UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA SPLETNE KRIMINALITETE TER OCENA NJENE EKONOMSKE ŠKODE

Ljubljana, julij 2016 LUKA ŠKOF

IZJAVA O AVTORSTVU

Podpisani Luka Škof, študent Ekonomske fakultete Univerze v Ljubljani, avtor/-ica predloženega dela z naslovom Analiza spletne kriminalitete ter ocena njene ekonomske škode, pripravljenega v sodelovanju s svetovalko prof. dr. Borko Džonovo Jerman Blažič

IZJAVLJAM

1. da sem predloženo delo pripravil/-a 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/-a, 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/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;

7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a 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. 7. 2016 Podpis študenta:

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Internetno kriminaliteto (v nadaljevanju kiberkriminal) definiramo kot vedenje, pri katerem so računalniki ali računalniška omrežja orodja, tarče ali prostor kriminalnih dejanj (Newman, 2009). Kiberkriminal je v teoriji tesno povezan z informacijsko varnostjo, s katero skupaj tvorita znanost o kiberkriminalu. Gre za področje raziskovanja, katerega namen je preprečevanje kiberkriminala v kombinaciji s tehnikami informacijske varnosti, ki se osredotočajo na zaščito zaupnosti, dostopnosti, verodostojnosti in preprečitev zlorab (Hartel, Junger & Wieringa, 2010).

Kiberkriminal je vedno bolj razširjen in sofisticiran, s čimer povzroča resnejše posledice kot tradicionalen kriminal in je poseben v treh točkah: temelji na zahtevni tehnologiji in spretnostih, ima višjo stopnjo globalizacije kot tradicionalen kriminal ter je relativno nov (Kshetri, 2006). V gospodarstvu se kaže v obliki kraje intelektualne lastnine in finančnih sredstev, zaseganja bančnih računov, ustvarjanja in širjenja virusov in objavljanja zaupanih podatkov iz poslovanja. Na državni in korporacijski ravni pa opazimo tudi oviranje ključne omrežne infrastrukture. V letih 2014 in 2015 je ekonomska škoda kot posledica kiberkriminala v ZDA v podjetjih z več kot 1.000 zaposlenimi, vezanimi na interno omrežje, že presegala 10 milijonov dolarjev, blizu teh številk pa se gibljejo tudi Nemška (okrog 8 milijonov dolarjev) in Japonska največja podjetja (okrog 7 milijonov dolarjev) (Ponemon Institute, 2015). Ocena ekonomske škode kiberkriminala v EU se giblje okrog 0,6 % bruto dohodka (BND) in znaša približno 15 milijard letno (EU Law Analysis, 2015).

Predmet magistrskega dela je študija o pojavu in razvoju kiberkriminala ter okvirna ocena ekonomske škode, ki jo povzroča gospodarskim družbam, vladnim organizacijam, javnim zavodom in gospodarstvu na sploh. Naloga ne zajema škode, ki nastaja z uporabo socialnega inženiringa (primeri kraje identitete in goljufij, v katerih nas neznanec prek spleta prepričuje, da je odvetnik našega daljnega preminulega sorodnika, po katerem smo podedovali zajetne vsote), temveč zgolj tisto škodo, ki nastaja institucijam in organizacijam. Ker je razvoj konceptualnih in teoretičnih okvirjev za to še zelo pomanjkljiv, je glavni problem magistrske naloge določitev okvirnega teoretskega modela, s pomočjo katerega bi lahko opredelili obseg kiberkriminala in ocenjevali ekonomsko škodo, ki jo povzroča v gospodarstvu ter ugotovili, kateri so faktorji, ki povečujejo izpostavljenost kiberkriminalu v gospodarstvu in družbi. Pri tem bi upoštevali posamezne že izpeljane modele ter vključili še naslednje dodatne teorije: teorija rutinskih aktivnosti, teorija kriminalnih vzorcev in teorija racionalne izbire (Felson in Clarke, 1998), stroške, ki nastanejo ob uspešnem kiberkriminalu, pa bi razdelili v tri kategorije: neposredna izguba, posredna izguba in stroški zaščite (Anderson et al., 2012).

Teorija rutinskih aktivnosti (angl. *routine activity approach*) predpostavlja, da se priložnost za kriminalno dejanje pojavi med rutinskimi aktivnostmi, pri čemer so pomembni trije elementi: storilec (kaznivega dejanja), ustrezna tarča in odsotnost sposobnega varuha –

varnostnega pooblaščenca v organizaciji. V moderni družbi je veliko potencialnih storilcev – še posebej v situacijah, ko je malo nadzora in majhna verjetnost odkritja, so ljudje izpostavljeni skušnjavam (Felson in Boba, 2010). V kontekstu kiberkriminala je množica potencialnih storilcev praktično neomejena, najboljšo priložnost pa imajo t. i. »insajderji«, osebe znotraj organizacije, ki imajo dostop do internih informacij (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005).

Za teorijo kriminalnih vzorcev (angl. *crime patten theory*) je značilno, da se priložnost za kriminalno dejanje pojavi tekom dnevne rutine, tj. nekje med domom, delom in prostim časom. Posledično so kriminalna dejanja skoncentrirana v določen čas in prostor, kar označujemo s pojmom »vroče točke« (angl. *hot spots*). Z identifikacijo vročih točk je izvajanje preventivnih ukrepov veliko bolj učinkovito (Bowers et al., 2004). Nasprotno pa je opredelitev časa in prostora v spletnem kriminalu praktično nemogoča – storilec lahko izvede več kriminalnih dejanj naenkrat na različnih krajih (na tisoče računalnikih) povsod po svetu (Hartel et al., 2010).

Zadnja teorija, ki lahko pomaga pri opredeljevanju spletne kriminalitete, je teorija racionalne izbire (angl. *rational choice perspective*), ki pravi, da vedenje vodijo pričakovane posledice. V kontekstu kriminala to pomeni, da potencialni storilci pretehtajo stroške in koristi ter izvedejo kriminalno dejanje, ko so pričakovane koristi večje od stroškov (Cornish & Clarke, 2008), gre pa za omejeno racionalnost, ki je pogosto uporabljena tudi v ekonomiji – predpostavlja, da človek nikoli ne sprejema popolnoma racionalnih odločitev. Na tej točki je potrebno ugotoviti, kateri so stroški in koristi storilcev kiberkriminala. Tudi za preventivne ukrepe si raziskovalci kibernetske kriminalitete pomagajo z znanostjo o tradicionalnem kriminalu. Izpeljani so iz naslednjih generičnih principov (Hartel et al., 2010):

- povečanje potrebnega truda za izvedbo kriminalnega dejanja;
- povečanje tveganja;
- zmanjšanje koristi izvedenega kriminalnega dejanja;
- zmanjšanje provokativnosti, ki izvablja kriminalno vedenje, ter
- odstranitev »opravičil« za kriminalno vedenje.

Na podlagi zgornjih principov so razvite trenutne tehnike informacijske varnosti: gesla in PIN kode, kodiranje oziroma šifriranje podatkov, požarni zid, t.i. demilitarizirana cona, sistem za zaznavanje motenj, pregledovalnik za zaznavo virusov, programska oprema za odstranjevanje ranljivosti, radiofrekvenčna identifikacija (angl. *Radio Frequency Identification,* v nadaljevanju RFID) za zagotavljanje informacij o produktih, ID klicatelja, revizijski logaritem za zbiranje podatkov, visoka odgovornost ponudnikov internetnih storitev in izobraževanje uporabnikov spleta (Hartel et al., 2010). Učinkovitost teh tehnik pa se lahko oceni z vidika uspešnega preprečevanja kibernetske kriminalitete in zmanjšanja škode, ki jo povzroča.

Namen raziskave je s pregledom obstoječe literature določiti model, ki bi vključeval faktorje, vidike in posledice kiberkriminala ter omogočal opredelitev možnega pojava in uspeha kiberkriminala znotraj posamezne organizacije. V praksi bi ta model organizacijam pomagal, da kiberkriminal uspešneje preprečujejo, ga pravočasno prepoznavajo in znajo oceniti dejansko ekonomsko škodo, ki jo povzroči na kratek in dolgi rok. Z empiričnim delom bi ugotavljali situacijo v Sloveniji ter na podlagi interpretacij in povezav s teorijo izpeljali praktične napotke.

Odgovarjali bomo na naslednja raziskovalna vprašanja:

- RV1: Kakšen je trenuten obseg kiberkriminala v Sloveniji?
- RV2: V kakšnih oblikah se najpogosteje pojavlja znotraj gospodarskih družb?
- RV3: Na kakšen način se gospodarske družbe soočajo z njim?
- RV4: S katerimi metodami bi škodo lahko zmanjšali?

Pri prvem raziskovalnem vprašanju ne bomo skušali določiti celotnega obsega kiberkriminala v Sloveniji, ker ga zaradi pomanjkanja znanja in zavedanja veliko podjetij in organizacij ne meri ali meri napačno. Zato se bomo osredotočili na to, kakšen je obseg ekonomske škode v izbranih podjetjih in organizacijah.

Metodološko bo prvi del naloge temeljil na pregledu literature. Pri orisu osnovnih teorij bo kriterij za izbiro literature kvaliteta, pri preostalih poglavjih pa predvsem aktualnost – tj. čim novejše objave s področja, upoštevane bodo objave po letu 2000 ter poročila s problematiko povezanih konferenc.

Za empirični del naloge bo glavna raziskovalna metoda strukturiran intervju, ki ga bomo opravili s predstavniki 7 večjih organizacij v Sloveniji (pokritost različnih panog in tako javni kot zasebni sektor). Interpretacije rezultatov, pridobljene z intervjuji, bodo nato primerjane z analiznimi metodami, ki so bile uporabljene v tujini. V zadnjem delu bo empirični del povezan s teoretičnim, iz njiju pa bo povzetih čim več praktičnih implikacij in napotkov za bodočnost.

Prvo poglavje bo namenjeno opredelitvi internetne kriminalitete in njenih pojavnih oblik. Razloženi bodo tudi z njo povezani pojmi in odnos s sorodnima znanostma, tj. znanost o kriminalu in informacijska varnost. V nadaljevanju bo predstavljen širši teoretični okvir, ki temelji na uveljavljenih teorijah, pogledih in perspektivah s področja kriminala na splošno. Podrobneje bodo razložene teorija rutinskih aktivnosti, kriminalnih vzorcev in racionalne izbire ter koncept ponavljajoče se žrtve. Glavne implikacije teh teorij bodo aplicirane na področje internetne kriminalitete in v kolikor to ne bo možno, predstavljene možnosti za raziskovanje v tej smeri.

Tretje poglavje bo strukturirano v obliki pregleda razširjenosti tovrstne kriminalitete. Opredeljeni bodo dejavniki razvoja in širjenja, s pomočjo poročil inštitutov in organizacij, ki se ukvarjajo z merjenjem tovrstne problematike in zbiranjem podatkov iz različnih držav, pa bo prikazana rast v zadnjem obdobju, tj. v letih 2013–2015. Predstavili bomo tudi različne ekonomske poglede in ugotovitve o tem, v katerih državah je kiberkriminal najbolj prisoten (oziroma najbolj natančno merjen), kakšna je neto sprememba stroškov, ki jih povzroča v posameznih državah, kako se gibljejo stroški glede na velikost organizacije in glede na število zaposlenih, neposredno povezanih z internim omrežjem, kakšni so stroški kiberkriminala glede na vrsto napada (in kako se razlikujejo po državah), kakšne so razlike v stroških kiberkriminala po različnih industrijskih panogah in koliko časa je potrebnega za razrešitev enega kibernetskega napada glede na pojavno obliko.

Četrto poglavje bo spet namenjeno znanosti o tradicionalnem kriminalu – »izposojeni« bodo generični principi, na katerih temeljijo tehnike preprečevanja pojava kriminalnih dejanj, nato razčlenjeni in na podlagi razširitve konceptov v kontekst kibernetskega prostora predstavljene možne tehnike za preprečevanje kibernetske kriminalitete in predstavitev tistih, ki se v kontekstu kiberkriminala že pojavljajo tako v praksi kot v empirično podprtih raziskavah. Teoretični del bo zaključen s pregledom kazalnikov in ekonomske škode.

Empirični del bo temeljil na intervjujih, ki bodo natančno strukturirani – predvsem z namenom pridobivanja rezultatov, ki bodo uporabljeni v primerjalni analizi (s pomočjo metod, uporabljenih v obstoječih sorodnih študijah). Vzorec intervjuvancev bo zajemal direktorje in zaposlene na vodilnih položajih podjetij oziroma organizacij različnih velikosti (kot kriterij velikosti bo število zaposlenih) ter iz različnih panog – prehrambna industrija, finančne storitve računalniško programiranje in podobno.

Za empiričnim delom bo bistven del magistrskega dela, tj. predlog modela za celostno obravnavo kiberkriminala v podjetjih in organizacijah. Temeljil bo na predelani literaturi, bistvenih ugotovitvah globalnih raziskav in intervjujih, ki jih bomo izvedli. Še posebej se bo osredotočal na ekonomski vidik – škodo, ki jo kiberkriminal povzroča v finančnem smislu.

Zadnji del magistrskega dela bo sklep, v katerem bodo povzete ključne ugotovitve, povezave med obravnavano teorijo in ugotovljenimi empiričnimi dognanji, odgovorjena raziskovalna vprašanja in podane praktične implikacije.

1 SPLETNA KRIMINALITETA

1.1 Opredelitev spletne kriminalitete in njenih pojavnih oblik

S hitro razvojem informacijske tehnologije se je močno spremenilo naše vsakdanje življenje, povečale pa so se tudi težave z varnostjo – enostavneje je povzročiti kriminalno dejanje in soočamo se s spletno kriminaliteto (v nadaljevanju kiberkriminal) (Solak & Topaloglu, 2015). Kiberkriminal definiramo kot vedenje, pri katerem so računalniki ali računalniška omrežja orodja, tarče ali prostor kriminalnih dejanj (Newman, 2009), ali kot katerokoli vrsto ilegalnega, neetičnega in nepooblaščenega obnašanja v sistemu, ki avtomatsko procesira informacije ali prenaša podatke (Keskin, 2007). Kot primere širše opredelitve kiberkriminala Zeviar-Geese (1997) navaja prevare, nepooblaščen dostop, otroško pornografijo in spletno nadlegovanje, skupaj pa lahko kiberkriminal tako povzamemo kot kriminalno dejanje, ki je povzročeno ali poenostavljeno z uporabo računalnika, omrežja ali druge računalniške naprave. Računalnik oziroma naprava je lahko povzročitelj (agent), posrednik ali tarča kriminalnega dejanja, prostor pa je lahko računalnik sam ali ne virtualni svet (Gordon & Ford, 2006), uspešen napad na informacijsko tehnologijo pa bi lahko imel prodoren učinek na moderne družbene, ekonomske in vojaške sposobnosti (Youd, 2015).

Pomembna značilnost kiberkriminala je ta, da eno dejanje lahko povzroči škodo na globalni ravni. Meddržavna narava večine kriminalnih dejanj, povezanih z računalniki in spletom, je že sprožila razvoj metod za soočanje z njimi tako na domači kot mednarodni ravni, a so zaenkrat neučinkovite tudi v bolj razvitih državah. Razdvojenost med digitalno bolj in manj razvitimi državami pa je povzročila nastanek t. i. »varnih oaz« (angl. *safe havens*), v katerih je storilce kiberkriminalnih dejanj težje ali nemogoče odkriti in kaznovati (Broadhurst, 2006).

Storilce organiziranih kiberkriminalnih dejanj razvrščamo v tri skupine. Prva skupina so tradicionalne kriminalne skupine, ki uporabljajo računalnike in omrežja, da povečajo oziroma okrepijo svoja dejanja tradicionalnega kriminala. V drugo skupino sodijo tisti, ki delujejo ekskluzivno na spletu, v tretjo pa organizirane skupine ideološko in politično motiviranih posameznikov, ki uporabljajo informacijsko in komunikacijsko tehnologijo za izvedbo večjih kiberkriminalnih dejanj (Choo, 2008). Gordon in Ford (2006) kiberkriminal delita na dva tipa:

I. **Prvi tip** je z vidika žrtve enkraten oziroma samostojen dogodek. Je bolj **tehnične narave**, običajno izveden s pomočjo škodljive programske opreme (angl. *crimeware*), kot je Trojanski konj, s katerim vršilec dejanja vdre v žrtvin računalnik. Izpeljavo tega tipa kiberkriminala lahko olajšajo tudi ranljivosti računalnika in njegove programske opreme. Primeri kiberkriminala prvega tipa so: ribarjenje, kraja identitete, kraja ali manipulacija s podatki (prek vdiranja in virusov), prevare spletnega trgovanja in drugo.

II. Kiberkriminal **drugega tipa** pa je izveden **brez škodljive programske opreme**. Običajno so to ponavljajoči se dogodki. Primeri kiberkriminala drugega tipa so: spletno zalezovanje in nadlegovanje, izsiljevanje, manipulacije na delniških trgih, kompleksno korporativno vohunjenje ter planiranje in izvajanje terorističnih aktivnosti.

Še eno kategorizacijo ponujata Huang in Wang (2009): **instrumentalni in ekspresivni** kiberkriminal. Instrumentalno dejanje kiberkriminala je tisto, pri katerem je namen določena pridobitev (na individualni ravni je primer kraja identitete, na organizacijski pa korporativno vohunjenje), ekspresivni kiberkriminal pa je tisti, pri katerem je dejanje izvedeno zaradi zadovoljstva pri izvajanju (na ravni posameznika je to lahko spletno izkoriščanje in nadlegovanje otrok, na ravni organizacije oziroma skupnosti pa spletni terorizem ali zrušenje spletne strani). Avtorja dodajata tudi, da so informacije v kiberkriminal vključene na tri različne načine – kot blago »tihotapljenja«, kot instrument za izvedbo kriminalnega dejanja ali kot dokaz, da se je dejanje zgodilo.

1.2 Znanost o kriminalu

Predmet znanosti o kriminalu so učinki tehnik za preprečevanje kriminala in izboljševanje le-teh. Glavne komponente znanosti o kriminalu so: konceptualni okvir, nabor tehnik za zmanjševanje priložnosti, znanje o dobri praksi ter študije o pregonu in difuziji prednosti (Hartel et al., 2009). Konceptualni okvir sestavljajo teorija rutinskih aktivnosti, teorija kriminalnih vzorcev in teorija racionalne izbire (Felson & Clarke, 1998) ter koncept ponavljajoče se žrtve (Farrell & Pease, 2001), ki se jim bomo bolj posvetili v naslednjem poglavju (tj. v poglavju Širši teoretični okvir).

Znanost o kriminalu se osredotoča na rezultate (Laycock, 2005) ter razlaga kratkoročne vzroke za prekrške oziroma kazniva dejanja in kako do njih pride (Clarke, 2010). V svojem bistvu skuša najti odgovore na naslednja vprašanja (Smith & Tilley, 2013, str. 9):

- Kaj nam znanost lahko pove o naravi kriminalnega dejanja?
- Kako lahko znanost prispeva k preprečevanju kriminalnih dejanj?
- Kako lahko znanost podpira odkrivanje kriminalnih dejanj?
- Kako lahko znanstvene metode uporabimo za zmanjševanje kriminalnih dejanj?

Preden razčlenimo znanost o kriminalu, moramo razložiti nekaj osnovnih pojmov. Kriminal lahko opredelimo na dva načina, glede na to ali gledamo z objektivne ali subjektivne perspektive. **Subjektivistična** definicija pravi, da je kriminal dejanje sile ali goljufija izvedena v težnji lastnih interesov storilca (Gottfredson & Hirschi, 1990). Ta pristop je uporaben, če želimo preučevati vedenje, ki je v družbi obravnavano kot moralno napačno ali protizakonito.

Druga, **objektivistična** definicija, pa pravi, da je kriminal vedenje, ki je splošno obravnavano kot škodljivo za posameznika ali družbo (Tappan, 1947). Še en pojem, ki se pojavlja znotraj znanosti o kriminalu, je prekršek. Prekršek je širši koncept kot kriminal, in zajema vse vidne fizične in družbene iztočnice, ki so splošno zaznane kot moteči dejavniki za uporabo javnih površin (Sampson & Raudenbush, 1999). Koncept prekrška torej vključuje tudi cigaretne ogorke, prazno embalažo in ostale smeti na pločnikih, popivanje na javnih površinah, prostitucija in podobno (Hartel et al., 2010).

Znanost o kriminalu temelji na multidisciplinarnem in kontekstualnem pristopu ter z dokazi podprtih raziskavah, ki vodijo v praktične rešitve in preprečevanje pojava kriminalnih dejanj (Hartel et al., 2010). Opišemo jo lahko s sedmimi glavnimi značilnostmi (Tilley, 2007):

I. V primerjavi s kriminologijo preučuje pojave, ne oseb. Znanost o kriminalu raziskuje, kdaj in kje se vlomi dogajajo, ne raziskuje osebnosti storilcev ali njihovih družin ali družabnega življenja. Ugotavlja, kaj so kratkoročni motivi, kot na primer: zakaj je storilec izbral posamezno bivališče, čas ali kaj je iskal. Kriminologija na drugi strani, kot pišejo Brown, Esbensen in Geis (2013), raziskuje kriminal, kriminalce in družbene reakcije na kriminalna dejanja. Odgovarja na vprašanja, kot so: zakaj ljudje storijo kriminalno dejanje? Zakaj se drugi temu prilagodijo? Kako lahko razložimo in razumemo kriminal in kazniva dejanja? Kriminološke teorije iščejo razlage, zakaj prihaja do dejanj, ki jih označujemo kot kriminalna.
II. V svojem jedru je problemsko orientiran znanstveni pristop in predstavlja model za iskanje načinov preprečevanja konkretnih nezgod, motenj, kriminalnih dejanj, pa tudi nesreč v javnem zdravstvu in na področju osebne varnosti. Znanost o kriminalu je torej neposredna in specifična.
III. Raziskovalne metode vključujejo:
    - ciljne raziskave,
    - geografske raziskave in
    - študije primera.

    Uporabljajo jih za ugotavljanje, kako specifične intervencije učinkujejo na kriminal.
IV. Pri svojem delu uporabljajo teoretski okvir, sestavljen iz teorije rutinskih aktivnosti, teorije kriminalnih vzorcev in teorije racionalne izbire
V. Z empiričnim raziskovanjem primerov znanost o kriminalu skuša razložiti pravila in vzorce, ki vodijo do teh pojavov kriminala. Rezultate raziskovanja in znanje, ki izhaja iz le-tega, uporabljajo za preprečevanje in nadziranje kriminala.
VI. Znanost o kriminalu je multidisciplinarno polje raziskovanja. Namen je razumeti in preprečiti kriminal s katerokoli metodo iz kateregakoli področja, ki je potrebno. Uporablja predvsem znanje in metode naslednjih področij: geografije, urbanega razvoja, matematike, industrijskega dizajna, gradbeništva, medicine, ekonomije, računalniške znanosti, psihologije, sociologije, kriminologije in prava.

VII. Potencialni uporabniki dognanj znanosti o kriminalu prihajajo iz različnih področij preprečevanja kriminala in kršitev; to so: policisti, oblikovalci zakonodaje, načrtovalci urbanizma, managerji in arhitekti.

Znanost o kriminalu je za preučevanje kiberkriminala pomembna predvsem zato, ker njenim dognanjem lahko dodamo tehnike informacijske varnosti, s čimer skupaj tvorijo novonastalo znanost o kiberkriminalu (Hartel et al., 2010). Za razvoj le-te je potrebno odgovoriti na naslednji vprašanji: Katere tehnike informacijske varnosti lahko uporabimo za preprečevanje in zaznavanje kiberkriminala (in tradicionalnega kriminala na splošno)? Ali lahko metode empiričnega raziskovanja znanosti o kriminalu uporabimo za raziskovanje učinkovitosti tehnik informacijske varnosti? V naslednjem podpoglavju bomo podrobno preučili informacijsko varnost ter njeno vpetost v znanost o kriminalu in znanost o kiberkriminalu.

1.3 Informacijska varnost

Učinkovitost tehnik informacijske varnosti je vprašljiva, saj so (sicer dobronamerne) politike pogosto ignorirane ali predrage za implementacijo. Tipičen primer so situacije, ko je od uporabnika zahtevano, da si izbere močno geslo (tj. takšno, ki vsebuje velike in male črke, številke …). Ker si ga ne more zapomniti, si ga zapiše na rumen lepljiv listek in prilepi na rob ekrana službenega računalnika, kjer ga lahko vidijo sodelavci in ostali mimoidoči. Če želimo, da so tehnike informacijske varnosti učinkovite, moramo torej pri razvijanju le-teh upoštevati tudi človeške in ekonomske faktorje, predvsem pa je potrebno razumeti odnos med informacijsko varnostjo in preprečevanjem kiberkriminala (Hartel et al., 2010).

Informacijsko varnost definiramo kot varovanje informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo, razkritjem, motnjami in prekinitvami, predelavami ali uničenjem z namenom zagotavljanja integritete, zaupnosti in dostopnosti (Hartel et al., 2010). Pogost predmet študij je že od 90. let prejšnjega stoletja, predvsem razvoj metod (Baskerville, 1993), interna zloraba informacij, eksterni napadi, politike dovoljene uporabe, računalniški kriminal in varnost gesel (Nazareth & Choi, 2015).

Z vidika organizacij in gospodarskih družb pa Tudor (2001) informacijsko varnost in upravljanje z njo predstavi kot sestavljeno iz petih komponent: organizacija in infrastruktura varnosti, varnostne politike, standardi in postopki, temeljna varnostna določila in ocene tveganj, zavedanje in izobraževalni programi ter upoštevanje določil. ISO/IEC 17799 (2000) pa določa še nekoliko širši obseg:

- vzpostavitev informacijsko-varnostnih politik in ovrednotenj,
- organizacija in odgovornosti informacijske varnosti,
- osebje za varnostni management in izobraževanja,

- računalniški sistem za varnostni management,
- omrežni varnostni management,
- sistem za nadzor dostopa,
- varnostni management za sistemski razvoj in ohranitev,
- varnostni management za informacijsko premoženje,
- varnostni management za fizične dobrine in okolje ter
- poslovno načrtovanje in management.

Ker je glavni namen uporabe računalnikov in računalniških omrežij delo z informacijami (v različnih formatih), je pojav kiberkriminala povezan s kršitvijo določil informacijske varnosti. Kršitev določil informacijske varnosti razumemo kot vdor prek varnostnih mehanizmov ali neupoštevanje varnostnih politik. Najpogostejše oblike kiberkriminala, kot so nepooblaščen dostop, spletne prevare in pornografija, običajno vsebujejo kršitev informacijske varnosti. Kljub temu, da je med kiberkriminalom in informacijsko varnostjo veliko polje prekrivanja, je tudi nekaj razlik: (1) obstajajo oblike kiberkriminala, ki ne vsebujejo kršitev informacijske varnosti in (2) obstajajo kršitve informacijske varnosti, ki niso kriminalna dejanja, temveč le motnje (Hartel et al., 2010).

