobi nadzora nad tem oblakom, ni zmožen povzročiti veliko škode tako uporabniku, kot podjetju. Seveda oblačne storitve niso stoodstotna zaščita pred kiberkriminalom. Če napadalec pridobi dostop do oblaka podjetja, lahko napadalec spremlja aktivnosti, poslovanje podjetja, spreminja podatke, preusmerja stranke do drugih nezakonitih spletnih strani. Priporočeno je da uporabniki mobilnih telefonov imajo na njihovih napravah nameščene anti-virusne programe ter da koristijo aplikacije, ki jih ponujajo znani ponudniki, na primer Google Play. Najbolj pogosto pot za vdor v podjetje seveda predstavljajo osebni računalniki (McAfee, 2015).

4 PRIPOROČENI UKREPI ZA ZAŠČITO PODJETIJ

Implementacija močnih gesel je najlažja stvar, ki jo lahko v podjetju naredimo, da okrepimo svojo varnostno politiko. Najboljša je uporaba gesel, ki so dolgi od 8 do 12 znakov in so kombinacija velikih, malih črk ter številk in simbolov. Pogoste besede, napisane nazaj, zaporedje številk ali pa znakov so lahko uporabljeni pri ustvarjanju močnih gesel. Priporočena je uporaba programov, ki preverjajo gesla ter njihovo možnost odkrivanja oziroma pridobivanja. Pomembno je, da se gesla spreminjajo, saj ni priporočeno, da neko geslo uporabljamo dlje časa ali pa celo na več napravah. Strokovnjaki iz informacijsko tehnološkega področja priporočajo, da se gesla spreminjajo vsakih 90 dni. Seveda ni nič narobe, če gesla spreminjamo še pogosteje. V podjetju morajo vsi zaposleni imeti svoja uporabniška imena ter gesla za vsak sistem, ki ga uporabljajo. Njihovi računalniki morajo biti povezni s Sistemom za upravljanje vsebin (angl. *Content Management System*). Ta sistem, poskrbi, ki omogoča urejanje in vzdrževanje vsebin spletnih strani. Najpomembnejše je, da si gesla nikamor ne zapisujemo, ker se nikoli ne ve, kakšni namene imajo ljudje okoli nas (Male & Bhasin, 2011).

Ogromne količine informacij so izpostavljene kibernetskim napadom, tako iz zunanjega okolja kot iz lastnega, notranjega okolja. Podjetja bodo morala razviti sposobnost združevanja ter analiziranja ustreznih podatkov in jo ustrezno uporabiti za razvoj obrambnega sistema, kot je na primer požarni zid. Da imamo ustrezno zaščiteno omrežje je uporaba požarnih zidov (angl. *firewall*) nuja. Požarni zid zaščiti omrežje podjetja z nadzorovanjem internetnega prometa, ki prihaja v in odhaja iz podjetja. So postali, kar standardni del varnostnega sistema vsakega podjetja in so ena od prvih obrambnih linij, na katero bodo naleteli kiberkriminalci, ko bodo napadli omrežno infrastrukturo organizacije. Požarne zidove lahko postavimo na različne ravni omrežne infrastrukture. Najbolje je imeti postavljen požarni zid na aplikacijskem sloju omrežja, ker poleg tega, da ima podjetje nadzor nad podatki, ki prihajajo v in odhajajo iz podjetja, podjetje ustvari tudi okolje, katerega napadalci zelo težko prebijejo z uporabo, na primer zlonamerne programske opreme. Z razvojem požarnih zidov, postajajo napadalci vse bolj izučeni zato je potrebno redno preverjanje varnosti požarnih zidov, da se zagotovi najboljša zaščita (Jang-Jaccard & Nepal, 2014).

