UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

SARA NOVAK

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

OBVLADOVANJE KIBERNETSKEGA TVEGANJA V RAČUNOVODSKIH SERVISIH

Ljubljana, 16. september 2018 SARA NOVAK

IZJAVA O AVTORSTVU

Podpisana Sara Novak, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Obvladovanje kibernetskega tveganja v računovodskih servisih, pripravljenega v sodelovanju s svetovalko prof. dr. Sergejo Slapničar in sosvetovalcem prof. dr. Tomažem Turkom,

IZJAVLJAM

1. da sem predloženo delo pripravila 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 poskrbela, 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 pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;
7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasja 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, ne izključno, 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 16. 9. 2018 Podpis študentke

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC:

ang. - angleško
GDPR – Splošna uredba EU o varstvu podatkov (ang. General Data Protection Regulation)
IT – informacijska tehnologija
IFAC – Mednarodna zveza računovodij
FCC – Federal Communications Commission
SI-CERT – Nacionalni odzivni center za kibernetsko varnost (ang. Slovenian Computer Emergency Response Team)
DMA – Direct Marketing Associaton

UVOD

Vsak dan so poslane milijarde zlonamernih elektronskih sporočil, vendar je potreben le majhen delež vseh, da uspejo in financirajo to nelegalno panogo (Werner, 2017). Kibernetski napadi so postali tako pogosti, da se v medijih pojavijo le tisti, ki imajo uničujoč učinek in dosežejo veliko število žrtev (Miller, 2016). V začetku maja leta 2017 se je po svetu razširila izsiljevalska okužba WannaCry. V enem dnevu je bilo okuženih več kot 230.000 računalniških sistemov po celem svetu. V Sloveniji je okužba WannaCry ohromila podjetje Revoz, v katerem so za cel konec tedna zaustavili proizvodnjo. V Sloveniji je bilo poleg Revoza evidentiranih še sedem drugih primerov (Perko, 2017).

Kibernetsko tveganje pomeni kakršno koli tveganje finančnih izgub oz. motenj v poslovanju zaradi izgube ključnih informacij ali škode ugledu podjetja zaradi vdorov v sisteme informacijske tehnologije. Kibernetsko tveganje je tveganje posameznikov ali podjetij in je povezano s spletnimi aktivnostmi (Institute of Risk Management, brez datuma b). Podjetja so pod naraščajočim pritiskom, da pokažejo zmožnost upravljanja in obvladovanja kibernetskih groženj ter da imajo učinkovite procese in nadzor za odkrivanje, odzivanje, ublažitev in okrevanje po vdorih in drugih za varnost zaskrbljujočih dogodkih (The American Institute of CPAs).

Poleg tega lastniki podjetij denarja ne želijo investirati v tisto, kar jim ne bo prineslo dobička, to pa vključuje tudi zavarovanje za kibernetsko tveganje in ostale ukrepe. Če podjetja ne upravljajo s kibernetskim tveganjem in ga ne obvladujejo, se lahko zgodi, da so zaradi finančne situacije, v kateri se znajdejo po napadu, prisiljena prenehati poslovati. Veliko podjetij informacijske varnosti še vedno ne jemlje dovolj resno in so prepričani, da se kibernetski napadi njim ne morejo zgoditi; vodje informacijske varnosti imajo težko nalogo, da vodstvo prepričajo, da obstaja resna potreba po upravljanju tega tveganja in izvajanju potrebnih ukrepov (Ashford, 2017).

Računovodskim servisom so za opravljanje dela posredovani osebni in zaupni podatki strank. Na žalost pa so v digitalnem svetu ti podatki izpostavljeni nepooblaščenemu dostopu in razkritju, če niso določeni dokončni standardi in prakse za varnostni nadzor. Računovodje in računovodski servisi niso nujno primarna tarča kibernetskega napada, ampak navadno le dostopna točka do informacij o njihovih strankah, s katerimi računovodski servisi razpolagajo. Ker je zaupnost najpomembnejša skrb, morajo računovodje v celoti razumeti tveganja in posledice neustrezne zaščite zaupnih in osebnih podatkov (Thompson, 2016). Ker je odvisnost od spleta zaradi uporabe elektronske pošte za komunikacijo s strankami, uporabe spletne banke, shranjevanja podatkov tudi v računovodskih servisih vse večja, je tudi večja verjetnost, da bo do teh podatkov dostopal nekdo, ki za to ni pooblaščen. Kibernetski napadi so vsako leto številčnejši, zato podjetja vsako leto izgubljajo podatke, ki so ključni za njihovo poslovanje. Zato bi se morala vsa računovodska podjetja zavedati obstoja kibernetskega tveganja in posledic, ki sledijo, če z njim ne upravljajo.

Namen magistrskega dela je preučiti in predstaviti kibernetsko tveganje v slovenskih računovodskih servisih, predvsem vzroke in ukrepe, ki so posebej značilni za računovodsko panogo. Pri tem me najbolj zanima, ali se podjetja zavedajo kibernetskega tveganja in kakšni so njihovi ukrepi za upravljanje s kibernetskim tveganjem. Ker je eden od glavnih ukrepov izobraževanje zaposlenih glede kibernetska tveganja, želim izvedeti, ali se tega ukrepa poslužujejo in kako pogosto.

Magistrsko delo je namenjeno predvsem v pomoč računovodjem, zaposlenim v računovodskih servisih, da bi znali tveganje, s katerim se soočajo vsakodnevno, prepoznati, jim predstaviti, kakšne so lahko posledice kibernetskih vdorov v informacijske sisteme, in jih seznaniti z najpogostejšimi ukrepi za upravljanje in obvladovanje tega tveganja.

Cilja magistrskega dela sta naslednja.

Prvi cilj je ugotoviti, v kolikšni meri so slovenska podjetja, ki ponujajo računovodske storitve, ozaveščena o kibernetskem tveganju in kako visoko ocenjujejo kibernetsko tveganje v računovodski panogi.

Drugi cilj je ugotoviti, katere ukrepe za upravljanje kibernetskega tveganja računovodski servisi v Sloveniji največkrat uporabljajo. Predvsem me zanima, ali svoje zaposlene izobražujejo na področju kibernetske varnosti in kako pogosto.

Raziskovalno vprašanje 1: Kako računovodski servisi v Sloveniji ocenjujejo svojo izpostavljenost kibernetskemu tveganju?

Raziskovalno vprašanje 2: Ali računovodski servisi v Sloveniji izvajajo ukrepe za zagotovitev kibernetske varnosti sebe in svojih strank?

Raziskovalno vprašanje 3: Kolikšen delež računovodskih servisov v Sloveniji izobražuje svoje zaposlene o pomenu kibernetske varnosti in morebitnih posledicah, če ta ni zagotovljena?

Raziskovalno vprašanje 4: Kako pogosto računovodski servisi v Sloveniji izvajajo izobraževanja in usposabljanja za zaposlene?

Magistrsko delo je sestavljeno iz uvoda, v katerem so opredeljeni področje raziskovanja, raziskovalni problem, namen in cilji magistrskega dela ter raziskovalna vprašanja. Sledi teoretični del, v katerem je podrobneje predstavljeno kibernetsko tveganje, razlogi za nastanek kibernetskega tveganja, najpogostejši načini, viri in posledice kibernetskih napadov, opisani so najbolj odmevni kibernetski napadi na svetovni ravni ter področje upravljanja kibernetskega tveganja z najpogostejšimi ukrepi za zagotovitev kibernetske

varnosti. Teoretični del se zaključi z opisom vplivov kibernetskega tveganja na računovodsko panogo.

V teoretičnem delu sem uporabila deskriptivno metodo, kar pomeni pregled strokovne literature, člankov in stališč domačih in tujih avtorjev s področja kibernetska tveganja in kibernetske varnosti. Literaturo sem poiskala v podatkovnih zbirkah, kot so Ebsco, ProQuest, Sciencedirect, Jstor idr. Uporabila sem tudi metodo kompilacije, saj sem povzemala ugotovitve različnih avtorjev, ki so raziskovali kibernetsko tveganje na splošno in v računovodski panogi.

Teoretičnemu delu sledi empirični del s predstavitvijo rezultatov izvedene raziskave. Empirični del magistrskega dela temelji na raziskavi, ki je bila opravljena z metodo zbiranja primarnih podatkov, in sicer z izvedbo ankete s pomočjo anketnega vprašalnika in globinskega intervjuja z Matejem Gorenškom, vodjo internega IT oddelka v računovodski hiši Unija. Vprašalnik je bil sestavljen iz zaprtih in odprtih vprašanj ter poslan na elektronske naslove slovenskih računovodskih servisov. S pomočjo spletne baze BIZI sem poiskala podjetja s SKD 69.200 (računovodske, knjigovodske in revizijske dejavnosti, davčno svetovanje) in njihove elektronske naslove. S programom SPSS sem analizirala pridobljene podatke ter skušala odgovoriti na zastavljena raziskovalna vprašanja.

Magistrsko delo se zaključi s predstavljenimi omejitvami raziskave, sklepom, povzetkom ugotovitev in navedbo virov in literature. V prilogi magistrskega dela se nahaja anketni vprašalnik, na katerem temeljijo rezultati raziskave.

1 OPREDELITEV KIBERNETSKEGA TVEGANJA

Predstavljajte si situacijo. Sreda zjutraj. Pridete v službo in ob zagonu vašega računalnika zamrznejo vsi zasloni. Nihče v podjetju ne more dostopati do informacijskega sistema in podatkov. Podjetje ne more komunicirati s svojimi strankami prek elektronske pošte, spletne strani in opravljati svoje vsakodnevne dejavnosti. Postavljajo se številna vprašanja, mnogi mislijo, da gre le za napako v sistemu (Dattu, 2016). Na ekranu se naenkrat pojavi sporočilo, ki pravi, da so podatki zakodirani, zato zahteva plačilo odkupnine za povrnitev podatkov. Zavedate se, da vas je pravkar doletel kibernetski napad. Eden od zaposlenih se spomni, da je med pregledovanjem elektronske pošte odprl nenavadno priponko k elektronskemu sporočilu, katerega pošiljatelja ni poznal in sporočila ni pričakoval.

To je le eden od primerov, kaj lahko doleti podjetje, če je napadeno. Če se podjetje znajde v taki situaciji, se vodstvo in zaposleni lahko odzovejo na različne načine. Podjetje lahko umirjeno izvleče svoj načrt za primer kibernetskega napada in se reševanja problema loti na načrtovan način. V nasprotnem primeru lahko zavlada panika. Če ima podjetje izdelan načrt,

potem je verjetno, da izvaja tudi ostale preventivne ukrepe za doseganje kibernetske varnosti in zato ni kritično ogroženo ob kibernetskem napadu.

Varovanje podatkov in informacij je eno ključnih področij, s katerim se soočamo vsi v sodobni družbi, tako posamezniki kot tudi podjetja, ki poslujejo v današnjem času – v digitalni eri, v kateri so informacije največja prednost in hkrati tudi največja slabost. Če podjetje razpolaga s pomembnimi informacijami, ki so ključne za njegov obstoj na trgu, je zelo verjetno, da jih želi imeti tudi nekdo drug in jih želi ukrasti, zato je to informacijo treba zaščititi. Ker večino informacij podjetja shranjujejo na svoje računalnike, s katerimi se povezujejo na splet, pomeni, da so te informacije ogrožene, saj obstaja velika verjetnost, da lahko do njih dostopa tudi nekdo, ki za to ni pooblaščen.

Računalniki in komunikacijska omrežja v sodobnem življenju prevladujejo. Pojav računalnikov je imel daljnosežne učinke in čeprav nekateri ljudje niso imeli priložnosti spoznati digitalnega sveta, so se jih verjetno računalniki dotaknili na drugačen način, na primer s proizvodnjo hrane, izobraževanjem, zdravstvenim varstvom in širjenjem idej. Ob vseh prednostih računalniške dobe, pa se nismo veliko menili za škodo, ki nam jo lahko računalniki prinesejo, dokler škoda ne nastane (Gabrys, 2002). Dramatična širitev kibernetskega prostora se je na globalni ravni dogajala v zadnjih dveh desetletjih. Do njega vsaj do neke mere lahko dostopa skoraj vsaka lokacija na zemlji, kar je preseglo optimistična pričakovanja začetnikov uporabe svetovnega spleta (Choucri, Madnick & Ferwerda, 2014). Zagovorniki digitalne dobe in njenega najbolj znanega izuma, spleta, omenjajo dramatično komercialno rast, uspešna gospodarstva in širjenje demokracije kot le nekaj koristi z dolgega seznama. Koristi spleta so resnično velike, prav tako pa so lahko veliki tudi stroški. Eden od takšnih stroškov, s katerimi se soočamo zdaj in je nova oblika tradicionalnega kriminala, je kibernetski kriminal. Kibernetski kriminal je razširitev tradicionalnega kriminala, vendar se dogaja v kibernetskem prostoru – nefizičnem okolju, ki ga je ustvaril računalniški sistem. V tem okolju kibernetski kriminal sprejema nefizične vidike kibernetskega prostora in postane brez meja, brezčasen in relativno anonimen. Z globalno povezanostjo telefonskega sistema in največjega svetovnega računalniškega omrežja, spleta, kibernetski kriminalci dosežejo skoraj vsak kraj na svetu in skoraj vsak računalniški sistem, vse dokler imajo dostop do komunikacijske povezave. S širjenjem brezžičnega omrežja in satelitsko tehnologijo lokacija sčasoma postane popolnoma nepomembna, globalni doseg do računalniških omrežij pa ustvari brezmejni dostop do kibernetskega kriminala. Če dodamo še avtomatizacijo, časovno in lokacijsko neomejen dostop do računalniških sistemov, čas izgubi pomen, težko pa je tudi vedeti, kdo ali kaj deluje za oddaljenim računalniškim sistemom. Danes je ukradene podatke osebi zelo težko vrniti, posebno če je kibernetski kriminalec dovolj usposobljen, da zakrije svoje sledi. Poleg tega kibernetski kriminalci še naprej izkoriščajo mednarodni vidik kibernetskega prostora, se povezujejo v mrežo z drugimi kriminalci in ustvarjajo kibernetske kriminalne tolpe. Biti kriminalec v kibernetskem prostoru zahteva tehnično znanje in izkušnje ter prefinjenost. Kibernetski kriminal zato povzroča številne težave na mednarodni ravni (Gabrys, 2002).

Deljenje informacij in investicije v varnost so ključne v internetni eri (Hausken, 2007). Hiter razvoj informacijske tehnologije in komunikacijskih sredstev, ki je v današnji družbi nujnost, je imel velik vpliv na družbo, ekonomsko filozofijo, politiko, kulturo idr. Praktičen, enostaven dostop do informacij in komunikacije je steber današnjega delovanja družbe. Informacije imajo pomembno vlogo tako za posameznika kot za organizacije in zahtevajo ustrezne varnostne ukrepe. Informacijska varnost ščiti informacijsko infrastrukturo pred grožnjami. V tem smislu je informacijska varnost tista, ki ustvarja in ohranja zaupnost, celovitost in trajnost. Informacijska varnost se doseže z izvajanjem vrste politik, praks, postopkov in ukrepov in z ustrezno organizacijsko strukturo (Nastasiu, 2016).

Kibernetska varnost ima na sodobno družbo velik vpliv, saj je večina vsakodnevnih dejavnosti odvisna od nekaterih informacij in komunikacijskih tehnologij, ki pa so nagnjene k neki obliki grožnje (Oliveira Albuquerque, García Villalba, Sandoval Orozco, Sousa Júnior & Kim, 2016). Informacijsko okolje je dinamično in s tem tudi grožnje. Zagotavljanje dostopnosti, celovitosti in zaupnosti podatkov je postalo ena največjih skrbi sodobne družbe v okviru vključevanja informacijskih tehnologij na vseh organizacijskih ravneh (Cioaca, Bratu & Ștefanescu, 2017). Trenutno ni splošno sprejete opredelitve kibernetske varnosti, razlog za to pa so različni pristopi med državami, med javnim in zasebnim sektorjem, med različnimi področji in dejavnostmi. Soglasno priznana pa je potreba po sodelovanju na področju kibernetske varnosti (Cioaca, Bratu & Ștefanescu, 2017). Po navedbah podjetja Gartner (2013) je kibernetska varnost skupek vodenja, razvoja, upravljanja in uporabe informacijske varnosti, operativne tehnološke varnosti in varnostnih orodij ter tehnik.

Povečanje pomena kibernetske varnosti v družbi je pripeljalo do oblikovanja novih orodij za odkrivanje in ravnanje z ranljivostmi, zlasti ob upoštevanju vedno večjega števila uporabnikov spleta. Če upoštevamo naraščajoče število podjetij in organizacij, ki uporabljajo računalnike in računalniško omrežje in s tem do njih lahko dostopamo, vidimo, da število kibernetskih napadov narašča v vseh državah sveta (Nastasiu, 2016). Problemi v zvezi s kibernetsko varnostjo so vse večja grožnja v poslovnem svetu. Naraščajoči stroški, pogostost in resnost kršitev ter kibernetskih napadov zdaj prevladujejo v razpravah o upravljanju s tveganji. Strokovnjaki ocenjujejo, da kršitve vsako leto svetovno gospodarstvo stanejo več kot 400 milijard dolarjev (Johnson, 2016).

Grožnje kibernetski varnosti v zadnjih letih postajajo vse bolj resne. Niso omejene z državnimi mejami, postale so vse bolj pogoste in sofisticirane (Nastasiu, 2016) ter ogrožajo temeljne infrastrukture družbe, kot so jedrska industrija, električna infrastruktura ipd. (Johnson, 2015). Sodelovanje in prisotnost podjetij v svetovnem kibernetskem prostoru, varnostna tveganja, vključena pri kibernetskih napadih, in značilnosti njihovega vpliva zahtevajo mednarodno sodelovanje pri zagotavljanju varnosti računalniških sistemov. Črvi in virusi so se iz preprostih groženj preoblikovali v resne varnostne grožnje in izzive in so odlično orodje za kibernetsko vohunjenje. Organizacije so postale odvisne od kibernetskih sistemov v celotnem obsegu človekove dejavnosti, vključno s trgovino, financami,

zdravjem, energijo, zabavo in komunikacijo. Globalno medsebojno povezana digitalna informacijska in komunikacijska infrastruktura, znana kot kibernetski prostor, podpira skoraj vsako področje sodobne družbe in zagotavlja podporo gospodarstvu, civilni infrastrukturi, javni in nacionalni varnosti (Nastasiu, 2016).

V vsakem trenutku so podatki oz. informacije lahko zlorabljeni. Zelo verjetno je, da se ukradejo in poškodujejo občutljivi in pomembni podatki in morda celo spravijo podjetje na kolena. Dejanske posledice so lahko uničujoče. Za razumevanje tveganja in proaktivnost za zaščito informacij, ki so ključna sredstva podjetja, to ne potrebuje strokovnjaka za informacijsko tehnologijo. Dejstvo je, da k zagotavljanju kibernetske varnosti podjetja prispevajo vsi njegovi člani, kar se lahko doseže z nekaj preprostimi vprašanji in s sledenjem postopkom (Dattu, 2016).

Kibernetsko tveganje lahko zapišemo z enostavno enačbo (1) (Kouns & Minoli, 2010):

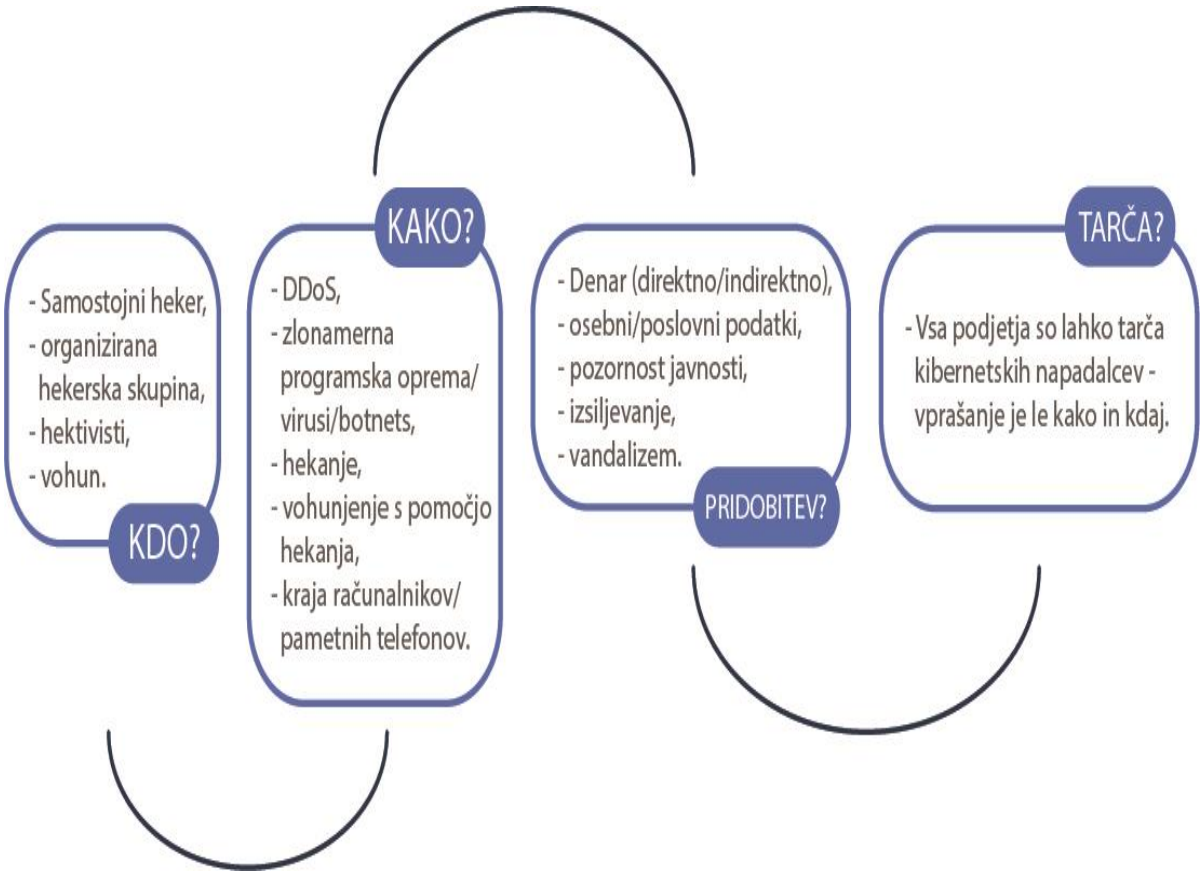
Tveganje = verjetnost za nastanek varnostnega incidenta × posledica incidenta (1)

Kot je razvidno iz enačbe, je tveganje skladno povezano s pričakovanimi izgubami, ki so posledice varnostnega incidenta (dogodka) in verjetnostjo za nastanek takega dogodka. Večje izgube in večja verjetnost za nastanek dogodka pomenijo večje kibernetsko tveganje. Temu tveganju pa se lahko izognemo ali ga upravljamo (Kouns & Minoli, 2010).