Znanost o kiberkriminalu združuje metodologijo znanosti o kriminalu in tehnologijo informacijske varnosti. V nadaljevanju bomo predstavili sedem značilnosti znanosti o kriminalu (razložene v prejšnjem podpoglavju), ki jim bomo dodali predpostavke informacijske varnosti in tako izpeljali podlago za razumevanje kiberkriminala (Hartel et al., 2010):

I. Informacijska varnost se ne ukvarja s kršitelji, temveč jo zanimajo pojavi, kot so neupoštevanje varnostnih politik, vdori prek varnostnih protokolov, ugotovljena gesla, klonirane pametne kartice in podobno. S tega vidika je bilo raziskovanje o kiberkriminalu in informacijski varnosti vedno podobno.
II. Tako kot znanost o kriminalu, se tudi informacijska varnost osredotoča na posamezne probleme in načine, kako preprečiti konkretne primere (kot na primer vdor v spletno stran). Je zelo specifična in vsak dobro oblikovan varnostni protokol lahko predpostavi določeno oceno moči napadalca in model grožnje. Z namenom preprečiti in zaznavati določene incidente je raziskovanje v informacijski varnosti usmerjeno na izide. Tudi v tem sta si bili znanost o kiberkriminalu in informacijska varnost vedno podobni.
III. Obratno kot znanost o kriminalu, se informacijska varnost običajno ne ukvarja z rezultati kršitev empirično. Aplikacija metod empiričnega raziskovanja znanosti o kriminalu bi študijam učinkov tehnik informacijske varnosti dodala prispevek predvsem z vidika povečevanja učinkovitosti teh tehnik.
IV. Raziskovanje informacijske varnosti nima konceptualnega okvirja za kriminalno vedenje kot ga ima znanost o kriminalu. Teorija racionalne izbire je podlaga za ekonomiko informacijske varnosti in zasebnosti, uporabni pa sta tudi teorija rutinskih

aktivnosti in teorija kriminalnih vzorcev, a v manjšem obsegu. Razlog za to je prevelika razlika med kibernetskim in tradicionalnim kriminalom, ki sicer močno vpliva na konceptualni okvir znanosti o kriminalu: problematično je predvsem različno zaznavanje časa in prostora v fizičnem in virtualnem svetu.

V. Za razliko od znanosti o kriminalu informacijska varnost ne raziskuje primerov, da bi prepoznala pravila in vzorce človeškega vedenja, ki razlaga kršitve, temveč razvija nove tehnike preprečevanja in zaznavanja kršitev varnostnih določil ter raziskuje značilnosti teh tehnik. Stremi k razumevanju njihovega delovanja in iskanju možnosti za izboljšave, kar lahko prispeva k preprečevanju kiberkriminala.

VI. Skupno znanosti o kriminalu in informacijski varnosti pa je to, da sta obe multidisciplinarni. Informacijska varnost je močno povezana z matematiko, fiziko, pravom, ekonomijo in psihologijo.

VII. Enako kot pri znanosti o kriminalu pa ima tudi informacijska varnost veliko potencialnih uporabnikov iz različnih panog: varnostne industrije, policije, vlade in poslovnega sektorja.

Glede na zgoraj opredeljenih sedem značilnosti lahko sklepamo, da se znanost o kriminalu in informacijska varnost med seboj dopolnjujeta in bogatita področje kiberkriminala in znanost o le-tem. Empirično oceno tega predstavlja tudi naslednja shema:

»Kontekst in obravnava pripeljeta do izida.«

Kontekst je okolje, v katerem obstaja priložnost za kriminalno dejanje; obravnava nastane z uporabo tehnik za preprečevanje kriminala; izid pa je rezultat uporabe obravnave v specifičnem kontekstu (Pawson & Tilley, 1997).

Ker so informacije ena izmed ključnih komponent premoženja gospodarskih družb in organizacij na splošno (Hong, Chi, Chao & Tang, 2003), je za zagotavljanje informacijske varnosti razvitih več teorij. Gre za pristope, tehnike in procese znotraj organizacij, ki naj bi ob uspešni implementaciji in konsistentnem upoštevanju določil njihovo premoženje varovale pred kiberkriminalom. Zaradi hitrega razvoja informacijske tehnologije (IT) nimajo dostopa do informacij in baz le IT strokovnjaki, temveč tudi drugi uporabniki znotraj organizacije in zunanji deležniki, s tem pa informacijska varnost dobiva nove izzive, učinkovito upravljanje pa je glavna skrb (Schultz, Proctor, Lien & Salvendy 2001). Poznamo pet glavnih teorij: teorija varnostnih politik, teorija managementa tveganj, teorija nadzora in revizije, teorija sistemskega managementa ter kontingenčna teorija (Hong et al., 2003).

2.3.1 Teorije informacijske varnosti

Teorija varnostnih politik pravi, da naj bi bila informacijska varnost najhitreje in učinkovito dosežena z vzpostavitvijo, implementacijo in ohranjanjem politik informacijske varnosti. V postopku le-tega Kabay (1996) izpostavlja pet ključnih korakov: prepričati vrhnji

management, analizirati zahteve informacijske varnosti, oblikovati politike, jih implementirati ter ohranjati. Življenjski cikel tovrstnih politik je sestavljen iz ocene politik, ocene tveganj, razvoja politik in opredelitev potreb oziroma zahtev ter pregleda trendov in managementa operacij (Gupta, Chaturvedi, Mehta & Valeri, 2000). Teorijo varnostnih politik lahko opredelimo s pomočjo treh funkcij: (1) informacijska varnost je funkcija informacijsko-varnostnih politik; (2) informacijsko-varnostne politike so funkcija vzpostavitve, implementacije in ohranitve teh politik; (3) vzpostavitev informacijske varnosti pa je funkcija zahtev organizacijske varnosti (Hong et al., 2003).

Naslednja teorija je **teorija managementa tveganja**, ki predlaga analizo in oceno organizacijskih tveganj, prek česar so lahko prepoznane grožnje in šibkosti informacijske varnosti. Sam management tveganja je definiran kot proces vzpostavljanja in ohranjanja informacijske varnosti znotraj organizacije (Wright, 1999), Reid in Floyd (2001) pa dodajata, da bi znotraj tega procesa organizacija morala dajati poudarek na prepoznavanju groženj in ranljivih točk informacijskega premoženja. Cilj je zmanjšati tveganje na sprejemljiv nivo.

V tem kontekstu lahko tudi to teorijo predstavimo z naslednjimi funkcijami: (1) informacijska varnost je funkcija ocene tveganja, nadzora tveganja, pregleda in prilagoditev; (2) ocena tveganja je funkcija analize in ocene tveganja; (3) nadzor tveganja je funkcija vzpostavitve in implementacije kazalnikov nadzora; (4) analiza tveganja je funkcija groženj in ranljivosti (oziroma šibkosti sistema); (5) ocena tveganja pa je funkcija vpliva vrednotenja premoženja (Hong et al, 2003).

Tretja teorija s področja upravljanja z informacijsko varnostjo je **teorija nadzora in revizije**. Weber (1999) nadzor opredeljuje kot sistem preprečevanja, zaznavanja in popravljanja nezakonitih dogodkov; kot posledico tega pa predpostavlja preventivne, zaznavne in korektivne sisteme nadzora. Opredelitev v ISO/IEC 17799 (2000) vključuje naslednje komponente nadzora:

- varnostne politike,
- organizacijska varnost,
- klasifikacija in nadzor premoženja,
- varnostno osebje,
- varovanje fizičnega okolja,
- varovanje komunikacije in operacij,
- nadzor dostopa,
- sistemski razvoj in ohranjanje,
- načrtovanje poslovne kontinuitete ter
- upoštevanje določil.

Teorijo nadzora in revizije tako opredelimo kot naslednje funkcije: (1) informacijska varnost kot funkcija vzpostavitve in implementacije sistemov nadzora ter informacijske revizije; (2) vzpostavitev sistemov nadzora kot funkcija varnostnih strategij in standardov (Hong et al., 2003).

Predzadnja, četrta teorija s tega področja, ki se pojavlja znotraj organizacij, je **teorija sistemskega managementa**, ki poudarja, da bi vsaka organizacija morala imeti vzpostavljen dokumentiran sistem informacijsko-varnostnega managementa prek šestih korakov: definiraj politike, definiraj obseg sistema informacijsko-varnostnega managementa, predvidi oceno tveganja, izberi cilje nadzora in izvedi ukrepe za doseg le-teh, pripravi izjavo o uporabi (BS 779-2, 1999).

Tudi to teorijo lahko predstavimo z opredelitvijo treh funkcij: (1) informacijska varnost je funkcija informacijsko-varnostnih politik, obsega informacijske varnosti, managementa tveganj in implementacije; (2) management tveganja je funkcija ocene in nadzora tveganja; (3) informacijsko-varnostne politike so funkcija notranjega in zunanjega okolja organizacije ter standardi.

Zadnja teorija pa je **kontingenčna teorija**, ki se od ostalih razlikuje predvsem po tem, da vključuje situacijske spremenljivke. Predpostavlja dinamiko zunaj in znotraj organizacije, k problematiki informacijske varnosti pa pristopa s prepoznavanjem in odzivanjem na situacijske spremenljivke z namenom učinkovitega doseganja organizacijskih ciljev (Robbins 1994). Znotraj petih nivojev informacijske varnosti, ki jih izpostavljajo Von Solms, Van Haar, Von Solms in Caelli (1994), tj. idealen, predpisan, osnovni, trenutni in preživetveni, so vsi nivoji razen idealnega odvisni od okolijskih dejavnikov, kot na primer grožnje, ranljivosti in vpliv na organizacijo; torej v skladu s predpostavkami kontingenčne teorije.

Povzamemo jo s tremi funkcijami: (1) informacijska varnost je funkcija informacijsko-varnostne strategije; (2) informacijsko-varnostna strategija je funkcija usmerjenosti politik, usmerjenosti managementa tveganja, usmerjenosti nadzora in revizije, usmerjenosti sistemskega managementa in kontingenčnega managementa; (3) kontingenčni management je funkcija organizacijskega okolja, managementa in tehnologije (Hong et al., 2003).

Vsem zgoraj predstavljenim teorijam je skupno vzpostavljanje informacijsko-varnostnih politik znotraj organizacije, nobena pa se ne poglablja v problem, omenjen v začetku poglavja, in sicer da so te politike predrage ali prezahtevne za implementacijo s strani vseh zaposlenih, tudi tistih, katerih osnovne delovne naloge niso strogo vezane na informacijsko tehnologijo ter so jim principi in določila težje razumljivi. Tehnikam informacijske varnosti se bomo ponovno posvetili v 5. poglavju, ko jih bomo aplicirali na principe zmanjševanja priložnosti tradicionalnega kriminala.

2.3.2 Varnostni sistemi v upravljanju z informacijskimi grožnjami

Informacijska varnost mora biti v organizacijah, ki želijo odgovorno slediti napredku v tehnologiji, med osnovnimi prioritetami. Skladno z željo po uspešnemu sledenju v času agresivne konkurenčnosti na trgu morajo organizacije biti fleksibilne, inovativne ter sposobne razvijati produkcijske in razvojne procese, pri tem pa sočasno razvijati pripadajoč informacijsko-komunikacijski sistem, da upravljajo z informacijami kar se da hitro in učinkovito. Pri tem izboljšujejo svoje poslovne operacije, a hkrati povečujejo informacijska varnostna tveganja (Prislan, 2014).

Prislan (2014) svoje delo gradi na naslednjih predpostavkah glede informacijske varnosti:

I. **Naraščajoče število primerov kiberkriminala**: z vidika informacijske varnosti in kiberkriminala je zadnje desetletje zaznamoval eksponenten razvoj in zloraba informacijsko-komunikacijske tehnologije.
II. **Naraščajoče število primerov kiberkriminala**, katerega **tarča je država**: pričakovati je vedno več napadov, pri katerih bo tarča državna omrežna infrastruktura (le-ta predstavlja državno suverenost in funkcionalni vidik družbe, zaradi česar je še bolj privlačna tarča).
III. **Naraščajoče število groženj in tveganj storitev »na oblaku«:** storitve »na oblaku« so postale neizogiben del interneta in uporabe organizacijske infrastrukture – predvsem zato, ker so prostor, kjer se shranjuje velike količine podatkov
IV. **Razvoj groženj, povezanih z mobilnimi platformami:** uporaba mobilnih telefonov v delovnem okolju je povzročila pojav novih oblik groženj, s tem pa preusmerila storilce kiberkriminalnih dejanj na mobilne platforme. Uporaba raznovrstnih aplikacij je poenostavila napade na velike količine podatkov, zaradi velikega porasta inovacij na področju mobilnih aplikacij pa bo to vedno večji izziv in predvsem proces, ki ga bo težko nadzorovati.

Na podlagi tega predpostavlja, da morajo organizacije v smeri zagotavljanja informacijske varnosti zagotavljati tri osnovne pogoje. V prvi vrsti morajo zaposlovati ljudi, ki so zadolženi za informacijsko varnost. Imeti morajo primerno znanje in sposobnosti, vodilni v podjetju oziroma organizaciji pa morajo te ljudi podpirati, jim omogočati avtoriteto in sprejemanje odločitev. Druga pomembna točka je sprejetje poglobljene in natančne strategije o informacijski varnosti. Vodilni management se mora zavzemati za uresničevanje strateškega načrta, ki jasno opredeljuje cilje in namene, kot tudi odgovornosti posameznih zaposlenih oziroma oddelkov. Tretji pogoj je analiziranje pomembnosti informacijskih virov in ocenjevanje učinkovitosti varnostnih ukrepov. Podjetje oziroma organizacija mora periodično ocenjevati varnostna tveganja in evalvirati rezultate varnostnih preverjanj. To razjasni, kateri deli informacijskih sistemov zatajijo, s tem pa se zagotavlja nemoteno kontinuiteto poslovanja (Prislan, 2014).

Stewart (2012) za tovrstno problematiko opisuje optimalno varnostno situacijo, v kateri vse organizacije sledijo trem korakom:

I. opredelitev varnostnih potreb,
II. alokacija potrebnih sredstev in
III. alokacija potrebne delovne sile oziroma človeških virov.

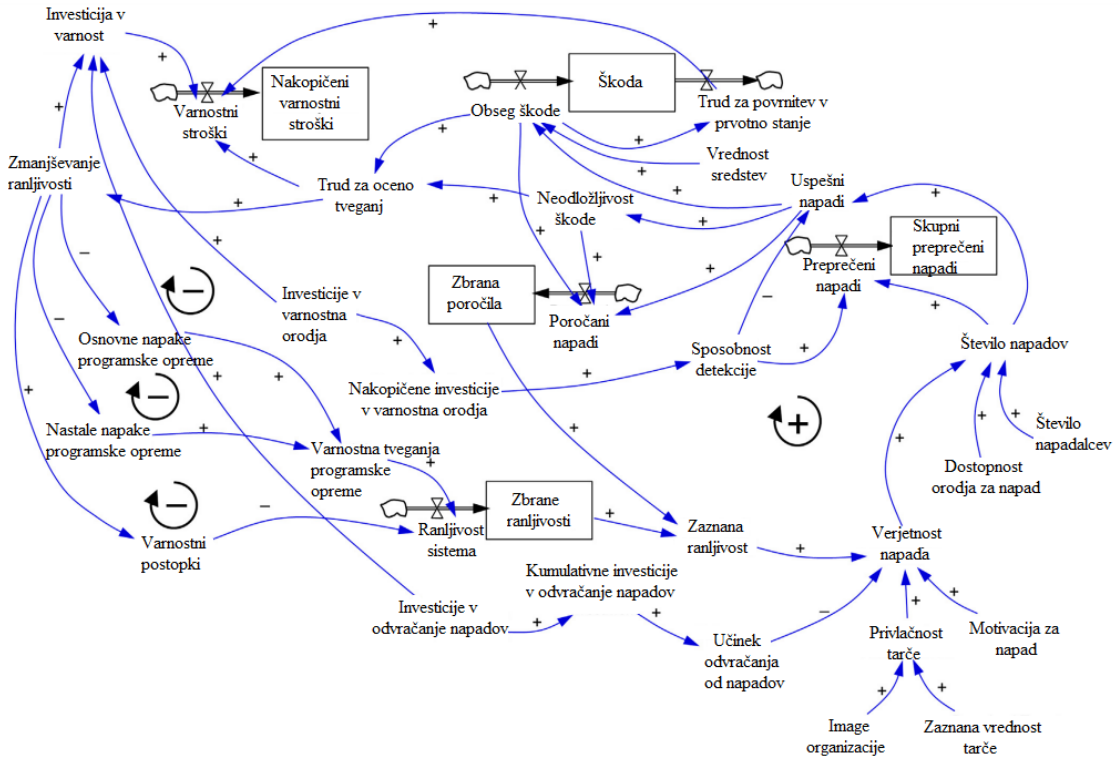
S tem predpostavlja, da je ena izmed ključnih zadev v informacijski varnosti ugotovitev, kakšne so v resnici potrebe po varnostnih ukrepih in kakšna so tveganja, ki jim je podjetje oziroma organizacija dejansko izpostavljena. Ta opredelitev je običajno zelo zahtevna zaradi posebnosti narave informacijske varnosti in kiberkriminala. Kljub raznovrstnim metodam merjenja in ocenjevanja še vedno obstajajo metodološka vprašanja in praktične omejitve (Stewart 2012).

Najtežja naloga vsakega raziskovalca na področju informacijske varnosti je zagotavljanje zanesljivih ocen, kakšne so zares potrebe in tveganja. Primer kiberkriminala se močno razlikuje od tradicionalnega, kjer je več kriminalnih dejanj na višjem nivoju. Grožnje škodljivih informacij so specifična odstopanja, za katere ni nujno, da vodijo v zaznavanje in poročanje o incidentu. Na eni strani veliko število zaznanih in prijavljenih primerov zlorabe informacij nakazuje na to, da so žrtve veliko bolj pripravljene sodelovati pri upravljanju s kibernetskimi napadi in da imajo varnostni sistemi visoke sposobnosti zaznavanja. Na drugi strani pa še vedno opažamo, da so »visoki« varnostni nivoji v resnici precej manj učinkoviti, kot je predvideno (Prislan, 2014). Organizacije še vedno redko primere kibernetskih napadov prijavljajo na policijo, zato so veliko bolj zanesljiva poročanja poslovnih študij, ki so pravzaprav edina možna alternativa (Goel & Shawky, 2009).

2.3.3 Dinamičen sistemski model upravljanja z informacijsko varnostjo

Nazareth in Choi (2015) izpostavljata problematiko, da formalni modeli za informacijsko varnost zagotavljajo vodila za vzpostavitev varnostnih politik, ekonomski modeli zagotavljajo vodila za investicije in varnost, vsak poskus upravljanja z viri z namenom izboljšanja informacijske varnosti pa mora vsebovati razumevanje dinamičnih vidikov informacijskih groženj ter naporov za preprečevanje in upravljanje s kibernetskimi napadi. Slika 1 prikazuje dinamičen sistem informacijsko-varnostnega sistema, ki bi bil ustrezen za podjetja in različne organizacije, ki delujejo v gospodarskem prostoru.

Slika 1: Dinamičen model informacijske varnosti



Vir: D. L. Nazareth in J. Choi, 2015, str. 126.

Model kot bistvene pojme navaja naslednje: **nakopičeni varnostni stroški, škoda, zbrana poročila, zbrane ranljivosti in skupni preprečeni napadi**. Vsak izmed pojmov je povezan z določenimi dejavniki, povezave s temi dejavniki pa so označene tudi s plusi in minusi, ki govorijo o tem, ali je vpliv pozitiven ali negativen.

Model vključuje celoten vidik informacijske varnosti, ki se začne pri investicijah v varnost in konča pri obsegu škode in skupnih preprečenih napadih. Znotraj procesa se zvrstijo različne komponente ranljivosti (osnovne in nastale napake programske opreme, varnostni postopki in varnostna tveganja), investicije so obravnavane posebej kot investicije v varnostna orodja in odvračanje napadov, napadi so razloženi z vidika verjetnosti, da se zgodi (privlačnost tarče, image organizacije, zaznana vrednost tarče, motivacija za napad).

Podane so tudi komponente, ki se ne nanašajo na organizacijo temveč storilce. Gre za število napadalcev in dostop do orodij, ki jih za napad potrebujejo. Iz investicij izhaja povezava s sposobnostmi detekcije, česar rezultat je lahko preprečen napad ali uspešen napad. V primeru, da so storilci in napad uspešni, model predpostavlja, da se o tem poroča, zbira informacije in ocenjuje škodo. Ta škoda mora biti opredeljena z vidika neodložljivosti,

obsega, truda, ki je potreben za pravilno oceno tveganj, in truda za povrnitev v prvotno stanje.

Zavedati se je potrebno, da stroški, ki nastanejo v popravljanju nastale škode in vračanju sistema v prvotno stanje, ne prispevajo k zmanjšanju napadov v prihodnosti. Zmanjšanje napadov je doseženo zgolj in samo z odpravljanjem napak in pomanjkljivosti v programski opremi ter s spremembami v varnostnih procesih. Managerji morajo biti previdni v izbiranju aktivnosti za zmanjševanje ranljivosti sistema z namenom varovanja informacijskega premoženja podjetja oziroma organizacije.

Na osnovnem nivoju model managerje opremi z vodili za investicije v varnost in vpliv le-teh na varnost podjetja ali organizacije. Rezultati preverjanj modela kažejo, da kibernetski napadi v primeru, da so uspešni, dajejo signale o ranljivosti sistema, to pa vodi v še bolj pogoste in močnejše napade ter nevzdržne situacije, ki lahko resno ogrozijo informacijsko premoženje. Investicije v varnostne tehnike in implementacija izboljšanih procesov učinkovito preprečujejo tovrstne situacije. Model nakazuje, da imajo različne investicije različne implikacije za skupne stroške, ki nastajajo kot posledica kibernetskih napadov. Splošne implikacije so naslednje (nekatere »samoumevne«, nekatere pa podajajo nov pogled na problematiko) (Nazareth & Choi, 2015):

- Na najbolj osnovnem nivoju – skupni stroški upravljanja z napadi se znižujejo z večanjem investicij v varnost. Ta implikacija pa se ne nadaljuje v nedogled: na neki točki bodo investicije vseeno presegle stroške napadov, nobena investicija pa ni vsemogočna in ne more preprečiti vseh možnih napadov.
- Testiranje različnih varnostnih investicij je pokazalo, da imajo različne učinke in podajajo različna povračila. Največje je pokazala investicija v orodja za zaznavanje in preprečevanje napadov. Izboljšano zaznavanje vodi v manjše število uspešnih napadov in manjšo škodo, ki jo povzročajo, če so uspešni.
- Investicije v odvračanje (varnostne politike, procesi za identifikacijo napadalcev in podobno) so imele precej manjše učinke – večinoma zato, ker vključujejo zaposlene, tj. človeški faktor, ki predstavljajo šibkejši element informacijske varnosti.
- Model prav tako kaže na dejstvo, da so investicije v določena področja boljše kot v druga. To nasprotuje predhodnim prepričanjem, da se bolj obrestujejo vsesplošne kot ozko specifične investicije.

ŠIRŠI TEORETIČNI OKVIR

1.2 Uvod v teoretični okvir

Za lažje razumevanje kiberkriminala si bomo podrobneje ogledali teorije, ki izhajajo iz znanosti o kriminalu, nato pa jih aplicirali v kibernetski prostor ter izpostavili skupne točke in vidike, v katerih teorije niso uporabne oziroma potrebujejo prilagoditve. **Teorija rutinskih aktivnosti** deluje na nivoju družbe oziroma večje organizacije. Glavno vprašanje, na katerega skuša odgovarjati, je, kako poiskati in preprečiti priložnosti za kriminal znotraj rutinskih aktivnosti potencialnih storilcev. Druga teorija, **teorija kriminalnih vzorcev,** temelji na ravni vsakdanjega življenja posameznih storilcev in njihovih lokacij. Raziskuje odkrivanje in preprečevanje priložnosti za kriminal v okviru dnevnih vzorcev, kot na primer vožnja na delo in domov. Tretja teorija je **teorija racionalne izbire.** Temelji na ravni posamezne priložnosti za kriminalno dejanje in se osredotoča na razmerje med stroški in koristmi, ki jih predstavlja priložnost. Glavno vprašanje pri teoriji racionalne izbire je, kako meriti pridobljene koristi v primerjavi s stroški, ki so osnova za kriminalna dejanja (Felson & Clarke, 1998). Pojem **ponavljajoča se žrtev** pa se nanaša na raziskave, ki pravijo, da je ena in ista tarča večkrat žrtev kriminalnih dejanj (Farrell & Pease, 2001).

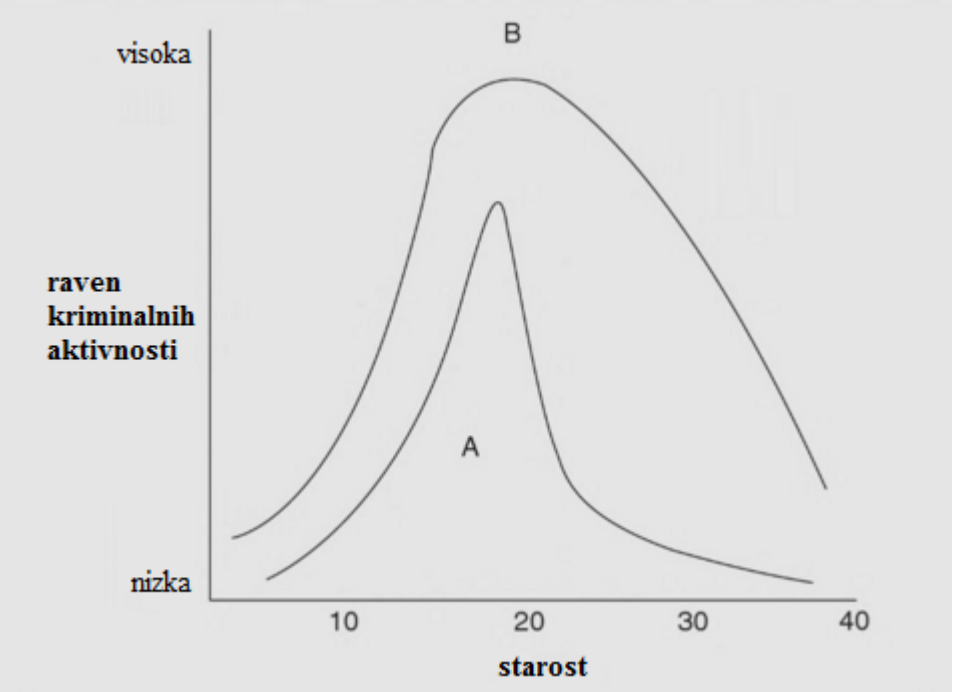
1.3 Teorija rutinskih aktivnosti

Teorija rutinskih aktivnosti predpostavlja, da priložnost za kriminalno dejanje nastane med dnevnimi rutinami, tj. doma, v službi ali med katerimikoli aktivnostmi izven doma, ko: (1) **potencialni storilec** sreča (2) **ustrezno tarčo** ob odsotnosti (3) **sposobnega varuha** (Hartel et al., 2010). Cohen in Felson (1979) trdita, da odsotnost enega izmed teh elementov že preprečuje kriminalno dejanje.

Potencialni storilec je glavni akter v kriminalu in v moderni družbi je kandidatov, ki to lahko postanejo, veliko – kar nekaj raziskav se posveča prepoznavanju agresivnega vedenja že pri otrocih in mladostnikih (Tremblay, 2000), še več pa splošni razširjenosti deviantnega obnašanja, ki vodi v kriminal (Clarke & Weisburd, 1990). Posamezniki so še posebej izpostavljeni skušnjavam v situacijah, kjer je malo nadzora in nizka verjetnost odkritja; zmotno pa je prepričanje o nedolžnosti mladih, saj je največ storilcev v poznih najstniških letih in zgodnjih dvajsetih (Felson & Boba, 2010).

To tudi nakazuje krivulja A na Sliki 2, ki prikazuje starostno gibanje vršilcev kriminalnih dejanj za splošno populacijo, medtem ko krivulja B prikazuje tiste, katerih kriminalna dejanja so vezana na zlorabo prepovedanih substanc, tj. trdih drog. Povzamemo lahko, da se starost storilcev kriminalnih dejanj giblje izrazito okrog 20. leta starosti in po tem letu število kriminalnih aktivnosti izrazito upade, zloraba prepovedanih substanc pa je prisotna tudi med starejšo populacijo – prav tako začne upadati po 20. letu, a bolj postopoma in vse do 40. leta starosti.