Antivirusni programi ter drugi programi za zaščito pred zlonamerno programsko opremo, so bistvenega pomena, za ustvarjanje varnega okolja v podjetju. So zadnja linija obrambe, če se nezaželen napad prebije skozi omrežje podjetja. Zagotavljanje pravočasnega in ustreznega posodabljanja računalnikov je nujno potreben korak za celovito zaščito sistema. Nima smisla nameščati drage programske opreme, ki je ne bomo pravilno vzdrževali. Varnostne aplikacije so le tako dobre, kot so njihove zadnje posodobitve. Aplikacije niso stoodstotno varne, zato jih je potrebno redno posodabljati in s tem zaščititi njihove uporabnike. Pogosto posodabljanje programov, odpravlja varnostne luknje, ki so jih imele prejšnje verzije. Z novejšimi verzijami programov, onemogočimo napadalcem izkoriščanje osnovnih ali pa avtomatiziranih napadov v celoti in ga mogoče celo odvrnemo od napada. Če bi se

programska oprema v podjetjih samodejno posodabljala, bi bil to velik korak proti večji varnosti računalniške opreme (Male & Bhasin, 2011).

Zaradi svoje prenosne narave so prenosni računalniki, izpostavljeni večjemu tveganju, da se izgubijo ali pa, da jih nekdo ukrade kot navadi, namizni računalniki podjetja. Zato je priporočeno, da se prenosni računalnik šifrira, ker je to najboljši način zaščite. Šifriranje programske opreme spreminja način izgleda informacij, podatkov na trdem disku, ki brez ustreznega gesla ne morejo biti prebrani. Danes veliko poslovnežev, ki gre na službeno potovanje, vzame s seboj prenosni računalnik in se po vsej verjetnosti uporabljajo javno brezžično omrežje (angl. *WI-FI*). Javno internetna omrežja so lahko zelo slabo zaščitena in omogočijo lahek dostop hekerjem, do občutljivih informacij, ki se nahajajo na računalniku. Zato je priporočeno, da se izogibajo uporabi javnih omrežij in uporabljajo virtualno privatna omrežja (angl. *virtual private network*). S tem zaščitnim ukrepom, zagotovimo varnost internetnih povezav ter varnost poslanih in prejetih datotek z računalnikov, ki se nahajajo skupaj v nekem omrežju in niso nujno na isti lokaciji (Barron, 2014).

Pametni mobilni telefoni imajo toliko podatkov, da jih moramo smatrati tako dragocene, kot so računalniki podjetja. Mobilni telefoni se lažje izgubijo ter se ukradejo, zato je zaščita mobilnih naprav še ena stvar, na katero moramo biti pozorni. Tako kot pri prenosnih računalnikih je priporočena namestitev enkripcijskega, šifrirnega programa. Mobilni telefoni morajo biti zaščiteni z geslom, ki se aktivira v primeru, ko telefon ni v uporabi. Z uporabo šifriranja in zapletenih gesel se lahko ustanova osredotoči na zaščito najbolj pomembnih informacijskih sredstev. Še ena stvar na katero moramo biti pozorni pri mobilnih telefonih, je onemogočanje oddaljenega brisanja podatkov. Na primer se je zgodilo, da je direktor podjetja izgubil svoj telefon, potem ko je pregledoval četrtletna finančna poročila podjetij in v 15 minutah so tatovi popolnoma izbrisali podatke s telefona (Male & Bhasin, 2011).

Ogrozitev, izguba podatkov je boleča izkušnja, ki jo lahko preprečimo z varnostnim kopiranjem. Načrtovanje rednih varnostni kopiranj na zunanje trde diske ali v oblak, je učinkovit način, da se zagotovi, da so podatki varno shranjeni. Pri strežnikih, osebnih računalnikih je potrebno vsak teden delati varnostne kopije. Vsako podjetje mora imeti nekoga, ki skrbi za varnost vse te tehnologije, ki jo zaposleni uporabljajo. Dobro orodje za nadzorovanje je programska oprema, ki preprečuje uhajanje podatkov in se nahaja na ključnih, stičnih omrežnih točkah ter išče specifične informacije, ki prihajajo iz notranjega omrežja. Programsko opremo lahko namestimo, da išče številke kreditnih kartic, koščke kod ali pa katerekoli bite informacij, ki bi namigovali na to, da je podjetje napadeno (Devaney & Stein, 2012).