Kibernetski napadi se povečujejo v številu, pogostosti in obsegu ter postajajo vse bolj sofisticirani (Dattu, 2016; Ehrlich, 2017). Kibernetski napadi so velika in naraščajoča grožnja malim in srednje velikim podjetjem, vendar obstajajo načini in ukrepi za boj proti njim. Medtem ko so napadi na velika podjetja, kot sta na primer Yahoo in Target, bolj medijsko odmevni, so majhna in srednje velika podjetja prav tako ranljiva. Po poročanju podjetja Symantec, ki ponuja storitve za zagotavljanje kibernetske varnosti, je bilo leta 2015 na mala in srednje velika podjetja izvedenih kar 43 % vseh kibernetskih napadov. Mala podjetja se ne zavedajo, da napadalci nanje gledajo kot na lahek plen. Seveda obstajajo ukrepi, s katerimi lahko podjetja postanejo manj ranljiva in se v primeru kibernetskega napada znajo braniti in boriti (Finkle, 2017).

Dandanes ni več vprašanje, ali podjetje bo žrtev kibernetskega napada, temveč je vprašanje, kdaj bo žrtev kibernetskega napada. Takšno je opozorilo strokovnjakov kibernetske varnosti, ki redno opozarjajo podjetja vseh velikosti v vseh panogah gospodarstva. To je realnost digitalne dobe. Notranji pravilniki podjetja o varnosti podatkov so lahko obširni in podrobni, vendar zadostuje le en utrujen, len ali zlonameren zaposleni, da v svet pošlje ključne podatke podjetja, ki morda nikoli ne bodo povrnjeni (Opderbeck, 2016).

Slika 1: Viri, načini, razlogi in tarče kibernetskih napadov



Vir: Willis (2013).

1.1 Razlogi za nastanek kibernetskega tveganja

Napadalci navadno ne načrtujejo kibernetskega napada, da bi pridobili slavo, ampak da bi imeli od njega finančno korist (Etsebeth, 2011). Glavni cilj napadalcev je največkrat denar ali pridobitev občutljivih oziroma zaupnih podatkov podjetja ali njihovih strank. Napadalci z izsiljevalskimi virusi navadno zakodirajo datoteke, do katerih lahko lastniki teh datotek pridejo po plačilu določene odkupnine (Perko, 2017). Višina odkupnine se lahko giblje od nekaj sto pa do nekaj tisoč evrov, odvisno od zmožnosti žrtve, da plača določen znesek (Werner, 2017). Prav ta način (odkupnina v zameno za zakodirane datoteke) je pri kibernetskih napadih najbolj pogost (Perko, 2017). Vendar plačilo odkupnine še ne pomeni, da bodo izgubljeni podatki oziroma datoteke povrnjene (Werner, 2017). Državni organi največkrat svetujejo, da se napadalcem ne odkupnina izplača, saj naj bi plačevanje le spodbujalo nadaljnje tovrstno početje, vendar pa je treba poudariti, da podjetjem, ki nimajo varnostnih kopij, ne preostane nič drugega, kot da odkupnino plačajo in si tako povrnejo izgubljene podatke (Perko, 2017). Zato morajo biti tudi računovodski servisi obveščeni o nevarnostih, ki jih predstavljajo hekerji in prevaranti, ter sprejeti določene ukrepe, da bi zaščitili sebe in svoje stranke (Werner, 2017). Kibernetsko tveganje ni izključno težava IT

oddelka, vendar ta očitno igra eno ključnih vlog v celotnem podjetju (Institute of Risk Management, brez datuma b). Vodja informacijske varnosti in finančni direktor morata postati partnerja in združiti moči, da bi razumela varnostno tveganje podjetja in vse z njimi povezane finančne stroške. Zdaj obstaja vrzel med večino finančnih direktorjev in varnostnimi strokovnjaki, ko gre za utrditev podjetja pred kibernetskimi napadi: nedavni podatki kažejo, da 39 % IT strokovnjakov ne verjame, da njihovo vodstvo razume vpliv, ki bi ga imela varnostna kršitev na ugled njihovega podjetja (Vintz, 2017). Tudi funkcija upravljanja s tveganji mora temeljito razumeti nenehno razvijajoča se tveganja, pa tudi praktična orodja in tehnike, ki so na voljo za njihovo reševanje oziroma upravljanje (Institute of Risk Management, brez datuma a).

1.2 Najpogostejši načini vdorov v informacijski sistem podjetij

Cilj večine kibernetskih napadov je krasti, izkoristiti ali uničiti podatke. Kršitve se lahko pojavijo v obliki nepredvidenih, naključnih napadov, da bi dobili čim več informacij, usmerjenih napadov z izbrano tarčo ali napadov zaradi brezskrbnih ali nezadovoljnih zaposlenih. Ne glede na cilj ali vrsto napada nekatere taktike napadov izstopajo. MSP (mala in srednje velika podjetja) in njihovi zaposleni morajo biti z njimi seznanjeni in nanje pozorni (Ramsay, 2015).

Vdor v računalniški sistem je najbolj klasična oblika hekerskega napada, ki se je v različnih oblikah pojavil že v 60. in 70. letih prejšnjega stoletja. Pomeni nepooblaščen dostop do sistema (ali omrežne opreme), v običajnem poteku pa napadalec pred vdorom izvaja pregledovanje (skeniranje) omrežja. Dva najbolj pogosta načina vdora v omrežno napravo se izvajata z izkoriščanjem ranljivosti programa in slabega gesla (ali odsotnosti kakršne koli avtentikacije) (SI-CERT, brez datuma b).

Zlonamerna programska oprema (ang. malware) pomeni kateri koli računalniški program, katerega namen je škoditi, ukrasti podatke, izterjati denar, uničiti žrtev ali storiti nekaj neželenega uporabniku računalnika. Zlonamerna programska oprema vključuje viruse, črve, ki se lahko sami širijo z računalnika na računalnik, izsiljevalske programe, ki lahko uporabnikom zaklenejo dostop do datotek, keyloggerse in trojanske konje. (Ramsay, 2015). Trojanski konj je vrsta zlonamerne programske opreme, ki vsebuje zlonamerno kodo z različnimi vplivi, kot sta izguba ali kraja podatkov (Ashtiani & Abdollahi Azgomi, 2014). Zlonamerna programska oprema lahko najde pot do računalnika na več načinov, vključno z obiskom spletnega mesta, okuženega z zlonamerno programsko opremo, povezovanje z zlonamerno programsko opremo prek elektronske pošte ali socialnih medijev ali z namestitvijo programske opreme iz neznanega vira (Ramsay, 2015). Poročilo The Ponemon Institute je pojasnilo, da sta zlonamerna programska oprema in zlonamerna koda povezani in da zlonamerni napadi pomenijo napad z zlonamerno kodo, če se le-tej uspe infiltrirati v sistem in omrežje podjetja. Večina metod potrebuje nevednega pomočnika v obliki

uporabnika računalnika, ki klikne na okužen dokument, uporablja slabo geslo, priključi okužen USB, ipd. (Kesan & Hayes, 2017).
Izsiljevalski programi so še ena taktika, ki se pogosto uporablja pri napadih na MSP-je. Računalniški programski gigant Microsoft je izsiljevalske programe opisal kot programe, ki jih uporabljajo napadalci, da bi prisilili tarčo, da naredi nekaj, kar bi uporabniku zaklenilo njegov računalnik ali datoteke. Lahko pa je tudi grožnja, da bodo napadalci javno objavili neugodne informacije o tarči (Microsoft). Poleg uporabe varnih računalniških praks za preprečevanje izsiljevalskih programov je pomembno varnostno kopiranje podatkov, saj omogoča obnovo zaklenjenih ali izgubljenih podatkov (Ramsay 2015).

Phishing (lažno predstavljanje) je proces prikritega in nezakonitega pridobivanja uporabnikovih vstopnih podatkov za prihodnjo korist in je trenutno ena najpogostejših taktik na področju kibernetskih napadov. Ocene vseh izgub, ki so posledica phishinga, se zelo razlikujejo, vendar se vse izražajo v milijardah dolarjev letno. To so ciljno usmerjeni napadi, najpogosteje prejeti po elektronski pošti, ki je do neke mere personalizirana in tarčo preusmeri na goljufivo spletno stran, ki je videti legitimna (opozorilni znak je na primer napačno črkovan spletni naslov). To preusmerjanje se pogosto pojavi, ko tarča klikne povezavo v elektronskem sporočilu. Tarča je nato usmerjena na vnos podatkov, ki napadalcu omogočajo, da zbira občutljive podatke, kot so evidence o računih, podatki za prijavo in podatki o kreditnih karticah. Tehnologije, ki jih uporabljajo napadalci, se nenehno izboljšujejo. To je postala velika nadloga za spletne prodajalce, finančne institucije in podobne organizacije (Aschenden, 2016; Ramsay, 2015; Fallon, 2015 v Ramsay, 2015; SI-CERT, brez datuma d). Ker splet ni omejen z državnimi mejami, se problem phishinga pojavlja tako v državah v razvoju kot tudi v razvitih državah zahodnega sveta (Al-Hamar, Dawson & Al-Hamar, 2011).

Izguba ali kraja podatkovnih medijev. Vsaka izguba ali kraja medija, ki nosi podatke o podjetju, napačna namestitev pogona v USB ali kraja prenosnega računalnika je ogrozitev integritete podjetja in podatkov (Ramsay, 2015).

Ostali načini kibernetskih napadov oziroma varnostne grožnje so še (Willis, 2013; SI-CERT, brez datuma a); The Ponemon Institute, 2016):

- DDoS (Distributed Denial of Services) in DoS (Denial of Services) pomenita napad za zavrnitev storitve in kibernetski napad, v katerem napadalci pošljejo veliko količino podatkov z namenom preobremenitve in posledično nedelovanja informacijskega sistema (Kouns & Minoli, 2010), kar lahko na primer pomeni nedelovanje spletne strani, to pa dejanskim uporabnikom ali kupcem oteži ali celo onemogoči izvedbo nakupa oz. uporabo spletne strani.
- Spam – neželena elektronska pošta. Vsi uporabniki elektronske pošte se soočamo s prejemanjem neželene elektronske pošte, ki zapolni naš elektronski poštni predal.

Namen neželene pošte je vsiljevanje določene vsebine in je navadno namenjena večjemu številu ljudi, ki se za prejemanje te vsebine ne odločijo sami.

- Spletni napadi in goljufije se navadno izvedejo s pomočjo lažnih oglasov, ponudb za nakup ali potvorjenih sporočil, s katerimi želijo napadalci priti do denarja.
- Kraja identitete pomeni nepooblaščeno pridobitev osebnih podatkov osebe in predstavljanje napadalca za osebo, katere osebne podatke je pridobil. Posledica kraje identitete je lahko zavajanje drugih oseb, škoda ugledu osebe, pridobitev dostopa do osebnih informacij, dokumentov, slik in denarja. Kraja identitete je najpogosteje posledica kraje uporabniškega imena in gesla (Varni na internetu, 2013; SI-CERT, brez datuma c).
- Socialni inženiring je vrsta napada, kjer napadalec izkoristi človeške lastnosti in z zavajanjem (manipulacijo, lažmi, triki, podkupninami, izsiljevanjem, grožnjami) žrtev prepriča, da naredi nekaj, česar oseba sicer ne bi naredila (Raba interneta v Sloveniji, 2009).

1.3 Viri kibernetskih napadov

Grožnje lahko podjetju pretijo z različnih virov (notranjih in zunanjih) in so lahko namerne ali nenamerne. Notranje in zunanje grožnje ločimo na podlagi tega, ali je vir kibernetskega napada znotraj ali zunaj podjetja (Siegel, Sagalow & Serritella, 2002).

Notranje grožnje sestavljata namerna in nenamerna izguba podatkov, najpogosteje s strani zaposlenih. Pogosto zaposleni sploh ne vedo, kdaj njihova dejanja podjetje izpostavijo tveganju, ko na primer postanejo žrtve phishing elektronske pošte ali nezavedno na računalnik namestijo nevarno programsko opremo. Medtem ko sistemi kibernetske varnosti in programi ozaveščanja pomagajo braniti podjetje pred temi nenamernimi človeškimi napakami, namerna notranja grožnja predstavlja drugačen izziv. Te osebe imajo lahko vodstvene privilegije ali pa si povečajo obstoječe privilegije z namenom kraje lastniških informacij podjetja in/ali podjetju povzročijo veliko škodo. Razkritje informacij načrtujejo in izvedejo z zlorabo svojih privilegijev ali preprosto zato, ker podatki niso bili varni. Grožnjo lahko predstavljajo tudi nekateri nekdanji zaposleni, še posebno, če imajo še vedno dostop do podatkov o podjetju, v katerem niso več zaposleni (Ramsay, 2015). Človeška napaka je lahko razlog za varnostno kršitev, kljub temu da zlonamerni napadalec ne obstaja (Kesan & Hayes, 2017).

Grožnje, ki izvirajo iz notranjega okolja, so za odkrivanje še posebno težke. Večina standardnih tehničnih kontrol, kot so požarni zid, antivirusni programi ali programi za zaznavanje vdorov, predvideva, da interni uporabniki delajo tako, da podpirajo varnostno infrastrukturo. Zato so te kontrole neučinkovite, če zaposleni delujejo aktivno, da bi zaobšli sistem (Siegel, Sagalow & Serritella, 2002).

O zunanjih grožnjah govorimo, ko kibernetski napad izvede heker, organizirana hekerska skupina, hektivist, nezadovoljni nekdanji zaposleni, konkurent podjetja, pošiljatelj neželene elektronske pošte (spama) ipd. iz razlogov, ki so bili že predhodno omenjeni (denar, podatki in informacije, slava, izsiljevanje, povzročanje škode ali vandalizem, …) (Willis, 2013; Dattu, 2016).

1.4 Možne posledice kibernetskega napada

Posledice kibernetskih kršitev in napadov so lahko precejšne in sežejo globoko v jedro podjetja. Vpliv kršitev lahko vključuje izgubo, prodajo ali objavo podatkov podjetja ali osebnih podatkov zaposlenih ali strank, kot so številke socialnega zavarovanja, domači naslovi, osebne telefonske številke, bančni računi, zdravstveni zapisi, elektronska sporočila gesla ipd. Stranke, zaposleni in gospodinjstva zaupajo organizacijam, tudi podjetjem, z dragocenimi informacijami in odgovornost podjetja je, da posamezniku zagotovi zaščito teh informacij (Dattu, 2016).

Posledica kibernetskega napada je lahko tudi poškodovan ugled podjetja v očeh kupcev in drugih deležnikov. Če se ugotovi, da je bilo podjetje žrtev napada zaradi malomarnosti in da so bili izgubljeni podatki o strankah ali končnih kupcih, je ugled podjetja še toliko bolj omadeževan. Za ugled podjetja pa velja, da se gradi dolgo in da ga je le stežka popraviti.

Finančne posledice so prav tako ena od pomembnih posledic kibernetskega napada. Podjetje lahko napadalci izsiljujejo in zahtevajo odkupnino za podatke, ki pa so v primeru neplačila lahko javno objavljeni. Po napadu je navadno treba vložiti finančna sredstva v povrnitev podatkov in ugleda ter vzpostaviti varnostne politike, ki bi v prihodnosti preprečile kibernetski napad.

1.5 Najbolj odmevni svetovni kibernetski napadi

Target, 2013. V podjetju Target je leta 2013 prišlo do kibernetskega napada, pri katerem so hekerji pridobili zaupne podatke o kreditnih in debetnih karticah več kot 40 milijonov strank. Po preiskavi je Target poročal, da je hekerjem uspelo pridobiti osebne podatke kar 110 milijonov strank (Johnson, 2016).

Home Depot, 2014. Leta 2014 je prišlo do kibernetskega napada, v katerem so s podobno metodo prevare napadli podjetje Home Depot, ki prodaja material in izdelke za vzdrževanje doma. Pridobili so informacije o kreditnih in debetnih računih 56 milijonov kupcev ter 53 milijonov elektronskih naslovov strank (Johnson, 2016).

Pri kibernetskih napadih na Target in Home Depot je zlonamerna programska oprema okužila sistem za beleženje kartičnega plačevanja, ki hekerjem omogoča pregledovanje, zapisovanje in spreminjanje podatkov (Johnson, 2016).

VTech, 2015. Globalno podjetje Vtech, ki proizvaja izdelke za elektronsko učenje in je hkrati največji svetovni proizvajalec otroških brezžičnih telefonov, je bilo napadeno novembra leta 2015. Ukradeni podatki so vključevali imena otrok, spol in datum rojstva, poštne naslove in elektronske naslove njihovih staršev, skrivna vprašanja za pridobitev gesel, IP naslove in zgodovino prenosov. V napadu je bilo pridobljenih dovolj podatkov, da bi lahko obnovili celotne družinske profile. Dnevnike, slike in posnetke je mogoče izslediti do določenih uporabniških imen, ki napadalcem omogočajo identifikacijo ljudi, ki klepetajo in se pojavijo na fotografijah. Analiza napada je pokazala, da podjetje VTech ni uspelo sprejeti niti najosnovnejših varnostnih ukrepov, vključno s tem, da podatki v tranzitu niso bili niti osnovno zakodirani, kar je bila na področju informacijske varnosti že vsaj desetletje standardna praksa ob napadu (Miller, 2016).

Deloitte, 2017. Podjetje Deloitte naj bi po navedbah revije The Guardian doživelo kibernetski napad, ki je razkril elektronske naslove strank. Deloitte je eno od »Big Four« računovodskih in revizijskih podjetij, ki je bilo tarča kibernetskega napada. Napad je ogrozil zaupne elektronske naslove in načrte nekaterih Blue-chip podjetij. Podjetje nekaj mesecev sploh ni vedelo, da se je napad zgodil. Za napad so izvedeli marca 2017, napadalci pa naj bi imeli dostop do sistema že od oktobra ali novembra leta 2016. Podjetje ponuja revizijske storitve, davčno svetovanje in ironično tudi svetovanje glede kibernetske varnosti nekaterim velikim svetovnim bankam, multinacionalkam, medijskim podjetjem, farmacevtskim podjetjem in vladnim organizacijam. Deloittove stranke v vseh teh sektorjih so imele podatke podjetja v sistemu elektronske pošte, ki je bil napaden. Deloitte je o nepooblaščenem dostopu do podatkov obvestil le nekaj strank, vse dokler novica ni prišla v medije. Podjetje Deloitte je takoj sprožilo notranjo revizijo glede varnostnega incidenta. Napadalci so dostopali do globalnega strežnika za elektronsko pošto prek administratorjevega računa, ki pa jim je dal možnost neomejenega dostopa do vseh podatkov. Administratorjev račun je zahteval samo eno geslo in ni imel dvostopenjskega preverjanja. Elektronska sporočila za Deloittovih 244.000 zaposlenih in od njih so bila shranjena na oblaku podjetja Azure, ki ga zagotavlja podjetje Microsoft. Poleg elektronskih sporočil naj bi imeli hekerji tudi dostop do uporabniških imen, gesel, IP naslovov in zdravstvenih informacij. Nekatera elektronska sporočila pa so imela tudi priloge z občutljivimi varnostnimi podrobnostmi. Napad naj bi bil usmerjen na ZDA in je veljal za tako občutljivega, da je bila obveščena le peščica Deloittovih najstarejših partnerjev in odvetnikov. Notranja raziskava je razkrila, da je bil napad izvršen pod imenom Windham. Raziskava je vključevala strokovnjake, ki so poskušali z analizo elektronskih sledi iskanih poizvedb natančno določiti, kje so se hekerji nahajali. Ekipa, ki preiskuje ta kibernetski napad, ve, da se je napad zgodil v pisarnah v mestu Roslyn v Virginiji. Ugotoviti morajo še, ali je za napad odgovoren samostojni heker, kateri od poslovnih tekmecev, ali heker, ki ga sponzorira država. Če hekerji niso mogli zakriti vseh svojih sledi, bi moralo biti mogoče ugotoviti, do katerih podatkov so dostopali. Podjetje Deloitte je aprila 2017 najelo ameriško odvetniško podjetje za »posebno nalogo«, ki so jo poimenovali »morebitni incident kibernetske varnosti«, za pravno svetovanje in pomoč

glede potencialnih izgub zaradi kibernetskega vdora. Deloitte je priznal, da je bil žrtev kibernetskega napada, vendar vztraja, da je bilo ogroženo majhno število strank. Po ocenah naj bi bilo v oblaku pet milijonov elektronskih naslovov, do katerih so hekerji lahko dostopali, Deloitte pa pravi, da je bil ogrožen le del teh elektronskih naslovov. Predstavnik za javnost podjetja Deloitte pravi, da je Deloitte kot odziv na kibernetski incident izvedel celovit varnostni protokol in začel intenziven in temeljit pregled vključno z mobilizacijo skupine notranjih in zunanjih strokovnjakov za kibernetsko varnost in zaupnost. V okviru pregleda je bil Deloitte v stiku z nekaj ogroženimi strankami, obvestili pa so tudi vladne organe in regulatorje. Ne želijo pa povedati, katere organe so obvestili in kdaj. Pregled jim je omogočil, da so razumeli, katere informacije so bile ogrožene in kaj je napadalec dejansko naredil. Pokazal je, da ni prišlo do motenj v poslovanju s strankami in sposobnost Deloitta, da še naprej služi strankam in potrošnikom. Zdaj se Deloitte trudi dokazati, da so globoko zavezani k zagotavljanju kibernetske varnosti in da so njihovi obrambni sistemi najboljši, da veliko vlagajo v varovanje zaupnih podatkov ter nenehno pregledujejo in izboljšujejo kibernetsko varnost (Hopkins, 2017).