Slika 2: Raven kriminalnih aktivnosti glede na starost



Vir: M. Felson in R. L. Boba, 2010, str. 8.

Število potencialnih storilcev je praktično neomejeno, v kontekstu kiberkriminala pa obstaja pomemben aspekt »insajderjev« (angl. *insiders*), oseb znotraj organizacije, ki imajo dostop do internih informacij. Tako imenovana »notranja grožnja« (angl. *insider threat*) ni problem le v večjih organizacijah, kot so CIA in Mednarodni denarni sklad, temveč tudi v manjših podjetjih. Ni težava le, kdo dostopa do informacij, temveč kakšna je narava le-teh: bolj kot so pomembne in občutljive, bolj sofisticirani, ciljno naravnani in pogosti bodo napadi; v zadnjem času pa se pojavljajo tudi tveganja zaradi nenadzorovanega deljenja datotek med sodelavci prek t. i. storitev na oblaku (Lee, 2012).

Ideja predpostavlja, da »mogočni insajderji« predstavljajo večje tveganje kot »šibkejši outsajderji« (Hartel et al., 2010). Notranji napad (angl. *insider attack*) Schultz (2002) opredeljuje kot namensko zlorabo računalniškega omrežja s strani uporabnikov, ki imajo pooblaščen dostop, a ga namesto za opravljanje svojih delovnih obveznosti uporabljajo z namenom izkoriščanja – uničujejo ali kradejo občutljive informacije. Schultz prav tako razbija mit, da so insajderji bolj nevarni. V preteklosti je veljalo, da je več kibernetskih napadalcev znotraj organizacije (izvor v FBI, a predvsem kot posledica slabih računalnikov), sedaj pa študije dokazujejo, da jih številčno ni več kot zunanjih, vendar so pogosteje uspešni. Indikatorji notranjih napadov so: zavestni znaki, ki jih puščajo napadalci, pomenljive napake, pripravljalno vedenje, povezani vzorci uporabe (računalnikov oziroma omrežij), verbalno obnašanje (kot na primer sovražni govor proti delodajalcu ali sodelavcem) ter osebne lastnosti.

Hartel et al. (2010) menijo, da je koncept insajderjev vedno manj pomemben; predvsem kot posledica zabrisanih mej med notranjimi in zunanjimi osebami. Kot prvo, organizacije pogosto z namenom nižanja stroškov zaupajo določene storitve zunanjim izvajalcem (outsourcing), drugi primer so strateške zveze, zaradi česar zaposleni ene organizacije dobijo dostop do informacij druge organizacije, tretja kočljiva zadeva pa so storitve na oblaku, pri katerih dobi dostop do informacij zunanji upravnik oziroma ponudnik storitve shranjevanja na oblaku. Tako do informacij, ki so bile prvotno na voljo le zaposlenim, lahko dostopa še veliko drugih, za katere ne drži več splošna distinkcija med insajderji in outsajderji. Kot rešitev za vedno težje razlikovanje med notranjimi in zunanjimi Felson in Boba (2010) predlagata uporabo termina specializiran dostop (angl. *specialised access*). Gre za pojem, ki loči zaposlene, strateške partnerje ali zunanje izvajalce od vseh ostalih.

Drugi pojem v teoriji rutinskih aktivnosti je **ustrezna tarča.** V znanosti o kriminalu se za ocenjevanje vabljivosti tarč pogosto uporablja seznam »CRAVED«, ki združuje naslednje lastnosti: predstavljiv (angl. ***c**oncealable*), odstranljiv (angl. ***r**emovable*), dosegljiv oziroma dostopen (angl. ***a**vailable*), koristen oziroma dragocen (angl. ***v**aluable*), zanimiv (angl. ***e**njoyable*) in razpoložljiv (angl. ***d**isposable*). Predmeti, ki ustrezajo tem kriterijem, so na primer mobilni telefoni in prenosni računalniki, pa tudi informacije, kot so podatki o kreditnih karticah in podobno. Bolj ko lahko predvidimo, katere stvari so tarče, uspešneje lahko kriminal preprečujemo (Clarke & Webb, 1999). Tarče pa seveda niso le predmeti, temveč tudi osebe – v kontekstu kiberkriminala so to tarče ustrahovanja in nadlegovanja.

Tretja, zadnja komponenta teorije rutinskih aktivnosti, je **sposoben varuh** oziroma **skrbnik.** Zelo tradicionalen primer, kaj se zgodi v odsotnosti skrbnika, je izrazita rast vlomov v 60. letih prejšnjega stoletja v ZDA, ko so tudi ženske začele hoditi v službo in so bili domovi prazni (Cohen & Felson, 1979). Skrbniki, ki bi preprečevali kiberkriminal so zelo različne osebe: v primeru spletnega nadlegovanja otrok so to lahko njihovi starši, na spletnih avkcijah pa so varuhi lahko vigilanti, tj. prostovoljni, samooklicani redarji (kar načeloma ni dobro, saj tako nestrokovnjaki »vzamejo pravico v svoje roke«) (Huang & Wang, 2010).

Debate o uporabnosti teorije rutinskih aktivnosti v kontekstu kiberkriminala so zelo raznolike. Največjo težavo oziroma razliko predstavlja ideja o »prostoru« na spletu. Yar (2005) trdi, da gre za novo družbeno okolje (kibernetski prostor kot nasprotje resničnemu), s svojimi ontološkimi in epistemološkimi strukturami, interakcijskimi oblikami, vlogami in pravili ter omejitvami in možnostmi. Hartel et al. (2010) predlagajo štiri alternative ideji prostora tradicionalnega kriminala:

- IP naslov (internetni protokol),
- geografsko temelječe predstave prostora, kot na primer ISP naslov ali točke z dostopom do brezžičnega interneta,
- internet sam, kot omrežje, katerega struktura je lahko izrabljena, ter

- semantična predstava prostora (virtualni prostori za srečevanje so lahko prostor kiberkriminala).

Če povzamemo, po teoriji rutinskih aktivnosti tudi kiberkriminal potrebuje potencialnega storilca, ustrezno tarčo in odsotnost sposobnega varuha oziroma skrbnika; dilema, ki jo je potrebno raziskati, pa je, kaj je v kibernetskem prostoru bližina v pojmu prostora.

1.4 Teorija kriminalnih vzorcev

Teorija kriminalnih vzorcev (angl. *crime patten theory*) predpostavlja, da storilci priložnost za kriminalno dejanje najdejo tekom dnevne rutine, tj. nekje med domom, delom in prostim časom. Posledično so kriminalna dejanja skoncentrirana v določen čas in prostor, kar označujemo s pojmom »vroče točke« (angl. *hot spots*) (Brantingham & Brantingham, 1993). Znanje o t. i. vročih točkah je lahko uporabljeno za zaščito oseb, ki so bile žrtev kriminala, saj je s predvidevanji o tem, kaj so vroče točke, kje so in kdo je potencialna žrtev, izvajanje preventivnih ukrepov veliko bolj učinkovito (Bowers et al., 2004). Po tem sistemu lahko, na primer, ugotovimo, kateri so najbolj pogosti deli mesta, na katerih se dogajajo kriminalna dejanja in na podlagi tega razporedimo policijsko delo bolj učinkovito (Bowers & Johnson, 2005).

Tradicionalni kriminal običajno poteka serijsko, saj zaradi fizičnih omejitev storilec ne more izvesti več dejanj hkrati. To pomeni, da sta s tradicionalnim kriminalnim dejanjem povezana določen prostor in čas, odnos med storilcem in žrtvijo pa je »ena-na-ena« (Brenner & Clarke, 2005). Nasprotno pa je opredelitev časa in prostora v spletnem kriminalu praktično nemogoča – storilec lahko izvede več kriminalnih dejanj naenkrat na različnih krajih (na tisoče računalnikih) povsod po svetu. Posledično za kiberkriminal ni splošne opredelitve, kaj bi lahko bile vroče točke. Do sedaj najdena izjema so nadlegovanja v spletnih klepetalnicah, ki jih lahko opredelimo kot neke vrste prostor, čeprav virtualni (Hartel et al., 2010).

Če je vzvod kriminalnega dejanja internet, ga je enostavno izvesti na več mestih na svetu istočasno; storilec lahko, na primer, združi računalnike v neke vrste zbirko in istočasno napade spletne strani po vsem svetu. V tem kontekstu lahko za vroče točke označimo računalnike, ki so bolj pogosto v uporabi, ker imajo več povezav in transakcij kot ostali računalniki. Če je internet vzvod kriminalnih dejanj, je lahko tudi vzvod preprečevanja le-teh (Hartel et al., 2010):

I. Obstajajo spletne strani, ki sledijo kreditnim karticam. Tako lahko kdorkoli preveri, če je bila njegova kartica ukradena oziroma zlorabljena (Franklin, Paxson, Perrig & Savage, 2007).
II. Vse aktivnosti na spletu puščajo neke vrste sledi. Na spletu je te sledi laže odkriti kot v fizičnem svetu (van der Aalst & de Medeiros, 2005).

1.5 Teorija racionalne izbire

Tretja teorija je teorija racionalne izbire. Koncept se uporablja predvsem v ekonomiji, psihologiji in sociologiji. Njene korenine segajo v filozofijo 19. stoletja, v kontekst kriminala pa sta jo vpeljala Cornish in Clarke (2008). Teorija racionalne izbire predpostavlja, da je obnašanje posameznika vodeno na podlagi pričakovanih posledic. Z vidika kriminala to pomeni, da potencialni storilci pretehtajo stroške in koristi ter se za izvedbo posameznega kriminalnega dejanja odločijo, ko so izračunane koristi večje od stroškov.

Zaradi pomanjkanja znanja in informacij, odločitve običajno temeljijo na *omejeni racionalnosti* – posameznik težko pozna vse možne posledice, lahko pa je tudi predmet določene situacije, na primer pod vplivom alkohola. Temu primerno teorija racionalne izbire ne pomeni, da se storilci odločajo preudarjeno in koristno v dolgoročnem smislu – ravno obratno. Za neko kriminalno dejanje se odločijo hitro in pod pritiskom, pri čemer skušajo maksimirati koristi in minimizirati tveganja (Hartel et al., 2010). Uporabljajo t. i. hitro in varčno hevristiko (angl. *fast and frugal heuristics*) (Gigerenzer & Goldstein, 1996), kar pomeni, da iščejo kognitivne bližnjice do sprejemanja odločitev, običajno glede na pretekle izkušnje ali izkušnje kolegov. Vlomilci, na primer, izbirajo enostavno dostopne hiše, prve ali zadnje v vrsti, in takšne, v katerih lahko storilec ostane skrit. Pogosto pa so bolj zaposleni z minimiziranjem tveganj kot povečevanjem koristi (Cromwell & Olson, 2004).

Teorija racionalne izbire je bila v preteklosti že aplicirana na znanost o informacijski varnosti. Študije so pokazale, da je deljenje gesel in odpiranje sumljive elektronske pošte pravzaprav dejanje racionalne izbire (Aytes & Connolly, 2004) ter da je nizka stopnja samokontrole, ki je faktor, ki vpliva na racionalnost izbire posameznika, povezana s piratskim prisvajanjem programske opreme (Higgins, 2004).

Te predpostavke so uporabili tudi na področju družbenih ved – Epstein (1999) na primeru omejene racionalnosti z vidika posameznikovega znanja in uporabe računalnika, Malleson, Heppenstall in See (2010) pa v obliki simulacije kriminalnih dejanj z osredotočenjem na vlamljanje, in sicer na individualni ravni.

V kontekstu kiberkriminala je hipoteza enaka kot pri tradicionalnem kriminalu – storilci so nagnjeni k omejeni racionalnosti. Iz tega izhaja, da moramo ugotoviti, kaj so pri kiberkriminalu koristi in stroški ter kaj je tisto, na podlagi česar se storilci kiberkriminalnih dejanj odločajo.

1.6 Koncept ponavljajoče se žrtve

Zadnja teoretična predpostavka, ki jo iz tradicionalnega kriminala lahko uporabimo pri razlaganju kiberkriminala je koncept ponavljajoče se žrtve (angl. *repeat victimization*). Nanaša se na dejstvo, da veliko kriminalnih dejanj cilja na eno in isto žrtev večkrat – te žrtve pa so lahko osebe, organizacije ali gospodinjstva. Kljub temu, da je trend dobro poznan, je boj proti pojavu ponavljajočih se žrtev težak, ker so policijski zapisniki problematični, raziskovanje z intervjuvanjem žrtev pa tudi povzroča določene težave. Če pa je ponavljanje prepoznano, je tudi reduciranje kriminala bolj dosegljivo (Farrel & Pease, 2001).

V raziskavi iz Velike Britanije je kar 63 % žrtev kriminalnih dejanj v zvezi z zasebno lastnino ter 77 % žrtev kriminalnih dejanj na osebni ravni že bilo žrtev ne dolgo nazaj. Gospodinjstva, ki so tarča vloma, so običajno tarča dvakrat v krajšem časovnem obdobju (Bowers & Johnson, 2005).

Koncept ponavljajoče se žrtve so raziskovali tudi na primeru študentk v ZDA. Rezultati so pokazali, da se spolni napadi pogosto ponovijo v roku enega meseca, vrste napada pa so večinoma enake kot prvič. V primerih, ko se je žrtev branila ali napad prijavila, je bilo ponavljajočih se napadov manj (Daigle, Fisher & Cullen, 2008). Druga raziskava, osredotočena na ponavljajoče se žrtve, pa je dokazala, da se v okviru nasilja v družini koncept zmanjšuje na podlagi dobrega osveščanja – 6 od 10 oseb po prvem primeru nasilja v družini ni bilo več žrtev (Robinson, 2006).

V kontekstu kiberkriminala je poročanje nedokončno. Tatovi na primer vedo, da če podjetju ukradejo vse prenosne računalnike, da jih bodo nadomestili, zato se bodo vrnili in jih ponovno okradli. Pri tem seveda ne gre le za strošek nakupa nove opreme, temveč za (lahko precej višje) stroške izgubljenih informacij. Na eni strani zaposleni izgubijo podatke, s katerimi delajo, na drugi strani pa dostop do le-teh dobijo nepooblaščene osebe, ki jih lahko zlorabijo (Kitteringham, 2008).

Drug primer ponavljajoče se žrtve v kontekstu kiberkriminala pa je vdiranje v elektronsko pošto, saj so starejše generacije za to področje precej bolj ranljive in s tem bolj privlačne za storilce (Templeton & Kirkman, 2007).

Koncept ponavljajoče se žrtve ni perspektiva, kot prej opisane teorija rutinskih aktivnosti, teorija kriminalnih vzorcev in teorija racionalne izbire, vendar je eden izmed pomembnih vidikov, ki izhajajo iz znanosti o kriminalu. Ravno rezultati zgoraj omenjenih študij kažejo na to, da je s prepoznavanjem koncepta število napadov možno zmanjšati.

2 RAZVOJ IN TRENUTNA RAZŠIRJENOST

2.1 Globalni obseg kiberkriminala

Kiberkriminal se širi predvsem s prisotnostjo povezav za komercialne namene. To pomeni, da so globalno gledano prve žrtve najbolj razvite države z najvišjimi stopnjami prihodkov. Posledica, ki jo razširjenost kiberkriminala povzroča, je škoda, ki jo dela uspehu podjetij in državnim gospodarstvom.

Kiberkriminal uničuje trgovanje, konkurenčnost, inovacije in globalno gospodarsko rast ter ima za svet precej širši pomen, kot je bilo predpostavljano. Po izračunih CSIS (2014) je letni strošek kiberkriminala na globalni ravni med 375 in 575 bilijoni dolarjev. V razvitih državah ima kiberkriminal tudi velik vpliv na zaposlovanje, in sicer z vidika prehoda zaposlovanja stran od delovnih mest, ki prinašajo vrednost.

Kot posledica manjšega BDP-ja v ZDA, študije namigujejo, da bi kiberkriminal lahko povzročil izgubo delovnega mesta za 200.000 državljanov. V Evropski uniji se številka giblje okrog 150.000, pri čemer je problematično dejstvo, da bi zaradi kiberkriminala ljudje morali zamenjati dobro plačane službe za nižje plačane, ali pa ostali brez nje. Napovedi so naslednje (CSIS, 2014):

- Stroški kiberkriminala se bodo povečevali s prenašanjem poslovnih funkcij na splet in z vedno večjo uporabo spleta s strani podjetij in potrošnikov.
- Povečevale se bodo izgube z naslova intelektualne lastnine, ker bodo tisti, ki si s kiberkriminalom prilaščajo tujo intelektualno lastnino, razvijali sposobnosti proizvodnje konkurenčnih izdelkov.
- Kiberkriminal postaja »davek« na inovacije in upočasnjuje hitrost globalnih inovacij z zmanjševanjem donosnosti naložb inovatorjev in investitorjev.
- Vlade bi morale začeti z vzpostavljanjem resnega in sistematičnega napora v zbiranje in objavljanje podatkov o kiberkriminalu, s čimer bi državam in podjetjem omogočali boljše sprejemanje odločitev v zvezi s tveganji in politikami.

Glede na delež BDP-ja imajo največ stroškov na račun kiberkriminala Nemčija, Nizozemska, Norveška, ZDA in Kitajska. Samo v ZDA je bilo v letu 2013 kar 3000 podjetij žrtev kiberkriminalnega napada, v Perzijskem zalivu sta dve banki izgubili 45 milijonov dolarjev v nekaj urah, britansko podjetje pa je v enem napadu izgubilo 1,3 milijarde dolarjev. Brazilske banke poročajo, da njihove stranke izgubljajo milijone zaradi spletnih prevar in goljufij, v Indiji pa je bilo v dveh letih napadenih 308.371 spletnih strani.

Glede na pomanjkljivo poročanje o napadih lahko sklepamo, da jih je še več in škoda še bolj obsežna. Ko je bil leta 2010 napaden Google, so skušali posledice prikriti, vseeno pa je na

dan prišla informacija, da je takrat izgubo intelektualne lastnine utrpelo 34 podjetij izmed Fortune 500. Kljub ogromnim napadom pa je zelo malo napadalcev identificiranih, kaj šele ujetih in kaznovanih (CSIS, 2014). Slika 3 prikazuje strošek kiberkriminala kot delež BDP-ja posameznih držav.

Kot je razvidno z zemljevida, so dobri faktorji napovedovanja stopnje dohodkov – bogatejše države (ali bogatejša podjetja in organizacije) so bolj pogoste tarče, kajti bogatejše in revnejše tarče običajno zahtevajo približno enako truda, bogatejše pa storilcem kiberkriminalnih dejanj prinašajo večje dobičke.

Po deležu BDP-ja kiberkriminal največ stroškov povzroča v Nemčiji, na Nizozemske, v ZDA in na Kitajskem, vse večje težave pa imajo tudi države v razvoju. V Braziliji, na primer, so hekerski napadi vedno bolj sofisticirani – hekerske skupnosti so aktivne in imajo dobre inženirske sposobnosti. To pa skupaj s slabim zavedanjem o nevarnostih kiberkriminala med podjetji in organizacijami (pa tudi med potrošniki) pojasni, zakaj so njihovi stroški iz tega naslova tako visoki.

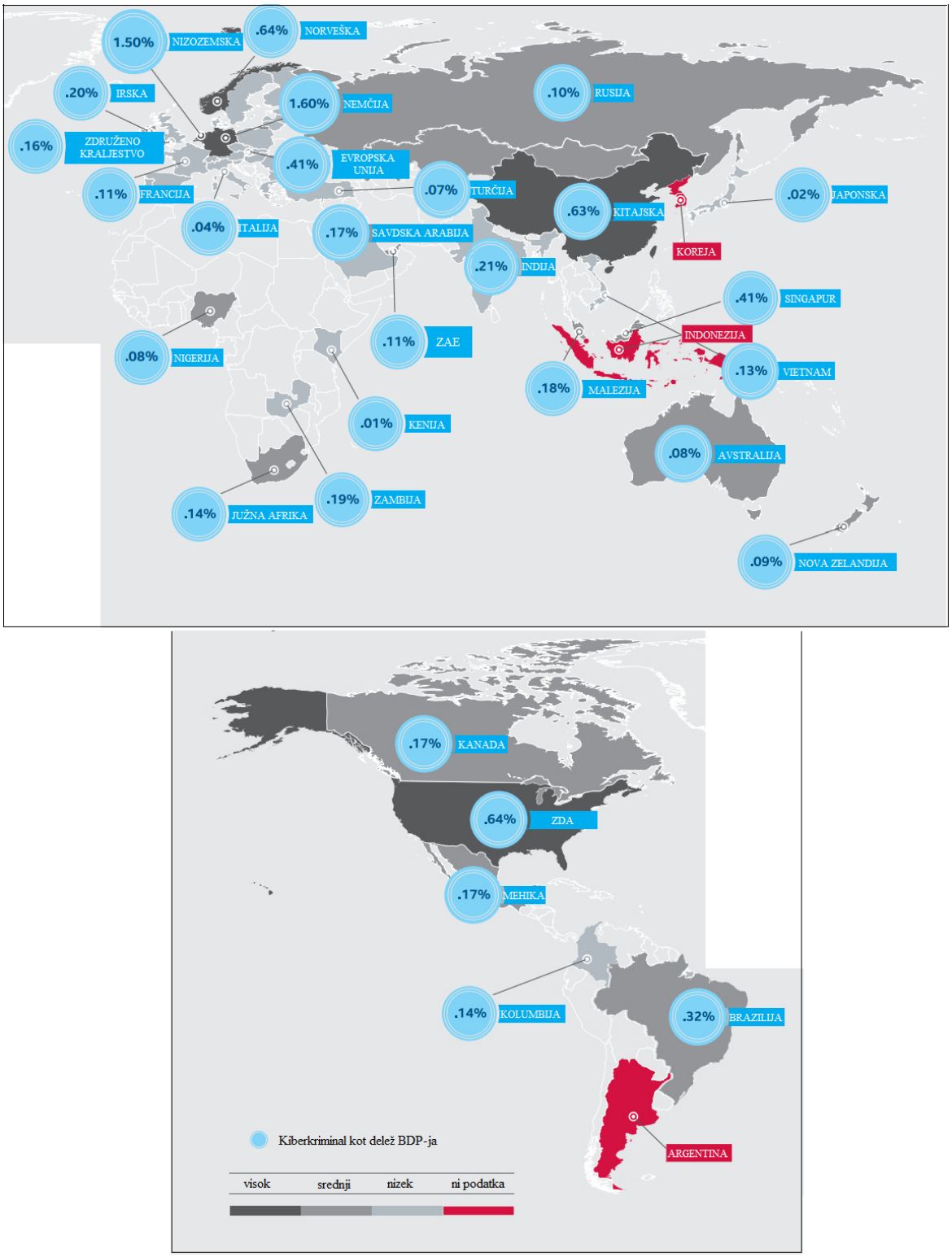
Pri merjenju stroškov, ki jih povzroča kiberkriminal, je najtežje oceniti strošek ukradene intelektualne lastnine. Izkoriščanje le-te s strani storilca kiberkriminalnega dejanja lahko traja dolgo časa, pri tem pa se ne da oceniti, kolikšne izgube ima podjetje ali organizacija kot posledica tega, da ni edina, ki deluje na podlagi te intelektualne lastnine (CSIS, 2014).

Raziskave kažejo tudi to, da spletno gospodarstvo na letni ravni ustvari približno 2 do 3 trilijone USD. Za ta delež se pričakuje, da bo zelo hitro naraščal. Če so izračuni CSIS (2014) pravilni, to pomeni, da kiberkriminal »vzame« med 15 in 20 % vrednosti, ki jo ustvari spletno gospodarstvo.

Pomanjkanje podatkov pomeni, da vsaka ocena škode, ki jo kiberkriminal povzroča, temelji na nepopolnih podatkih. Zelo malo držav se temu resno posveča, večina se sploh ne. Ocena CSIS (2014) temelji na podatkih o kraji intelektualne lastnine, prevarah in stroških sanacije nastale škode; podatki so bili pridobljeni za 51 držav sveta, ki skupaj tvorijo 80 % globalnih dohodkov.

Prisotne so velike razlike med državami (kot posledica enega napada največ izgubijo podjetja v ZDA); ena možna razlaga je, da storilci tarčo izbirajo glede na vrednost in enostavnost dostopa. Ravno kombinacija visokih vrednosti, nizkega tveganja in nizkega faktorja dela (relativno nizek napor za, na primer, vdor v neko omrežje), povzroča hitro rast kiberkriminala.

Slika 3: Kiberkriminal kot delež BDP-ja.



Vir: CSIS, 2014, str. 8 in 9.

Pri merjenju obsega in razširjenosti kiberkriminala je problematično tudi to, da so na voljo zelo različni podatki – za Evropsko unijo se številke gibljejo vse od 16 milijard dolarjev do slabega bilijona dolarjev, za Japonsko pa podatki pravijo, da v enem napadu nastane pol toliko škode kot v podjetjih v ZDA, Nemčiji ali na Kitajskem, kar pomeni, da so realne številke verjetno precej višje kot tiste v poročilih. Še večja težava pa so države v razvoju, saj večina vlad ne zbira nobenih podatkov o kiberkriminalu v svoji državi. Države z nižjimi stopnjami dohodkov zaenkrat ne trpijo velikih izgub, kar pa se bo spremenilo s povečanjem uporabe interneta za komercialne namene; za storilce kiberkriminalnih dejanj so še posebej privlačne mobilne platforme (CSIS, 2014).

2.2 Dejavniki razvoja in širjenja

Začetki kiberkriminala segajo v čase, ko so manjše skupine hekerjev za zabavo in prestiž vdirale v kompleksne, visoko organizirane hierarhije voditeljev, inženirjev, denarnih mul in vojaških redov. Z razvojem je kiberkriminal postal dobro organiziran več milijard vreden posel, s katerim se ukvarjajo specialisti, katerih glavni namen je iskanje novih načinov za vdiranje v omrežja in krajo podatkov. Storilci so v prisvajanju informacij in denarja inovativni ter ostajajo en korak pred varnostno industrijo s širokim naborom področij: od kreditnih kartic in informacij o bankah do podatkov o identifikaciji oseb. Trud, da bi rast upočasnili (zaščita, obramba in zapiranje spletnih trgovin »podzemlja«), je precej neučinkovit (Thompson, 2014).

Glavni dejavniki razvoja kiberkriminala so na eni strani stopnja razvitosti države, višina prihodkov, zaščita, zakonodaja in uporaba interneta za komercialne namene, na drugi strani pa splošna vrednost tarč ter nizko tveganje nizek faktor potrebnega dela oziroma truda. Kibernetski napadalci običajno svojo žrtev izberejo na podlagi razmerja med enostavnostjo izvršitve napada in vrednostjo, ki jo lahko pridobijo (CSIS, 2014).

2.3 Globalni obseg kiberkriminala v obdobju 2013–2015

Glede na zgoraj omenjene dejavnike obseg kiberkriminala in stroški le-tega vsako leto nekoliko narastejo. Po vsakoletni raziskavi, ki jo na primeru sedmih držav opravlja Ponemon Institute, je skupen strošek napadov v letu 2015 znašal 7,7 milijonov ameriških dolarjev, kar je skoraj dva odstotka več kot leta 2014 (Ponemon Institute, 2015).

