Rok Bojanc
Borka Jerman-Blažič
Metka Tekavčič

Informacijska varnost v podjetniškem okolju

Potrebe, ukrepi in ekonomika vlaganj

Univerza v *Ljubljani* **EKONOMSKA** FAKULTETA
Založništvo

Znanstvene monografije Ekonomske fakultete

Rok Bojanc, Borka Jerman-Blažič, Metka Tekavčič
Informacijska varnost v podjetniškem okolju: potrebe, ukrepi in ekonomika vlaganj

Založila:	Ekonomska fakulteta v Ljubljani, Založništvo
za založnika:	dekanja prof. dr. Metka Tekavčič
Šifra:	BJT14ZM114
Uredniški odbor:	doc. dr. Mojca Marc (predsednica), doc. dr. Mateja Bodlaj, lekt. dr. Nadja Dobnik, prof. dr. Marko Košak, prof. dr. Vesna Žabkar
Recenzenta:	doc. dr. Tomaž Klobučar prof. dr. Tomaž Turk
Lektorica:	Danijela Čibej
Oblikovanje besedila:	Darija Lebar
Oblikovanje naslovnice:	Robert Ilovar
Tisk:	Copis d.o.o., Ljubljana
Naklada:	40 izvodov

Ljubljana, 2014

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

342.738:658(0.034.2)

BOJANC, Rok
Informacijska varnost v podjetniškem okolju [Elektronski vir] : potrebe, ukrepi in ekonomika vlaganj / Rok Bojanc, Borka Jerman-Blažič, Metka Tekavčič. - El. knjiga. - Ljubljana : Ekonomska fakulteta, 2014. - (Znanstvene monografije Ekonomske fakultete)

ISBN 978-961-240-284-6 (pdf)
1. Jerman-Blažič, Borka 2. Tekavčič, Metka
276133632

KAZALO

UVOD **1**

1 POSLOVNE INFORMACIJE IN NJIHOVO VAROVANJE **11**

1.1 Elektronska oblika in vrednost poslovnih informacij 11

1.2 Osnovni principi varovanja elektronskih informacij 14

1.3 Cilji informacijske varnosti 19

1.3.1 Zaupnost informacij 21

1.3.2 Celovitost informacij 23

1.3.3 Razpoložljivost storitev 24

1.3.4 Avtentičnost 24

1.3.5 Neovrgljivost 28

2 TEHNIKE VAROVANJA IN RAVNANJE Z VARNOSTNIMI TVEGANJI **30**

2.1 Varnostna tveganja 30

2.1.1 Mit popolne varnosti 30

2.1.2 Varnostni incidenti 31

2.1.3 Metode in tehnike za ravnanje s tveganji 36

2.1.4 Izračun pričakovane letne izgube zaradi incidentov (ALE) 40

2.2 Grožnje in ranljivosti informacijske tehnologije 42

2.2.1 Grožnje informacijskim sredstvom 42

2.2.2 Povzročitelji groženj 47

2.2.3 Tehnike napadov 50

2.2.4 Ranljivosti sredstev 51

2.3 Investicije v varnostne ukrepe in rešitve 55

2.3.1 Vrste varnostnih ukrepov 55

2.3.2 Kaj vpliva na izbiro ukrepa? 59

2.3.3 Zmanjšanje tveganja prek zavarovalnice 60

2.4 Pristopi, procesi in sistemi za zagotavljanje varnosti 63

2.4.1 Obvladovanje tveganja 63

2.4.2 Možne obravnave tveganja 64

2.4.3 Proces obvladovanja tveganja 67

3 ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI V POSLOVNIH SISTEMIH IN EKONOMIKA VLAGANJ 69
3.1 Vloga ekonomske vede pri zagotavljanju informacijske varnosti 69
3.1.1 Značilnosti trga IT-izdelkov in storitev 72
3.2 Analiza stroškov in koristi pri vlaganju v informacijsko varnost.....75
3.2.1 Opredelitev stroškov in koristi.....75
3.2.2 Alternativni pristopi.....78
3.3 Ocene o donosnosti vlaganj.....79
3.3.1 Donosnost investicije.....80
3.3.2 Neto sedanja vrednost.....82
3.3.3 Notranja stopnja donosa.....83
3.3.4 Kateri kazalec je najprimernejši?.....84
3.4 Postopek izbire optimalne varnostne rešitve.....86
3.5 Iskanje optimalne stopnje informacijske varnosti.....91
3.6 Praktična uporaba modela za iskanje optimalnega obsega investicije ...97

4 STANDARDI IN SISTEM RAVNANJA Z INFORMACIJSKO VARNOSTJO.....102
4.1 Pregled standardov na področju informacijske varnosti 102
4.2 Sistem vodenja informacijske varnosti.....105
4.3 Standard ISO/IEC 27001.....110
4.4 Revizija informacijske varnosti.....113
4.5 Dobra praksa uvajanja sistema za vodenje varovanja informacij v podjetniškem okolju 115

5 SLOVENSKA REGULATIVA S PODROČJA INFORMACIJSKE VARNOSTI.....119
5.1 Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) 119
5.2 Zakon o elektronskih komunikacijah (ZEKom-1) 120
5.3 Zakon o elektronskem poslovanju na trgu (ZEPT) 125
5.4 Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A).....128
5.5 Zakon o tajnih podatkih (ZTP).....130
5.6 Zakon o varstvu potrošnikov (ZVPot).....133

5.7 Zakon o varstvu osebnih podatkov (ZVOP-1) 133
5.8 Kazenski zakonik RS (KZ-1) 136

ZAKLJUČEK IN NAPOTKI 139

LITERATURA IN VIRI 146

SEZNAM UPORABLJENIH KRATIC IN IZRAZOV 166

KAZALO SLIK

Slika 1: Shematični prikaz triade CIA 20
Slika 2: Postopek izdelave in preverjanja digitalnega podpisa 27
Slika 3: Postopek časovnega žigosanja 28
Slika 4: Postopek izračuna časovnega žiga 29
Slika 5: Tolerančni okvir za kvalitativno vrednotenje tveganj 39
Slika 6: Vrste napadov, ki jih je podjetje že utrpelo 43
Slika 7: Vrste napadov, ki jih je podjetje že utrpelo 44
Slika 8: Rezultati raziskave analiza ranljivosti in ocenitve tveganja 45
Slika 9: Doživeti varnostni incidenti v preteklem letu 46
Slika 10: Zaznani vdori v omrežje in kraje zaupnih podatkov 48
Slika 11: Ali je najhujši varnostni incident povzročil zunanji ali notranji uporabnik 49
Slika 12: Glavni procesi varnostnega ekosistema glede ranljivosti 53
Slika 13: Vrste uporabljenih varnostnih ukrepov v odstotkih glede na delež sodelujočih podjetij 57
Slika 14: Izvedeni koraki po najhujšem incidentu v letu 58
Slika 15: Prikaz odvisnosti med tveganjem, sredstvi, ranljivostmi, grožnjami in ukrepi 59
Slika 16: Različne možnosti obravnave tveganja 65
Slika 17: Grafični prikaz porazdelitve posamezne obravnave tveganja glede na vrednosti L, ρ in R 66
Slika 18: Postopek izbire ustrezne obravnave tveganja 68
Slika 19: Iskanje optimalne rešitve med višino stroškov varnostnega dogodka in stroški ukrepa (tj. obsega naložbe v informacijsko varnost) 75

Slika 20: Delež uporabe ROI, NPV in IRR za varnostni kazalec 85
Slika 21: Model analize tveganja 86
Slika 22: Merjenje koristi in stroškov informacijske varnosti 92
Slika 23: Delež IT proračuna, namenjen informacijski varnosti 93
Slika 24: Vpliv omejitve proračuna na investicijo v informacijsko varnost 94
Slika 25: Delež podjetij, ki formalno dokumentirajo varnostno politiko 107
Slika 26: Model PDCA za SVIV 108
Slika 27: Hierarhija dokumentacije sistema SVIV 109
Slika 28: Relacije med standardi družine SVIV 113

KAZALO TABEL

Tabela 1: Primerjava prednosti in slabosti kvantitativnih in kvalitativnih metod za obvladovanje tveganja 40
Tabela 2: Primeri groženj različnih povzročiteljev 49
Tabela 3: Primeri različnih vrst varnostnih ukrepov 56
Tabela 4: Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov ... 99
Tabela 5: Izračun kazalcev ROI, NPV in IRR za posamezne ukrepe 99
Tabela 6: Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov . 100
Tabela 7: Izračun kazalcev ROI, NPV in IRR za posamezne ukrepe 101

UVOD

Za današnje poslovanje organizacij je povezanost z različnimi kompleksnimi okolji, kot je internet, ne le izbira, temveč nujnost za preživetje na trgu. S povezanostjo z drugimi okolji pa organizacije dobršen del svojih sredstev (podatkovne baze, računalniški programi, proizvodnji procesi, podatki o strankah, poslovne skrivnosti idr.) izpostavijo različnim grožnjam. Vsak dan smo priča primerom, ko lahko posameznik ali organizacija postane žrtev raznih napadov na informacije in informacijske sisteme. Glede na raziskavo BIS (2013) je kar 93 % sodelujočih večjih organizacij in 87 % manjših podjetij odgovorilo, da so v preteklem letu v svojem sistemu ali omrežju zaznali vsaj en varnostni incident. Pri tem so varnostni incidenti lahko zelo različni, od okužbe z računalniškim virusom in drugo zlonamerno kodo do zlorabe s strani zaposlenih, kraje opreme, napada z ohromitvijo storitve, neavtoriziranega dostopa do podatkov in omrežij idr. Porast t. i. kibernetske kriminalitete, ki se danes kaže predvsem v pridobivanju koristi posameznih kriminalnih združb, je v zadnjih letih presenetil tako organe pregona kot posameznike in podjetja, ki delujejo na spletu.

Podjetja in druge organizacije se pred varnostnimi grožnjami zavarujejo tako, da vzpostavijo določene varnostne rešitve. Zaradi nepredvidljive narave in rasti varnostnih groženj pa je izbira ustrezne varnostne rešitve lahko težja, kot je videti na prvi pogled. Kot ugotavljata Gordon in Loeb (2005), se odgovorne osebe za informacijsko varnost v podjetju o izbiri varnostnih rešitev pogosteje odločajo na podlagi osebnega občutka kot pa na podlagi resne ekonomske analize o upravičenosti vlaganj.

Informacijska varnost se tradicionalno šteje za tehnično disciplino, katere namen je zagotoviti najvišjo raven varnosti (McGraw, 2006). Kot ugotavljajo mnogi raziskovalci (Anderson, 2001; Schneier, 2004b; Cavusoglu, Cavusoglu & Raghunathan, 2004a), pa tehnologija sama ne more zadovoljivo rešiti varnostnih problemov. Anderson (2001) je bil eden izmed prvih avtorjev, ki je zagovarjal stališče, da se morajo problemi informacijske varnosti obravnavati ne le s tehnološke, ampak tudi z ekonomske perspektive. Tak pristop omogoča managerjem v podjetjih boljše razumevanje varnostnih investicij.

Ko gledamo na sistem informacijske varnosti z ekonomskega stališča, lahko najdemo odgovore na mnoga vprašanja, na katera zgolj s tehnično razlago ne moremo zadovoljivo odgovoriti. Kako lahko managerji določijo optimalno raven financiranja pri zaščiti in varovanju informacij, ki jih obdeluje in hrani informacijska tehnologija v organizaciji in podjetju? Kako naj se to financiranje porazdeli med različnimi projekti, v katerih so vgrajene informacijske varnostne rešitve? Kako naj vodja informacijske varnosti učinkovito vodi proces obvladovanja varnostnih tveganj in ravnanja z informacijsko varnostjo? Z odgovori na ta in še mnoga podobna vprašanja, povezana z investicijami v informacijsko varnost, se ukvarja osrednji del te monografije.

Zgodovina oblikovanja področja informacijske varnosti. Odkar je Ross Anderson (2001) pokazal pomen ekonomskih vidikov za informacijsko varnost, se je to raziskovalno področje začelo močno razvijati. Ekonomika informacijske varnosti je razmeroma novo raziskovalno področje, ki uporablja ekonomsko teorijo in modele za analizo spodbud med sodelujočimi deležniki (Bojanc & Jerman-Blažič, 2008; Anderson & Moore, 2006; Anderson, Böhme, Clayton & Moore, 2007). Moore in Anderson (2011) sta podrobno preučila ekonomske izzive, s katerimi se informacijska varnost sooča zaradi neusklajenih spodbud, asimetrije informacij in eksternalij omrežja. Kot sta avtorja odkrila že v svoji predhodni raziskavi (Anderson & Moore, 2008), so v informacijskih okoljih pogoste neusklajene spodbude med tistimi, ki so odgovornimi za varnost, in tistimi, ki imajo zaradi varnosti dejanske koristi. Kwon in Johnson (2012) sta ugotovila, kako varnostni viri, zmogljivosti sistemov in kulturne vrednote vplivajo na uspešnost varovanja in zagotavljanja skladnosti s predpisi.

V zadnjem času se je bistveno spremenil tudi pogled organizacij na informacijsko varnost. V preteklosti so organizacije gledale na informacijsko varnost kot na strošek, v zadnjih letih pa jo večina organizacij razume kot naložbo (Tordoff, 2006). Tak pogled so zagovarjali že Cavusoglu, Mishra in Raghunathan (2004b), ki trdijo, da je treba informacijsko varnost gledati ne samo kot strošek, ampak kot dodano vrednost, ki podpira in omogoča izvajanje e-poslovanja. Obenem avtorji tudi trdijo, da lahko varno okolje za informacijske in transakcijske tokove ustvarja vrednost za podjetja in njihove partnerje. Ker višja raven informacijske

varnosti pomeni dodatne stroške, je pomembno, da organizacije ugotovijo in določijo optimalno stopnjo naložb v informacijsko varnost.

Izračun optimalne investicije v informacijsko varnost je relativno nov ukrep pri načrtovanju uporabe in nabave informacijske tehnologije v podjetjih. Demetz in Bachlechner (2012) sta identificirala, primerjala in ovrednotila različne pristope, ki se v literaturi navajajo za vrednotenje investicij v informacijsko varnost. Ti pristopi imajo iste cilje – zagotoviti optimalnost investiranja, vendar se razlikujejo po tem, kako pridejo do ciljev.

Za določitev optimalne stopnje naložb v informacijsko varnost je treba obravnavati optimalna razmerja med stroški naložb in stroški zaradi povzročenih incidentov. Stroški naložbe vključujejo ceno potrebne strojne opreme, programske opreme in delovne sile. Oceno celotnih stroškov varnostnih incidentov je mogoče pridobiti na več načinov. Nekateri pristopi poskušajo kvantitativno opredeliti kratkoročne in dolgoročne stroške ali materialne in nematerialne stroške, medtem ko nekatere druge metode uporabljajo za kvantitativno ovrednotenje stroškov teorije učinkovitosti trga in vrednotenje tržne vrednosti podjetja (Bojanc & Jerman-Blažič, 2011). Pri tem Farahmand, Navathe, Sharp in Enslow (2003) opozarjajo, da je izguba tržne vrednosti podjetja v dnevih, ki sledijo obvestilu o varnostnem incidentu, zgolj približna vrednost dejanskih stroškov zaradi incidenta.

Brecht in Nowey (2012) obravnavata štiri pristope za kategorizacijo in določitev stroškov informacijske varnosti v podjetju. Ugotovila sta štiri vidike stroškov varovanja informacij: stroški, ki so povzročeni zaradi varnostnih incidentov, stroški za upravljanje informacijske varnosti, stroški, ki so povezani z merjenjem informacijske varnosti, ter stroški kapitala, ki nastanejo zaradi varnostnih tveganj. Anderson je s sodelavci (2012) predstavil prvo sistematično študijo stroškov kibernetske kriminalitete. Za vsako od glavnih kategorij kibernetske kriminalitete so določili, kaj so in kaj niso neposredni stroški, posredni stroški in stroški zaščite.

Pomembno vprašanje je ne samo koliko vlagati, temveč tudi kdaj vlagati. V ta namen so Ioannidis, Pym in Williams (2011) predstavili analitično rešitev

problema iskanja optimalnega časa za vlaganje ob navzočnosti obstoječih in prihodnjih groženj. Predstavili so koncept investicijskega cikla v informacijsko varnost, ki je analogen klasični keynesianski obravnavi togosti.

Gordon in Loeb (2005) sta pripravila konkretnejše smernice za vrednotenje stroškov informacijske varnosti, ki so organizacijam lahko v pomoč. Obenem pojasnjujeta vlogo tveganj pri dodeljevanju virov, strategije za zmanjšanje učinka varnostnih incidentov ter pristop za določitev poslovne vrednosti, ki omogoča zagotovili prihodnja financiranja. Pomen obvladovanja tveganj za sodobno poslovanje organizacij poudarjajo tudi mnogi standardi (SIST ISO 31000, 2011; SIST ISO 27001, 2013; NIST 800-27, 2004), ki obenem podajajo tudi vodič skozi različne faze ocene ter obravnave tveganja.

Potencialno tveganje za varnostne incidente se najpogosteje določa glede na verjetnost, da se incident zgodi, in glede na morebitno škodo. Hoo (2000) je predlagal enega izmed prvih analitičnih okvirov odločanja za ocenjevanje različnih varnostnih IT-politik. V svoji raziskavi je primerjal skupino varnostnih ukrepov ali politik ter za vsako politiko poskušal najti najboljši kompromis med stroški in koristmi. Longstaff, Chittister, Pethia in Haimes (2000) (upoštevajoč kompleksnost problema) so predlagali hierarhični model za oceno varnostnih tveganj v informacijski tehnologiji. Gordon in Loeb (2002b) pa sta zatem predlagala ekonomski model, ki določa optimalno stopnjo vlaganj v informacijsko varnost, ki temelji na izračunu mejnih koristi investicij v informacijsko varnost. Kot navajata, naj organizacija vlaga v informacijsko varnost samo do točke, do katere so mejne koristi investicije enake mejnim stroškom. Dokler pa je mejna korist večja od mejnih stroškov, se organizacijam splača investirati.

Mizzi je pozneje (2010) zagovarjal, da je investicija v informacijsko varnost ekonomsko upravičena le, če so izdatki za varnost manjši od skupnih letnih izgub. Vendar sta Gordon in Loeb (2002b) ocenila, da je optimalna količina investicij v informacijsko varnost v obsegu do 37 % pričakovanih izgub, nastalih zaradi varnostnega incidenta. Splošno veljavnost tega pravila je deset let pozneje dokazal Baryshnikov (2012). Willemson (2006, 2010) je to oceno razširil in z omilitvijo nekaterih prvotnih zahtev (Gordon & Loeb, 2002b) opozoril na situacije, kjer je upravičeno, da izdatki na področju informacijske varnosti lahko

segajo tudi do 100 % vrednosti pričakovanih izgub. Te ugotovitve so bile tudi uspešno dokazane z empiričnimi raziskavami (Tanaka, Matsuura & Sudoh, 2005; Tanaka, Liu & Matsuura, 2006). Nekateri drugi pristopi pa pri izračunu ocene investicij v informacijsko varnost temeljijo na izračunu finančnih kazalcev, kot je donosnost investicije (Bojanc & Jerman-Blažič, 2008; Sonnenreich, Albanese & Stout, 2006).

Alternativna metoda za oceno stroškov tveganja uporablja tako imenovano teorijo iger (Cavusoglu et al., 2004a; Böhme & Moore, 2009). Cavusoglu zagovarja, da tradicionalni analitični pristopi odločanja za ocenjevanje investicij v informacijsko varnost obravnavajo varnostno tehnologijo kot črno škatlo in ne upoštevajo razlike med naložbami v rešitve informacijske varnosti od splošnih naložb v IT. V svojih študijah ta avtor obravnava informacijsko varnost kot igro med organizacijo in morebitnimi napadalci, ki imajo motiv povzročiti organizaciji škodo – lahko gre za osebno korist ali le za zadovoljstvo.

Namen in cilji raziskave. V monografiji obravnavamo področje ekonomike informacijske varnosti (ta v zadnjih letih vse bolj pridobiva na veljavi) kot del znanstvene discipline informacijska varnost. V raziskavi smo za namen študije, ki opredeljuje to znanstveno področje, obdelali informacijske grožnje, varnostna tveganja, pristope, procese in sisteme za zagotavljanje varnosti ter različne metode za analizo stroškov in koristi pri vlaganju v informacijsko varnost ter merjenje donosnosti vlaganj. Poglobljena analiza pa je namenjena tudi predstavitvi pomena razmeroma novega raziskovalnega področja ekonomike informacijske varnosti za varno e-poslovanje med podjetji in organizacijami.

Namen znanstvene monografije je preučiti in analizirati različne metode in modele za vrednotenje vlaganj v informacijsko varnost, da bi preprečili varnostna tveganja, ter predstaviti novo metodo za reševanje teh problemov s pomočjo splošnega matematičnega modela za kvantitativno vrednotenje naložb v različne varnostne ukrepe in izbor optimalne varnostne rešitve. Z investicijami v informacijsko varnost organizacije se zmanjšujejo varnostna tveganja, ki grozijo njihovim informacijskim sredstvom. Predstavljeni kvantitativni model lahko organizacijam pomaga pri odločitvah o vlaganjih, ki so namenjena zagotavljanju varnosti informacij. Organizacije lahko pri zagotavljanju ustrezne ravni

informacijske varnosti izbirajo med različnimi rešitvami, kot so tehnične rešitve (požarni zid, protivirusna zaščita, varni prostori …), organizacijske rešitve (politike, pravilniki), izobraževanja zaposlenih, zavarovanja idr.

Pri investicijah v varnostne rešitve sta za organizacijo pomembna dva pristopa, ki zahtevata ustrezne odločitve. Prvi je povezan z višino investicij, ki jih organizacija nameni za informacijsko varnost, drugi pa s tem, v katere rešitve naj ta sredstva investira. Na primer, organizacija se odloči, da bo za informacijsko varnost namenila 2.000 €, s čimer želi zmanjšati tveganje pred neželeno zlonamerno programsko opremo. Katera rešitev za ta denar je za organizacijo optimalna? Ali naj investira v programsko rešitev, pripravi ustrezen interni pravilnik, izvede seminar za ozaveščanje zaposlenih ali izbere kakšno drugo rešitev? V monografiji raziskujemo, ali lahko organizacija z enim standardnim modelom primerja različne varnostne rešitve in si tako pomaga pri sprejemanju odločitve, katera rešitev je v določenih okvirih zanjo optimalna izbira.

V raziskavi se za potrebe optimalnega modela pri izbiri odločitve osredotočamo na različne načine merjenja donosnosti vlaganj (donosnost investicije, neto sedanja vrednost in notranja stopnja donosa) in poskušamo ugotoviti, ali za določitev optimalne rešitve zadostuje uporaba zgolj enega pristopa ali pa jih je treba uporabiti več in primerjati možne rezultate izračunov. Raziskava vključuje tudi praktični primer izračuna optimalne rešitve na podlagi predstavljenega kvantitativnega modela.

Raziskava podaja tudi pregled najpomembnejših standardov s področja informacijske varnosti ter s tem povezane slovenske zakonodaje. Tako seznani bralca s pravnimi vidiki in stanjem na področju splošnoveljavne standardizacije.

Za dosego zastavljenih ciljev podajamo v raziskavi tri hipoteze.

- **Hipoteza 1** – Z uporabo standardiziranega modela ocene vlaganj je mogoče določiti optimalni varnostni ukrep za zmanjšanje informacijsko-varnostnih tveganj.
- **Hipoteza 2** – Za določitev stroškovno optimalnega varnostnega ukrepa za določeno grožnjo je treba upoštevati in primerjati različne kazalce za merjenje donosnosti vlaganj.

- **Hipoteza 3** – Čeprav uvedbe varnostnih ukrepov podjetju ne prinašajo neposredne finančne koristi, je za odločanje o investicijah v varnostne rešitve mogoče učinkovito uporabiti ekonometrične metode za analizo stroškov in koristi.

Za potrditev hipotez so v raziskavi opredeljeni ključni elementi informacijske varnosti, poseben poudarek pa je na kvantitativnem pristopu k obvladovanju varnostnih tveganj, na modeliranju vlaganj v informacijsko varnost, na analizi stroškov in koristi ter na različnih metodah merjenja informacijske varnosti. Predstavljen je tudi matematični model za kvantitativno analizo vlaganj v informacijsko varnost v poslovnih sistemih. Za potrditev hipotez je opravljen empiričen preizkus predstavljenega modela v konkretnem podjetju.

Prispevek raziskave k znanosti. Izvedena raziskava je znanstveni prispevek, v katerem podajamo okvir za učinkovito ravnanje z informacijsko varnostjo v podjetjih na podlagi originalnega razvitega modela za podporo odločanju pri izbiri varnostne tehnologije in drugih varnostnih ukrepov, ki je bil preverjen v praksi in v znanstvenih publikacijah (Bojanc, 2010; Bojanc & Jerman-Blažič, 2013; Bojanc, Jerman-Blažič & Tekavčič, 2012a). Model omogoča kvantitativno vrednotenje varnostnih tveganj in ustreznih varnostnih ukrepov, ki preprečujejo posamezna tveganja, pri čemer model upošteva vrednost investicije in kvantitativno analizo varnostnih tveganj. Rezultat uporabe modela je ocena donosnosti posameznih ukrepov ter njihovo medsebojno vrednotenje.

Pomemben prispevek znanstvene monografije k znanosti je razvit postopek za izbiro stroškovno optimalne varnostne rešitve, ki temelji na predstavljenem kvantitativnem modelu. Uporaba postopka je v monografiji praktično prikazana na dveh konkretnih primerih vlaganja v informacijsko varnost za zaščito pred virusi in pred spletnim ribarjenjem (angl. *phishing*). Postopek podaja priporočila managerjem, ki se ukvarjajo z ekonomskimi in finančnimi pogledi na zagotavljanje informacijske varnosti. Prispevek k znanosti se nanaša tudi na pregled ekonometričnih metod vrednotenja za potrebe predlaganega modela ter na analizo najpomembnejših mednarodnih standardov in slovenske zakonodaje na področju informacijske varnosti.

Naš prispevek lahko razumemo tudi kot spodbudo managerjem in drugim, ki so v podjetjih odgovorni za področje informacijske varnosti in obvladovanje varnostnih tveganj, da bi svoje odločitve sprejemali na podlagi kvantitativnega pristopa za vrednotenje varnostnih tveganj ter analize stroškov in koristi pri izboru ustreznih varnostnih rešitev.

Ker je vprašanje iskanja ekonomsko optimalnih varnostnih ukrepov in tehnologij v družbi čedalje bolj pereč problem, lahko predstavljena rešitev tako teoretično kot praktično veliko pripomore k reševanju tovrstne problematike. Managerjem v podjetjih omogoča ovrednotiti tveganja v obliki finančnih vrednosti, s čimer lahko dobijo boljši vpogled v finančne učinke vlaganj ter nazornejšo predstavitev pričakovanih rezultatov in vpliva vlaganj na poslovanje.

Monografija je tako koristen vir informacij za vse, ki se ukvarjajo z vodenjem informacijske varnosti v podjetjih: za finančne managerje, ki so odgovorni za dodelitev sredstev projektom informacijske varnosti, in za druge strokovnjake informacijsko-komunikacijske tehnologije (IKT), ki so v podjetjih vključeni v proces odločanja o ravnanju z informacijsko varnostjo. Monografija je lahko dragocen vir tudi za študente, ki se pri predmetih srečujejo z informacijsko varnostjo in jo želijo podrobneje spoznati še z ekonomskega in finančnega vidika.

Monografija od bralca ne pričakuje predhodnega znanja s področja ekonomike in informacijske varnosti. V nekaterih poglavjih, ki prikazujejo praktično uporabo razvitega modela, je vsebina izražena z matematično formulacijo, ki za potrebe te knjige ni zahtevna in je podrobno obrazložena.

Uporabljena metodologija. Pri znanstveni študiji, ki smo jo izvedli, da bi potrdili ali zavrnili postavljene hipoteze, smo uporabili več različnih metod znanstvenega raziskovanja. Opravljena raziskovalna dela so sestavljena iz teoretičnega in praktičnega dela. Teoretični del prinaša izhodišča in dosedanja spoznanja s področja informacijske varnosti in obvladovanja tveganja. Pri tem smo uporabili metodo deskripcije, s pomočjo katere opišemo teorijo, pojme in ugotovljena dejstva, ter metodo klasifikacije, s katero definiramo pojme, ki so predmet raziskovanja v raziskavi.

Zanima nas, kako se izhodišča in spoznanja različnih avtorjev s področja ekonomike informacijske varnosti (Anderson et al., 2012; Böhme & Moore, 2009; Brecht & Nowey, 2012; Ioannidis et al., 2011; Gordon & Loeb, 2002b; Soo Hoo, 2000; Longstaff et al., 2000; Gordon & Loeb, 2005; Butler, 2002; Xie & Mead, 2004; Cavusoglu et al., 2004b; Garcia & Horowitz, 2006; Gal-Or & Ghose, 2005; Horowitz & Garcia, 2005; Andrijcic & Horowitz, 2004; Willemson, 2006; Huang, Hu & Behara, 2005a; Huang, Hu & Behara, 2005b) med seboj dopolnjujejo ali razlikujejo ter kako so teoretični koncepti preizkušeni v praksi (Tanaka, 2005; Tanaka et al., 2005; Tanaka et al., 2006; Ioannidis, Pym & Williams, 2009). Na osnovi že obstoječih spoznanj avtorjev in znanstvenega pristopa dedukcije smo prišli do novih, izvirnih sklepov. Pri tem smo uporabili metodo kompilacije, s katero s povzemanjem spoznanj in sklepov drugih avtorjev v zvezi z izbranim raziskovalnim problemom oblikujemo nova stališča, ter metodo komparacije, s katero primerjamo dela in raziskave različnih avtorjev.

Na podlagi razvitega modela za podporo odločanju pri izbiri varnostnih ukrepov razvijemo postopek za izbiro stroškovno optimalne varnostne rešitve. V nadaljevanju teoretični del nadgradimo z analitičnimi metodami in empiričnimi ugotovitvami, ki so objavljene v različnih raziskavah in poročilih (BIS, 2013; CSI, 2011; DSCI, 2009; BERR, 2008; DTI, 2006). Sledi praktični del, v katerem za določeno podjetje prikažemo praktično uporabo razvitega postopka za izbiro optimalnega varnostnega ukrepa na primeru dveh konkretnih groženj (okužba z računalniškimi virusi ter spletnim ribarjenjem). Na koncu naredimo sintezo ugotovitev in analiz preteklih študij in raziskav.

Vsebina monografije je naslednja. V prvem poglavju so opredeljene informacije v poslovnem okolju, kaj so informacije v elektronski obliki, kakšno vrednost imajo za podjetje, kako jih lahko varujemo, kaj so osnovna načela informacijske varnosti ter kaj so ključna vprašanja, povezana z varnostjo v poslovnem okolju. V drugem poglavju so podrobneje razčlenjena varnostna tveganja, kaj jih povzroča, kakšne posledice lahko imajo ter kaj podjetja lahko storijo, da bi zmanjšala tveganja in morebitne posledice. V tretjem poglavju se osredotočimo na ekonomski vidik informacijske varnosti ter si ogledamo možnosti, ki nam jih njegova uporaba omogoča. Ekonomski okvir za ravnanje z informacijskimi

sredstvi temelji na principu analize stroškov in koristi. Ta okvir omogoča oceno donosnosti investicij v informacijsko varnost, izbiro optimalne varnostne rešitve, medsebojno ekonomsko primerjavo različnih varnostnih ukrepov ter oceno optimalne stopnje varnosti za posamezno podjetje. Četrto poglavje je posvečeno standardom s področja informacijske varnosti ter podaja splošen pristop za uvajanje varnostnih rešitev v podjetniškem okolju. Peto poglavje vsebuje pregled slovenske regulative na področju informacijske varnosti, zadnje poglavje pa je namenjeno zaključnim mislim, ki so povezane s pomembnimi vprašanji informacijske varnosti.

Pri uporabi določene terminologije smo se odločili za naslednje: za prevod izraza *information security* nekateri slovenski avtorji poleg izraza *informacijska varnost* (na primer Islovar, SiQ, SIST) uporabljajo tudi izraz *varovanje informacij* (na primer Palsit d.o.o.). Avtorji smo imeli težko nalogo, kateri izraz uporabiti, saj se oba pogosto uporabljata v slovenski literaturi. Po razmisleku smo se odločili za izraz informacijska varnost, saj po našem mnenju bolje opisuje področje, izraz varovanje informacij pa bolj povezujemo z aktivnostmi. Poleg tega se ta izraz, ki ga uporabljamo v monografiji, uporablja tudi v slovenskem prevodu standarda ISO/IEC 27001 (SIST, 2013).

Druga terminološka dilema pa je bila povezana z uporabo izraza *management*, ki ga slovenska strokovna literatura na področju poslovne informatike zelo pogosto prevaja kot *upravljanje*, kar se v nekaterih primerih izkaže za neustrezno. Ob upoštevanju utemeljitve stroke na področju managementa smo za izraz *information security management* uporabili prevod *vodenje informacijske varnosti* ter za izraz *risk management* prevod *obvladovanje tveganja*.

1 POSLOVNE INFORMACIJE IN NJIHOVO VAROVANJE

1.1 Elektronska oblika in vrednost poslovnih informacij

Podjetja in organizacije pri svojem poslovanju uporabljajo različna **sredstva**. Pri tem se izraz sredstvo v skladu s standardi ISO s področja varovanja informacij uporablja zelo na široko, saj je sredstvo pravzaprav vse, kar ima za podjetje določeno vrednost (ISO 27000, 2014). K sredstvom prištevamo f**izična sredstva** (računalniška strojna oprema, naprave za komunikacijo in hrambo, nosilci podatkov, zgradbe in lokacije), **programska sredstva** (operacijski sistemi, programske aplikacije in storitve, ki obdelujejo, shranjujejo ali posredujejo informacije, in razvojna orodja), **informacijska sredstva** (znanje ali podatek, ki ima določeno vrednost za podjetje), **storitve** (informacijski sistemi za obdelavo in hrambo informacij, podporni sistemi: ogrevanje, osvetlitev, fizično varovanje, elektrika in klimatske naprave), **človeški viri** (zaposleni v podjetju, ki imajo veščine, znanje in izkušnje, ki jih je težko nadomestiti) in **neopredmetena sredstva** (ugled in podoba podjetja, morala zaposlenih, blagovne znamke in produktivnost zaposlenih).

V tem poglavju se osredotočamo na informacijska sredstva oziroma informacije. **Informacija** je znanje ali podatek, ki ima za podjetje določeno vrednost. Lahko je pravzaprav vse, kar lahko digitaliziramo, se pravi, kodiramo v zaporedje bitov (Shapiro & Varian, 1998). Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, 2004) definira, da so podatki v elektronski obliki tisti podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.

Za podjetja je elektronska oblika informacij ključen pogoj za prehod v elektronsko poslovanje in delovanje na trgu v sodobnem omreženem gospodarstvu. Informacije v elektronski obliki omogočajo podjetjem hitrejše izvajanje poslovnih procesov. Postopki, ki temeljijo na delu s klasičnimi papirnimi dokumenti, so dolgotrajni in izmenjava papirnih dokumentov med podjetji se lahko meri v dnevih. Prenos informacij v elektronski obliki med dvema lokacijama, ki sta med seboj lahko oddaljeni več tisoč kilometrov, pa se izvede v manj kot sekundi. Elektronska oblika tudi občutno zmanjšuje napake pri ravnanju z informacijami, saj ni potrebe po ročnem vnosu informacij na papirju v informacijski sistem

podjetja. Sodobno gospodarstvo danes ne more delovati in poslovati brez elektronske oblike informacij in procesov, ki so povezani z njimi. Pomembna značilnost elektronskih informacij je tudi zmanjšanje prostora za njihovo hrambo. Vse informacije, ki so zbrane v veliki omari, polni fasciklov, se lahko shranijo na velikost trdega diska, ki je danes v vsakem računalniku. Ključna prednost uporabe elektronskih dokumentov v sodobnem poslovanju med podjetji pa je avtomatizacija poslovnih procesov. Podjetja se med seboj povezujejo z izmenjavo različnih elektronskih dokumentov, vsak elektronski dokument pa predstavlja določeno aktivnost, ki je del poslovnega procesa. Avtomatizacija obdelave elektronskih dokumentov je ključna za učinkovito poslovanje podjetij.

Kot smo navedli, ima za podjetje vsako sredstvo določeno vrednost. Za določanje vrednosti sredstev je razvitih več metod, ki različno vrednotijo sredstva. Nekateri pristopi pri vrednotenju sredstev, ki se nanašajo na probleme informacijske varnosti, upoštevajo stroške izdelave (oziroma ustvarjenja) sredstev, drugi upoštevajo nastale stroške zaradi varnostnega incidenta, medtem ko poskušajo tretji pristopi zajeti vse učinke incidenta na prihodke in stroške podjetja ali organizacije (Mercuri, 2003; Power, 1999; Campbell, Gordon, Loeb & Zhou, 2003; Soo Hoo, 2000; Garg, Curtis & Halper, 2003; Cavusoglu et al., 2004b).

Sredstva so lahko zelo različna in vrednotenje nekatere vrste sredstev je lahko preprostejše kot vrednotenje drugih. Ne glede na izbrani pristop vrednotenja lahko podjetje dokaj preprosto določi vrednost svojih fizičnih in programskih oziroma elektronskih sredstev, saj lahko hitro izračuna njihovo knjigovodsko vrednost v določenem trenutku. Vrednost sredstev se meri v denarju, pri čemer se upošteva tudi njihova amortizacija.