Čeprav so kibernetski napadi usmerjeni na vsa večja podjetja, je ta kibernetski napad za Deloitte velika sramota, saj strankam nudi svetovanje in pomoč tudi o tem, kako obvladati kibernetsko tveganje, ki ga povzročajo prefinjeni napadi na kibernetsko varnost. Leta 2012 je bilo podjetje Deloitte, ki ima svoje pisarne po vsem svetu, uvrščeno med najboljše svetovalce za kibernetsko varnost na svetu (Hopkins, 2017).

Stuxnet, 2010. Virusni napad na iranski jedrski program v letu 2010 – to se zgodi, ko je izgubljeno zaupanje v sistem, na katerega se podjetje zanaša; ko prikazi in nadzorne plošče izkazujejo normalno delovanje, že na prvi pogled pa so opazne napake. O tehnoloških učinkih virusa Stuxnet je bilo izdatno poročano, nasprotno pa ni bilo preučeno, kaj je bil razlog tega napada; ta je Irance prepričal, da ne verjamejo ne svojim napravam ne lastnim očem. To je bil prvi večji napad na industrijski nadzorni sistem, ki se je izkazal kot zunanja sovražna grožnja. Učinek je presegel fizično uničenje – v sistem je zasejal takšen dvom in nezaupanje, da so Iranci na obrat z namenom opazovanja in poročanja postavili fizične osebe. Predvidevajo, da se je napad zgodil s prehodom zlonamerne kode na sistem iz prenosnega računalnika, ki ga je uporabljal vzdrževalni inženir. Virus je čakal na prenosnem računalniku, ki se je povezal s sistemom podjetja, kar je virusu dalo priložnost, da se prenese na omrežje in začne napad, za katerega je bil ustvarjen (Ashenden, 2016).

Napad na SCADA sistem. V tem primeru je šlo za notranji napad na radijsko nadzorovano opremo za kanalizacijo v Avstraliji. Motiv za napad je bilo maščevanje. Nezadovoljen nekdanji zaposleni je opremi, s katero je bil seznanjen in je z njo v preteklosti delal, izdal radijske ukaze. Povzročil je poplavo odplak v parkih, rekah in stavbah. Število napadov na sistem SCADA in proizvodne obrate je še vedno nizko. Poudarek je na obravnavanju tehničnih ranljivosti. V takšnih obratih je vedno več tehnologije, ki je povezana z spletom (navadno za namene vzdrževanja) (Ashenden, 2016).

Vsako napadeno podjetje ni vedno tako dobro znano, kot so Home Depot, Target, Deloitte, idr. Samo zato, ker podjetje morda meni, da je premajhno in premalo znano, ne pomeni, da je za kibernetske napadalce nemogoča tarča. Eden od primerov malega oz. srednje velikega podjetja (MSP), ki je bilo napadeno, je Direct Marketing Association (dalje DMA). DMA je svoje stranke obvestil, da so zaznali napad na spletni strežnik knjigarne, na katerega je bila nameščena zlonamerna programska oprema, ki bi lahko ogrozila podatke o kreditnih in debetnih karticah (Direct Marketing Association, 2015).

Medijska izpostavljenost kibernetskih incidentov je pripomogla k večji pozornosti vodstva in temu, da lahko tisti zaposleni v podjetju, ki so zadolženi za kibernetsko varnost, lažje poudarijo potrebo po kibernetski varnosti in zahtevajo več sredstev za programe kibernetske varnosti v prihodnosti (Deloitte, 2017). Ne samo, da kibernetski napadi povzročijo neposredne stroške, ampak ogrozijo tudi prihodnje poslovanje podjetja (Ramsay, 2015).

1.6 Upravljanje s kibernetskim tveganjem in ukrepi

Razvoj tehnologije in prefinjenost hekerjev sta kibernetsko varnost postavili za eno najpomembnejših področij upravljanja tveganj za podjetja (Tysiac, 2016). Ker poslovanje podjetij postaja vse bolj digitalno, mora kibernetska varnost postati del vsakodnevnih aktivnosti. To pomeni, da se v podjetjih na kibernetsko tveganje gleda kot na še eno operativno tveganje, enako kot na primer na fizično škodo ali krajo in ni omejeno le na IT oddelek (Ashford, 2017; Epstein, 2014). Splet kibernetskim napadalcem omogoča, da napadejo in pridobijo informacije podjetja, zato morajo le ta oblikovati obrambne ukrepe (Hausken, 2017). Strokovnjaki za informacijsko varnost imajo ključno vlogo pri preoblikovanju digitalnih procesov za zagotavljanje, da podjetja razumejo kibernetsko tveganje in izvajajo potrebne ukrepe za zagotovitev kibernetske varnosti. Razumevanje kibernetskega tveganja navadno ni največji izziv, ampak je to reševanje komunikacijske vrzeli med tehničnim osebjem in lastniki oziroma vodstvom podjetja. IT strokovnjaki lahko s pravilno komunikacijo ostalim zaposlenim pomagajo razumeti, da je kibernetsko tveganje tudi poslovno tveganje. Kulturo kibernetske varnosti je treba promovirati z uporabo poslovnega in ne informacijsko tehničnega (IT) jezika, saj posamezniki prenehajo poslušati, ko vsebine ne razumejo. Strokovnjaki za informacijsko varnost morajo zato komunicirati publiki razumljivo in razumeti tveganje v poslovnem kontekstu, zato da je njihovo svetovanje relevantno in pragmatično za izvajanje. Ta tveganja morajo biti razložena tako, da so posledice v podjetju v primeru zlonamernega ali slučajnega incidenta jasno razumljive (Ashford, 2017).

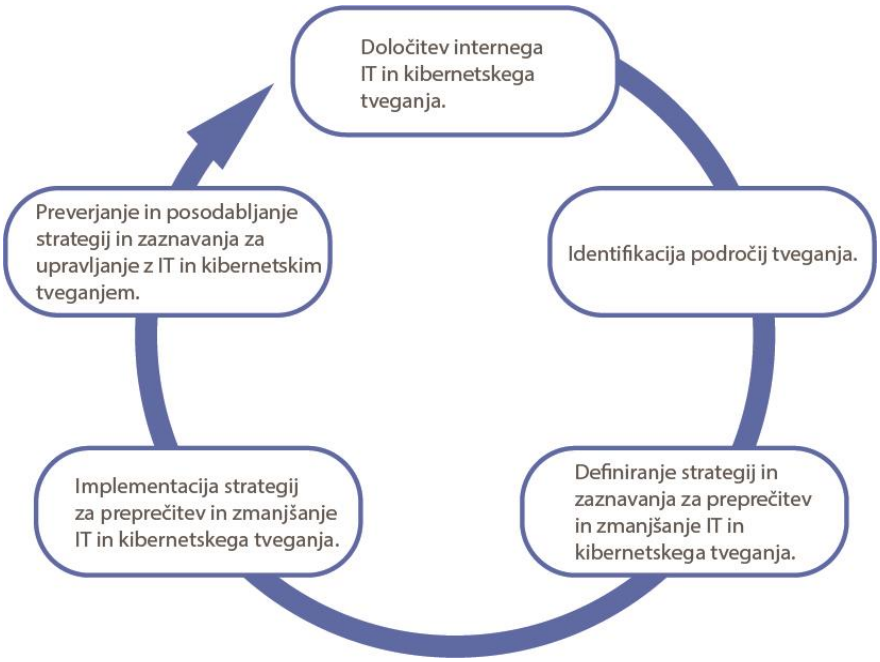
Čeprav se v zadnjih letih izdatki podjetja za zagotavljanje kibernetske varnosti povečujejo, je to še vedno premalo. IT proračun navadno znaša od 3 do 7 % prihodkov podjetja, varnostni proračun pa 5 % IT proračuna. To pomeni, da se finančnim direktorjem vlaganje v varnost podjetja izplača. V poročilu za leto 2016 (Forrester Consulting, 2017) je bilo ugotovljeno,

da so v zadnjih dveh letih podjetja, ki v IT varnostne sisteme vlagajo več sredstev, zaznala 6,8-krat manj kršitev in prihranila več kot 5 milijonov dolarjev. Eksplozija podatkov in povezanih naprav torej širi površino napadov za podjetja, ki so bila do nedavnega relativno zaščitena z zavarovalnimi parametri (Vintz, 2017).

Informacijska varnost se ukvarja s tem, kako vodstvo podjetja upošteva, uporablja in upravlja z informacijsko tehnologijo pri nadzoru, spremljanju in usmerjanju družbe. Iz varnostnih informacij lahko izhajajo različne koristi, vključno z večjo gospodarsko učinkovitostjo, večjo produktivnostjo in rastjo, zadostno varnostjo informacijskih sredstev, virov in sistemov ter zagotavljanjem trajne sposobnosti preživetja in blaginje podjetja. Ne gleda na vse je verjetno najpomembnejša prednost, ki jo lahko najdemo v sposobnosti te discipline, upravljanje z mehanizmom za izogibanje pravni odgovornosti, ki temelji na neuspešnem in neustreznem varovanju informacij. Če vodstvo lahko dokaže obstoj učinkovitega programa za varovanje informacij v podjetju, je lahko prepričano, da je skrbno izpolnilo svojo dolžnost. To velja ne glede na vrsto ali naravo varnostnih incidentov, ki se lahko pojavijo v prihodnosti ali so se zgodili v preteklosti (Etsebeth, 2011).

Gaudenzi in Siciliano (2017) predlagata naslednji postopek zagotavljanja kibernetske varnosti (grafični prikaz v sliki 2): Podjetje naj najprej opredeli notranje IT in kibernetsko tveganje. To lahko naredi v dokumentu varnostne politike. Naslednji korak je identifikacija področij, kjer se ta tveganja lahko pojavijo. Nato podjetje opredeli strategijo in ukrepe za preprečitev IT in kibernetskega tveganja ter jih v naslednjem koraku implementira v poslovanje in jih izvaja. Zadnji korak je preverjanje in posodabljanje strategij in ukrepov za zagotavljanje kibernetske varnosti. Da pa podjetje lahko identificira tveganja in nevarnosti, ki mu pretijo, mora najprej dobro poznati svoj celotni sistem in funkcije (Tudose, 2012).

Slika 2: Koraki za zagotovitev kibernetske varnosti



Vir: Gaudenzi & Siciliano (2017).

Čeprav izpostavljenost podjetja tveganju nikoli ne more biti popolnoma izničena, bi morali biti izvedeni vsi koraki, da se izpostavljenost minimizira, škoda pa omeji (Siegel, Sagalow & Serritella, 2002).

Prvi korak za zaščito informacij podjetja in zagotovitev kibernetske varnosti pred načrtovanimi napadi je ugotoviti, katere informacije so ogrožene in kdo so potencialni napadalci. Zastaviti si je treba vsaj štiri vprašanja (Hackett, 2013):

1. Kdo bi se lahko zanimal za informacije, ki jih podjetje ima?
2. Kakšne zmogljivosti imajo napadalci?
3. Kje je podjetje najbolj ranljivo?
4. Kaj lahko podjetje stori, da bo manj ranljivo?

Ko ima podjetje odgovore na zgornja vprašanja, mora raziskati orodja za kibernetsko varnost in oceniti, katera so primerna za njegove potrebe ter kakšne so prednosti in slabosti teh orodij glede na situacijo podjetja. Če želi biti podjetje pripravljeno na napad, mora preučiti strategije napadalcev; to pomeni, da se spozna s tehnikami in programi, ki jih uporabljajo kibernetski napadalci. Ko se podjetje zaveda okolice in orodij, ki se lahko uporabijo proti njemu, lahko začne razmišljati o načinih nenamernega razkritja informacij ljudem, s katerimi pridejo v stik. Če vemo, kako se zaščititi proti tehnikam, ki jih uporabljajo, potem se lahko načeloma počutimo varne (Hackett, 2013).

Varnostna politika je prvi korak do upravljanja s kibernetskim tveganjem in zagotavljanja varnosti podatkov in informacij v podjetju. Varnostna politika informacijskega sistema podjetja je interni dokument, ki podrobneje določa, na katerih področjih je treba varovati informacijski sistem. Oblika in vsebina tega dokumenta nista določena, zato ima podjetje proste roke pri vsebinskem in oblikovnem ustvarjanju svoje varnostne politike. Vseeno obstajajo določene smernice, kaj naj podjetje v svojo varnostno politiko vključi in v njej opredeli. V dokumentu varnostne politike naj se podjetje dotakne tem, kot so dejavniki, ki vplivajo na delovanje informacijskega sistema, pravila organizacije in pa postopki oz. poslovni procesi. Dokument varnostne politike je treba nenehno posodabljati, saj se za podjetje ključne informacije lahko spremenijo, iz podjetja lahko odide oseba, ki je bila v varnostni politiki navedena kot skrbnik določenih informacij, nenehno se spreminjajo tudi programske rešitve in še marsikaj drugega. Najpomembneje pa je, da so vsi v podjetju seznanjeni z dokumentom in ga znajo uporabljati. Varnostna politika podjetja vključuje seznam podatkov (katalog podatkov), varnostno kvalifikacijo, tveganje, določi entitete (na primer stranke) in atribute entitet (podatki ali poslovni dogodki o tej stranki), imenuje skrbnike podatkov, njihov dostop do podatkov, njihove dolžnosti, pristojnosti in odgovornosti, določi, kateri podatki so ključni za podjetje, postopke oziroma poslovne procese, programske rešitve za zaščito teh podatkov, tehnične ukrepe za zagotovitev informacijske varnosti, postopek v primeru varnostnega incidenta, ipd. Šele ko podjetje opredeli vse podatke, s katerimi upravlja in jih obvladuje, lahko začne izvajati ukrepe za zagotovitev kibernetske varnosti.

Podjetje lahko imenuje pooblaščeno osebo za varstvo podatkov. Splošna uredba za varstvo osebnih podatkov posebej opredeljuje, katera podjetja morajo imenovati pooblaščeno osebo. Ostalim podjetjem pooblaščene osebe ni treba imenovati, za imenovanje pa se lahko vseeno odloči, v kolikor meni, da jo potrebuje.

1.6.1 Ustrezna tehnična in informacijska tehnologija in podpora

Najosnovnejši ukrep je uporaba ustrezne tehnične in informacijske tehnologije ter sistemov za zagotavljanje informacijske varnosti. Eno od najbolj zanesljivih orodij za zagotovljeno informacijsko varnost so varnostne kopije. Te pomagajo v primeru zakodiranih podatkov z virusom ali izsiljevalskim programom, ki je bolj tehnično napreden in za katerega še ni znanih orodij za povrnitev datotek (Perko, 2017). Za nekatere napade je na spletu že mogoče najti rešitve za povrnitev datotek. Zato je za računovodstva priporočljivo uvesti politiko za pogosto (dnevno) ustvarjanje varnostnih kopij za podatke, ki jih ne smejo izgubiti (Werner, 2017). Varnostne kopije pa ne pomagajo, če je podjetje deležno izsiljevanja z objavo kočljivih podatkov v primeru neplačila odkupnine (Perko, 2017). Prav tako je priporočljivo testirati restavriranje podatkov iz narejenih varnostnih kopij, da se zagotovi zanesljivost varnostnih kopij (Siegel, Sagalow & Serritella, 2002).

Nekateri napadi vključujejo tudi zasedbo varnostnih kopij, zato jih je priporočljivo narediti več (Werner, 2017). Podatkovne baze je priporočljivo imeti na več različnih mestih oziroma podatkovnih nosilcih, tudi v programih v oblaku in na zunanji strojni opremi, ki ni povezana na omrežje podjetja. To varuje pred nekaterimi vrstami napadov, tudi pred izsiljevalskim virusom, ki namerno cilja na varnostne kopije (Finkle, 2017). Računalniške storitve v oblaku postajajo pomembno orodje za računovodje in računovodska podjetja, saj ponujajo učinkovito, fleksibilno in cenovno ugodno rešitev in možnost dostopa do računalniškega sistema podjetja od kjerkoli, kjer je splet (Kuang-Hua, Fu-Hsiang & Wei-Jhou, 2016). Treba pa se je zavedati tudi pomanjkljivosti, povezanih z računalništvom v oblaku. Ker gostiteljeve storitve navadno služijo več strankam, se lahko pojavijo različna vprašanja, povezana z varnostjo. Če na primer druga stranka gostitelja ogrozi sistem, lahko to vpliva tudi na varnost informacij ostalih strank ponudnika oblačnih storitev. Oblačne storitve pa pomenijo tudi možnost dostopa do informacij tretjim osebam, kar lahko predstavlja varnostne, skladnostne in regulativne težave (Grossman, 2009).

Priporoča se tedensko posodabljanje programske opreme. To je na prvi pogled videti zamudno, vendar je ohranjanje posodobljene programske opreme ključnega pomena za preprečevanje napadov. Symantec, podjetje, ki ponuja storitve za zagotavljanje kibernetske varnosti, ocenjuje, da ima več kot tri četrtine zakonitih spletnih strani ranljivosti, ki zahtevajo popravilo. Izdajatelji programske opreme in operacijskih sistemov nenehno izdajajo nove varnostne posodobitve in popravke, ki pa se na napravo ne namestijo samodejno. Če podjetje nima sposobnosti, da bi posodobitve nameščalo pravočasno, je treba razmisliti o zaposlitvi osebe, ki to nalogo opravlja vsaj na tedenski ravni (Finkle, 2017).

Za zagotovitev zaščite računalnika uporabnik ne sme pozabiti niti na antivirusni program, ki spada k osnovni programski opremi. Antivirusni program je računalniški program, ki je namenjen odkrivanju in odstranjevanju računalniških virusov in zlonamerne programske opreme, preden ima ta priložnost prodreti v sistem (FCC, 2012). Kljub temu pa naložen antivirusni program uporabniku ne zagotavlja popolne varnosti. Na internetu se vsakodnevno pojavljajo nove grožnje, zato morajo proizvajalci antivirusnih programov le te nenehno posodabljati. Pomembno je, da jih posodobijo tudi uporabniki in da imajo naloženo zadnjo različico programa, ki vsebuje zaščito za najnovejše grožnje.

Prav tako se odsvetuje uporaba spletne banke na javnih računalnikih ali odprtih wi-fi omrežjih, saj lahko vsebujejo zlonameren program, ki prestreže številke bančnih računov, gesla in ostale pomembne podatke (Consumer reports, 2011).

Veliko ljudi uporablja kratka in preveč enostavna gesla, s katerimi dostopajo do različnih spletnih strani in aplikacij, morda uporabljajo le eno za dostopanje do vseh aplikacij (Kupec, 2017). Uporaba dovolj zahtevnih gesel je eden izmed temeljnih ukrepov, ki ga lahko kot posamezniki v podjetju zlahka uresničimo. Strokovnjaki priporočajo, da gesla vsebujejo tako velike kot male črke, številke, še bolje v pomešanem vrstnem redu. Lahka gesla kot so ime,

priimek, zaporedne številke (kot na primer 1234), kibernetskim napadalcem namreč omogočijo hiter in lahek dostop do vpisnih podatkov posameznika (Consumer reports, 2011). Vodstva podjetij bi se morala potruditi, da v podjetju vlada politika zdravih, močnih gesel. Dober antivirusni program in previdnost pri obiskovanju spletnih strani nista v pomoč, če so gesla v programu elektronske pošte šibka in omogočajo hiter vdor v sistem in do skrivnosti podjetja. Ko se na spletnih straneh ustvarja nov uporabnik, je ob polju »geslo« po navadi merilec, ki oceni moč vpisanega gesla. Vendar se ni vedno najbolje zanašati na te merilce, saj lahko tudi amaterski kibernetski kriminalci v nekaj sekundah ali minutah razbijejo tako imenovana močna gesla. Težava je v tem, da ti merilci uporabljajo nezanesljivo meritev za merjenje moči gesel in ne upoštevajo tehnik za razbijanje gesel v resničnem svetu. Klasični merilec moči gesel predpostavlja, da bodo napadalci vedno uporabili tehniko, ki bo preizkusila vse možne kombinacije znakov in poiskala ujemanje. Če je na primer število znakov v geslu 10, bi ta tehnika poskusila vsako kombinacijo od 10 A-jev do 10 Z-jev, kar lahko traja zelo dolgo časa. Namesto te tehnike večina napadalcev uporablja seznam z najpogostejšimi besedami in kombinacijami, uporabljenimi za gesla, kar je hitrejša in bolj uspešna tehnika, ki pa je merilci za merjenje moči gesel ne upoštevajo. Zato je priporočljivo, da so gesla dolga najmanj 11 znakov, ne tvorijo vzorca in vključujejo velike in male začetnice ter številke. Lahko se ustvari edinstveno geslo za vsak ustvarjen račun z upraviteljem gesel ali eno glavno geslo, ki odklene vsa ostala gesla (Hackett, 2013).

1.6.2 Izobraževanje zaposlenih

Zaposleni so običajno razlog za večino kršitev zaupnih podatkov. V svetu kibernetske varnosti je podjetje samo tako močno, kolikor je močan najšibkejši člen, kar je po navadi zaposleni, ki nenamerno odpre zlonamerno ali sumljivo priponko elektronskega sporočila (Thompson, 2016). Statistično gledano je 60 % napadov na informacijske sisteme posledica takega notranjega dejanja. 61 % zaposlenih z dostopom do računalnikov podjetja naj bi uporabljalo ista prijavna gesla na spletnih straneh za podjetje, platformah za podjetje, informacijskem sistemu za podjetje in na svojih družbenih omrežjih, kot so na primer Facebook, Twitter in Linkedin, kar hekerjem omogoča lažji vdor in identifikacijo gesel podjetja (Marquette, 2015). Poleg tega številni zaposleni v podjetju uporabljajo javne wi-fi signale pri elektronskem prenosu informacij, ne zavedajo pa se tveganja, da lahko javne spletne povezave nadzirajo tretje osebe. Zato je za zagotovitev zaupnosti podatkov za številne zaposlene potrebno ustrezno usposabljanje in nadaljnje izobraževanje o ustrezni zaščiti osebnih identifikacijskih podatkov, kar vključuje najmanj uvedbo kompleksne politike gesel. Dejansko bi morala podjetja v večini primerov razmisliti o oblikovanju širše politike socialnih medijev, ki bi veljala za vse zaposlene, da bi se izognili namernemu ali nenamernemu razkrivanju občutljivih podatkov (Thompson, 2016).