Ponemon Institute je sprva (šest let nazaj) svoje raziskave izvajal le v ZDA, nato dodal Združeno Kraljestvo, Nemčijo, Avstralijo in Japonsko, zatem še Rusijo, v letu 2015 pa prvič vključil tudi Brazilijo. Rezultati kažejo, da kibernetski napadi, ki ciljajo na vlade in komercialne organizacije, kontinuirano naraščajo tako v pogostosti kot v stopnji silovitosti

napadov. V študijo so bili vključeni napadi, ki so se zgodili kot posledica spletne aktivnosti (torej napadi, izvedeni prek interneta). Te napadi so vključevali krajo intelektualne lastnine organizacije, zaseganje spletnih bančnih računov, ustvarjanje in razširjevanje škodljivih virusov, objava občutljivih informacij (poslovnih skrivnosti) ter motenje državne ključne omrežne infrastrukture. Raziskava je vsako leto izvedena z namenom ocenjevanja ekonomske škode, ki jo kiberkriminal povzroča – boljše razumevanje in poznavanje omogoča učinkovitejše načrtovanje zaščite in alokacije sredstev za preprečevanje in blaženje kiberkriminala. Pri oceni ekonomske škode se upošteva tako neposredne kot posredne stroške.

Med **neposredne stroške** (ali interne) sodijo:

I. stroški zaznavanja,
II. stroški obnove in povrnitve v stanje pred napadom,
III. stroški preiskovanja napadov in
IV. stroški upravljanja z napadi.

Posredni stroški (ali eksterni), ki nastanejo kot posledica napadov, pa so naslednji:

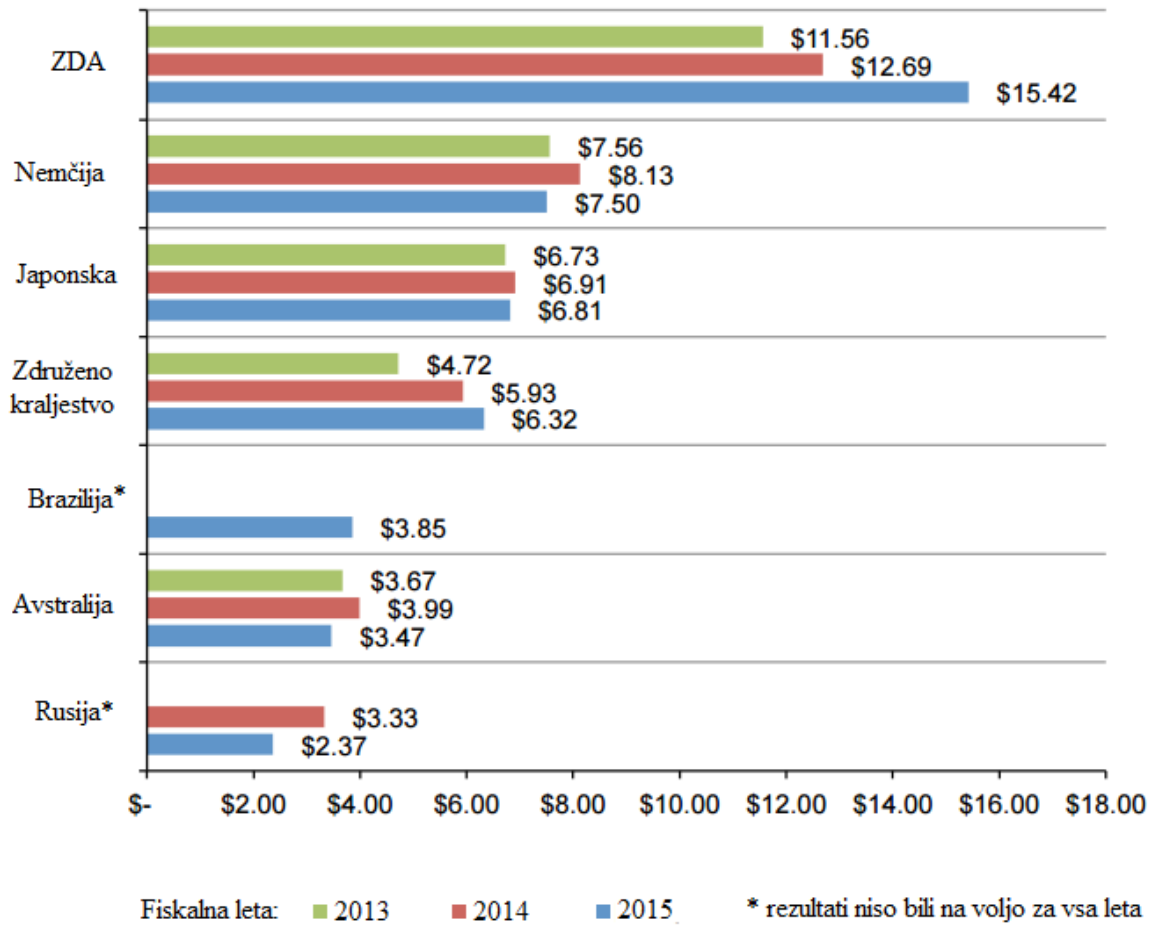
V. prekinitve in motnje poslovanja ter
VI. izguba (zaupanja) strank.

V te stroške pa niso vključeni tisti stroški, ki nastanejo kot izdatki in investicije za vzpostavljanje in ohranjanje informacijske varnosti znotraj organizacij ter usklajevanje z državnimi standardi, pravili in predpisi.

V nadaljevanju bomo na podlagi grafičnih prikazov predstavili gibanje – predvsem naraščanje – ekonomske škode, ki jo povzroča kiberkriminal v sedmih obravnavanih državah: ZDA, Nemčiji, na Japonskem, v Združenem Kraljestvu, Braziliji, Avstraliji in Rusiji. Raziskava je vključevala 252 organizacij, znotraj katerih je bilo intervjuvanih 2.128 zaposlenih na vodstvenih pozicijah, v izračune pa je bilo vključenih 1.928 napadov. Ocena ekonomske škode bo predstavljena glede na pretekla leta, po posameznih državah, vrstah napadov in upravljanja z le-temi (Ponemon Institute, 2015).

Slika 4 prikazuje skupen strošek, ki ga na letni ravni kiberkriminal povzroča v sedmih izbranih državah. Stroški so izraženi v milijonih, valuta pa je ameriški dolar (n=252).

Slika 4: Skupen strošek na letni ravni po posameznih državah

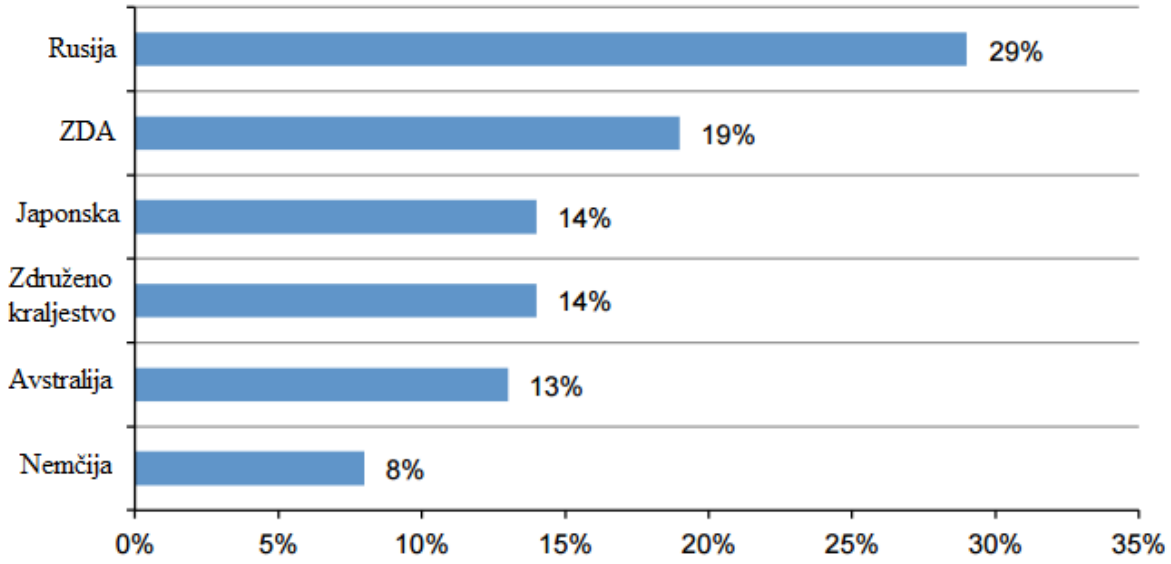


Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015, str. 2.

Kot je razvidno iz grafa, so med državami velike razlike. Najvišje stroške in tudi najbolj izrazito naraščanje stroškov kiberkriminala je opaziti pri ZDA, nekoliko manj pri Združenem kraljestvu. Pri Rusiji manjka podatek za leto 2013, ker je bila prvič v raziskavo vključena šele v letu 2014, pri Braziliji pa manjkata podatka tako za leto 2013 kot 2014, ker je bila v letu nastajanja poročila, tj. 2015, vključena prvič.

Pri branju grafa je potrebno upoštevati, da za Nemčijo, Japonsko, Avstralijo in Rusijo rezultati kažejo na nižanje stroškov kot posledica kiberkriminala, vendar je do tega prišlo zaradi menjalnih razmerij med lokalno valuto in močnim ameriškim dolarjem. Preračunano v dolarje procentualna sprememba med letoma 2014 in 2015 znaša 1,9 %. Ob upoštevanju lokalnih valut, pa je naraščanje stroškov kiberkriminala vidno pri vseh sodelujočih državah, kar prikazuje Slika 5.

Slika 5: Neto sprememba skupnih stroškov kiberkriminala v enem letu



Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015, str. 3.

Za Brazilijo izračun spremembe ni bil mogoč zaradi manjkajočih podatkov iz leta 2014. Največja neto sprememba je prisotna v Rusiji in ZDA, najmanjša pa v Nemčiji.

Procentualna povprečna neto sprememba, izračunana na podlagi lokalnih valut, znaša 13,9 %. Spodnje ugotovitve so povzete glede na vrednosti, izražene v ameriških dolarjev. Bistvene implikacije globalnih opažanj (Ponemon Institute, 2015):

I. **Kiberkriminal znotraj organizacij še vedno narašča**. Srednja letna vrednost 252 vključenih organizacij znaša 7,7 mio USD (najnižja vrednost je 0,31 mio USD, najvišja pa 65 mio USD). V letu 2014 je bila skupna letna vrednost 7,6 mio USD.
II. **Strošek kiberkriminala variira glede na velikost organizacije**. V študiji je bila velikost organizacij opredeljena glede na »sedeže« – število zaposlenih, ki so neposredno povezani na osrednje omrežje organizacije. Rezultati so pokazali pozitivno razmerje med velikostjo organizacije in višino stroškov, povzročenih s strani kiberkriminala, vendar pa imajo manjše organizacije glede na »sedeže« izrazito višji strošek *per capita* (1.388 USD) kot večje organizacije (431 USD).
III. **Organizacije v vseh panogah so žrtev kriminala, le ne v enaki meri.** Največji letni stroški, ki jih povzroča kiberkriminal, so prisotni v sektorju finančnih storitev, javnih služb in energetike. Precej nižji so stroški v zdravstvu, avtomobilski industriji in kmetijstvu.

IV. **Največje stroške povzročajo naslednje oblike kiberkriminala:** zlonamerni zaposleni, odpoved storitve in spletni napadi. Blaženje in zmanjševanje tovrstnih oblik zahteva posebno specializirano tehnologijo, kot na primer sisteme za preprečevanje vdorov, SIEM – pristop k varnostnemu managementu, ki omogoča zaznavanje groženj organizacijski varnosti in holističen pogled na organizacijsko varnost informacijske tehnologije (angl. *Security Information and Event Management*), uporaba testnih sistemov za ugotavljanje varnosti ter GRC pristop (angl. *Governance, Risk management, and Complience*), ki ima podobno vlogo kot SIEM.

V. **Kibernetski napadi postanejo zelo dragi, če niso razrešeni takoj.** Rezultati so pokazali povezanost med časom, potrebnim za zajezitev napada, in stroški za organizacijo. Razrešen napad sicer ne pomeni, da je bil dokončno ustavljen. Povprečno število dni za odpraviti napad je 46; povprečni stroški na dan znašajo 21.155 USD, skupaj to nanese 973.130 USD.

VI. **Prekinitev poslovanja oziroma motenje le-tega predstavlja največji eksterni strošek; drugi največji pa je strošek, povezan z izgubo informacij.** Na letni ravni prekinitev poslovanja predstavlja 39 % vseh eksternih stroškov. V to so vključeni stroški zaradi prekinitve dela zaposlenih in neuspešni poslovni procesi.

VII. **Največji interni strošek predstavlja zaznavanje napadov; drugi največji strošek pa je »okrevanje«, vrnitev v prvotno stanje.** Na letni ravni stroški zaznavanja in okrevanja skupaj znašajo 53 % vseh stroškov internih aktivnosti – predvsem nastajajo kot izgubljena produktivnost zaposlenih in neposredno delo zaposlenih na tem, da poslovanje spravijo nazaj v primarno stanje.

VIII. **Znotraj organizacij na področju omrežne infrastrukture največ sredstev dobijo aktivnosti, ki so povezane z informacijsko-tehnološko zaščito.**

IX. **Uvedba varnostno-obveščevalnega sistema naredi razliko.** Strošek kiberkriminala je ublažen z uporabo varnostno-obveščevalnega sistema – rezultati raziskave sugerirajo, da je s pomočjo tovrstne tehnologije organizacija bolj uspešna in učinkovita pri zaznavanju in omejevanju kibernetskih napadov. Organizacije brez takšnih sistemov imajo povprečno 1,9 milijonov USD več stroškov s kiberkriminalom.

X. **Organizacije, ki imajo varnostno-obveščevalni sistem, so dosegale do 23 % večji ROI.** Precej višji ROI (21 %) so dosegle organizacije, ki imajo izdatne kodirne tehnologije, ter tudi visok ROI (20 %) so dosegle organizacije, ki imajo ogradne nadzorne sisteme, kot so na primer: UTM, NGFW in IPS.

XI. **Uporaba varnostnih praks v upravljanju znotraj organizacij znižuje stroške kiberkriminala.** V organizacijah, kjer so zaposleni strokovnjaki za to področje, se stroški kiberkriminala lahko znižajo tudi do 1,5 milijona USD; v organizacijah, kjer je nekdo vodja varnosti na visokem nivoju, pa so stroški nižji za 1,3 milijona USD.

Te rezultati so zelo podobni predhodnim (Ponemon Institute, 2014). Izredno zaskrbljujoče je le, da vsako leto narašča čas, ki je potreben za obvladovanje napada. V letu 2013 je bilo potrebno število dni 27, v letu 2014 je bilo potrebno število dni 31, kar je pomenilo 23-odstotno rast, v letu 2015 pa je številka zrastla na 46 dni.

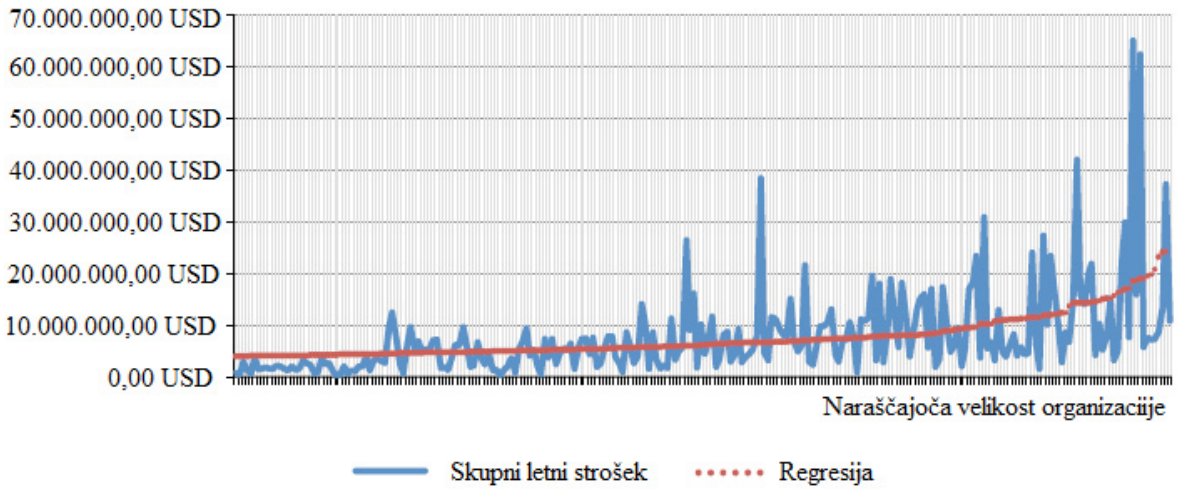
Povečali so se tudi stroški – leta 2013 je bil strošek 27-dnevnega obvladovanja 509.665 USD, leta 2014 za 31-dnevnega obvladovanja (posameznega) napada 639.462 USD, leta 2015 pa je – skladno z izrednim naraščanjem števila dni za obvladovanje, strošek znašal 973.130 USD.

To pomeni, da se je število dni za obvladovanje v teh letih skoraj podvojilo, prav tako stroški, ki pri tem nastajajo (Ponemon Institute, 2014; Ponemon Institute 2015). Iz tega sklepamo, da če organizacije vedno več pozornosti, časa, truda in sredstev namenjajo varnostnim ukrepom, lahko zgoraj opisano naraščanje dni, potrebnih za razrešitev, in naraščanje stroškov, za odpravo škode, nakazuje na to, da so napadi postali dvakrat bolj resni oziroma škodljivi. To pomeni, da so napadalci kljub vsem varnostnim politikam in obveščevalnim sistemom še vedno en korak pred organizacijami (in stroko).

2.4 Kazalniki in ocena ekonomske škode za obdobje 2013–2015

V prejšnjem podpoglavju smo med glavnimi ugotovitvami zapisali, da strošek kiberkriminala variira glede na velikost organizacije – večja kot je organizacija, večji so stroški (predvsem kot močnejša preventiva, pa tudi kot posledica). Slika 6 prikazuje, kako naraščajo stroški glede na število »sedežev« – najmanjša organizacija, ki je bila vključena v raziskavo (leva stran slike), ima 673 »sedežev«, največja pa 79.367 »sedežev«.

Slika 6: Letni stroški kiberkriminala glede na velikost organizacije



Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015, str. 8.

Modra črta prikazuje skupni letni strošek organizacij, rdeča pa indicira pozitivno korelacijo med večanjem organizacije in naraščanjem stroškov kiberkriminala. Razen petih večjih odstopanj, stroški naraščajo precej enakomerno z večanjem organizacije. V naslednjih dveh tabelah so podani bolj podrobni stroški kiberkriminala v letih 2013, 2014 in 2015. Organizacije so glede na velikost razdelili v štiri kvartile. Prva tabela prikazuje povprečni strošek glede na posamezen kvartil, druga pa prikazuje strošek na »sedež« v organizaciji, prav tako so organizacije glede na velikost porazdeljene v kvartile. V vsakem kvartilu je približno 62 organizacij. V prvem kvartilu so najmanjše organizacije, v četrtem pa največje.

Tabela 1: Letni stroški kiberkriminala po kvartilih (v USD)

	2013	**2014**	**2015**
	(n=234)	**(n=257)**	**(n=252)**
Prvi kvartil (najmanjše organizacije)	2.965.464	2.967.723	3.279.376
Drugi kvartil	4.453.688	5.107.532	5.246.519
Tretji kvartil	6.659.478	8.321.024	8.987.450
Četrti kvartil (največje organizacije)	14.707.980	13.805.529	13.372.861

Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015 , str. 8.

V organizacijah, ki so razvrščene v prvi, drugi in tretji kvartil, stroški vsako leto naraščajo, pri organizacijah četrtega kvartila pa je strošek od leta 2013 naprej padal. Možen razlog je lahko to, da so zaradi ogromnih izgub z naslova kibernetskih napadov izgubili že ogromno sredstev in časa ter so temu primerno začeli uvajati varnostno-obveščevalne sisteme in ostale

ukrepe za preprečevanje kiberkriminala. Naslednja tabela (Tabela 2) prikazuje stroške kiberkriminala na »sedež« v organizaciji. Razporejenost organizacij po kvartilih je enaka kot pri Tabeli 1 (tj. približno 62 organizacij na kvartil; organizacije z najmanj »sedeži« so v prvem kvartilu, tiste z največ pa v četrtem).

Tabela 2: Letni stroški kiberkriminala per capita po kvartilih (v USD)

	2013	**2014**	**2015**
	strošek na »sedež«	**strošek na »sedež«**	**strošek na »sedež«**
Prvi kvartil (najmanjše organizacije)	1.388	1.601	1.555
Drugi kvartil	710	962	878
Tretji kvartil	532	726	709
Četrti kvartil (največje organizacije)	431	437	368

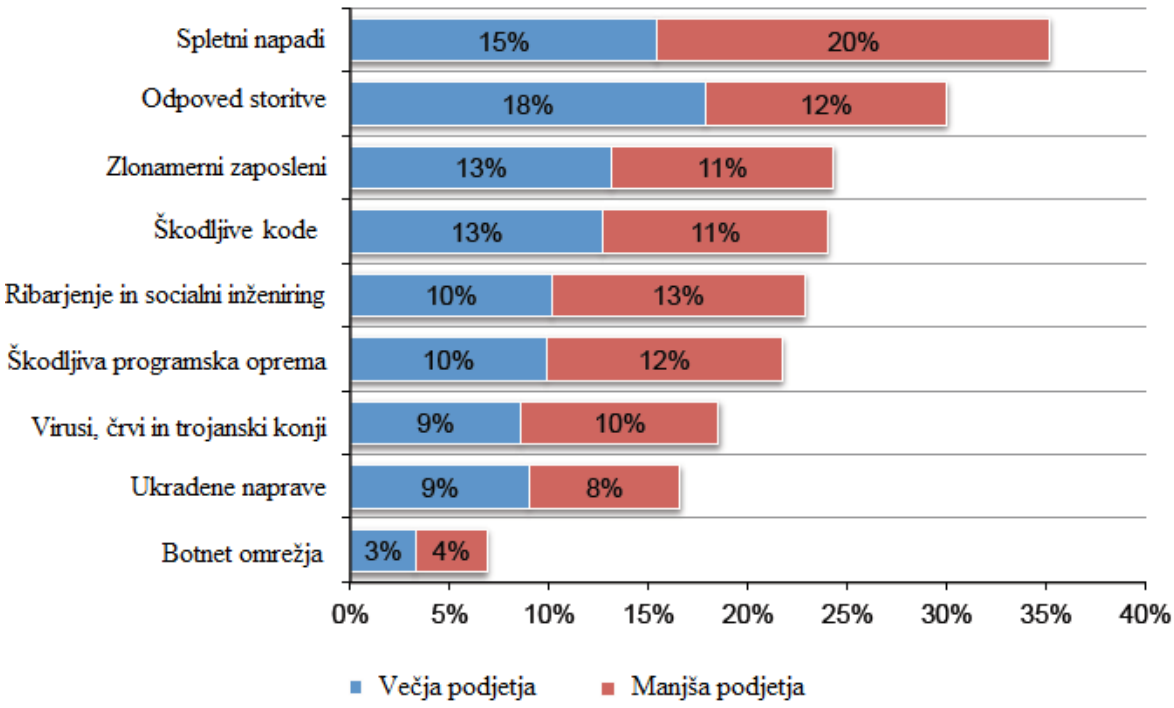
Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015 , str. 8.

Iz tabele je razvidno, da je bil že leta 2013 strošek *per capita* v najmanjših organizacijah kar 3,2-krat višji kot v največjih organizacijah. Leta 2014 se je ta razlika povečala, v najmanjših organizacijah je strošek kiberkriminala *per capita* znašal 3,6-krat več kot v največjih organizacijah, leta 2015 pa celo 4,2-krat več. V vseh štirih kvartilih se je strošek leta 2014 v primerjavi z 2013 povečal, nato pa v 2015 zmanjšal, le da za različno stopnjo.

Najbolj izrazito razliko stroškov *per capita* med najmanjšimi in največjimi organizacijami v letu 2015 lahko pripišemo dvema razlogoma: pri najmanjših je opaziti trend splošnega naraščanja kibernetskih napadov na organizacije, pri največjih pa ponovno – zaradi velikih stroškov kot posledica kibernetskih napadov v preteklosti, so temu primerno začeli uvajati varnostno-obveščevalne sisteme in ostale ukrepe za preprečevanje kiberkriminala.

Slika 7 prikazuje, kako se razlikuje strošek za upravljanje s kiberkriminalom v manjših podjetjih (tj. podjetjih, manjših od mediane vzorca) in v večjih podjetjih (tj. podjetjih, ki so večja od mediane vzorca), **glede na posamezno vrsto napada** (mediana je znašala 8.703 »sedežev«).

Slika 7: Razmerje stroškov kiberkriminala glede na vrsto napada



Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015, str. 9.

Iz slike je jasno razvidno, da nekatere vrste napadov povzročajo veliko več stroškov kot druge. Manjše organizacije, tj. tiste z manj kot 8.703 »sedeži«, imajo največ stroškov z upravljanjem s spletnimi napadi, precej manj z odpovedjo storitve, zlonamernimi zaposlenimi, škodljivimi kodami, ribarjenjem in socialnim inženiringom, škodljivo programsko opremo ter virusi, še manj z ukradenimi napravami, daleč najmanj stroškov (4 % vseh stroškov kiberkriminala v organizaciji) pa povzročajo bonet omrežja.

Pri večini vrst napadov imajo podoben delež stroškov tudi velike organizacije, pomembna razlika pa je pri spletnih napadih in odpovedih storitev. V manjših organizacijah spletni napadi predstavljajo 20 % stroškov, v velikih le 15 %. Kar se tiče odpovedi storitev, pa je trend obraten – večji delež stroškov imajo velike organizacije, kar 18 %, manjše organizacije pa imajo z odpovedjo storitev stroške v vrednosti 12 % stroškov vseh kibernetskih napadov.

Kljub temu, da stroški zaradi zlonamernih zaposlenih niso najvišji, pa so najbolj pogosti in tudi zahtevajo več časa za rešitev. Znotraj tega pojma moramo upoštevati tudi »insajderje«, ki niso neposredno zaposleni – na primer poslovni partnerji, ki imajo dostop do različnih informacij. Po eni izmed tovrstnih raziskav 59 % ljudi, ki so odpuščeni ali dajo odpoved, ukradejo podatke, ki so last organizacije.

Izpostavljene so tri vrste **zlonamernih »insajderjev«** (Zaharia, 2015):

- »zlonamerni zaposleni« so najmanj pogosti, ampak imajo potencial za povzročitev izredne škode – na podlagi stopnje dostopa, ki jo imajo. Še posebej tvegani so administratorji s privilegiranimi identitetami.
- »izkoriščeni zaposleni« so tisti, ki jih zunanje stranke prelisičijo in pripravijo do tega, da razkrijejo gesla ali podatke, ki jih ne bi smeli.
- »neprevidni zaposleni« pa so tisti, ki preprosto pritisnejo napačno tipko in nenamerno izbrišejo ali spremenijo ključne informacije.