Težje pa je z informacijami, saj se njihova vrednost običajno ne da določiti enako kot vrednost fizičnih in programskih sredstev. Informacija ima lahko vrednost za podjetje s tem, da pomaga podjetjem do večje produktivnosti, kar pomeni, da določa načrt novega izdelka oziroma procesa (ter vsebuje pomembno intelektualno vrednost), pomaga do boljšega marketinga, boljših finančnih odločitev, boljšega nadzora aktivnosti in procesov ali pomaga pri ravnanju z zaposlenimi. Določene informacije so za podjetje strateškega pomena, kot na primer informacije o skrivnih receptih, produktih v razvoju, marketinških

načrtih, združitvah in prevzemih, o osebju in demografiji strank. Take strateške informacije so ključne za razvoj ter rast podjetja in imajo za podjetja še posebno veliko vrednost (Gordon & Loeb, 2005). Vse te informacije v poslovnem okolju imajo določeno vrednost, ki je večja ali enaka nič.

Dodatna značilnost informacij je, da so drage za ustvarjanje, po drugi strani pa poceni za reproduciranje (Shapiro & Varian, 1998). Na primer, pisanje knjige lahko naročnika ali založnika stane nekaj deset tisoč evrov, knjiga pa se lahko natisne za vsega nekaj evrov. Ali pa snemanje filma, ki lahko stane več milijonov evrov, na disk Blu-Ray ali DVD pa se presname za vsega nekaj centov. Z ekonomskega stališča ustvarjanje informacij zahteva visoke fiksne in nizke mejne stroške. Strošek izdelave prve kopije informacij je lahko ogromen (nov izdelek, načrti, zasnove procesov ipd.), strošek izdelave (oziroma reprodukcija) nadaljnjih kopij pa je ponekod lahko zanemarljiv.

Taka struktura stroškov informacij pomeni, da njihova vrednost ne more temeljiti na stroških izdelave informacije, saj so ti stroški za nadaljnje kopije lahko blizu nič, temveč mora temeljiti na vrednosti za podjetje oziroma za njegove kupce ali uporabnike. Ne glede na to, ali je informacija namenjena poslovni rabi ali za zabavo, so ljudje pripravljeni zanjo plačati. Vrednost informacije se lahko predstavi tudi kot izguba, ki bi jo podjetje utrpelo zaradi potencialne izgube te informacije.

Anderson (2008) je na podlagi takšnega videnja strukture stroškov informacij razložil, zakaj je na internetu toliko informacij na voljo brezplačno. V konkurenčnem ravnovesju, po Andersonu, naj bi bila cena informacije mejni strošek proizvodnje, ki pa je v digitalni obliki skoraj nič, zato je nič pravična cena. Če več konkurenčnih podjetij ponuja na primer program za obdelavo slik, operacijski sistem ali zemljevid v elektronski obliki, lahko proizvod razmnožujejo praktično brez dodatnih stroškov, zato lahko cene razmnoženih proizvodov znižajo skoraj brez omejitev. Shapiro in Varian (1998) pa ugotavljata, da se je ravno to zgodilo z enciklopedijami v elektronski obliki. Kot navajata, je 32 knjig enciklopedije Britannica stalo 1.600 USD, nato pa je Microsoft ponudil enciklopedijo Encarta za 49,95 USD, kar je Britannico prisililo k poceni izdaji svoje enciklopedije na zgoščenki. Sedaj pa je na internetu brezplačno na voljo

vsebina enciklopedije Wikipedija, ker so se posamezni ustvarjalci prostovoljni odpovedali vrednosti informacij, ki so jih naložili v Wikipediji. Tako je ta enciklopedija nastala s prispevki številnih avtorjev in nizko plačanega dela urednikov.

Veliko industrij sodobnega trga, ki imajo visoke fiksne in nizke mejne stroške, uporablja danes oglaševalski ali storitveni model poslovanja, v katerem so dobrine na voljo brezplačno, denar pa prihaja od oglaševanja ali iz drugih vzporednih virov na drugih trgih. Tak primer je medijska industrija, saj veliko časopisov dobi večino prihodkov od oglaševanja, zato ponujajo na internetu brezplačne spletne izdaje časopisnih člankov in novic vzporedno s plačljivo tiskano izdajo.

Primer takega pristopa je tudi operacijski sistem Linux, ki ga podjetja ponujajo brezplačno, denar pa služijo prek plačljive podpore za delovanje operacijskega sistema na opremi svojih strank. Veliko Linuxovih razvijalcev dela na projektu brezplačno v svojem prostem času med študijem, ker njihovo sodelovanje na projektu izboljša njihove reference ter izkušnje in jim to po končanem študiju pomaga do boljše zaposlitve.

1.2 Osnovni principi varovanja elektronskih informacij

Sodobna informacijska tehnologija omogoča, da podjetja poslujejo hitreje, učinkoviteje in ceneje. Zaradi povečanega obsega elektronskega poslovanja postajajo podjetja čedalje bolj odvisna od zanesljivosti in stabilnosti delovanja svojih informacijskih sistemov in od zanesljive zaščite poslovnih informacij, ki jih obdelujejo. Pri uporabi različnih modelov elektronskega poslovanja (B2B, B2C in B2G) se vsi sodelujoči zanašajo na to, da je prenos informacij med partnerjema varen in da je varna tudi hramba zaupnih informacij. Pri tem je ključna vzpostavitev zaupanja med partnerji, ki sodelujejo v elektronskih transakcijah.

Ker imajo informacije za podjetje določeno vrednost, jih je treba ustrezno varovati. Pri tem je poznavanje vrednosti informacij osnova za odločanje o tem, koliko in kako jih varovati, ter za oceno finančnih izgub, ki bi nastale ob morebitnem varnostnem incidentu (Su, 2006). Pri tem je prvo pravilo zagotavljanja

informacijske varnosti, da naj podjetje za varovanje ne porabi več od vrednosti tistega, kar dejansko varuje (Crume, 2001).

Informacijska varnost je široko področje, ki danes zajema mnoga podpodročja: od varovanja omrežja in infrastrukture, varovanja aplikacij in podatkovnih zbirk, varnostnega testiranja, revizije informacijskih sistemov, zaščite in varovanja osebnih podatkov ter planiranja neprekinjenega poslovanja do digitalne forenzike in postopkov za preprečevanje računalniške kriminalitete.

Čeprav se z varovanjem informacij ne srečujemo šele v današnjem času, je dobilo nove dimenzije predvsem z razvojem interneta kot globalnega medija za dostop do informacij in z izmenjavo podatkov. Internet velja danes za nepogrešljivo elektronsko komunikacijsko omrežje, ki povezuje računalnike in druge sisteme (na primer pametne telefone) po vsem svetu. Internet se je razvijal od leta 1970 (preden je prišel do stopnje, ki jo poznamo danes) in pomeni povezanost več kot dveh milijard sistemov in naprav. Evolucijo interneta dobro opisuje Internet Society (2012), prihod interneta v Slovenijo in njegov razvoj pa podrobno opisuje Jerman-Blažičeva (2011).

Internetna revolucija je prinesla edinstven informacijski in tehnološki napredek tudi v poslovanju in delovanju svetovnega trga. Internet je spremenil način našega dela, ustvarjanja, zabave, učenja in pogleda na življenje. Ljudje uporabljamo internet za stik z družino in prijatelji, spletno nakupovanje, za iskanje odgovorov na pravna in zdravstvena vprašanja ter za zabavo. Internet je močno spremenil tudi način delovanja podjetij. Podjetja lahko poslujejo elektronsko od direktnega nakupa pri dobaviteljih do prodaje svojim strankam po vsem svetu v realnem času. Internet omogoča zaposlenim, da delajo praktično s katere koli lokacije.

Za podjetja in posameznike so koristi uporabe interneta večinoma povezane z eksternalijami omrežja (Gordon & Loeb, 2005). To pomeni, da je povečanje števila uporabnikov omrežja povezano tudi s tem, da veliko drugih uporabnikov že uporablja isto omrežje. Na primer, če veliko naših prijateljev in znancev uporablja internetno socialno omrežje Facebook, ima uporaba tega omrežja za nas večjo vrednost kot pa neko drugo omrežje, v katerega ni prijavljen nobeden od naših prijateljev in znancev. Izjemna rast interneta in ključnih aplikacijskih

storitev, kot so elektronska pošta, splet, socialna omrežja in internetna telefonija v poznih 90. letih prejšnjega stoletja, je večinoma posledica tovrstnih pozitivnih eksternalij omrežja.

Medtem ko so pridobitve uporabe interneta na vseh segmentih gospodarskega in družbenega življenja številne, je povezanost v internet tudi grožnja in nevarnost za poslovanje podjetij, če povezani sistemi informacijske tehnologije (v nadaljevanju IT) niso ustrezno zaščiteni. Računalniški virusi, kraja identitete in vohunjenje so med najbolj poznanimi primeri napadov, ki se zgodijo sistemom, povezanim z internetom. Virusi in črvi, kot so »MyDoom« in »CodeRed«, lahko zaustavijo na tisoče računalnikov po svetu v nekaj minutah (Strickland, 2008). Stroški, povezani s takimi virusi, so bili ocenjeni na milijarde evrov, če pri tem upoštevamo vse organizacije in posameznike, ki so bili zaradi tega prizadeti (Garson, 2006). Zaradi velike odvisnosti podjetij od informacijskih sistemov so grožnje, ki pretijo njihovim informacijskim sredstvom, toliko resnejše in nevarnejše (Cagnemi, 2001). Negativne posledice možnega napada na informacijske sisteme so lahko velike in v nekaterih primerih za podjetja celo pogubne. Zlasti so te grožnje narasle z razvojem elektronskega bančništva. Banke, ki svojim uporabnikom omogočajo, da elektronsko upravljajo s svojimi računi, so postale izjemno ranljive. Največ zlorab in kraj se dogaja prav z elektronskimi računi komitentov bank, ki poslujejo elektronsko. Da bi se podjetja zavarovala pred grožnjami, ki pretijo njihovim informacijskim sistemom, in ustrezno zaščitila informacije, morajo vzpostaviti varnostne mehanizme, ki varujejo njihov informacijski sistem in poslovne podatke ter hkrati zagotavljajo ustrezno zaščito uporabnikom njihovih storitev.

Informacijski varnosti se v preteklosti ni posvečalo pretirano veliko pozornosti. Razlog je predvsem v tem, da se je internet kot primarni globalni povezovalni medij razvijal v okolju in času, ko še ni bilo nevarnosti napadov in vdorov v računalniška omrežja, ker je sistem nastajal v akademskem okolju in ni bilo priložnosti za zlonamerno uporabo in krajo denarja ter podatkov. Ker je bil na začetku internet zaprto omrežje, ki je povezovalo le določene izbrane akademske organizacije in ustanove, tudi ni bilo posebne potrebe po varnosti in načrtovalci omrežij se s samo varnostjo niso kaj prida ukvarjali. Kot navajata Gansler in Lucyshyn (2005), je bil internet načrtovan za širjenje informacij, ne za njihovo

zaščito. Hitra rast in globalizacija interneta povečujeta njegovo heterogenost in kompleksnost. Zaradi distribuiranega upravljanja in nadzora je danes internet medij, ki mu ne moremo zaupati, zato je potreba po večji varnosti postala nujnost (Bojanc, 2010).

Internet je občutno spremenil pogled organizacij na varnost informacijskih sistemov in njihovih podatkov. V današnjem svetu medsebojno povezanih omrežij uporabnikov in organizacij je zaščita elektronskih informacij najmanj tako pomembna kot zaščita fizičnih sredstev, na primer trezorjev v bankah.

Gordon in Loeb (2005) to ilustrirata na primeru razlike varnosti v banki danes in leta 1950. Leta 1950 je vodja banke za njeno zaščito pred roparji najel varnostnika, ki je poskrbel, da je bil bančni trezor zaklenjen in ustrezno zavarovan. Obenem je vodja banke dal namestiti skrite javljalnike, ki so jih zaposleni v primeru ropa sprožili in obvestili policijo. Ko se je bančni ropar odločal o ropu banke, si je pripravil načrt, kako bo vstopil v banko in kako bo od zaposlenih zahteval denar. Ropar je v pripravah na rop zbral potrebne pripomočke in sredstva za izvedbo ropa, kot so pištola, maska, avto za pobeg s prizorišča zločina in voznika avtomobila. Ropar je pri odločitvi o svojem podvigu najbrž pomislil tudi na možne telesne poškodbe vseh vpletenih. Vodja banke je z različnimi pripomočki skrbel za to, da so bili prostori in zaposleni zaščiteni pred možnim ropom. Danes lahko ropar še vedno oropa banko po starem s podobnimi orodji kot v 50. letih, le da bo najbrž orožje močnejše in avtomobil občutno hitrejši. Vendar je za 21. stoletje bolj značilno, da roparji za rop uporabijo računalnik in omrežje, tako da oropajo banko z elektronskim prenakazilom finančnih sredstev posameznih bančnih strank. Ta sodobni pristop ropanja uporablja drugačna orodja, izniči možnost telesnih poškodb vseh vpletenih, vsebuje tudi manjše tveganje, da bi roparja ujeli na mestu zločina, saj je ta daleč od prizorišča zločina. Obenem ta način omogoča roparju potencialno občutno večji izkupiček, ker ni več omejen zgolj na denar, ki ga lahko fizično odnese iz banke, ampak na denar, ki je elektronsko zapisan in ga lahko prenakaže. Današnji vodja banke se torej glede varnosti sooča z veliko večjim izzivom. Danes je poleg fizičnega varovanja podjetij ali bank enako pomembno ali celo pomembnejše zagotavljati varnost bančnih informacij in preprečevati nepooblaščene dostope zlonamernim hekerjem (posameznikom, ki pridobijo neavtoriziran dostop do računalniškega

sistema), ki vstopajo v informacijski sistem z namenom, da bi denar ukradli. V tem poenostavljenem primeru seveda niso upoštevani drugi varnostni izzivi, s katerimi je soočen vodja banke, kot na primer kraja denarja s strani zaposlenih, ki imajo dostop do bančnih sistemov. Tudi takšni primeri so pogosti v 21. stoletju, le da prizadete ustanove zaradi ugleda (če ne gre za obsežen poseg) tega ne razkrivajo.

Kot je prikazano v navedenem primeru, se za informacijsko varnost lahko uporabijo različni pristopi in metode. Izbira je odvisna od tega, ali gre za informacijsko varnost v podjetjih ali v državni upravi, ali je informacijski sistem velik ali majhen, kako zaupne so informacije itd. Principi varovanja so visokonivojska obravnava informacijske varnosti, ki zajema veliko področij, na primer odgovornost, stroškovno učinkovitost in integracijo (NIST 800-14, 1996) OECD (2002). Dokumenti o tem navajajo nekaj principov, ki naj bi bili ključni za informacijsko varnost.

- **Zavedanje** – Lastniki, ponudniki, uporabniki in drugi udeleženci se morajo zavedati potrebe po informacijski varnosti in tega, kaj lahko storijo, da bi izboljšali varnost. Pri tem je zelo pomembna ozaveščenost o tveganjih in razpoložljivih varnostnih ukrepih.
- **Odgovornost** – Za informacijsko varnost so odgovorni vsi sodelujoči. Ponudniki in uporabniki so odvisni od medsebojno povezanih lokalnih in globalnih informacijskih sistemov in omrežij, morajo pa sprejeti tudi svojo odgovornost za varovanje informacij, sistemov in omrežij.
- **Odziv** – Ukrepati je treba pravočasno, vsi sodelujoči naj medsebojno sodelujejo pri odkrivanju incidentov, njihovem preprečevanju in ukrepanju.
- **Etika** – Treba je spoštovati legitimne interese drugih. Zaradi globalne povezanosti informacijske družbe morajo sodelujoči prepoznati, da njihovo ukrepanje (ali neukrepanje) lahko škoduje drugim.
- **Demokracija** – Informacijska varnost naj ne bi zaklenila informacij, pomembnih za razvoj družbe, zato se mora izvajati skladno z bistvenimi vrednotami demokratične družbe, vključno s svobodo izmenjave misli in idej, prostim pretokom informacij, zaupnostjo informacij in komunikacij, z ustreznim varovanjem osebnih podatkov, odprtostjo in preglednostjo.

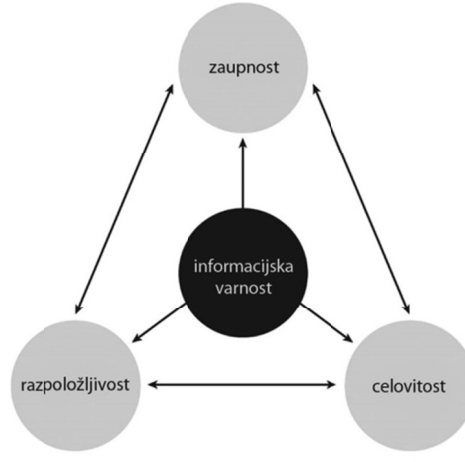
- **Obvladovanje tveganja** – Udeleženci, ki so skrbniki informacij, naj opravijo oceno tveganja, ki identificira grožnje in ranljivost, omogoči določitev sprejemljive ravni tveganja ter pomaga pri izbiri ustreznega ukrepa za zmanjševanje morebitne škode skladno z vrsto in pomembnostjo informacij, ki jih je treba varovati.
- **Načrtovanje in izvajanje varnosti** – Udeleženci morajo vključevati varnost kot bistveni element informacijskih sistemov in omrežij. Farahmand (2004) je mnenja, da informacijska varnost ni ločeno področje od informacijske tehnologije, temveč je vidik oziroma njen sestavni del, ki kaže, kako je informacijska tehnologija specificirana, načrtovana, razvita, nameščena in vzdrževana. Vidik varnosti mora biti vključen v življenjski cikel izdelka informacijske tehnologije ali storitve že od samega začetka. Varnosti se namreč ne da kar tako vključiti v sistem, ko je okolje informacijske tehnologije že uvedeno. Informacijska varnost ni lastnost izdelka ali storitve, temveč okolja.
- **Obvladovanje varnosti** – Udeleženci naj uporabljajo celovit pristop obvladovanja varnosti. Obvladovanje varnosti mora temeljiti na oceni tveganja in mora biti dinamično, zajemati mora vse ravni aktivnosti udeležencev. Schneier (2004a) poudarja, da varnost informacijskih sistemov ni izdelek, temveč proces. Izdelki zagotavljajo določeno stopnjo zaščite, toda edini način za učinkovito poslovanje je vzpostavitev procesov, ki prepoznajo nevarnosti in potencialne napade.
- **Ponovna presoja** – Informacijsko varnost je treba pregledovati, ponovno ocenjevati in izvajati ustrezne spremembe varnostnih politik, praks, ukrepov in postopkov. Neprestano se odkrivajo nove in spreminjajoče se grožnje in ranljivost, zato je potrebno redno pregledovanje, ocenjevanje in spreminjanje vseh vidikov informacijske varnosti. Schneier (2002) ugotavlja, da v informacijski varnosti znane vrste napadov ne zastarijo, novi napadi pa so z razvojem tehnologije le še hujši.

1.3 Cilji informacijske varnosti

Glavni cilji informacijske varnosti so zaščita zaupnosti informacij, zaščita celovitosti informacij ter zagotavljanje pravočasne razpoložljivosti informacij

avtoriziranim uporabnikom (ISO 27000, 2014). Po začetnicah glavnih ciljev zagotavljanja varnosti informacij in sistemov (to so zaupnost, celovitost in razpoložljivost) v angleščini (C – *confidentiality*, I – *integrity*, A – *availability*) se za osnovne cilje informacijske varnosti pogosto uporablja naziv triada CIA, kar je shematično prikazano na Sliki 1. Poleg osnovnih ciljev zaupnosti, celovitosti in razpoložljivosti obstajajo še drugi pomembni cilji zagotavljanja informacijske varnosti, to so zagotavljanje avtentičnosti/overjanje, zagotavljanje neovrgljivosti postopkov ter nadzor dostopa.

Slika 1: *Shematični prikaz triade CIA*



Podjetja za posamezne cilje informacijske varnosti običajno določijo želeno stopnjo varnosti. To pomeni, da podjetje za vsak poslovni proces določi zahteve po zaupnosti, celovitosti in razpoložljivosti sistema in podatkov. Zavedati se moramo, da si lahko cilji informacijske varnosti v nekaterih primerih nasprotujejo. Za spletno knjigarno je na primer najpomembnejša razpoložljivost spletnega dostopa, ki ji omogoča neprekinjeno poslovanje. To se lahko doseže s postavitvijo več strežnikov na različne geografske lokacije, s tem pa se povečajo tudi možnosti za napade, s čimer se dodatno ogrozi zaupnost in celovitost podatkov (Gordon & Loeb, 2005). Drugi primer je vladna obveščevalna služba, ki je pripravljena žrtvovati razpoložljivost na račun zaupnosti, s katero varuje svoje skrivnosti (Ioannidis et al., 2009). Tretji primer je zahteva, da avtorizirani uporabniki uporabljajo različna gesla in identifikacijske informacije, ki lahko

okrepijo zaupnost zasebnih informacij, vendar na račun zmanjšanja pravočasne razpoložljivosti teh informacij.

1.3.1 Zaupnost informacij

Zaupnost (angl. *confidentiality*) je preprečitev nepooblaščenega ali nenamernega razkritja informacij nepooblaščenim posameznikom, osebam ali procesom (ISO 27000, 2014). Zaupnost je zato pogosto jedro vseh varnostnih politik v podjetju, ki določajo, kateri posameznik ima dostop do določenih informacij (DOD, 1985). Kot primer varovanja zaupnosti si oglejmo izvajanje plačilnih transakcij prek interneta. Pri postopku transakcije je treba informacijo o številki kreditne kartice prenesti od kupca do prodajalca in od prodajalca do omrežja za obdelavo plačilnih transakcij. Zaupnost se lahko zlorabi tako, da nepooblaščena oseba pridobi številko kreditne kartice in ukrade identiteto njenega lastnika. Zaupnost podatkov se v tem primeru lahko zavaruje s šifriranim prenosom številke kartice, z zmanjšanjem mest za hranjenje podatka o številki kartice (na primer podatkovne baze, dnevniki, varnostne kopije, tiskani računi itd.) ter z omejevanjem dostopa do mest, kjer se podatek o številki kartice hrani.

Posamezniki ali organizacije lahko zaupne informacije, do katerih nimajo dostopa, nepooblaščeno pridobijo na različne načine, kot so prisluškovanje, vključevanje hroščev v izhodne naprave, zbiranje podatkov iz posod za smeti, spremljanje elektromagnetnega sevanja, podkupovanje ključnih zaposlenih ali izsiljevanje. Pridobljene zaupne podatke lahko uporabijo za lastne interese, informacije prodajo drugim organizacijam ali jih javno razkrijejo. Ni pa nujno, da je vsaka pridobitev (ali razkritje) zaupnih informacij zlonamerna. Lahko gre za posledico napake v programu, postopku ali posledico človeške napake oziroma malomarnosti.

Za varovanje zaupnosti informacij v elektronski obliki se pogosto uporablja šifriranje informacij, kar je tudi osnovni namen kriptografije (Ferguson, Schneier & Kohno, 2010). Poglejmo primer, ko želita dve osebi (ali podjetji) komunicirati med seboj in pri tem uporabljata komunikacijski kanal, ki ni varen. Tretja oseba lahko v tem primeru prisluškuje temu kanalu in tako prejme in prebere vsako izmenjano informacijo. Če pa osebi pri komunikaciji uporabljata šifriranje

informacij s pomočjo sistema in modulov sodobne kriptografije, je prisluškovanje skoraj onemogočeno. Za uporabo šifriranja se morata osebi, ki želita varno komunicirati, najprej dogovoriti za sistem šifriranja. Informacije se ob oddaji šifrirajo s skrivnim ključem in ob prejemu s skrivnim ključem dešifrirajo. Če se za šifriranje informacij uporablja isti skrivni ključ za šifriranje in dešifriranje, potem so v informacijski sistem vgrajeni simetrični šifrirni algoritmi, kot je ameriški standardni algoritem *Advanced Encryption Standard* (AES) (FIPS 197, 2001). Seveda si morata osebi skrivni ključ izmenjati prek varnega kanala, ki se mu ne prisluškuje, ali kako drugače.

Dobri šifrirni algoritmi zagotavljajo, da ni mogoče pridobiti originalnega besedila iz šifriranega besedila brez uporabe skrivnega ključa. Pri tem velja Kerckhoffov princip (Ferguson et al., 2010), da je varnost šifriranja odvisna zgolj od skrivnosti in dolžine ključa in ne od uporabljenega algoritma. To je še zlasti pomembno, ker je algoritme težko razvijati in potem spreminjati. Algoritmi so sestavni del programske in strojne opreme, kar je težko posodabljati. Poleg tega se algoritem, ki se je izkazal za uspešnega, običajno uporablja zelo dolgo, zato bi bilo varovanje njegove skrivnosti veliko težje in precej dražje.

Pri tem se moramo zavedati, da tehnologija sama ne more rešiti vseh varnostnih vprašanj. Kot navajajo Ferguson in soavtorja (2010), je šifriranje podatkov samo del rešitve varnostnega problema, zato je treba module za šifriranje podatkov upoštevati kot del nekega večjega sistema. Šifriranje lahko primerjamo s ključavnicami pri fizičnem varovanju, kjer je ključavnica sama zase neuporabna. Da bi postala uporabna, jo moramo povezati z večjim sistemom, na primer z vrati stavbe, verigo, sefom ali s čim drugim. Večji sistem vključuje tudi človeške vire, ki ključavnico uporabljajo. Ljudje si morajo zapomniti, da dejansko zaklenejo ključavnico stanovanja ali sefa ter ne pustijo ključa kjer koli, kjer bi ga lahko našel kdo drug. Enako velja za module šifriranja podatkov, so le majhen, vendar zelo pomemben del znotraj veliko večjega varnostnega sistema.

1.3.2 Celovitost informacij

Celovitost (angl. *integrity*) zagotavlja pravilnost in popolnost sredstev, kar pomeni, da se podatki ne morejo spreminjati brez avtorizacije pooblaščenih oseb (ISO 27000, 2014). Primeri zlorabe celovitosti so, če zaposleni namenoma ali pomotoma izbrišejo pomembne informacije, če računalniški virus okuži računalnik in pri tem spremeni vsebine okuženih datotek, če lahko zaposleni sam popravlja znesek na svoji plačilni listi, če lahko nepooblaščena oseba spremeni vsebino na spletni strani podjetja itd.

Mehanizmi za varovanje celovitosti informacij so razvrščeni v dve skupini. Prva skupina so mehanizmi, ki preprečujejo zlorabo celovitosti. Ti mehanizmi poskušajo ohraniti celovitost informacij z blokiranjem vseh nepooblaščenih poskusov spreminjanja informacij. Druga skupina so mehanizmi, ki odkrivajo zlorabo celovitosti. Ti mehanizmi ne preprečujejo zlorabe celovitosti, temveč zgolj preverijo celovitost informacij. Če mehanizmi zaznajo, da je bila informacija spremenjena, sporočijo, da ni več vredna zaupanja.

Tehnično se celovitost informacij v elektronski obliki običajno zagotavlja s kontrolnimi podatki, za kar se uporabljajo enosmerne zgoščevalne (angl. *hash*) funkcije. Zgoščevalni algoritmi delujejo na principu izgube informacij. To pomeni, da je izvleček za poljubno dolg niz informacij vedno enako dolg, zato rekonstrukcija originalne informacije iz izvlečka matematično ni mogoča. Tudi če se informacija le za malenkost spremeni, to pomeni popolnoma drugačno vrednost izvlečka. Teoretično sicer lahko obstaja več različnih datotek, ki imajo enak izvleček, vendar je računsko nemogoče najti dve datoteki, ki dasta enak rezultat.

Celovitost informacij se zagotavlja tako, da se pri pošiljanju oziroma shranjevanju informacije izračuna izvleček z znanimi algoritmi in izvleček pošlje (oziroma shrani) skupaj s samo informacijo. Ob prejemu se iz informacije ponovno izračuna izvleček in se primerja s prejetim izvlečkom (izračunanim ob pošiljanju). Če sta izvlečka identična, pomeni, da se informacija od pošiljanja do prejema ni spremenila.

Primeri enosmernih standardiziranih zgoščevalnih algoritmov so *Secure Hash Algorith* (SHA-1, SHA-265 …) (FIPS 180-3, 2008) ali *Message-Digest Algorith 5* (MD5) (RFC 1321, 1992). Težava pri zagotavljanju celovitosti na podlagi enosmernih zgoščevalnih funkcij je v tem, da lahko tisti, ki spremeni informacijo, tudi ponaredi izvleček (ga ponovno izračuna na podlagi spremenjene informacije in z njim zamenja prvotni izvleček). Zato je za večjo varnost zaželeno, da se izvleček dodatno šifrira ali pa se uporabi zgoščevalna funkcija s ključem (angl. *Hash-based Message Authentication Code – HMAC*) (Yener, 2003; RFC 2104, 1997).

1.3.3 Razpoložljivost storitev

Razpoložljivost (angl. *availability*) pomeni, da je storitev (ali sistem) dostopna in uporabna na zahtevo pooblaščene osebe (ISO 27000, 2014). Primer zlorabe razpoložljivosti je ohromitev storitve (angl. *Denial of Service – DoS*). Ta napad na informacijski sistem namerava onesposobiti delovanje sistema ali storitev za določen čas. Gre za pogosto uporabljen napad na sisteme, saj je po raziskavi BIS iz leta 2013 doživelo napad DoS kar 39 % velikih organizacij ter 23 % malih podjetij. Zloraba razpoložljivosti je lahko tudi nenamerna, kot na primer prekinitev dobave infrastrukturnih storitev (elektrike, vode, telekomunikacijskih storitev itd.) zaradi različnih težav ponudnikov ali napake zaposlenih.

Za zaščito razpoložljivosti se v zadnjem času pogosto uvaja obvladovanje neprekinjenega poslovanja (angl. *Business Continuity Management – BCM*), ki vključuje dobre prakse in priporočila (ISO 22301, 2012). Ena izmed rešitev je razpršeno izvajanje storitev na več geografsko ločenih lokacijah.

1.3.4 Avtentičnost

Avtentičnost (angl. *authenticity*) je lastnost, ki zagotavlja, da je identiteta osebe, procesa, sistema ali informacije tista, za katero se izdaja (ISO 27000, 2014). Avtentičnost osebe se dokazuje skozi proces overjanja, ki poveže elektronsko identiteto s fizično osebo (Bishop, 2003). Oseba mora navesti informacije, na podlagi katerih sistem potrdi njeno identiteto. Te informacije lahko izhajajo iz ene ali več naslednjih možnosti:

- kaj oseba ve (na primer geslo ali zaupne informacije),
- kaj oseba ima (na primer kartico, digitalno potrdilo),
- kaj oseba je (na primer biometrija, prstni odtis, značilnosti mrežnice),
- kje se oseba nahaja (na primer pri določenem terminalu).

Največkrat se za overjanje uporabljata uporabniško ime in geslo, na voljo pa so tudi varnejši mehanizmi, na primer uporaba digitalnih potrdil in protokolov za varno overjanje (RFC 2459, 1999). Ločimo med enosmernim overjanjem, kjer le sistem preveri pristnost uporabnika, in dvosmernim, ki zahteva, da tudi uporabnik preveri pristnost sistema.

Pogosto uporabljena tehnična rešitev za dokazovanje avtentičnosti podpisnika elektronskega dokumenta ter zagotavljanja celovitosti podatkov je digitalni podpis (angl. *digital signature*). Pri tem je treba opozoriti na razliko med pojmoma elektronski in digitalni podpis. Elektronski podpis (angl. *electronic signature*) pomeni kakršne koli oznake, narejene z elektronskimi mediji z namenom, da označijo neki dokument ali datoteko. Digitalni podpis pa je elektronski podpis, narejen z uporabo kriptografije. Elektronski podpis je torej širši pojem in vsak elektronski podpis ni nujno tudi digitalni podpis. Primer elektronskega podpisa, ki ni digitalni podpis, je elektronska slika lastnoročnega podpisa določene osebe.

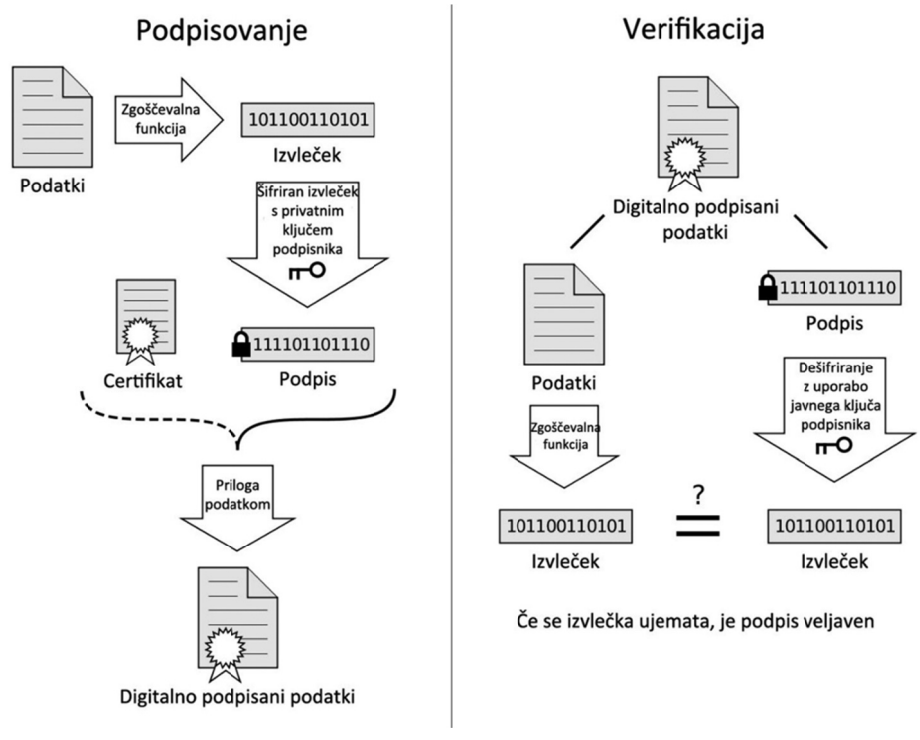
Digitalni podpis temelji na kombinaciji različnih kriptografskih algoritmov ter asimetrični (javni) kriptografiji (angl. *public key cryptography*), ki namesto enega skrivnega ključa uporablja par ključev (Rivest, Shamir & Adleman, 1978). Ključa sta uparjena, tako da en ključ (zasebni ključ) zašifrira informacijo, drugi ključ (javni ključ) pa jo dešifrira in obratno. Pošiljatelj s pomočjo svojega zasebnega ključa iz informacij določenega dokumenta, ki ga podpisuje, izračuna podpis in pošlje prejemniku tako informacije kot izračunan podpis. Prejemnik uporabi javni ključ pošiljatelja in preveri podpis, tako da podpis dešifrira in vsebino primerja s poslanimi informacijami. Če so istovetni, je podpis pristen. Kot že ime pove, se lahko javni ključ poljubno distribuira naokrog, saj omogoča zgolj preverjanje celovitosti in avtentičnosti informacij, svoj zasebni ključ pa vsak posameznik skrbno varuje. Pri strogem overjanju po sistemu X.509 je postopek podoben. Uporabnik podpiše informacijo in dostavi digitalno potrdilo, na katerem je zapisan in digitalno overjen njegov javni ključ. Sistem preveri po

dešifriranju istovetnosti informacije in če je ta pravilna, dovoli uporabniku vstop v sistem.

Z uporabo para ključev se močno poenostavi distribucija ključev med uporabniki. Pri simetrični kriptografiji si morata pošiljatelj in prejemnik izmenjati skrivni ključ. Pri tem je prvi problem varna izmenjave ključev, saj si partnerja ključa zaradi varnosti ne moreta izmenjati prek istega kanala kot sporočilo. Drugi problem je kompleksnost izmenjave, ki narašča s številom posameznikov, s katerimi želimo komunicirati. Za primer vzemimo skupino 10 ljudi, ki želijo varno komunicirati med seboj z uporabo simetrične kriptografije. Vsak od njih si mora z drugimi izmenjati 9 ključev, skupaj pa bo cela skupina za varno komuniciranje potrebovala kar 45 ključev. Število skupnih ključev pa z večanjem števila posameznikov hitro narašča. Pri skupini 100 ljudi je skupno število potrebnih ključev že 4.950. Pri asimetrični kriptografiji (uporablja se tudi ime kriptografija javnih ključev) pa vsak javno objavi ali pa pošlje z digitalnim potrdilom svoj javni ključ in ga ponudi vsem ostalim, svoj zasebni ključ pa obdrži in ga skrbno varuje.

Asimetrična kriptografija se lahko uporablja tudi za šifriranje. V tem primeru pošiljatelj šifrira sporočilo z uporabo javnega ključa prejemnika, prejemnik pa uporabi svoj zasebni ključ in dešifrira sporočilo. Pošiljatelj ve, da se šifrirane informacije lahko dešifrirajo le z zasebnim ključem naslovnika. Tako je zaupnost informacij zagotovljena, ker informacije prebere le oseba, ki so ji namenjene. Slabost kriptografije javnih ključev je, da je postopek šifriranja in dešifriranja nekajkrat (od 1.000- do 10.000-krat) počasnejši kot pri simetrični kriptografiji (Schneier, 1996) zaradi dolžine ključev, ki je več desetkrat večja od ključev, uporabljenih pri asimetričnem šifriranju. Zato se v praksi najpogosteje uporablja kombinacija obeh tipov kriptografije.

Slika 2: *Postopek izdelave in preverjanja digitalnega podpisa*



Vir: Prirejeno po Digital Signature diagram, 2008.