Veliko zaposlenih se ne zaveda, da lahko z odpiranjem neznanih priponk v elektronskih sporočilih ogrozijo celotno podjetje (Suhadolnik, 2017). Ker je povezanost s svetovnim spletom vse bolj prisotna, se bo število vdorov in napadov še povečevalo. Obvladovanje tega

tveganja bo predstavljalo vedno večji pritisk na vire, tako tehnološke kot človeške. Pri preprečevanju napadov, nadzoru in spremljanju nam lahko do neke mere pomaga tudi tehnologija, lahko pa storimo še več. S pomočjo tehnologije lahko omejimo primere nenamernih varnostnih kršitev, prav tako pa lahko izkoristimo sposobnosti zaposlenih, da prevzamejo aktivnejšo vlogo pri preprečevanju zlonamernih napadov (Ashenden, 2016). Zato je drugi pomemben ukrep za zagotavljanje kibernetske varnosti izobraževanje in obveščanje zaposlenih o informacijski varnosti v podjetju (Perko, 2017). Kibernetska varnost ni odgovornost le vodstva podjetja in oddelka za informacijsko tehnologijo, ampak je odgovornost vseh zaposlenih v podjetju. Zaposleni so lahko največja prednost podjetja, lahko pa so tudi največje potencialno tveganje (Ashford, 2017). Napadi postajajo vse bolj izpopolnjeni, vendar se večina kršitev zgodi prav zaradi človeške napake. Zato strokovnjaki predlagajo zgodnje in pogosto usposabljanje zaposlenih o grožnjah, ki pretijo podjetjem zaradi vključenosti v kibernetski prostor (Finkle, 2017). Še tako napredni varnostni sistemi namreč ne pomagajo, če nekdo od zaposlenih klikne tja, kamor ne bi smel (Perko, 2017). Kako se zaposleni odločajo in odzivajo v ključnih trenutkih, je bistvenega pomena za krepitev odpornosti podjetja proti kibernetskim napadom. Če zaposleni v ključnih trenutkih ne vedo, kako se odzvati, je bolj verjetno, da bodo izbrali slabšo možnost (Ashford, 2017). Nekateri strokovnjaki predlagajo izvajanje izobraževanja in usposabljanja vsaj enkrat letno (Werner, 2017).

V podjetju je treba natančno določiti, do katerih podatkov imajo zaposleni dostop, saj to lahko odločilno zmanjša varnostno tveganje in je na splošno dobra praksa. Zaposlene pa je treba tudi izobraziti, kako opravljati naloge na varen, zakonit in strokoven način (Ramsay, 2015). Mnoge organizacije namreč prevelikemu številu zaposlenih omogočajo celovit dostop do sistemov, zanemarjajo pa, da bi morali zaposlenim posodabljati dostop do informacij, ko se spremeni njihova vloga v podjetju ali ko podjetje zapustijo. Vse to pa povečuje tveganje nepooblaščenega dostopa, kar vodi do izrabe podatkov (Forrester Consulting, 2017).

Prvi korak pri spreminjanju organizacijskega vedenja je določitev specifičnega vedenja, ki ga želimo spremeniti. Z varnostnega vidika je to lahko držanje ograje, ko gremo po stopnicah. To je na primer zelo specifična vedenjska zahteva. Enakovredno vedenje z informacijskega varnostnega vidika je lahko na primer zaklepanje zaslona računalnika, ko se oddaljimo od mize, ali pa izogibanje uporabi ključev USB (lahko tudi fizično preprečenje vrat za USB). Na žalost pa je veliko vedenj težko opredeliti na tako specifičen način, zato zaposleni težje razumejo, kaj točno morajo spremeniti (Ashenden, 2016). Na primer, v podjetju bi bilo dobro vzpostaviti varnostno vedenje, da zaposleni ne bi odpirali phishing elektronskih sporočil. Vendar je težko opredeliti specifično vedenje, ki bo zaposlenim preprečilo, da bi postali žrtve phishing napadov. Če je očitno, da je elektronsko sporočilo zlonamerno, ga zaposleni seveda ne bodo odprl, zato spretni napadalci phishing sporočila oblikujejo kot običajna elektronska sporočila. Če zaposleni sledijo navodilu, da sumljivih sporočil ali sporočil neznanega pošiljatelja ne odpirajo, tvegajo škodo podjetju, saj lahko

izbrišejo tudi nekatera pomembna elektronska sporočila. Zaposleni bodo popolnoma upravičeno želeli vedeti, katera merila je treba upoštevati pri presoji o avtentičnosti, pristnosti in verodostojnosti elektronskega sporočila. Pomembno merilo je tudi čas, ki ga zaposleni porabi za odločitev o tem, ali sporočilo odpreti ali ne in pričakovanja podjetja o času, potrebnem za to odločitev (Ashenden, 2016).

Kako torej zmanjšati tveganje, da bi zaposleni odprl phishing elektronsko sporočilo? Eden od trenutno najbolj priljubljenih načinov je uporaba programskega orodja, ki pošlje phishing elektronska sporočila zaposlenim, vendar pod nadzorom podjetja. To preveri, ali obstaja verjetnost, da bi zaposleni postali žrtve napada. To je dobra in dokaj enostavno izvedljiva preverba, kljub temu pa ima določene pomembne pomanjkljivosti. Če zaposleni postane žrtev nadzorovanega phishing napada in testa ne opravi uspešno (in ga posledično celo oštejejo ali ga doleti dodatno sankcijsko usposabljanje), ga kasneje manj zanima pomoč pri izboljšanju informacijske varnosti. Zaposleni morda meni, da ga je podjetje v tej situaciji prelisičilo. Druga nevarnost pa je, da zaposleni začnejo kazati znake »naučene nemoči«. To je psihološko stanje, ko posameznik meni, da se ni vredno truditi, saj karkoli bi naredil, bi naredil narobe (Ashenden, 2016).

Zaposleni in vsi ostali pogodbeni delavci v podjetju morajo razumeti, da morajo kakršno koli izgubo ali krajo informacij takoj sporočiti ustreznemu nadrejenemu. Ker sta informacijska varnost in zakonodaja, ki ureja področje kibernetskih napadov, precej splošni in rigidni, nobena kršitev ne sme biti ignorirana. V primeru izgube občutljivih podatkov (na primer, da je zaposleni založil podatkovni nosilec z varnostno kopijo) to vseeno pomeni kršitev informacijske varnosti in zahteva ustrezno ukrepanje (FCC, 2012).

Tudi uporaba pametnih telefonov predstavlja določeno tveganje, ne le za lastnika pametnega telefona, ampak tudi za podjetje (Imgraben, Engelbrecht & Choo, 2014), saj vse več zaposlenih tudi prek zasebnih telefonov pregleduje službeno elektronsko pošto.

1.6.3 Zavarovanje za kibernetsko tveganje

Podjetja pogosto sklenejo zavarovanje za različna poslovna, naravna in politična tveganja. Vendar pa tradicionalne zavarovalne police nepopolno naslovijo dodatna tveganja, s katerimi se soočajo podjetja, ki so del digitalnega gospodarstva. Rastoča uporaba svetovnega spleta je tako ustvarila potrebo po novih zavarovalniških produktih. Zavarovalniška podjetja so predstavila nove zavarovalne možnosti, ki pokrivajo različne vidike kibernetskega tveganja. V procesu oblikovanja teh novih polic so se zavarovalnice lotile vprašanj, kot so cena, problem nepravilne izbire in problem moralnega tveganja. Čeprav so vsa ta vprašanja skupna vsem oblikam zavarovanj, kibernetsko tveganje ustvari drugačne skrbi (Gordon, Loeb & Sohail, 2003).

Obvladovanje kibernetskega tveganja vključuje dobro obvladovanje vseh tveganj in upoštevanje specializiranega zavarovanja za ublažitev finančnega vpliva, če se zgodi varnostni incident (Marsh, 2014). Podjetjem je težko nameniti denar za nekaj, za kar upajo, da ne bodo nikoli potrebovali. Ko pride do upravljanja s kibernetskim tveganjem, ki lahko podjetje uniči v nekaj dneh, se nekateri odločijo za varnejšo pot in izberejo zavarovanje za kibernetsko tveganje (Briody, 2007).

Uporaba spleta je pomembno povečala ranljivost organizacij za informacijsko krajo, vandalizem in napad za zavrnitev storitve in tako pripeljala težave informacijske varnosti v ospredje. To težavo je osvetlila raziskava iz leta 2002 (CSI/FBI), ki je ugotovila, da je 90 % vseh anketirancev v predhodnem letu že zaznalo vdor v računalniško varnost in da je povprečna ocenjena izguba (za podjetja, ki so podala ocenjeno vrednost) več kot 2 milijona ameriških dolarjev na organizacijo. Še več, 74 % anketirancev je povedalo, da je prav spletna povezava vstopna točka za pogoste napade (Gordon, Loeb & Sohail, 2003).

Podjetja so bila dolgo obremenjena z varovanjem lastninskih informacij, ohranjanjem integritete podatkovnih baz in zagotavljanjem pravočasnih dostopov do informacij pooblaščenih uporabnikov. Povečana ranljivost in precejšnje ekonomske izgube zaradi napadov preko spleta so povzročile, da mnogi izvršni direktorji iščejo dodatne možnosti za upravljanje informacijskega kibernetskega tveganja. Eno od orodij je zavarovanje za kibernetsko tveganje. To je zavarovanje, ki pokriva izgube, povezane z uporabo spleta v informacijski varnosti. Z zavarovanjem izgub zaradi vdorov v informacijsko varnost bi se podjetje lahko izognilo potencialnim izgubam zaradi kibernetskega kriminala (Gordon, Loeb & Sohail, 2003).

Zavarovanje je ključni mehanizem za prevalitev tveganja in podjetju omogoča finančno varnost v primeru izgube podatkov. Najprej je treba določiti potencialne izgube in vpliv na podjetje v primeru incidenta, kar podjetju omogoča, da izbere za njihove specifične potrebe primerno zavarovalno polico. Zavarovalna komponenta dopolni tehnične rešitve in procese (Siegel, Sagalow & Serritella, 2002).

Čeprav je poslovno tveganje povezanosti na splet podobno ostalim tradicionalnim poslovnim tveganjem, se od njega razlikuje na področju lokacije, stopnje in vidnosti. Storilec informacijske kraje ali škode lastnine je v času spletnega napada lahko na tisoče kilometrov oddaljen od lokacije podjetja. Virus, ki poškoduje podatke in programsko opremo podjetja, se lahko razširi tudi na druga podjetja in prvotnemu nakoplje odgovornost (Gordon, Loeb & Sohail, 2003).

Cena zavarovalnih produktov tradicionalno temelji na aktuarskih tabelah, sestavljenih iz številnih preteklih podatkov. Ker pa je svetovni splet relativno nov, poglobljena zgodovina spletnega kriminala in povezanih izgub ne obstaja. Baza vdorov v informacijsko varnost ne

obsega dovolj dolgega časovnega obdobja in ni popolna, saj podjetja pogosto ne razkrijejo podrobnosti kibernetskega napada (Gordon, Loeb & Sohail, 2003; Briody, 2007).

1.6.4 Ostali ukrepi

Ko je proces zagotavljanja kibernetske varnosti vzpostavljen in v uporabi, je treba oceniti skladnost ravnanja podjetja z zastavljenimi cilji varnostne politike in uspešnost izvajanja ukrepov za zagotovitev kibernetske varnosti. Vsaj enkrat letno je priporočljivo najeti zunanje, neodvisne strokovnjake, da ocenijo kibernetsko varnost podjetja. Proces opazovanja in kontrole se imenuje revizija kibernetske varnosti, namenjena pa je ocenjevanju in popravljanju obstoječih varnostnih napak. Strokovnjaki testirajo obstoječo informacijsko varnost podjetja, navadno s simulacijo vdora, in ugotovijo neskladnosti. Testiranje ne zajema le informacijske varnosti, ampak tudi fizično varnost podatkov. Proces revizije se dopolnjuje s procesom načrtovanja in kontrole, ki je povezana z razporejanjem virov za kibernetsko varnost. Revizija pomaga odkriti pomanjkljivosti obstoječega načrta (varnostne politike), pomaga pa tudi izboljšati načrt kibernetske varnosti za naslednje obdobje. Obsežnost revizije je odvisna od poslovanja podjetja, varnostnih tveganj in velikosti podjetja. Podjetje na koncu dobi poročilo, kjer so zapisane ugotovitve in neskladnosti, ki so jih ugotovili zunanji strokovnjaki. Neskladnosti so rangirane glede na resnost in z njo povezana tveganja. Če je neskladnost pomembna, jo mora podjetje takoj odpraviti, za srednje in manj pomembne neskladnosti pa ima več časa. Ko podjetje odpravi neskladnosti, se varnostni pregled ponovi in ponovno izda poročilo o stanju. Ker je podjetje v času med dvema varnostnima pregledoma verjetno začelo uporabljati nove aplikacije, programske rešitve in procese, je zelo verjetno, da se bodo ob varnostnem pregledu ponovno pokazale določene neskladnosti. V splošnem bi morala revizija vključevati vsaj fizično varnost in kontrolo dostopnosti, pregled administrativnih procesov in kontrol, ovrednotenje učinkovitosti sistema za odkrivanje vdorov v informacijski sistem podjetja ter ocenjevanje zaposlenih, ki skrbijo za kibernetsko varnost v podjetju (vključno z vodstvom). Oceniti je treba tudi ekonomske koristi, ki so posledica aktivnosti informacijske varnosti, v odvisnosti s stroški, ki so potrebni za izvedbo teh aktivnosti (Gordon & Loeb, 2006).

Podjetje lahko aktivnosti za doseganje kibernetske varnosti v celoti ali le do neke mere zaupa tudi zunanjim izvajalcem, ki poskrbijo, da je podjetje zaščiteno pred kibernetskimi napadi. Z oddajanjem storitev zunanjim izvajalcem (outsourcing) lahko podjetje izkoristi njihovo strokovnost in tako zmanjša začetno investicijo, ki je potrebna za vzpostavitev informacijskega sistema, programske opreme in zaposlenih na področju za informacijsko tehnologijo ter oddelku za obvladovanje tveganj. Zunanji izvajalci bodo za svoje storitve seveda zaračunali določeno provizijo, zato se pojavi vprašanje, ali je te aktivnosti ceneje oddajati zunanjim izvajalcem ali jih obdržati v podjetju (Gordon & Loeb, 2006).

Podjetje se lahko odloči, da bo zunanjim izvajalcem zaupalo le nekatere ukrepe za zagotavljanje kibernetske varnosti, na primer le zagotavljanje ustrezne informacijske in

programske tehnologije ter podporo in uporabo oblačnih storitev za poslovanje, ne pa tudi izobraževanja zaposlenih – ali obratno.

Za kibernetski prostor je značilna odsotnost meja, dinamičnost in anonimnost ter ustvarjanje priložnosti za razvoj znanja, ki temelji na informacijah o družbenih tveganjih. Če družba temelji na informacijah, bo postala bolj ranljiva, varnost kibernetskega prostora pa mora postati zadeva vseh deležnikov, zlasti na institucionalni ravni, kjer je pozornost treba usmeriti k razvoju varnostne politike in njenega izvajanja. Čeprav se informacijska tehnologija razvija, njena prisotnost pa narašča, družba postaja odvisna od njenega področja uporabe. Kibernetska varnost postopno pada v kategorijo področij nacionalnega interesa. Zagotovitev kibernetske varnosti temelji na sodelovanju na nacionalni in mednarodni ravni. Za zaščito kibernetskega prostora je treba uskladiti ukrepe nacionalnih smernic in ukrepe na mednarodni ravni v obliki sodelovanja. Na nacionalni ravni je treba uvesti minimalne standarde infrastrukture informacijske varnosti, da bi utemeljili učinkovitost pristopov za zaščito pred kibernetskimi napadi in omejili tveganje za incidente z morebitnim znatnim vplivom (Nastasiu, 2016). Z namenom zagotavljanja informacijske varnosti na področju varstva osebnih podatkov posameznikov rezidentov držav članic Evropske unije je Evropska unija sprejela Splošno uredbo za varstvo osebnih podatkov (GDPR), ki je pričela veljati 25. 5. 2018. Uredba zaostruje pogoje za kakršno koli obdelavo osebnih podatkov, vključno z golo hrambo podatkov, tako za upravljalce (lastnike podatkov) kot tudi obdelovalce, h katerim sodijo tudi računovodski servisi. Največja novost uredbe je, da morajo obdelovalci podatkov zabeležiti vsako posredovanje osebnih podatkov, tudi če gre za državne ustanove. Obdelovalci podatkov, ki se ukvarjajo z obsežnim, rednim in sistematičnim obdelovanjem osebnih podatkov, morajo imenovati pooblaščeno osebo za varstvo podatkov, ki mora biti neodvisna in ji morajo biti zagotovljena sredstva za nemoteno delo, oseba pa je lahko notranji ali najeti zunanji strokovnjak za varstvo osebnih podatkov. Računovodski servisi morajo imeti popoln pregled nad osebnimi podatki, ki jih obdelujejo ali le hranijo, in sicer popis podatkov, kje se nahajajo, kdo ima dostop, od kje jih dobi, kdo jih posreduje, koliko časa jih hranijo, itd. Če računovodski servis nima pravne podlage za hranjenje oz. obdelovanje podatkov, podatkov ne sme imeti. Pravno podlago predstavlja zakon, pogodba o sodelovanju ali privolitev stranke. Mnenja o tem, ali je samoumevno, da računovodski servisi podatke obdelujejo obsežno, redno in sistematično, se razlikujejo. Res pa je, da je to odvisno tudi od količine podatkov oz. števila strank računovodskega servisa. Za vse kršitve uredbe je zagrožena kazen v višini 4 % letnih prihodkov podjetja, najvišja možna kazen pa je 20.000.000 €. Uredba tudi zahteva, da se vse nepooblaščene dostope do osebnih podatkov oz. kršitve osebnih podatkov, kar vključuje tudi kibernetske napade, takoj sporoči oškodovani stranki in v 72 urah tudi državnim organom. S tem želijo vzpostaviti evidenco kibernetskih napadov, ki je trenutno zelo okrnjena, saj večina podjetij kršitev ne želi razkriti, ker bi to lahko močno zmanjšalo njihov ugled in povzročilo težave v nadaljnjem poslovanju. Računovodski servisi morajo zato dobro premisliti, ali njihovo podjetje potrebuje pooblaščeno osebo za varstvo podatkov in v nadaljnje zagotoviti, da bodo za potrebe

izpolnitve pogodbenih obveznosti obdelani osebni podatki na varnem, njihova obdelava pa v skladu z uredbo.

Načrt – 79 % malih podjetij nima vzpostavljenega načrta za primer kibernetskega napada (Finkle, 2017). Vsako podjetje bi moralo načrtovati nepričakovane dogodke, kar vključuje tudi izgubo ali krajo podatkov podjetja. Izguba ali kraja podatkov škodi poslovanju, znamki in strankam podjetja, podjetje pa lahko izpostavi tudi državnim organom, ki so pristojni za področje zaščite zasebnih podatkov. Izguba ali kraja podatkov lahko podjetje izpostavi tudi pravnemu tveganju. Zato je ključno razumeti, katera varnostna zakonodaja vpliva na poslovanje podjetja in kako se pripraviti nanjo. To bi morala biti osnova načrta za primer kibernetskega napada, ki bi omogočila lažji, hitrejši in bolj koordiniran odziv podjetja na napad (FCC, 2012).

Kaj storiti, ko napadalci vseeno prodrejo skozi obrambo podjetja? (Finkle, 2017)

1. Priprava – Investitorje in stranke je treba obvestiti o problemu in povedati, kateri koraki bodo potrebni, da se podjetje ponovno postavi na noge. Podjetje naj ima pripravljen priročnik, ki ga uporabi ob morebitnem napadu.
2. Najem zunanjega strokovnjaka – Tudi če v podjetju je oddelek za informacijske tehnologije, je koristno imeti zunanji pogled na nastalo težavo. Podjetje mora biti prepričano, da dobi objektivno oceno škode s strani tretje osebe, in ne nekoga, ki poskuša prikriti svoje napake.
3. Ukrepati je treba čim hitreje. Prvih 48 ur po napadu je ključnega pomena za določitev, kateri računalniki in omrežja so bila napadena, kako so bili izkoriščeni in kateri podatki so ogroženi.
4. Pred plačilom odkupnine je treba dobro premisliti. Večina strokovnjakov odsvetuje plačilo odkupnine, razen če je to zadnja in edina možnost za podjetje. Napadalci namreč računajo prav na psihološki učinek na žrtve, da brez odkupnine ne morejo rešiti situacije. Ključe za dekodiranje podatkov za nekatere starejše prevare je mogoče brezplačno najti na spletu, prav tako pa plačilo odkupnine pogosto ne zagotavlja vrnitve ukradenih in zakodiranih podatkov. Če se podjetje odloči, da bo v rešitev podjetja vložilo nekaj denarja, je bolj smotrno, da najame strokovnjaka.