Če se stvari v podjetju ne nadzorujejo, se po nepotrebnem izgublja čas ter viri, saj podjetje ne bo vedelo, da je ogroženo, dokler ne bo prepozno. Sami zaposleni velikokrat predstavljajo največjo ranljivost za podjetje. Ni nič nenavadnega, da nič hudega sluteč zaposleni klikne na povezavo ali prilogo, ki naj bi bila po njihovem mnenju popolnoma neškodljiva in ugotovijo, da so bili okuženi z nevarnim zlonamerno programsko opremo. Povezave so najpogostejši

način prenosa zlonamernih programov na računalnik. Zato morajo biti zaposleni prepričani o izvoru e-pošte. Morajo biti pametni, ko brskajo po internetu. Vsako opozorilno okence, ki se pojavi na njihovem zaslonu morajo vzeti resno in razumeti, da vsak programska oprema ima svoj nabor varnostnih ranljivosti. Poučevanje svojih zaposlenih o varnih spletnih navadah in proaktivnih dejavnostnih je ključnega pomena. Seznanjanje s tem, kaj delajo in zakaj je to nevarno, je bolj učinkovita strategija, kot pričakovati, da se bo varnostno osebje IT oddelka nenehno odzivalo na slabe odločitve uporabnikov, zaposlenih. Vendar to ni tako preprosto. Ena izmed najtežjih stvari. je zaščititi končne uporabnike, pred samimi seboj. Ampak takšni preventivni ukrepi so najboljši pristop, za učinkovito ravnanje z varnostjo podatkov. Mora biti poskrbljeno, da zaposleni razumejo pomembnost podatkov podjetja ter kateri ukrepi so potrebni, da se jih ustrezno zaščiti (Male & Bhasin, 2011).

Bistveno je, da vključujemo veliko različnih akterjev v organizaciji, ne samo informacijsko tehnološkega oddelka ter varnostne službe. Poleg raznih managerjev je priporočljivo, da podjetje sodeluje z zunanjimi ponudniki storitve, ki preverjajo njihove varnostne sposobnosti in tako pomagajo vzpostaviti še bolj učinkovit varnostni sistem. Prav tako je pomembno, da varnostni delavci razumejo odnose v organizaciji, med njenimi zaposlenimi in informacijsko tehnologijo ter kakšne nevarnosti jim pretijo. Šele ko varnostna služba razume podjetje, kot celoto se naredi ustrezen varnostni program, ki se oblikuje in izvaja na podlagi proračuna, spretnosti, učinkovitosti, intenzivnosti in je uravnotežen na vseh varnostnih ravneh (Schwartz, 2015).

Organizacije imajo zelo malo ali pa skoraj nič proaktivnih ukrepov za spremljanje notranjih dejavnosti, ki lahko predstavljajo nekakšno tveganje. Skoraj vsi incidenti, ki so bili posledica notranjega napada, so bili storjeni zaradi dodatnih privilegijev, ki so določenim zaposlenim omogočili, da na primer sabotirajo omrežje podjetja. Managerji, ki nadzorujejo zaposlene s pooblaščenim dostopom, bi morali resno razmisliti o omejiti dostopa zaposlenim, v primeru slabe učinkovitosti ali pa kakršnekoli kršitve zaposlenega. Najbolj osnovna praksa prekinitve dostopa je, ko zaposleni zapušča podjetje in se podjetje želi obvarovati pred nepotrebnimi notranjimi napadi. Priporočeno je, da podjetja omogočijo zaposlenim uporabniške dostop in privilegije na podlagi raznih seminarjev, programov o kibernetskih grožnjah, pri katerih so sodelovali. Zaposlenim, ki niso sodelovali ni priporočeno niti, da se jim omogoči dostop do interneta. Redno opravljanje testnih napadov, na primer phising napadov znotraj organizacije ter objava rezultatov teh napadov, lahko pozitivno vpliva na ozaveščenost zaposlenih, glede zlonamernih e-poštnih sporočil. Za dodatno zaščito zaposlenim je priporočeno, da kakršnakoli e-sporočila, ki vsebujejo exe, rar kratice ne prenašajo (Pilling, 2013).