Kot je prikazano na Sliki 2, pošiljatelj pri postopku izdelave digitalnega podpisa najprej izračuna izvleček sporočila ter nato s svojim zasebnim ključem šifrira izvleček. Prejemnik šifrirani izvleček dešifrira z javnim ključem pošiljatelja, nato sam izračuna izvleček dokumenta z enakim algoritmom in primerja enakost obeh izvlečkov. Če sta izvlečka enaka, je podpis veljaven. Drugi način za krajšanje postopka je, da se z metodo javne kriptografije šifrira ključ simetričnega šifriranja z javnim ključem naslovnika ter se ta pošlje naslovniku. Naslovnik dešifrira ključ (ki je kratek) in s tem ključem dešifrira informacije, šifrirane z algoritmom simetrične kriptografije.

V praksi se za digitalni podpis pogosto uporablja kombinacija algoritmov SHA-1 (FIPS 180-3, 2008) z RSA (Rivest et al., 1978), kot je določeno v standardu PKCS#1 (RFC 3447, 2003).

1.3.5 Neovrgljivost

Neovrgljivost (angl. *non-repudiation*) je zmožnost sistema za dokazovanje dogodka ali dejanja, ki se je zgodilo, ter vključenosti posameznikov v dogodek (ISO/IEC 27000, 2014). Povedano drugače, neovrgljivost preprečuje zanikanje posredovanega sporočila ali drugega dejanja bodisi s strani pošiljatelja bodisi prejemnika. Prejemnik lahko dokaže, da je domnevni pošiljatelj dejansko poslal sporočilo ali opravil določeno dejanje na IT-sistemu. Podobno lahko pošiljatelj dokaže, da je sporočilo dejansko prejel domnevni prejemnik.

Pogosto se tudi za zagotavljanje neovrgljivosti uporabljajo sistemi za digitalno podpisovanje. Če je treba v informacije, ki zagotavljajo neovrgljivost, vključiti tudi časovne podatke (čas dogodka, časovno zaporedje dogodkov), pa se uporablja časovno žigosanje. Časovni žig (angl. *time stamp*) je posebna oblika digitalnega podpisa, ki vključuje še čas nastanka podpisa.

Če je časovni žig izdan s strani overjenega izdajatelja časovnih žigov (angl. *Time Stamping Authority – TSA*), to zagotavlja, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem trenutku. To omogoča lažje razčiščevanje ob morebitnih sporih, ko je treba dokazati časovne lastnosti transakcij in drugih storitev. TSA je časovno sinhroniziran s svetovnimi časovnimi strežniki interneta (zaupanja vrednimi časovnimi viri).

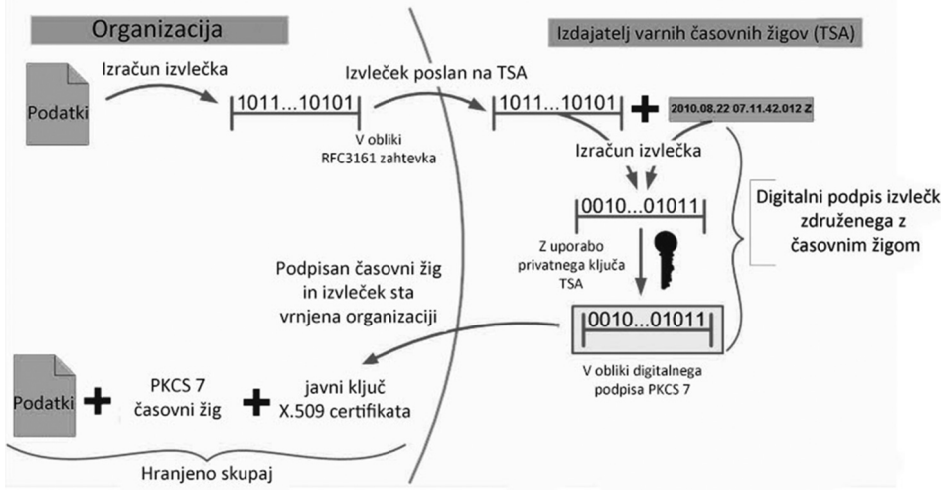
Slika 3: *Postopek časovnega žigosanja*

Vir: Ministrstvo za notranje zadeve RS, Osnove varnih časovnih žigov, 2010.

Izdajatelj varnih časovnih žigov SI-TSA deluje na ministrstvu za notranje zadeve kot del nalog overitelja digitalnih potrdil. Časovno žigosanje SI-TSA deluje kot spletna storitev (angl. *Web Service*), kar pomeni, da si aplikacija in strežnik za časovno overjanje izmenjujeta zahtevke v XML po protokolu SOAP prek HTTP oziroma HTTPS (Slika 3).

Postopek časovnega žigosanja je prikazan na Sliki 4. Ko želimo časovno žigosati neki elektronski dokument oziroma podatke, pošljemo strežniku TSA z zgoščevalno funkcijo izračunan izvleček dokumenta oziroma podatkov.

Slika 4: *Postopek izračuna časovnega žiga*



Vir: Prirejeno po How a digital timestamp works, 2010.

Strežnik TSA temu izvlečku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem – to je časovni žig. S tem je dokazano, da je elektronski dokument obstajal pred časom, navedenim v časovnem žigu, poleg tega pa se da preveriti, ali se je od časa žigosanja dokument spremenil (SI-TSA, 2014). Postopek opisuje RFC 3161 (2001).

2 TEHNIKE VAROVANJA IN RAVNANJE Z VARNOSTNIMI TVEGANJI

2.1 Varnostna tveganja

Kot poudarja Schneier (2004a), informacijska varnost ni izdelek, temveč proces. V prvem poglavju smo si ogledali, kaj so poslovne informacije in zakaj jih je treba varovati, v tem poglavju pa si bomo ogledali, kakšen je proces varovanja informacij.

2.1.1 Mit popolne varnosti

Strokovnjaki, ki se v podjetjih ukvarjajo z informacijsko varnostjo, nenehno proučujejo, kako varen je njihov sistem. Pomembno je, da se zavedamo, da popolnoma varen sistem ne obstaja. Gene Spafford, direktor Computer Operations, Audit and Security Technology (COAST) na Purdue University, opisuje, kakšen naj bi bil popolnoma varen sistem (Bowen, 2002):

> *»Edini sistem, ki je zares varen, je takšen, ki je izključen in izklopljen iz električnega omrežja, zaklenjen v sefu, narejenem iz titana, zakopan v betonskem bunkerju, ki ga obdaja plast živčnega plina in zelo dobro plačani oboroženi stražarji. Vendar niti takrat ne bi zastavil svojega življenja zanj.«*

Ker popolnoma varnega sistema ne moremo imeti, je treba ugotoviti, koliko varen je lahko sistem glede na potrebe po varovanju informacij. Splošnega odgovora na to ni. Vsako podjetje mora glede na svoje varnostne zahteve določiti, kakšno stopnjo varnosti želi imeti. Popolno varnost lahko torej razumemo kot stopnjo varnosti, ki je za podjetje sprejemljiva (Schneier, 2003). Določitev ustrezne stopnje varnosti pa ni preprosta naloga (Geer, 2004).

Podjetja pri iskanju ustrezne stopnje varnosti najprej ugotavljajo **varnostna tveganja,** ki so jim podvržena njihova sredstva. Z analizo tveganj določijo, kakšno stopnjo varnosti potrebujejo. Ker se razmere, na podlagi katerih se ocenjujejo varnostna tveganja, s časom spreminjajo, je treba analizo tveganj ustrezno umestiti v čas oziroma jo periodično ponavljati.

Pravzaprav sta tveganje in informacijska varnost neločljivo povezana pojma. V splošnem se tveganje nanaša na negotovost izvedbe dogodka in je opredeljeno kot kombinacija verjetnosti, da se neželen dogodek zgodi, in negativnih posledic, ki pri tem lahko nastanejo (ISO Guide 73, 2009). Na področju informacijske varnosti se tveganje pogosto nanaša na negotovost, ki je povezana s pojavom potencialno nevarnih dogodkov. Tveganje informacijske varnosti lahko natančneje opredelimo kot možnost, da bo določena grožnja izkoristila ranljivost sredstva ali skupino sredstev ter povzročila škodo podjetju (ISO 27000, 2014). Tveganje je tako kombinacija grožnje in ranljivosti informacijskega sredstva, kar pripelje do negativnega učinka, ki škoduje enemu ali več informacijskim sredstvom. Grožnje in ranljivost so del vzroka tveganja, učinek pa je posledica tveganja (Mayer, Heymans & Matulevičius, 2007).

Za lažje razumevanje si oglejmo primer zlonamernega uporabnika, ki želi pridobiti neavtoriziran dostop do sistema. Da bi zlonamerni uporabnik pridobil želene informacije, uporabi pri komunikaciji z zaposlenimi tehniko socialni inženiring, s katero nagovarja zaposlene, da mu posredujejo informacije, do katerih nima dostopa in ki so lahko po svoji naravi zaupne ali pomembne za podjetje. V primerih, ko zaposleni niso ustrezno izobraženi ali informirani, mu lahko (ne da bi se zavedali nevarnosti) posredujejo določene pomembne ali zaupne informacije. Na podlagi teh informacij lahko zlonamerni uporabnik pridobi neavtoriziran dostop do računalnikov in sistemov, pobere informacije ali pa zagreši kakšno drugo kaznivo dejanje. Podjetje je oškodovano, ker so lahko občutljive informacije razkrite, ali pa utrpi drugo škodo. V navedenem primeru je zlonamerni uporabnik s socialnim inženiringom grožnja, slaba ozaveščenost zaposlenih je ranljivost sistema, izguba zaupnosti ter celovitosti občutljivih informacij pa je učinek oziroma posledica.

2.1.2 Varnostni incidenti

Če se tveganje oziroma grožnja napada dejansko realizira, se zgodi neželen dogodek, ki se na področju informacijske varnosti imenuje **varnostni incident**. Natančneje lahko informacijski varnostni incident opredelimo kot enega ali več neželenih ali nepričakovanih dogodkov v zvezi z informacijsko varnostjo, za katere je zelo verjetno, da bodo ogrozili poslovanje in informacijsko varnost v podjetju (ISO 27000, 2014).

Pri vrednotenju škode, ki jo lahko naredi incident, je pomembna vrednost ogrožene informacije ali sredstva. Na primer neavtoriziran dostop do skrivne formule določenega proizvoda oziroma recepta lahko pomeni za podjetje veliko večjo škodo, kot če heker za eno uro onesposobi spletno stran podjetja. Vrednost informacije je tudi močno odvisna od tega, kdo informacijo poseduje. Občutljive poslovne informacije v rokah konkurenta so bistveno bolj problematične, kot če bi jih imel v rokah neki najstnik (Gordon & Loeb, 2005). Časovna občutljivost še dodatno otežuje vrednotenje. Na primer geslo, ki poteče v desetih sekundah, je po poteku tega časa brez vrednosti, je pa precej dragoceno v tistih desetih sekundah, v katerih je z geslom mogoč dostop do omrežja (Soo Hoo, 2000). Kot izhaja iz definicije tveganja, se pri vrednotenju varnostnega incidenta osredotočamo na dva parametra: na verjetnost, da se varnostni incident zgodi, ter kakšna bo posledica za podjetje v primeru, da bo dejansko prišlo do incidenta.

Določanje **verjetnosti, da se bo incident zgodil,** je za primere naravnih nesreč (na primer potres, poplava) precej lažje kot za človeške grožnje, saj se pričakovana ponovitev incidentov lahko predvideva na podlagi zgodovinskih podatkov (Anderson, 1991; Soo Hoo, 2000) in statistike ter se zatem izračuna verjetnost. Modeli lahko natančno napovedujejo prihodnje dogodke na podlagi zgodovinskih podatkov le, kadar so statistična razmerja, na katerih je model zgrajen, stacionarna skozi čas. Kadar se vpliv neodvisnih spremenljivk na odvisne spremenljivke spreminja, je predvidevanje dogodkov nezanesljivo. Za modeliranje dogodkov, ki jih povzroča človek (na primer zlonamerni posamezniki ali kriminalci), je to stacionarno zahtevo težko doseči. Za razliko od narave poskušajo zlonamerni uporabniki izvesti napad na najšibkejšo točko sistema, neprestano izboljšujejo svoja znanja in uporabljeno tehnologijo ter onemogočajo poskuse merjenja njihovega obnašanja (Schechter, 2004). Četudi bi se zlonamerni uporabniki obnašali stacionarno, na tem področju primanjkuje zgodovinskih podatkov za človeške grožnje (Farahmand, 2004). Ocenjevanje verjetnosti incidentov, ki jih povzroča človek, je torej zapleteno in običajno precej subjektivno. Farahmand (2004) priporoča, da se za pomoč pri ocenjevanju upoštevajo nekateri dejavniki.

- **Motiv**. Kako motiviran je napadalec? Ali je napadalec politično ali kako drugače motiviran (koristoljubje)? Ali je napadalec nezadovoljen zaposleni? Ali je sredstvo privlačen cilj za napadalce?

- **Način**. Kateri incidenti lahko vplivajo na ključna sredstva? Kako napredni so napadi? Ali imajo možni napadalci zadosti znanja in spretnosti za izvedbo napadov?
- **Priložnost**. Kako ranljiva je računalniška infrastruktura? Kako ranljiva so določena ključna sredstva?

Če se varnostni incident zgodi, je njegova **posledica** potencialna izguba, ki bi jo podjetje utrpelo. Čeprav so lahko ekonomske posledice varnostnih incidentov zelo velike, raziskave kažejo, da se v zadnjih letih (zaradi vpeljanih boljših sistemov za zaščito) povprečna letna izguba zaradi varnostnih incidentov zmanjšuje (CSI, 2011). Merjenje izgub ni preprosto, saj so dejanske izgube večplastne in jih je težko ovrednotiti. Običajno se izgube v podjetjih zaradi neželenih varnostnih dogodkov merijo glede na to, kako vplivajo na poslovanje (Farahmand, 2004). Pri tem se posledice dogodka lahko močno razlikujejo od podjetja do podjetja. Kadar dve podjetji doleti enak varnostni dogodek, lahko eno podjetje utrpi škodo, medtem ko drugo ne. Eno podjetje ima lahko uvedene učinkovite postopke varnega arhiviranja, medtem ko drugo ne. Eno podjetje ima lahko učinkovite povezave s svojimi proizvajalci varnostnih rešitev in zunanjimi izvajalci, medtem ko drugo ne.

Vendar pa je treba biti pri merjenju vpliva varnostnega incidenta na poslovanje pozoren. Ni priporočljivo preprosto privzeti, da je potencialna izguba enaka izgubi obsega poslovanja za čas incidenta. Če na primer sistem naročanja pri proizvajalcu utrpi enotedenski izpad, izguba ni kar enaka enotedenskemu izpadu poslovanja, ker sistem ni mogel sprejemati naročil. Proizvajalec bi za čas nedelovanja lahko poiskal alternativo za naročanje, zato je treba pri merjenju izgub zaradi incidenta primerjati dva scenarija: po prvem scenariju se varnostni incident zgodi, po drugem pa ne (Soo Hoo, 2000). V tem primeru je osnova za vrednotenje stroškov posledic razlika prihodkov med obema scenarijema.

Pri oceni vrednosti izgub običajno ločimo **takojšnje** in **posredne** izgube. Takojšnje izgube so stroški, ki jih lahko jasno povežemo s posameznimi incidenti. To so običajno stroški, povezani z osebjem, strojno opremo in programsko opremo. Tipične takojšnje izgube so na primer izguba prihodka, izguba produktivnosti in povečanje stroškov zaradi nadur, višje zavarovalne premije itd. (Gordon & Loeb, 2005).

V nasprotju s takojšnjimi izgubami se posredne izgube ne morejo z dovolj veliko verjetnostjo povezati neposredno s posameznim incidentom. Posredne izgube se lahko nanašajo na podobo blagovne znamke, javni ugled in dobro ime na trgu, na finančne vrednosti poslov, zaupanje javnosti in strank, na izgubo intelektualne lastnine idr. (Gordon & Loeb, 2005; Farahmand, 2004; Bojanc & Jerman-Blažič, 2008). Varnostni incident lahko zmanjša zaupanje med podjetjem in njegovimi strankami ter partnerji. Nezadovoljni kupci lahko preidejo h konkurenci. Varnostne težave so lahko tudi znak pomanjkanja skrbi za zasebnost strank in slabe varnostne prakse znotraj podjetja. To lahko povzroči tudi nezanimanje vlagateljev, ki se zanimajo za dolgoročno uspešnost podjetja. Varnostni incidenti zmanjšujejo prihodne denarne tokove, obenem pa lahko tudi znižujejo ceno delnic. Posredne izgube je težko izračunati. Čeprav so posredni stroški za podjetja izredno pomembni pri merjenju dejanskih stroškov varnosti (Su, 2006), se njihova pomembnost izgubi ravno zaradi težavnega izračunavanja (Farahmand, Navathe, Sharp & Enslow, 2004). Posredne izgube lahko v določenih situacijah veliko dlje negativno vplivajo na stranke, dobavitelje, finančni trg, banke in poslovne partnerje kot takojšnje izgube (Camp & Wolfram, 2004; Dynes, Andrijcic & Johnson, 2006; Rowe & Gallaher, 2006).

Ne glede na metodo izračuna posledic incidenta se izgube najpreprosteje izračunajo tako, da jih razdelimo na posamezne kategorije in podkategorije. Nekatere kategorije lahko izračunamo dokaj natančno, pri drugih (še zlasti pri posrednih izgubah) pa je ocena vrednosti težja. Primer take razdelitve izgub je predstavil Denning (1999), pri čemer je izgube razdelil na tri kategorije, ki so povezane z zlorabo zaupnosti, celovitosti in razpoložljivosti. Prva kategorija izgub so **stroški zamenjave**, do katerih pride, če so sredstva uničena, pokvarjena, onesnažena ali fizično ukradena. Ti stroški nastanejo zaradi zlorabe celovitosti in lahko vključujejo:

- stroške nakupa nove opreme (zaradi uničenja, kraje, okvare, izgube …), ki so sestavljeni iz:
  - nabavne cene, stroškov proizvajalca,
  - prevoznih stroškov in dostave,
  - stroškov namestitve,
  - začasne zamenjave (da se podjetje izogne kaznim in globam),
  - stroškov najema,

- dodatnega dela;
- stroške popravila ali zamenjave (ure, nadure, najeti zunanji izvajalci …).

Druga kategorija izgub so **stroški zaradi nedostopnosti**, ki nastanejo, kadar informacijska sredstva niso na voljo v določenem časovnem obdobju, ker so bila uničena, ukradena, poškodovana ali onesnažena in so zaradi tega delno ali popolnoma neuporabna. Ti stroški so ocenjeni z upoštevanjem časovnega intervala, ki se začne v trenutku, ko sredstvo ni na voljo, in konča, ko je sredstvo ponovno na voljo. Ti stroški nastanejo zaradi zlorabe razpoložljivosti in lahko vključujejo:

- izgubo prihodkov zaradi nedelovanja (neposredna izguba, izguba prihodnjih prihodkov),
- stroške popravila nedelovanja (ure, nadure, zunanji izvajalci),
- nezmožnost plačila računov ali plačila strank,
- nezmožnost dostave proizvodov ali storitev,
- stroške uporabe alternativnih virov,
- stroške zaradi nespoštovanja zakonske obveznosti,
- stroške zaradi nespoštovanja pogodbene obveznosti,
- izgubo dobrega imena,
- izgubo bonitetne ocene,
- izgubo vrednosti zalog,
- izgubo produktivnosti.

Tretja kategorija izgub so stroški, ki izhajajo iz **zlorab zaupnosti**. Ti stroški lahko vključujejo:

- stroške zaradi razkritja zaupnih informacij,
- stroške zaradi nespoštovanja zakonskih obveznosti,
- stroške zaradi nespoštovanja pogodbenih obveznosti,
- dolgoročno izgubo prihodkov zaradi izgube ugleda (stranke, dobavitelji, finančni trgi, banke, poslovni partnerji itd.),
- stroške popravila zlorab razkritja zaupnih informacij (porabljene ure, nadure, marketing …).

Izgube, ki sodijo v tretjo kategorijo (še zlasti tiste, ki vključujejo nepooblaščen dostop do zaupnih podatkov), so lahko zelo velike in so pogosto povezane z odškodninami. Po raziskavah je pri zlorabah zaupnosti lahko reakcija trga zelo

negativna, medtem ko pri zlorabah razpoložljivosti in celovitosti tako posebnih reakcij trga ni zaznati (Campbell et al., 2003; Hovava & D'Arcy, 2003, Farahmand, 2004).

2.1.3 Metode in tehnike za ravnanje s tveganji

Pregled literature poda številne raziskave s področja merjenja tveganj (Alberts & Dorofee 2002; Bennett & Kailay, 1992; Blakley, 2001; Campbell & Sands, 1979; Neumann, 2000). Veliko študij, ki preučujejo znana tveganja, se osredotoča na tveganja, ki vključujejo predvsem oceno posameznika za verjetnost, da se nekaj zgodi, ki izhaja iz njegovih dejanskih izkušenj (Boss, 2007). Pri tem se teži k temu, da bi bila kar najbolj izključena subjektivnost, ki po navadi vpliva na posameznikove ocene tveganja. Sturrock (2005) navaja, da zaradi subjektivnosti posamezniki večkrat kot večja tveganja zaznajo dogodke, ki se zelo verjetno nikoli ne bodo zgodili (na primer teroristični napad, napad morskega psa itd.), in manjša tveganja za dogodke, ki se pogosteje zgodijo (na primer zamašene arterije, kožni rak, avtomobilske nesreče itd.). Prav tako nekatere raziskave kažejo, da je veliko informacij, ki jih posamezniki prejmejo v zvezi z grožnjami računalniške varnosti, osredotočenih na subjektivno oceno spletnega kriminala (Hughes & DeLone, 2007). Dojemanje tveganja je običajno povezano z izkušnjami, ki jih ima posameznik v zvezi z varnostnimi incidenti (Skogan & Maxfield, 1981; Stinchcombe et al., 1980; Taylor & Todd, 1995).

Obstaja veliko različnih metod in tehnik za merjenje tveganja. Med najbolj priljubljenimi, ki jih priporoča tudi Evropska agencija za varnost informacij, so naslednje metode (ENISA, 2014):

- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) (2011) je metoda, ki je razvita in vzdrževana s strani DCSSI (Central Information Systems Security Division) v Franciji.
- MEHARI (Method for Harmonized Analysis of Risk) (2010) je metodologija obvladovanja tveganja, razvita s strani CLUSIF in zgrajena na podlagi dveh metod obvladovanja tveganja MARION in MELISA.
- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) (Alberts & Dorofee, 2001, 2002; CERT, 2005) omogoča

vrednotenje tveganja za različne tipe in velikosti podjetij, ki ga ponuja CERT na Carnegie Mellon University.

- CRAMM (CCTA Risk Analysis and Management Method) (2003) je metoda obvladovanja tveganja, originalno razvita s strani UK Government's Central Computer and Telecommunications Agency (CCTA) leta 1985. Trenutno se vzdržuje s strani podjetja Insight Consulting.
- ISAMM (Information Security Assessment and Monitoring Method) (2008) je metoda upravljanja tveganja s podpornimi orodji.
- MAGERIT (2012) je odprta metodologija, razvita s strani španskega ministrstva za javno upravo.

Metode in tehnike za merjenje in analizo tveganja na podlagi znane literature lahko razdelimo v dve osnovni kategoriji: kvantitativne in kvalitativne. Kvantitativne metode merjenja tveganja poskušajo določiti numerične vrednosti za verjetnost in posledico tveganja ter ovrednotiti stroške in koristi, povezane z uvedbo varnostnih rešitev. Kvantitativni pristop predpostavlja, da je mogoče vsako tveganje numerično ovrednotiti in izračunati vrednost verjetne škode, če se tveganje uresniči. Ključna prednost kvantitativne metode je, da omogoča analizo stroškov in koristi ter da so rezultati predstavljeni tako, da jih razume vodstvo podjetja. Po drugi strani pa kvantitativni pristop običajno zahteva poglobljeno in obsežno raziskavo o grožnjah, sistemu in podjetju, da se lahko določijo numerične vrednosti za verjetnosti in potem za posledice.

Največja težava kvantitativnega pristopa je pomanjkanje dobrih statističnih oziroma zgodovinskih podatkov, ki so potrebni za oceno parametrov tveganja. Statistični podatki so običajno na voljo za tveganja, pri katerih so grožnje naravne nesreče (na primer potres, poplava), precej težje pa je pridobiti statistične podatke za človeške grožnje. Eden od razlogov za pomanjkanje tovrstnih statističnih podatkov je, da večina podjetij sistematično ne odkriva, nadzira in beleži varnostnih incidentov. Drugi razlog je, da podjetja, ki doživijo napad, pogosto o tem raje molčijo, kot da bi napad objavila. V primeru javnega razkritja varnostnega incidenta lahko tvegajo zmanjšanje svojega ugleda, izgubo zaupanja strank ali (kar je še huje) razkrivajo svoje ranljivosti drugim hekerjem. Zato veliko resnih varnostnih incidentov ni nikoli objavljenih (Bojanc & Jerman-

Blažič, 2008). V raziskavi CSI (2011) je bilo le 22 % sodelujočih pripravljenih razkriti podrobnosti o finančnih izgubah, ki so jih utrpeli, in to kljub anonimnosti raziskave. Zato nekateri avtorji (kot na primer Gardner (1989)) opozarjajo, da se je treba pri oceni tveganja zavedati, da izračun tveganj sloni na podatkih in verjetnosti, ki pogosto nimajo močne empirične podlage. Težave lahko nastopijo takrat, ko se slepo verjame, da so podatki, ki jih imamo na voljo, točni, v resnici pa pogosto niso prav natančni.

Kvalitativne metode merjenja tveganja poskušajo izraziti vrednost sredstev, pričakovano izgubo in stroške uvedbe zaščite v opisnih spremenljivkah, kot so »visoka«, »srednja« ali »nizka«. Na Sliki 5 je prikazan primer tolerančnega okvira za kvalitativno vrednotenje tveganj. Verjetnost in posledica sta na primeru vrednotena z vrednostmi od 1 do 5, vrednost tveganja pa je dobljena z množenjem vrednosti za verjetnost in vrednosti za posledico. Izračunane vrednosti tveganj so razdeljene na tri območja. Vrednosti tveganja, ki so manjše ali enake 6, predstavljajo nizko tveganje, vrednosti med 7 in 12 predstavljajo srednje tveganje, vrednosti nad 13 pa visoko tveganje.

Slika 5: *Tolerančni okvir za kvalitativno vrednotenje tveganj*

Verjetnost						
	Skoraj zanesljivo – 5	**5**	**10**	**15**	**20**	**25**
	Zelo verjetno – 4	**4**	**8**	**12**	**16**	**20**
	Verjetno – 3	**3**	**6**	**9**	**12**	**15**
	Malo verjetno – 2	**2**	**4**	**6**	**8**	**10**
	Skoraj neverjetno – 5	**1**	**2**	**3**	**4**	**5**
		Zelo majhna – 1	Majhna – 2	Srednja – 3	Velika – 4	Kritična – 5
		Posledica				

Kvalitativni pristop zagovarja načelo, da posledic nekaterih vrst izgub (na primer okvare ali spremembe podatkov) ni mogoče izraziti z denarnimi vrednostmi (Farahmand, 2004). Pri primerjavi kvalitativnih vrednosti moramo biti pazljivi, saj gre za subjektivne ocene. Za nekoga je lahko določeno tveganje visoko, nekdo drug pa isto tveganje lahko razume kot nizko. V splošnem se kvalitativne metode lahko izvedejo v krajšem času z manjšim številom osebja kot kvantitativne metode. Izvedba poteka običajno skozi kombinacijo vprašalnikov in skupnih delavnic. Največji prednosti kvalitativnega pristopa sta porabljen čas in strošek za izvedbo ocene. Slabost kvalitativnega pristopa je splošnost in netočnost rezultatov, ki so posledica relativnih vrednosti vhodnih podatkov. Običajno je za manjša podjetja z omejenimi človeškimi viri primernejši kvalitativni pristop. Pregled prednosti in slabosti posamezne metode je prikazan v Tabeli 1.

Tabela 1: *Primerjava prednosti in slabosti kvantitativnih in kvalitativnih metod za obvladovanje tveganja*

	Kvantitativna metoda	Kvalitativna metoda
Prednosti	▪ Veliko truda je že vloženega v definiranje vrednosti virov in zmanjševanja tveganja. ▪ Ključna je stroškovno učinkovita ocena. ▪ Rezultati so predstavljeni na način, ki ga razume vodstvo (v denarni vrednosti, odstotkih, verjetnostih).	▪ Izračuni so preprosti. ▪ Ne zahteva prikaza vrednosti sredstev v denarnih enotah. ▪ Ne zahteva izračuna pogostosti groženj. ▪ Preprosteje je vključiti zaposlene, ki niso tehnični ali varnostni strokovnjaki. ▪ Daje fleksibilnost procesa in poročanja. ▪ Zahteva občutno manj osebja. ▪ Ni potrebe po izračunu vrednosti sredstev ali izračunu stroška zaščite.
Slabosti	▪ Izračuni so kompleksni, težavni in zahtevni. ▪ Zahteva veliko pripravljalnega dela. ▪ Udeležencev ne moremo kar voditi skozi proces. ▪ Težko je spremeniti usmeritve. ▪ Potrebuje dobre zgodovinske podatke.	▪ Zelo subjektivne ocene. ▪ Omejene aktivnosti v določanju denarnih vrednosti za sredstva. ▪ Ni osnova za analizo stroškov in koristi.

Vir: R. Bojanc, Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih, 2010.

2.1.4 Izračun pričakovane letne izgube zaradi incidentov (ALE)

Leta 1975 je Nacionalni urad za standarde (*National Bureau of Standards*) v ZDA, predhodnik Nacionalnega inštituta za standarde in tehnologijo (*National Institute of Standards and Technology – NIST*), objavil standard Federal

Information Processing Standard (FIPS) 65: Smernice za avtomatsko obdelavo podatkov analize tveganja (angl. *Guideline for Automatic Data Process Risk Analysis*). Standard opredeljuje kvantitativno merjenje tveganja informacijske varnosti, ki definira in predlaga uporabo metode pričakovana letna izguba (angl. *annual loss expectancy – ALE*) za morebitne uresničene informacijske incidente.

Pričakovana letna izguba ALE (oziroma natančneje pričakovana vrednost izgub) se izračuna z množenjem verjetnosti za neželen dogodek in velikosti izgube zaradi dogodka. Predpostavimo, da je n možnih dogodkov, ki se lahko zgodijo v obdobju enega leta, in vsak možen dogodek označimo z indeksom $i = 1, 2 \ldots, n$. Naj I predstavlja možno investicijo v informacijsko varnost ali določeno skupino takih investicij. Investicija v informacijsko varnost I lahko vpliva na verjetnost, da se dogodek zgodi v danem letu, in na obseg izgube, povezane z dogodkom. Naj bo $P_i(I)$ verjetnost za dogodek i v obdobju enega leta ob izvedeni investiciji I. Naj $L_i(I)$ predstavlja letno izgubo v denarni enoti, ki jo podjetje utrpi, če se zgodi dogodek i ob investiciji I. ALE, vezano na investicijo I, zapišemo:

$$ALE(I) = \sum_{i=1}^{n} L_i(I) P_i(I) \qquad (1)$$

Zgornji izračun si oglejmo na preprostem primeru okužbe z računalniškim virusom. Če okužba računalnikov z virusom podjetju povzroči 7.500 € izgube in se pričakuje ena okužba na dve leti (verjetnost za okužbo je 0,5), znaša ALE 7.500 € × 0,5 = 3.750 €.

Gordon in Loeb (2005) navajata naslednje pomanjkljivosti pri uporabi metode ALE. Kot prvo ALE ne upošteva časovne dinamike in predpostavlja, da so možne izgube zaradi varnostnih incidentov konstantne skozi čas. To je še zlasti moteče, če se neki dogodek v obdobju enega leta zgodi večkrat. Poleg tega ALE opredeli tveganje glede na izgube, ki so odvisne od izvedene investicije, ne podaja pa pravila za izbiro najboljše investicije. Kot tretjo slabost pa avtorja izpostavljata, da ALE gleda na investicijo v informacijsko varnost le s strani koristi in ne upošteva stroškov, povezanih z investicijo.

Standard FIPS 65 je bil leta 1995 sicer preklican (Withdrawn FIPS, 2010) in merjenje tveganj po metodi ALE ni postalo del obvezujočih standardov v ameriški administraciji, je pa metoda ALE v krogih informacijske varnosti postala splošno znana in pogosto uporabljena. Ne glede na zgoraj navedene pomanjkljivosti se metoda ALE danes uporablja v večini kvantitativnih analiz tveganj informacijske varnosti (Soo Hoo, 2000; Gordon & Loeb, 2005). Znano je, da jo uporabljajo predvsem zavarovalnice. Za razliko od zavarovalniških tveganj, ki se osredotočajo na izgube, ki izhajajo iz zavarovalnih zahtevkov, varnostna tveganja ocenjujemo z upoštevanjem kompleksnih kombinacij možnih posledic.

2.2 Grožnje in ranljivosti informacijske tehnologije

Informacijska tveganja, ki smo jih spoznali v prejšnjem poglavju, so odvisna od vrednosti sredstev, groženj, ranljivosti in uvedenih varnostnih rešitev. Kot smo ugotovili, so grožnje in ranljivosti del vzroka za tveganje, zato si jih bomo v tem poglavju ogledali podrobneje.

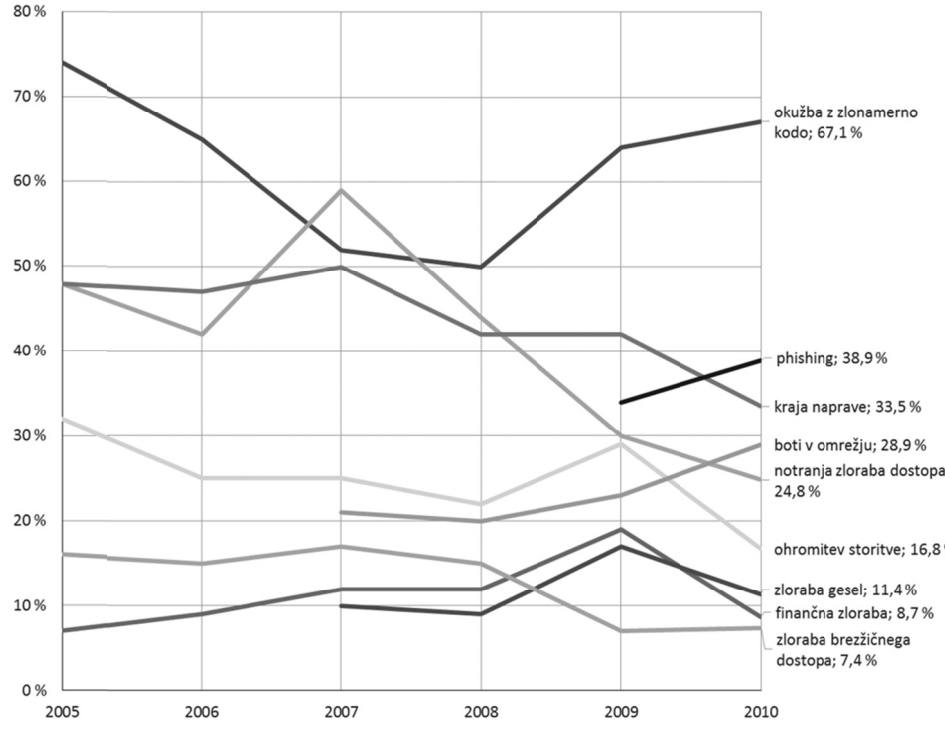
2.2.1 Grožnje informacijskim sredstvom

Informacijska sredstva so izpostavljena grožnjam. **Grožnje** informacijskemu sistemu podjetja so viri možnih neželenih dejavnosti ali dogodkov, ki lahko povzročijo škodo sistemu ali podjetju (ISO 27000, 2014; Gordon & Loeb, 2005). Grožnje imajo različen vpliv na informacijska sredstva, v splošnem pa jih lahko glede na njihovo usmeritev razdelimo na:

- uničenje informacijskih sredstev,
- spremembo informacijskih sredstev,
- krajo informacijskih sredstev,
- razkritje zaupnih informacij,
- prekinitev delovanja storitev.

Po raziskavi CSI (2011), v kateri je sodelovalo 351 podjetij, so najpogostejše grožnje, ki so jih podjetja že izkusila, okužba z zlonamerno kodo, spletno ribarjenje (phishing) in kraja sredstev. Rezultati so prikazani na Sliki 6.