1.7 Vpliv kibernetskega tveganja na računovodstvo

Računovodska podjetja delujejo v konkurenčnem in hitro spreminjajočem okolju (Stanciu & Bran, 2015). Še nekaj let nazaj je veljalo, da je kibernetska odgovornost eksotična in redka težava v odgovornosti računovodskega poklica (Russel, 2015). Podjetja spremljajo novi poslovni modeli, od katerih jih veliko temelji na informacijski tehnologiji. Podjetja vlagajo sredstva v IT rešitve za izboljšanje upravljanja in nadzora poslovnih procesov. IT okolje je v podjetjih postalo zapleteno in dinamično. Računovodska stroka se sooča z visokimi zahtevami na IT področju, ki izhajajo iz notranjih sprememb in razvoja znotraj poklica. IT

okolje, v katerem podjetja delujejo in vodijo svoje poslovanje ter računovodje opravljajo svoje delo, ustvarja nove zahteve v zvezi z IT spretnostmi, veščinami in strokovnim znanjem, ki jih potrebujejo računovodje in od katerih je del povezan z informacijsko tehnologijo. Od finančnih in računovodskih strokovnjakov se zahteva, da izboljšajo in razvijejo svoje informacijske spretnosti in ostanejo usklajeni z IT dinamiko v podjetju (Stanciu & Bran, 2015).

Mednarodna zveza računovodij (IFAC) v svoji vlogi vodstva za računovodski poklic po vsem svetu poudarja pomen informacijske spretnosti in strokovnosti za poklic računovodje. Pomemben izobraževalni standard, ki ga izdaja IFAC (2003), IEG-11 – Mednarodni izobraževalni priročnik o IT in računovodskem programu, poudarja nujnost informacijske tehnologije za računovodski poklic. V svojih dokumentih IFAC imenuje pomembne akterje za načrtovanje, izvajanje ali ocenjevanje izobraževalnih programov za računovodje, kot so univerze, zaposleni in ostali deležniki. V svojem poročilu za leto 2013 je Združenje zapriseženih računovodij (ACCA) poudarilo potrebo, da finančni in računovodski strokovnjaki ostanejo odprti za spremembe, ki nastanejo z uporabo nove informacijske tehnologije in trajno izboljšajo svoje znanje ter spretnosti, da bi razumeli in znali uporabljati IT rešitve ter prilagodili svoje delo v IT okolju (Stanciu & Bran, 2015).

V vsakem podjetju, tako malem kot multinacionalnem, finančni in računovodski strokovnjaki opravljajo svoje delo z uporabo programskih aplikacij. Danes obstaja zelo raznovrstna računovodska programska oprema in infrastruktura, namenjena podpori avtomatske obdelave računovodskih podatkov, ki se začnejo s samostojnimi aplikacijami monopostov in končajo s kompleksno integrirano programsko opremo, ki temelji na tehnologiji odjemalec – strežnik. Mala podjetja, ki razumejo pomembnost informacij za postopek odločanja in so omejena na informacijskotehnološke in finančne vire, analizirajo priložnost rešitev v oblaku (Stanciu & Bran, 2015). Anketa, ki jo je leta 2013 izvedla skupina Aberdeen, je pokazala, da 80 % vprašanih uporablja programsko opremo v javnem oblaku, 18 % aplikacij pa je bilo finančno računovodskih (Aberdeen, 2013). V informacijskem okolju se računovodsko delo spreminja, pretok informacij in dokumentov (veliko dokumentov, ki jih ustvarjajo informacijski sistemi) je v veliki meri zagotovljen in poteka pod nadzorom programske opreme. Celoten računovodski proces in njegov nadzor sta prilagojena novim zahtevam in omejitvam, ki jih določa programska oprema. Tudi če se kompleksnost programske opreme stalno povečuje, finančni direktorji še vedno niso vedno zadovoljni z rezultati oziroma izpisi programske opreme. Menijo, da aplikacij in programov ni vedno mogoče enostavno prilagoditi spremembam poslovnih modelov (značilnost sedanjosti je hitra sprememba sprejetih poslovnih modelov) in zato ne zagotavljajo vedno poštene in ustrezne slike podjetja, da bi olajšali postopek odločanja. Finančni direktorji se zavedajo tveganj, povezanih z avtomatsko obdelavo računovodskih podatkov in hrambo. Poročilo za tretje četrtletje leta 2014, ki ga je izdalo podjetje Deloitte, razkriva, da finančni direktorji na kibernetsko varnost gledajo kot na visoko prednost, vendar so zaskrbljeni zaradi izvedbe načrtov varovanja informacij (Stanciu & Bran, 2015).

Ocenjevanje kibernetskega tveganja je postalo ena glavnih nalog za računovodje in računovodska podjetja. Prvi korak k varovanju pred tveganjem kibernetskega napada je identificiranje in lociranje zaupnih podatkov v podjetju, kar je nujno za ocenjevanje vsakega kibernetskega tveganja in posledičnega načrta. Nenehno spremljanje teh informacij in točk dostopa do podatkov je prav tako pomembno za nadaljnji uspeh načrta za kibernetsko tveganje (Thompson, 2016).

Medtem ko so tveganja za kibernetski napad očitno precejšnja, se pomisleki glede tega tveganja povečajo z dejstvom, da bi ena sama kršitev zaupnosti podatkov lahko škodila ugledu računovodskega servisa, kar bi bilo nepopravljivo. V zelo konkurenčnem okolju se računovodski servisi pogosto obotavljajo glede javnega priznanja napada na informacijski sistem podjetja zaradi strahu pred oškodovanjem ugleda. Kljub temu morajo računovodska podjetja ustvariti nek mehanizem za izmenjavo ključnih varnostnih informacij, kar bi bilo v korist celotni računovodski panogi. Ta vrsta proaktivnega vedenja bi pokazala, da ne gre za vprašanje, »če« bo računovodsko podjetje doživelo kibernetski napad, temveč »kdaj«. Računovodje in računovodska podjetja se morajo zavedati etičnih zahtev sodobne digitalne dobe ter varnosti podatkov in oblikovati načrt za zadovoljitev ne le potreb svojih strank, temveč tudi za vse večje tehnološke potrebe računovodskega poklica. Računovodje morajo priznati, da so informacije njihovega podjetja ranljive za kibernetski napad, da bi zaščitili svoje podjetje, svoje stranke in njihove podatke, da ne bi padli v napačne roke in da bi v prihodnosti zagotovili informacijsko varnost proti nastajajočim grožnjam zaupnosti podatkov strank (Thompson, 2016). Prav zato bodo morali računovodski servisi resno pristopiti k reševanju problematike nepooblaščenega dostopanja do osebnih podatkov, ki ga zakonsko ureja GDPR.

Mala in srednje velika podjetja (MSP), kar večina slovenskih računovodskih servisov je, so lahko uresničitev sanj kibernetskih napadalcev. Ta trditev temelji na dejstvu, da malim in srednje velikim podjetjem običajno primanjkuje sredstev za varnostne sisteme, ki temeljijo na obrambi in vključujejo več plasti varnostnih kontrol (Strohmeyer, 2013 v Ramsay 2015). Mala in srednje velika podjetja se zaradi svoje majhnosti, pomanjkanja obsežne tržne izpostavljenosti in napačne ugotovitve, da nimajo vrednih, za napadalce zanimivih in koristnih informacij, običajno ne vidijo kot potencialne tarče za kibernetske napade. Poleg tega menijo, da nimajo vedno dovolj sredstev, da bi se proti napadalcem lahko borila. Ta način razmišljanja je daleč od realnosti, saj imajo mala in srednje velika podjetja dragocene informacije za spletne kriminalce, kot so na primer evidenca zaposlenih in kupcev, informacije o bančnih računih, dostop do financ itd. Kljub obsežnim podatkom, ki jih morajo MSP varovati, pomanjkanje virov in informacij pogosto prispevata k slabo opremljenemu stanju MSP na področju kibernetske varnosti. Kibernetski napadalci so prepoznali to pomanjkanje zaščite, zaradi česar so MSP privlačne tarče. Mnogi lastniki malih podjetij pogosto ne naredijo dovolj, da bi svoje organizacije zaščitili pred napredno zlonamerno programsko opremo in drugimi kibernetskimi napadi zaradi pomanjkanja informacij. To

pomanjkanje razumevanja kibernetskega tveganja pogosto izhaja iz osredotočanja na netočna prepričanja in zastarelo znanje. Poleg tega da imajo lažen občutek varnosti, MSP nimajo vedenja o tem, kje so ranljivosti in grožnje v njihovih podjetjih. Ne da bi vedeli, katere informacije in sredstva so najpomembnejša za organizacijo in njene stranke, prodajalce, zaposlene in druge uporabnike, je težko vedeti, na katerih področjih je najbolje investirati v kibernetsko varnost. To pomanjkanje informacij MSP vodi v dodelitev nezadostnih virov za kibernetsko varnost, še zlasti, ker nimajo sredstev za zaposlitev rednega osebja in analitikov za kibernetsko varnost ali sklenitev pogodbe z dragimi ponudniki teh storitev (Ramsay, 2015).

2 RAZISKAVA O OBVLADOVANJU KIBERNETSKEGA TVEGANJA V SLOVENSKIH RAČUNOVODSKIH SERVISIH

2.1 Opredelitev raziskovalnih hipotez

Da bi proučila zavedanje o kibernetskem tveganju in načine varovanja proti njemu med slovenskimi računovodskimi servisi, sem med njimi izvedla raziskavo. Opravljena je bila z metodo zbiranja primarnih podatkov, in sicer z anketnim vprašalnikom in intervjujem. Vprašalnik je bil sestavljen iz zaprtih in odprtih vprašanj, vabilo za sodelovanje v spletni anketi, ki je bila izvedena s pomočjo spletnega orodja 1KA, pa je bilo prek elektronske pošte poslano kontaktnim osebam v slovenskih računovodskih servisih. S pomočjo spletne baze BIZI sem poiskala podjetja s SKD 69.200 – Računovodske, knjigovodske in revizijske dejavnosti, davčno svetovanje.

Raziskovalno vprašanje 1: Kako računovodski servisi v Sloveniji ocenjujejo svojo izpostavljenost kibernetskemu tveganju?

Werner (2017) pravi, da so tudi računovodski servisi ena od skupin podjetij, ki meni, da se jim zaradi njihove majhnosti kibernetski napad ne more pripetiti. Zato želim preveriti, kakšno je mnenje slovenskih računovodskih servisov glede verjetnosti za napad na njihovo podjetje, oziroma kako visoko ocenjujejo kibernetsko tveganje glede na verjetnost kibernetskega napada in njegovih posledic.

Raziskovalno vprašanje 2: Ali računovodski servisi v Sloveniji izvajajo ukrepe za zagotovitev kibernetske varnosti sebe in svojih strank?

Glede na to, da je kibernetsko tveganje že nekaj časa prisotno tudi v slovenskem prostoru, naj bi se večina podjetij tega tudi zavedala. Vendar to še ne pomeni, da potrebne ukrepe za upravljanje s tem tveganjem tudi izvajajo. Ukrepi za upravljanje kibernetskega tveganja so na primer ustrezna tehnična in informacijska tehnologija ter varnostni sistemi, varnostne

kopije, izobraževanje in usposabljanje zaposlenih, obveščanje zaposlenih o informacijski varnosti v podjetju, zavarovanje za kibernetsko tveganje idr. Z raziskavo želim ugotoviti, kolikšen delež slovenskih računovodskih servisov izvaja vsaj enega od prej naštetih ukrepov, saj lahko le tako pokažejo, da se kibernetskega tveganja zavedajo in z njim upravljajo.

Raziskovalno vprašanje 3: Kolikšen delež računovodskih servisov v Sloveniji izobražuje svoje zaposlene o pomenu kibernetske varnosti in morebitnih posledicah, če ta ni zagotovljena, in na kakšen način?

61 % vdorov v informacijske sisteme naj bi bila posledica dejanj zaposlenih (Marquette, 2015), lahko pa so tudi posledica neizobraženosti zaposlenih glede kibernetske varnosti. Zato je eden od ključnih ukrepov za zagotavljanje kibernetske varnosti izobraževanje in usposabljanje zaposlenih glede politik informacijske varnosti v podjetju. Kot je bilo že omenjeno, še tako napredni varnostni sistemi ne pomagajo, če gre za napako enega od zaposlenih. Zaposlene je treba naučiti, kje vse se lahko grožnje za vdor v informacijski sistem podjetja skrivajo (v priponkah elektronskih sporočil, spletnih povezavah, ki so pripete k elektronskim sporočilom, ki od nas zahtevajo geslo, obiskovanje sumljivih spletnih strani itd.). Možen je tudi vdor v elektronsko pošto strank, tako da mora zaposleni nenavadne zahteve stranke, na primer nakazilo visokega zneska na tujo banko, dodatno preveriti pri stranki, da se prepriča, ali je to res izvedeno. To je le nekaj primerov, na kaj morajo zaposleni biti še posebno pozorni. Zaposleni se morajo naučiti prepoznati te pasti in biti usposobljeni za ukrepanje v primeru zlonamerne elektronske pošte ali drugega načina poskusa kibernetskega napada.

Raziskovalno vprašanje 4: Kako pogosto računovodski servisi v Sloveniji izvajajo izobraževanja in usposabljanja za zaposlene?

Strokovnjaki priporočajo izvajanje izobraževanja in usposabljanja o kibernetski (ne)varnosti za zaposlene vsaj enkrat letno (Werner, 2017). Stanje na področju informacijske tehnologije in spletnega poslovanja se namreč neprestano in zelo hitro spreminja. Treba je biti dobro obveščen o novostih za zagotovitev kibernetske varnosti v podjetju. Za izobraževanje zaposlenih je lahko odgovoren IT oddelek v sodelovanju z vodstvom podjetja, podjetje pa lahko najame tudi zunanjega strokovnjaka za informacijsko varnost.

2.2 Raziskovalna metoda

S programom SPSS sem analizirala pridobljene podatke in skušala odgovoriti na zastavljena raziskovalna vprašanja. Šlo je za analizo deskriptivne statistike (frekvence odgovorov, povprečja, mediane).

Opis vzorca

Populacija raziskave so bili računovodski servisi v Sloveniji. Vzorčni okvir (spisek enot) sem pridobila s pomočjo podatkovne baze BIZI. Na dan 2. 1. 2018 je bilo v bazi BIZI s SKD dejavnostjo 69.200 najdenih 4727 enot. Ker je populacija raziskave znana, sem lahko uporabila verjetnostno vzorčenje, zato je bil vzorec raziskave izbran s sistematičnim vzorčenjem, kar pomeni, da je bila prva enota v vzorec izbrana naključno, vse naslednje enote pa s korakom 27. Za izbrane enote sem elektronske naslove pridobila na portalu BIZI, s spletnim brskalnikom ali po telefonu.

V populaciji podjetij z dejavnostjo 69.200 je 52,6 % samostojnih podjetnikov, 45 % družb z omejeno odgovornostjo, 1,1 % družb z neomejeno odgovornostjo, 0,4 % komanditnih družb in 0,9 % podjetij z drugo pravno organizacijsko obliko.

Anketni vprašalniki so bili izbranim 288 podjetjem prek elektronske pošte poslani 9. 4. 2018. Po preteku enega tedna sem podjetja ponovno prosila za sodelovanje. Ker so bili nekateri elektronski naslovi neaktivni in ker je bil odziv slab (izpolnjenih vprašalnikov sem namreč dobila le 24), sem se odločila, da vabila za sodelovanje v raziskavi pošljem še enkrat, tokrat večjemu številu podjetij. Tako sem dobila še 63 izpolnjenih vprašalnikov. Glede na to, da je bila tema anketnega vprašalnika dokaj občutljiva, je bilo pričakovati, da bo delež odgovorov nizek, in sicer je znašal 4,65 %.

Prvi sklop vprašanj anketnega vprašalnika je bil namenjen osnovnim podatkom o podjetjih, ki so se odločila za sodelovanje v raziskavi. Osnovnih vprašanj je bilo pet. V raziskavo so bili vključena tako mala računovodska podjetja kot tudi velika. To je razvidno iz največjih vrednosti, ki so zapisane pri osnovnih podatkih podjetja. Število observacij, ki so odgovorile na vprašalnik, je 87 podjetij. V povprečju podjetje v vzorcu zaposluje 5,74 ljudi, mediana pa znaša dva zaposlena. Podjetje z največ zaposlenimi, ki je sodelovalo v raziskavi, zaposluje 172 ljudi. Povprečno število strank, ki jih imajo podjetja, zajeta v raziskavo, je 78,68 z mediano 30 strank. Največja vrednost pri vprašanju o številu strank je 1500 strank, najnižja pa štiri stranke. Prihodki podjetja se pri računovodskih servisih gibljejo od 500 pa vse do 6 milijonov evrov. Povprečni dohodek podjetja v raziskavi je 216.735 evrov, mediana pa 50.000 evrov. Vrednost sredstev v podjetju se giblje od 0 do 7 milijonov evrov, s povprečjem pri 160.266 evrih in mediano 15.444 evrov. 12,6 % podjetij, zajetih v raziskavo, ima dislocirane enote, preostalih 87,4 % pa ne.

2.3 Predstavitev rezultatov

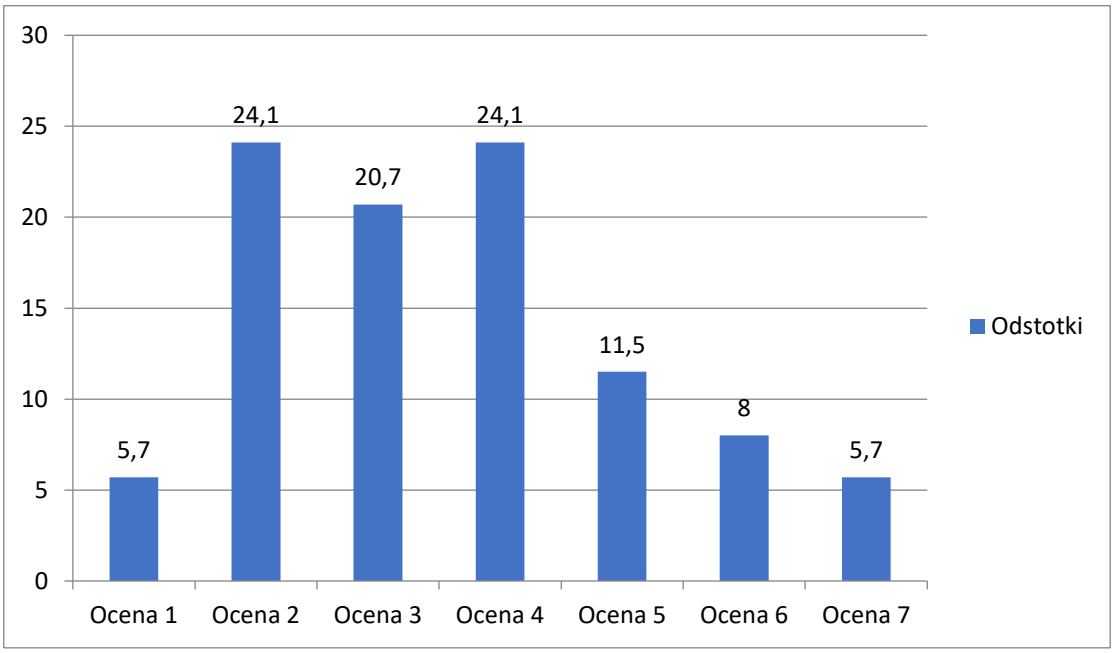
2.3.1 Anketni vprašalnik

Sledilo je 16 vprašanj, ki so se nanašala na obvladovanje kibernetskega tveganja v računovodskih servisih in so odgovorila na zastavljena raziskovalna vprašanja magistrskega

dela. Prvo vprašanje anketnega vprašalnika je odgovorilo na prvo raziskovalno vprašanje tega magistrskega dela.

Prvo vprašanje se je glasilo: Kako verjeten se vam zdi kibernetski napad oziroma vdor v informacijski sistem vašega podjetja? Odgovor so anketiranci podali na podlagi ocene od 1 do 7, kjer je ocena 1 predstavljala neverjeten in ocena 7 zelo verjeten kibernetski napad. Rezultati so predstavljeni na sliki 3.

Slika 3: Verjetnost kibernetskega napada oziroma vdora v informacijski sistem podjetja



Vir: lastno delo.

Kot je razvidno z zgornje slike, večina anketiranih računovodskih servisov še vedno meni, da je verjetnost za kibernetski napad majhna, saj so najpogosteje izbrane ocene 2, 3 in 4. Za skrajni dve oceni, oceno 1 in oceno 7, se je odločil enak odstotek podjetij, to je 5,7 %. To pomeni, da le 5,7 % podjetij meni, da je verjetnost za kibernetski napad zelo visoka. Za oceno 6 se je odločilo 8 % podjetij. Rezultati kažejo, da anketiranci na lestvici od 1 do 7 verjetnost kibernetskega napada za anketirano podjetje ocenjujejo s povprečno oceno 3,59 in z mediano pri oceni 3, pri največji vrednosti 7.

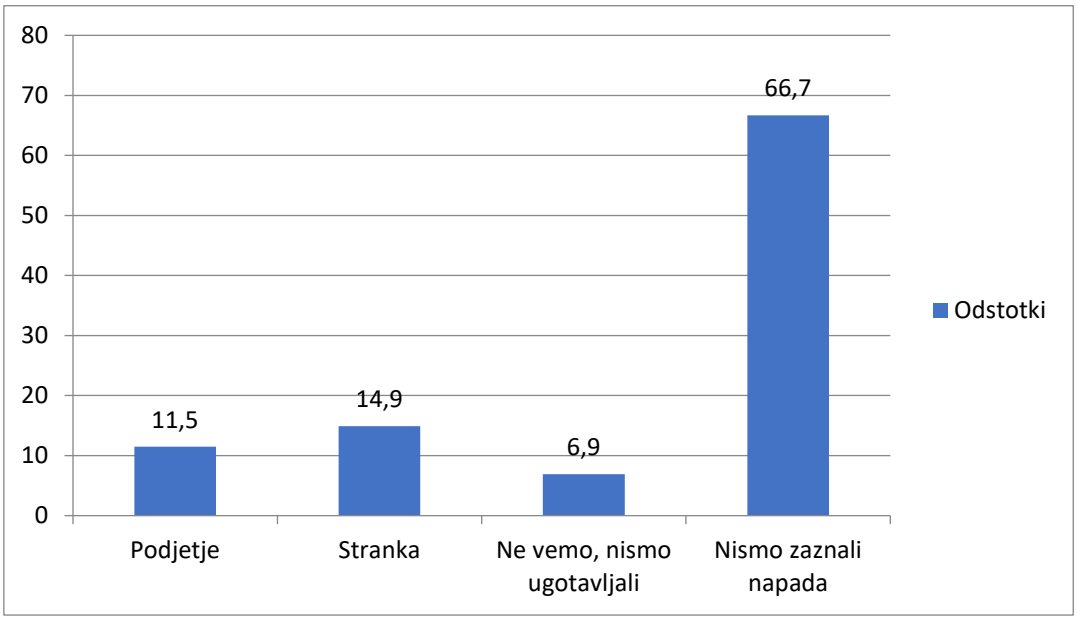
Kot je bilo zapisano v literaturi (Werner, 2017; Ramsay 2015), lahko na podlagi izvedene raziskave potrdim, da tudi v Sloveniji velja, da se majhna in srednje velika podjetja še vedno premalo zavedajo nevarnosti kibernetskih napadov in menijo, da se jim zaradi majhnosti kibernetski napad ne more pripetiti. Velika računovodska podjetja (več strank, zaposlenih, višji prihodki), ki so bila vključena v raziskavo, so za verjetnost kibernetskega napada izbrala višje ocene verjetnosti, kar kaže, da se bolje zavedajo nevarnosti.