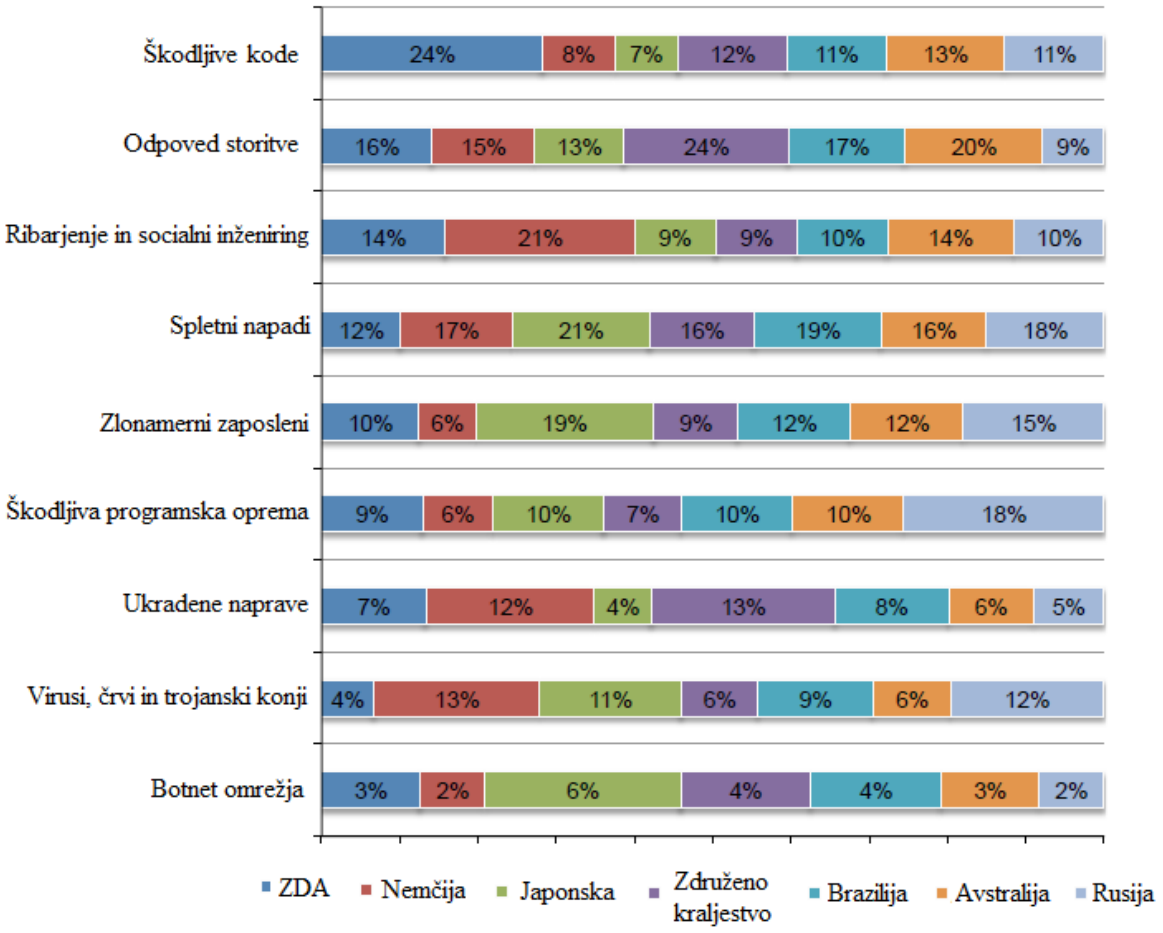
Povprečni čas, ki ga organizacije porabijo za razrešitev škode, nastale zaradi zlonamernih zaposlenih, je 54,4 dni. Glede na vrste napadov je to največ, na drugem mestu so škodljive kode (47,5 dni), ostale vrste napadov pa so razrešene v pol krajšem času kot napadi zlonamernih zaposlenih ali še hitreje (Ponemon Institute 2015):

- Spletni napadi: 27,7 dni,
- Ribarjenje in socialni inženiring: 21,9 dni,
- Odpoved storitve: 19,3 dni,
- Ukradene naprave: 12,3 dni,
- Škodljiva programska oprema: 5,8 dni,
- Virusi: 2,4 dni ter
- Botnet omrežja: 2,2 dni.

Stroški, ki jih povzročajo posamezne oblike kiberkriminala se močno razlikujejo tudi po državah. Škodljive kode so, na primer, daleč največja težava v ZDA, odpoved storitev, na drugi strani, pa je velik problem v Združenem Kraljestvu in Avstraliji. Ribarjenje in socialni inženiring v največji meri predstavljata težavo v Nemčiji, s spletnimi napadi se morajo največ ukvarjati podjetja in organizacije na Japonskem, prav tako imajo na Japonskem največ problemov z zlonamernimi zaposlenimi, škodljiva programska oprema izrazito največ škode dela v Rusiji, ukradene naprave v Združenem kraljestvu in v Nemčiji, isti državi in Rusija imajo tudi največ stroškov z virusi, črvi in trojanskimi konji, botnet omrežja pa največ – a še vedno zelo malo – stroškov povzročijo na Japonskem. (Ponemon Institute, 2015).

Slika 8 prikazuje procentualne deleže stroškov, ki jih kiberkriminal povzroča, glede na posamezno obliko napada in ločeno glede na sedem obravnavanih držav.

Slika 8: Procentualni deleži letnih stroškov glede na obliko napada

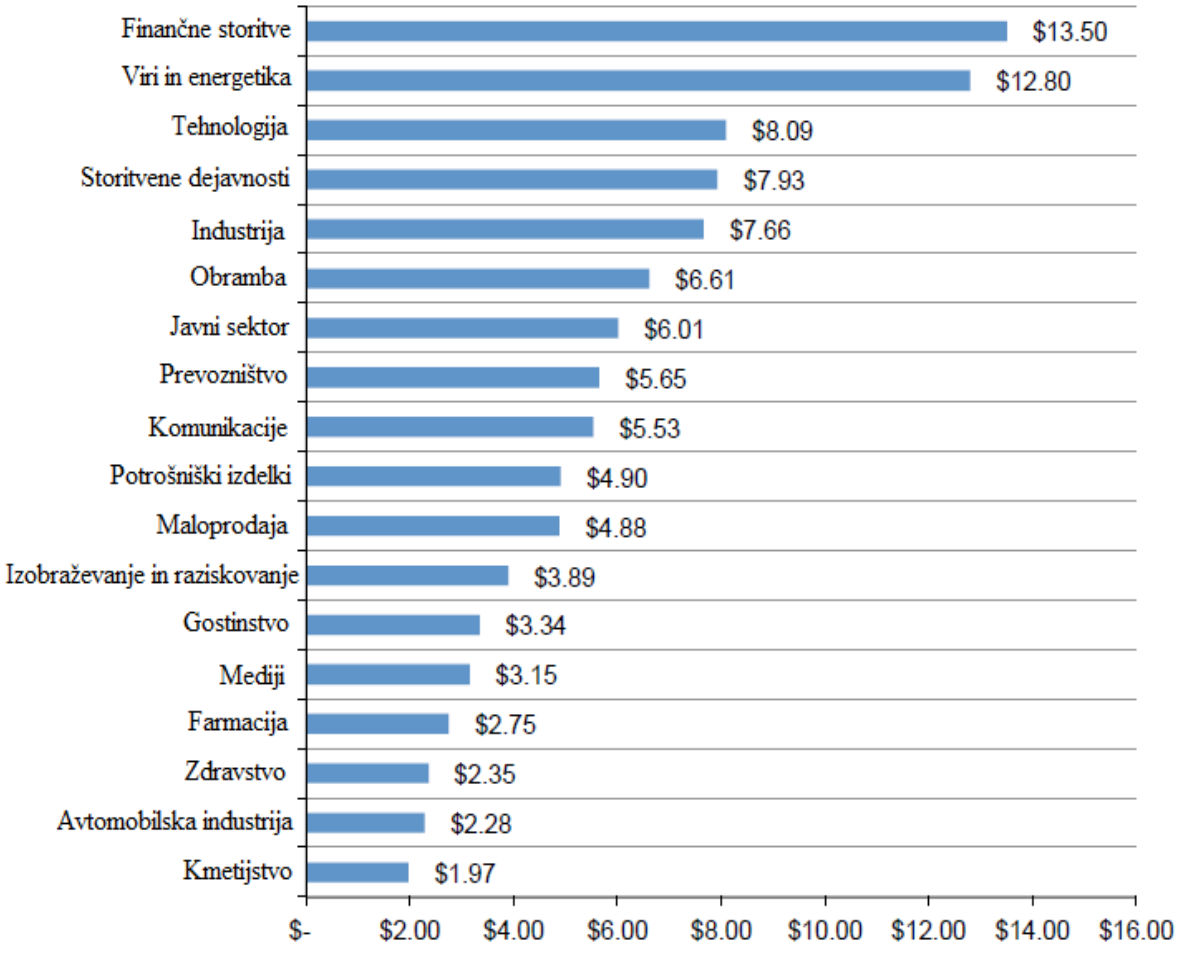


Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015, str. 12.

V eni izmed poglavitnih ugotovitev o globalnem kiberkriminalu (v poglavju 4.2) smo zapisali, da **prizadene vse industrijske panoge, le ne vseh v enaki meri**. Največje stroške imajo ponudniki finančnih storitev ter viri in energetika, najmanj pa področje zdravstvene oskrbe in farmacija, izobraževalni sektor, mediji, avtomobilska industrija in kmetijstvo. Na Slika 9 prikazuje letne stroške po posameznih panogah. Zneski so izraženi v milijonih dolarjev (USD).

Kot razlog, zakaj imajo največje stroške ponudniki finančnih storitev ter viri in energetika, lahko navedemo tudi stalno posodabljanje varnostnih sistemov, saj so stroški napadov veliko bolj ključni za posel kot, na primer, pri maloprodaji, kjer bistvo panoge ni tako močno vezano na računalniško infrastrukturo.

Slika 9: Letni strošek kiberkriminala glede na industrijo



Vir: Ponemon Institute, Global Report on the Costs of Cyber crime 2015 , str. 8.

Strošek, ki ga kiberkriminal predstavlja v finančnih storitvenih podjetjih, je skoraj 7-krat večji kot tisti v kmetijstvu, kar potrjuje zgoraj opisano trditev, da je kiberkriminal prisoten v vseh panogah, le v nekaterih precej več kot drugih. V srednjih razredih stroškov se gibljejo, na primer, maloprodaja, potrošniški izdelki, komunikacije in prevozništvo.

Sami stroški pa nastanejo predvsem kot (Ponemon Institute, 2015):

- izguba produktivnosti,
- neposredno dodatno delo,
- denarni izdatki,
- posredno dodatno delo in
- režijski stroški.

Pomemben aspekt stroškov, ki nastajajo kot posledica kiberkriminalnih napadov, so tisti stroški, ki jih je težko ali nemogoče meriti neposredno. V raziskavo, ki jo izvaja Ponemon Institute tako, na primer, niso vključeni stroški kraje intelektualne lastnine, ki lahko na področjih, kot so različne vrste oblikovanja (industrijsko, grafično … sploh v digitalni obliki), nastanejo v zelo kratkem času in v enako kratkem času uidejo izpod nadzora.

Druga problematika, ki je ne merijo eksplicitno, pa je izguba strank ali njihovega zaupanja – če pride do odpovedi storitve ali uhajanja informacij, stranka hitro oceni, da podjetje morda ni več zanesljivo in poišče novega ponudnika oziroma partnerja. Na dolgi rok to lahko povzroča ogromne stroške, saj mora podjetje oziroma organizacija iskati nove stranke, graditi novo zaupanje, pri vsem tem pa morda tudi veliko sredstev vlagati v odnose z javnosti, da popravi zunanji imidž.

Čisto drugačen pogled na zadevo pa v svojem delu predstavi Bernik (2014), ki meni, da je izjemno vseobsegajoča ekonomska škoda, ki jo zaradi kriminalitete v kibernetskem prostoru trpijo države, posamezne organizacije in tudi individualne osebe, pravzaprav fiktivna. Stroški, ki jih raziskave s poročili o velikih finančnih izgubah merijo, naj bi bili večinoma stroški investicije v zaščito, ki pa ni 100-odstotno učinkovita. Tisti, ki se ukvarjajo z varnostjo v kibernetskem prostoru, ugotavljajo, da je bolj pomembno in predvsem ceneje ozaveščanje zaposlenih (in ostalih, če govorimo o izpostavljenosti kiberkriminalu na ravni posameznikov), to pa naj bi imelo večji vpliv na varnost s kibernetskega vidika.

Poudarja, da so stroški napadov in zlorab sistemov veliko nižji, kot so stroški zaščite sistema. Velika večina načinov merjenja, ki so se v zadnjem času uveljavili na nivoju tehničnih služb znotraj organizacij, ni premostilo tega prepada. Zaradi tega razloga so storilci kiberkriminalnih dejanj v toliko boljšem položaju, da s svojimi aktivnostmi dosežejo še večjo dobičkonosnost. Zgoraj omenjeni prepad se še bolj veča kot posledica tehnološkega napredka in predstavitvijo novih, predvsem mobilnih tehnologij, istočasno pa časopisi vsakodnevno poročajo o napadih, kar v splošni javnosti povzroča še večjo pozornost in previdnost v zvezi s to problematiko. Bernik (2014) svoje ugotovitve podkrepi in primerja tudi z raziskavo, ki jo izvaja Ponemon Institute. Kot pomanjkljivost te raziskave ne omenja tiste, ki smo jo opisali zgoraj (intelektualna lastnina ter izguba strank in njihovega zaupanja), temveč to, da v oceno ekonomske škode niso vključeni stroški, ki nastanejo kot posledica pravnih storitev, ki nastanejo, če stranka, ki je bila napadena, toži neko podjetje oziroma organizacijo in gre zadeva na sodišče.

Med ugotovitvami navaja, da se je skupno število žrtev spletnih napadov zmanjšalo, kar je lahko posledica večjega zavedanja različnih groženj in nevarnosti ter posledica bolj premišljenega obnašanja naprednejših uporabnikov spleta (Bernik, 2014).

Na drugi strani je strošek posameznega napada zrastel za 50 %. Višji strošek posameznega napada naj bi bil posledica vedno bolj sofisticiranih napadov, ki storilcem kiberkriminalnih dejanj omogočajo, da v enem napadu pridobijo več denarja kot kadarkoli prej. Število naivnih uporabnikov, ki še vedno menijo, da bodo z lahkoto pridobili velike vsote denarja, pa še vedno ostaja visoko – njihovo upanje je kot tarča kibernetskih napadalcev hitro spremenjeno v razočaranje obup, čemur sledijo stroški in sorodna škoda. Takšni napadi so še posebej prisotni v organizacijah, in sicer kot zloraba s strani zaposlenih. Posledica so izgubljene informacije poslovnega značaja (Bernik, 2014).

Detica (2011) pa v svojem poročilu vključuje tudi stroške, ki smo jih omenili kot pomanjkljivost raziskave, ki jo opravlja Ponemon Institute – škoda, ki jo kiberkriminal povzroči ugledu podjetja oziroma organizacije ter splošna izguba zaupanja v spletne transakcije. Detica svoj model merjenja stroškov, ki v organizacijah nastajajo kot posledica kiberkriminala, postavi na podlagi naslednjih treh tipov kibernetskih napadov:

- tradicionalne oblike kriminalnih dejanj, kot so prevare in ponarejanje, le da so izvedene v kibernetskem kontekstu (vezano predvsem na elektronsko posredovano komunikacijo, omrežja in informacijske sisteme);
- javno objavljanje nelegalnih vsebin prek elektronskih medijev (na primer: otroška pornografija, rasna nestrpnost in širjenje sovraštva na podlagi le-te);
- kriminalna dejanja, ki so značilna posebej za elektronska omrežja: napadi na informacijske sisteme, odpoved storitev in hekerski napadi.

Na podlagi teh vrst napadov predlagajo naslednje štiri kategorije stroškov (Detica, 2011):

I. **stroški predvidevanja kiberkriminala**, ki vključujejo varnostne ukrepe posameznikov in organizacij, stroške zavarovanja in stroške za vzpostavljanje zahtevanih standardov informacijske tehnologije;
II. **stroški posledic kiberkriminala**, ki vključujejo neposredne izgube posameznikov ali organizacij ter posredne stroške, ki nastanejo zaradi zmanjšane komercialne uporabe IP-jev in kot izgubljene priložnosti zaradi zmanjšane konkurenčnosti;
III. **stroški, ki nastanejo kot odgovor na kiberkriminal**, kot na primer kompenzacija plačil žrtvam kraje identitete in posredni stroški vključenih pravnih entitet;
IV. **neposredni stroški kiberkriminala** pa vključujejo tudi faktorje, kot so: škoda ugledu, izguba zaupanja posameznikov in organizacij v spletne transakcije, zmanjšanje prihodkov iz javnega sektorja in porast sive ekonomije.

3 ZMANJŠEVANJE KIBERKRIMINALA

3.1 Uvod v zmanjševanje kiberkriminala

Največjo težavo pri zmanjševanju in preprečevanju kiberkriminala predstavlja dejstvo, da z nastajanjem novih tehnologij kiberkriminal ni omejen na nove metode starih oblik kriminalnih dejanj, tako kot je tradicionalni kriminal, temveč nastajajo popolnoma nove oblike, drugačne od obstoječih (Brenner, 2012).

Konvencionalni model zaščite osebnih in poslovnih računalniških omrežij temelji na statični obrambi, ki vključuje (Thompson, 2014):

- sistem za zaznavanje motenj (IDS; angl. *intrusion detection system*),
- sistem za preprečevanje motenj (IPS; angl. *intrusion prevention system*) in
- antivirusne programe.

Neodvisno predstavljajo posamezne končne točke varnostnih ukrepov, skupaj pa tvorijo poglobljeno obrambno strategijo. Sistemi delujejo na podlagi prepoznavanja znakov škodljive programske opreme (ali škodljivih datotek). Kar je zaznano sumljivo, je poslano naprej opremi, ki jih preveri in temu primerno reagira.

Ko so vse tri zgoraj opisane komponente uporabljene skupaj, kot model poglobljene zaščite uspešno zmanjšujejo tveganja škode, ki bi lahko nastala kot posledica kiberkriminalnega napada. Ta vrsta zaščite pa sicer predpostavlja, da imajo napadalci ves čas prednost pred tistimi, ki skušajo napade preprečiti, zaradi konstantno spremenljive tehnologije in neodkritih šibkih točk programske opreme in računalniških omrežij (Thompson, 2014).

V raziskavi, ki se je osredotočala na učinkovitost 26 najboljših antivirusnih programov, so ugotovili, da niti eden izmed izbranih pri zaznavanju škodljivih vsebin ne deluje 100 % učinkovito. Nesposobnost zaznave je bila posledica novih virusov in nazadovanje v zaznavanju predhodno znanih a nekoliko posodobljenih virusov. Glavna implikacija raziskave je bila, da je za 100-odstotno zaznavanje potrebnih 15 antivirusnih orodij (Bishop, Bloomfield, Gashi & Stankovic, 2011).

Leto kasneje je bila izvedena zelo podobna raziskava, ki je podala sorodne rezultate. V vzorec je bilo vključenih 32 antivirusnih programov, ki so bili izpostavljeni 1599 virusom. Ponovno se noben izmed antivirusnih programov ni izkazal za 100-odstotno zanesljivega oziroma ni zaznal vseh virusov. Sicer so imeli antivirusni programi zelo visoke stopnje zaznavanja in niti en virus se ni izognil več kot 14 različnim antivirusnim programom.

Tudi pri tej raziskavi sta bila razloga za nezaznavanje določenih virusov pojav novih virusov in nazadovanje v zaznavanju predhodno znanih virusov, ki jih napadalci le nekoliko posodobijo oziroma spremenijo (Bishop, Bloomfield, Gashi & Stankovic, 2012).

3.2 Principi za zmanjševanje priložnosti tradicionalnega kriminala

Tako kot pri osnovnih teorijah, ki izhajajo iz znanosti o kriminalu in so poenostavile razumevanje kiberkriminala, je možno iz tradicionalnega kriminala povzeti tudi principe in tehnike za zmanjševanje priložnosti. Pri tem je potrebno upoštevati naslednji dejstvi (Hartel et al., 2010):

I. Če želimo preprečiti kriminalno dejanje, ga moramo najprej dobro razumeti – razumeti, zakaj je prišlo do dejanja; na podlagi tega je kriminalna dejanja laže preprečiti, vse pa je odvisno od specifičnih kontekstov in ciljev deležnikov.
II. Vsi principi in posledično tudi tehnike pa morajo biti obravnavane kot delo v nastajanju.

Z napredkom v raziskovanju in s širjenjem znanja o kriminalu se bo preprečevanje povečalo, principi in tehnike bodo narastle v številu, upravljanje s kiberkriminalom pa bo s tem postalo bolj uspešno in učinkovito.

Pet osnovnih principov za zmanjšanje priložnosti za izvedbo tradicionalnega kriminalnega dejanja je (Hartel et al. 2010):

- **povečanje potrebnega truda** za izvedbo kriminalnega dejanja (na primer: boljše ključavnice zahtevajo več truda za odklepanje na silo, prav tako bolj kompleksna gesla zahtevajo več časa, da se jih ugane);
- **povečanje tveganja** (na primer: dobro osvetljena okna povečajo možnost, da se vlomilca opazi in ujame pri delu, povečati se da tudi možnost, da je heker ujet med opazovanjem omrežij);
- **zmanjšanje koristi** izvedenega kriminalnega dejanja (na primer: označene dele ukradenega avta ali drugega vozila je teže preprodati naprej, enako velja za zakodirane podatke);
- **zmanjšanje provokativnosti**, ki izvablja kriminalno vedenje (na primer: hitra odstranitev grafitov odvrača grafitarje k ustvarjanju novih, podobno velja za zrušene spletne strani, ki jih hitro postavijo nazaj), ter
- **odstranitev »opravičil«** za kriminalno vedenje (na primer: znak, ki ljudi spodbuja k plačevanju neke storitve je bolj učinkovit, če z njega »gleda« par oči, izobraževanje uporabnikov interneta o tem, katere storitve so brezplačne in katere plačljive, pa bi tudi zmanjšalo piratsko prisvajanje vsebin).

Za vsakega od teh generičnih principov obstaja pet tehnik, kar je skupaj povezano pod imenom »**25 tehnik za zmanjševanje priložnosti kriminalnih dejanj**«. Prvi trije principi se nanašajo na **ekonomske** stroške in koristi, četrti in peti pa se nanašata na **psihološke** stroške in koristi. Za vsak generični princip so izpeljane naslednje tehnike (Cornish & Clarke, 2003):

- **Povečanje potrebnega truda za izvedbo kriminalnega dejanja**:
- utrjevanje tarče (ključavnice za volan),
- nadzorovanje dostopa (vnos telefona),
- pregledovanje izhoda (vstopnice tudi za izhod),
- preusmerjanje storilcev kriminalnih dejanj (zapora ceste) in
- nadzor posrednikov (»pametne« pištole).

- **Povečanje tveganj**:
- razširitev in podaljšanje varovanja (dodatni varnostni ukrepi – večerni izhodi v skupinah; puščanje znakov uporabe; prenašanje telefona),
- naraven nadzor (izboljšana ulična razsvetljava),
- zmanjšanje anonimnosti (ugotavljanje taksistove identitete),
- postavljanje »managerjev« (video nadzor dvonadstropnih avtobusov) in
- formalen nadzor (kamere ob semaforjih).

- **Zmanjšanje koristi izvedenega kriminalnega dejanja**:
- skrivanje tarč (parkiranje izven ulic),
- odstranjevanje tarč (odstranljivi avto-radii),
- identifikacija lastnine (označevanje osebnih predmetov),
- motnje trga za potencialno preprodajo (nadzor zastavljalnic) in
- zanikanje koristi (označbe blaga s črnilom, ki se razlije ob nasilni odstranitvi).

- **Zmanjšanje provokativnosti, ki izvablja kriminalno vedenje**:
- zmanjševanje frustracij (učinkovite čakalne vrste in vljudnost pri storitvah),
- izogibanje nasprotnikov (ločeni vhodi na stadion za navijače posameznih nasprotnih nogometnih ekip),
- zmanjševanje razburjenja (nadzor nad nasilno pornografijo),
- nevtraliziranje pritiska vrstnikov (spodbujanje in vsesplošno objavljanje sloganov, kot je »Ko pijem, ne vozim«) in
- odvračanje od posnemanja (hitro popravilo škode, ki nastane zaradi vandalizma)

- **Odstranitev »opravičil« za kriminalno vedenje**:
- vzpostavitev pravil (najemna pogodba),
- objava navodil (»Ni parkiranja«),
- opozorila (znaki za omejitev hitrosti ob cesti),
- podpora predpisom (enostaven izpis iz knjižnice) in

- nadzor zaviralcev predpisov (alkotesti v lokalih).

3.3 Aplikacija principov tradicionalnega na kiberkriminal

V prejšnjem podpoglavju naštetih 25 generičnih tehnik za zmanjševanje priložnosti za izvedbo kriminalnih dejanj se ne da neposredno aplicirati na kiberkriminal, obstaja pa kar nekaj študij, ki predlagajo uporabo orodij informacijske varnosti v skladu s temi 25 tehnikami.

Prva takšna študija je delo avtorjev Beebe in Rao (2005). Temelji na povezavi 44 tehnik informacijske varnosti in 16 tehnik, ki so bile predhodnice prej razloženih 25 tehnik. Več kot polovica izmed teh 44 tehnik se nanaša na prvi princip zmanjševanja priložnosti kriminalnih dejanj, tj. »povečanje potrebnega truda za izvedbo kriminalnega dejanja«. Sklep avtorjev je, da je potrebno raziskovanje v smeri, ki bi podala različne tehnike preprečevanja priložnosti kiberkriminala tudi za področje preostalih generičnih principov, ne le prvega.

Naslednjih nekaj sorodnih del se nanaša na 25 generičnih tehnik zmanjševanja priložnosti. Prva se je osredotočala na (Brookson, Farrell, Mailley, Whitehead & Zumerle, 2007):

- prevare prek mobilnih telefonov,
- prevare prek stacionarnih telefonov,
- prevare v zvezi s predvajanjem TV-vsebin,
- vdore prek spleta,
- zlorabo brezžičnih omrežij in
- zlorabo povezav Bluetooth.

Tehnike so bile uspešno aplicirane na zgoraj naštete primere kiberkriminala, kar prikazuje Tabela 3.

Tabela 3: Aplikacija 25 tehnik na kiberkriminal

I. Povečanje truda	**II. Povečanje tveganj**	**III. Zmanjšanje koristi**	**IV. Zmanjšanje provokativnosti**	**V. Odstranitev "opravičil"**
utrjevanje tarče	**razširitev varovanja**	**skrivanje tarč**	**zmanjševanje frustracij**	**vzpostavitev pravil**
- algoritmi za kodiranje	- sistem za zbiranje info o prevarah	- začasne identifikacije	- večkratno preverjanje uporabnika	- pravila za uporabo omrežij

Se nadaljuje

Tabela 3: Aplikacija 25 tehnik na kiberkriminal (nadaljevanje)

I. Povečanje truda	**II. Povečanje tveganj**	**III. Zmanjšanje koristi**	**IV. Zmanjšanje provokativnosti**	**V. Odstranitev "opravičil"**
- požarni zid		- izklop vidnosti povezave Bluetooth	- nižanje stroškov končnih uporabnikov	
- video prenos		- demilitarizirana območja za prikrivanje omrežij		
nadzorovanje dostopa	**naraven nadzor**	**odstranjevanje tarč**	**izogibanje nasprotnikov**	**objava navodil**
- overitev brezžičnih telefonov	- oznaka za uporabo Bluetooth povezave	- izklop povezave Bluetooth	- upravljanje z blogi, klepetalnicami …	- jasno vpisovanje za pooblaščen dostop
- pametne kartice				- varnostne politike v podpis zaposlenim
pregledovanje izhoda	**zmanjšanje anonimnosti**	**identifikacija lastnine**	**zmanjševanje razburjenja**	**opozorila**
- implementacija revizijskih vpisov	- standardi za digitalne podpise	- standardi za digitalne podpise		- okenca "poskus ilegalnega dostopa"
- zakonito prestrezanje podatkov	- preprečevanje namišljenih IP-jev	- mednarodna identifikacijska št. klicatelja		- opozorila o piratskih poskusih
	- ID klicatelja			
preusmerjanje storilcev	**postavljanje "managerjev"**	**motenje preprodaje**	**nevtraliziranje pritiska vrstnikov**	**podpora predpisom**
	- sistemi za zaznavo motenj	- naprave po dostopnih cenah	- podpora obsojanju spletnih vdorov	- večstopenjsko preverjanje uporabnika
		- preverjanje prodajaln		

Se nadaljuje

Tabela 3: Aplikacija 25 tehnik na kiberkriminal (nadaljevanje)

I. Povečanje truda	II. Povečanje tveganj	III. Zmanjšanje koristi	IV. Zmanjšanje provokativnosti	V. Odstranitev "opravičil"
nadzor posrednikov	**formalen nadzor**	**zanikanje koristi**	**odvračanje od posnemanja**	**nadzor zaviralcev predpisov**
- uvrščanje ukradenih naprav na črn seznam	- zakonito prestrezanje podatkov	- črni seznami ukradenih naprav	- opozarjanje na neuspele vdore	
			- preprečevanje širjenja informacij o tehnikah vdorov	

Vir: C. Brookson, G. Farrell, J. Mailley, S. Whitehead & D. Zumerele, 2007, str. 27.