Slika 6: *Vrste napadov, ki jih je podjetje že utrpelo*

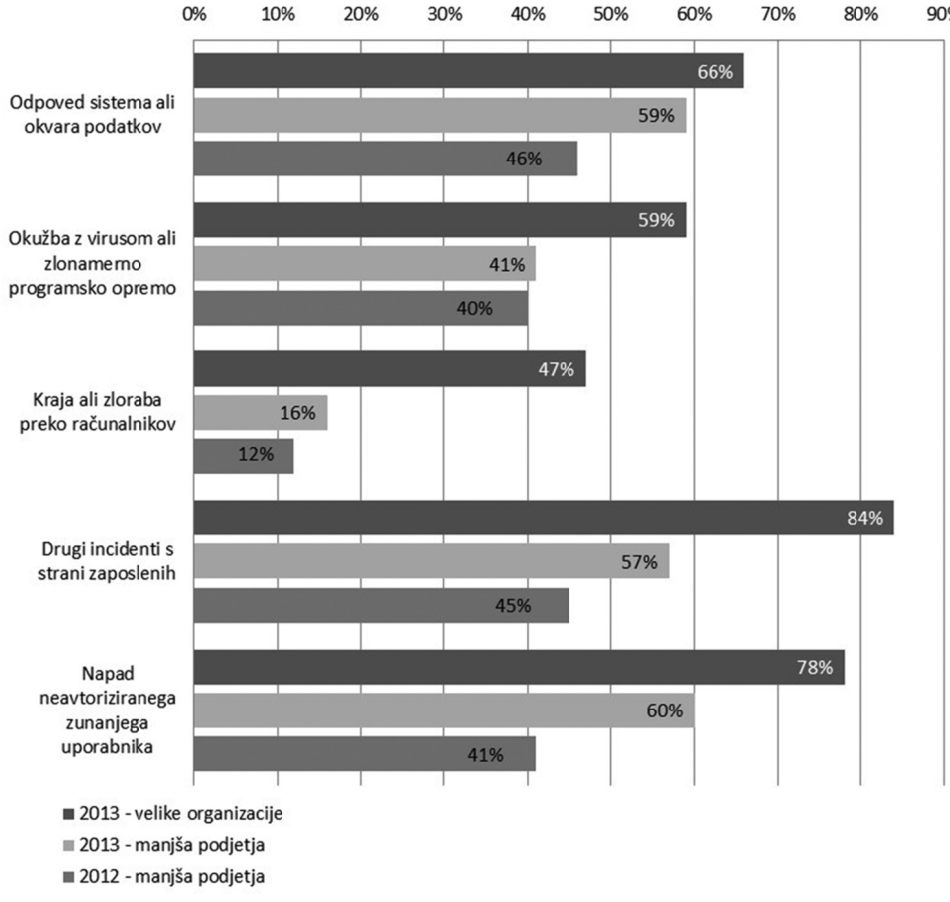


Vir: CSI, Computer Crime and Security Survey, 2011.

Po raziskavi BIS (2013) so najpogostejši incidenti okvara sistema ali uničeni podatki, okužba z virusom ali zlonamerno kodo ter kraja. Rezultati so prikazani na Sliki 7.

Dejstvo je, da se število groženj z razvojem tehnologije, kot so brezžična omrežja in mobilne pametne naprave, nenehno povečuje (Swartz, 2005). Po podatkih CERT-a (*Computer Emergency Response Team*), ki zbira podatke o varnostnih incidentih že vse od leta 1988, se je število incidentov dramatično povečalo od leta 1998. Na primer, leta 1998 je CERT objavil 3.734 incidentov, povezanih z varnostjo, medtem ko je bilo leta 2003 teh incidentov že 137.529 (CERT, 2008).

Slika 7: *Vrste napadov, ki jih je podjetje že utrpelo*



Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

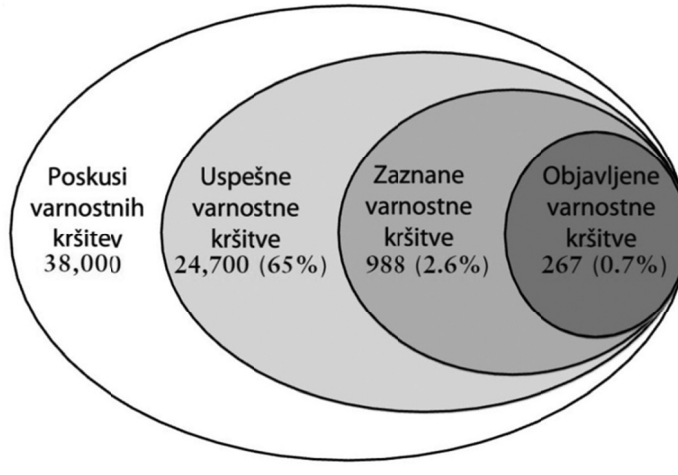
Strokovnjaki za varnost se strinjajo, da je število dejanskih incidentov precej večje, kot pa prikazujejo uradno objavljeni podatki, in sicer zaradi zatajitve nastalih incidentov zaradi neznanja ali pa zaradi zaščite dobrega imena.

Veliko podjetij namreč nima vzpostavljenega sistema za sistematično odkrivanje, nadzor in beleženje varnostnih incidentov, zato ostane veliko varnostnih kršitev nezaznavnih. Poleg tega o številnih varnostnih kršitvah nikoli ne poročajo, ker se podjetja s temi problemi ukvarjajo interno. Podjetja, ki doživijo napad,

pogosto o tem raje molčijo, kot da bi napad objavila. Če namreč javno razkrijejo varnostni incident, lahko tvegajo zmanjšanje svojega ugleda, izgubo zaupanja strank ali, kar je še huje, razkrivajo svoje ranljivosti drugim zlonamernežem. V zadnji raziskavi CSI (2011) je bilo le 22 % sodelujočih pripravljenih razkriti podrobnosti o finančnih izgubah, ki so jih utrpeli, in to kljub anonimnosti raziskave.

Koliko kršitev je dejansko zaznanih in objavljenih, dobro prikazujejo rezultati raziskave, s katero je Ameriška agencija za obrambo informacijskih sistemov (*Defense Information Systems Agency – DISA*) analizirala ranljivosti in ocenjevala različna tveganja. DISA v poročilu ocenjuje, da ostaja 96 % uspešnih kršitev nezaznavnih, izmed vseh zaznanih pa poročajo le o 27 %. Podatki so predstavljeni na Sliki 8.

Slika 8: *Rezultati raziskave analiza ranljivosti in ocenitve tveganja*

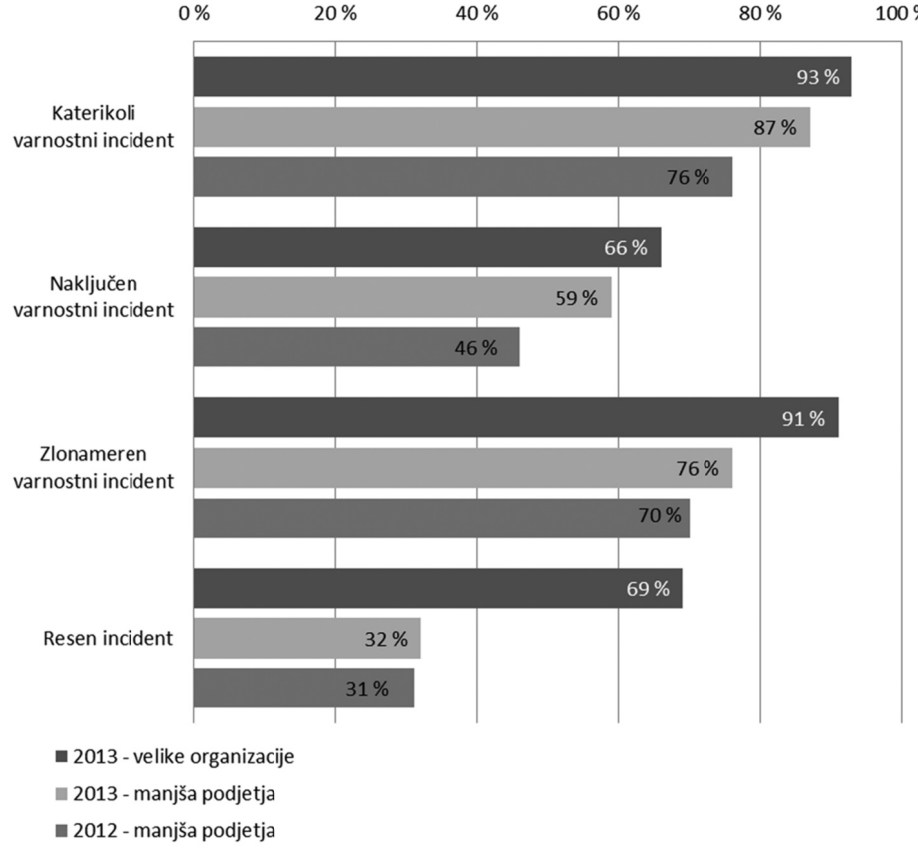


Vir: K. J. Soo Hoo, How Much Is Enough? A Risk-Management Approach to Computer Security, 2000.

Raziskava je bila sicer izvedena leta 1996 znotraj programa Vulnerability Analysis and Assessment Program, zato so navedeni podatki že zastareli, vendar vseeno kažejo neko razmerje med številom izvedenih groženj in javno objavljenimi podatki.

Po zadnji raziskavi, ki jo je v letu 2013 opravil Department for Business Innovation & Skills v Veliki Britaniji (BIS, 2013), je kar 93 % velikih organizacij imelo v preteklem letu varnostni incident. Za več kot 10 % se je povečalo število malih podjetij, ki so imela v zadnjem letu varnostni incident (s 76 % v letu 2012 na 87 % v letu 2013).

Slika 9: *Doživeti varnostni incidenti v preteklem letu*



Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

Obenem se je močno povečalo tudi povprečno število incidentov, ki jih je zaznalo posamezno podjetje. Za večje organizacije se je povprečno število incidentov povečalo z 71 (v letu 2012) na 113 (v letu 2013). Tudi pri manjših podjetjih je

opazno občutno povečanje števila zaznanih incidentov, z 11 v letu 2012 na 17 v letu 2013. Rezultati so prikazani na Sliki 9.

2.2.2 Povzročitelji groženj

Vsaka grožnja ima izvor oziroma **povzročitelja grožnje**, teh pa je lahko več vrst (Mayer et al., 2007). Grožnje lahko izhajajo iz narave, posameznikov, skupin ali organizacij, ki lahko namerno ali nenamerno povzročijo kršitve informacijske varnosti. Grožnja je na primer tornado, ki lahko uniči računalniško strojno opremo podjetja, ravno tako pa je grožnja kriminalec, ki namerava vdreti v računalniški sistem organizacije, da bi ukradel številke kreditnih kartic ali opravil nedovoljeno transakcijo denarja. V splošnem povzročitelje grožnje delimo na dogodke, povezane z okoljem in naravnimi pojavi, ter na kriminalne grožnje, ki jih imenujemo tudi kibernetske grožnje (Bojanc, 2010).

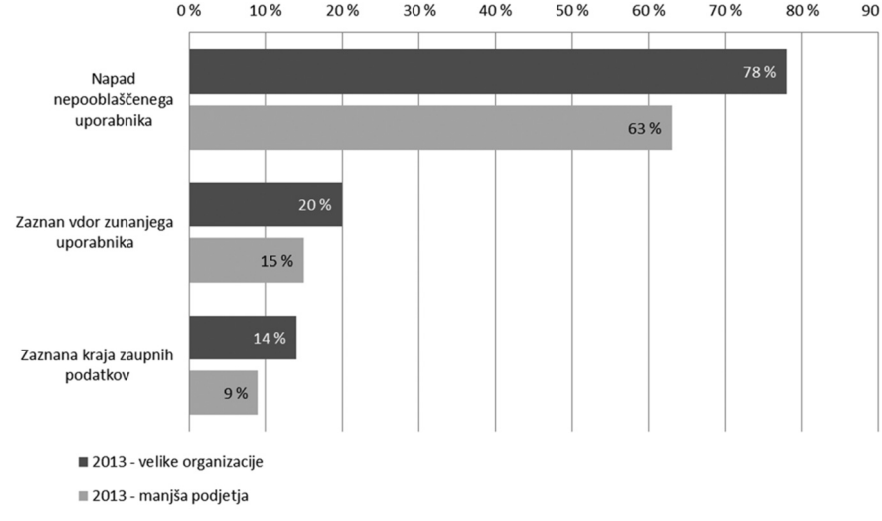
Naravni pojavi so lahko odvisni od lokacije, saj so nekatere lokacije bolj dovzetne za določene okoljske vplive in naravne nesreče kot druge. Nekatere vrste nesreč niso geografsko odvisne (na primer požar, udar strele), medtem ko so druge specifične za določena območja (na primer poplave, potresi, izbruh vulkana). Grožnje, ki izvirajo iz okolja, so lahko okvare mehanske in električne opreme (na primer računalniška oprema, klimatska naprava, telekomunikacijska oprema) ter prekinitev napajanja ali inštalacijskih vodov (na primer vodovodna, plinska, električna inštalacija, izpad elektrike) (ISO 27005, 2011).

Če je povzročitelj grožnje **človek**, je to lahko oseba, zaposlena v podjetju (notranji, pooblaščeni uporabnik), ali zunanji (nepooblaščeni) uporabnik. **Zunanji oziroma nepooblaščeni uporabnik** je lahko kdor koli, ki ne izvaja podpore poslovnim procesom in poskuša prekiniti produktivnost ali delovanje sistema. Taki uporabniki so na primer posamezniki, ki poskušajo vdreti v sistem zgolj za izziv, tatovi, nezadovoljni bivši zaposleni, industrijski vohuni, organizirani kriminalci, zunanji agenti ali teroristi. Grožnje lahko zunanji povzročitelj izvaja odkrito, kot je na primer sabotaža, ali pa prikrito. **Notranji oziroma pooblaščeni uporabniki** pa lahko pomenijo grožnjo, kadar presežejo svoja pooblastila ali storijo nenamerno napako (na primer brisanje datotek, fizične

nesreče), s čimer vplivajo na delovanje sistema, tako da ta ne opravlja svoje naloge. Lahko pa izvedejo dejanja zaradi osebne koristi. Težava je, ker veliko zaposlenih v podjetjih na varnost pogosto ne gleda kot na prednostno nalogo ali se ne zavedajo svoje ogroženosti (Boss, 2007).

V raziskavi BIS (2013) je ugotovljeno, da bilo je kar 78 % velikih organizacij v zadnjem letu napadenih s strani nepooblaščenega zunanjega uporabnika oziroma kibernetskega kriminalca. Kar 20 % velikih organizacij je zaznalo, da je zunanji uporabnik uspešno vdrl v njihovo omrežje, od tega je 14 % organizacij zaznalo, da je zunanji porabnik ukradel njihovo intelektualno lastnino ali zaupne podatke. Podatki za mala podjetja so le malo nižji, kar je presenetljivo, ker ta podjetja naj ne bi bila pogosta tarča napadalcev. Rezultati so prikazani na Sliki 10.

Slika 10: *Zaznani vdori v omrežje in kraje zaupnih podatkov*

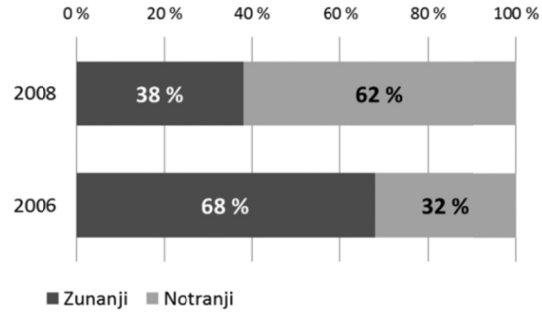


Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

Po podatkih v raziskavah postajajo notranji uporabniki čedalje pogostejši povzročitelji grožnje (CSI, 2011). Z leti se spreminja tudi razmerje med notranjimi in zunanjimi povzročitelji. Po raziskavi BERR (2008) je bilo leta 2006 občutno več tistih podjetij, pri katerih so najhujše incidente povzročili zunanji uporabniki, leta 2008 pa je bilo stanje ravno obratno. To pomeni, da je

pri teh podjetjih zelo pomembno izobraževanje in ozaveščanje uporabnikov. Rezultati so prikazani na Sliki 11.

Slika 11: *Ali je najhujši varnostni incident povzročil zunanji ali notranji uporabnik*



Vir: BERR, BERR 2008 Information Security Breaches Survey, Technical Report, 2008.

Človeške grožnje lahko razdelimo na namerne in nenamerne. **Namerne grožnje** lahko povzročijo zunanji ali notranji uporabniki, ki želijo škodovati podjetju, **nenamerne grožnje** (napake) pa lahko povzročijo zaposleni v podjetju pri svojem delu (na primer brisanje datotek, fizične nesreče …) ali pa neustrezno usposobljeno IT-osebje podjetja. Primeri posameznih groženj so prikazani v Tabeli 2.

Tabela 2: *Primeri groženj različnih povzročiteljev*

Človeški dejavnik		**Okoljski/naravni dejavnik**
Namerne grožnje	**Nenamerne napake**	
prisluškovanje sprememba podatkov vdor v sistem zlonamerna koda kraja	napake in izostanki izbris datotek nepravilno usmerjanje fizične nesreče	potres udar strele poplava požar izpad elektrike

Vir: ISO 13335-1, 2004.

Po podatkih BIS (2013) je bilo kar 36 % najhujših varnostnih incidentov povzročeno nenamenoma zaradi človeške napake, 10 % pa zaradi namerne zlorabe sistema s strani zaposlenih.

2.2.3 Tehnike napadov

Povzročitelj grožnje za dosego želenega učinka na napadenem sredstvu izvede določeno aktivnost oziroma uporabi določeno **tehniko napada** (Farahmand, 2004). Tehnike napada se neprenehoma razvijajo vzporedno z razvojem tehnologije, pri tem pa se še vedno pogosto uporabljajo starejše obstoječe tehnike. Schneier (2002) kot primer tehnike, ki se že dalj časa pogosto uporablja, navaja napade s prekoračitvijo pomnilnika (angl. *buffer overflow*). Ti napadi so ena izmed najstarejših vrst računalniških napadov. Prvič so bili omenjeni po letu 1960, v 70. letih pa je bila ta tehnika med najpogosteje uporabljenimi zlasti za napade v omrežju povezanih računalnikov. Zgodovinski pomen ima črv Morris, ki je s prekoračitvijo pomnilnika v letu 1988 onemogočil 10 % gostiteljskih računalnikov na internetu (Morris worm, 2008; Bluejackel's finds, 2009). Napadi s prekoračitvijo pomnilnika so še danes velik problem, saj je največ napadov na internetu ravno te vrste, čeprav so na voljo avtomatični programi, ki lahko poiščejo in odpravijo tovrstne ranljivosti že med razvojem informacijskega sistema. Seveda je veliko napadov, ki so bolj prikriti in jih je težje odpraviti kot napade s prekoračitvijo pomnilnika, vendar so slednji še vedno zelo pogosti in povzročajo škodo.

Na splošno lahko tehnike napadov razvrstimo v več kategorij (Bojanc, 2010):

- **Fizični napadi** oziroma nepooblaščen dostop do varovanih področij, kot so poslovni prostori, strežniška soba ali drugi varovani prostori.
- **Napadi na osebje**, ki ima določeno stopnjo dostopa in privilegije v sistemu. Osebje so lahko navadni uporabniki ali upravljavci sistema (na primer sistemski analitiki, programerji in sistemski administratorji). Povzročitelj grožnje lahko zlorabi osebje za vdor v sistem, omejitev delovanja sistema ali pa povzroči, da posamezniki postanejo nezadovoljni in nemotivirani. Primer takšne tehnike je socialni inženiring.
- **Napadi na strojno opremo**, s katerimi se lahko doseže, da strojna oprema omejuje ali preprečuje delovanje sistema. Lahko gre za fizični napad na opremo, lahko je to hrošč, podtaknjen v krmilnik strojne opreme, ali napad na podporno opremo. Strojna oprema običajno vključuje vsak kos opreme, ki je del informacijskega sistema (na primer strežniki,

periferna oprema in komunikacijska oprema), ter podporno opremo, kot so napajalniki, klimatske naprave, rezervno energetsko napajanje itd.

- **Napadi na programsko opremo** so lahko usmerjeni na operacijski sistem ali aplikacijske programe. Lahko obsegajo majhne spremembe, ki so uvedene skrivoma in ogrozijo delovanje sistema, ali manj diskretne spremembe, ki povzročijo uničenje podatkov ali drugih pomembnih funkcionalnosti sistema.
- **Napadi na postopke**, ki zaradi pomanjkanja ustreznih kontrol ali neustreznega izvajanja kontrol omogočajo povzročitelju grožnje vdor v sistem. Primer zlorabe postopkov je, da bivši zaposleni za dostop v sistem še dolgo uporabljajo stara veljavna gesla, ki jih lahko tretje osebe razkrijejo.

2.2.4 Ranljivosti sredstev

Povzročitelji groženj uspešno napadejo informacijska sredstva, tako da izkoristijo njihovo ranljivost. Ranljivost sredstva lahko opredelimo kot šibkost sredstva ali ukrepa, ki jo grožnja lahko zlorabi ter s svojo prisotnostjo v sistemu poveča verjetnost za uspešen napad na sistem (ISO 27000, 2014). Na primer, puščanje prenosnega računalnika v nezaklenjeni namesto v zaklenjeni pisarni znatno poveča ranljivost prenosnega računalnika za grožnjo kraje. Verjetnost, da bo prenosnik dejansko ukraden, je odvisna od prisotnosti grožnje in ranljivosti. Ranljivost sama po sebi ne povzroča škode, je zgolj pogoj (ali niz pogojev), ki omogoči nastanek škode (ISO 13335-1, 2004).

Povzročitelji groženj izkoriščajo različne vrste ranljivosti. Veliko varnostnih incidentov nastane zaradi ranljivosti, ki je posledica napak v programski opremi (Arora & Telang, 2005). Strokovnjaki ocenjujejo, da je na vsakih 1000 vrstic programske kode približno 20 napak in da število prijavljenih ranljivosti z leti narašča (Dacey, 2003). Poleg ranljivosti tehnične narave je veliko ranljivosti povezanih tudi s človeško naravo. Taki primeri so uporaba šibkih gesel ali neustrezno varovanje gesel, nerazumevanje ali ignoriranje varnostnih politik, nenadzorovano odpiranje priponk v e-poštnih sporočilih, ogled sumljivih spletnih strani ali nameščanje programske opreme, ki vsebuje zlonamerno kodo. Standard ISO 27005 (2011) podaja naslednji popis pogostih ranljivosti:

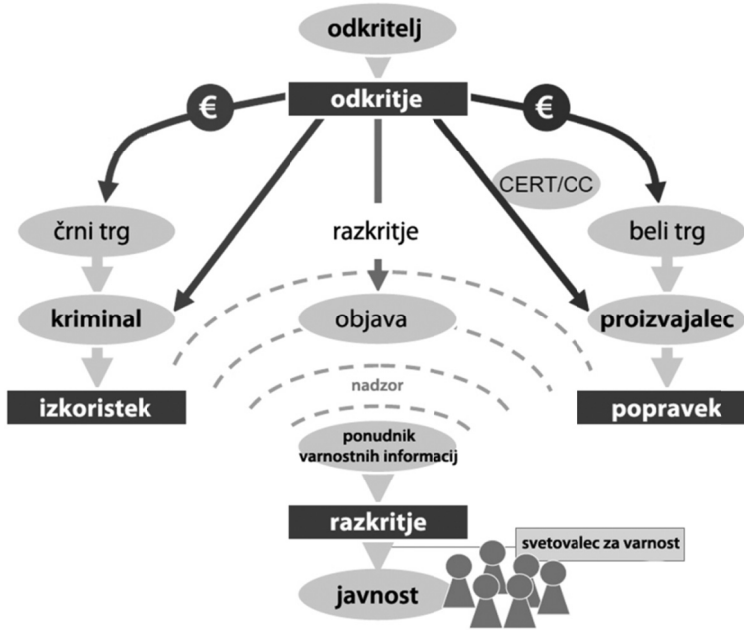
- slaba skrb za gesla (na primer zapisovanje gesel),
- splošno pomanjkanje zavedanja zaposlenih za informacijsko varnost,
- nepravilna uporaba interneta (na primer ogled nedovoljenih vsebin),
- nepravilna uporaba programskih licenc (piratstvo),
- neustrezna hramba podatkov,
- slaba varnost delovnih postaj in prenosnikov,
- pomanjkanje nadzora dostopa,
- pomanjkanje naprav za odkrivanje požarov,
- nezaklepanje računalnika ob zapustitvi delovnega mesta,
- pomanjkanje revizijske sledi,
- pomanjkanje dokumentacije,
- zapleten uporabniški vmesnik,
- napačna dodelitev pravic za dostop,
- nepravilni datumi,
- nejasne specifikacije za razvijalce,
- omogočeni nepotrebni strežniški servisi,
- pomanjkanje varnostnih kopij,
- dovoljeni nepotrebni mrežni protokoli,
- nefiltriranje prometa med mrežnimi segmenti,
- nestabilno električno omrežje,
- pomanjkanje ali nedefinirani disciplinski postopki v primeru varnostnih incidentov,
- pomanjkanje politike za e-pošto,
- lokacija podjetja na poplavnem področju.

Informacijski sistemi postajajo čedalje bolj kompleksni (Schneier, 2004a; Perrow, 1999), s tem pa se njihova ranljivost veča. S stališča kupca je kompleksnost sistema vsekakor dobra, saj zanj pomeni več izbire, več možnosti, več nalog, ki jih ta lahko naredi. Po drugi strani pa se število ranljivosti s kompleksnostjo informacijskega sistema povečuje, zato se varnost sistema zmanjšuje. Varnostno testiranje kompleksnih sistemov je težavno, saj je preverjanje vseh možnih konfiguracij v kompleksnih sistemih praktično nemogoče. Dodatno težavo povzroča modularnost sodobnih informacijskih sistemov. Modularnost je seveda dobra, saj omogoča medsebojno neodvisnost posameznih komponent informacijskega sistema, vendar pa se lahko ob združevanju modulov, ki med

seboj sodelujejo, pojavijo nove ranljivosti. Kot poudarja Schneier (2004a), je varnost celotnega sistema tolikšna kot varnost najšibkejšega člena, kar pomeni, da ena ranljivost lahko uniči celoten sistem. Rešitev problema je vključevanje zaščitnih modulov za varnost v procese.

Camp in Wolfram (2000) sta že leta 2000 opredelila ranljivost kot tržno blago in napovedala obstoj trga ranljivosti. Na tem trgu naj bi proizvajalec ali lastnik sredstva ponujal nagrado za osebo, ki odkrije ranljivost. Schechter (2004) je ta koncept razširil na odprt trg še neodkritih ranljivosti. Tržna cena za najdeno in poročano ranljivost je ocena stroškov iskanja ranljivosti v programski opremi.

Slika 12: *Glavni procesi varnostnega ekosistema glede ranljivosti*



Vir: S. Frei et al., Modelling the Security Ecosystem – The Dynamics of (In)Security, 2009.

Da trg ranljivosti dejansko obstaja, sta potrdili podjetji iDefense in Tipping Point, ki odprto kupujeta ugotovitve uporabnikov o ranljivosti. Njihov poslovni model je istočasna objava podatkov o ranljivosti njihovim strankam in proizvajalcu, na katerega se ranljivost nanaša. Njihove stranke lahko na ta način

naredijo varnostne posodobitve (na primer na požarnih pregradah) pred drugimi. Drugi primer trga ranljivosti je CERT, ki pa odkrite ranljivosti ne zaračunava. CERT deluje kot informacijski posrednik med uporabniki, proizvajalcem in dobronamernim odkriteljem, ki prostovoljno in brez finančnih koristi poroča o ranljivosti. Da bi zagotovili, da takšnih javnih obvestil ne bi izkoriščali napadalci, CERT najprej posreduje odkrite ranljivosti proizvajalcu, da pripravi ustrezen popravek in čaka na primeren čas, preden javno razkrije ranljivost (Bojanc & Jerman-Blažič, 2008). Slika 12 prikazuje procese med posameznimi fazami življenjskega cikla ranljivosti (Frei, Schatzmann, Plattner & Trammell, 2009).

O tem, ali je javno razkritje odkritih ranljivosti dobro ali ne, je bila v preteklosti pogosto vroča debata med varnostnimi strokovnjaki (Anderson & Schneier, 2005; Kannan & Telang, 2004; Arora & Telang, 2005). Na eni strani so zagovorniki odprtokodnih skupnosti, ki zagovarjajo, da je iskanje in razkrivanje ranljivosti družbeno zaželeno. Rescorla (2004) po drugi strani trdi, da v programski opremi z mnogo ranljivosti odstranitev ene ranljivosti le malo doprinese k skupni varnosti, saj je velika verjetnost, da bo napadalec kasneje odkril nove ranljivosti. Anderson (2005) je leta 2002 pokazal, da objava ranljivosti enako pomaga tako napadalcem kot proizvajalcem. Pri tem pa razkritje ranljivosti pomaga motivirati proizvajalce, da odpravijo hrošče v programski opremi (Arora, Telang & Xu, 2004b). Arora je pokazal, da javno razkritje ranljivosti proizvajalce spodbudi, da se s popravki odzovejo hitreje (Arora et al., 2004b). Ker so ranljivosti javno objavljene, to izkoriščajo tudi napadalci, zato napadi na začetku naraščajo, sčasoma pa se število objavljenih ranljivosti zmanjšuje.

CERT navaja, da bi lahko z ažurnim nameščanjem varnostnih popravkov, ki jih proizvajalci programske opreme razvijajo za odpravo ranljivosti, preprečili približno 95 % varnostnih incidentov (Dacey, 2003). Podjetja se morajo prilagoditi in varnostne popravke namestiti takoj, ko jih objavi proizvajalec (August & Tunca, 2005; Cavusoglu, Cavusoglu & Zhamg, 2006). Cavusoglu pa je pokazal, da sinhronizacija izida popravka in posodobitvenih ciklov zmanjšuje izgube (Cavusoglu, Cavusoglu & Zhang, 2008). Časovno okno med identifikacijo ranljivosti in ugotovitvijo načina za zlorabo se je v preteklih letih že dramatično zmanjšalo. V preteklosti pa je bilo veliko primerov, ko številni sistemi tudi več mesecev ali celo let niso bili posodobljeni, kar je povzročilo

resne posledice in škodo (Shostack, 2003; McGhie, 2003; Moore, Shannon & Brown, 2002). En tak primer je črv Nimbda, ki je leta 2001 samo v prvih 24 urah delovanja okužil 2,2 milijona računalnikov, popravek za odpravo te ranljivosti pa je bil na voljo že skoraj eno leto pred incidentom (Dacey, 2003). Drugi primer posledic zapoznele namestitve popravkov je črv SQL Slammer. Čeprav je bil popravek javno na voljo že 6 mesecev prej, je črvu uspelo okužiti kar 90 % ranljivih sistemov. Poleg tega je še več drugih primerov (na primer črva Code Red in Blaster), ko je bil popravek za ranljivost na voljo že precej časa pred incidentom (Strickland, 2008). Tudi v Sloveniji imamo primer zlonamerne kode, ki jo je zlonamerni izdelovalec iz Slovenije prodajal po svetu. Koda je okužila veliko računalnikov in povzročila finančno škodo – nepooblaščen prenos tujega denarja (SI-CERT, 2013a). Sodni postopek se je zaključil tako, da je bil izdelovalec obsojen na denarno in zaporno kazen.

2.3 Investicije v varnostne ukrepe in rešitve

2.3.1 Vrste varnostnih ukrepov

V prejšnjem poglavju smo si ogledali, kje so viri tveganja, v tem poglavju pa si poglejmo, kaj lahko podjetja storijo, da bi se zaznana tveganja zmanjšala. Najpogosteje se tveganja zmanjšujejo z investicijami v varnostne ukrepe in rešitve. Varnostni ukrepi so aktivnosti, postopki ali mehanizmi, ki zmanjšujejo verjetnost ali posledico varnostnih incidentov, na tveganje pa vplivajo različno. Lahko odkrivajo in preprečujejo incidente, odvračajo grožnje, omejujejo tveganja, popravljajo nastalo škodo zaradi incidenta, pomagajo pri okrevanju po incidentu, izvajajo nadzor ali ozaveščajo (ISO 13335-1, 2004).

Varnostni ukrepi so lahko fizične ovire, senzorji, programska oprema, algoritmi, izboljšave obstoječih politik za varnost ali postopkov za zagotavljanje varnosti. Glede na učinke lahko varnostne ukrepe razvrstimo v tri glavne skupine: preventivne, korektivne in detekcijske ukrepe (NIST 800-14, 1996). **Preventivni ukrepi** zmanjšujejo število uspešnih incidentov in s tem verjetnost za incident, **korektivni ukrepi** zmanjšujejo izgubo v primeru incidenta, **detekcijski ukrepi** pa skrajšajo čas, v katerem se incident zazna, in omogočajo zbiranje podatkov o

grožnjah. V Tabeli 3 je prikazanih nekaj primerov različnih vrst varnostnih ukrepov.

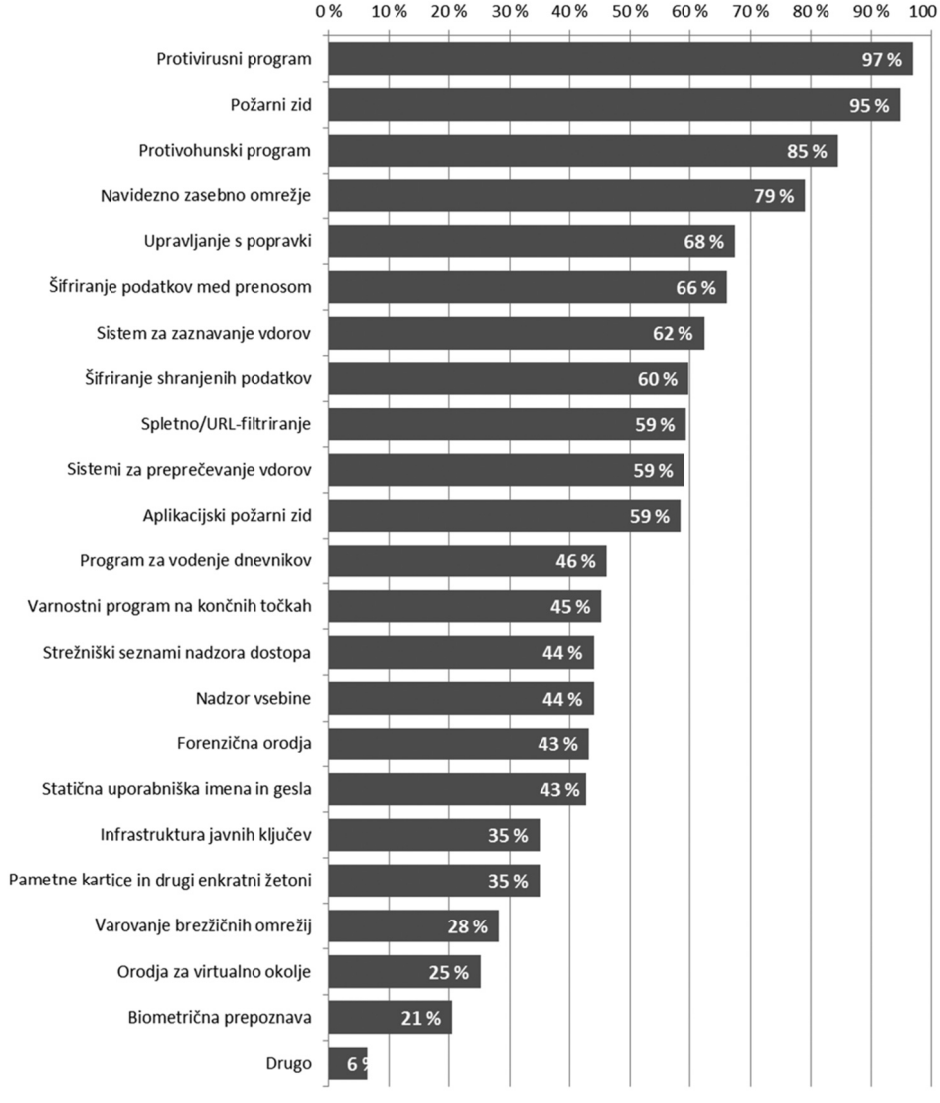
Tabela 3: *Primeri različnih vrst varnostnih ukrepov*

Preventivni varnostni ukrepi	Korektivni varnostni ukrepi	Detekcijski varnostni ukrepi
varnostna politika	varovalna pravila in postopki (okrevalni načrt, načrt neprekinjenega delovanja …)	sistemi za zaznavanje vdorov v omrežju (IDS)
kriptografija (šifriranje za potrebe zaupnosti, elektronski podpis)	varnostno kopiranje in arhiviranje	limanica (angl. *honeypot*)
varna arhitektura omrežja in aplikacij	uporaba programa za prijavo incidentov	zaznavanje vdorov na računalnikih
ažurno posodabljanje programske opreme s popravki	redundančnost sistema in okolij	
požarni zid	zavarovanje tveganja	
sistemi za preprečevanje vdorov v omrežju (IPS)	gostovanje storitve (podpisan SLA)	
mehanizmi overjanja in avtorizacije	nadomestni sistemi električnega napajanja	
protivirusna programska oprema		
program za zavedanje o varnosti (izobraževanje uporabnikov in IT-strokovnjakov)		
gostovanje storitve (podpisan SLA)		

Varnostni strokovnjaki že dalj časa ugotavljajo, da tveganja težko učinkovito zmanjšamo samo z uvedbo tehničnih rešitev, zato so nujno potrebni tudi človeški viri, ki znajo te tehnične rešitve pravilno uporabljati (Gordon & Loeb, 2005). Po raziskavi CSI (2011) sta v podjetjih najpogosteje uporabljena varnostna

ukrepa protivirusna programska oprema in požarni zid, ki ju ima praktično vsako podjetje. Podatki o najpogosteje uporabljenih varnostnih ukrepih so prikazani na Sliki 13.