Če podjetje prodaja svoje storitve, izdelke preko interneta, morajo od kupcev zahtevati verifikacijsko kodo (angl. *Card Verification Value,* v nadaljevanju CVV). Ta tri mestna kombinacija številk, se nahaja na zadnji strani fizične kreditne kartice in lahko pomaga preprečiti številne goljufije nakupov preko spleta. Priporočeno je za podjetje, da zahteva to kodo, preden je nakup konča. CVV koda je napisana samo na fizični kreditni kartici, kar pomeni, da nekdo, ki ima samo številke kreditne kartice ne more zagotoviti CVV kode in

opraviti goljufivega nakupa. Ko gre za kibernetsko varnost, ne želimo čakati, da gre kaj narobe in šele nato ugotovimo, da naši zaščitni ukrepi ne delujejo. Nenehno testiranje, na primer požarnih zidov je odličen način, da se zagotovi, da so naši varnostni ukrepi, kar se da najboljši (Barron, 2014).

SKLEP

Kibernetski kriminal bo nadomestil klasične oblike kriminala. Vse večja škoda, ki jo povzroča kiberkriminaliteta, je realni kazalnik, da so klasične oblike kriminala v zatonu. Zakaj bi se kriminalci naprezali, če pa lahko vse storijo v udobju svojega doma. Kibernetski prostor ponuja številne možnosti kiberkriminalce, ki lahko bodisi škodujejo ljudem, podjetjem ali pa hitro pridejo do denarja, na račun nič hudega slutečega posameznika. Seznanitev z različnimi vrstami kibernetskega kriminala je ključnega pomena, da ne postanemo žrtev kiberkriminalcev. Človeški element lahko bodisi naredi ali pa uniči obrambno strategijo vsakega podjetja. Ne glede na to kakšno moderno tehnologijo podjetja uporabljajo za zaščito pred napadi, pomanjkljivo znanje zaposlenih, lahko povzroči velike luknje v varnostnem sistemu.

Ljudje, podjetja se ne zavedajo, kakšno škodo lahko povzročijo kiberkriminalci. Kdo bi rekel, da lahko en sam napad povzroči za več milijonov dolarjev, evrov škode. Nihče ne bi pomislil, da je kibernetski kriminal, posel, katerega vrednost se giblje v milijardah dolarjev in presega vrednost podjetja Microsoft in ga lahko smatramo kot 23. največje gospodarstvo na svetu. Strokovnjaki menijo, da v prihodnosti ne bomo več govorili o milijardah dolarjev škode, ampak o bilijonih dolarjev škode.

Namen diplomske naloge je bil seznaniti tako podjetja, kot slehernega posameznika o nevarnostih, ki jim pretijo v današnjem internetno povezanem svetu in o njegovih negativnih vplivih na poslovanje podjetij. Diplomska naloga je sestavljena iz štirih poglavij. V prvem poglavju sem predstavil kibernetski kriminal, kaj to sploh je, kdo je tarča kiberkriminalcev. V drugem poglavju sem opisal, v kakšnih oblikah se pojavlja kibernetski kriminal. V tretjem poglavju opisujem, kakšne vplive imajo kiberkriminalci na gospodarstvo, podjetja in na praktičnih primerih je prikazano, koliko škode lahko povzročijo posamezne vrste napadov. V zadnjem, četrtem poglavju podajam priporočene ukrepi, ki bi jih moralo vsako podjetje upoštevati, če bi hotelo imeti ustrezno zaščitni sistem.

S tem ko naša življenja postajajo vse bolj odvisna od tehnologije, postajamo vse bolj dovzetni za kibernetski kriminal in brez ustreznega znanja bo vedno več in več ljudi, podjetij postalo tarča kiberkriminalcev.