Naslednja raziskava, ki je tehnike tradicionalnega kriminala aplicirala na kiberkriminal, je delo avtorjev Coles-Kemp in Theoharidou (2010). Osredotočala se je na problematiko zlonamernih »insajderjev« in v teoretični okvir informacijske varnosti s pomočjo tehnik tradicionalnega kriminala dodala psihološke in organizacijske faktorje.

Newman in Clarke (2003) predstavita aplikacijo tehnik na primeru spletnih trgovin, Willison in Siponen (2009) pa na primerih poneverb in v povezavi z zlonamernimi »insajderji« (še vedno je zaslediti pomanjkanje razumevanja motivacij za dejanja zaposlenih 28 % raziskovanih organizacij, kjer prihaja do tovrstnih težav; raziskani pa so načini vzpostavljanja varnostnega sistema).

Najpogosteje so v študijah omenjene in pojasnjene, tudi empirično potrjene s strani različnih avtorjev, naslednje tehnike (Hartel et al., 2010):

I. **Gesla in PIN kode**: So v uporabi za dokazovanje avtentičnosti; omenjeni v vseh študijah, so osnovno orodje informacijske varnosti. Žal si je dobro geslo ali PIN kodo težko zapomniti, zato je večina gesel in PIN kod, ki so trenutno v uporabi, zelo preprostih.
II. **Kodiranje podatkov**: Večinoma omenjeno kot tehnika prvega principa za zmanjševanje priložnosti, in sicer »utrjevanje tarče«, ali kot zmanjšanje oziroma zanikanje koristi. Če so podatki kodirani, jih je moč razvozlati samo z ustreznim dekodirnim sistemom, le-tega pa tisti, ki ukrade prenosni računalnik (ali drugo sorodno napravo), običajno nima. S tem ukradena naprava za storilca dejanja nima vrednosti.

III. **Požarni zid**: je v uporabi za preprečitev dostopa potencialno zlonamernim in škodljivim povezavam ali računalniškim omrežjem. Tudi požarni zid se večinoma omenja kot tehnika prvega principa, utrjevanje tarče, občasno kot nadzor izhodov.

IV. **Demilitarizirana cona:** v uporabi za izolacijo javnega spletnega strežnika organizacije od internega omrežja. V različnih raziskavah je omenjena kot tehnika prikrivanja tarče.

V. **Sistem za zaznavanje motenj:** običajno obravnavan kot tehnika formalnega nadzora, tudi kot postavljanje »managerjev« – v tem primeru naj bi se sodelavci nadzorovali en drugega med seboj.

VI. **Pregledovalnik za zaznavo virusov:** večinoma omenjen kot metoda tehnike za utrjevanje tarče ali formalen nadzor.

VII. **Programska oprema za odstranjevanje ranljivosti:** načeloma je tudi ta tehnika vrsta utrjevanja tarče, je pa tudi način za odvračanje imitacije – če je neka ranljivost računalnika ali računalniškega omrežja po napadu odpravljena, bo manjša verjetnost, da bo napadalec ciljal na isto tarčo.

VIII. **RFID oznake za zagotavljanje informacij o produktih:** razložimo jih lahko na štiri različne načine: kot širitev varovanja (ker sproži alarm), zmanjšanje anonimnosti (ker vzpostavlja sled do osebe, ki jo nosi), formalni nadzor (ker omogočajo lažje prepoznavanje tatov), najbolj primarno pa kot identifikacija lastnine.

IX. **ID klicatelja:** uporablja se kot tehnika za nadzor dostopa, zmanjševanje anonimnosti in nadzor posrednikov. Identifikacija klicateljev je dejansko v preteklosti zmanjšala nadlegovanje po telefonu, kar je indikator, da bi bilo potrebno podobne tehnike raziskati in aplicirati na internet.

X. **Revizijski logaritem za zbiranje podatkov:** je močno orodje za ugotavljanje zaporedja dogodkov, ki so pripeljali do določenega stanja. Sam revizijski logaritem ne preprečuje kiberkriminalnih dejanj, ampak dejstvo, da so vsa dejanja zabeležena, je lahko sredstvo odvračanja storilcev.

XI. **Visoka odgovornost ponudnikov internetnih storitev:** ponudniki internetnih storitev bi morali prakticirati višjo stopnjo odgovornosti, še posebej kar se tiče nalaganja vsebin iz spleta. Raziskave kažejo, da je le 5 % naloženih vsebin plačanih, kar predstavlja zelo resen problem za glasbeno industrijo. Ponudniki internetnih vsebin bi odgovornost lahko povečali na dva načina:

- **Prvi** način je, na primer, predstavitev novih poslovnih modelov, kot je znan Nokijin »Comes with Music« – kupec naprave dobi eno leto brezplačnega nalaganja glasbenih vsebin. S tem je v ceno naprave vključena pristojbina za glasbene vsebine, ki jih kupec obdrži tudi, ko se izteče doba enega leta. To je lahko obravnavano kot poskus ponudnika internetnih storitev za zmanjševanje koristi nelegalnega nalaganja vsebin.
- **Drugi** način pa je poudarjanje dejstva, da se velik delež širokopasovnih povezav uporablja za nelegalno nalaganje vsebin, kar zmanjšuje širino za legalno uporabo omrežja. Z blokiranjem Torrentov (kar bi storil visoko odgovoren ponudnik internetnih storitev) bi uporabili tehniko nadzora posrednikov.

XII. **Izobraževanje uporabnikov spleta: storilcev, tarč in varnostnikov**. Izobraževanje uporabnikov spleta je zaznano kot najbolj učinkovita metoda za področje odstranjevanja opravičil in izgovorov za izvedbo kaznivega dejanja. Različne študije vključujejo tako zaposlene, ki naj bi upoštevali interne pravilnike informacijske varnosti, kot stranke spletnih bank, ki bi z upoštevanjem navodil v precejšnji meri zmanjšale zlorabo spletnih računov in podobno.

Pri najbolj preprostih ukrepih bi morali biti najbolj natančni, a smo še vedno najbolj brezbrižni. V letu 2015 je bilo še vedno najbolj pogosto geslo na spletu »123456« (ostalo nespremenjeno iz leta 2014), na drugem mestu je geslo »password« (ki je angleška beseda za geslo; nespremenjeno iz leta 2014), med prvimi 15 najbolj pogostimi gesli pa je še šest kombinacij številk – ali zaporedje ali same enice.

Poleg številk, ki jih za geslo določimo s sprehodom prstov po vrhu tipkovnice, se pogosto pojavljajo športi, na primer »baseball« in »football«, ki sta še vedno med prvimi 25, in liki iz serij ali filmov: »dragon«, »princess« (oba iz trenutno priljubljene serije Igra prestolov) ter »starwars«. Med najbolj osnovnimi vsebinami, ki jih strokovnjaki odsvetujejo pri sestavljanju gesel, so: uporabniško ime, osebno ime, ime podjetja, geslo pa mora biti dolgo vsaj 8 znakov (Davis, 2016).

Velik del tehnik, ki izhajajo iz tradicionalnega kriminala, je torej uporabnih tudi za kiberkriminal. Potrebno je le ugotoviti, katera je za določene kontekste in specifične primere najbolj primerna in kako jo uporabiti, da bo v kar se da veliki meri preprečevala (neposredno in posredno) ekonomsko škodo kiberkriminala. Kajti če podjetje velike vsote denarja vlaga v zaščito, različne varnostno-obveščevalne sisteme, gre sicer veliko sredstev, a v primeru uspešnih napadov, bi poleg sredstev porabili tudi veliko časa, pri tem pa izgubili produktivnost tekočega poslovanja, potencialno pa izgubili tudi stranke.

Ko gre za preprečevanje kiberkriminalnih dejanj v organizacijah, podjetjih ali celo državnih institucijah, pa ni dovolj le uporaba ustrezne tehnike. Potreben je integriran sistem, ki vključuje različne možne oblike napadov; sistem, ki je vezan na panogo oziroma sektor delovanja, na eni strani stabilen, a vseeno dovolj fleksibilen, da ga je možno posodabljati vsakič, ko pride do nove grožnje; predvsem pa mora biti sistem implementiran tako, da ga razumejo in podpirajo vsi zaposleni, ne le tisti v oddelku za informacijsko tehnologijo, kar mora biti podprto z ustreznim izobraževalnim sistemom.

V naslednjem poglavju si bomo ogledali, koliko je kiberkriminal raziskan v Sloveniji, kakšne tehnike so v uporabi in kakšna je ekonomska škoda kiberkriminala pri nas.

4 SPLETNA KRIMINALITETA V SLOVENIJI

4.1 Uvod v spletno kriminaliteto v Sloveniji

S prvimi poglavji magistrskega dela smo opredelili širši teoretični okvir ter razširjenost in ekonomsko škodo, ki jo kiberkriminal povzroča v zadnjih letih. Z empiričnim delom želimo prikazati, kakšno je stanje v Sloveniji. Odgovarjali bomo na naslednja raziskovalna vprašanja:

- Kakšen je trenuten obseg kiberkriminala v Sloveniji?
- V kakšnih oblikah se najpogosteje pojavlja znotraj gospodarskih družb?
- Na kakšen način se gospodarske družbe soočajo z njim?
- S katerimi metodami bi škodo lahko zmanjšali?

Na prva tri vprašanja bomo odgovarjali s pomočjo intervjujev, na četrto, zadnje vprašanje, pa tudi s pomočjo literature (na podlagi ugotovljenih najpogostejših težavah). Še prej pa si bomo pogledali, kakšne raziskave so bile na to temo v Sloveniji že opravljene in kaj so bile ključne ugotovitve.

V okviru diplomskih del je kiberkriminal omenjen, ni pa še bil obravnavan z vidika ekonomske škode. Perič (2014) se je, na primer, osredotočal na krajo in zlorabo identitete v informacijski družbi. V svojem delu omeni, da je večina kršiteljev s področja spletnega kriminala težko odkrita in kaznovana s strani organov pregona, izpostavi tudi problematiko anonimnosti in brez prostorskosti kibernetskega prostora.

Problematiko opredelitve prostora v virtualnem svetu smo omenili v podpoglavju 3.1, in sicer v kontekstu teorije rutinskih aktivnosti ter kasneje v podpoglavju 3.2 v kontekstu teorije kriminalnih vzorcev, v kateri pomembno vlogo igrajo t. i. »vroče točke«, ki pri aplikaciji teorije v kibernetski prostor predstavljajo veliko težavo. Perič (2014) tudi meni, da je varnost stvar tehnoloških rešitev in zakonitosti trga.

Z isto problematiko se je v diplomskem delu ukvarjal tudi Furlan (2015). Izvedel je anketiranje med 120 uporabniki spleta (anketiranci so bili prebivalci notranjsko-kraške regije). Glavni rezultati so bili, da se anketiranci zavedajo nevarnosti spletnega kriminala in temu primerno tudi uporabljajo antivirusne programe. Nekateri izmed anketirancev so že bili tudi žrtev kraje identitete na spletu.

Tudi znanstvena literatura je že merila elemente kiberkriminala v Sloveniji, vendar v smislu odnosa posameznika do kibernetske kriminalitete. Študija avtorjev Dimc in Dobovšek (2013) je primerjala ozaveščenost posameznikov in njihovo ravnanje v virtualnem okolju med slovenskimi in ameriškimi anketiranci. Rezultati so pokazali, da se Slovenci sicer v

smislu kiberkriminala počutijo bolj varne kot prebivalci ZDA, a dvomijo v sposobnosti organov pregona oziroma menijo, da niso sposobni obravnavati primerov kiberkriminala.

Prav tako je bilo ugotovljeno, da se posamezniki, ki so bili anketirani, zavedajo nevarnosti, a se v virtualnem okolju vseeno obnašajo neskladno s tem. Avtorja predlagata ozaveščanje splošne javnosti in spodbujanje bolj previdnega ravnanja na spletu ter krepitev zaupanja v organe pregona. Vzorec je bil relativno majhen (sestavljen po metodi snežne kepe), zato bi bilo potrebno dodatno raziskovanje v tej smeri.

S podobnim vprašanjem se je v svoji magistrski nalogi ukvarjala avtorica Pinterič (2015). Kiberkriminal označi kot grožnjo uporabnikom spleta in organizacijam, še posebej vladnim – katerih informacije lahko storilci kradejo in razširjajo, s tem pa manipulirajo z velikim številom ljudi. Avtorica meni, da gre za sodobno obliko kriminala, ki ni dodatna oblika kriminala temveč nadomešča tradicionalno obliko. Varnost in zasebnost uporabnikov spleta označi kot največji izziv sodobne družbe.

Še en primer raziskovanja kiberkriminala v Sloveniji je profiliranje storilcev kibernetske kriminalitete, in sicer hekerjev. Tudi Blažič (2014) v tem kontekstu omenja problematiko opredeljevanja prostora kiberkriminalnih dejanj. Kot pomoč pri prepoznavanju kaznivih dejanj pa poda profiliranje hekerjev, ki pomaga odkrivati storilce s pomočjo prepoznanih značilnosti, predvsem pa zmanjša krog možnih osumljencev in s tem izboljšuje delovanje organov pregona.

Avtor meni, da vsak storilec, ni pomembno ali v fizičnem ali virtualnem prostoru, naredi napako, profiliranje pa bi podalo preiskovalcem vpogled v psihološke lastnosti posameznih storilcev, s čimer bi napake laže zaznali in tudi znali razložiti ter s tem odkriti kiberkriminalno dejanje ter storilca. Tudi ta prispevek se ne ukvarja z ekonomsko škodo, ki nastane kot posledica kiberkriminala, niti ne razlaga pojava spletne kriminalitete v gospodarstvu, podjetjih ali organizacijah.

Sinanović (2015) pa se v magistrskem delu ukvarja s problematiko intelektualne lastnine. Loti se je bolj z vidika zakonodaje, ki bi ščitila ustvarjalce, ki so izpostavljeni piratskemu nalaganju vsebin s spleta. Kot problematično točko izpostavi konstanten tehnološki napredek, ki zahteva nenehno prilagajanje. V informacijski tehnologiji igrajo veliko vlogo pravo, avtorsko pravo in intelektualna lastnina. Avtorica dodaja, da je s pravnega vidika težko, v nekaterih primerih tudi nemogoče, slediti ustvarjalnosti in inovativnosti ter potrebi po zaščiti, ki jo zastavlja piratsko nalaganje vsebin s svetovnega spleta.

Le eden izmed zgoraj opisanih virov se nanaša na problem kiberkriminala na nivoju organizacij, podjetij in institucij, niti eden pa se ne nanaša na ekonomsko škodo, ki jo kiberkriminal povzroča. V Sloveniji je še vedno najbolj pogosto slišati o spletnem nadlegovanju in ribarjenju, večina primerov gre za poskus pridobitve podatkov o posamezniku, na primer številko bančne kartice. To pomeni, da je prisotna potreba po sistematičnem merjenju ekonomske škode, ki jo povzroča kiberkriminal.

4.2 Metodologija

Glavna raziskovalna metoda empiričnega dela je bil strukturiran intervju. Intervjuvali smo direktorje ali zaposlene na vodilnih položajih v različnih vrstah gospodarskih družb ter iz različnih gospodarskih panog. S tem smo skušali zajeti izsledke iz prejšnjega poglavja, ki so vezani na velikost in panogo.

Ker so ekonomske posledice kiberkriminala v Sloveniji še slabo raziskane, predvsem pa jih je težko oceniti in veliko organizacij tega sploh ne počne, smo se osredotočili na kvalitativno, ne kvantitativno raziskovanje. Z intervjujem smo skušali dobiti čim boljši vpogled v to, kako organizacije v Sloveniji razumejo kiberkriminal, kako ga zaznavajo, se z njim soočajo ter predvsem: ali in kako ocenjujejo finančno škodo, ki jo povzroča. Zanimalo nas je še, ali so trendi kiberkriminala v Sloveniji skladni z globalnimi. Zajeli smo tudi problematiko kraje intelektualne lastnine, ki jo je izredno težko meriti.

Intervjuji so bili izvedeni osebno, prek telefona in elektronske pošte. Pri vseh vprašanjih so bile sproti zagotovljene vse razlage, ki so respondentom omogočale, da odgovorijo kar se da dobro. Pred začetkom vsakega intervjuja smo vsem intervjuvancem predstavili definicijo in širše opredelitve samega pojma kiberkriminal. S tem so odgovori bolj skladni s teorijo in rezultati raziskav iz podpoglavij 4.2 in 4.3, prav tako pa so s tem možne primerjave (iz kvalitativnega vidika).

Vzorec je bil zastavljen tako, da so bili pokriti naslednji tipi gospodarskih družb: delniška družba, družba z omejeno odgovornostjo, samostojni podjetnik, socialno podjetje, organizacija; po panogah bodo vključeni prehrambna industrija, finančne storitve, grafično oblikovanje, programske rešitve, mobilne aplikacije ter izobraževanje. Vsi intervjuvani so ostali anonimni, saj bi v primeru razkritih ranljivosti postali potencialne tarče. Namesto »sedežev«, smo za klasifikacijo glede na velikost uporabljali število zaposlenih – v vzorcu bodo tako primeri z enim zaposlenim (s.p.), kot tudi podjetje s 1500 zaposlenimi.

4.3 Zasnova vprašalnika za intervjuje

V prvih vprašanjih smo odkrivali splošen odnos organizacije do kiberkriminala in njihovo poznavanje te problematike – kdaj so tovrstno problematiko prvič zaznali. Drugi sklop vprašanj je bil namenjen preverjanju, ali so trendi v Sloveniji podobni globalnim. V tretjem, zadnjem sklopu, pa smo skušali čim več izvedeti o posameznem kibernetskem napadu, katerega tarča so bili. Zanimalo nas je predvsem, kako so se z njim soočili, kakšne so bile kratkoročne in dolgoročne posledice ter posredni in neposredni stroški, ki so s tem nastali.

Čisto za konec smo intervjuvane vprašali še, ali in kako ocenjujejo ekonomsko škodo, ki jim jo kiberkriminal povzroča na letni ravni.

4.4 Vzorec

Spodnja tabela (Tabela 4) prikazuje značilnosti posameznih intervjuvancev. Skušali smo zajeti čim bolj različne predstavnike, ki bi podali čim večjo raznolikost odgovorov. Intervjuvanca B in C sta iz iste gospodarske družbe – prvi je direktor programa HoReCa, drugi pa je z oddelka za informacijsko tehnologijo.

Tabela 4: Sestava vzorca intervjuvancev

Intervjuvanec	**Vrsta gospodarske družbe**	**Število zaposlenih**	**Dejavnost**
A	d.o.o.	1500	računalniško programiranje
B	d.d.	450	prehrambna industrija
C	d.d.	450	prehrambna industrija; IT oddelek
D	d.o.o.	70	dejavnost finančnega zakupa
E	organizacija	7	dejavnost drugje nerazvrščenih članskih organizacij
F	socialno podjetje	5	drugo podjetniško in poslovno svetovanje
G	s.p.	1	fotografska dejavnost (oblikovanje, arhitektura)

4.5 Analiza rezultatov in interpretacije

Prvo vprašanje se je glasilo: »*Kdaj ste tovrstno problematiko začeli zaznavati v vašem podjetju oz. organizaciji in v kakšni obliki?*«

Odgovori so bili zelo različni – od »*10 let nazaj*« (intervjuvanec G) in »*od samega začetka podjetja*« (intervjuvanec A), pa do »*Kolikor mi je znano, v našem podjetju tega ni, razen računalniškega virusa pred mesecem dni.*« (intervjuvanec B). Prva dva odgovora sta vsekakor posledica panoge (fotografska dejavnost in računalniško programiranje), pri intervjuvancu B pa je odgovor zanimiv predvsem s tega vidika, da je intervjuvanec C, ki je iz iste delniške družbe, le drugega programa, odgovoril povsem drugače: »*Tovrstna problematika se pojavlja na dnevni ravni, najpogosteje v obliki spletnega nadlegovanja*«. Že pri prvem vprašanju smo torej naleteli na težavo, da so zaposleni (tudi na vodilnih položajih) o kiberkriminalu slabo obveščeni.

Intervjuvanec D, ki je s področja finančnih storitev (vodja oddelka), je problematiko začel zaznavati približno eno leto nazaj, ko je začel od IT službe prejemati opozorila o škodljivi elektronski pošti. Intervjuvanec E je težave zaznal pred leti, ko se je zaradi povečanega obiska začela sesuvati spletna stran, intervjuvanec F pa pred dvema mesecema, ko jim je nekdo načrtno – z namenom očrnitve – vdrl na spletno stran.

Pri **drugem vprašanju** smo intervjuvancem našteli nekaj glavnih izsledkov globalne raziskave, ki jo izvaja Ponemon Institute (2015). Trditve je najbolj izčrpno komentiral intervjuvanec A, saj je kiberkriminal zelo tesno vezan na njihov posel. Odgovori so bili naslednji:

Trditev št. **1**: »*Pojavi spletne kriminalitete so vedno bolj pogosti in povzročajo vedno večje stroške.*«

Komentar intervjuvanca A: »*Vsekakor so pojavi spletnega kriminala bolj pogosti kot npr. 10 let nazaj, je pa tudi res, da se o tem zadnja leta v medijih piše veliko več. Za nas to v resnici pomeni več projektov in več dela, saj stranke zahtevajo vedno boljšo varnost v naših produktih.*«

Trditev št. **2**: »*Največ stroškov v zvezi s spletno kriminaliteto povzročajo: zlonamerni »insajderji« (zaposleni, partnerji ...), odpoved storitev in spletni napadi.*«

Komentar intervjuvanca A: »*Intelektualna lastnina ima v podjetju, kot smo mi, največjo vrednost, in zaposleni so večkrat v veliki nevarnosti, da vede ali nevede prenesejo določeno informacijo na napačno mesto. Večina spletnih napadov se začne ravno tako, zato se naše podjetje veliko ukvarja z ozaveščanjem zaposlenih, o čem se sme govoriti in kaj je poslovna skrivnost. Po drugi strani pa je odpoved različnih storitev precej pogost pojav, kar lahko*

povzroči ogromne stroške zaradi izgube dela, ampak s primerno varnostjo predstavlja veliko manjše tveganje.«

Trditev št. **3**: »*Spletni kriminalni napadi povzročajo višje stroške, če niso rešeni in upravljani takoj.*«

Komentar intervjuvanca A: »*Stroški vsakega napada so sestavljeni iz reševanja varnostnega sistema, reševanja ukradenih podatkov in izgubo dela na razvoju. Dalj časa, ko je delo moteno z reševanjem napada, več posla izgubimo.*«

Trditev št. **4**: »*Največji eksterni strošek spletnega kriminala je motenje poslovanja, drugi največji pa izgubljene informacije*.«

Komentar intervjuvanca A: »*Informacije so lahko bolj ali manj občutljive, zato so njihove vrednosti zelo različne. Velikokrat pa izguba informacij direktno vpliva tudi na izgubo posla.*«

Trditev št. **5**: »*Največji interni strošek spletnega kriminala predstavlja detekcija napada in reševanje nastalih problemov.*«

Komentar intervjuvanca A: »*Pri vsakem napadu je potrebno upoštevati še to, da se takrat razvoj ustavi. To lahko predstavlja še veliko večji strošek kot samo reševanje.*«

Trditev št. **6**: »*Veliko razliko (pozitiven učinek – manj pogosti pojavi in nižji stroški) predstavlja vzpostavljanje varnostnega sistema.*«

Komentar intervjuvanca A: »*Dober varnostni sistem je osnova vsakega našega produkta, zahteva po tem pa se iz leta v leto veča.*«

Medtem ko pri podjetju intervjuvanca A napadi in vedno večja pogostost problematike pomenijo tudi posel, pri ostalih intervjuvancih pomeni zgolj škodo. Intervjuvanci so večinoma pri vseh trditvah komentirali, da držijo oziroma so skladne z opažanji dogajanja v njihovem podjetju. Intervjuvanec B je pri prvi trditvi zapisal: »*Drži, poleg tega pa to predstavlja tudi uhajanje podatkov nepooblaščenim osebam*«. Ob isti trditvi je bil zanimiv tudi komentar intervjuvanca C: »*Spretna kriminaliteta je vedno bolj pogosta in tudi vedno bolj iznajdljiva, zaradi tega so potrebne vpeljave novih varnostni sistemov, kar povzroča tudi višje stroške podjetju.*«

Pri trditvi številka 4. (»*Največji eksterni strošek spletnega kriminala je motenje poslovanja, drugi največji pa izgubljene informacije*.«) je bilo večinsko mnenje nekoliko drugačno – motenje poslovanja se večini ne zdi največji strošek, kar trije (C, D in G) pa so izpostavili, da največjo težavo predstavljajo izgubljene informacije. Intervjuvanec F, katerega zaenkrat

edina tovrstna izkušnja je napad na spletno stran, pa je povedal, da pri njih ni šlo niti za strošek motenja poslovanja niti izgube informacij, najbolj je trpel ugled.

Glede trditve št. 5 (»*Največji interni strošek spletnega kriminala predstavlja detekcija napada in reševanje nastalih problemov.*«) je bilo tudi nekaj zanimivih odstopanj. Intervjuvanec D je povedal, da »*Reševanje problemov oziroma podatkov verjetno terja največ stroškov, saj je potrebno stanje, ki ga podjetje ima, vzpostaviti na pravilno oziroma prvotno raven.*« Podobnega mnenja je bil tudi intervjuvanec F, ki problema detekcije ni zaznal kot strošek – takoj jim je bilo jasno, da je bila njihova spletna stran napadena; intervjuvanec G pa je povedal, da je v njegovem primeru to strošek, ki je že vštet v ceno strežnika.

Za trditev št. 6 (o pozitivnih učinkih vzpostavljanja varnostnega sistema) so bili vsi mnenja, da drži.

Pri **tretjem vprašanju** so morali intervjuvanci razvrstiti oblike kibernetskih napadov glede na to, koliko stroškov jim povzročajo – na 1. mesto tisto obliko, ki povzroča največ stroškov, na zadnje mesto pa tisto obliko, ki povzroča najmanj stroškov. Rezultati so prikazani v spodnji tabeli (Tabela 5). Kjer je črka X, to pomeni, da s to obliko kiberkriminala še nimajo izkušenj.