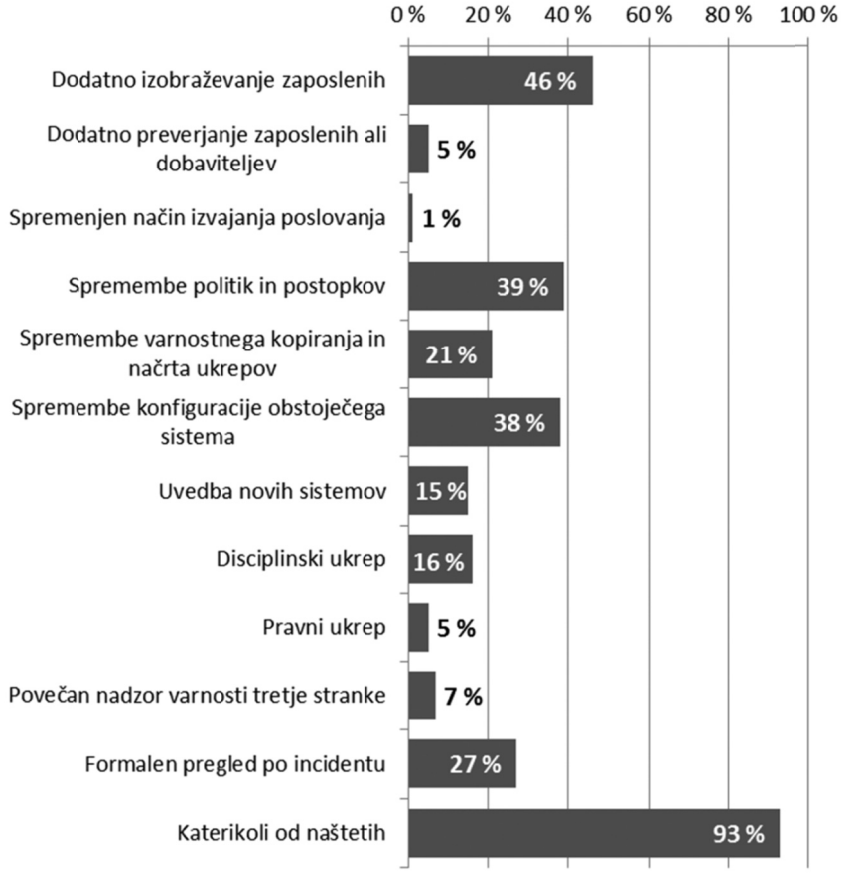
Slika 13: *Vrste uporabljenih varnostnih ukrepov v odstotkih glede na delež sodelujočih podjetij*



Vir: CSI, 2010/2011 Computer Crime and Security Survey, 2011.

Raziskava BIS (2013) je pokazala, da sta ob hujših varnostnih incidentih najpogostejša organizacijska ukrepa izobraževanje ter spremembe politik in postopkov. Rezultati so prikazani na Sliki 14.

Slika 14: *Izvedeni koraki po najhujšem incidentu v letu*

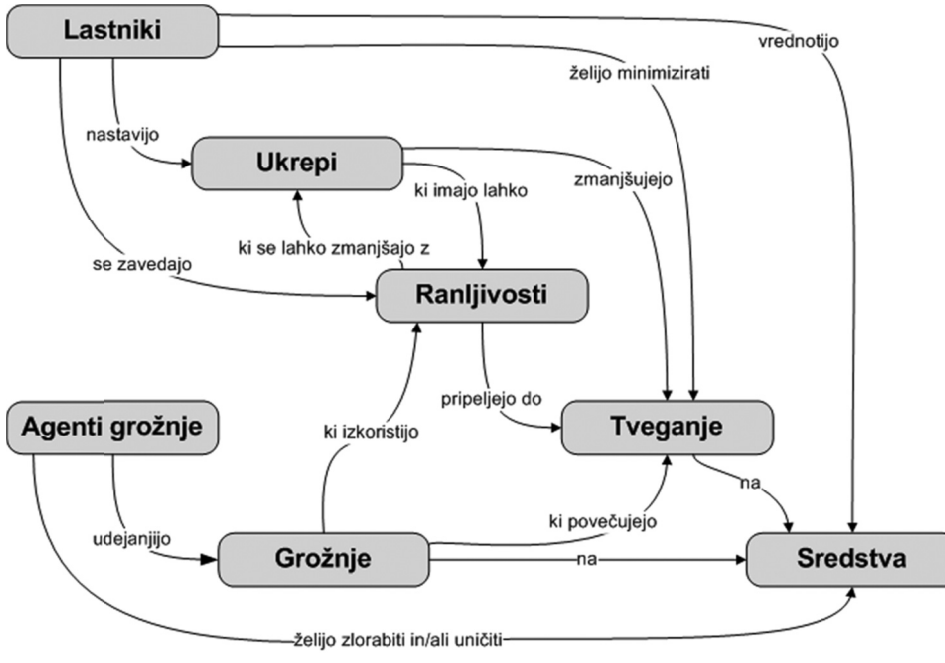


Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

2.3.2 Kaj vpliva na izbiro ukrepa?

Kot smo spoznali, grožnje in ranljivosti sredstev povečujejo tveganje, ukrepi pa tveganja zmanjšujejo. Relacije med temi osnovnimi elementi, ki vplivajo na tveganje, so predstavljene na Sliki 15. Kot je prikazano na sliki, imajo lahko varnostni ukrepi tudi povratno negativno povezavo. Uvedeni ukrepi imajo lahko nove ranljivosti, ki lahko povzročijo nova tveganja, zato je zelo pomembno, da podjetja natančno ocenijo vpliv varnostnega ukrepa in so pri tem pozorna na nova tveganja, ki jih ukrepi lahko prinašajo (Schneier, 2003; Schneier, 2004b).

Slika 15: *Prikaz odvisnosti med tveganjem, sredstvi, ranljivostmi, grožnjami in ukrepi*



Vir: ISO 15408-1, 2009.

Pri izbiri varnostnega ukrepa je treba upoštevati dilemo med varnostjo in uporabnostjo (funkcionalnostjo), saj si varnost in uporabnost sistema med seboj nasprotujeta. Če se izboljša varnost sistema, se s tem omeji njegova uporabnost (Schneier, 1996). Informacijska varnost obvladuje in nadzoruje dostop do

informacij in s tem omejuje svobodo posameznika pri prosti uporabi tehnologije v polnem obsegu. Po drugi strani pa je ravno zmožnost prostega pretoka informacij ključna prednost informacijske tehnologije. Soo Hoo (2000) navaja, da podjetja v konkurenčnem okolju običajno postavljajo uporabnost pred varnost.

Kako dobro ukrep zmanjšuje tveganja, se ocenjuje z njegovo učinkovitostjo. Za določene vrste ukrepov, kot so požarni zid, protivirusna programska oprema in sistemi za detekcijo vdorov v sistem (angl. *Intrusion Detection System – IDS*), merjenje učinkovitosti že obstaja, za ostale ukrepe pa je ocenjevanje učinkovitosti zaradi kompleksnosti problema lahko težavno. Težavnost povečuje tudi to, da je problem odvisen od ljudi z različnimi videnji in navadami ter nenehno spreminjajočimi se tehnologijami. Če so na voljo pretekli podatki v zvezi z ukrepom in incidenti, se ti lahko analizirajo in uporabijo za merjenje učinkovitosti, v nasprotnem primeru pa lahko pri oceni učinkovitosti pomaga varnostni strokovnjak. Butler (2002) je raziskoval, ali je s subjektivno oceno varnostnega strokovnjaka sploh mogoče dobiti smiselne in uporabne vrednosti, in ugotovil, da je s strani varnostnih strokovnjakov mogoče zagotoviti grobe kvantitativne ocene učinkovitosti varnostnih ukrepov.

2.3.3 Zmanjšanje tveganja prek zavarovalnice

Podjetje lahko varnostna tveganja zmanjša tudi tako, da se zavaruje in tveganje prenese na zavarovalnico, kar pa ne zmanjšuje verjetnosti za varnostni incident, temveč zmanjšuje izgube ob morebitnem incidentu. Zavarovanje je običajno primerno za tveganja, za katera je majhna verjetnost, da bo prišlo do incidenta, izgube ob incidentu pa so lahko visoke. Pozitivna stran zavarovanja je tudi ta, da spremenljive stroške tveganja prevede v fiksne stroške, ki jih je mogoče zajeti v proračun (Schneier, 2004a). Pri zavarovanju informacij se izgube krijejo iz dveh razredov tveganja (Gordon, Loeb & Sohail, 2003).

- Tveganja prve osebe se nanašajo neposredno na imetnika zavarovanja. Zavarovanja običajno vključujejo izgubo dobička zaradi kraje poslovnih skrivnosti, uničevanja premoženja (programska oprema, strojna oprema in podatki), prekinitev poslovanja zaradi vdora hekerja ali napadov virusov in napake programske opreme itd.

- Tveganja tretje stranke pokrivajo finančno kompenzacijo izgub zaradi tretje stranke. Na primer škoda, povzročena z nenamernim posredovanjem računalniških virusov, pogodbene kazni zaradi nedelovanja IT-okolja, objava vsebin na spletni strani podjetja (kršitev avtorskih pravic), kraje informacij o tretjih osebah.

Obvladovanje tveganja skozi zavarovanje raziskujejo mnogi avtorji (Baer, 2003; Conrad, 2005; Farahmand, Navathe, Sharp & Enslow, 2005; Geer, 2004; Haimes & Chittester, 2005; Soo Hoo, 2000; Baer & Parkinson, 2007). V preteklosti je bilo kar nekaj poskusov opredelitve zavarovalniškega sektorja v informacijski varnosti, pri tem pa zavarovalnice pokrivajo naslednja področja (Gordon et al., 2003; Schneier, 2001):

- odgovornosti spletnih vsebin,
- poklicne odgovornosti,
- odgovornosti mrežne varnosti tretjih oseb,
- izgubo informacij,
- izgubo prihodkov,
- internetno izsiljevanje.

Trenutno sta vodilna ponudnika zavarovanja za primere informacijskih varnostnih tveganj AIG in Lloyd's of London. Slednji je v letu 2003 tudi prvi ponudil posebne zavarovalne police za informacijsko varnost (Counterpane, 2000). Po raziskavi CSI 2007 le 29 % podjetij uporablja zavarovanje informacij (CSI, 2007), nekateri raziskovalci pa svarijo pred uporabo tovrstnih zavarovanj in trdijo, da so trenutne zavarovalne police, ki jih ponujajo zavarovalnice, skoraj neuporabne (Majuca, Yurcik & Kesan, 2006).

Anderson in Moore (2008) opozarjata, da je trenutni informacijsko-zavarovalniški trg še precej nerazvit in slabo izkoriščen. Največja težava za zavarovalnice je, kako natančneje vrednotiti informacijsko varnostna tveganja, saj nimajo dobrih aktuarskih podatkov, na podlagi katerih bi lahko izračunavale premije. Poleg tega je za informacijska tveganja značilna lokalna in globalna soodvisnost tveganja (Böhme & Kataria, 2006). To pomeni, da je IT-infrastruktura podjetja povezana z drugimi zunanjimi okolji, zato napaka v drugih okoljih lahko vpliva na varnost informacij lokalnega podjetje. To izkoriščajo tudi napadalci in

dostikrat zlorabijo ranljivost v programu, ki ga uporablja veliko podjetij. Poseben problem nastaja s pojavom oblačnega računalništva in ponujenih storitev, ki jih uporablja čedalje več slovenskih podjetij. Ponudniki teh storitev, ki so za podjetja cenovno ugodne, ker se tako podjetja razbremenijo stroškov postavitve in vzdrževanja lastne IT-infrastrukture, imajo povezane gostiteljske računalnike po vsej zemeljski obli. To pomeni, da podjetja, ki uporabljajo te storitve, nimajo podatkov, kje se njihove informacije hranijo in obdelujejo. Varovanje v teh novih oblikah uporabe IT še zmeraj ni dovolj raziskano in rešeno, ranljivost informacij uporabnikov teh storitev pa je veliko večja.

V Sloveniji zavarovalnice v zadnjem času že ponujajo nekatere zavarovalniške produkte, ki pokrivajo posamezna tveganja s področja informacijske varnosti (Bojanc, 2010). Že dalj časa je na voljo zavarovanje pred krajo strojne opreme v obliki vlomskega zavarovanja, ki zajema krajo v poslovnih prostorih in na terenu (na primer prenosni računalniki). Zavarovalnice v Sloveniji običajno krijejo stroške popravila ali zamenjave fizične opreme ter stroške demontaže in montaže te opreme. Za kritje stroškov vzpostavitve delovanja IT-sistema podjetja je potrebno posebno zavarovanje. Tehnično okvaro in nenamerno poškodbo strojne opreme pokriva strojelomno zavarovanje, namerno uničenje strojne opreme (na primer vandalizem, demonstracije) pa pokriva požarno zavarovanje. Možno je tudi zavarovanje pred nenamerno izgubo podatkov, pri katerem zavarovalnica krije stroške ponovnega vnosa podatkov. Za razliko od nenamernih škod so namerne škode vedno izključene iz zavarovanja. Možno je zavarovanje pred izgubo prihodkov zaradi okvare strojne opreme v obliki posebnega dogovora v okviru zavarovanja obratovalnega zastoja zaradi strojeloma ali streloloma. Ravno tako je možno zavarovanje pred izgubo prihodka zaradi naravnih/okoljskih pojavov (požar, poplava, potres, neurje …) v okviru zavarovanja obratovalnega zastoja zaradi požara. Zavarovalnice v Sloveniji ne ponujajo zavarovanja pred izgubo prihodkov zaradi prekinitve dobave storitev (elektrike, internetne povezave, vodovodne napeljave …).

2.4 Pristopi, procesi in sistemi za zagotavljanje varnosti

2.4.1 Obvladovanje tveganja

V preteklih poglavjih smo si ogledali osnovne elemente, ki so povezani z obvladovanjem varnostnih tveganj. Ogledali smo si informacije in sredstva ter kakšno vrednost imajo za podjetja. V nadaljevanju smo si ogledali, kaj so varnostna tveganja, kaj jih povzroča (grožnje in ranljivosti) ter kako tveganja zmanjšamo (ukrepi). Na Sliki 15 so prikazane odvisnosti med varnostnimi elementi, ki sodelujejo pri ravnanju s tveganjem, v tem poglavju pa bomo vse te elemente povezali v poslovni proces obvladovanja tveganja.

Obvladovanje tveganja (angl. *risk management*) je postopek ugotavljanja tveganja, ocenjevanje tveganja in sprejetje ukrepov za zmanjšanje tveganja na sprejemljivo raven (NIST 800-30, 2002). Podjetja večinoma že obvladujejo različne vrste poslovnih tveganj, zato so tveganja informacijske varnosti le še dodatna vrsta tveganja. Proces obvladovanja tveganja sestavljata dve glavni fazi: ocena tveganja in obravnava tveganja.

Ocena tveganja (angl. *risk assessment*) je celoten proces analize tveganja in vrednotenja tveganja (ISO Guide 73, 2009). Pri tem je analiza tveganja (angl. *risk analysis*) opredeljena kot sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja, vrednotenje tveganja (angl. *risk evaluation*) pa kot proces primerjave ocenjenega tveganja z danimi kriteriji tveganja, da se določi njegova pomembnost. Poenostavljeno povedano, ocena tveganja je proces, v katerem se možna tveganja identificirajo in zabeležijo ter za posamezno tveganje ovrednoti potencialna škoda in oceni verjetnost, da se bo dogodek zgodil. Cilj ocene tveganja je identifikacija in merjenje tveganja z namenom informiranja procesa odločanja. Za oceno tveganja potrebujemo podatke o informacijskih sredstvih v podjetju, o grožnjah, ki so jim sredstva izpostavljena, in o ranljivostih, ki jih grožnje lahko zlorabijo.

Ko podjetje ugotovi in oceni tveganja, se mora odločiti, kako bo posamezno tveganje obravnavalo. **Obravnava tveganja** (angl. *risk treatment*) je proces izbire in vpeljave ukrepov za spremembo tveganja (ISO Guide 73, 2009). V fazi

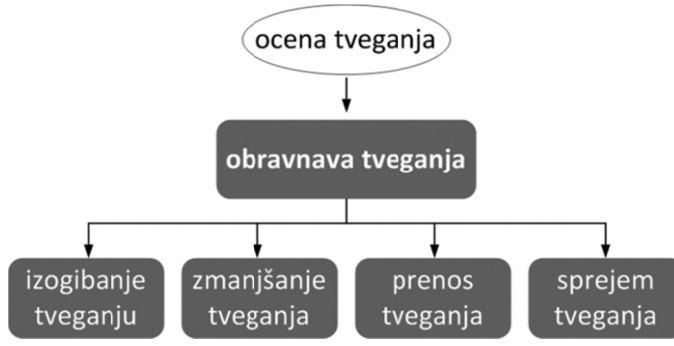
obravnave tveganja se torej določi, kako se bo posamezno tveganje reševalo in uvedene rešitve kasneje tudi validirale.

2.4.2 Možne obravnave tveganja

Za vsako zaznano in ovrednoteno varnostno tveganje je na voljo več možnosti, kako podjetje to tveganje obravnava. Glede na opravljeno oceno tveganja ima podjetje na izbiro obravnave, ki so shematično prikazane na Sliki 16 (Mehr & Hedges, 1974; Pritchard 1978; NIST 800-30, 2002):

- **Zmanjšanje** (angl. *risk mitigation* ali *risk reduction*) izpostavljenosti sredstva tveganju z uvedbo ustreznih tehnologij in orodij (na primer požarnega zidu, protivirusne zaščite) ali z uvedbo ustreznih postopkov (na primer varnostne politike, politike gesel, nadzora dostopa itd.). S tem se zmanjša verjetnost za škodljive dogodke ali omeji škoda, ki jo povzroči dogodek. Zmanjšanje tveganja je osnovna strategija obvladovanja tveganja.
- **Prenos** tveganja (angl. *risk transfer*) na drugo stranko, lahko prek zunanjega izvajanja storitev (na primer storitve v oblaku) ali z zavarovanjem (Böhme & Kataria, 2006). Primer je prenos tveganja na zavarovalnico, ki smo ga opisali v poglavju 2.3.3. Strategija prenosa postaja v zadnjem času čedalje pomembnejša.
- **Izogibanje** grožnjam in napadom (angl. *risk avoidance*) z omejevanjem izvorov tveganja oziroma izpostavljenostjo sredstev tveganju. To se večinoma uporablja v primerih, ko resnost učinka tveganja pretehta koristi, ki jih prinaša posamezno sredstvo (na primer odprt dostop do interneta). Podjetje se z izogibanjem tveganim aktivnostim odpove aktivnosti, vendar pa se zaščiti pred tveganjem, ki bi imelo prevelike posledice.
- **Sprejem** tveganja (angl. *risk acceptance*) kot posledice poslovanja. To je smiselna strategija, če se tveganju ni mogoče izogniti ali če so stroški uvedbe zaščitnih ukrepov znatno večji kot skupne izgube zaradi tveganja.

Slika 16: *Različne možnosti obravnave tveganja*

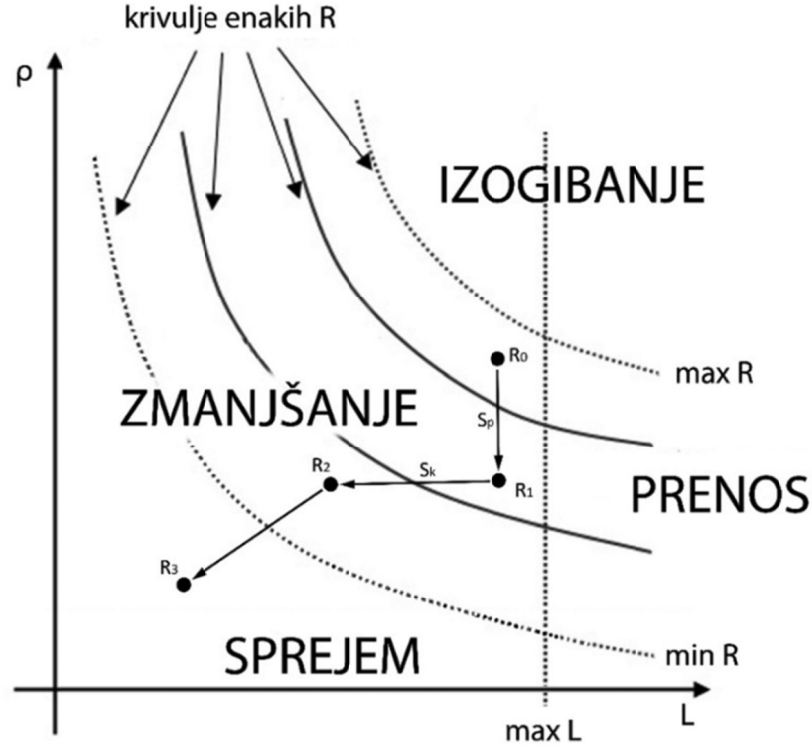


Cilji obravnave tveganja so stroškovno učinkovite zaščite, ki ne stanejo več, kot je pričakovana izguba zaradi napada. Zavedati se moramo, da izbrana obravnava tveganja lahko privede do novih tveganj, ki jih je treba prav tako oceniti in obravnavati (Schneier, 2003). V nekaterih primerih je težko določiti mejo med posameznimi obravnavami. Na primer požarni zid lahko razumemo kot zmanjšanje tveganja ali pa tudi kot izogibanje tveganju, ker se s tem podjetje odreče prednosti odprtih omrežij, da bi se izognilo tveganju. Zato je izbira ustrezne obravnave tveganja lahko precej težavna in pri odločanju večkrat zahteva sklepanje kompromisov ali uporabo in kombiniranje dveh strategij (Bosworth & Kabay, 2002).

Izbiro ustrezne obravnave tveganja lahko prikažemo grafično, kot je prikazano na Sliki 17 (Bojanc & Jerman-Blažič, 2012). Na vertikalni osi je verjetnost za incident, na horizontalni osi pa izguba zaradi incidenta. Ker je vrednost tveganja (R) opredeljena kot produkt verjetnosti (ρ) in izgube (L), krivulje na grafu predstavljajo točke z enako vrednostjo tveganja, ki pa se med seboj razlikujejo v vrednosti verjetnosti in izgube. Notranje krivulje predstavljajo nižje vrednosti tveganja, zunanje krivulje pa višje. Izbrana obravnava tveganja, ki zmanjšuje vrednost tveganja, prestavi točko tveganja z višje krivulje tveganja na nižjo krivuljo tveganja. Uvedba preventivnega ukrepa, ki zmanjšuje verjetnost za incident, je na grafu prikazana kot vertikalen premik vrednosti tveganja navzdol iz točke R_0 v točko R_1, ki leži na nižji krivulji tveganja. Uvedba korektivnega ali detekcijskega ukrepa, ki zmanjšuje izgubo zaradi incidenta, je na grafu

prikazana kot horizontalen premik vrednosti tveganja proti levi iz točke R_1 v točko R_2, ki leži na nižji krivulji tveganja.

Slika 17: *Grafični prikaz porazdelitve posamezne obravnave tveganja glede na vrednosti L, ρ in R*



Vir: R. Bojanc in B. Jerman-Blažič, Quantitative model for economic analyses of information security investment in an enterprise information system, 2012.

Vsaka izmed štirih možnih obravnav tveganja predstavlja določeno področje na grafu. Razdelitev posameznih področij predstavljajo mejne vrednosti parametrov tveganja, ki področje grafa razdelijo na štiri enote, ki ustrezajo posameznim obravnavam tveganja. Te vrednosti so:

- največja vrednost tveganja (R_{max}), ki je za podjetje še sprejemljiva;
- največja enkratna izguba (L_{max}), ki je za podjetje še sprejemljiva;
- najmanjša vrednost tveganja (R_{min}), ki je za podjetje že zanimiva.

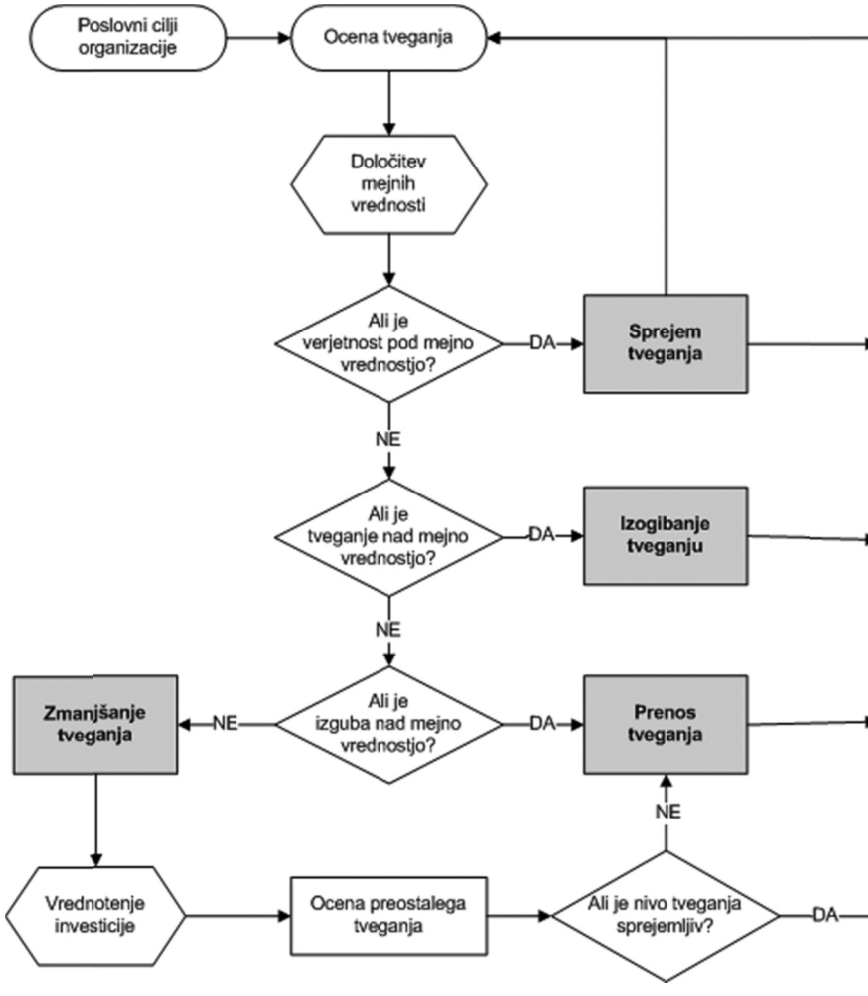
Ustrezna obravnava tveganja se določi tako, da se za posamezno tveganje vrednosti R in L primerjata z mejnimi vrednostmi R_{max}, L_{max} in R_{min}. Prva mejna črta določa najmanjšo smiselno verjetnost za incident ($R < R_{min}$). Pod to vrednostjo je tveganje zanemarljivo nizko, zato uvajanje varnostnega ukrepa finančno ni upravičeno in tveganja se sprejmejo. Druga mejna črta je največja možna vrednost tveganja ($R > R_{max}$), nad katero se podjetje tveganju izogne. Tretja mejna črta je največja možna izguba zaradi incidenta ($L > L_{max}$). Nad to vrednostjo ima zaradi visoke izgube učinek lahko katastrofalne posledice in je priporočljivo oblikovati prenos tveganja. Schneier (2003) pravi, da res velike posledice niso sprejemljive ne glede na pogostost. Tveganja v preostalem območju ($L < L_{max}$) odpravimo z zmanjševanjem prek investicij v varnostne ukrepe.

2.4.3 Proces obvladovanja tveganja

Fazi ocena in obravnava tveganja z različnimi možnimi obravnavami tveganja sta prikazani na primeru procesa izbire ustrezne obravnave tveganja na Sliki 18. Na podlagi poslovnih ciljev podjetja se izvede ocena tveganja, ki kvantitativno ali kvalitativno ovrednoti posamezna tveganja. Ustrezna obravnava se določi glede na vrednosti verjetnosti za incident in velikost potencialne izgube v odvisnosti od mejnih vrednosti parametrov tveganja (največja vrednost tveganja, največja enkratna izguba in najmanjša vrednost tveganja).

Včasih je potrebnih več zaščitnih ukrepov za zmanjšanje preostalega tveganja na sprejemljivo raven. Možne so tudi kombinacije teh obravnav. Na primer podjetje najprej izvede varnostne ukrepe, ki zmanjšajo izgubo, preostanek tveganja pa prenese na zavarovalnico. V nekaterih primerih, ko je tveganje sprejemljivo, se ne uvede noben zaščitni ukrep, četudi grožnje obstajajo. V drugih primerih lahko ranljivosti obstajajo, vendar ni znanih groženj, ki bi jih izkoriščale.

Slika 18: *Postopek izbire ustrezne obravnave tveganja*



Vir: R. Bojanc in B. Jerman-Blažič, An economic modelling approach to information security risk management, 2008.

3 ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI V POSLOVNIH SISTEMIH IN EKONOMIKA VLAGANJ

3.1 Vloga ekonomske vede pri zagotavljanju informacijske varnosti

Do konca 90. let prejšnjega stoletja je strokovna javnost obravnavala informacijsko varnost zgolj s tehničnega vidika v iskanju tehnoloških rešitev zaščite informacijskih sistemov. Razširjeno je bilo splošno prepričanje, da internetno okolje ni varno zaradi tehnoloških pomanjkljivosti, pomanjkanja kriptografskih tehnik, šibkega overjanja uporabnikov, nadzorovanja in filtriranja omrežnih podatkovnih paketov itd. Zato so varnostni inženirji pospešeno delali na tehnoloških rešitvah in izboljševali kriptografske algoritme, izboljševali požarne pregrade, uvajali sisteme za uporabo infrastrukture javnih ključev in druge tehnične rešitve, s katerimi so zmanjševali varnostna tveganja.

Od leta 2000 dalje pa je čedalje več raziskovalcev s področja informacijske varnosti začelo opozarjati, da se informacijske varnosti ne da uspešno obvladovati zgolj s tehnologijo. Ross Anderson (2001) trdi, da so neprimerne spodbude za ustvarjanje varnega sistema povzročile toliko škode kot tehnološke pomanjkljivosti. Pogosto se je izkazalo, da izbrane tehnične rešitve niso ustrezen odgovor na varnostna tveganja. Gordon in Loeb (2005) to razlagata s tem, da odločitve o rešitvah v informacijski varnosti pogosto temeljijo na instinktu v trebuhu tehnikov, namesto na ekonomski analizi. Varnost pogosto spodleti tudi v primeru, ko posamezniki, ki varujejo sistem, ne nosijo tudi finančnih posledic zaradi neustrezne varnosti (Anderson, 1993; Varian, 2000).

V zadnjem času se tudi podjetja sama čedalje bolj zavedajo, da zgolj tehnični vidik ne zadostuje za uspešno reševanje problema informacijske varnosti, zato pri obravnavi informacijske varnosti upoštevajo tudi ekonomski pogled (Anderson & Schneier, 2005; Anderson & Moore, 2006; Frei et al., 2009). Če na informacijsko varnost gledamo tudi z vidika ekonomije, lahko dobimo odgovore na mnoga vprašanja, na katera zgolj tehnologija ne more zadovoljivo odgovoriti (Bojanc & Jerman-Blažič, 2008). Večina osnovnih varnostnih vprašanj je vsaj

toliko ekonomskih kot tehničnih, za primer si oglejmo naslednja varnostna vprašanja:

- Kako si lahko podjetje zagotovi varnost na področju IT?
- Katera stopnja varnosti IT je najprimernejša?
- Koliko finančnih sredstev naj podjetje investira v varnost?
- Ali podjetje porabi dovolj finančnih sredstev, da bi zlonamernežem preprečilo vdor v računalniški sistem?
- Ali podjetje porabi preveč za informacijsko varnost?
- Ali podjetje porabi varnostni proračun za primerno ukrepanje?

Zaradi povečanja obsega elektronskega poslovanja si odgovorni za informacijsko varnost prizadevajo za čedalje večji proračun, namenjen varnostnim rešitvam (Su, 2006). Sredstva, ki so podjetju na voljo za varnostne ukrepe, so omejena in jih podjetja lahko porabijo tudi za druge naložbe, zato postaja ekonomija vlaganja v varnostne rešitve tako pomembna. Naraščanje izdatkov za varnostne rešitve je danes pod čedalje večjim nadzorom. Vodstva podjetij čedalje pogosteje zahtevajo ekonomsko utemeljitev pri sprejemanju odločitev za naložbo v informacijsko varnost (Bojanc et al., 2012a). Swire (2001) tudi sicer ugotavlja, da vodstvo podjetja bolje razume predlog, ki je predstavljen tudi s pomočjo ekonomske in ne zgolj tehnične analize, saj si laže predstavlja (ne)pomembnost škode ob varnostnih dogodkih, če je ta izražena kot višina finančne izgube (Bojanc & Jerman-Blažič, 2008).

Z ekonomskim pristopom lahko podjetja uvedejo optimalne varnostne rešitve (Gordon & Loeb, 2005). Lahko ocenijo, katera izmed rešitev, ki jih imajo na voljo, ima najboljše razmerje med ceno in kakovostjo glede rešitve varnostnega problema (Locher, 2005). Uporaba ekonomskega pristopa k obvladovanju varnostnih tveganj omogoča podjetjem tudi oceno optimalne stopnje informacijske varnosti. Ker ekonomski pristop bolje razloži varnostne težave, postajata danes teorija iger in mikroekonomska teorija kot orodji za reševanje teh problemov za varnostne inženirje tako pomembni, kot sta bili pred četrt stoletja matematika in kriptografija (Anderson & Moore, 2008).

Oglejmo si dva primera, ki ju s tehnično varnostjo ne moremo uspešno rešiti, saj večja varnost ni nujno vedno tudi najboljša za podjetje. Prvi primer je varnost v

banki, ki jo ogrožajo bančni roparji. Banke bi lahko izboljšale varnost tako, da bi na vhod postavile varnostnike, ki bi osebno preiskali vsakega, ki bi vstopil, vendar bi ob taki uvedbi najbrž ostale brez velikega števila svojih strank. Drugi primer je nevarnost kraje v trgovini z oblačili, kjer se po raziskavah največ kraj zgodi v garderobah. Tveganje za krajo bi sicer lahko zmanjšali tako, da bi odstranili garderobe ali v garderobe namestili videonadzor, vendar bi to lahko pomenilo precej manjšo prodajo, saj bi se stranke taki trgovini izogibale zaradi ogrožanja zasebnosti. Zato veliko trgovin sprejme določeno raven tveganja kraje kot sprejemljivo ali pa to preprečujejo z označbami blaga, ki pri blagajni na izhodu iz trgovine oddajo signal in opozorijo osebje, če označba ob nakupu seveda ni bila odstranjena.

Kot smo že omenili, se je ekonomski pogled na informacijsko varnost (in s tem novi pristopi za reševanje problema) začel razvijati po letu 2000. Na več različnih univerzah in organizacijah v ZDA so raziskovalci skoraj sočasno začeli delovati na novem raziskovalnem področju ekonomika informacijske varnosti (Camp, 2006). Leta 2000 so raziskovalci iz CERT-a predstavili osnutek mehanizma za oceno tveganja. Ta mehanizem, znan kot hierarhični holografski model, je bil prvo večplastno ocenjevalno orodje za pomoč pri oceni vlaganj v varnost z upoštevanjem tveganja (Longstaff et al., 2000). CERT je v nadaljevanju razvil metodo, znano pod imenom OCTAVE, ki velikim in manj velikim podjetjem pomaga pri oceni tveganja. Le malo pred tem sta Campova in Wolframova (2000) na harvardski univerzi objavili ekonomske definicije za opredelitev specifične »dobrine«, ki je danes splošno veljaven element v različnih teoretičnih varnostnih modelih za ocene primernih vlaganj v varnost. Definirali sta trg ranljivosti, ki je bil s strani podjetij 3Com in Microsoft v naslednjih letih potrjen kot veljaven model trga (Espiner, 2005; Wang, Beck, Jiang & Roussev, 2006). Leta 2001 je Ross Anderson (2001) z univerze Cambridge objavil pomembno razpravo na to temo z naslovom »Why Information Security is Hard: An Economic Perspective«, v kateri je pojasnil težave pri razvoju varnostnih rešitev, ki ne upoštevajo ekonomskih elementov problema. Ravno tako sta v letu 2001 Larry Gordon in Marty Loeb (2001) z univerze v Marylandu objavila študijo strateške uporabe informacijske varnosti s klasičnega vidika poslovanja. Dan Geer (2002) je v svojem delu zagovarjal, da se vlaganje v

varnost ne sme meriti s tehničnimi ukrepi ali zgolj s štetjem denarja za investicije, temveč s sistematično analizo donosnosti investicije.

K uveljavitvi ekonomskega pogleda na informacijsko varnost je pomembno prispevalo zavedanje, da je treba na informacijsko varnost gledati kot na investicijo in ne zgolj kot na strošek. Varno informacijsko okolje ustvarja dodano vrednost za podjetje in njegove partnerje, zato so za ustvarjanje tega okolja potrebna vlaganja. Enega izmed prvih okvirjev analitičnega odločanja za ocenjevanje različnih politik IT-varnosti z vidika ekonomije je predstavil tudi Soo Hoo (2000). Gordon in Loeb (2002a) sta izdelala ekonomski model za oceno optimalne investicije v informacijsko varnost, ki temelji na izenačevanju mejnih finančnih koristi informacijske varnosti in mejnih finančnih stroškov zaščite. Njun model je v nadaljevanju postal osnova za veliko drugih modelov, ki informacijsko varnost obravnavajo s kvantitativnega vidika potrebnih investicij.

3.1.1 Značilnosti trga IT-izdelkov in storitev

Za razumevanje ekonomskega pogleda na informacijsko varnost si oglejmo analizo trga IT-izdelkov in storitev, v kateri Anderson (2008) navaja nekaj pomembnih značilnosti.

Prva značilnost je učinek povezanosti v omrežju, kjer vrednost omrežja narašča veliko hitreje kot linearno s številom uporabnikov. Po Metcalfovem zakonu je na primer vrednost omrežja enaka kvadratu števila uporabnikov (Metcalfe's law, 2013). To lahko razložimo z eksternalijami omrežja. Eksternalija po definiciji pomeni strošek ali korist, ki ga ima neka tretja oseba, neudeležena v menjalnem odnosu. Kot primer lahko vzamemo naprave za pošiljanje faksiranih sporočil. Čedalje več uporabnikov je v 80. letih prejšnjega stoletja uporabljalo faksirne naprave, okoli leta 1985 so postale nujnost in jih je potrebovalo vsako podjetje (Anderson, 2008). Podobno se je zgodilo z e-pošto okoli leta 1995 in nekaj let pozneje z mobilnimi pametnimi telefoni. Učinek multiplikativnosti omrežja v primerjavi s številom uporabnikov ne velja samo za področje računalništva in informatike, temveč za storitve na splošno. Kdor želi prodati neki svoj predmet na dražbi, bo običajno šel k največji dražbeni hiši, ker bo ta privabila več ponudnikov. To se nanaša tudi na programsko opremo, kjer podjetja največ

razvijajo za najbolj razširjene in uporabljene operacijske sisteme, ker imajo tako dostop do več uporabnikov (primer Windows na osebnih računalnikih ter Android in iOS na mobilnih napravah). Če torej želijo biti uporabniki združljivi z drugimi uporabniki (ali proizvajalci programske opreme), se bodo logično odločili za proizvajalce, za katere predvidevajo, da imajo največji tržni delež.