Drugo vprašanje: Ali ste v podjetju v zadnjih petih letih že zaznali kibernetski napad, to je vdor v informacijski sistem podjetja?

85,1 % podjetij, vključenih v raziskavo, je odgovorilo, da v zadnjih petih letih ni zaznalo kibernetskega napada, 13 podjetij oziroma 14,9 % pa je kibernetski napad v zadnjih petih letih zaznalo.

Tretje vprašanje se je navezovalo na drugo vprašanje v raziskavi. Z njim sem preverjala, ali je bila tarča napada podjetje ali stranka. Rezultati tega vprašanja se niso ujemali s prejšnjim, saj je odgovor »nismo zaznali napada« izbralo le 66,7 % podjetij in ne 85,1 %, ki so ta odgovor izbrala pri prejšnjem vprašanju. Na vprašanje, kdo je bil tarča kibernetskega napada, je odgovarjalo 33,3 % podjetij, kar pomeni, da je dejansko tretjina podjetij že zaznala kibernetski napad. Slika 4 predstavlja zbrane odgovore.

Slika 4: Ali ste bili tarča vi ali katera od vaših strank?

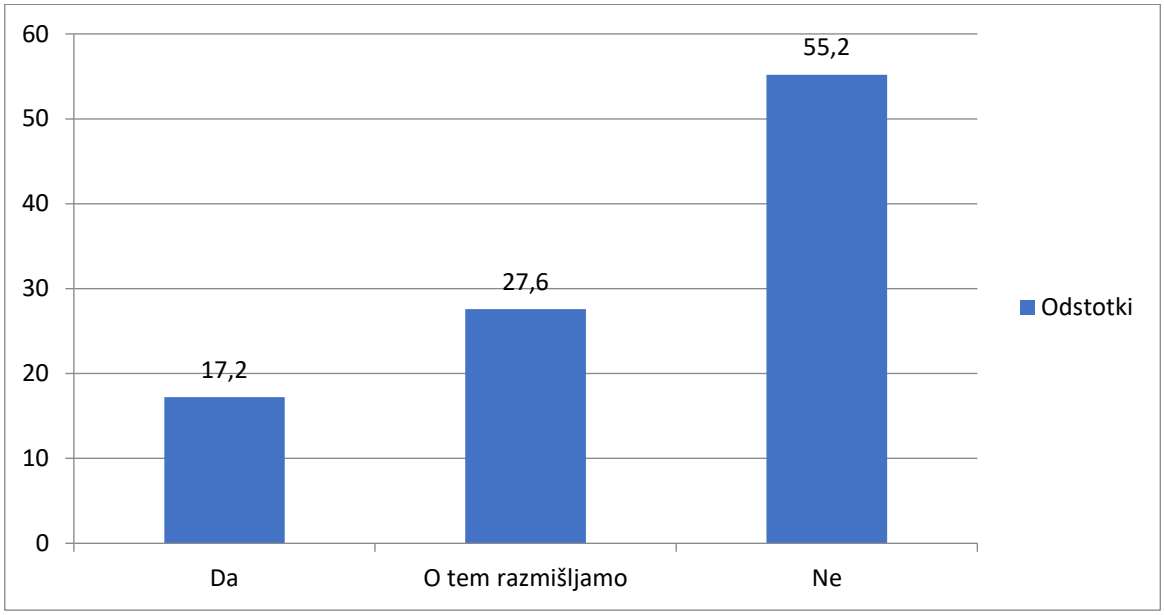


Vir: lastno delo.

Glede na to, da se števili odgovorov na drugo in tretje vprašanje ne ujemata, ne moremo zagotovo trditi, koliko podjetij v raziskavi je zaznalo kibernetski napad oz. vdor v informacijski sistem podjetja.

Četrto vprašanje je podjetja spraševalo po tem, ali imajo v podjetju sprejet interni dokument (varnostno politiko), kjer imajo zapisane vse pomembne ukrepe, postopke in odgovornosti, ki se nanašajo na varnost podatkov.

Slika 5: Sprejet interni dokument

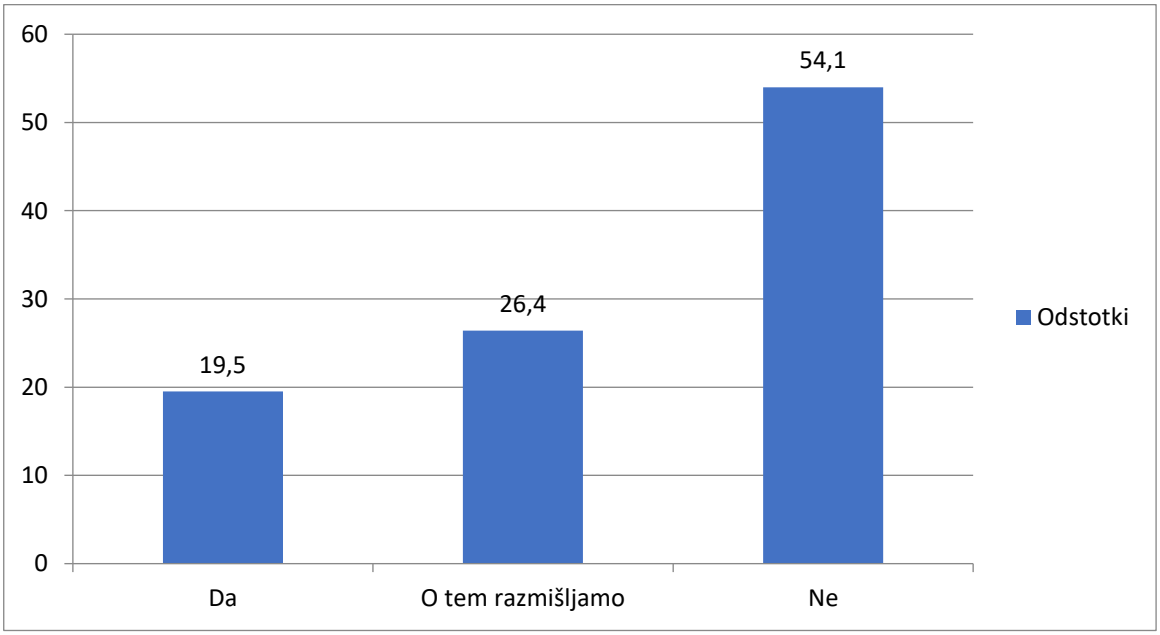


Vir: lastno delo.

Več kot polovica računovodskih servisov (55,2 %) nima sprejetega dokumenta varnostne politike, kjer bi imeli zapisane vse pomembne ukrepe, postopke in odgovornosti, ki se nanašajo na varnost podatkov. Če želi podjetje sistematično pristopiti k varovanju podatkov, tako lastnih kot podatkov strank, in imeti urejene postopke, bi tak interni dokument moralo imeti. Dolžina dokumenta ni pomembna, pomembna je vsebina.

Peto vpraševanje se je glasilo: Ali imate v podjetju izdelan načrt, kako ravnati ob morebitnem napadu?

Slika 6: Izdelan načrt ob morebitnem napadu



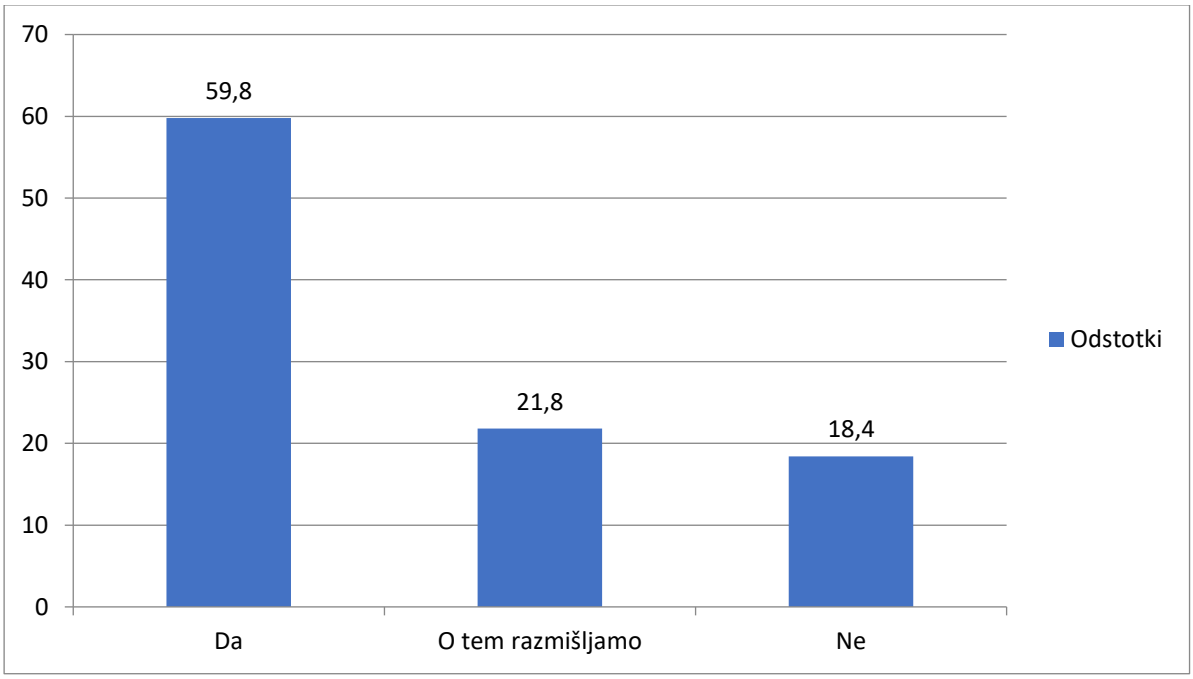
Vir: lastno delo.

2,3 % več podjetij ima izdelan načrt ravnanja ob morebitnem kibernetskem napadu kot sprejeti interni dokument oz. varnostno politiko, kar znaša 19,5 %. 26,4 % podjetij razmišlja o takem načrtu in 54,1 % podjetij takega načrta nima in o pripravi še ne razmišlja.

Šesto vprašanje je služilo preverjanju raziskovalnega vprašanja 2, ki je spraševalo, ali računovodski servisi v Sloveniji izvajajo ukrepe za zagotovitev kibernetske varnosti sebe in svojih strank. Z odgovorom na to vprašanje so podjetja sama ocenila, ali ukrepe izvajajo ali ne, vendar pa bo šele iz odgovorov na nadaljnja vprašanja vidno, ali to drži.

Rezultati na spodnji sliki kažejo, da 59,8 % podjetij ocenjuje, da izvajajo ukrepe za zagotovitev kibernetske varnosti, 21,8 % podjetij razmišlja, da bi te ukrepe začelo izvajati, 18,4 % podjetij pa ocenjuje, da ukrepov za zagotovitev kibernetske varnosti ne zagotavlja. Tu je treba poudariti, da je pri odgovorih podjetij mogoče, da so podjetja napačno ocenila, ali ukrepe zares izvajajo ali ne.

Slika 7: Ali izvajate ukrepe za zagotovitev kibernetske varnosti?



Vir: lastno delo.

Sedmo vprašanje je spraševalo po izvajanju prvega, najbolj osnovnega ukrepa, in sicer: Ali imate ustrezno informacijsko podporo in zaščito računalnikov (redno posodabljanje programov, ustrezna gesla, nameščeni antivirusni programi itd.)?

96,6 % podjetij v raziskavi je odgovorilo, da ima ustrezno informacijsko podporo in zaščito računalnikov, kar vključuje redno posodabljanje programov, ustrezna gesla, nameščene antivirusne programe itd. Visok odstotek odgovora ne preseneča, saj večina uporabnikov računalnikov in računalniških sistemov sedaj že ve, katere osnovne postopke in programe je treba izvajati oziroma imeti, da je računalnik osnovno zaščiten. 3,4 % anketiranih

računovodskih servisov meni, da nima ustrezne informacijske podpore in zaščite računalnikov, kar pomeni, da nimajo zagotovljene niti osnovne varnosti svojih podatkov in podatkov strank.

Osmo vprašanje se je vezalo na prejšnje: Ali za ustrezno varnost informacijskega sistema skrbite sami ali imate za to sklenjeno pogodbo z zunanjim izvajalcem?

40,2 % računovodskih servisov samih skrbi za ustrezno varnost informacijskega sistema, 59,8 % podjetij pa ima za to najete zunanje izvajalce, navadno specializirana podjetja, kot je na primer Akson d.o.o.

Deveto vprašanje: Ali delate varnostne kopije ključnih podatkov kot ukrep za zagotovitev kibernetske varnosti? Če da, kako pogosto?

Tabela 1: Rezultati devetega vprašanja anketnega vprašalnika

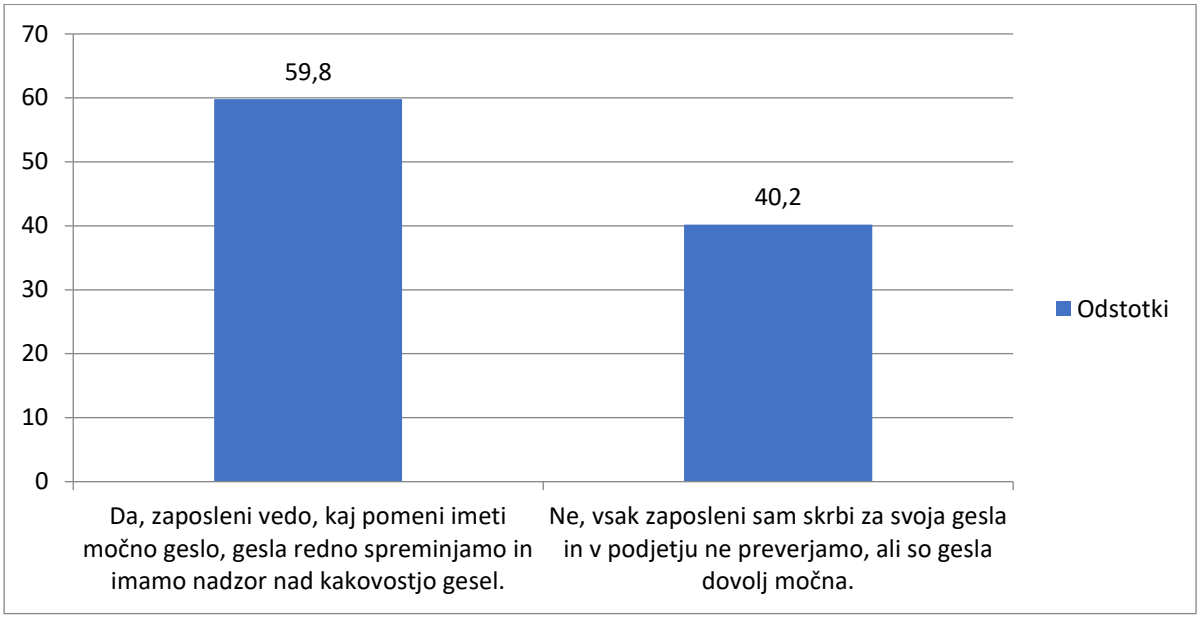
Ali delate varnostne kopije ključnih podatkov kot ukrep za zagotovitev kibernetske varnosti? Če da, kako pogosto?		
	f	f%
Da, dnevno	41	47,1
Da, tedensko	25	28,7
Da, mesečno	13	14,9
Da, letno	4	4,6
Ne	4	4,6
Skupaj	87	100,0

Vir: lastno delo.

Skupaj kar 95,4 % anketiranih podjetij za svoje podatke poskrbi tudi tako, da naredi varnostno kopijo, nekateri pogosteje kot drugi. 4,6 % računovodskih servisov varnostnih kopij ne dela.

Deseto vprašanje anketnega vprašalnika je spraševalo po kakovosti gesel, in sicer se je glasilo: Ali dajete posebno pozornost kakovosti gesel za različne uporabniške račune, elektronsko pošto, dostop do oblaka itd.? Rezultati so predstavljeni na spodnji sliki.

Slika 8: Kakovost gesel



Vir: lastno delo.

Z naslednjima dvema vprašanjema sem preverjala raziskovalno vprašanje 3, ki se glasi: Kolikšen delež računovodskih servisov v Sloveniji izobražuje svoje zaposlene o pomenu kibernetske varnosti in morebitnih posledicah, če ta ni zagotovljena, in na kakšen način?

V letu 2004 je raziskava Ernst & Young pokazala, da kar 70 odstotkov podjetij, vključenih v raziskavo, ni navedlo izobraževanja zaposlenih kot enega od ukrepov za zagotavljanje kibernetske varnosti. Obenem podjetjem ni uspelo zaščititi podatkov in informacij pred zaposlenimi (Swartz, 2004). Zato me je zanimalo, ali slovenski računovodski servisi v letu 2018 dajejo večji pomen izobraževanju zaposlenih, kot so ga dajala podjetja v letu 2004, ki so bila vključena v raziskavo Ernst & Young.

Vprašanje 11 se glasi: Ali izobražujete in usposabljate svoje zaposlene na področju kibernetske varnosti?

In 12 vprašanje: Če da, na kakšen način?

Rezultati kažejo, da največji odstotek anketiranih računovodskih servisov (72,4 % oziroma 63 enot) svojih zaposlenih ne izobražuje o pomenu kibernetske varnosti. Svoje zaposlene izobražuje manjši odstotek servisov (27,6 %).

Na kakšen način podjetja izobražujejo in usposabljajo svoje zaposlene, pa so podjetja odgovorila tako:

- 13,8 % podjetij ukrep izobraževanja in usposabljanja zaposlenih izvaja s predavanji o kibernetski varnosti,

- 11,5 % podjetij ukrep izvaja na druge načine, navedli so interne posvete, občasne pogovore, prilagajanje, spletno prebiranje novic in objav, stalno opozarjanje in informiranje, usposabljanje v praksi in z zunanjimi izvajalci,
- 74,7 % podjetij (65 enot) pa je odgovorilo, da izobraževanj ne izvajajo, kar pomeni, da pri 2 enotah prihaja do odstopanj glede na prejšnje vprašanje, saj je tam 63 podjetij odgovorilo, da izobraževanj ne izvajajo.

S trinajstim vprašanjem sem preverjala raziskovalno vprašanje 4, ki se glasi: Kako pogosto računovodski servisi v Sloveniji izvajajo izobraževanja in usposabljanja za zaposlene?

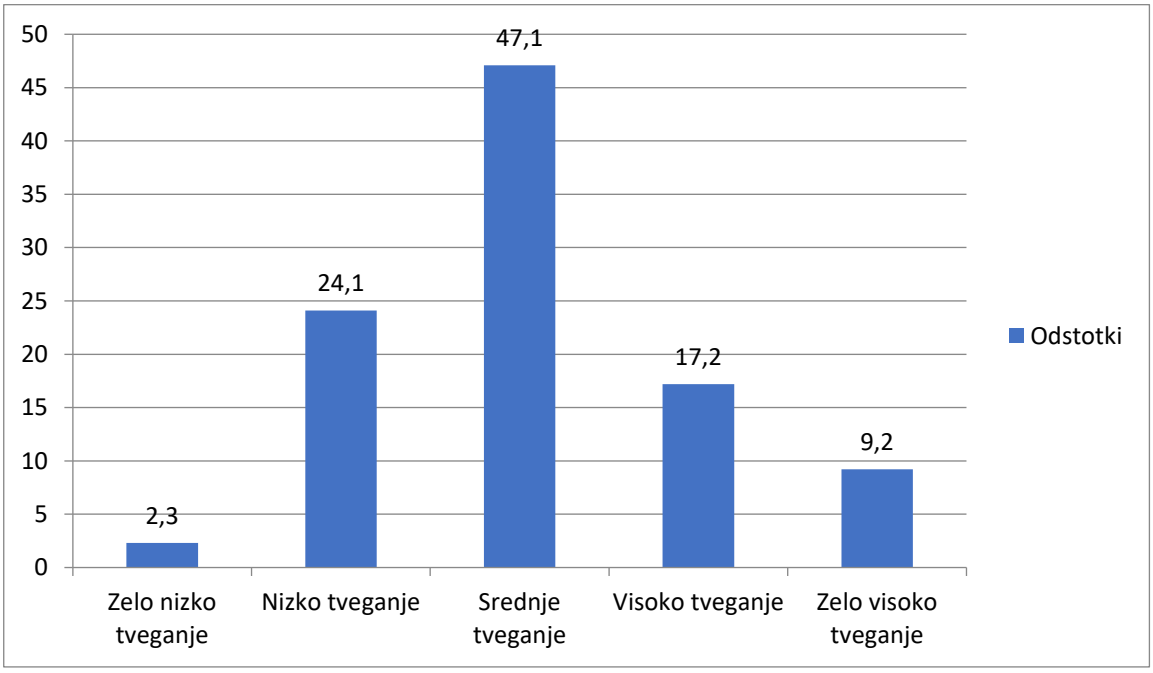
13. vprašanje: Če izobražujete in usposabljate svoje zaposlene, kako pogosto?