LITERATURA IN VIRI

1. Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3),183-196.
2. Aghatise, J. E. (2006, 28. junij). Cybercrime definition. *Computer Crime Research Center*. Najdeno 15. junija 2016 na spletnem naslovu http://www.crime-researc h.org/articles/joseph06/
3. Alkaabi, A., & Mohay, G. M. (2010). Dealing with the Problem of Cybercrime. *Computer Fraud & Security*, *2*(3),6-7.
4. Australian Cybercrime Online Reporting Network. (2014a, 6. november). *Email spam and phishing*. Najdeno 16. junija 2016 na spletnem naslovu https://www.acorn.gov.au/learn-about-cybercrime/email-spam-and-phishing
5. Australian Cybercrime Online Reporting Network. (2014b, 3. november). *Identity theft*. Najdeno 16. junija 2016 na spletnem naslovu https://www.acorn.gov.au/learn-about-cybercrime/identity-theft
6. Barron, B. (2014, 7. september). 7 Ways Small Businesses Can Protect Against Cybercrime. *Care.com*. Najdeno 15. julija 2016 na spletnem naslovu https://www.car e.com/a/7-ways-small-businesses-can-protect-against-cybercrime-1409673107465
7. Boyes, H. (2013, 28. avgust). News analysis: Calculating the true cost of cyber-crime. *Engineering and Technology Magazine*. Najdeno 11. julija 2016 na spletnem naslovu http://eandt.theiet.org/magazine/2013/08/news-analysis-cybercrime.cfm
8. Chinn, D., Kaplan, J., & Weinberg, A. (2014, 1. januar). Risk and responsibility in a hyperconnected world: Implications for enterprises. *McKinsey & Company.* Najdeno 7. julija 2016 na spletnem naslovu http://www.mckinsey.com/business-functions/bu siness-technology/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises
9. Computer virus. (2016, 3. marec). V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu http://www.britannica.com/technology/computer-virus
10. Computer worm. (2015, 11. september). V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu: https://www.britannica.com/technology/computer-worm
11. Cross Domain Solution. (2013, 8. marec). *Cybercrime*. Najdeno 15. junija 2016 na spletnem naslovu http://www.crossdomainsolutions.com/cyber-crime/
12. Cybercrime. (2011, 2. avgust). V *Technopedia*. Najdeno 15. junija 2016 na spletnem naslovu https://www.techopedia.com/definition/2387/cybercrime
13. Denial of Service Attack. (2011, 24. julij). V *Technopedia*. Najdeno 22. junija 2016 na spletnem naslovu https://www.techopedia.com/definition/24841/denial-of-service-atta ck-dos
14. Dennis, M. A. (2015, 15. februar). Spam. V *Encyclopedia Britannica*. Najdeno 17. junija 2016 na spletnem naslovu http://www.britannica.com/topic/cybercrime/Spam
15. Dennis, M. A. (2016, 15. februar). Cybercrime. V *Encyclopedia Britannica*. Najdeno 15. junija 2016 na spletnem naslovu http://www.britannica.com/topic/cybercrime
16. Devaney, T., & Stein, T. (2012, 17. december). 5 Ways Small Businesses Can Protect Against Cybercrime. *Forbes.* Najdeno 14. julija 2016 na spletnem naslovu

http://www.forbes.com/sites/capitalonespark/2012/12/17/5-ways-small-businesses-can-protect-against-cybercrime/#259fcac84d36
17. Emm, D. (2013). Security for SMBs: why it's not just big businesses that should be concerned. *Computer Fraud & Security*, *2013*(4), 5-8.
18. Eriksen-Jensen, M. (2013). Holding back the tidal wave of cybercrime. *Computer Fraud & Security*, *2013*(3), 10-16.
19. Fisher, T. (2016, 26. april). What is Malware. *About Tech*. Najdeno 27. junija 2016 na spletnem naslovu http://pcsupport.about.com/od/termsm/g/malware.htm
20. Fougere, N. (2016, 14. januar). What is the true cost of cyber crime? *ThisData*. Najdeno 11. julija 2016 na spletnem naslovu https://thisdata.com/blog/what-is-the-true-cost-of-cyber-crime/
21. Gil, P. (2016, 27. marec). What Is 'Whaling'? Is Whaling Like 'Spear Phishing'? *About.com.* Najdeno 17. junija 2016 na spletnem naslovu http://netforbeginners.about. com/od/scamsandidentitytheft/f/What-Is-Whaling-Spear-Phishing.htm
22. Hosch, W. L. (2009, 9. maj). Malware. V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu http://www.britannica.com/technology/malware
23. Incapsula. (2011, 14. junij). *Denial of Service Attacks?* Najdeno 22. junija 2016 na spletnem naslovu https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html
24. Indiana University. (2016, 13. junij). *What are phishing scams and how can I avoid them?* Najdeno 17. junija 2016 na spletnem naslovu https://kb.iu.edu/d/arsf
25. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(3), 973-993.
26. Karanpreet, S., Paramvir, S., & Krishan, K. (2015). A systematic review of IP traceback schemes for denial of service attacks. *Computers & Security*, *56,* 111-139.
27. Khanse, A. (2014, 9. september). Online Identity Theft: Prevention and Protection. *The Windows Club.* Najdeno 16. junija 2016 na spletnem naslovu http://www.thewind owsclub.com/online-identity-theft
28. Khanse, A. (2014, 21. november). Types of Cybercrime Acts and Preventive Measures. *The Windows Club.* Najdeno 16. junija 2016 na spletnem naslovu http://www.thewindowsclub.com/types-cybercrime
29. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22,* 113-122.
30. Larson, D. (2016). Distributed denial of service attacks – holding back the flood. *Network Security*, *2016*(3), 5-7.
31. Male, B., & Bhasin, K. (2011, 16. avgust). 10 Ways To Protect Your Business From Cyber Attacks. *Bussines Insider.* Najdeno 14. julija 2016 na spletnem naslovu http://www.businessinsider.com/10-ways-to-protect-your-business-from-cyber-attacks-2011-8#
32. Manajit, C., Sukomal, P., Rahul, P., & Ravindranath, C. (2016). Recent developments in social spam detection and combating techniques: A survey. *Information Processing & Management*, *52*(6), 2-4.
33. McAfee. (2014, 9. junij). *Net Losses: Estimating the Global Cost of Cybercrime.* Najdeno 1. julija 2016 na spletnem naslovu http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