Druga značilnost so visoki fiksni in majhni mejni stroški (angl. *marginal costs*), o čemer smo že govorili v prvem poglavju. V konkurenčnem okolju naj bi bila cena informacije enaka mejnim stroškom proizvodnje, kar je skoraj nič. Konkurenčna podjetja, ki ponujajo programsko opremo, jo lahko razmnožujejo praktično brez stroškov, zato lahko znižujejo ceno izdelka skoraj brez omejitve. To otežuje povrnitev kapitalskih investicij, razen v primeru, če se podjetje zaščiti s patenti, trgovsko znamko, nekompatibilnostjo izdelkov – tehničnim zaklepanjem itd. Podjetja so morala zato pogosto prilagoditi poslovni model, v katerem so dobrine na voljo za majhno vsoto denarja, denar pa so pridobili z oglaševanjem ali iz drugih virov. Veliko podjetij z visokimi fiksnimi in nizkimi mejnimi stroški se je premaknilo na oglaševalski ali storitveni model (Anderson, 2008).

Tretja značilnost je drag prehod med različnimi ponudniki. Ponudniki prehod še dodatno omejujejo s tehničnim zaklepanjem, ki izhaja iz interoperabilnosti. Na primer, če imamo predvajalnik iPod, ki je vreden 200 €, in smo prek Applove spletne trgovine kupili še za dodatnih 5.000 € glasbe, smo privezani ali »zaklenjeni« na proizvajalca Apple. Če želi podjetje na primer zamenjati operacijski sistem Okna na Linux, to zanj pomeni dodatno izobraževanje zaposlenih, reprogramiranje aplikacij itd., zato je sprememba za podjetje lahko precej draga. Shapiro in Varian (1998) navajata, da je neto sedanja vrednost podjetja, ki razvija programsko opremo, enaka skupnim stroškom zamenjave njihove programske opreme.

Vsaka od teh značilnosti sama zase vodi k trgu dominantnih podjetij, kjer imajo prvi na tržišču veliko prednost. Če upoštevamo vse karakteristike skupaj, pa je verjetnost, da zmagovalec pobere vse, še toliko večja (Anderson, 2008). Zato je pravočasen prihod na trg IT kritičen kljub ne dovolj zrelemu izdelku. Anderson (2001) je obrazložil, da je filozofija podjetij, ki razvijajo programsko opremo, da ponudijo izdelek čim prej ter ga nato z varnostnimi popravki dopolnjujejo in

popravljajo, s tega stališča popolnoma racionalna. Anderson v svoji razpravi sicer to pojasnjuje na primeru Microsofta, vendar dodaja, da bi enako ravnalo vsako podjetje, ki bi dobilo prevladujoč položaj na trgu operacijskih sistemov.

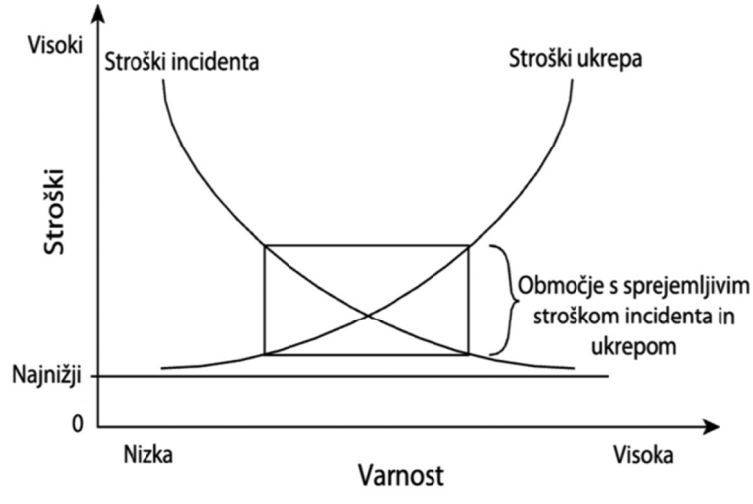
Ker v tej bitki, kdo bo prvi dobil prevlado na trgu, proizvajalci pogosto posvečajo varnosti premalo pozornosti, so raziskovalci trg varne programske opreme označili kot trg za limone (Anderson, 2001; Schechter, 2004; Anderson & Moore, 2006). Ta izraz je prvi uporabil Nobelov nagrajenec za ekonomijo George Akerlof (1970), ki je tako poimenoval metaforo prodaje rabljenih avtomobilov na trgu nesimetričnih informacij. Pri tem se izraz limona nanaša na slabe oziroma pomanjkljive izdelke. Podobna prispodoba po mnenju zgoraj navedenih raziskovalcev velja za varnostne rešitve v obliki programske opreme. Predpostavimo, da se prodaja 100 rabljenih avtomobilov, od tega jih je 50 dobrih (ti so vredni 3.000 €) in 50 slabih (z vrednostjo 1.000 €). Prodajalci vedo, kateri so dobri in kateri slabi, kupci pa ne (imamo informacijsko asimetrijo). Kakšna je v danem primeru mejna cena (angl. *market-clearing price*) za rabljene avtomobile? Na prvi pogled bi predpostavili, da je 2.000 €, vendar to ne drži. Za 2.000 € namreč noben prodajalec ne bo prodal dobrega avtomobila, ker bi bila zanj ta cena prenizka. Izkaže se, da bi bila mejna cena zato na koncu blizu 1.000 €. Trg za limone je torej tisti trg, v katerem potrošniki ne morejo ločiti kakovostnih proizvodov od pomanjkljivega blaga (t. i. limon), zato niso pripravljeni plačati dodatne cene za kakovost, ki je ne morejo izmeriti. Na takem trgu je za proizvajalca najboljša strategija prodajati limone, saj je zanj to ceneje. Po drugi strani pa zato potrošniki predvidevajo, da je vsak prodajan proizvod lahko limona. Cena za proizvod, ki so jo potrošniki pripravljeni plačati, je izračunana na podlagi predpostavke, da bo prejeti izdelek limona. Podjetja, ki proizvajajo visokokakovostne proizvode, bodo tako izrinjena s trga zaradi tistih, ki proizvajajo limone po nižji ceni.

3.2 Analiza stroškov in koristi pri vlaganju v informacijsko varnost

3.2.1 Opredelitev stroškov in koristi

Kot smo spoznali že v drugem poglavju, morajo podjetja določiti ustrezno stopnjo informacijske varnosti glede na njihove potrebe in varnostne zahteve. Ustrezna stopnja informacijske varnosti je določena z razmerjem med vrednostjo naložbe in koristmi varovanja (zmanjševanja stroškov dogodka), kar je prikazano na Sliki 19.

Slika 19: *Iskanje optimalne rešitve med višino stroškov varnostnega dogodka in stroški ukrepa (tj. obsega naložbe v informacijsko varnost)*



Vir: R. Kaplan, A Matter of Trust, v Tipton in Krause (ur.), Information Security Management Handbook, 6th edition, 2007.

Optimalna raven informacijske varnosti je torej odvisna od dveh elementov, in sicer od stroškov ukrepa in stroškov dogodka. Strošek ukrepa je vrednost naložbe v informacijsko varnost, s katero se podjetje želi izogniti posledicam varnostnega dogodka, strošek dogodka pa so sredstva, ki jih podjetje porabi, ko odpravlja posledice varnostnega dogodka. Podjetje, ki nameni zelo malo sredstev

za informacijsko varnost, bo praviloma porabilo več sredstev za odpravo posledic pogostih varnostnih dogodkov, zelo velika vlaganja v informacijsko varnost pa bodo praviloma močno zmanjšala stroške dogodka, saj se bodo ti pojavljali redko in z manjšimi posledicami.

Ker koristi večje informacijske varnosti pogosto niso omejene le na podjetje, ampak se pojavljajo tudi v širšem družbenem okolju, v katerem podjetje deluje, si pri ocenjevanju optimalne stopnje varnosti lahko pomagamo z analizo stroškov in koristi (Bojanc, Mörec, Tekavčič & Jerman-Blažič, 2012b). **Analiza stroškov in koristi** (angl. *cost benefit analysis*) je sistematičen pristop ocenjevanja primernosti sprejetja nekega ukrepa, ki primerja vse koristi (vrednostno izražene koristi ukrepa) in vse stroške, ki so povezani z uvedbo tega ukrepa (Gordon & Loeb, 2002b). Analiza izhaja iz osnovnega pogoja, ki mora biti izpolnjen za sprejetje katere koli odločitve (Brent, 2007):

$$B > C \tag{2}$$

pri čemer je B korist, C pa strošek. Navedeni pogoj zapišemo v obliki količnika razmerja med stroški in koristi (angl. *Cost-benefit ratio – CBR*):

$$\frac{B}{C} > 1 \tag{3}$$

Količnik mora biti večji od 1 – koristi sprejetja nekega ukrepa morajo presegati stroške, ki jih bomo imeli z njegovo uvedbo.

Dejanski strošek vlaganja v informacijsko varnost je mogoče dobiti dokaj preprosto. Upoštevajo se operativni stroški, ki vključujejo izdatke, od katerih se pričakuje korist v eni periodi izvajanja (pri tem je ena perioda običajno fiskalno leto). Operativni stroški predstavljajo letno vzdrževanje (posodobitve in varnostne popravke), izobraževanje uporabnikov in skrbnikov omrežja ter nadzor rešitve. Primer operativnih stroškov je nameščanje varnostnih popravkov (ki vključujejo stroške osebja) za odpravo varnostnih vdorov, ki so se zgodili med letom.

Pri oceni stroškov je treba upoštevati tudi kapitalske naložbe. Za razliko od operativnih stroškov, ki se računajo kot izdatek v enem obdobju, so kapitalske naložbe izdatki, ki prinesejo podjetju korist v več zaporednih obdobjih. Primer kapitalske naložbe je nabava novega sistema za zaznavanje vdorov v omrežje, ki pomaga podjetju zmanjševati verjetnost vdorov v določenem prihodnjem obdobju (na primer triletnem).

Gordon in Loeb (2002b) ocenjujeta, da naj bi optimalni strošek za varnostni ukrep znašal od 0 % do 37 % možne izgube zaradi varnostnega incidenta. Drugi raziskovalci so to ugotovitev razširili in našli situacije, v katerih je upravičeno pričakovati, da bo strošek ukrepa znašal celo do 100 % možne izgube (Willemson, 2006). Te ugotovitve so tudi uspešno preverili na empiričnih primerih (Tanaka et al., 2005; Tanaka et al., 2006).

Za razliko od stroškov, ki se določijo sorazmerno preprosto, pa je precej težje opredeliti, oceniti ali meriti koristi (Soo Hoo, 2000). Varnostne rešitve (na primer požarni zid, protivirusni program in IDS-sistemi za zaznavo vdorov) same po sebi namreč ne prinašajo finančnih koristi, ki jih je mogoče izmeriti, lahko pa so koristi investicije v informacijsko varnost izražene drugače (Gordon & Loeb, 2005), na primer zmanjšanje verjetnosti za ponovitev incidenta, povečanje produktivnosti ostalih investicij v informacijsko varnost ali zmanjševanje izgub v primeru incidenta. Koristi in stroški pogosto nimajo fizične oblike. Na primer občutek varnosti sam po sebi nima fizične oblike, lahko pa merimo njegove posledice (opazimo na primer več transakcij prek varnega kanala kot pa prek tistega, ki ni zaščiten) (Bojanc et al., 2012a).

Na splošno se na koristi zaradi vlaganja v informacijsko varnost gleda kot na prihranek stroškov incidenta zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta (Gordon & Loeb, 2006). Te koristi je običajno zelo težko točno napovedati. Največja težava je, ker gre za ocenjevanje prihrankov stroškov, vezanih na potencialne varnostne incidente, ki se še niso zgodili. Uspešnejša kot je informacijska varnost, težje je opaziti dejanske koristi.

V poglavju 2.1.4 smo obravnavali pričakovane letne izgube zaradi varnostnih incidentov z oceno ALE. Analitično lahko koristi *B* zaradi investicije v varnostni

ukrep dobimo kot razliko vrednosti ALE pred uvedbo varnostnega ukrepa in vrednosti ALE po njegovi uvedbi.

$$B = ALE_{brez\ investicije} - ALE_{z\ investicijo} \quad (4)$$

3.2.2 Alternativni pristopi

Analiza stroškov in koristi omogoča racionalen pristop k obravnavi varnostnih tveganj, vendar pa veliko raziskovalcev opozarja, da je težavna za uporabo (Geer, 2002), ker je treba stroške in koristi umeriti v skupno denarno valuto. Geer to težavo pri izračunu stroškov in koristi ponazarja s primerom zdravstvenega varstva. Koliko evrov je vredno človeško življenje? Koliko evrov je vredno porabiti, da bi rešili človeško življenje? Geer predlaga, da v primerih, ko stroškov in koristi ne moremo preprosto primerjati, raje primerjajmo stroške in učinkovitost rešitve (analiza stroškovne učinkovitosti). Merjenje stroškov in koristi zahteva, da se vsi vpleteni strinjajo glede tega, koliko je korist vredna, kar je običajno težko. Merjenje stroškov in učinkovitosti pa nasprotno zahteva, da vpleteni soglašajo, da bodo porabili X €, poleg tega pa še ocenijo, koliko vrednosti lahko dobijo za teh X €. Stroškovna učinkovitost se ogne problemu vrednotenja ob predpostavki, da bo podjetje v vsakem primeru imelo stroške, vprašanje je le, kaj je najboljše, kar lahko dobi za to ceno. Učinkovitost je bolj prilagodljiv parameter, ker ne zahteva cene dogodkov. Tak pristop odgovori na vprašanje, kaj je največ, kar lahko dobim za X €, če sem odločen porabiti teh X €. Pristop z analizo stroškov in koristi pa namesto tega odgovori na vprašanje, ali bi raje imel korist X ali pa Y € (Geer, 2004). Povzamemo lahko, da gre pri stroškovni učinkovitosti za maksimiranje učinkovitosti odhodka, kadar je koristi težko ovrednotiti.

Druga alternativna metoda, ki poskuša analizirati vlaganja v informacijsko varnost, je tako imenovana teorija iger. Cavusoglu in soavtorja (2004b) trdijo, da tradicionalni odločitveno-analitični pristopi za vrednotenje IT-investicij v varnost obravnavajo varnostne tehnologije kot črno škatlo in ne upoštevajo, da se investicija v informacijsko varnost razlikuje od drugih splošnih IT-investicij. Avtorji zagovarjajo trditev, da se pri varnosti podjetja srečujejo s strateškimi

nasprotniki, ki iščejo priložnosti, da bi izkoristili ranljivosti v sistemih, zato lahko na informacijsko varnost gledamo kot na neke vrste igro med napadalci in podjetji. Teorija iger gleda interakcijo med potencialnim napadalcem in podjetjem ter skuša pojasniti primere vdorov v podjetje, kjer ima napadalec motiv za napad in povzroči podjetju določeno škodo. Gal-Or in Ghose (2005) sta z uporabo teorije iger raziskala, kolikšni so stroški in kolikšne koristi izmenjave informacij o varnostnih incidentih.

Nekatera podjetja, ki se izogibajo pristopu stroškov in koristi za razporeditev sredstev, namenjenih informacijski varnosti, uporabljajo za obvladovanje tveganja najboljše prakse in industrijske standarde. Zagovorniki takega pristopa to izbiro argumentirajo s tem, da je merjenje stroškov in koristi skoraj nemogoče, zato je po njihovem mnenju najpreprosteje sprejeti in uporabiti rešitve informacijske varnosti, ki jih je uvedlo že veliko drugih podjetij. Tak pristop daje managerjem občutek varnosti skozi številke o podjetjih, ki so te rešitve uvedla v svoje poslovanje. Običajno je sicer res preprost in ga lahko hitro uvedemo, vendar pa lahko podjetje za informacijsko varnost hitro porabi preveč ali ostane ranljivo za določena nepotrebna tveganja.

Gordon in Loeb (2005) kljub vsem tem pomislekom zagovarjata analizo stroškov in koristi. Po njunem mnenju mora razdelitev sredstev za informacijsko varnost temeljiti na ekonomskem principu analize stroškov in koristi, tako kot se obvladujejo sredstva za druge aktivnosti v podjetju.

3.3 Ocene o donosnosti vlaganj

Pri analizi stroškov in koristi je treba ugotoviti tudi količinske (fizične) tokove gibanja koristi in stroškov ter njihov časovni razpored. Sestavni del tega koraka je ocena verjetnosti, da se bodo ti tokovi tudi dejansko pojavili in v kolikšnem obsegu. Običajno večina stroškov nastane na začetku življenjskega cikla projekta, koristi pa lahko nastajajo v celotnem življenjskem ciklu naložbe, lahko celo z velikim časovnim zamikom, zato jih je pogosto težko točno napovedati (Gordon & Loeb, 2005).

Ker koristi in stroški nastajajo v različnih časovnih trenutkih, moramo v enačbi 2 primerjati njihove sedanje vrednosti. Kaldor-Hicksovo načelo tako pravi, da projekt sprejmemo, če je sedanja vrednost koristi večja od sedanje vrednosti stroškov (Munger, 2000). Tu pa se pojavi vprašanje, kako določiti primerno diskontno stopnjo, ki jo v ta namen uporabimo, saj z njo lahko vplivamo na izid enačbe. Neto sedanja vrednost projektov, kjer tokovi koristi in stroškov časovno med seboj niso usklajeni, je namreč odvisna od višine diskontne stopnje. Tudi zato je analiza občutljivosti kazalnikov, ki se najpogosteje uporabljajo za oceno primernosti vlaganj v informacijsko varnost, tj. donosnosti investicije (ROI), neto sedanje vrednosti (NPV) in notranje stopnje donosnosti (IRR), za spremembe posameznih ocen in predpostavk nujni sklepni del vsake analize stroškov in koristi vlaganj v informacijsko varnost (Bojanc et al., 2012b).

3.3.1 Donosnost investicije

Donosnost investicije (angl. *Return on Investment – ROI*) je priljubljen finančni kazalec za primerjavo poslovnih investicij (Blakley, 2001; Butler, Chalasani, Jha, Raz & Shaw, 1999; Jacobson, 2000; Geer, 2001; Soo Hoo, 2000). V literaturi o informacijski varnosti nekateri avtorji za kazalec ROI uporabljajo tudi izraz donosnost varnostne investicije (angl. *Return on Security Investment, ROSI*) (Sonnenreich et al., 2006) ali donosnost informacijske varnostne investicije (angl. *Return on Information Security Investment – ROISI*) (Mizzi, 2005). Ti različni izrazi zgolj poudarijo, da gre za merjenje donosnosti ukrepov informacijske varnosti, medtem ko sta postopek izračuna in rezultat enaka za vse.

ROI preprosto določa, koliko podjetje dobi glede na porabljen znesek denarja, in tako pomaga pri odločitvah, ali je vložek v varnost upravičen. S pomočjo ROI se lahko podjetje odloči, katera od možnih rešitev daje največjo dodano vrednost za vložen denar. Podjetje lahko na primer uporabi ROI pri odločitvi, ali vlagati v notranji razvoj novih tehnologij oziroma rešitev ali kupiti komercialni izdelek. Donosnost investicije je priljubljen kazalec tudi zato, ker ga poznajo finančni direktorji in drugi, ki v podjetjih skrbijo za proračun in so odgovorni za odobritev izdatkov (Schechter, 2004). ROI je izražen kot neto dobiček, deljen z investicijo:

$$ROI = \frac{B - C}{C} \tag{5}$$

Kazalec ROI je izražen kot odstotek vrnjene investicije v določenem času. ROI je enak sedanji vrednosti neto koristi v določenem časovnem obdobju, deljen z začetnim stroškom investicije *C*. Pozitivna vrednost ROI pomeni, da je vlaganje v izbrano varnostno rešitev ekonomsko upravičeno. Če se letna korist varnostne investicije ne bo prejemala samo v prvem letu, temveč tudi v kasnejših letih, je ROI določen kot znesek vseh letnih koristi glede na stroške (Blakley, 2001). Pri tem se za vse stroške predpostavlja, da bodo nastali takoj.

Če za izračun koristi uporabimo razliko v vrednosti ALE pred investicijo in po njej, kot je prikazano v enačbi 4, lahko enačbo 5 za ROI zapišemo:

$$ROI = \frac{ALE_{brez\,investicije} - ALE_{z\,investicijo} - C}{C} \tag{6}$$

Managerjem, ki jih za sprejem odločitve o določeni investiciji zanima zgolj pričakovana donosnost investicije, podatek o izračunu pričakovane letne izgube (ALE) popolnoma zadostuje. Gordon in Loeb (2005) take managerje imenujeta nevtralne za tveganje (angl. *risk-neutral manager*). Njihovo nasprotje so tveganju nenaklonjeni managerji (angl. *risk-averse manager*), ki bolj favorizirajo investicijo z zanesljivo donosnostjo kot investicijo z negotovo donosnostjo, pri čemer imata investiciji enako pričakovano vrednost ALE. Tak manager bo vedno pripravljen žrtvovati nekaj pričakovane donosnosti za zmanjšanje tveganja, povezanega z donosnostjo. Z drugimi besedami, tak manager je pripravljen plačati 13.000 € za ukrep, ki preprečuje tveganje s pričakovano izgubo 12.000 €, če ukrep zagotavlja, da do dogodka ne bo prišlo.

Izračun ponazorimo s preprostim primerom. Recimo, da je tveganje okužbe z virusom v organizaciji ocenjeno na 8.750 €, z uvedbo varnostnega ukrepa v vrednosti 1.600 € pa se tveganje zmanjša na 3.400 €. K stroškom nakupa ukrepa moramo prišteti še 450 € letnih stroškov za vzdrževanje zaščite. Za prvo leto uporabe znaša tako ROI:

$$ROI = \frac{8.750\ € - 3.400\ € - 1.600\ € - 450\ €}{1.600\ € + 450\ €} = 160\ \% \qquad (7)$$

Medtem ko ROI pove odstotek donosa zaradi investicije v določenem časovnem obdobju, ne pove ničesar o velikosti investicije. Na primer, 124-odstotna donosnost je lahko na začetku zelo privlačna, vendar s pojavi vprašanje, ali bi bilo bolje imeti 124 % donosa na investicijo 10.000 € ali 60 % donosa na investicijo 300.000 € (Bojanc & Jerman-Blažič, 2008).

3.3.2 Neto sedanja vrednost

V primeru dolgoročnih finančnih investicij je časovna komponenta problem pri izračunu ROI, zato se v takih primerih namesto ROI raje uporablja kazalec neto sedanja vrednost (angl. *Net Present Value – NPV*). NPV je finančni kazalec za primerjavo koristi in stroškov v različnih časovnih obdobjih, lahko primerja pričakovane koristi in stroške glede na današnjo vrednost (angl. *present value*). NPV je razlika med sedanjo vrednostjo in začetnimi stroški projekta. Bistvo pristopa NPV je primerjava diskontiranih denarnih tokov, vezanih na prihodnje koristi in stroške, z začetnimi stroški investicije, pri čemer so celotne koristi in stroški izraženi v denarni enoti. Zaradi lažjega izračuna se pogosto privzame, da so prihodnje koristi in stroški (z izjemo stroškov začetne investicije) realizirani na koncu posameznega obdobja. S tem ko se denarni tokovi diskontirajo, se ustrezno vključi časovna komponenta, tako da so zneski koristi in stroškov v različnih časovnih obdobjih primerljivi.

Pri izračunu kazalca NVP se izračuna vsota sedanjih vrednosti neto koristi in od nje odštejejo začetni stroški investicije. Naj bo n število obdobij, B_t sedanja vrednost neto koristi v časovnem obdobju t, C_t vsi stroški v časovnem obdobju t in k diskontna stopnja. Izračun kazalca NPV je:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+k)^t} \qquad (8)$$

Diskontna stopnja k se običajno razume kot povprečni strošek kapitala. Izbor ustrezne diskontne stopnje je za izračun kazalca NPV zelo pomemben. Model

NPV prek diskontne stopnje uravnava tveganje, pri tem večja diskontna stopnja pomeni manjšo vrednost kazalca NPV (Gordon & Loeb, 2005).

NPV je merjen v denarnih enotah. Pozitivna vrednost NPV pomeni, da sedanja vrednost pričakovanih koristi presega sedanjo vrednost pričakovanih stroškov in da projekt ustvarja dobiček, medtem ko negativna vrednost NPV pomeni, da je sedanja vrednost pričakovanih koristi manjša od sedanje vrednosti pričakovanih stroškov ter da projekt ustvarja izgubo. Če je NPV enak nič, pomeni, da sta sedanja vrednost pričakovanih koristi in sedanja vrednost pričakovanih stroškov enaki. Projekt je torej donosen, če je vrednost NPV večja od nič. Višja vrednost NPV je vedno boljša, medtem ko nizka vrednost NPV (še zlasti negativna vrednost NPV) kaže na nesprejemljive investicije (Su, 2006).

NPV je zelo uporaben pri vrednotenju različnih alternativ. Podjetje na primer izbira med dvema varnostnima rešitvama, pri katerih so stroški prve 15.000 € kot enkratni strošek na samem začetku investicije, druge pa 5.000 € letnih stroškov za obdobje treh let. Pri obeh rešitvah so stroški 15.000 €, vendar je druga rešitev boljša, saj lahko podjetje za določen čas vlaga denar na drugih področjih, zato so dejanski stroški pri drugi rešitvi manjši od 15.000 €.

Pomembna značilnost NPV je, da podaja informacije o denarni vrednosti pričakovanega donosa in s tem kaže obseg projekta, slabost pa je, da ne podaja informacij, kdaj naj bi prišlo do pričakovanega donosa (Bojanc & Jerman-Blažič, 2007).

3.3.3 Notranja stopnja donosa

Kazalec notranja stopnja donosa (angl. *internal rate of return – IRR*) se (tako kot NPV) pogosto uporablja za analiziranje dolgoročnih investicij. Vrednost IRR je enaka diskontni stopnji, pri kateri je NPV investicije enak nič. Drugače povedano, kazalec IRR določi diskontno stopnjo, pri kateri so stroški začetne investicije C_0 enaki sedanji vrednosti pričakovanih prihodnjih neto koristi (tj. koristi minus stroški).

$$\sum_{t=0}^{n} \frac{B_t - C_t}{\left(1 + IRR\right)^t} = 0 \tag{9}$$

Kazalec IRR je še zlasti uporaben v primerih, če se stroški večletne investicije iz leta v leto precej spreminjajo. Za oceno donosnosti potrebujemo primerjalno vrednost *k*, ki je enaka diskontni stopnji, ki se običajno upošteva kot povprečni strošek kapitala podjetja (najmanjša stopnja, ki jo mora projekt vrniti, da se vrednost podjetja ne bo zmanjšala). Projekt je donosen, če je vrednost IRR večja od *k*.

3.3.4 Kateri kazalec je najprimernejši?

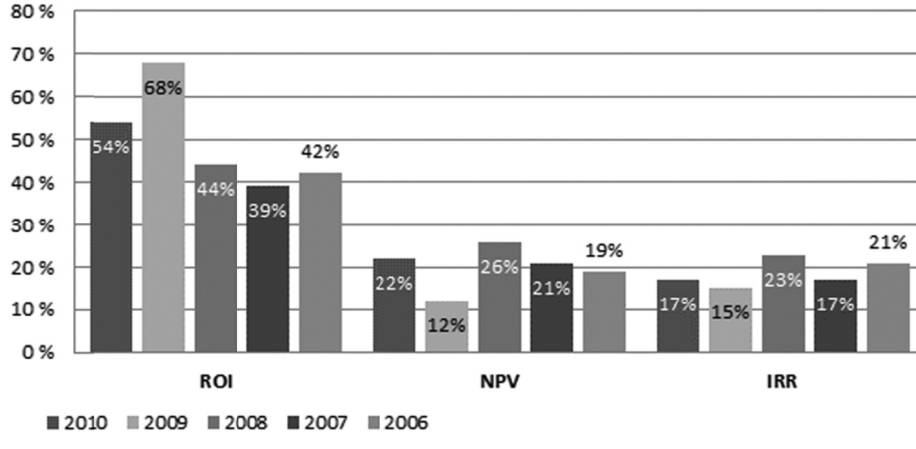
Odločitev glede uporabe kazalcev ROI, NPV ali IRR je prepuščena podjetjem in posameznikom, odgovornim za vrednotenje varnostnih investicij. Vsak od teh finančnih kazalcev ima svoje prednosti in slabosti. Pogosto se zgodi, da so rezultati enaki pri uporabi vseh treh kazalcev, včasih pa se pri odločanju pokažejo razlike. ROI se večinoma uporablja za vrednotenje preteklih investicij, medtem ko se NPV in IRR navadno uporabljata za sprejemanje odločitev glede novih investicij (Gordon & Loeb, 2006). Tako kot ROI tudi IRR ne daje nobenega podatka o obsegu investicije. V nasprotju z NPV in IRR ROI ne upošteva časovne vrednosti denarja, izračunavanje ALE pa je težje za NPV in IRR kot za ROI.

O primerjavi in izbiri med kazalci ROI, NPV in IRR je bilo opravljenih precej raziskav. Gordon in Richardson (2004) sta v svoji analizi primerjala ROI in NPV ter ugotovila, da je za vrednotenje informacijske varnosti bolje uporabiti NPV. Tudi sicer sta po njunem mnenju NPV in IRR boljša kazalca od preprostega izračuna ROI. V primeru različnih odločitev ima običajno rezultat NPV večjo težo kot rezultat IRR (Gordon, 2004; Brealey & Myers, 2000). Gordon in Loeb (2002a) ugotavljata, da bi morala podjetja namesto ROI uporabljati IRR, ker vključuje diskontirane denarne tokove za investicije, ki imajo različne stroške in koristi v različnih letih. Čeprav trdita, da je IRR boljši kazalec od ROI, Gordon in Loeb hkrati opozarjata, da se lahko stopnja donosa uporablja neustrezno. Opozarjata, da naj se stopnja donosa ne uporablja za primerjavo dveh investicij,

ker imajo investicije lahko večjo neto korist, vendar manjšo stopnjo donosnosti. Če je na voljo dovolj denarja za investicijo v različne možnosti, vendar pa podjetje lahko investira le v eno, je za podjetje lahko bolj donosno, da investira v rešitev, ki ima večjo neto korist, kot pa v rešitev z višjo stopnjo donosa (Schechter, 2004). Da bi dobili jasno in popolno sliko o prihodnjih investicijah, je dobro upoštevati vse tri kazalce in jih primerjati med seboj.

Čeprav ima ROI svoje pomanjkljivosti v primerjavi z NPV in IRR (Gordon & Loeb, 2002a), je po raziskavah CSI (2011, 2008) najpogosteje uporabljen kazalec v praksi (Slika 20).

Slika 20: *Delež uporabe ROI, NPV in IRR za varnostni kazalec*



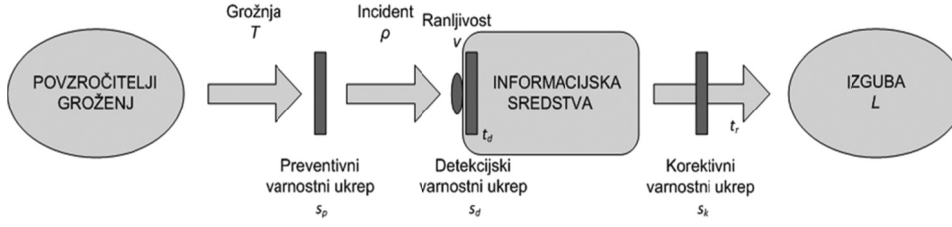
Vir: Prirejeno po CSI Computer Crime and Security Survey, 2011 in CSI Survey, 2008.

Veliko managerjev za vrednotenje prihodnjih investicij uporablja ROI, ker je za uporabo najpreprostejši. Čeprav se podatki skozi leta malo spreminjajo, uporablja ROI približno polovica podjetij, ki so sodelovala v raziskavi. Delež podjetij, ki uporabljajo NPV ali IRR, pa je približno enak.

3.4 Postopek izbire optimalne varnostne rešitve

V tem poglavju si bomo ogledali postopek izbire optimalne varnostne rešitev za določeno tveganje. Pri izbiri bomo predstavili postopek, ki temelji na kvantitativnem modelu, ki ga je razvil Bojanc (2010). V modelu se za vsako informacijsko sredstvo določijo ter kvantitativno ovrednotijo ranljivosti in grožnje, ki so povezane s tem sredstvom, ter ukrepi, ki ta tveganja zmanjšujejo. Model analize tveganja z varnostnimi ukrepi je prikazan na Sliki 21.

Slika 21: *Model analize tveganja*



Vir: R. Bojanc, Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih, 2010.

Povzročitelji groženj izvajajo **grožnje *T*** oziroma napade na sistem. Verjetnost grožnje ($0 \leq T \leq 1$) opredelimo kot verjetnost, da se zgodi dogodek, ki ima neželene učinke na informacijska sredstva. Verjetnost grožnje predstavlja število napadov na enoto časa. Informacijska sredstva imajo **ranljivosti *v***, prek katerih lahko grožnje zlorabijo sredstva. Ranljivost sredstva ($0 < v < 1$) zato opredelimo kot verjetnost, da bo grožnja, usmerjena na neko informacijsko sredstvo, uspešna. Mejna vrednost $v = 0$ bi pomenila, da so informacijska sredstva popolnoma varna, $v = 1$ pa, da so informacijska sredstva popolnoma ranljiva.

Podjetje tveganja informacijske varnosti zmanjšuje z vlaganjem v **varnostne ukrepe *s***. Lahko izbira med preventivni varnostni ukrepi s_p, ki zmanjšujejo verjetnost varnostnega dogodka, korektivnimi varnostnimi ukrepi s_k, ki zmanjšujejo izgubo ob varnostnem dogodku, in detekcijskimi varnostnimi ukrepi s_d, ki zmanjšujejo čas za odkritje dogodka ter omogočijo pridobitev informacije o grožnjah. Vlaganje v varnostni ukrep je na splošno opredeljeno s **ceno ukrepa *C*** in **učinkovitostjo ukrepa *α*** (Gordon & Loeb, 2002b). Cena ukrepa *C* je denarna

naložba v varnostni ukrep, ki vsebuje vse izdatke, povezane z uvedbo varnostnega ukrepa, učinkovitost varnostnega ukrepa α pa pomeni vpliv varnostnega ukrepa na zmanjšanje tveganja. Zbirka mogočih groženj se neprestano spreminja in je podjetjem le delno znana (ISO 13335-1, 2004), zato učinkovitost zaradi vedno novih groženj s časom konveksno pada, če ni dodatnih vlaganj v varnostne ukrepe. Zaradi razumljivosti označimo parametra C in α z istim indeksom kot varnostni ukrep. Preventivni varnostni ukrep s_p opredeljujeta cena C_p in učinkovitost α_p, korektivni varnostni ukrep s_k cena C_k in učinkovitost α_k ter detekcijski varnostni ukrep s_d cena C_d in učinkovitost α_d.

Nekateri dogodki, ki imajo neželene učinke na informacijska sredstva, so za povzročitelja grožnje uspešni in povzročijo, da se v podjetju zgodi varnostni incident. Verjetnost, da bo izvedena grožnja uspešna, oziroma verjetnost za **varnostni incident ρ** je odvisna od verjetnosti grožnje T, ranljivosti sredstva v in preventivnega varnostnega ukrepa s_p. V skrajnih primerih je verjetnost varnostnega dogodka $\rho = 0$, če ni nobenega napada (verjetnost grožnje $T = 0$). Enako je verjetnost varnostnega dogodka $\rho = 0$, če informacijski sistem ni ranljiv (ranljivost sredstva $v = 0$). Poenostavljeno povedano, verjetnost grožnje T in ranljivost sredstev v povečujeta verjetnost varnostnega dogodka ρ, preventivni varnostni ukrep s_p pa to verjetnost zmanjšuje. Predstavljenih je precej različnih funkcij verjetnosti za varnostni incident ρ, v predstavljenem modelu je uporabljena funkcija, ki je med raziskovalci precej priljubljena (Matsuura, 2008; Gordon & Loeb, 2002b; Bojanc, 2010):

$$\rho = T \cdot v^{\alpha_p C_p + 1} \tag{10}$$

Če se varnostni dogodek zgodi, podjetje utrpi finančno **izgubo L**. Za lažji izračun izgub razdelimo izgubo na posamezne faktorje:

$$L = L_s + L_r + L_i + L_p + L_{SLA} + L_{posredne} \tag{11}$$

Strošek zamenjave opreme L_s je strošek nakupa nove opreme. To vrsto izgub je najpreprosteje ovrednotiti, saj so podatki običajno že na voljo ali pa se lahko dokaj preprosto pridobijo. V primeru okvare opreme se lahko ta strošek občutno

zmanjša ob investiciji v garancijo, ki jo ponujajo proizvajalec in razni vzdrževalci opreme.

Strošek popravila L_r predstavljajo stroški dela zaposlenih ali zunanjih izvajalcev, da se posledice incidenta odpravijo in ponovno vzpostavi normalno delovanje sistema ali storitve.