Tabela 5: Razvrstitev oblik kiberkriminala glede na povzročene stroške

Oblika napada:	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**nikoli:**
Zlonamerni "insajderji", tj. zaposleni, partnerji …	4	X	1	X	1	X	X	4
Odpoved storitve	1	X	1	X	7	X	6	3

Se nadaljuje

Tabela 5: Razvrstitev oblik kiberkriminala glede na povzročene stroške (nadaljevanje)

Oblika napada:	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**nikoli:**
Spletni napadi	3	X	5	X	3	1	7	2
Ribarjenje in socialni inženiring	7	X	5	X	6	X	1	3
Škodljive kode	5	X	8	X	4	X	2	3
Ukradene naprave	X	X	3	5	5	X	X	4
Škodljiva programska oprema	6	X	9	3	X	X	X	4
Virusi, črvi, trojanski konji	8	1	9	2	2	X	X	2
Botnet oz. okužba internega omrežja	9	X	1	X	X	X	X	5
Kraja intelektualne lastnine	2	2	X	X	X	2	2	3

O statistični analizi in konkretnih razvrstitvah ne moremo govoriti, ker je bil vzorec absolutno premajhen za takšna posploševanja, opazimo pa lahko naslednje:

- Največ stroškov (označilo 5 od 7 intervjuvanih) povzročajo spletni napadi ter virusi, črvi in trojanski konji.
- Nekje v sredini so (označili 4 od 7 intervjuvanih): odpoved storitve, ribarjenje in socialni inženiring, škodljive kode in kraja intelektualne lastnine.
- Najmanj stroškov (označila le 2 od 7 intervjuvanih) pa povzroča botnet oziroma okužba internega omrežja.

S **četrtim vprašanjem** smo jih povprašali o varnostnih ukrepih, ki jih prakticirajo. Našteli smo tri preproste oblike, na koncu pa pustili še odprto vprašanje za morebitne ukrepe, ki jih nismo omenili. Prvi varnostni ukrep je bil »*Menjava gesel (npr. enkrat na mesec, vsake pol leta ...)*«. odgovori so bili sledeči:

Intervjuvanec A: »*Vsak zaposleni v podjetju mora zamenjati geslo vsake tri mesece, novo geslo pa ne sme biti enako kot prejšnjih 10 gesel. Poleg tega mora vsako geslo vsebovati 15 znakov, vsaj eno veliko in malo črko, vsaj eno cifro in vsaj en poseben znak. Poleg tega ima vsak projekt dodatna gesla pri stranki, ki imajo svoj varnostni sistem poleg našega.*«

Intervjuvanec B: »*Menjamo vsake pol leta.*«

Intervjuvanec C: »*Menjava gesla je obvezna vsake tri mesece.*«

Intervjuvanec D: »*Vsa gesla v podjetju menjavamo vsake 3 mesece. Programi so nastavljeni na avtomatsko opozarjanje, ko je čas, da se gesla zamenjajo. Novo geslo mora biti vedno dovolj različno od starega, da ga sistem sprejme.*«

Intervjuvanec E: »*Menjamo na pol leta.*«

Intervjuvanec F: »*Ne.*«

Intervjuvanec G: »*Da. Na pol leta večinoma.*«

Po odgovorih na prvo podvprašanje lahko sklepamo, da so pri večjih podjetjih precej bolj pozorni na ravnanje z gesli, še posebej napreden sistem pa imajo v podjetjih, kjer je panoga računalništvo ali finančne storitve (kar je smiselno glede na naravo dela).

Drugo podvprašanje o varnostnih ukrepih se je nanašalo na »*Ločitev službene elektronske pošte in datotek od zasebnih telefonov in računalnikov.*«

Tudi tokrat sta najbolj izstopala odgovora intervjuvancev A in D:

Intervjuvanec A: »*Vsi naši zaposleni dobijo celotno službeno opremo, imamo pa par projektov, ki se ukvarjajo z BYOD (bring your own device), kar pomeni razvoj varnostnih dodatkov za zasebne naprave, da so dovolj varne tudi za bolj občutljive podatke. Taki projekti so v zadnjih letih zelo v vzponu, saj predstavljajo veliko večjo fleksibilnost zaposlenih.*«

Intervjuvanec D: »*Službeni računalniki nimajo zunanjega dostopa (omejen internet, ni USB priklopa, ni možnost branja CD ploščkov …). Vsi službeni telefoni pa so zaklenjeni in je na njih možno odpiranje samo vnaprej odobrenih aplikacij*.«

Delno je urejeno to področje tudi v podjetju intervjuvanca C:

»*Službenega računalnika ni dovoljeno uporabljati v privat namene.*«

Ponovno opazimo, da intervjuvanec B, ki je zaposlen v isti gospodarski družbi, tega ni zapisal. Ločitev službene elektronske pošte in datotek od zasebnih telefonov in računalnikov je potrdil tudi intervjuvanec E; ukrepa pa eksplicitno ne prakticirajo v podjetjih intervjuvancev F in G.

Zadnja trditev pri tem vprašanju se je nanašala na izobraževanje zaposlenih. Intervjuvanec F je odgovoril z »*ne*«, intervjuvanci B, E in G so odgovorili z »*da*«, nekoliko več pa so povedali naslednji:

Intervjuvanec A: »*Naši zaposleni so redno vključeni v izobraževanja dodatnih tehnologij, kar med drugim vsebuje tudi izobraževanja o varnosti.*«

Intervjuvanec C: »*Ob vsakem pojavu novega spletnega kriminala, ki bi potencialno lahko ogrozil naše podjetje, obvestimo zaposlene, kakšni so simptomi napada in kako se zavarovati pred tem napadom*.«

Intervjuvanec D: »*Vsako leto poteka seminar o varnosti pred tovrstnimi in ostalimi nevarnostmi, ki bi lahko škodovali podjetju.*«

Na podlagi odgovorov sklepamo, da je tudi pri izobraževanju pomemben faktor velikost podjetja – več kot je zaposlenih, več se temu posvečajo; ponovno pa je tu pomembna panoga – izstopanje intervjuvancev A in D, tokrat tudi C.

Zadnje podvprašanje na temo varnostnih ukrepov je bilo odprto. Intervjuvanec A je povedal, da: »*Med najbolj pomembne ukrepe vsekakor spada enkripcija podatkov, ki se kot kriptologija redno razvija skupaj s spletnim kriminalom.*«

V podjetju intervjuvancev B in C uporabljajo sledljivost elektronske pošte, intervjuvanec G je dodal: »*Hranjenje kopij podatkov na dveh ločenih lokacijah*«, pri ostalih pa ne prakticirajo nobenih dodatnih ukrepov.

S **petim vprašanjem** smo želeli dobiti kvalitativen vpogled v to, s kakšnim kiberkriminalom so se že soočili. Prosili smo jih za naslednje informacije: **vrsta napada**, **kdaj** se je to zgodilo, **koliko časa** so potrebovali za razrešitev (približno število dni), koliko neposrednih in posrednih **stroškov** je napad povzročil (lahko so si pomagali s spodnjimi alinejami), kako menijo, da je to **dolgoročno vplivalo** na njihovo podjetje oziroma organizacijo, ali so za tem napadom vzpostavili poseben **varnostni sistem** oz. ali so na podlagi izkušnje kaj spremenili svoje delovanje ter ali je bila **ista tarča** napadena že kdaj prej ali kasneje. Spodaj so njihove zgodbe.

Opredelitev stroškov za pomoč: Med **neposredne stroške** sodijo:

I. stroški zaznavanja,
II. stroški obnove in povrnitve v stanje pred napadom,
III. stroški preiskovanja napadov in
IV. stroški upravljanja z napadi.

Posredni stroški, ki nastanejo kot posledica napadov, pa so naslednji:

V. prekinitve in motnje poslovanja in
VI. izguba (zaupanja) strank.

Intervjuvanec A: »*Naše podjetje še ni bilo resno napadeno, imamo pa več strank, ki imajo slabe izkušnje z napadi. Najbolj pogost pojav je odpoved storitev, ki pravzaprav niti ni stvar kiberkriminala. Npr. pri nekaterih strankah smo blokirani od dela povprečno tudi do 6 ur na teden (odpoved strežnika ali VPN, slaba internetna povezava, motnje v komunikaciji), kar za našo stranko predstavlja direkten strošek 10.000 Evrov. V kolikor mi ne uspemo primerno utemeljiti izgube dela, mi utrpimo posredni strošek pri izgubi zaupanja in nadalje manj projektov pri isti stranki. V tem primeru lahko izguba doseže tudi milijonske stroške*.«

Intervjuvanec B na to vprašanje ni odgovoril, a je zgodbo iz tega podjetja zelo natančno opisal intervjuvanec C: »*Štiri mesece nazaj smo dobili izsiljevalski virus Locky, ki nam je okužil 10 računalnikov in skupni Share. Zakriptiranih je bilo več kot milijon datotek. Zadevo smo rešili v roku osmih ur z restavriranjem podatkov iz arhivov, tako da dejansko neke velike škode ni bilo. Rešitev je bila v spremembi filtriranja elektronskih sporočil že na poštnem strežniku, da take oblike napadov (priponka v mailu) ne ogrožajo več našega sistema, ker niti ne pridejo do uporabnika*.«

V podjetju intervjuvanca D prav napada še niso imeli, kot pravi: »*na srečo*«. V organizaciji intervjuvanca E je prišlo do zrušene spletne strani, rezultat česar je bilo nedelovanje, ki je trajalo približno tri dni. Dogajanje je ponavljajoče, s čimer potrjujemo v začetku naloge opisan koncept ponavljajoče se žrtve.

V podjetju intervjuvanca F je bil napad sledeč: *»… ko so nam sesuli spletno stran. To je bilo kakšna dva meseca nazaj. Takrat je nekdo napadel server krovne entitete, pod katero spadamo, in je stran izginila za en teden oziroma ni bila vidna ostalim uporabnikom. Dokler problem ni nastal, se ga nismo zavedali, ker smo mislili, da ma institucija zaščitene zadeve. Celoten strošek obnovitve in povrnitve v stanje pred napadom je znašal približno 500 €. Iz IT službe so potem potrdili, da so takrat po napadu bolj zaščitili spletno stran.*«

Kot izrazit napad pa so zaznali še enega: »*Bil je pa še en incident v zvezi z intelektualno lastnino, ki sicer ni povzročil materialnih stroškov. Nekdo, ki ima dostop do notranjih informacij, je dokument, ki je imel oznako interno gradivo, skeniral, potem pa po elektronski pošti v pdf formatu pošiljal okrog medijem in tudi delil natisnjenega. Tukaj so bili potem stroški PR-ja in pa ugleda*.«

Pri tem odgovoru je moč zaznati problematiko zlonamernih »insajderjev«, in sicer bi primer po tipologiji iz podpoglavja 4.3 uvrstili pod »zlonamerne zaposlene«, saj tukaj ni šlo za izkoriščanje zaposlenega s strani tretje osebe ali nekaj, kar je storilec povzročil nevede – šlo je za namerno povzročanje škode s ciljem očrnitve direktorja. V poročilih globalnih raziskav, ki jih opravlja Ponemon Institute (2015), so stroški zaradi zlonamernih »insajderjev« zelo visoki. V tem slovenskem primeru materialno niso bili ocenjeni, vidimo pa, da je težava prisotna tudi že pri nas.

Zadnji intervjuvanec, intervjuvanec G, pa ima naslednjo izkušnjo: »*Bil je napad na spletno stran. Šlo je za izkoriščanje varnostne luknje s pomočjo mysql injection v starejši programski opremi na strežniku. Reševali smo en dan, stroški so všteti v upravljanje s strežnikom. Razen zastoja pri dostavi elektronskih sporočil in nedelovanja spletne strani en dan ostalega ni bilo. Sistem so vzpostavili vzdrževalci strežnika s posodobitvami. Podoben napad se je zgodil že prej z istim vzrokom in isto rešitvijo.*«

Tudi ta izkušnja nakazuje na koncept ponavljajoče se žrtve. Ranljivosti strežnika očitno po prvem napadu očitno niso bile odpravljene.

Šesto, predzadnje vprašanje, je bilo na temo merjenja in ocenjevanja ekonomske škode, ki jo v podjetju oziroma organizaciji povzroča kiberkriminal. Odgovori so bili spet zelo raznoliki, in sicer:

Intervjuvanec A: »*Direktne ekonomske škode kriminala ne merimo. Zaposlenih izključno za varnost imamo 2 v vsaki veji podjetja (vse skupaj 10). Vsak projekt ima tudi svoje ukrepe za varnost. Vsega skupaj ima podjetje okoli 5 milijonov EUR stroška letno za preventivo kiberkriminala.*«

Intervjuvanec B na vprašanje ni odgovoril, je pa odgovoril drugi intervjuvanec iz tega podjetja, tj. C: »*Škode do sedaj nismo merili, znaša pa približno 10.000 EUR letno.*« Tudi v podjetju intervjuvanca D ekonomske škode ne merijo: »*Škode, ki bi jo morebitni kiberkriminal povzročil, ne merimo. Vse moči so usmerjene k preprečitvi tovrstnih dejanj.*«

Intervjuvanec E je zapisal: »*Ocenjujem na 5.000 EUR letno*«, intervjuvanec F je ocenil, da so bili do sedaj le stroški prej opisanega napada, tj. 500 EUR, pri intervjuvancu G pa gre za specifično porazdelitev stroškov, in sicer spadajo v ceno strežnika, zato je njegov dejanski strošek kiberkriminala, kot pravi sam, zanemarljiv.

Kakršnakoli statistična obdelava pridobljenih informacij o ekonomski škodi bi bila nesmiselna, lahko pa odgovore iz intervjujev povežemo s prej opisani teorijo in z rezultati globalne študije, ki jo vsako leto opravi Ponemon Institute (2014 in 2015).

V večini primerov so stroški vse prej kot zanemarljivi, sploh glede na majhnost podjetij, ki jih obravnavamo. Obe podjetji, ki sta zaradi narave panoge in velikosti najbolj izpostavljeni (računalništvo in finančne storitve), ogromno sredstev vlagata v preventivo – in očitno učinkovito, saj o hujših napadih ne poročajo. Pri podjetju, iz katerega izhajata intervjuvanca B in C, so tudi vidne povezave z globalnimi trendi: gre za večje podjetje, zato strošek na zaposlenega ni tako visok, kar pa je skladno tudi s tem, da gre za prehrambno industrijo, ki se po stroških glede na panogo uvršča med tiste z nižjimi stroški.

Številka pri intervjuvancu E je glede na število zaposlenih zaskrbljujoča (5.000 EUR in le sedem zaposlenih, kar znaša na letni ravni več kot 700 EUR na zaposlenega), vendar v tem primeru ne gre za podjetje, temveč organizacijo, ki jo sestavlja veliko posameznikov, ki niso zaposleni, temveč delajo prek študentske napotnice ali prostovoljno. Pri socialnem podjetju (intervjuvanec F) bi bilo potrebno tako izboljšati varnostne politike kot meriti dejansko škodo v materialni obliki, saj lahko dodatne PR storitve v resnici predstavljajo velike izgube zaradi zmanjšane siceršnje produktivnosti.

Čisto zadnje vprašanje pa je bilo opcijsko, in sicer smo intervjuvance vprašali, če imajo glede kiberkriminala v Sloveniji ali na splošno v svetu še kakšen komentar ali nasvet, morda izkušnjo, ki bi prispevala k preprečevanju tovrstnih težav v podjetjih in organizacijah. Odgovorila sta intervjuvanca A in G.

Intervjuvanec A: »*Z razvojem tehnologije se razvija tudi kriminal in obratno. Boljši kot so kiberkriminalci, večja je zahteva po varnosti. Za podjetja, ki ponujajo računalniške storitve, je to lahko možnost boljšega poslovanja, medtem ko je za računalniška podjetja z direktnim produktom to vedno večje tveganje. Več kot bodo vložili v preventivo, manj bo dejanskih napadov*.«

Intervjuvanec G: »*Večinoma je še vedno najhujši cybercrime tisti, ki je povezan s slabo izobraženostjo uporabnika in temelji izključno na njihovih napakah. Torej slaba gesla, ista gesla za vse storitve, omogočen terminalski dostop do računalnikov s slabim geslom, klikanje in odpiranje emailov, ki so očitno phishing narave, itd. Dobra protivirusna zaščita lahko reši težave s phishingom in vdori preko okuženih spletnih strani. Še vedno pa ne obvaruje vdorov preko slabih gesel. Za to je potrebno izobrazit uporabnika oziroma imeti sistem tako zaščiten, da zahteva od uporabnika redno menjavo gesel, ki jih ni mogoče enostavno uganiti ali dešifrirati*.«

Splošen vtis, ki ga dobimo ob prebiranju odgovorov, je, da se vodilni zaposleni v podjetjih in organizacijah nevarnosti kiberkriminala zavedajo, a v zvezi z nevarnostmi, ki jih predstavlja, ravnajo zelo različno.

Odgovori načeloma potrjujejo dognanja iz raziskav, ki jih opravlja Ponemon Institute. Največja razlika je v tem, da so intervjuvanci v zvezi s stroški kiberkriminala bolj obremenjeni z vidika izgubljenih informacij. Le pri intervjuvancih A in D je bilo moč zaznati, da imajo v podjetju integriran sistem, ki jih varuje, sicer pa je vsak pozoren na neko komponento, vsak pri obravnavi kiberkriminala zadeve upravlja nekoliko drugače.
Izredna raznolikost odgovorov pomaga razumeti vlogo kiberkriminala v podjetjih in organizacijah, doprinaša pa nekaj novih idej:

- Prva je ta, da bi bila bolj kot zgoraj podana razdelitev stroškov primerna sledeča: stroški preventive, stroški kurative in neoprijemljivi stroški, ki se jih ne da meriti neposredno.
- Znotraj stroškov kurative pa potem pride v poštev prej opisana delitev.
- Intervjuji, predvsem izkušnje z napadi, so poudarili predvsem to, da je na kiberkriminal treba gledati s širšega zornega kota in da je obseg te problematike veliko večji tako v izvoru kot v dolgoročnih posledicah, ki jih je v tem trenutku težko ali celo nemogoče izmeriti.

Vsekakor je veliko skupnih točk s prej obravnavano teorijo, rezultati študij instituta Ponemon ter našimi rezultati intervjuvanja, a ogromno je še potrebno raziskati, v prvi vrsti pa začeti izobraževati o nevarnostih in nuji merjenja škode, ki jo povzroča kiberkriminal – šele merjenje omogoča, da ocenimo, ali napadi napredujejo ali je naš varnostni sistem učinkovit. In šele ko bodo številke na papirju, se bodo ljudje zavedali dejanske ogroženosti.

7. PREDLOG MODELA ZA CELOSTNO OBRAVNAVO KIBERKRIMINALA V PODJETJIH IN ORGANIZACIJAH

Cilj magistrskega dela je bil določitev teoretskega modela, s pomočjo katerega bi lahko opredelili obseg kiberkriminala in ocenjevali ekonomsko škodo, ki jo povzroča v gospodarstvu ter ugotovili, kateri so faktorji, ki povečujejo izpostavljenost kiberkriminalu v gospodarstvu in družbi na splošno.

I. Prvi korak je **zavedanje**. To pomeni, da morajo posamezniki na vodilnih položajih v podjetjih in organizacijah vedeti, da je kiberkriminal vsakršno vedenje, pri katerem so računalniki ali računalniška omrežja orodje, tarče ali prostor kriminalnih dejanj. Zavedati se morajo, da v sodobnem času zaradi razširjenosti in sofisticiranosti povzroča večje posledice kot tradicionalni kriminal. Posamezniki na vodilnih položajih pa morajo svoje znanje o kiberkriminalu prenašati na svoje zaposlene v obliki izobraževanj.

   V intervjuju smo opazili, da sta zaposlena v isti delniški družbi precej drugače odgovarjala na ista vprašanja – iz tega sklepamo, da se marsikdo na vodilnem položaju podjetja ne zaveda nevarnosti kiberkriminala; ali misli, da mu njegovo podjetje ali organizacija ni izpostavljena, ali pa da to ni nekaj, kar bi lahko povzročalo velike stroške.

II. Drugi korak je **vzpostavitev varnostnega sistema**. Skladno s panogo oziroma sektorjem, v katerem podjetje ali organizacija posluje, je potrebno oblikovati varnostni sistem ter znotraj njega implicirati in vzdrževati izbrane tehnike zaščite in tehnike za zmanjševanje priložnosti kiberkriminala.

Pri implementaciji je ponovno pomembno izobraževanje zaposlenih, ki se morajo načel varnostnega sistema držati tudi, če so na hierarhični ravni nižje in imajo občutek, da sami na to nimajo vpliva. Izobraževanje je pomembno tudi zato, ker je veliko kiberkriminalnih dejanj v obliki zlonamernih »insajderjev«, ki (vede ali) nevede povzročajo škodo, na primer kot izdajanje internih informacij – ali z neprevidnim ravnanjem, ali pa ob prisili s strani tretje, neke zunanje osebe, ki informacije izkoristi za zasebne interese.

Ob vzpostavitvi varnostnega sistema je potrebno dodati tudi obveščevalno komponento, ki skrbi za ažurno prenašanje informacij v horizontalni in vertikalni smeri. Z vzpostavljanjem varnostnih politik, ki jih morajo poznati vsi zaposleni, pa je pomembno tudi določiti, čigava dolžnost je posamezna komponenta sistema in kdo je tisti, ki celoten sistem nadzoruje.

III. Tretji korak je **prepoznavanje** kiberkriminalnih dejanj. Na tej točki gre v prvi vrsti za zaposlene, ki so odgovorni za področje informacijske tehnologije, ki morajo vsakršno sumljivo poročanje zaposlenih takoj obravnavati kot urgentno in se truditi v čim krajšem času ugotoviti, ali gre za malenkost ali za resno grožnjo, ki bi lahko škodovala podjetju oziroma organizaciji. Če se problema ne prepozna takoj, namreč povzroča vedno več stroškov in tudi dolgoročnih posledic.

Ta točka je vezana tako na prvo kot na drugo točko, saj je prepoznavanje možno le, če se vsi zaposleni prej zavedajo, da so (njihovi računalniki ali omrežje) potencialne tarče, veliko pa temelji tudi na izobraževanju o varnostnem sistemu, ki zaposlene naredi pozorne na spremembe in sposobne prepoznavati značilnosti napadov oziroma odstopanj od varnostnih protokolov.

IV. Za prepoznavanjem pride na vrsto **reševanje**. Tudi na tej stopnji gre predvsem za delo strokovnjakov za informacijsko tehnologijo, ki morajo (ob podpori vseh zaposlenih) zadevo rešiti čim hitreje.

V. Naslednji korak je **posodobitev sistema za odpravo ranljivosti.** To pomeni, da po vsakršnem napadu v podjetju to obravnavajo kot lekcijo, iz katere se morajo naučiti, kaj narobe delajo oziroma kaj je tisto, zaradi česar so postali žrtev. Skladno s tem je treba pomanjkljivosti varnostnega sistema odpraviti – ga posodobiti, da za takšen napad ni več potencialna žrtev in ni več ranljiv. S tem se zmanjšuje možnost pojava koncepta ponavljajoče se žrtve.

VI. Zadnji korak pa je **merjenje stroškov.** To v prvi vrsti pomeni, da morajo odgovorni poznati vse vrste stroškov, ki nastajajo: najprej nastopijo stroški zaščite, nato neposredna izguba, zatem posredna izguba ter na koncu še neoprijemljivi stroški, ki

jih je najteže določiti. Čeprav so **stroški zaščite** bolj investicija kot stroški, jih je potrebno vključiti z namenom zagotavljanja nadzora nad količino sredstev, ki jo je potrebno imeti na voljo za upravljanje s kiberkriminalom (še posebej zaradi sprotnega posodabljanja varnostnega sistema zaradi preteklih napadov).

Pri **neposredni izgubi** se upošteva stroške, ki nastanejo takoj ob napadu in se kažejo v obliki kraje intelektualne lastnine, izgube informacij in podobno. Sem spadajo tudi stroški reševanja in povračanja v stanje pred napadom, stroški preiskovanja in stroški celostnega upravljanja z napadi, ki se pojavijo v podjetju oziroma organizaciji.

Posredno izgubo predstavljajo prekinitve in motenje poslovanja ter izguba (zaupanja) strank – pravzaprav vseh deležnikov, ki ali direktno ali pa indirektno vplivajo na entiteto. Pri posredni izgubi je potrebno vključiti vse delovne ure, ki jih zaposleni namenijo aktivnostim, povezanim z napadom, namesto da bi v tem času opravljali siceršnje delovne naloge. V merjenje posredne izgube spadajo tudi posledice, ki nastanejo kot zakasnitev izvedbe že dogovorjenih poslov. Gre torej za velike izgube produktivnosti, ki se kažejo tudi v monetarni obliki.

Zadnji vidik merjenja stroškov pa so **neoprijemljive posledice**, ki jih je težko ali celo nemogoče meriti. Do teh pride v primeru večjih napadov, ki povzročajo posledice tudi izven napadenega podjetja ali organizacije – v takšnih primerih lahko pride ne samo do izgube zaupanja obstoječih strank, ki se lahko odločijo za prekinitev poslovanja ali da za naslednji posel izberejo drugega partnerja, temveč tudi do velike škode zaradi negativne publicitete v javnosti, ki jo lahko sprožijo mediji, nezadovoljne stranke in partnerji ali celo konkurenca. Tukaj zato lahko nastajajo veliki stroški kriznega managementa in pa odnosov z javnostmi, ki se v času po napadu ukvarjajo z reševanjem nastale negativne publicitete, namesto da bi gradili pozitivno zgodbo med različnimi deležniki.

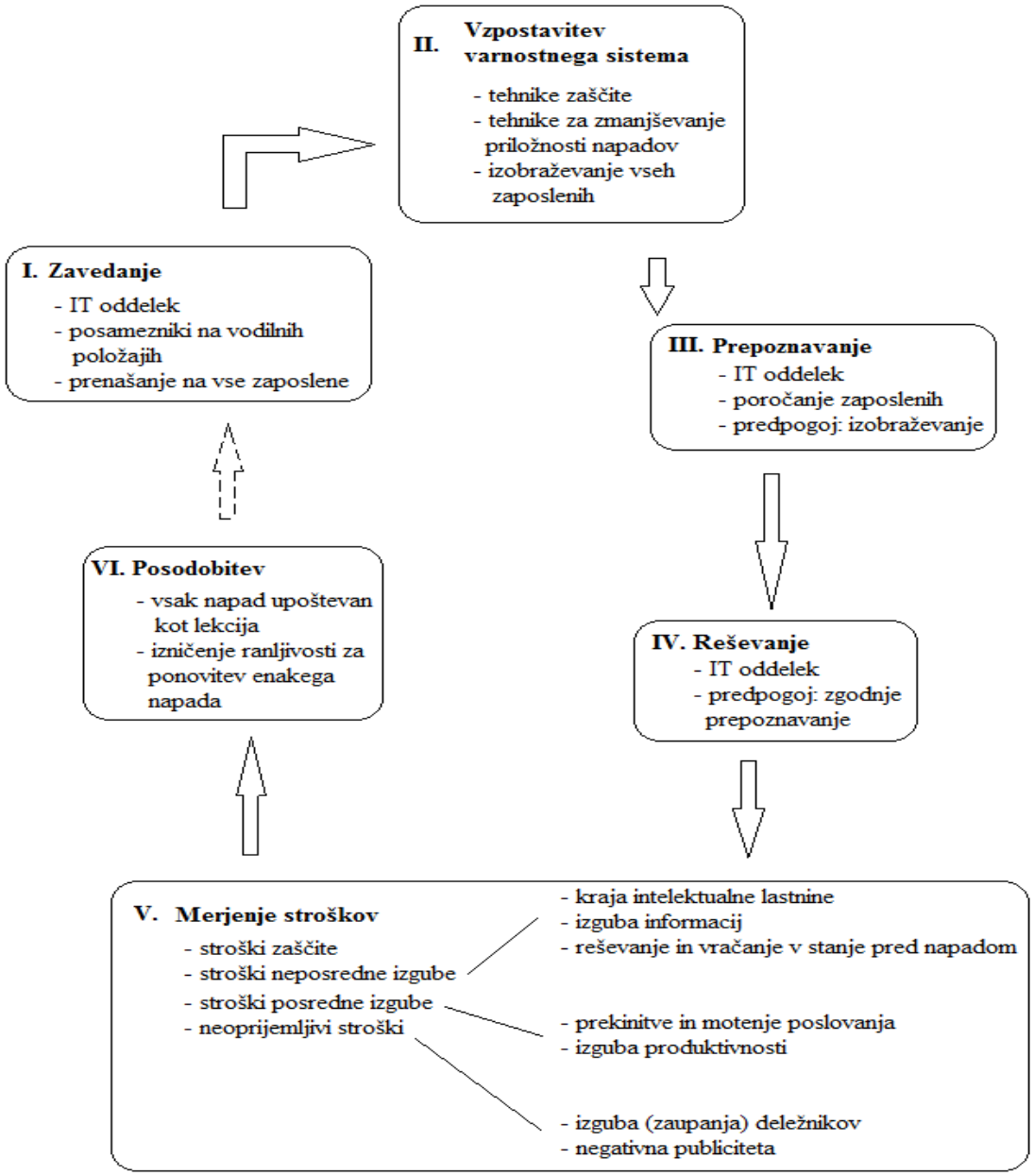
Pri kibernetskih napadih na večja podjetja ali organizacije deležniki niso le zaposleni, kupci in poslovni partnerji, temveč tudi lokalno okolje, institucije, »opinion makerji« … in če gre za napad na pomembno državno institucijo, so deležniki vsi državljani, ki lahko posledično izgubijo svoje zaupanje v državne institucije.