34. McAfee. (2015, 15. november). *McAfee Labs Threats Report.* Najdeno 12. julija 2016 na spletnem naslovu http://www.mcafee.com/kr/resources/reports/rp-quarterly-threats-nov-2015.pdf
35. Mitchell, B. (2009, 3. februar). What is hacking? *About Tech.* Najdeno 21. junija 2016 na spletnem naslovu http://compnetworking.about.com/od/networksecurityprivacy/f/what-is-hacking.htm
36. Monsum, L. (2014, 29. maj). DoS VS DDoS – What is the difference? *Security-FAQs.* Najdeno 22. junij 2016 na spletnem naslovu http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html
37. Nachenberg, C. (2005, 28. avgust). Hacking. V *Encyclopedia.com*. Najdeno 21. junija 2016 na spletnem naslovu http://www.encyclopedia.com/topic/Hacking.aspx
38. National Crime Prevention Council. (2012, 1. september). *Cybercrimes.* Najdeno 15. junija 2016 na spletnem naslovu http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf
39. Pilling, R. (2013). Global threats, cyber-security nightmares and how to protect against them. *Computer Fraud & Security*, *2013*(9), str. 14-18.
40. Ponemon Institut. (2015, 6. oktober). *2015 Cost of Cyber Crime Study.* Najdeno 27. julija 2016 na spletnem naslovu http://img.delivery.net/cm50content/hp/hosted-files/ 2015_US_CCC_FINAL_4.pdf
41. PwC. (2016, 25. februar). *Adjusting the Lens on Economic Crime.* Najdeno 11. junija 2016 na spletnem naslovu http://www.pwc.com/gx/en/economic-crime-survey/pdf/Glo balEconomicCrimeSurvey2016.pdf
42. Rootkit. (2016, 3. junij). V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu http://www.britannica.com/technology/rootkit
43. Rouse, M. (2011, 15. marec). Spear phising. *TechTarget.* Najdeno 17. junija 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/spear-phishing
44. Rouse, M. (2015, 27. oktober). Phising. *TechTarget.* Najdeno 17. junija 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/phishing
45. Rouse, M. (2016, 15. februar). Social engineering. *TechTarget.* Najdeno 27. junija 2016 na spletnem naslovu http://searchsecurity.techtarget.com/definition/social-engin eering
46. Saini, H., Shankar Rao, Y., & Panda, T. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*, *2015*(10), 202-209.
47. Scareware. (2011, 21. oktober). V *Technopedia.* Najdeno 27. junija 2016 na spletnem naslovu https://www.techopedia.com/definition/4345/scareware
48. Schwartz, E. (2015, 12. februar). Security Think Tank: Four steps to defend against cyber attack. *ComputerWeekly.com*. Najdeno 14. julija 2016 na spletnem naslovu http://www.computerweekly.com/opinion/Security-Think-Tank-Four-steps-to-defend-against-cyber-attack
49. Spyware. (2009, 1. januar). V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu https://www.britannica.com/technology/spyware