Izguba prihodkov podjetja L_i je izguba, ki jo utrpi podjetje na prihodkovni strani zaradi nedelovanja sistema ali storitve kot posledice incidenta.

Izguba produktivnosti podjetja L_p je zmanjšanje produktivnosti v času nedelovanja sistema ali storitve

Izguba zaradi nespoštovanja zakonskih predpisov ali pogodbenih obveznosti L_{SLA} je odvisna od pogodbe oziroma zakonodaje. Za primer poglejmo podjetje, ki strankam ponuja določeno storitev in ima z njimi sklenjeno pogodbo SLA. Če je razpoložljivost storitve, ki jo ponuja podjetje, pod mejo, določeno v SLA, je to za podjetje strošek, saj mora strankam povrniti del plačila.

Posredne izgube $L_{posredne}$ so izgube, ki imajo lahko dolgoročne posledice.

Varnostni incidenti lahko povzročijo nedelovanje storitev ali informacijskega sistema. Trajanje nedelovanja je sestavljeno iz **časa detekcije t_d**, v katerem varnostni incident zaznamo, in **časa popravila t_r**, v katerem informacijski sistem ali storitve ponovno vzpostavimo za normalno delovanje. Čas t_d se šteje od trenutka, ko se incident zgodi, do trenutka, ko incident zaznamo. Kvantitativno lahko izgube L v enačbi 11 zapišemo v obliki treh členov, od katerih prvi člen vsebuje faktorje, odvisne od t_r, drugi člen vsebuje faktorje, odvisne od t_d, tretji člen pa faktorje brez časovne odvisnosti:

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 \tag{12}$$

Podrobna opredelitev in izračun posameznih faktorjev je v Bojanc et al. (2012a). Izgubo, ki nastane zaradi varnostnih dogodkov, lahko podjetje zmanjša z investicijo v korektivni varnostni ukrep s_k, ki zmanjšuje čas popravila t_r, ali v detekcijski varnostni ukrep s_d, ki zmanjšuje čas za detekcijo t_d.

Čas popravila t_r opišemo s funkcijo, ki je padajoča in konveksna; če je cena varnostnega ukrepa C neskončna (v varnostne ukrepe vlagamo neskončna sredstva), čas popravila t_r limitira proti nič. Funkcija, ki ustreza tem pogojem, je zato (Bojanc, 2010):

$$t_r = t_r^{\,0} e^{-\alpha_k C_k} \tag{13}$$

pri čemer je $t_r^{\,0}$ čas popravila brez uvedenega varnostnega ukrepa.

Tudi za čas detekcije t_d lahko veljajo enaki robni pogoji kot za čas popravila t_r ob vlaganju v korektivni ukrep s_k, le da govorimo o vplivu vlaganja v detekcijski ukrep s_d. Funkcija, ki ustreza tem robnim pogojem, je (Bojanc, 2010):

$$t_d = t_d^{\,0} e^{-\alpha_d C_d} \tag{14}$$

Poseben primer korektivnega ukrepa je prenos tveganja na zavarovalnico. V tem primeru je strošek C mesečna ali letna premija, ki jo podjetje plačuje zavarovalnici, v primeru incidenta pa zavarovalnica izplača podjetju kompenzacijo za kritje izgube v vrednosti I.

Z upoštevanjem enačb 13 in 14 lahko izgube v primeru varnostnega incidenta v enačbi 12 zapišemo:

$$L = L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \tag{15}$$

Na podlagi ocenjene verjetnosti varnostnega dogodka ρ v enačbi 10 in izgube L v enačbi 15 lahko izračunamo **varnostno tveganje *R*** kot produkt verjetnosti za incident in možne izgube:

$$R = \rho \cdot L = T \cdot v^{\alpha_p C_p + 1} \left[L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{16}$$

Tveganje R pomeni pričakovano izgubo zaradi nastanka varnostnega dogodka, ki jo enako kot L merimo v enakih denarnih enotah.

Za primer ocene ekonomske upravičenosti uvedbe varnostnega ukrepa uporabimo kazalec donosnosti investicije ROI. Kot je zapisano v enačbi 5, ROI primerja

koristi vlaganj v varnostni ukrep *B* s stroški *C*. Pozitivna vrednost ROI pomeni, da je vlaganje ekonomsko upravičeno. Koristi od vlaganj v varnostni ukrep *B* so enake zmanjšanju tveganja zaradi uvedbe ukrepa. Tako lahko zapišemo:

$$B = R_0 - R \tag{17}$$

pri čemer je R_0 varnostno tveganje pred uvedbo varnostnega ukrepa in R varnostno tveganje po uvedbi varnostnega ukrepa. Če v enačbo 5 vstavimo koristi iz enačbe 17, dobimo:

$$ROI = \frac{R_0 - R - C}{C} \tag{18}$$

Izračun ROI lahko prilagodimo različnim obravnavam tveganja. Če se varnostno tveganje R v enačbi 16 odpravlja (zmanjšuje) z **vlaganjem v preventivni varnostni ukrep s_p**, lahko enačbo 18 za ROI zapišemo:

$$ROI = \frac{T \cdot v\left(1 - v^{\alpha_p C_p}\right) \cdot L - C_p}{C_p} \tag{19}$$

Če se tveganje R v enačbi 16 odpravlja z **vlaganjem v korektivni varnostni ukrep s_k**, lahko enačbo 18 za ROI zapišemo:

$$ROI = \frac{TvL_1 t_r^{\,0}\left(1 - e^{-\alpha_k C_k}\right) - C_k}{C_k} \tag{20}$$

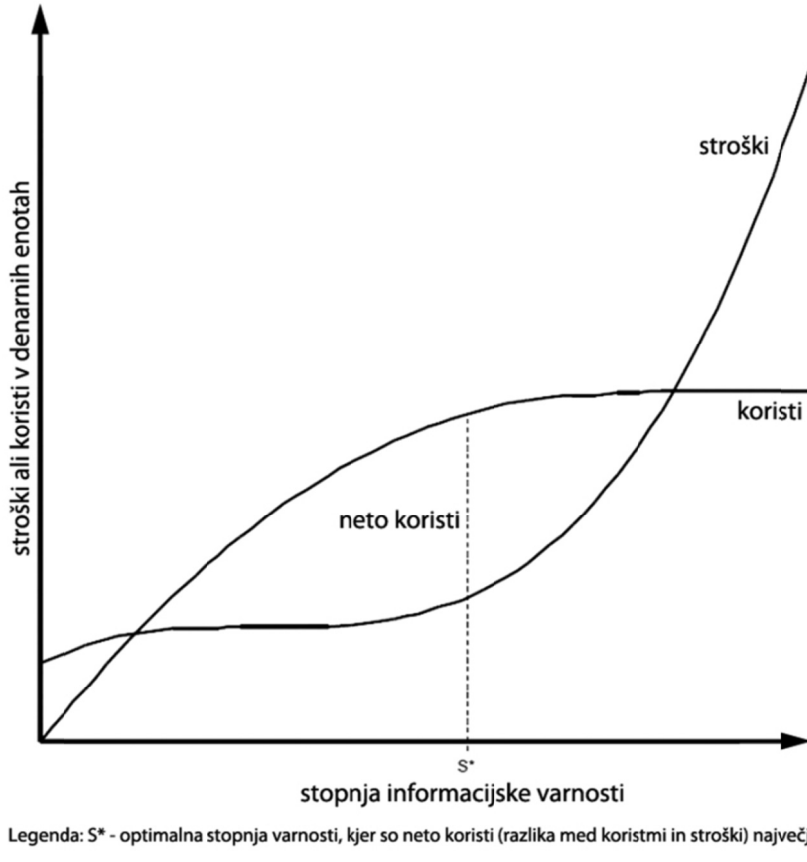
Pri **prenosu tveganja na zavarovalnico** je uveden korektivni varnostni ukrep s_k, saj s takim prenosom tveganja ne zmanjšujemo verjetnosti za varnostni incident, temveč le blažimo posledice, če je bil varnostni incident uspešen. Strošek *C* je znesek mesečne premije, ki se plačuje zavarovalnici. Enačba 18 se zato poenostavi v:

$$ROI = \frac{TvI - C}{C} \tag{21}$$

3.5 Iskanje optimalne stopnje informacijske varnosti

Eno izmed osnovnih vprašanj, ki si ga strokovnjaki na področju varovanja informacij zastavljajo, je, kako varen bi moral biti informacijski sistem. Poskusimo na to vprašanje odgovoriti z uporabo analize stroškov in koristi. Predpostavimo, da lahko zanesljivo ovrednotimo vse pričakovane skupne koristi v podjetju in širšem družbenem okolju ter vse pričakovane skupne stroške za različne ravni dejavnosti informacijske varnosti. Pri tem se seveda zavedamo, da je to v praksi zelo težko doseči. Dokler koristi dodatne aktivnosti informacijske varnosti presegajo stroške, je uvedba aktivnosti smiselna. Optimalna uvedba varnostnih ukrepov pa je dosežena v točki, kjer je razlika med koristmi in stroški največja. Uvedba dodatne aktivnosti informacijske varnosti, ki bi presegala to točko, namreč pomeni, da so mejni stroški njene uvedbe večji od mejnih koristi, ki jih s to dodatno aktivnostjo pridobimo. Z drugimi besedami, neto koristi (tj. koristi minus stroški) uvedbe mejne aktivnosti informacijske varnosti prek največje točke so negativne. Za podjetje ni smiselno, da bi za varnostno rešitev porabilo več, kot znašajo možne izgube v primeru incidenta. Grafični prikaz neto koristi v odvisnosti od stopnje informacijske varnosti je na Sliki 22.

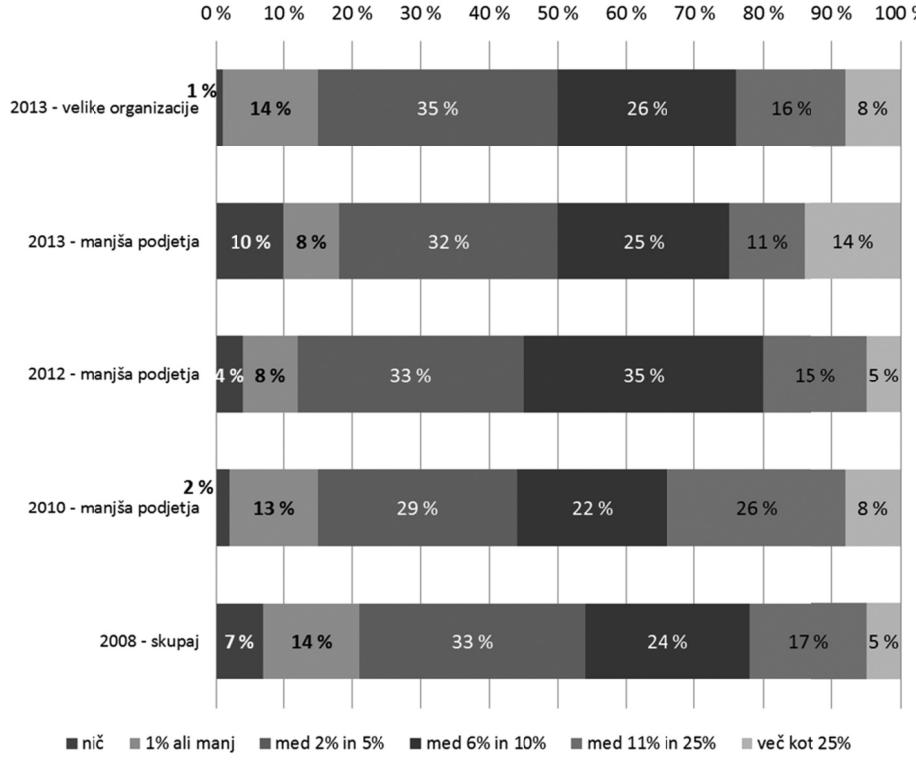
Slika 22: *Merjenje koristi in stroškov informacijske varnosti*



Vir: A. L. Gordon in P. M. Loeb, Economic Aspects of Information Security, 2003.

V praksi se podjetja srečujejo z omejenimi proračunskimi sredstvi za vlaganje v informacijsko varnost (Gordon & Loeb, 2005). Po raziskavi BIS (2013) se delež IT proračuna podjetja, namenjenega informacijski varnosti, v zadnjih letih povečuje in v letu 2013 znaša povprečno 10 % (v letu 2012 je znašal 8 %). Rezultati raziskave BIS so prikazani na Sliki 23. Tudi raziskava BERR (2008) je med podjetji v Veliki Britaniji zaznala občuten porast deleža IT proračuna, namenjenega informacijski varnosti, in sicer leta 2002 le 2 % IT proračuna, medtem ko leta 2008 že 7 %.

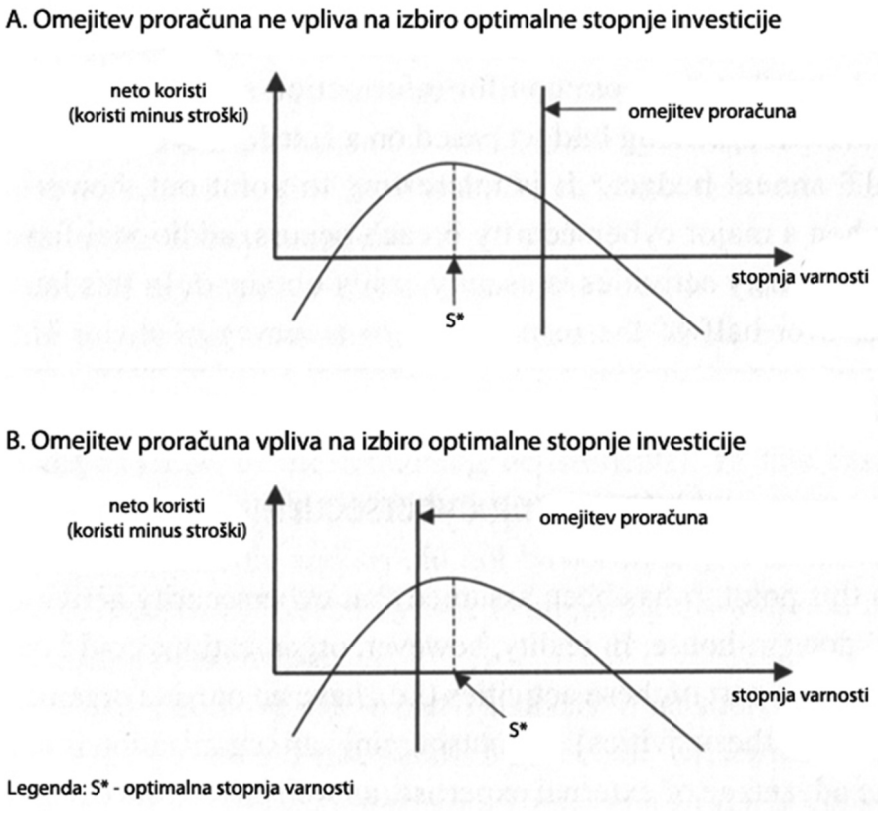
Slika 23: *Delež IT proračuna, namenjen informacijski varnosti*



Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

Omejitev proračuna je dodaten pogoj pri doseganju optimalne stopnje informacijske varnosti in je grafično prikazan na Sliki 24. Če je proračunskih sredstev več, kot bi jih potrebovali za optimalno vlaganje v informacijsko varnost, bo racionalno podjetje lahko vlagalo vse do optimalne stopnje varnosti. Če pa je višina proračunskih sredstev, ki so na voljo, manjša od tiste, ki je potrebna za optimalno vlaganje v informacijsko varnost, pa bo podjetje vložilo vsa razpoložljiva sredstva, vendar ne more investirati do optimalne stopnje, ker za to nima dovolj finančnih sredstev.

Slika 24: *Vpliv omejitve proračuna na investicijo v informacijsko varnost*



Vir: A. L. Gordon in P. M. Loeb, Managing Cyber-Security Resources, 2005.

S pomočjo modela za vrednotenje varnostnih tveganj in ukrepov, ki smo ga predstavili v poglavju 3.4, lahko ocenimo, kolikšna je potrebna investicija v varnostni ukrep, da bi se dosegla optimalna stopnja informacijske varnosti. Pri izračunu ocenimo, kdaj je neto korist ukrepa (razlika med koristmi in stroški) največja. Pri tem iščemo vrednost investicije v varnostni ukrep s*, s katerim dosežemo optimalno stopnjo informacijske varnosti, kar je prikazano na Sliki 22. Najprej opravimo izračun za preventivni ukrep. Če zapišemo razliko med koristmi in stroški, dobimo:

$$B(C_p) - C_p = \eta TvL \cdot (1 - v^{\alpha_p C_p}) - C_p \qquad (22)$$

Ker iščemo največjo neto pridobitev, veljata robna pogoja:

$$\frac{\partial(B(C_p)-C_p)}{\partial C_p}=0 \tag{23}$$

$$\frac{\partial^2(B(C_p)-C_p)}{\partial {C_p}^2}<0 \tag{24}$$

Zapišemo lahko:

$$\frac{\partial(B(C_p)-C_p)}{\partial C_p}=\frac{\partial(\eta TvL\cdot(1-v^{\alpha_p C_p})-C_p}{\partial C_p}=0 \tag{25}$$

$$-\alpha_p \eta TvLv^{\alpha_p C_p^*}\cdot\ln v-1=0 \tag{26}$$

$$v^{\alpha_p C_p^*}=-\frac{1}{\alpha_p \eta TvL\cdot\ln v}=\frac{1}{\alpha_p \eta TvL\cdot\ln\frac{1}{v}} \tag{27}$$

Pri tem je C_p* optimalna vrednost investicije:

$${C_p}^*=\frac{1}{\alpha_p}\log_v\left[\frac{1}{\alpha_p \eta TvL\cdot\ln\frac{1}{v}}\right]=\frac{\log_v}{{\alpha_p}^2\eta TvL\cdot\ln\frac{1}{v}} \tag{28}$$

Preverimo, ali je dobljeni rezultat zares maksimum:

$$\frac{\partial^2(B(C_p)-C_p)}{\partial {C_p}^2}=-{\alpha_p}^2\eta TvLv^{\alpha_p C_p}\cdot\ln^2 v \tag{29}$$

Zgornji rezultat daje negativno vrednost za vsak ukrep, zato je C_p* zares maksimum.

Izračuna za korektivni in detekcijski varnostni ukrep sta podobna, zato navedemo le izračun za korektivni ukrep. Za detekcijski ukrep lahko dobljeni rezultat

za korektivni ukrep le prepišemo. Koristi korektivnega varnostnega ukrepa zapišemo:

$$B(C_k) = \eta T v L_1 t_r^0 (1 - e^{-\alpha_k C_k}) \tag{30}$$

Za največjo neto pridobitev zapišemo:

$$\frac{\partial (B(C_k) - C_k)}{\partial C_k} = \frac{\partial (\eta T v L_1 t_r^0 (1 - e^{-\alpha_k C_k}) - C_k)}{\partial C_k} = 0 \tag{31}$$

$$\alpha_k \eta T v L_1 t_r^0 e^{-\alpha_k C_k^*} - 1 = 0 \tag{32}$$

$$e^{-\alpha_k C_k^*} = \frac{1}{\alpha_k \eta T v L_1 t_r^0} \tag{33}$$

$$C_k^* = \frac{1}{\alpha_k} \ln \left[\alpha_k \eta T v L_1 t_r^0 \right] \tag{34}$$

Tudi tu preverimo, ali je dobljeni rezultat zares maksimum:

$$\frac{\partial^2 (B(C_k) - C_k)}{\partial C_k^{\,2}} = -\alpha_k^{\,2} \eta T v L e^{-\alpha_k C_k} < 0, \forall C_k \tag{35}$$

Zgornji rezultat daje negativno vrednost za vsak ukrep, zato je C_k* zares maksimum.

Za detekcijski varnostni ukrep lahko enačbo 34 priredimo v:

$$C_d^* = \frac{1}{\alpha_d} \ln \left[\alpha_d \eta T v L_2 t_d^0 \right] \tag{36}$$

3.6 Praktična uporaba modela za iskanje optimalnega obsega investicije

Za praktičen prikaz uporabe modela si oglejmo dva primera izbire optimalne varnostne rešitve za grožnjo računalniški virus in spletno ribarjenje (phishing). Izračun je narejen na podlagi podatkov, pridobljenih v sodelovanju s slovenskim podjetjem, ki deluje na področju IT. Za izračun tveganja je treba dobiti podatke o grožnji, ranljivosti ter izgubi. Težava kvantitativnih metod je, da so rezultati zelo odvisni od natančnosti vhodnih podatkov. Trenutno za nekatera tveganja še vedno primanjkuje dobrih zgodovinskih podatkov, na podlagi katerih se lahko vhodni podatki natančno določijo, je pa zaradi novejših raziskav na voljo čedalje več statističnih podatkov. Pri vrednotenju verjetnosti grožnje T se moramo zavedati, da na verjetnost lahko vpliva veliko dejavnikov, in sicer kolikšna je vrednost informacijskih sredstev podjetja za napadalca, viri, ki jih ima napadalec na voljo, ali je informacija o stopnji varnosti v podjetju na voljo napadalcu (informacija o visoki stopnji varnosti lahko napadalca odvrne, saj mora imeti na voljo več virov).

Računalniški virusi so po raziskavah že vrsto let najpogostejša grožnja v podjetjih (CSI, 2011, 2009, 2008). Verjetnost grožnje je ocena pogostosti prejema okuženih datotek ali drugega načina okužbe in je ocenjena na enkrat na teden (T = 1/7 dni = 0,143/dan). Ranljivost je verjetnost, da bo računalniški virus okužil sredstvo, na katero je usmerjen. V okolju brez protivirusne programske rešitve je enaka ozaveščenosti zaposlenih, da v primeru, ko dobijo virus, tega ne aktivirajo. Podjetje ocenjuje, da bi glede na trenutno ozaveščenost in v okolju brez protivirusne zaščite virus prek okužene datoteke aktivirali dve tretjini zaposlenih (v = 0,66).

Za izračun izgube ob incidentu so ocenjene vrednosti L_1 = 41,53 €/uro, L_2 = 18,41 €/uro in L_3 = 0 €. Čas popravila in detekcije sta t_r^0 = 8 ur in t_d^0 = 2 uri. Če ni uvedenega nobenega varnostnega ukrepa, je izračunana verjetnost za incident ρ = 0,0952/dan, izguba v primeru incidenta L = 369,07 € in tveganje R = 35,15 €/dan. Podrobnejši postopek izračuna navedenih vrednosti je v Bojanc (2010).

Oglejmo si izračun za tri različne vrste potencialnih ukrepov. Prvi možen ukrep je nakup protivirusne programske opreme, ki jo podjetje namesti na svoje delovne postaje, prenosnike in strežnike, s centralnim posodabljanjem in analizo. Letno je potrebno podaljševanje naročnine za nove virusne definicije. Podjetje potrebuje licence za 50 računalnikov. Stroški nakupa znašajo 1.204 €, uvedba rešitve je 277 €, letni stroški nadgradenj 835 €, letni stroški upravljanja rešitve pa 138 €. Učinkovitost ukrepa je ocenjena na $\alpha = 2{,}10 \times 10^{-4.}$. Kot je navedeno v poglavju 2.3.2, se učinkovitost ukrepa lahko določa različno, za protivirusne programe je podatek dobljen na osnovi zbranih podatkov o učinkovitosti protivirusnih rešitev (AV-Test, 2008).

Drugi možen ukrep je izobraževanje in ozaveščanje zaposlenih prek spletnih izobraževanj. Podjetje izvede izobraževanje vsako leto, stroški izobraževanja znašajo 1.600 € na leto, poleg tega pa podjetje oceni še strošek uvedbe na 46 €. Učinkovitost ukrepa se zaradi vsakoletnega ponavljanja z leti povečuje. Tako znaša učinkovitost za prvo leto $\alpha = 0{,}48 \times 10^{-4}$, za četrto leto pa že $\alpha = 1{,}13 \times 10^{-4}$. V obeh primerih gre za preventiven ukrep, s katerim zmanjšujemo verjetnost, da se bo računalniška oprema v podjetju okužila z virusom.

Tretji možen ukrep je sistem za varnostno kopiranje ter redno izvajanje izdelave varnostnih kopij, ki zmanjšujejo čas okrevanja in zmanjšajo izgubo podjetja v primeru okužbe z virusom (to velja le v primeru, če podatki na varnostnih kopijah niso okuženi z virusom). Stroški nakupa rešitve so 2.650 €, uvedba rešitve 647 €, letni stroški upravljanja rešitve so ocenjeni na 1.387 €. Učinkovitost tega korektivnega ukrepa je ocenjena na $\alpha = 0{,}29 \times 10^{-4}$.

Pri izračunu so namenoma izbrani tehnični preventivni in korektivni tehnološki ukrepi ter izobraževanje uporabnikov, da se na ta način demonstrira zmogljivost modela za medsebojno vrednotenje različnih vrst varnostnih ukrepov. V izračunu je upoštevano časovno obdobje za investicijo 4 leta in diskontna stopnja 2,7 %. Prikaz stroškov in koristi za posamezne ukrepe je v Tabeli 4.

Tabela 4: *Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov*

	Protivirusna programska oprema			**Izobraževanje zaposlenih**			**Varnostno kopiranje**		
Leto	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)
0		1,481			1,646			3,297	
1	4.118	0	138	1.520	0	0	2.681	0	1,387
2	4.118	835	138	2.144	1,600	0	2.681	0	1,387
3	4.118	835	138	2.734	1,600	0	2.681	0	1,387
4	4.118	835	138	3.291	1,600	0	2.681	0	1,387

Na podlagi ocenjenih stroškov in koristi za posamezen ukrep lahko izračunamo kazalce donosnosti za posamezne ukrepe. Rezultati so prikazani v Tabeli 5. Prva zanimiva ugotovitev je, da dajo vsi ukrepi pri vseh izračunanih kazalcih pozitiven rezultat. Ekonomsko optimalna izbira je protivirusna programska oprema, na drugem mestu pa izobraževanje uporabnikov. Rezultati izračuna donosnosti z različnimi kazalci kažejo tudi na to, da se lahko rezultati izbire posameznih ukrepov za različne kazalce med seboj razlikujejo, zato jih je pri odločitvi dobro primerjati med seboj, kar potrjuje postavljeno hipotezo 2.

Tabela 5: *Izračun kazalcev ROI, NPV in IRR za posamezne ukrepe*

Ukrep	**ROI**	**NPV**	**IRR**
Protivirusna programska oprema	263 %	13.701 €	251 %
Izobraževanje zaposlenih	50 %	6.046 €	63 %
Varnostno kopiranje	21 %	7.930 €	21 %

Drugi praktični primer uporabe modela je grožnja spletno ribarjenje (phishing). Gre za potvorjena elektronska poštna sporočila in spletne strani s ponarejeno vsebino, s katero želijo zlonamerneži od naivnih uporabnikov pridobiti določene zaupne informacije (na primer gesla za dostop do banke ali podobnih ustanov ali pa številke kreditnih kartic). V takem primeru je ranljivost ocenjena na $v = 0{,}1$, grožnja na $T = 2{,}73*10^{-4}$/dan ter verjetnost za incident na $\rho = 2{,}73*10^{-5}$/dan. Faktorji izgube so ocenjeni na $L_1 = 23{,}5$ €/uro, $L_2 = 11{,}7$ €/uro in $L_3 = 1000$ €.

Čas popravila in detekcije sta t_r^0 = 16 ur in t_d^0 = 0 ur. Če ni uvedenega nobenega varnostnega ukrepa, je izračunana izguba v primeru incidenta L = 1.376,47 € in tveganje R = 13,76 €/leto. Podrobnejši postopek izračuna navedenih vrednosti je v Bojanc in Jerman-Blažič (2013).

Tveganje poskušamo zmanjšati na dva načina. Prvi je izobraževanje in ozaveščanje uporabnikov. Stroški prve izvedbe izobraževanja so ocenjeni na 2.047 €, nato pa še vsako leto 500 € dodatnega izobraževanja. Letni strošek organizacije izobraževanja je 141,18 €. Učinkovitost te rešitve je ocenjena na $\alpha = 4{,}09 \times 10^{-3}$. Druga možna rešitev je uvedba tehnične zaščite, ki filtrira neustrezno vsebino. Strošek uvedbe takega sistema je ocenjen na 2.225,59 €, letni strošek vzdrževanja pa 282,35 €. Učinkovitost rešitve je ocenjena na $\alpha = 0{,}65 \times 10^{-3}$. Izračunani stroški in koristi obeh ukrepov so prikazani v Tabeli 6.

Tabela 6: *Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov*

	Izobraževanje zaposlenih			**Tehnična rešitev**		
Leto	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)
0		2.047			2.226	
1	13,76	0	141,18	13,67	0	282,35
2	13,76	500	141,18	13,67	0	282,35
3	13,76	500	141,18	13,67	0	282,35
4	13,76	500	141,18	13,67	0	282,35

Na podlagi ocenjenih stroškov in koristi za posamezen ukrep lahko izračunamo kazalce donosnosti za posamezne ukrepe. Rezultati so prikazani v Tabeli 7. Zanimivo je, da dasta kazalca ROI in NPV negativne vrednosti za obe možni rešitvi, izračun IRR pa zaradi negativnih vrednosti NPV sploh ni mogoč. Poleg tega sta rezultata za obe rešitvi približno enako »slaba«.

Tabela 7: *Izračun kazalcev ROI, NPV in IRR za posamezne ukrepe*

Ukrep	ROI	NPV	IRR
Izobraževanje zaposlenih	–99 %	–3.909 €	–
Tehnična rešitev	–98 %	–3.231 €	–

Če bi podjetje obravnavalo obe navedeni grožnji skupaj (ribarjenje in virus), bi lahko ukrep izobraževanje zaposlenih dal drugačen rezultat. V tem primeru bi bili stroški izvedbe izobraževanja približno tolikšni kot pri uvedbi samo enega ukrepa, korist zaradi uvedbe pa bi bila seveda ustrezno velika. Seveda bi bilo treba v tem primeru, ko podjetje skupaj obravnava grožnji, izračunati tudi za druge predlagane rešitve in preveriti, ali bi kakšna druga rešitev dala še ugodnejše rezultate.

4 STANDARDI IN SISTEM RAVNANJA Z INFORMACIJSKO VARNOSTJO

4.1 Pregled standardov na področju informacijske varnosti

Pri uvedbi aktivnosti informacijske varnosti so podjetjem lahko v pomoč različni mednarodni standardi. Podjetja imajo namreč pogosto težave s prepoznavanjem groženj, ki pretijo njihovim informacijskim sredstvom, in s tem, kako naj se z grožnjami spopadejo (Farahmand, 2004). Sookdawoor (2005) zato podjetjem priporoča, naj se seznanijo s standardi in priporočili najboljše prakse, ki jih lahko uporabljajo kot vodilo pri izvajanju informacijske varnosti. Varnostni standardi in priporočila lahko pomagajo podjetjem pri zmanjševanju varnostnih tveganj in učinkovitejšem ravnanju s sistemi in omrežji, vplivajo pa tudi na uvedbo varnostnih tehnologij (Tudor, 2000). Farahmand (2004) ocenjuje, da podjetja običajno porabijo več energije in denarja za izpolnjevanje varnostnih ciljev, če ne upoštevajo standardov pri uvedbi tehnologij.

Pregled literature pokaže, da se s standardi in priporočili na področju informacijske varnosti ukvarja veliko organizacij. Med pomembnejšimi so naslednje:

- ISO – International Organization for Standardization,
- BSI – British Standards Institute,
- ENISA – European Union Agency for Network and Information Security,
- CEN – European Committee for Standardization,
- ETSI – European Telecommunications Standards Institute,
- NIST – National Institute of Standards and Technology,
- CERT – Computer Emergency Response Team,
- ISACA – Information Systems Audit and Control Association,
- SANS – (SysAdmin, Audit, Network, Security) Institute,
- ISSA – Information Systems Security Association,
- CSI – Computer Security Institute,
- ISA – Internet Security Alliance,
- CIS – Center for Internet Security.

Standarde in priporočila s področja informacijske varnosti lahko razvrstimo v več področij glede na to, na čem je poudarek posameznega standarda ali priporočila (Bojanc, 2010). Med standarde, ki so usmerjeni na obvladovanje tveganja, razvrščamo naslednje:

- ISO Guide 73 (2009). Vodič definira slovar obvladovanja tveganja in priporočila za uporabo v standardih ISO. Osredotočen je na terminologijo.
- ISO 31000 (2009) podaja principe in splošne smernice za obvladovanje tveganja in ni vezan na industrijo ali sektor. Napotke za učinkovito obvladovanje tveganja z izvajanjem ISO 31000 daje ISO/TR 31004 (2013), napotke za izbiro in uporabo sistematičnih tehnik za oceno tveganja pa ISO/IEC 31010 (2009).
- Standard ISO/IEC 27005 (2011) podaja metodologijo obvladovanja tveganja, ki je namenjena predvsem pomoči pri uvedbi standarda ISO/IEC 27001 (2013).
- Razne metode za obvladovanje tveganja (OCTAVE, CRAMM, EBIOS, MEHARI itd.).

Nekateri standardi povzemajo najboljšo prakso, ki pomaga podjetjem pri uvedbi sistema informacijske varnosti:

- ISO/IEC 27001 (2013) »Sistemi upravljanja informacijske varnosti – Zahteve« in ISO/IEC 27002 (2013) »Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti«. Cilj teh dveh standardov je ponuditi model za vzpostavitev, uvedbo, ravnanje, nadzor, pregled, vzdrževanje in izboljšave sistema vodenja informacijske varnosti (angl. *Information Security Management System – ISMS*).
- RFC 2196 (1997) »Site Security Handbook« je vodič za razvoj varnostnih politik in postopkov za sisteme, ki so dostopni prek interneta.
- Information Technology Infrastructure Library (ITIL) je zbirka najboljše prakse s področja obvladovanja IT-storitev, ki vključuje tudi področje varnosti.
- ISO/IEC 15408 je zbirka treh standardov (ISO/IEC 15408-1, 2009; ISO/IEC 15408-2, 2008; ISO/IEC 15408-3, 2008), ki podajajo merila za ocenjevanje IT-varnosti. Standardi ponujajo nabor zahtev za varnostne funkcije v IT-produktih in sistemih, ki jih je treba izpolnjevati. Namen

standardov je pomoč razvijalcem, ocenjevalcem in kupcem varnostnih produktov.

Med standardi, ki podajajo smernice s področja informacijske varnosti, so med najbolj upoštevanimi v stroki naslednji:

- Standard ISO/IEC 13335-1 (2004) je prvi v seriji priporočil ISO/IEC 13335. Ukvarja se z načrtovanjem, obvladovanjem in uvedbo informacijske varnosti. Prvi del predstavlja koncepte in modele, ki se lahko uvedejo v različne organizacije.
- NIST 800-27 (2004) in NIST 800-30 (2012). National Institute of Standards and Technology (NIST) izdaja publikacije iz serije 800 s področja računalniške varnosti. Publikaciji NIST 800-27 in NIST 800-30 podajata terminologijo in koncepte s tega področja. Leta 1996 je National Institute for Standards and Technology (NIST) objavil publikacijo SP800-14 »Generally Accepted Principles and Practices for Securing Information Technology Systems«, v kateri je navedenih osem principov, ki so postali znani kot splošno sprejeti sistem varnostnih principov (*Generally Accepted System Security Principles – GASSP*) (NIST 800-14, 1996). Ti principi so bili prvotno predstavljeni v drugem poglavju NIST-publikacije »An Introduction to Computer Security: The NIST Handbook« iz leta 1995. Leta 2001 je NIST objavil publikacijo SP800-27 »Engineering Principles for Information Technology Security (A Baseline for Achieving Security)«, ki se osredotoča na principe in prakso iz SP800-14 s sistemskega vidika in ne toliko z organizacijskega vidika (NIST 800-27, 2004).

Določeni standardi so usmerjeni bolj v sam proces izvajanja informacijske varnosti. Taka standarda sta na primer:

- ISO/IEC 21827 (2008), ki določa ključne karakteristike procesa varnostnega inženiringa v organizaciji, in
- CobiT – Control Objectives for IT (ISACA), ki podaja fleksibilno ogrodje, da organizacije dosežejo poslovne cilje ter zahteve po kvaliteti, financah in varnosti. Določa sedem informacijskih kriterijev: učinkovitost, zmogljivost, zaupnost, celovitost, razpoložljivost, skladnost in zanesljivost informacij.

O uporabi varnostnih standardov, priporočil in politik je bilo izvedenih precej raziskav (BIS, 2013; CSI, 2011; DSCI, 2009; BERR, 2008; DTI, 2006; Berinato, 2004). Veliko ugotovitev je spodbudnih in so zelo razveselile strokovnjake za informacijsko varnost. Nekaj pozitivnih ugotovitev teh študij:

- velika potreba po izobraževanju s področja varnosti in ozaveščanja vseh zaposlenih;
- investicije v varnostne projekte se na splošno povečujejo;
- organizacije po vsem svetu so zaskrbljene zaradi varnostnih politik in ugotovitev skladnosti, pri tem so potrebna prizadevanja za odpravo vseh vrzeli v skladnosti.

Na nekaterih področjih so bile ugotovitve zaskrbljujoče in zahtevajo ukrepanje. Ključna negativna spoznanja so naslednja:

- neskladnost z informacijsko varnostno politiko, standardi in predpisi;
- obstaja veliko primerov, kjer varnostna politika ni ustrezno opredeljena;
- pomanjkanje prizadevanja za merjenje varnostnih projektov in njihovo sledenje;
- če obstajajo varnostne politike, je bilo ugotovljeno, da niso bile redno vzdrževane;
- pravila in postopki v varnostnih politikah so pogosto prezapleteni in jih je težko uvesti v realno poslovanje;
- nekatere raziskave so pokazale nizko zavezanost najvišjega vodstva na določenih področjih uvedbe varnosti.