26,4 % vseh anketiranih podjetij izvaja izobraževanja in usposabljanja za svoje zaposlene, 12,6 % podjetij ukrep izvaja večkrat letno, 11,5 % enkrat letno in 2,3 % anketiranih podjetij izvaja ukrep manj kot enkrat letno, vendar ga vseeno izvaja. 73,6 % anketiranih podjetij tega ukrepa ne izvaja. Spet pa je prišlo do razlike glede na enajsto vprašanje, in sicer pri eni anketirani enoti.

14. vprašanje: Kako visoko ocenjujete kibernetsko tveganje v računovodski panogi (glede na verjetnost nastanka napada in posledice)?

Rezultati kažejo, da anketiranci na lestvici od 1 do 5 (pri čemer 1 pomeni zelo nizko tveganje in 5 pomeni zelo visoko tveganje) kibernetsko tveganje v računovodski panogi pri največji vrednosti 5 ocenjujejo s povprečno oceno 3,07.

Slika 9: Ocena kibernetskega tveganja v računovodski panogi



Vir: lastno delo.

Vprašanje 15 se je glasilo: Ali imate sklenjeno zavarovanje za kibernetsko tveganje?

Le tri anketirana računovodska podjetja (3,4 %) imajo sklenjeno zavarovanje za kibernetsko tveganje, ostala pa tega zavarovanja nimajo.

Zadnje, šestnajsto vprašanje je spraševalo še o drugih ukrepih za zagotavljanje kibernetske varnosti, ki bi jih anketirana podjetja morebiti izvajala: Ali izvajate še kak drug ukrep za zagotavljanje kibernetske varnosti? Če da, kateri?

90,8 % anketiranih podjetij je izbralo odgovor ne, kar pomeni, da drugih ukrepov za zagotavljanje kibernetske varnosti ne izvajajo. 9,2 % podjetij izvaja tudi druge ukrepe za zagotavljanje kibernetske varnosti. Navedli so:

- spremljanje gospodarskega in političnega dogajanja,
- računalniki s podatki niso povezani z internetom,
- obveščanje o napadih in vzrokih ter primerih dobre prakse,
- izogibanje uporabi internetnih oblakov za shranjevanje podatkov,
- DDOS zaščita,
- arhiv na več lokacijah,
- antivirusni programi in
- antivirusni program, sprememba gesel.

Treba je poudariti, da so odgovori »antivirusni program«, »sprememba gesel« in »lokacije arhiva« že vključeni v druga vprašanja, saj je prvo vprašanje že spraševalo, ali ima podjetje nameščen antivirusni program in če uporablja ustrezna gesla. Odgovor na deseto vprašanje je prav tako vključeval redno spreminjanje gesel, zato zadnjih dveh odgovorov ne moremo imeti za dodatna ukrepa za zagotovitev kibernetske varnosti.

Prav tako dodatnega ukrepa ne pomeni arhiv na več lokacijah, gre namreč za več narejenih varnostnih kopij na različnih lokacijah. Res pa je, da anketni vprašalnik ni imel podvprašanja, ki bi se nanašalo specifično na število varnostnih kopij, ampak le na pogostost delanja varnostnih kopij.

2.3.2 Globinski intervju

Ker so se za sodelovanje v raziskavi in izpolnjevanje anketnega vprašalnika večinoma odločila manjša podjetja, sem želela raziskati tudi, kako se z zagotavljanjem kibernetske varnosti spopadajo v vsaj eni večji slovenski računovodski hiši. Za sodelovanje in intervju sem prosila nekaj večjih slovenskih podjetij, ki ponujajo računovodske storitve, odgovor in pripravljenost za sodelovanje v intervjuju pa sem dobila le iz računovodske hiše Unija. Intervju v njihovih prostorih na Brezovici sem opravila 24. 7. 2018, in sicer z vodjo internega IT oddelka, Matejem Gorenškom (v nadaljevanju sogovornik).

Okvir za vprašanja sem črpala iz anketnega vprašalnika, dodala pa sem tudi nekaj bolj poglobljenih vprašanj, nekaj vprašanj pa se je porodilo tudi med pogovorom. Sogovornik je najprej odgovoril na nekaj osnovnih vprašanj glede podjetja Unija. Podjetje je prisotno tako na slovenskem tržišču kot tudi izven meja Slovenije, in sicer v kar 13 drugih evropskih državah, članicah Evropske unije in tretjih državah. Podjetje je med vodilnimi slovenskimi računovodskimi servisi in ima po oceni sogovornika 2-% tržni delež. V vseh podružnicah Unije v Sloveniji je zaposlenih okoli 50 ljudi, v celotni regiji, kjer delujejo, pa še okoli 120 ljudi. Unija računovodska hiša d.o.o. ima približno 350 strank, Unija XS, računovodske storitve, d.o.o. pa okoli 150 strank. Unija XS je ločeno podjetje, ki nudi računovodske storitve mikro in majhnim podjetjem ter podjetnikom in prav tako deluje na slovenskem trgu. Podjetji Unija računovodska hiša d.o.o. in Unija XS, računovodske storitve, d.o.o. imata skupne lastnike, in sicer sta to Unija holding, holdinška družba, d.o.o. z 49 % in Miroslav Pikovnik z 51-% deležem. Podjetje deluje na več lokacijah po Sloveniji, npr. v Ljubljani, Škofji Loki, Kranju, Novem mestu, Celju in drugje. Prihodki podjetja Unija d.o.o. so v letu 2017 znašali 3.632.240 evrov, vrednost sredstev pa 4.459.057 evrov. Prihodki podjetja Unija XS so v letu 2017 znašali 190.192 evrov, vrednost sredstev pa 266.043 evrov.

V nadaljevanju predstavljam odgovore na vprašanja glede kibernetskega tveganja in zagotavljanja kibernetske varnosti v podjetju. Najprej sem sogovornika prosila, da oceni verjetnost kibernetskega napada oziroma vdora v informacijski sistem podjetja Unija. Na lestvici od 1 do 6 je sogovornik verjetnost nastanka varnostnega incidenta ocenil z oceno 6, predvsem zaradi prepoznavnosti podjetja v širši javnosti in velikosti podjetja.

Za celotno računovodsko panogo meni, da je podvržena srednjemu tveganju za primer kibernetskega napada, saj naj bi bila manjša podjetja manj na udaru spletnih kriminalcev zaradi majhnosti in manjše prepoznavnosti. V pregledu literature se je ravno to izkazalo za napačno mišljenje, saj naj bi bila manjša podjetja prav tako tarče kibernetskih napadalcev. Manjša podjetja ne želijo ali ne morejo vložiti toliko finančnih sredstev in časa v zagotavljanje kibernetske varnosti in so zato lažje tarče, česar pa se spletni kriminalci dobro zavedajo. Medtem lahko podjetje, kot je Unija, vloži sredstva v zagotavljanje visoke ravni kibernetske varnosti, kar kaže tudi pridobljeni certifikat ISO 27001.

Na vprašanje, ali so v zadnjih petih letih v podjetju zaznali kibernetski napad, je sogovornik odgovoril, da so pred dvema letoma v sistemu zaznali virus. Krivec za virus v informacijskem sistemu podjetja je bila okužena priponka v elektronskem sporočilu zaposlene osebe, ki je večkrat kliknila na priponko. Nameščeni antivirusni program je virus zaznal in javil okužbo, kar je pomenilo, da so lahko začeli ukrepati takoj in virus ni povzročil škode. Delo se je ustavilo le za nekaj ur, dokler niso zaključili z varnostnim pregledom in se prepričali, da ni bilo storjene nobene druge škode. Po navedbah sogovornika niso bili ogroženi nobeni podatki podjetja ali strank. Varnostni incident ni bil poročan nobeni instituciji, saj so ga reševali interno.

To kaže, da se podatki o številu varnostnih incidentov v Sloveniji, ki jih navajajo vladne institucije, verjetno razlikujejo od dejanskega števila varnostnih incidentov, saj jih podjetja velikokrat ne poročajo in jih raje rešujejo interno. Če bi bili vsi varnostni incidenti prijavljeni pristojni instituciji, bi strokovnjaki za kibernetsko varnost lažje ugotovili, kje se pojavlja največ kršitev, zakaj in na kakšen način se pojavljajo ter kakšne so njihove posledice. Za podjetja bi to lahko bila podlaga za pripravo smernic o kibernetski varnosti, hkrati pa bi postalo jasneje, na kaj morajo biti podjetja najbolj pozorna in sprejetje katerih ukrepov je najbolj potrebno. Če podatki niso popolni, lahko dajejo napačno sliko o problematiki in vodijo v napačno razumevanje kibernetskega tveganja.

Podjetje ima sprejete interne akte, ki urejajo varnost podatkov, in certifikat ISO 27001, ki zagotavlja visoko raven varovanja informacij v različnih oblikah in medijih. V Sloveniji naj bi bili edini s tovrstnim certifikatom, ki zahteva veliko vlaganj, tako finančnih kot tudi strokovnih. Prav tako imajo v podjetju sprejet interni dokument, kako postopati v primeru kibernetskega napada. Načrt so dve leti nazaj tudi uporabili in po mnenju sogovornika se je to izkazalo za učinkovito sredstvo za hitro zajezitev virusa in posledično preprečitev kraje podatkov. Pobudo za sprejetje internih aktov in standarda ISO 27001 je dal IT oddelek, vodstvo pa je potrdilo predlog, saj se je tudi samo zavedalo groženj, ki pretijo podjetjem v informacijski dobi.

Podjetje izvaja dva izmed treh pomembnih ukrepov za zagotavljanje kibernetske varnosti. V prvi vrsti je to zagotavljanje ustrezne varnosti informacijskega sistema, kar pomeni redno in skrbno posodabljanje operacijskega sistema in programske opreme, nameščene antivirusne programe, zaklenjene porte in dvojno identifikacijo za vstop do informacijskega sistema podjetja (z uporabniškim imenom in geslom ter potrditvijo prek telefona). Gesla zaposlenih morajo biti kreirana v skladu s standardom ISO 27001, kar pomeni najmanj 8 znakov dolga gesla z velikimi in malimi črkami, številkami in enim znakom (.,! …). Gesla se morajo spremeniti na vsaj tri mesece. Varnost informacijskega sistema zagotavljajo v internem IT oddelku, sodelujejo pa tudi s podjetjem Sibit iz Ljubljane, ki ponuja informacijske rešitve. Odvisno od pomembnosti podatkov delajo tudi dnevne, mesečne in letne varnostne kopije podatkov.

Drugi ukrep je izobraževanje in usposabljanje zaposlenih, ki poteka na dva načina. Prvi je izobraževanje zaposlenih, ki ga izvedejo zunanji strokovnjaki in kjer se zaposleni seznanijo z nevarnostmi, ki jim pretijo na spletu in se naučijo prepoznati phishing elektronsko sporočilo. Taka izobraževanja potekajo dvakrat do trikrat letno ali po potrebi. Drugi način je interno izvajanje izobraževanja z mesečnim pošiljanjem elektronskih sporočil o aktualnih novicah na področju kibernetske varnosti. Odzivi zaposlenih na tovrstna izobraževanja so pozitivni, saj se z zavedanjem kibernetskega tveganja in resnosti tega problema lahko skupaj z vodstvom borijo proti spletnim kriminalcem.

Zaposlenim v podjetju Unija so svetovali previdnost pri odpiranju priponk, zato vsa sumljiva elektronska sporočila posredujejo IT oddelku, kjer sporočilo pregledajo in zaposlenemu sporočijo, ali je priponko varno odpreti. Tako preprečijo, da bi se morali zaposleni, ki niso strokovnjaki na področju kibernetske varnosti, sami odločati o verodostojnosti priponke in bi v primeru napačne odločitve nenamerno škodovali podjetju. To do neke mere razbremeni zaposlene, ki se lahko osredotočijo na strokovno opravljanje svojega dela. Na ta način zaposleni sodelujejo v zagotavljanju kibernetske varnosti podjetja, za kar pa niso posebej nagrajeni.

Podjetje se še ni poslužilo testiranja zaposlenih s kontroliranim phishing napadom, saj naj to ne bi bilo potrebno, ker zaposleni sami posredujejo sumljivo elektronsko pošto v pregled IT oddelku, kar je primer dobre prakse.

Tretji ukrep je zavarovanje za kibernetsko varnost, katerega pa podjetje nima sklenjenega. Sogovornik ni mogel odgovoriti na to, ali o sklenitvi takega zavarovanja razmišljajo. Razlog za nesklenjeno zavarovanje je lahko nepoznavanje takšnega zavarovanja, kar je precej neverjetno, saj imajo vsa velika podjetja oddelek za upravljanje s tveganji. Drugi razlog vidim v tem, da podjetje meni, da je z visokimi standardi glede varovanja podatkov, ki jih zahteva ISO 27001, dovolj zaščiteno pred spletnimi kriminalci. Sogovornik se zaveda, da so kibernetski kriminalci vedno bolj iznajdljivi, kar od podjetja zahteva nenehno iskanje novih rešitev za učinkovito upravljanje operativnega tveganja. Čeprav so cene zavarovanj za kibernetsko tveganje visoke, menim, da bi podjetje, kot je Unija, lahko sklenilo tako zavarovanje. Pomagalo bi pri morebitnih finančnih izgubah, ki bi jih imelo podjetje ob kibernetskem napadu, vsekakor pa ne bi pomagalo pri zaščiti ugleda ali povrnitvi sedanjega ugleda podjetja.

Kot dodatni ukrep je sogovornik navedel določilo iz internega dokumenta, da imajo zaposleni omogočen dostop le do podatkov, ki jih potrebujejo za svoje delo in do strank, za katere vodijo računovodstvo. Tudi tako lahko tudi do neke mere zajezijo namerno škodovanje morebitnih zlonamernih zaposlenih.

Po mnenju sogovornika je najpomembnejši in najučinkovitejši ukrep izobraževanje zaposlenih, saj so zaposleni največkrat razlog za varnostni incident. Oba načina izobraževanja, ki se ju poslužujejo, to sta izobraževanje v tradicionalni obliki in v obliki pošiljanja internih elektronskih sporočil s tematiko zagotavljanja kibernetske varnosti, sta pomembna.

Najpomembnejše posledice za podjetje v primeru kibernetskega napada bi po mnenju sogovornika bile finančne izgube, morebitna tožba in oškodovan ugled podjetja v očeh javnosti. Ob vsakem kibernetskem napadu so finančne posledice neizogibne, če ne drugega za vzpostavitev novih ukrepov ali posvetovanja z zunanjimi strokovnjaki.

2.4 Omejitve raziskave

Izvedena raziskava z anketo ima štiri glavne omejitve, in sicer:

1. Število podjetij, ki se je odločilo za sodelovanje v raziskavi. Zaradi občutljive teme se je za izpolnitev anketnega vprašalnika odločil le nizek odstotek podjetij, ki so dobila vabilo k sodelovanju. Delež odgovorov je namreč znašal le 4,65 %, kar ni omogočilo posploševanja na celotno populacijo računovodskih servisov v Sloveniji. Izvedena raziskava je le pokazala, kako kibernetsko tveganje ocenjujejo podjetja v vzorcu in katere ukrepe ta podjetja izvajajo za zagotovitev kibernetske varnosti.
2. Dejavnost 69.200 – Računovodske, knjigovodske in revizijske dejavnosti, davčno svetovanje. Populacija je bila izbrana na podlagi registrirane dejavnosti 69.200 in na tej osnovi so bila poslana tudi vabila za izpolnitev vprašalnika z naslovom »Obvladovanje kibernetskega tveganja v računovodskih servisih«. Mogoče je, da je anketni vprašalnik, ki je specifično naslavljal računovodske servise, izpolnilo podjetje, ki sicer ima registrirano to dejavnost, dejansko pa te dejavnosti ne opravlja. To bi pomenilo, da je v raziskavo vključeno podjetje, ki dejansko ni računovodski servis.
3. Nepriznavanje kibernetskega napada oz. vdora v informacijski sistem. Zaradi občutljivosti teme obstaja tveganje, da je katero od podjetij, ki je sodelovalo v raziskavi, zanikalo kibernetski napad v podjetju. Anketni vprašalnik je zagotovil popolno anonimnost in zaupnost pridobljenih podatkov ter obljubil, da bodo rezultati objavljeni le v agregirani obliki. Kljub temu obstaja možnost, da je katero od podjetij kibernetski napad raje zanikalo.
4. Glede na to, da je poznavanje kibernetskih napadov oz. vdorov v informacijski sistem vedno bolj medijsko izpostavljeno, menim, da večina ljudi ne pozna vseh oblik kibernetskih napadov in so bili omejeni le na najbolj očitne, kot sta na primer zakodiranje podatkov ter izsiljevanje, ki ima kot posledico krajo podatkov ali finančne izgube. Večina ljudi se verjetno ne zaveda, da se kot kibernetski napad oz. vdor v informacijski sistem obravnava kakršen koli nepooblaščen dostop do podatkov podjetja ali strank. Če bi se tega podjetja, ki so sodelovala v raziskavi, zavedala, bi bil odstotek zaznave kibernetskega napada verjetno višji.

SKLEP

Informacije so vedno bile eno od najpomembnejših sredstev, ki jih podjetje lahko ima. To vključuje poslovne skrivnosti, patente in »know-how«. V postindustrijskem gospodarstvu so sredstva, ki temeljijo na znanju, postala ključna, ne le za trenutni obstoj podjetja, ampak tudi za njegovo dolgoročno poslovanje. Podjetja zadržujejo kopico pomembnih, občutljivih in zaupnih podatkov o svojih računalniških sistemih in omrežjih. Iz tega sledi, da bi kakršna koli grožnja sredstvom, ki temeljijo na znanju, računalniškim sistemom in omrežjem neposredno ogrozila uspešnost in učinkovitost ter s tem obstoj podjetja. Na žalost so te

informacije dovzetne za različne oblike kibernetskih napadov. Ti napadi so lahko nepooblaščen dostop do podatkov, zlonamerne kode, neprimerna uporaba do razkritja in kraja podatkov/informacij, če naštejemo le najbolj pogoste. Povečana uporaba spleta s strani podjetij te ranljivosti še bolj izpostavlja in tako je učinkovita zaščita podatkov še toliko bolj relevantna. Podjetja morajo vzpostaviti ravnovesje med zaščito občutljivih in zaupnih informacij o podjetju ter razpoložljivostjo teh informacij svojim deležnikom. Korporacijski podatki morajo biti na voljo deležnikom in v nekaterih primerih tudi javnosti, ne le za spodbujanje naložb v podjetje, temveč tudi za izpolnjevanje zakonske dolžnosti obveščanja in preglednosti nad podjetjem. Pomen informacij o podjetju in zaščita njegove integritete pred naraščajočim tveganjem in grožnjami zahtevata, da podjetja sprejmejo razumne ukrepe za zavarovanje informacijskih sredstev podjetja. Če podjetju tega ne uspe zagotoviti, se lahko podjetje in njegovi zaposleni soočijo z morebitno pravno in finančno odgovornostjo (Etsebeth, 2011).

Informacijska tehnologija je prisotna v vseh dejavnostih in procesih podjetja. Pri odnosih med posamezniki, podjetjem in javnimi ustanovami vse bolj posredujejo IT rešitve. V tem kontekstu so informacijske spretnosti in znanje vsakega posameznika nujno potrebni za zagotavljanje strokovne usposobljenosti za socialno vključevanje v okolje. Ker bo digitalni svet še naprej širil svoj vpliv, bo novi poklicni profil na različnih področjih povzročil pomembne izzive za učni proces študentov računovodstva. Akademske ustanove se morajo zavedati potrebe in pomena poglobitve na področju informacijske tehnologije na vseh programih ter prilagoditi kurikulum in metode poučevanja novim strokovnim zahtevam.

Rezultati raziskave so pokazali, da se slovenski računovodski servisi resnosti svetovnega fenomena kibernetskih napadov in vdorov v informacijske sisteme še vedno ne zavedajo dovolj. To potrjujejo tudi rezultati izvajanja ukrepov. Bolj kot bi se podjetja zavedala nevarnosti in tveganj, v večjem številu bi izvajala tudi potrebne ukrepe.

Večina podjetij ima zagotovljeno ustrezno informacijsko podporo in zaščito računalnikov, vsaj tista, ki imajo za to najete zunanje specializirane izvajalce. Kljub temu je za kakovost gesel treba poskrbeti interno. Zunanji izvajalci kakovosti gesel namreč ne preverjajo, razen če se za to podjetje dogovori posebej.

Večina podjetij še vedno ne daje velike teže ostalim ukrepom, kot so izobraževanje in usposabljanje zaposlenih ter zavarovanje za kibernetsko varnost. Zavarovanje za kibernetsko zavarovanje imajo sklenjena le tri podjetja, razlog za to lahko verjetno najdemo predvsem v visoki ceni zavarovanj in prepričanju podjetij, da se jim kibernetski napad ne more zgoditi. Presenetljivo je, da ta tri podjetja ne spadajo v skupino velikih podjetij, ki so bila vključena v raziskavo. Ta podjetja zaposlujejo enega, dva in pet ljudi, imajo 30, 40 in 70 strank in prihodke 30.000, 45.000 in 260.000 evrov. Glede na to, da imata prvi dve podjetji nizke prihodke, cene zavarovanj za kibernetsko tveganje pa so visoke, je težko verjeti, da imata takšno zavarovanje zares sklenjeno in je ta dva odgovora treba upoštevati z nekaj distance.

Vsa podjetja imajo sprejet dokument varnostne politike, dve podjetji imata načrt ravnanja ob morebitnem napadu, eno podjetje pa o tem razmišlja. Vsem varnost informacijskega sistema zagotavlja zunanji izvajalec. Vsa podjetja delajo varnostne kopije, dva dnevno in eno tedensko, vsa so pozorna na kakovost gesel. Eno podjetje enkrat letno izobražuje in usposablja zaposlene na področju kibernetske varnosti, ostali dve podjetji pa tega ukrepa ne izvajata.

Zanimivo je, da največje podjetje v raziskavi ukrepa izobraževanja in usposabljanja zaposlenih ne izvaja in nima sklenjenega zavarovanja za kibernetsko tveganje.