50. Teach ICT. (2009, 24. april). *What is a hacker*. Najdeno 21. junija 2016 na spletnem naslovu http://www.teach-ict.com/gcse_new/protecting_systems/hackers/miniweb/pg 2.ht m
51. Trojan. (2008, 12. november). V *Encyclopedia Britannica*. Najdeno 27. junija 2016 na spletnem naslovu https://www.britannica.com/technology/trojan-computing
52. Warren, T., Favole, J., Haber, S., & Hamilton, E. (2016, 2. februar). Cybercrime Costs More Than You Think. *Hamilton Place Strategies.* Najdeno 1. julija 2016 na spletnem naslovu http://www.hamiltonplacestrategies.com/news/cybercrime-costs-more-you-thi nk #Paper
53. Webroot. (2011, 28. september). *What is Social Engineering?* Najdeno 24. junija 2016 na spletnem naslovu http://www.webroot.com/us/en/home/resources/tips/online-shopp ing-banking/secure-what-is-social-engineering
54. Williams, J. (2014, 29. oktober). What Is Cyber Crime? - Definition, Types & Examples. *Study.com*. Najdeno 15. junija 2016 na spletnem naslovu http://study.com/academy/lesso n/what-is-cyber-crime-definition-types-examples.html

PRILOGE

KAZALO PRILOG

PRILOGA 1: Seznam v delu uporabljenih kratic

Tabela 1: Seznam v delu uporabljenih kratic

BYOD	prinesite svojo napravo (angl. *Bring Your Own Device*).
CMS	Sistem za upravljanje vsebin (angl. Contact Managament System), omogoča urejanje in vzdrževanje vsebin spletnih strani podjetij
CVV	verifikacijska koda (angl. *Card Verification Value),* zadnje tri številke na posameznikovi bančni kartici, ki omogočajo varno spletno nakupovanje
DDoS	porazdeljena zavrnitev storitve (angl. *Distributed Denial of Service)*, podobno kot DoS napadi, vendar je uporabljeno večje število računalnikov in povezav
DoS	zavrnitev storitve (angl. *Denial of Service*), napadi povzročeni z namenom prekinitve dostopnosti do spletnih strani
e-poštni naslov	elektronski pošni naslov
e-poštna	elektronska pošta
e-pošti račun	elektronski poštni račun
e-sporočila	elektronsko sporočilo
IT	informacijska tehnologija
VPN	virtualno privatno omrežje (angl. *Virtual Private Network*)
WI-FI	okrajšava angleške besede *Wireless Fidelity*, brezžična omrežna tehnologija
ZDA	Združene države Amerike

PRILOGA 2: Seznam v delu uporabljenih tujk

Tabela 2: Seznam v delu uporabljenih tujk

cracking	zlonamerni napadi na računalniške sisteme, z namenom pridobivanja finančne koristi
backdoor	zadnja vrata
brut force	napad s surovo silo
Federal Bureau of Investigation	Zvezdni preiskovalni urad
firewall	požarni zid
key logger	iskalnik ključev, gesel
malware	zlonamerna programska oprema
phising	spletno ribarjenje
ping sweep	preverjanje odzivnosti omrežja
port scan	preverjanje računalniških vmesnikov
rootkit	korensko orodje, najhujša oblika zlonamerne programske opreme
scareware	strašilna tehnika, programi, ki naj bi rešili določen, navidezen problem na računalniku
spam	nezaželena pošta
spear phising	ribarjenje s kopjem, ena izmed oblik ribarjenja, pri kateri se pošiljajo elektronska pošta sporočila, zaposlenim v podjetju z namenom pridobivanja zaupnih podatkov
whaling	podobno kot ribarjenje s kopjem, s to razliko da se sporočila pošiljajo zaposlenim, ki se nahajajo višje v organizacijski strukturi