Ta predlog modela za obravnavo kiberkriminala v podjetjih in organizacijah zajema vse vidike, ki so se tekom našega raziskovanja izkazali kot pomembni – ali znotraj teorije, prebranih poročil organizacij, ki se s tem ukvarjajo, ali med intervjuvanjem subjektov, ki delujejo v slovenskem gospodarskem prostoru.

Ob vsakem takšnem modelu ni ključno, da se ga sestavi in predstavi, temveč da je pravilno implementiran in obravnavan skladno s kontekstom ter specifičnimi potrebami podjetja ali organizacije, ki ga uporablja. Primeren je za trenutne razmere, tako kot vsak varnostni sistem pa bo tudi ta model potreboval posodabljanje v koraku s časom in težavami, ki jih bo prinesla prihodnost.

Model je prikazan tudi grafično.

Slika 10: Predlog modela za celostno obravnavo kiberkriminala v podjetjih in organizacijah



SKLEP

Magistrsko delo se posveča problematiki kibernetskega kriminala, t. i. kiberkriminala. Le-ta v gospodarstvu in svetu na splošno že nekaj let povzroča milijonske izgube, zato predstavlja problematiko, ki jo je potrebno obravnavati celostno ter z upoštevanjem teorij in empiričnih raziskav. Za teoretično razumevanje si je smiselno izposoditi koncepte in predpostavke iz znanosti o tradicionalnem kriminalu ter informacijski varnosti.

Iz tradicionalnega kriminala je možno na kiberkriminal aplicirati naslednje teorije: teorijo rutinskih aktivnosti, teorijo kriminalnih vzorcev, teorijo racionalne izbire in pa koncept ponavljajoče se žrtve. Za teorijo rutinskih aktivnosti je značilno, da so za kriminalno dejanje potrebni trije elementi: storilec kaznivega dejanja, ustrezna tarča in odsotnost sposobnega varuha.

Vse tri elemente je možno prenesti v kontekst kiberkriminala in razložiti njegovo pojavnost. Možnih storilcev je praktično neomejeno, v najboljši poziciji za izvedbo kibernetskega kriminalnega dejanja pa so zlonamerni »insajderji« – ali zaposleni (oziroma partnerji), ki želijo škodovati, ali zaposleni, ki so neprevidni in škodo naredijo nevede, ali pa zaposleni, ki dejanje naredijo pod pritiskom tretje osebe, ki želi to izkoristiti. Odsotnost sposobnega varuha je v kibernetskem prostoru moč razumeti kot odsotnost varnostno-obveščevalnega sistema in kot množico tehnik za preprečevanje ali vsaj zmanjševanje priložnosti.

Pri teoriji kriminalnih vzorcev je za kontekst kiberkriminala uporabno to, da predpostavlja »vroče točke«, v okviru katerih se kriminalna dejanja izvedejo. V tradicionalnem kriminalu so to fizične točke, v kibernetskem pa virtualne, ki nas zaradi neskončnega obsega opozarjajo na nevarnost, da postanemo žrtev na več računalnikih hkrati, ter da je lahko v enem napadu okuženih tudi več internih omrežij po celem svetu.

Teorija racionalne izbire predpostavlja, da za vsakim napadom stoji kalkulacija, kakšni so stroški (in tveganja) izvedbe kriminalnega dejanja ter kakšne so možne koristi in pridobitve. Storilec naj bi se tako za kriminalno dejanje odločil, če predvidene koristi in pridobitve odtehtajo stroške in tveganja. Za kibernetski prostor je problematično to, da je težje vnaprej oceniti, kakšne bodo pridobitve; tako za tradicionalni kot za kibernetski kriminal pa je težava omejena racionalnost, ki je posledica človeškega faktorja (čustev) in pomanjkanja informacij (v kontekstu kiberkriminala je bolj pomembno slednje). Omejena racionalnost je tukaj aktualna tudi z ekonomskega vidika.

Še en pomemben koncept tradicionalnega kriminala je koncept ponavljajoče se žrtve. Strokovnjaki za informacijsko tehnologijo v podjetjih in organizacijah morajo vsak napad vzeti kot lekcijo, na podlagi katere lahko prepoznajo šibkosti njihovega varnostnega sistema oziroma ranljivosti, ki jih izpostavljajo napadalcem.

V kiberkriminalu je morda laže po vsakem napadu tarčo zaščititi, da se enak napad ne more ponoviti, veliko težavo pa predstavlja nenehen napredek tehnologije, zaradi katerega je izredno zahtevno žrtev zaščititi pred obliko napada, ki bo iz predhodne nastala z – lahko le malenkostno – posodobitvijo.

Prav tako uporabno pa je iz tradicionalnega kriminala upoštevati načine zmanjševanja priložnosti (ali vsaj privlačnosti) za izvedbo kibernetskih napadov. Izpeljani so iz naslednjih generičnih principov:

- povečanje potrebnega truda za izvedbo kriminalnega dejanja,
- povečanje tveganja,
- zmanjšanje koristi izvedenega kriminalnega dejanja,
- zmanjšanje provokativnosti, ki izvablja kriminalno vedenje, ter
- odstranitev »opravičil« za kriminalno vedenje.

Pri vsakem principu je izpeljanih pet tehnik preprečevanja, ki se jih da aplicirati tudi v kibernetski prostor, kot so na primer: algoritmi za kodiranje, požarni zid, video prenos, sistemi za zbiranje informacij o prevarah, začasne identifikacije, izklop vidnosti povezave, demilitarizirana območja za prikrivanje omrežij, večkratno preverjanje uporabnika, pravila za uporabo internih omrežij, implementacija revizijskih vpisov, zakonito prestrezanje podatkov, uvrščanje ukradenih naprav na »črne sezname«, standardi za digitalne podpise, preprečevanje namišljenih IP-naslovov, preprečevanje širjenja informacij o tehnikah vdorov in napadov, jasno vpisovanje za pooblaščen dostop, varnostne politike v podpis zaposlenim ter večstopenjsko preverjanje uporabnikov.

Poročila globalnih raziskav kažejo na milijonske izgube, še posebej v ZDA, Nemčiji, na Japonskem in v Združenem kraljestvu. Skupen strošek kiberkriminala se sicer povečuje, v zadnjih treh letih pa se je v večjih organizacijah znižal strošek *per capita*.

Dejavniki razvoja in širjenja so predvsem komercialna uporaba spleta (in mobilnih omrežij), napadalci pa pri izbiri tarč upoštevajo dva kriterija: prvi kriterij je vrednost, ki bi jo uspešen napad prinesel (pri tem je prisotna omejena racionalnost, ki izhaja iz koncepta teorije racionalne izbire), drugi kriterij pa je stopnja zaščite, ki jo prakticira potencialna tarča. V Sloveniji do sedaj še niso bile izvedene raziskave, ki bi podale oceno ekonomske škode na podoben način, kot je prikazano v poročilih iz bolj razvitih držav.

Empirični del magistrskega dela smo zasnovali z namenom kvalitativne raziskave. Najprej smo preverili, kaj je bilo do sedaj na temo kiberkriminala v Sloveniji že raziskano. Glavna ugotovitev je bila, da je to področje izredno podhranjeno, tako z vidika kvalitativnih kot kvantitativnih raziskav, pa tudi glede razvoja terminologije.

Nato smo s pomočjo prej opisane teorije izvedli strukturirane intervjuje z direktorji ali zaposlenimi na vodstvenih pozicijah. Odgovarjali smo na naslednja raziskovalna vprašanja:

- Kakšen je trenuten obseg kiberkriminala v Sloveniji?
- V kakšnih oblikah se najpogosteje pojavlja znotraj gospodarskih družb?
- Na kakšen način se gospodarske družbe soočajo z njim?
- S katerimi metodami bi škodo lahko zmanjšali?

Raziskovalna metoda je bil torej strukturiran intervju, ki je vključeval 7 predstavnikov iz različnih podjetij in organizacij v Sloveniji. Vzorec je vključeval različne oblike gospodarskih entitet (s.p., d.o.o., d.d., socialno podjetje in organizacijo), in različne gospodarske panoge: računalniško programiranje, prehrambno industrijo, dejavnost finančnih zakupov, podjetniško in poslovno svetovanje ter fotografsko dejavnost. Zajeli smo tudi entitete različnih velikosti, ki smo jo merili na podlagi števila zaposlenih. s tem smo omogočili, da so bili rezultati vsaj v določeni meri primerljivi s tistimi, ki smo jih opisali v teoretičnem delu (predvsem v 3. poglavju).

Glavni rezultati so naslednji: trenuten obseg kiberkriminala v Sloveniji je težko ocenljiv, saj skoraj nihče njegovega pojava in škode, ki jo povzroča, ne meri natančno. Ocenjena škoda se razlikuje od podjetja do podjetja – ponekod so stroški kiberkriminala všteti v postavitev strežnikov (torej entiteta nima neposrednih stroškov), ponekod pa znašajo na letni ravni do 10.000 EUR. V podjetju, ki se ukvarja z računalniškim programiranjem, so stroški kiberkriminala še najbolj opredeljeni – zaradi možnosti izgube (zaupanja) strank predvidevajo, da so skupni stroški tudi do milijonskih izgub.

Oblike kiberkriminala, ki se najpogosteje pojavljajo, so spletni napadi ter virusi, črvi in trojanski konji. Nekoliko manj, a še vedno precej pogosti, so odpoved storitve, ribarjenje in socialni inženiring, škodljive kode in pa kraja intelektualne lastnine, ki jo je težko nadzorovati in še težje oceniti z materialnega vidika. Gospodarske družbe, v katerih so zaposleni naši intervjuvanci, se s kiberkriminalom soočajo na različne načine: od tega, da niti ne menjajo gesel niti ne ločujejo zasebne elektronske pošte od službenih računalnikov in službenih informacij od zasebnih računalnikov in telefonov, do zelo naprednih varnostnih sistemov.

Intervjuvanci so podali izčrpne odgovore, kot na primer: menjanje gesel vsake tri mesece, pri čemer geslo ne sme biti enako zadnjim desetim geslom, vsebovati pa mora 15 znakov, vsaj eno veliko in malo črko, številko in vsaj en poseben znak. V enem izmed podjetij pa imajo sistem, v katerem službeni računalniki nimajo zunanjega dostopa (omejen internet, ni USB priklopa, ni možnosti branja CD-jev), službeni telefoni pa so zaklenjeni in omogočajo odpiranje zgolj in samo tistih aplikacij, ki so vnaprej odobrene.

Metode, s katerimi bi škodo lahko zmanjšali, so predvsem zgoraj naštete, kot predlog pa svetujemo integracijo celostnega sistema, ki bi vključeval tako zavedanje kot vzpostavitev varnostnega sistema, prepoznavanje kibernetskih napadov, reševanje napadov, posodabljanje varnostnega sistema ob vsakem novem napadu, na koncu pa seveda natančno merjenje ekonomske škode, ki jo kiberkriminal povzroča. Ker je ekonomsko škodo težko neposredno meriti, v prvi vrsti predlagamo delitev stroškov na stroške zaščite ter neposredne in posredne stroške.

Veliko težavo pri ocenjevanju ekonomske škode predstavljajo tudi komponente, ki so neoprijemljive – lahko je oceniti, koliko je potrebno plačati nekega informatika, da nazaj postavi spletno stran ali odšifrira datoteke, ki jih je nek virus zaklenil, teže pa je oceniti posledice, ki nastanejo kot izgubljene ali razkrite zaupne informacije, ukradena intelektualna lastnina, ki je bila prej konkurenčna prednost, negativna publiciteta v javnosti, izguba zvestih strank in poslovnih partnerjev, nadaljnjih poslov ter širjenje delovanja.

Splošno gledano je model uporaben ob upoštevanju naslednjih faktorjev: treba ga je implementirati celostno – tj. da ga razumejo vodilni managerji, kot tudi zaposleni v nižjih nivojih (saj morajo varnostne politike upoštevati vsi), integrirati se ga mora v vse oddelke, ne le informacijsko tehnološkega.

Druga pomembna stvar je izobraževanje – vsakič ko pride do napada in se posodobi sistem skladno s preprečevanjem pojava koncepta ponavljajoče se žrtve, je o tem potrebno obvestiti in izobraziti vse, ki se jih to tiče. Zadnja stvar pa je upoštevanje konteksta – model naj ne bo kot GPS, temveč bolj kot kompas, ki podaja smernice za delovanje. V podjetjih in organizacijah naj ne bo implementiran korak po koraku, temveč ciklično, z nenehnim prepletanjem in prilagajanjem. Ob uspešni implementaciji bi ne le preprečevali hujše napade, temveč tudi laže merili in opazovali nove oblike kiberkriminala, kar bi omogočilo bolj natančno oceno ekonomske škode, ki jo povzroča, ter razvoj zaščitnih varnostno-informacijskih sistemov.

Magistrsko delo je prispevek k razumevanju teoretičnega ozadja kiberkriminala, saj vključuje teoretične pristope in koncepte tradicionalnega kriminala. Iz sorodnih področij tudi izpelje generične principe in tehnike zmanjševanja priložnosti za izvedbo napadov. Iz poročil globalnih raziskav je izpeljana splošna ocena in sestava ekonomskih posledic kiberkriminala, na podlagi dognanj je bilo zastavljeno tudi empirično raziskovanje v slovenskih podjetjih oziroma organizacijah.

Zaradi slabe informiranosti o kiberkriminalu je v tem trenutku težko meriti ekonomsko škodo v tako podrobne detajle, kot na primer v ZDA in Nemčiji, s kvalitativno analizo pa smo dobili dober vpogled v pojavnost kiberkriminala v Sloveniji ter kako je pravzaprav pri nas sploh obravnavan – kako ga zaznavajo in skušajo preprečevati.

Magistrsko delo tako odgovarja na določena kvalitativna vprašanja, predlaga model za implementacijo v prakso, odpira pa nova vprašanja in postavlja izziv za nadaljnje – predvsem kvantitativno raziskovanje ekonomske škode kiberkriminala v Sloveniji.

LITERATURA

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T. & Savage, S. (2012). Measuring the cost of cybercrime. V *The economics of information security and privacy* (str. 265–300). Berlin: Springer Berlin Heidelberg.
2. Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective. *Advanced topics in end user computing*, *4*, 257.
3. Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*(4), 375–414.
4. Beebe, N. L., & Rao, V. S. (2005, december). Using situational crime prevention theory to explain the effectiveness of information systems security. V *Proceedings of the 2005 SoftWars Conference* (str. 1–18). Las Vegas, NV: The University of Texas in San Antonio.
5. Bernik, I. (2014). Cybercrime: The Cost of Investments into Protection. *Varstvoslovje, 16*(2), 105.
6. Bishop, P., Bloomfield, R., Gashi, I., & Stankovic, V. (2011, November). *Diversity for security: a study with off-the-shelf antivirus engines.* Software Reliability Engineering (ISSRE), 2011 IEEE 22nd International Symposium (str. 11–19). London: IEEE.
7. Bishop, P. G., Bloomfield, R. E., Gashi, I., & Stankovic, V. (2012). *Diverse protection systems for improving security: a study with AntiVirus engines.* London: City University London.
8. Blažič, M. (2014). *Profiliranje storilcev kibernetske kriminalitete: primer hekerji*. (diplomsko delo) Ljubljana: FVV.
9. Brenner, S. W., & Clarke, L. L. (2005). Distributed security: A new model of law enforcement. *John Marshall Journal of Computer & Information Law, Forthcoming*.
10. Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. Boston: UPNE.
11. Brookson, C., Farrell, G., Mailley, J., Whitehead, S., & Zumerle, D. (2007). ICT product proofing against crime. *ETSI White Paper*, 5, 1–33.
12. Bowers, K. J., & Johnson, S. D. (2005). Domestic burglary repeats and space-time clusters the dimensions of risk. *European Journal of Criminology*, *2*(1), 67–92.
13. Bowers, K. J., Johnson, S. D., & Pease, K. (2004). Prospective hot-spotting the future of crime mapping? *British Journal of Criminology*, *44*(5), 641–658.
14. Brantingham, P., & Brantingham, P. (1993). Environment routine and situation: Towards a pattern of crime. *Routine Activity and Rational Choice: Advances in Criminological Theory*, *5*.
15. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing. *An International Journal of Police Strategies & Management*, *29*(3), 408–433.

16. Brown, E. S., Esbensen, F. A., & Geis, G. (2013). Theories of crime. *Criminology (8th)*, 149–151
17. BS 7799-2 (1999). *Information Security Managmenet Part 2: Specification for Information Security Management Systems.* British Standards Institute, London.
18. Clarke, R. V. (2010). *Crime science.* Thousand Oaks, CA: SAGE Publications.
19. Clarke, R. V. G., & Webb, B. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods. *Police Research Series (Paper 112).* London: Home office for Policing and Reducing Crime Unit.
20. Clarke, R. V., & Weisburd, D. (1990). *On the distribution of deviance*. V D. M. Gottfredson & R. V. Clarke (ur.), *Policy and Theory in Criminal Justice: Contributions in Honour of Leslie T. Wilkins* (str.10–27). Avebury: Aldershot.
21. Clarke, R. V., & Newman, G. R. (2003). *Superhighway robbery: preventing e-commerce crime*. London: Routledge
22. Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, *11*(3), 270–295.
23. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588–608.
24. Coles-Kemp, L., & Theoharidou, M. (2010). *Insider threat and information security management. In Insider threats in cyber security*. New York: Springer US.
25. Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies, 16*, 41–96.
26. Cornish, D. B., & Clarke, R. V. (2008). *The rational choice perspective. Environmental criminology and crime analysis*. London: Routledge.
27. Cromwell, P. F., & Olson, J. N. (2004). *Breaking and entering: Burglars on burglary*. Wadsworth: Thomson.
28. CSIS (2014). Estimating the Global Cost of Cybercrime. *McAfee, Centre for Strategic & International Studies*. Santa Clara: McAfee
29. Daigle, L. E., Fisher, B. S., & Cullen, F. T. (2008). The Violent and Sexual Victimization of College Women Is Repeat Victimization a Problem? *Journal of Interpersonal Violence*, *23*(9), 1296–1313.
30. Davis, J. (2016). These Were The 25 Most Popular Passwords In 2015. *Iflscience*. Najdeno 10. maja 2016 na spletnem naslovu: http://www.iflscience.com/technology/25-most-popular-passwords-2015/all/
31. Detica (2011). *Detica and office of cyber crime security and information assurance: The cos tof cyber crime.* Najdeno 25. maja na spletnem naslovu: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
32. Dimc, M., & Dobovsek, B. (2013). Percepcija kibernetske kriminalitete pri nekaterih uporabnikih interneta v Sloveniji in ZDA. *Varstvoslovje, 15*(3), 338.
33. Epstein, J. M. (1999). Agent-based computational models and generative social science. *Complexity, 4*(5), 41–60.

34. EU Law Analysis. (2015). *The European Investigation Order. Cyber Crime.* Najdeno 18. januarja 2016 na spletnem naslovu: http://eulawanalysis.blogspot.si/2014/05/the-european-investigation-order-new.htmlCybercrime
35. Farrell, G., & Pease, K. (2001). *Repeat victimization* (Vol. 12). New York: Criminal Justice Press.
36. Felson, M., & Clarke, R. V. G. (1998). *Opportunity makes the thief: Practical theory for crime prevention* (Vol. 98). London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.
37. Felson, M., & Boba, R. L. (2010). *Crime and everyday life*. London: Sage.
38. Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007, oktober). An inquiry into the nature and causes of the wealth of internet miscreants. *ACM conference on Computer and communications security* (str. 375–388). Dunaj: ACM.
39. Furlan, N. (2015). *Kraja identitete na spletu* (diplomsko delo). Koper: Fakulteta za management.
40. Gigerenzer, G., & Goldstein, D. G. (1996). Reasoning the fast and frugal way: models of bounded rationality. *Psychological review*, *103*(4), 650.
41. Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410.
42. Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford: University Press.
43. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20.
44. Gupta, M., Chaturvedi, A. R., Mehta, S., & Valeri, L. (2000, December). The experimental analysis of information security management issues for online financial services. V *Proceedings of the twenty first international conference on Information systems* (str. 667–675). Atlanta: Association for Information Systems.
45. Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). *Cyber-crime science = crime science + information security.* Enschede: University of Twente.
46. Higgins, G. E. (2004). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior*, *26*(1), 1–24.
47. Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248.
48. Huang, W., & Wang, S. Y. K. (2009). Emerging cybercrime variants in the Socio-Technical space. *Handbook of Research on Socio-Technical Design and Social Networking Systems*, 195.
49. ISO/IEC 17799 (2000). *Information Technology Code of Practice for Information Services.* Geneva: International Organization for Standardization.
50. Kabay, M. E. (1996). *NCSA Guide to Enterprise Security*. New York: McGraw-Hill Companies.
51. Keskin, İ. (2007). Bilisim Sucları. *Adalet Dergisi, Adalet Bakanlıgı Yayın Isleri Baskanlıgı*. 29:6.

52. Kitteringham, G. (2008). Lost laptops= lost data: Measuring costs, managing threats. V *Crisp report, ASIS International Foundation*. Washington, DC: USDOJ.
53. Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE*, *4*(1), 33–39.
54. Laycock, G. (2005). Defining crime science. V *Crime science: new approaches to preventing and detecting crime*, (str. 3-24). Devon: Willan Publsihing
55. Lee, M. (2012). Cyber crimes: preparing to fight insider threats. *Computer Fraud & Security*, *2012*(6), 14–15.
56. Malleson, N., Heppenstall, A., & See, L. (2010). Crime reduction through simulation: An agent-based model of burglary. *Computers, environment and urban systems*, *34*(3), 236–250.
57. Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123–134.
58. Newman, G. R. (2009). Cybercrime. In *Handbook on Crime and Deviance* (str. 551–584). New York: Springer.
59. Newman, G., & Clarke, R. V. (2003). Superhighway robbery: Crime prevention and e-commerce. *Cullompton, Devon: Willan Publishing*.
60. Pawson, R., & Tilley, N. (1997). *Realistic evaluation*. New York: Sage.
61. Perič, G. (2014). *Kraja identitete v informacijski družbi* (diplomsko delo). Ljubljana: FDV.
62. Pinterič, V. (2015). *Ozaveščenost evropskih spletnih uporabnikov o kiberkriminalu* (magistrsko delo). Novo mesto: FIŠ
63. Ponemon Institute (2014). *2014 Global Report on the Costs of Cyber crime*. Benchmark study on global companies. Ponemon Institute.
64. Ponemon Institute (2015). *2015 Global Report on the Costs of Cyber crime*. Benchmark study on global companies. Ponemon Institute.
65. Prislan, K. (2014). Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation. *Varstvoslovje, 16*(2), 128.
66. Reid, R. C., & Floyd, S. A. (2001). Extending the risk analysis model to include market-insurance. *Computers & Security*, *20*(4), 331–339.
67. Robbins, S. P. (1994). *Management,* 4th edition. New Jersey: Prentice-Hall, Upper Saddle River.
68. Robinson, A. L. (2006). Reducing Repeat Victimization Among High-Risk Victims of Domestic Violence The Benefits of a Coordinated Community Response in Cardiff, Wales. *Violence against women*, *12*(8), 761–788.
69. Sampson, R. J., & Raudenbush, S. W. (1999). Systematic social observation of public spaces: A new look at disorder in urban Neighborhoods 1. *American journal of sociology*, *105*(3), 603–651.
70. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531.

71. Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security*, *20*(7), 620–634.
72. Sinanović, S. (2015). *Intelektualna lastnina in piratstvo v digitalni informacijski dobi* (magistrsko delo). Kranj: FDŠ.
73. Smith, M. J., & Tilley, N. (Eds.). (2013). *Crime science*. London: Routledge.
74. Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia-Social and Behavioral Sciences*, 182, 590–595.
75. Stewart, A. (2012). Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor. *Information Management & Computer Security, 20*(4), 312–326.
76. Tappan, P. W. (1947). Who is the Criminal? *American Sociological Review*, *12*(1), 96–102.
77. Templeton, V. H., & Kirkman, D. N. (2007). Fraud, vulnerability, and aging: Case studies. *Alzheimers Care Quaterly, 8*(3), 265–277.
78. Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484.
79. Thompson, L. (2014). *Defending against cybercrime* (doktorska disertacija). New York: Utica College
80. Tilley, N. A. L. (2007). *From crime prevention to crime science*. Devon: Willan Publishing.
81. Tremblay, R. E. (2000). The development of aggressive behaviour during childhood: What have we learned in the past century? *International Journal of Behavioral Development*, *24*(2), 129–141.
82. Tudor, J. K. (2001). *Information Security Architecture,* CRC Press, Boca Raton, FL.
83. Van der Aalst, W. M., & de Medeiros, A. K. A. (2005). Process mining and security: Detecting anomalous process executions and checking process conformance. *Electronic Notes in Theoretical Computer Science*, *121*, 3–21.
84. Von Solms, R., Van Der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. Information & Management, 26(3), 143–153.
85. Weber, R. (1999). *Information System Control and Audit.* New Jersey: Prentice-Hall, Englewood Cliffs.
86. Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133–137.
87. Wright, M. (1999). Third generation risk management practices. *Computer Fraud & Security*, *1999*(2), 9–12.
88. Zaharia, A. (2015). 10 Surprising Cyber Security Facts That May Affect Your Online Safety. *Heimdal Security.* Najdeno 1. junija 2016 na spletnem naslovu:

https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/
89. Zeviar-Geese, G. (1997). State of the Law on Cyber jursidiction and Cybercrime on the Internet, *The Gonz. J. Int'l L., 1,* 119.
90. Yar, M. (2005). The novelty of 'cybercrime'an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.
91. Youd, N. (2015). Cyber deterrence: is a deterrence model practical in cyberspace? *Space & defence*, *8*(1), 47–59.