Odgovor na raziskovalno vprašanje 1: Anketirani računovodski servisi kljub vse večji izpostavljenosti kibernetskemu tveganju zaradi digitalizacije poslovnih procesov, ki prinaša tudi novo tveganje, še vedno verjamejo, da je verjetnost za kibernetski napad v njihovem podjetju srednja do srednje majhna. Za slovenske računovodske servise je kibernetska varnost še vedno nekaj samoumevnega, ne zavedajo pa se, da so podatki in informacije o njih samih in o strankah ključni del njihovega poslovanja. Hitra rast števila kibernetskih napadov in njihova resnost je vse bolj vidna tudi v medijski sferi, ki pa poroča le o napadih, ki dosežejo veliko število uporabnikov spleta ali pa javnosti znano podjetje. Zato imajo podjetja lahko napačno predstavo, da kibernetski napadi doletijo le velika in znana podjetja. Za vse kibernetske napade javnost sploh ne izve, največkrat je to posledica tega, da podjetja ne želijo priznati, da se je napad na njihov informacijski sistem zgodil, saj bi to lahko močno omajalo njihovo podobo in ugled na trgu. To spreminja Splošna uredba EU o varstvu podatkov, ki zahteva, da se vsak kibernetski napad ali vdor tudi prijavi pristojni instituciji. Šele takrat bo vidno, kakšno je dejansko število kibernetskih napadov v slovenskem gospodarskem prostoru.

Odgovor na raziskovalno vprašanje 2: Večina anketiranih računovodskih servisov je bila mnenja, da izvajajo ukrepe za zagotavljanje kibernetske varnosti. Raziskava je pokazala, da večina računovodskih servisov izvaja le najbolj osnovni ukrep za zagotavljanje kibernetske varnosti, kar je ustrezna informacijska podpora in zaščita računalnikov (redno posodabljanje programov, ustrezna gesla, nameščeni antivirusni programi, itd.). Skoraj polovica anketiranih računovodskih servisov (47,1 %) skrbi za dnevne varnostne kopije in 59,8 % servisov skrbi, da njihovi zaposleni uporabljajo močna gesla, ki jih tudi redno spreminjajo. Težava izvajanja ukrepov se pojavi že pri izobraževanju in usposabljanju zaposlenih ter sklepanju zavarovanja za kibernetsko tveganje. Zavarovanje za kibernetsko tveganje imajo sklenjeno le tri podjetja, ki so sodelovala v raziskavi, kar predstavlja 3,4 % anketiranih. Težava ni le v izvajanju ukrepov, ampak izvira že iz dejstva, da 55,2 % podjetij nima sprejete varnostne politike oz. internega dokumenta, v katerem bi imeli zapisane pomembne ukrepe, postopke in odgovornosti, ki se nanašajo na varnost podatkov, čeprav je to prvi korak k sistematičnemu in uspešnemu upravljanju s kibernetskim tveganjem.

Raziskovalno vprašanje 3: Z raziskavo sem ugotovila, da le nekaj več kot četrtina (27,6 %) anketiranih računovodskih servisov pripravlja izobraževanja in usposabljanja za svoje zaposlene o pomenu kibernetske varnosti in jih poduči o morebitnih posledicah varnostnih incidentov.

Čeprav raziskave kažejo, da je pri varnostnih incidentih največkrat prisoten človeški faktor (Suhadolnik, 2017; Ashenden, 2016; Perko, 2017; Ashford, 2017; Finkle, 2017), podjetja temu ukrepu ne dajejo velike teže. Tehnologija namreč težko prepreči zaposlenemu, da nenamerno odpre zlonamerno priponko elektronskega sporočila, če ne prepozna vidnih znakov okuženega sporočila. Zlonamernemu zaposlenemu pa tako tehnologija kot izobraževanje težko preprečita nepooblaščeni vdor v sistem, če informacijski sistem podjetja pozna in ga vsakodnevno uporablja.

13,8 % anketirancev izobraževanje izvaja s predavanjem o kibernetski varnosti, 11,5 % pa na drugačen način, kot so interni posveti, pogovori, prebiranje novic, opozarjanje in informiranje. Skoraj četrtina anketiranih računovodskih servisov izobraževanj in usposabljanj ne izvaja.

Raziskovalno vprašanje 4: Nekateri strokovnjaki predlagajo izvajanje izobraževanja in usposabljanja vsaj enkrat letno (Werner, 2017). Računovodski servisi, vključeni v raziskavo, v 12,6 % izobraževanja izvajajo večkrat letno, v 11,5 % enkrat letno in v 2,3 % manj kot enkrat letno. Preostali izobraževanj in usposabljanj ne izvajajo.

Končni sklep izvedene raziskave je, da slovenski računovodski servisi še vedno podcenjujejo obstoj kibernetskega tveganja pri njihovem poslovanju. Bojim se, da bodo do spoznanja, da bi morali kibernetsko tveganje prepoznati in z njim upravljati, prišli, ko bo zanje že prepozno. Kibernetski napad ne pomeni le finančnih izgub za podjetje, usodni so lahko tudi izguba ugleda, odhod strank in nezmožnost pridobivanja novih strank zaradi okrnjenega ugleda.

Vsem podjetjem, ne le računovodskim servisom, svetujem, da resno razmislijo o upravljanju kibernetskega tveganja, če želijo, da so njihovi podatki in podatki strank varni in da do njih ne bodo dostopali ter jih izkoristili nepooblaščena oseba, spletni kriminalci ali zlonamerni zaposleni. Upravljanje s kibernetskim tveganjem je proces, ki se ne zgodi čez noč, saj zahteva čas za vzpostavitev postopkov, ki bodo zagotovili kibernetsko varnost. Najprej pa je potrebno zavedanje. Ko se vodstvo, lastniki in zaposleni zavedajo obstoja kibernetskega tveganja, v prvem koraku sprejmejo interni dokument oz. varnostno politiko. Uvedba in izvajanje ukrepov sledijo šele v drugem koraku. Če podjetje ne ve, katere podatke mora varovati in na katerih točkah je najbolj ranljivo, potem je izvajanje ukrepov neučinkovito in samemu sebi namen.

Za zagotovitev kibernetske varnosti na visoki ravni so potrebni visoki finančni vložki, tako v začetni fazi vzpostavitve kot tudi v nadaljevanju, ko so potrebne posodobitve in prilagoditve varnostne politike ter izvajanje dodatnih ukrepov. Treba se je zavedati, da vsa podjetja, predvsem manjša, ne morejo vlagati znatnih sredstev v varnostno politiko podjetja, saj se primarno ukvarjajo s tem, da so storitve zagotovljene strokovno in da zaposleni v podjetju redno dobivajo plače. Višek denarja se razporedi na po njihovem mnenju »manj pomembne« projekte, med katerimi je na žalost tudi vzpostavitev sistema kibernetske varnosti. V kolikor se podjetja ne bodo zavedala, da je kibernetska varnost pomemben proces v zagotavljanju storitev strankam, bo to vedno odrinjeno na konec seznama potrebnih investicij ali na seznam sploh ne bo uvrščeno. Ker pa se število in resnost kibernetskih napadov iz leta v leto povečujeta, bo prizadetih vedno več podjetij.

Ker so cene računovodskih storitev v Sloveniji zaradi velike konkurence med številnimi ponudniki nizke, lahko podjetje, kateremu je računovodstvo vodilo v kibernetskem napadu prizadeto podjetje, hitro in brez visokih stroškov računovodstvo prenese na podjetje, katerega ugled ni omadeževan.

LITERATURA IN VIRI

1. Aberdeen Group. (2013, januar). *SaaS Data Loss: The Problem you Didn't Know You Had*. Pridobljeno 15. februarja 2018 iz http://go.spanning.com/rs/832-UFI-346/images/Aberdeen_Research_SaaS_Data_Loss.pdf
2. ACCA. (2012). *ACCA Report: Digital Darwinism: thriving in the face of technology change*. Pridobljeno 10. januarja 2018 iz http://www.accaglobal.com/content/dam/acca/global/PDF-technical/other-PDFs/Fivemins-on-Digital-Darwinism.pdf
3. Al-Hamar, M., Dawson, D. & Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. *Campus-Wide Information Systems, 28*(5), 308–319.
4. Ashenden, D. (2016). The Human Shield. *TCE: The Chemical Engineer*, (896), 22–25.
5. Ashford W. (2017, 31. januar). *Awaken business to Cyber Risk Reality*. Pridobljeno 10. avgusta 2018 iz http://www.computerweekly.com/news/252436453/Awaken-business-to-Cyber-Risk-Reality
6. Ashtiani, M. & Abdollahi Azgomi, M. (2014). A distributed simulation framework for modeling cyber attacks and the evaluation of security measures. *Simulation, 90*(9), 1071–1102.
7. Briody, D. (2007). Full Coverage: How to Hedge Your Cyber Risk. *Inc, 29*(4), 47–49.
8. Choucri, N., Madnick, S. & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology For Development, 20*(2), 96–121.

9. Cioaca, C., Bratu, A. & Ștefanescu, D. (2017). The Analysis of Benchmarking Application in Cyber Security. *Proceedings Of The Scientific Conference AFASES*, 257–62.
10. Consumer reports (2011, junij). *Your security. 25 things cops and crooks are saying you're doing wrong.* Consumer reports, 20–2.
11. Dattu, V. (2016). Protecting Data Starts with Education and a Plan. *Capitol Ideas*, *59*(3), 16–19.
12. Deloitte. (2017, 15. junij). *Cyber risk in consumer business*. Pridobljeno 20. januarja 2018 iz https://www2.deloitte.com/insights/us/en/industry/retail-distribution/cyber-risk-management-in-consumer-business.html
13. Direct Marketing Association. (2015). Important credit card security notification. Pridobljeno 2. marca 2018 iz https://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-248525.pdf
14. Ehrlich, P. (2017). Building Cyber-Physical Security. *Engineered Systems*, *34*(12), 28–32.
15. Epstein, A. J. (2014). Thinking strategically about cyber risk. *NACD Directorship*, 32–35.
16. Etsebeth, V. (2011). Defining the Current Corporate IT Risk Landscape. *Journal Of International Commercial Law & Technology*, *6*(2), 62–73.
17. Federal Communications Commission. (2012). *Cyber Security Planning Guide.* Washington: Federal Communications Commission.
18. Finkle, V. (2017). No Hackers Allowed. *Inc*, *39*(2), 52–53.
19. Forrester Consulting. (2017, februar). *Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model*. Pridobljeno 24. januarja 2018 iz https://www.centrify.com/media/4594046/stop-the-breach.pdf
20. Gabrys, E. (2002). The International Dimensions of Cyber-Crime, Part 1. *Information Systems Security*, *11*(4), 21–32.
21. Gartner Inc. (2013, 7. junij). *Definition: Cybersecurity.* Pridobljeno 2. februarja 2018 iz https://www.gartner.com/doc/2510116/definition-cybersecurity/
22. Gaudenzi, B. & Siciliano, G. (2017). Just do it: Managing IT and Cyber Risks to Protect the Value Creation. *Journal Of Promotion Management*, *23*(3), 372–385.
23. Gordon, L. A. & Loeb, M. P. (2006). *Managing cybersecurity resources: a cost-benefit analysis* (1 izd.). New York: McGraw-Hill.
24. Gordon, L. A., Loeb, M. P. & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communications Of The ACM*, *46*(3), 81–85.
25. Grossman, R. L. (2009). The case for cloud computing. *IT professional*, *11*(2), 23–27.
26. Hackett, K. (2013). Best Practices for Minimizing Your Digital Security Risk. *Quill*, *101*(4), 34–39.
27. Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, *26*(6), 639–688.
28. Hausken, K. (2017). Security Investment, Hacking, and Information Sharing between Firms and between Hackers. *Games*, *8*(2), 1–23.

29. Hopkins, N. (2017, 25. september). *Deloitte hit by cyber-attack revealing clients' secret emails.* Pridobljeno 13. marca 2018 iz https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails
30. IFAC. (2003). *International Educational Guide – IEG11: Information technology for professional accountants, International Federation of Accountants Education Committee,* Pridobljeno 12. februarja 2018 iz https://www.imanet.org/pdf/ITPA.pdf
31. Imgraben, J., Engelbrecht, A. & Choo, K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347–1360.
32. Institute of Risk Management. (brez datuma a). *Cyber risk and risk management*. Pridobljeno 29. decembra 2017 iz https://www.theirm.org/media-centre/press-releases/irm-unveils-global-cyber-risk-report.aspx
33. Institute of Risk Management. (brez datuma b). *Cyber risk and risk management*. Pridobljeno 29. decembra 2017 iz https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
34. Johnson, K. N. (2015). Cyber Risks: Emerging Risk Management Concerns for Financial Institutions. *Georgia Law Review*, *50*(1), 131–211.
35. Johnson, K. N. (2016). Managing cyber risks. *Georgia Law Review*, *50*(2), 547–592.
36. Kesan, J. P. & Hayes, C. M. (2017). Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment. *Minnesota Law Review*, *102*(1), 191–276.
37. Kouns, J. & Minoli, D. (2010). *Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams*. Hoboken: John Wiley & Sons.
38. Kuang-Hua, H., Fu-Hsiang, C. & Wei-Jhou, W. (2016). Exploring the Key Risk Factors for Application of Cloud Computing in Auditing. *Entropy*, *18*(8), 1–24.
39. Kupec, B. (2017). Kako podatke na spletu zaščititi s samo enim geslom. *Manager,* 34–35.
40. Marquette, J. (2015, 5. marec). *Biggest Cyber Security Threat to Law Firms Is Not What You Think*. Pridobljeno 12. julija 2018 iz http://accellis.com/biggest-cyber-securitythreat-to- law-firms-is-not-what-you-think/
41. Marsh. (2014). Helping you understand, quantify and manage cyber risk. London: Marsh Ltd.
42. Miller, K. L. (2016). What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach. *Florida Bar Journal*, *90*(8), 22–31.
43. Nastasiu, C. (2016). Cyber Security Strategies in the Internet Era. *Proceedings Of The Scientific Conference AFASES*, *2*619–624.
44. Oliveira Albuquerque, R., García Villalba, L., Sandoval Orozco, A., Sousa Júnior, R. & Kim, T. (2016). Leveraging information security and computational trust for cybersecurity. *Journal Of Supercomputing*, *72*(10), 3729–3763.

45. Opderbeck, D. W. (2016). Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry. *Maryland Law Review*, *75*(4), 935–983.
46. Perko, B. (2017). Kako se ubraniti pred spletnimi izsiljevalci. *Glas gospodarstva*, 37–41.
47. Raba interneta v Sloveniji. (2009). *Socialni inženiring na internetu*. Pridobljeno 12. aprila 2018 iz http://www.ris.org/db/17/11807/Publikacije/Socialni_in%C5%BE-eniring_na_internetu/?&p1=1504
48. Ramsay, W. (2015). *Assisting small businesses in cyber security planning and implementation.* Pridobljeno 3. januarja 2018 iz https://search-proquest-com.nukweb.nuk.uni-lj.si/docview/1749687023?accountid=16468
49. Russel, R. (2015). Cyber Risks Get Real. *Accounting today*, *29*(7), 41–42.
50. SI-CERT. (brez datuma a). *Varnostne grožnje*. Pridobljeno 14. maja 2018 iz https://www.cert.si/varnostne-groznje/
51. SI-CERT. (brez datuma b). *Vdor*. Pridobljeno 15. maja 2018 iz https://www.cert.si/si/varnostne-groznje/vdor/
52. SI-CERT. (brez datuma c). *Kraja identitete*. Pridobljeno 15. maja 2018 iz https://www.cert.si/si/varnostne-groznje/kraja-identitete/
53. SI-CERT. (brez datuma d). *Phishing kraja podatkov*. Pridobljeno 16. maja 2018 iz https://www.varninainternetu.si/article/phishing-kraja-podatkov/
54. Siegel, C. A., Sagalow, T. R. & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Systems Security*, *11*(4), 33.
55. Stanciu, V. & Bran, F. P. (2015). The Accounting Proffesion in the Digital Era. *Calitatea*, *16*, 546–550.
56. Suhadolnik, G. (2017). Če najdete varnostno luknjo v iOS, vam črni trg plača 1,5 milijona. Pri Applu tega zneska ne boste dobili. *Manager*, 11–13.
57. Swartz, N. (2004). Businesses Improve Cyber Security. *Information Management Journal*, *38*(6), 18.
58. The American Institute of CPAs. (brez datuma). SOC for Cybersecurity. Pridobljeno 29. decembra 2017 iz https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html
59. The Ponemon Institute. (2016, junij). *Cost of Data Breach Study: Global Analysis.* Pridobljeno 16. februarja 2018 iz https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
60. Thompson, R. S. (2016). Cybersecurity: Getting Proactive About Data Vulnerability. *Florida Bar Journal*, *90*(1), 36–37.
61. Tudose, M. (2012). Identifying the Risks Towards Critical Information and Communications Technology Infrastructure. *Buletin Stiintific*, *17*(1), 77–85.
62. Tysiac, K. (2016, 1. november). *New path for CPAs in Cyber Risk Management*. Pridobljeno iz https://www.journalofaccountancy.com/issues/2016/nov/cyber-riskmanagement.html

63. Varni na internetu. (2013, oktober). *Kraja identitete*. Pridobljeno 12. aprila 2018 iz https://www.varninainternetu.si/article/kraja-identitete-2
64. Vintz, S. (2017, 1. december). *CFOs Don't Worry Enough About Cyber Risk*. Pridobljeno iz https://hbr.org/2017/12/cfos-dont-worry-enough-about-cyber-risk.html
65. Werner, R. R. (2017). How to Protect Against Common Cyberattacks and Insure Against Potential Losses. *The CPA Journal*, 87(3), 16–21.
66. Willis. (2013). *Insurance cyber risk*. Kopenhagen: Willis.

PRILOGA

PRILOGA 1:

ANKETNI VPRAŠALNIK

Osnovni podatki o podjetju:

1. Število zaposlenih v podjetju: _____
2. Število strank: _____
3. Prihodki podjetja: _____
4. Vrednost sredstev podjetja: _____
5. Ali ima vaše podjetje dislocirane enote (DA/NE): _____

Vprašanja glede kibernetskega tveganja v računovodski panogi:

1. Na lestvici od 1 do 7 ocenite, kako verjeten se vam zdi kibernetski napad oziroma vdor v informacijski sistem vašega podjetja? (1 neverjeten, ... , 7 zelo verjeten)

   Neverjeten ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 Zelo verjeten

2. Ali ste v podjetju v zadnjih petih letih že zaznali kibernetski napad, to je vdor v informacijski sistem podjetja?
   ☐ Da
   ☐ Ne

3. Ali ste bili tarča vi ali katera od vaših strank?
   ☐ Podjetje
   ☐ Stranka
   ☐ Ne vemo, nismo ugotavljali
   ☐ Nismo zaznali napada

4. Ali imate v podjetju sprejet interni dokument, tako imenovano varnostno politiko, kjer imate zapisane vse pomembne ukrepe, postopke in odgovornosti in ukrepe, ki se nanašajo na varnost podatkov?

   ☐ Da
   ☐ O tem razmišljamo
   ☐ Ne

5. Ali imate v podjetju izdelan načrt, kako ravnati ob morebitnem napadu?
   ☐ Da

☐ O tem razmišljamo

☐ Ne

6. Ali izvajate ukrepe za zagotovitev kibernetske varnosti?

   ☐ Da

   ☐ O tem razmišljamo

   ☐ Ne

7. Ali imate ustrezno informacijsko podporo in zaščito računalnikov (redno posodabljanje programov, ustrezna gesla, nameščeni antivirusni programi)?

   ☐ Da

   ☐ Ne

8. Ali za ustrezno varnost informacijskega sistema skrbite sami ali imate za to sklenjeno pogodbo z zunanjim izvajalcem?

   ☐ Sami

   ☐ Zunanji izvajalci

9. Ali delate varnostne kopije ključnih podatkov kot ukrep za zagotovitev kibernetske varnosti? Če da, kako pogosto?

   ☐ Da, dnevno

   ☐ Da, tedensko

   ☐ Da, mesečno

   ☐ Da, letno

   ☐ Ne

10. Ali dajete posebno pozornost kakovosti gesel za različne uporabniške račune, elektronsko pošto, dostop do oblaka, itd.?

    ☐ Da, zaposleni vedo, kaj pomeni imeti močno geslo, gesla redno spreminjamo in imamo nadzor nad kakovostjo gesel.

    ☐ Ne, vsak zaposleni sam skrbi za svoja gesla in v podjetju ne preverjamo, ali so gesla dovolj močna.

11. Ali izobražujete in usposabljate svoje zaposlene na področju kibernetske varnosti?

    ☐ Da

    ☐ Ne

12. Če da, na kakšen način?

    ☐ Predavanje o kibernetski varnosti

☐ Testiranje zaposlenih z navideznim kontroliranim napadom

☐ Drugo: _____

☐ Ne izvajamo izobraževanja in usposabljanja za zaposlene

13. Če da, kako pogosto?

☐ Večkrat letno

☐ Enkrat letno

☐ Manj kot enkrat letno

☐ Ne izvajamo izobraževanja in usposabljanja za zaposlene

14. Kako visoko ocenjujete kibernetsko tveganje v računovodski panogi (glede na verjetnost nastanka napada in posledice)? Odgovori so grafično prikazani v spodnji tabeli.

☐ 1 - Zelo nizko tveganje

☐ 2 - Nizko tveganje

☐ 3 - Srednje tveganje

☐ 4 - Visoko tveganje

☐ 5 - Zelo visoko tveganje

		VERJETNOST ZA NASTANEK KIBERNETSKEGA NAPADA		
		Zelo verjetno	Verjetno	Malo verjetno
POSLEDICE	Kritične	5 – zelo visoko tveganje	4 – visoko tveganje	3 – srednje tveganje
	Opazne	4 – visoko tveganje	3 – srednje tveganje	2 – nizko tveganje
	Zanemarljive	3 – srednje tveganje	2 – nizko tveganje	1 – zelo nizko tveganje

15. Ali imate sklenjeno zavarovanje za kibernetsko tveganje?

☐ Da

☐ Ne

16. Ali izvajate še kakšen drug ukrep za zagotavljanje kibernetske varnosti? Če da, kateri?

☐ Da, _____

☐ Ne