4.2 Sistem vodenja informacijske varnosti

Informacijska varnost vključuje tehnologijo in ljudi, zato je učinkovito reševanje informacijske varnosti odvisno od tehničnih rešitev in človeških virov. S tehnične strani mora podjetje uporabiti ustrezno kombinacijo sredstev, kot na primer šifrirne tehnike, požarne zidove, sisteme za učinkovit nadzor dostopa in sisteme za zaznavanje vdorov. Poleg tega so za zagotovitev ustrezne stopnje varnosti potrebni še človeški viri, ki znajo te tehnične rešitve pravilno uporabiti (Gordon & Loeb, 2005; Boss, 2007). Tehnološki napredek je sicer čedalje večji, vendar je vse očitneje, da je človek še vedno najšibkejši člen varnosti (Germain, 2007; Gonzalez & Sawicka, 2002). Kot poudarja Schneier (2004a), je varnost

predvsem človeški in ne tehnološki problem, zato je treba v podjetjih uvesti sisteme za ravnanje z informacijsko varnostjo, ki varnostno problematiko obravnavajo celovito. To je med drugimi ugotovil Straub (1990), ki je v svoji študiji, v kateri je zajel 1.211 podjetij, ugotovil, da je ozaveščanje o varnosti (na primer uvedba politik in postopkov) učinkovitejše kot tehnične rešitve.

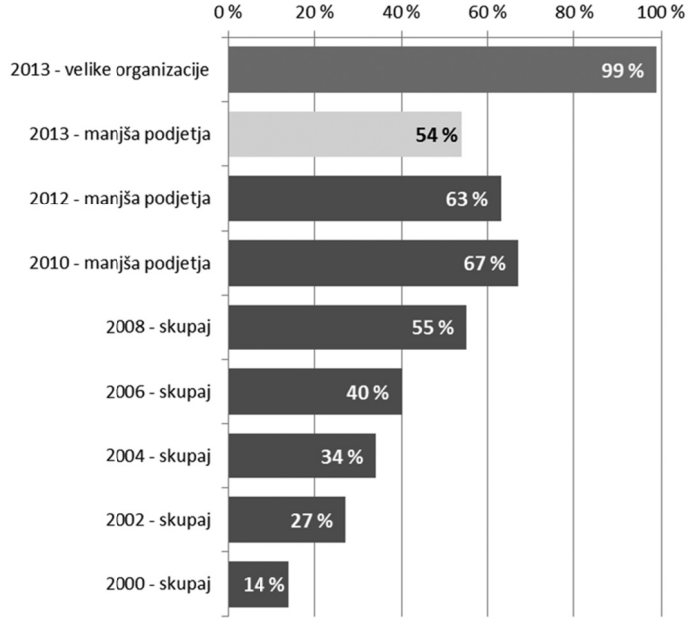
Za sistem vodenja informacijske varnosti (angl. *Information Security Management System – ISMS*) se v Sloveniji uporablja kar nekaj različnih izrazov. Najpogosteje se uporabljajo izrazi »sistem upravljanja varovanja informacij«, »sistem vodenja varovanja informacij«, »sistem upravljanja informacijske varnosti« ter »sistem vodenja informacijske varnosti«. Kot smo obrazložili že v uvodu, menimo, da je informacijska varnost ustreznejši prevod izraza information security, kar se ujema tudi s slovenskim prevodom standarda SIST ISO/IEC 27001:2013. Standard sicer za ISMS uporablja prevod »sistem upravljanja varovanja informacij«, kot pa smo razložili že uvodoma, menimo, da je management bolje prevajati kot vodenje namesto upravljanje. Tako za ISMS v monografiji uporabljamo izraz »sistem vodenja informacijske varnosti« (SVIV). SVIV omogoča sistematičen in strukturiran pristop ravnanja z informacijami, ki zagotavlja zaupnost, celovitost in razpoložljivost informacij. Uvedba sistema SVIV vključuje politike, procese, procedure, organizacijsko strukturo ter programske in strojne rešitve. Vodstvo podjetja mora jasno izreči svojo podporo uvedbi in izvajanju sistema SVIV, njegova uvedba pa je povezana s strateškimi cilji podjetja, varnostnimi zahtevami, poslovnimi procesi, velikostjo in strukturo podjetja. Pri uvedbi sistema SVIV si podjetja pomagajo z različnimi standardi. Ne glede na izbiro standarda, na katerem temelji SVIV, pa vsi sistemi SVIV temeljijo na obvladovanju varnostnih tveganj, ki vplivajo na poslovanje podjetja. Z vzpostavitvijo sistema SVIV podjetje

- pridobi strukturiran način vodenja informacijske varnosti znotraj podjetja,
- omogoča neodvisno oceno skladnosti podjetja z najboljšimi praksami informacijske varnosti,
- izboljša vodenje informacijske varnosti v podjetju,
- poveča svoj ugled in pozicioniranje na trgu,
- poveča stopnjo informacijske varnosti v podjetju.

Informacijski sistemi imajo določene aktivnosti avtomatizirane in se izvajajo skladno z nastavitvami računalniškega sistema, določene aktivnosti pa so odvisne od interakcij z uporabniki. V takih primerih je treba uvesti politike, ki uporabniku predstavijo pravila dela in ga ozaveščajo o varnostnih zlorabah, ki lahko vodijo v varnostne incidente. Te politike so jedro sistema SVIV in pravilo-ma temeljijo na določenem standardu. Uporaba standarda omogoča sistematično izvedbo analize tveganja na vsaki točki kontrole. Sistematični pristop zagotavlja, da se politike pripravljajo enotno, se ne podvajajo ter so med seboj skladne (Broderick, 2006; Overill, 2008).

Po podatkih raziskave BIS (2013) imajo skoraj vse velike organizacije doku-mentirano varnostno politiko, pri manjših podjetjih pa se število podjetij z doku-mentirano varnostno politiko v zadnjih letih zmanjšuje. V raziskavi ugotavljajo, da se v manjših podjetjih zanašajo na ustne dogovore. Rezultati so prikazani na Sliki 25.

Slika 25: *Delež podjetij, ki formalno dokumentirajo varnostno politiko*

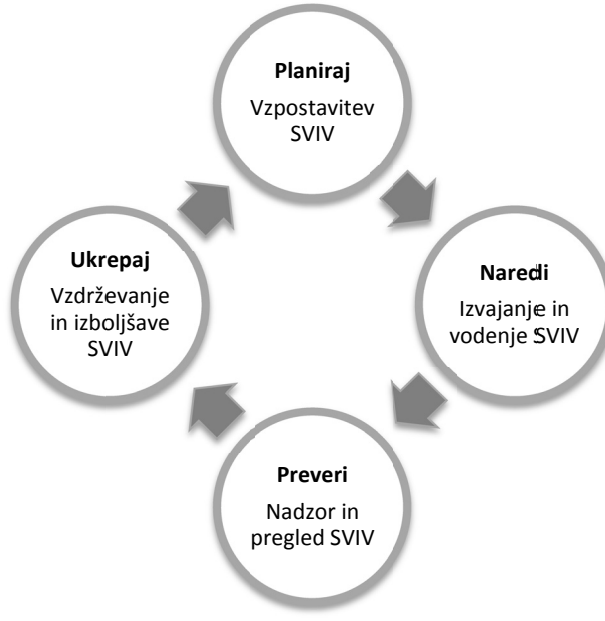


Vir: BIS, 2013 Information Security Breaches Survey, Technical Report, 2013.

Procesi SVIV običajno temeljijo na Demingovem modelu PDCA (angl. *Plan-Do-Check-Act,* v nadaljevanju PDCA) (ISO 9001, 2008; Hoyle, 2009; Oakland, 2003), ki opredeljuje štiri ključne faze neprestanega izboljševanja procesov, kot je prikazano na Sliki 26.

- **Planiraj** (angl. *Plan*), kjer se določijo cilji in planirajo pričakovani rezultati.
- **Naredi** (angl. *Do*), kjer se skladno z zahtevami procesa izvajajo potrebne aktivnosti.
- **Preveri** (angl. *Check*), kjer se s pomočjo notranjih presoj in vodstvenih pregledov nadzoruje skladnost delovanja glede na zastavljene cilje.
- **Ukrepaj** (angl. *Act*), kjer se določijo korektivni ukrepi in izboljšajo obstoječi procesi.

Slika 26: *Model PDCA za SVIV*

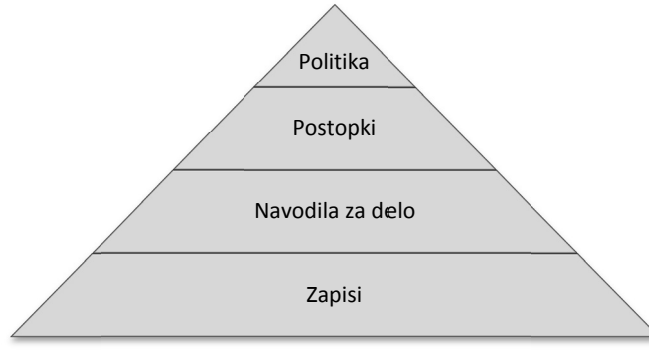


Vir: J. H. P. Eloff in M. M., Eloff, Information Security Architecture, 2005.

Vsak sistem SVIV je treba ustrezno dokumentirati. Dokumentacija sistema SVIV je hierarhična, kot je prikazano na Sliki 27. Na vrhu so politike, ki

podajajo splošne cilje skupaj z vlogami in odgovornostmi posameznikov. Sledijo postopki, ki določajo, kako se dosegajo cilji politik in kako se izvajajo procesi. V navodilih za delo se podajajo podrobna navodila, kako uporabniki izvajajo politiko ter kako se izvajajo naloge. Na najnižji ravni so zapisi, ki omogočajo evidence, da se politika izvaja skladno z zastavljenimi cilji. Zapisi so tudi povratna zanka za preglede in popravke uvedenih politik, če se izrazimo skladno z modelom PDCA. Na podlagi ciljev in procesov načrtujemo pričakovane rezultate, naredimo sistem, preverimo pravilnost rezultatov in ukrepamo, če ugotovimo razlike.

Slika 27: *Hierarhija dokumentacije sistema SVIV*



Vir: D. H. Besterfield, Total Quality Management, 2002.

Navedeno hierarhijo dokumentacije si oglejmo na naslednjem primeru. Podjetje ima uvedeno politiko uporabe računalniške opreme, v kateri je navedeno, da imajo vsi uporabniki enoličen identifikator (ID uporabnika) za dostop do vseh informacijskih storitev podjetja. Za podporo te politike se uvede postopek, v katerem je navedeno, da se lahko ID uporabnika za študente ustvari samo prek aplikacije v kadrovski službi. Navodila za delo natančno opredelijo delo kadrovske službe za ustvarjanje ID uporabnika, dnevniki tega postopka pa predstavljajo zahtevane zapise.

4.3 Standard ISO/IEC 27001

V praksi večina sistemov SVIV temelji na standardu ISO/IEC 27001 (2013) in drugih povezanih standardih iz družine ISO 27000. Začetki standarda ISO/IEC 27001 segajo v leto 1995, ko je organizacija British Standards Institution (BSI) objavila standard BS 7799, v katerem so zbrane najboljše prakse vodenja informacijske varnosti. Standard je bil leta 1998 revidiran, leta 2000 pa ga je sprejela International Organisation for Standardisation (ISO) in objavila kot ISO/IEC 17799: »Pravila obnašanja pri vodenju informacijske varnosti« (angl. *A Code Of Practice For Information Security Management*). Namen ISO 17799 je bil zagotoviti skupno osnovo za razvoj standardov za varovanje organizacij in učinkovito prakso vodenja varnosti in za zagotovitev zaupanja v medorganizacijsko poslovanje. Cilj standarda ISO 17799 je omogočiti podjetjem zmanjšanje tistih IT-groženj, ki izhajajo iz fizičnih okvar, zlorab in industrijskega vohunjenja. Standard ISO/IEC 17799 je bil leta 2005 revidiran in pridružen v družino standardov ISO 27000 kot ISO/IEC 27002. Zadnja prenova ISO/IEC 27002 je bila leta 2013, ko so se kontrole precej preuredile. Zadnja različica standarda ISO/IEC 27002 predstavlja katalog 114 varnostnih kontrol, ki naj bi jih sistem SVIV uvedel. Kontrole so razvrščene v skupno 14 varnostnih področij, ki jih standard pokriva:

- informacijske varnostne politike,
- organiziranje informacijske varnosti,
- varnost človeških virov,
- ravnanje s sredstvi,
- nadzor dostopa,
- kriptografija,
- fizična in okoljska varnost,
- varnost poslovanja,
- varnost komunikacij,
- pridobivanje, razvoj in vzdrževanje sistemov,
- odnosi z dobavitelji,
- ravnanje z incidenti informacijske varnosti,
- vidiki informacijske varnosti pri obvladovanju neprekinjenega poslovanja,
- skladnost.

Leta 1999 je BSI izdal drugi del standarda BS 7799-2 »Sistemi vodenja informacijske varnosti – specifikacije in priporočila za uporabo« (angl. *Information Security Management Systems – Specification with guidance for use*). BS 7799-2 se osredotoča na to, kako naj organizacije uvedejo SVIV. Leta 2002 je bila izdana revizija BS 7799-2, katere namen je bil uskladitev z ostalimi standardi, ki pokrivajo sisteme vodenja, in v BS 7799-2 vključila tudi Demingov model PDCA. Dokument BS 7799-2 je novembra 2005 sprejela organizacija ISO kot svoj standard ISO/IEC 27001. ISO je leta 2013 standard ISO/IEC 27001 prenovil, da bi ga bolj poenotil z drugimi standardi vodenja ISO, predvsem s prihajajočo izdajo standarda ISO 9001.

Po raziskavi BIS (2013) ima približno četrtina sodelujočih podjetij v celoti uveden standard ISO 27001 (2013), približno enak delež pa ga nima in ga tudi ne namerava uvesti. Kar 76 % velikih organizacij, ki se zavedajo pomena standarda ISO 27001, pa ima ta standard tudi delno ali v celoti uveden. Po raziskavi BERR (2008) kar 40 % podjetij izvaja izobraževalne programe za zaposlene s področja informacijske varnosti.

Družina standardov SVIV je rezervirana za sistem vodenja informacijske varnosti, katere namen je pomagati podjetjem in organizacijam pri uvedbi in izvajanju SVIV. Družina standardov SVIV ima skupen naslov »Informacijska tehnologija – Varnostne tehnike« in jo sestavljajo naslednji standardi:

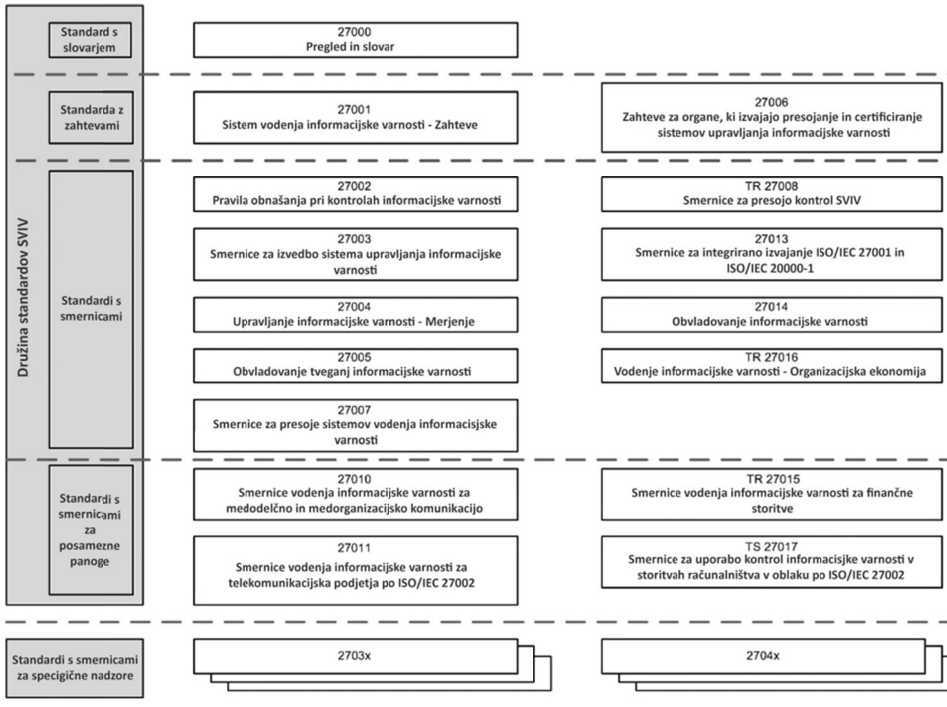
- ISO/IEC 27000:2014, ki podaja pregled družine standardov ISO 27000 in slovar uporabljenih izrazov;
- ISO/IEC 27001:2013, ki določa zahteve sistema vodenja informacijske varnosti (SVIV) in specifikacije, po katerih se lahko organizacije certificirajo;
- ISO/IEC 27002:2013, ki podaja pravila obnašanja pri kontrolah informacijske varnosti ter vključuje nabor 114 varnostnih kontrol, ki so sprejete kot dobra praksa;
- ISO/IEC 27003:2010, ki ponuja pomoč pri uvedbi sistema SVIV, ki temelji na standardu ISO/IEC 27001;
- ISO/IEC 27004:2009, ki predlaga kazalce za pomoč pri izboljšavi učinkovitosti SVIV;
- ISO/IEC 27005:2011, ki obvladuje varnostno tveganje;

- ISO/IEC 27006:2011, ki podaja zahteve za organizacije, ki izvajajo revizijo in certifikacijo sistemov SVIV;
- ISO/IEC 27007:2011, ki je vodič za revizijo SVIV s poudarkom na vodenju sistema;
- ISO/IEC TR 27008:2011, ki je vodič za revizijo SVIV s poudarkom na varnostnih kontrolah;
- ISO/IEC 27010:2012, ki je vodič SVIV za komunikacijo med oddelki in med organizacijami;
- ISO/IEC 27011: 2008, ki je vodič SVIV za vodenje informacijske varnosti, ki temelji na standardu ISO/IEC 27002, namenjen pa je telekomunikacijskim organizacijam (standard je tudi objavljen kot ITU X.1051);
- ISO/IEC 27013:2012, ki je vodič za integrirano izvajanje ISO/IEC 27001 in ISO/IEC 20000-1 (izhaja iz ITIL);
- ISO/IEC 27014:2013, ki pokriva obvladovanje informacijske varnosti;
- ISO/IEC TR 27015:2012, ki je vodič SVIV za vodenje informacijske varnosti, namenjen finančnim organizacijam in zavarovalnicam;
- ISO/IEC TR 27016:2014, ki je osredotočen na ekonomski vidik sistema SVIV.

Družino standardov SVIV sestavljajo med seboj povezani standardi, ki so glede na svojo vlogo razdeljeni na štiri področja (Slika 28):

- standardi, ki podajajo pregled in terminologijo;
- standardi, ki določajo zahteve;
- standardi, ki opisujejo splošne smernice;
- standardi, ki opisujejo smernice, specifične za posamezen sektor.

Slika 28: *Relacije med standardi družine SVIV*



Vir: ISO 27000, 2014.

4.4 Revizija informacijske varnosti

Kot smo spoznali v preteklih poglavjih, je naloga informacijske varnosti načrtovanje in nadzorovanje procesov, ki zagotavljajo zaščito zaupnosti informacij, časovno ustrezno razpoložljivost informacij pooblaščenim uporabnikom in zaščito celovitosti informacij. Vendar je vzpostavitev in izvajanje informacijske varnosti le prvi korak. Ko je varnostni proces vzpostavljen, je treba redno preverjati, kako uspešno se dosegajo zastavljeni cilji. S preverjanjem izvajanja varnostnega procesa se ukvarja revizija informacijske varnosti. Pri tem ne gre le za izvedbo popravnih ukrepov za trenutno stanje, temveč se na ta način tudi pomaga izboljšati prihodnje stanje informacijske varnosti. V splošnem je obseg revizije informacijske varnosti usmerjen na preverjanje fizične varnosti in nadzora dostopa, preverjanje skrbniških postopkov, ocenjevanje učinkovitosti

sistemov za preprečevanje vdorov in ocenjevanje varnostnega osebja v podjetju. Revizija lahko v podrobni analizi ocenjuje tudi ekonomske učinke aktivnosti informacijske varnosti glede na stroške, ki so potrebni za izvedbo teh aktivnosti (Gordon & Loeb, 2005).

Običajno v podjetjih in organizacijah pripravijo seznam varnostnih postopkov, ki jih skozi revizijo pregledajo in preverijo stanje varnosti. Pri varnostnih postopkih je treba upoštevati pravilo stroškov in koristi, se pravi, da so koristi izvajanja postopka večje ali vsaj enake stroškom tega postopka. Izvajanje revizije informacijske varnosti zahteva pripravo načrta presoje. Gordon in Loeb (2005) zagovarjata, da naj se načrt začne s presojo ciljev informacijske varnosti ter nadaljuje s poudarkom na naslednjih šestih področjih, povezanih z varnostjo:

- politike in postopki,
- operativni in tehnični pogledi na računalniško strojno in programsko opremo,
- zadeve, povezane z osebjem,
- ranljivosti in grožnje,
- ocenjeni stroški varnostnih kršitev,
- povrnitve investicij v informacijsko varnost.

Pogosto uporabljena tehnika pri revizijah informacijske varnosti je penetracijsko testiranje, ki predstavlja poskuse vdorov v lastno računalniško omrežje. Penetracijsko testiranje lahko izvaja notranji zaposleni v podjetju ali pa se za izvajanje najame podjetje, ki se profesionalno ukvarja z varnostnim preverjanjem. Pomembno je, da se z vdori simulirajo realni možni napadi. V nekaterih organizacijah vodstvo podjetja naroči in odobri penetracijsko testiranje, ne da bi o tem seznanilo varnostno osebje podjetja, saj tako dobijo celovitejše in realistične rezultate testiranja (Gordon & Loeb, 2005).

Revizija informacijske varnosti lahko poveča vrednost podjetja na vsaj dva načina. Prvič, že zgolj dejstvo, da ima podjetje uvedene take procese, poveča odgovornost managerjev, ki vodijo informacijsko varnost, saj se zavedajo, da bodo odgovarjali za svoje odločitve in aktivnosti. Povedano drugače, vodje informacijske varnosti sedaj vedo, da je vzpostavljen postopek, ki bo povezal njihovo dejansko uspešnost s pričakovano uspešnostjo. Tako vzpostavljen proces

je močan motivator, ki zagotavlja, da bodo managerji resno in zavzeto reševali težave informacijske varnosti.

Drugi način za povečanje vrednosti podjetja skozi revizijo je pridobitev informacij o stanju varnosti ter kako uspešno se izvajajo procesi informacijske varnosti. Dejanska stopnja informacijske varnosti se lahko razlikuje od planirane stopnje in razlika med dejansko in planirano varnostjo lahko služi kot osnova za izvedbo sprememb v načinu, kako podjetje planira, izvaja in nadzoruje aktivnosti informacijske varnosti. Z drugimi besedami, revizija informacijske varnosti je sestavni del procesa obvladovanja planiranja in nadzora.

4.5 Dobra praksa uvajanja sistema za vodenje varovanja informacij v podjetniškem okolju

V tem poglavju bomo predstavili dobro prakso uvajanja sistema za vodenje informacijske varnosti SVIV. Predstavljena uvedba sistema zajema 12 korakov, ki podjetjem omogočajo vpogled v potrebne aktivnosti za uvedbo sistema SVIV.

1. korak: seznanitev s standardi ISO/IEC

Pred začetkom uvedbe se je treba seznaniti z nekaterimi standardi ISO/IEC. Obvezen je pregled vsebine standardov ISO/IEC 27001 (2013) in ISO/IEC 27002 (2013), ki je temelj uvedbe SVIV. Za lažjo uvedbo se priporoča še seznanitev z ISO/IEC 27000 (2014), ISO/IEC 27003 (2010) in ISO/IEC 27005 (2011). Standarde je mogoče dobiti na spletni strani

- Slovenskega inštituta za standardizacijo SIST (http://www.sist.si) in
- Mednarodne organizacije za standardizacijo ISO (http://www.iso.org).

2. korak: pridobitev podpore vodstva

Kot navaja ISO/IEC 27001, igra vodstvo podjetja pomembno vlogo pri uspešni uvedbi SVIV. To je navedeno tudi v posebnem razdelku varnostne politike – odgovornost vodstva. Vodstvo se mora zavezati k uvedbi, izvajanju, delovanju, nadzoru, pregledu, vzdrževanju in izboljševanju SVIV. Zavezanost mora vključevati aktivnosti, ki zagotavljajo ustrezno razpoložljivost virov na področju SVIV, ter da bodo vsi zaposleni, ki so vključeni v SVIV, imeli ustrezno

izobraževanje, ozaveščenost in kompetence. Poleg tega vodstvo sodeluje v procesu SVIV PDCA.

3. korak: določitev obsega SVIV

Treba je določiti, katera sredstva obsega SVIV in kje so meje sistema. Določi se, katere poslovne procese, lokacije, strojno opremo, programsko opremo, podatke in informacije ter človeške vire vključuje SVIV. Obseg naj bo obvladljiv. Lahko se vključi samo del podjetja, kot so logične in fizične skupine znotraj podjetja. To velja še zlasti za večja podjetja.

4. korak: določitev metode za oceno tveganja

Oceno tveganja smo podrobno predstavili v drugem poglavju. Kot smo ugotovili, je ocena tveganja proces prepoznave tveganj z analizo grožen ter njihovih posledic, ranljivosti informacij in informacijskih sistemov ter verjetnosti za to, da se zgodijo. Izbira metode za oceno tveganja je eden najpomembnejših delov vzpostavitve SVIV.

Za izpolnitev zahtev ISO/IEC 27001 je treba določiti in dokumentirati metodo za oceno in obravnavo tveganja ter jo nato redno uporabljati za ocenjevanje tveganj, ki so vezana na informacijska sredstva, na odločanje, katera tveganja so sprejemljiva in katera je treba zmanjšati ter skrbeti, da bodo ta tveganja upoštevana v politikah, procedurah in kontrolah. ISO/IEC 27001 ne določa, katero metodo za oceno tveganja naj podjetja uporabijo, zahteva pa, da izbrana metoda omogoča:

- vrednotenje tveganj glede na zaupnost, celovitost in razpoložljivost;
- določitev ciljev za zmanjšanje tveganj na sprejemljivo raven;
- določitev kriterijev za sprejem tveganja;
- vrednotenje različnih obravnav tveganja.

Za pomoč pri izbiri metode za oceno tveganja ter izvajanje rednih ocen tveganj je na voljo standard ISO/IEC 27005 (2011) Information security risk management, dodatno pa si lahko pomagamo s standardom ISO 31000 (2009) in z NIST SP 800-30 (Risk Management Guide for Information Technology Systems).

5. korak: priprava seznama informacijskih sredstev

Da bi se lahko določila tveganja, povezana z informacijami in sredstvi, ki jih želimo varovati, je treba najprej pripraviti seznam vseh informacijskih sredstev, ki so zajeta v obsegu SVIV. Za vsako informacijsko sredstvo je treba navesti lastnika sredstva ter kako kritično je sredstvo za poslovanje podjetja.

6. korak: določitev tveganj

Za vsako sredstvo s seznama, pripravljenega v prejšnjem koraku, moramo skladno z izbrano metodologijo tveganja določiti tveganja, povezana s posameznim sredstvom. Za začetek je dobro pripraviti seznam možnih ranljivosti in seznam možnih groženj, kot je navedeno v drugem poglavju. Vsa prepoznana tveganja naj se zapišejo v obliki seznama, kjer je posamezno tveganje povezano z določenim informacijskim sredstvom, določeno grožnjo in določeno ranljivostjo.

7. korak: ocena tveganj

Ko so tveganja prepoznana in zabeležena, jih moramo ovrednotiti. Vrednotenje se izvaja na podlagi sprejete metode tveganja, ki je lahko kvantitativna ali kvalitativna. Za vsako tveganje se določi verjetnost, da se bo zgodilo, ter možna posledica v primeru izvedbe tveganja. Ko so vsa tveganja ovrednotena, se določi, katera tveganja so pod pragom obravnave tveganja in jih lahko sprejmemo. Za preostala tveganja se v naslednjem koraku določi ustrezna obravnava – kako naj se tveganja zmanjšajo.

8. korak: določitev uporabljenih ciljev in kontrol

Za tveganja, ovrednotena kot nesprejemljivo visoka, je treba izbrati ustrezno obravnavo tveganja:

- izogibanje tveganja,
- prenos tveganja na zavarovalnico ali zunanjega izvajalca,
- zmanjšanje tveganja na sprejemljivo raven skozi uporabo kontrol.

Za zmanjšanje tveganja je treba izbrati ustrezne kontrole. To so lahko kontrole, ki jih je podjetje že uvedlo, ali kontrole, ki jih določa standard ISO/IEC 27002. Preučevanje kontrol, ki jih je podjetje že uvedlo, in tistih, ki jih mora glede na

standard še uvesti, se običajno imenuje »analiza razkoraka« (angl. *gap analysis*), seznam vseh uporabljenih kontrol v podjetju pa je zbran v dokumentu Izjava o uporabnosti (angl. *Statement of Applicability – SOA*).

9. korak: uvedba politik in procedur za nadzor tveganj

Za vsako uporabljeno kontrolo je treba imeti ustrezno izjavo v politiki ali v določenih primerih v podrobnih procedurah. Politike in procedure so namenjene temu, da bi zaposleni razumeli svojo vlogo in odgovornost ter da bi se kontrola lahko konsistentno izvajala. Podjetje ima lahko eno varnostno politiko, ki združuje vsa področja, ali pa več politik, ki ločeno pokrivajo posamezna področja (na primer fizična varnost, politika nadzora dostopa, politika ravnanja s tajnimi podatki, politika varnostnega kopiranja, politika ravnanja z opremo IKT).

10. korak: razporeditev virov in izobraževanje zaposlenih

Za izvajanje SVIV je potrebna ustrezna razporeditev virov (osebje, čas, denar). Zaposleni, ki delujejo na področju SVIV, se morajo tudi ustrezno izobraževati, uspeh izobraževanja pa moramo nadzorovati in zagotavljati njegovo učinkovitost.

11. korak: nadzor izvajanja SVIV

Ko je SVIV vzpostavljen, je treba zagotoviti ažurnost, primernost, ustreznost in učinkovitost, zato zahteva ISO/IEC 27001 notranjo revizijo in vodstveni pregled v rednih časovnih intervalih. Pregled mora vsebovati ocenjevanje priložnosti za izboljšave in potrebne spremembe SVIV.

12. korak: priprava na certifikacijsko presojo

Če želi podjetje certificirati svoj SVIV, je treba izvesti celoten krog notranje revizije, vodstvenega pregleda in aktivnosti v procesu PDCA. Zunanji presojevalci najprej pregledajo dokumentacijo SVIV, da določijo obseg in vsebino SVIV v podjetju, nato pa presojevalec preveri potrebne zapise in dokaze, da se to, kar je navedeno v SVIV, tudi res izvaja.

5 SLOVENSKA REGULATIVA S PODROČJA INFORMACIJSKE VARNOSTI

Slovenska zakonodaja ureja področje informacijske varnosti v različnih zakonih na več področjih. V nadaljevanju povzemamo del vsebine različnih zakonov, ki opredeljujejo vidike, povezane z informacijsko varnostjo (SI-CERT, 2013; RIS, 2013).

5.1 Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ureja področje elektronskega poslovanja, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih.

ZEPEP prepoveduje diskriminacijo elektronskega podpisa in opredeljuje pogoje, pod katerimi je elektronski podpis enakovreden lastnoročnemu podpisu, o čemer še posebej govorita 14. in 15. člen.

14. člen

Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.

15. člen

Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.

ZEPEP opredeljuje elektronski podpis kot niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika. Poleg tega ZEPEP

podrobneje opredeljuje tudi varen elektronski podpis, ki mora izpolnjevati še naslednje zahteve:

- da je povezan izključno s podpisnikom;
- da je iz njega mogoče zanesljivo ugotoviti podpisnika;
- da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
- da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

Varen elektronski podpis, overjen s kvalificiranim digitalnim potrdilom, ima po ZEPEP enako dokazno vrednost kot lastnoročni podpis. Kvalificirano digitalno potrdilo je potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP in ga izda overitelj, ki deluje v skladu z zahtevami iz členov ZEPEP od št. 29 do 36.

Elektronsko poslovanje in elektronski podpis podrobneje opredeljuje podzakonski akt Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (neuradno prečiščeno besedilo št. 2, 2006). Uredba podrobneje določa:

- merila, ki se uporabljajo za presojanje izpolnjevanja zahtev za delovanje overiteljev, ki izdajajo kvalificirana potrdila;
- podrobnejšo vsebino notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila;
- podrobnejše tehnične pogoje za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov;
- časovno veljavnost kvalificiranih potrdil;
- podrobnejše pogoje glede uporabe varnih časovnih žigov;
- vrsto in uporabo označbe akreditiranih overiteljev;
- pogoje za elektronsko poslovanje v javni upravi.

5.2 Zakon o elektronskih komunikacijah (ZEKom-1)

Zakon o elektronskih komunikacijah (ZEKom-1) ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev. Področje informacijske varnosti pokriva ZEKom-1 v 7. poglavju »Varnost omrežij in storitev ter delovanje v izjemnih stanjih«. Operaterjem določa, da morajo izdelati varnostni načrt, v katerem naj predvidijo ukrepe za

zmanjševanje verjetnosti pojava varnostnega incidenta, ter definirati ukrepe za primer, če se incident zgodi. Operaterji morajo o kršitvah varnosti in celovitosti obveščati regulatorni organ (Agencijo za komunikacijska omrežja in storitve – AKOS).

Za področje informacijske varnosti so pomembni tudi podzakonski akti, izdani na podlagi ZEKom-1:

- splošni akt o varnosti omrežij in storitev,
- splošni akt o zavarovanju hranjenih podatkov,
- splošni akt o zbiranju, uporabi in dajanju podatkov o razvoju trga elektronskih komunikacij,
- pravilnik o opremi in vmesnikih za zakonito prestrezanje informacij,
- pravilnik o načinu posredovanja hranjenih podatkov o prometu telefonskih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju.

V členih od 79 do 82 ZEKom-1 opredeljuje varnost omrežij in storitev, obveščanje o kršitvah in revizijo.

79. člen

1) Operaterji morajo sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, zlasti zaradi preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, primerno predvidenemu tveganju.

2) Med ukrepe iz prvega odstavka spada tudi sprejem in izvajanje ustreznega varnostnega načrta, ki ga operater določi kot poslovno skrivnost.

3) Varnostni načrt zajema najmanj:

- *opredelitev vseh varnostnih tveganj znotraj operaterja, kakor tudi tistih zunaj operaterja, ki lahko ogrozijo delovanje javnega komunikacijskega omrežja oziroma lahko motijo delovanje javno dostopnih elektronskih komunikacijskih storitev, ki jih ta operater ponuja,*

- *opredelitev verjetnosti dogodka za vsa varnostna tveganja iz prejšnje alineje,*
- *opredelitev stopnje negativnih učinkov in posledic za delovanje javnega komunikacijskega omrežja, in za javno dostopne komunikacijske storitve za vsa varnostna tveganja iz prve alineje,*
- *opredelitev ukrepov za zmanjšanje verjetnosti za nastop varnostnega incidenta,*
- *opredelitev ukrepov za zmanjšanje negativnih učinkov in omilitev posledic varnostnega incidenta,*
- *opredelitev ustreznega načina organiziranja varnosti znotraj operaterja, katerega integralni del je varnost omrežja, informacijskega sistema in fizično varovanje objektov in naprav,*
- *opredelitev ustreznega načina zagotovitve kadrovske zasedbe na ključnih delovnih mestih pri operaterju, ki se poklicno ukvarjajo z varnostjo,*
- *opredelitev načina rednega preverjanja skladnosti izvajanih ukrepov in postopkov s tistimi, ki so opisani v varnostnem načrtu.*

80. člen

Operaterji omrežij morajo sprejeti vse potrebne ukrepe za zagotovitev celovitosti svojih omrežij, da se zagotovi neprekinjeno izvajanje storitev prek teh omrežij.

81. člen

1) *Operaterji morajo, takoj ko to zaznajo, obvestiti agencijo o vseh kršitvah varnosti ali celovitosti, če so te kršitve pomembno vplivale na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev.*
2) *Agencija o posameznih kršitvah varnosti omrežij in storitev ter o kršitvah celovitosti omrežij po potrebi in glede na stopnjo kršitve obvešča nacionalno kontaktno točko za obravnavo varnostnih incidentov (SI-CERT).*
3) *Agencija obvešča o posameznih kršitvah varnosti omrežij in storitev ter o kršitvah celovitosti omrežij po potrebi in glede na stopnjo kršitve nacionalne regulatorne organe v drugih državah članicah EU in Evropsko agencijo za varnost omrežij in informacij (ENISA).*

4) Če agencija meni, da je razkritje kršitve iz prejšnjega odstavka v javnem interesu, lahko o tem sama obvesti javnost ali pa to naloži operaterju, ki ga zadeva kršitev varnosti in celovitosti.

5) Agencija Evropski komisiji in ENISA vsako leto najpozneje do konca februarja za preteklo leto predloži kratko letno poročilo o prejetih prijavah in ukrepih, ki so bili sprejeti v skladu s prvim, drugim oziroma tretjim odstavkom tega člena.

82. člen

1) Operaterji morajo na zahtevo agencije privoliti v revizijo varnosti, ki jo na stroške operaterja izvede usposobljena neodvisna organizacija, ki rezultate te revizije, ki ohrani stopnjo zaupnosti iz drugega odstavka 79. člena tega zakona, posreduje agenciji in revidirancu.

2) Operater mora za izvedbo revizije iz prejšnjega odstavka izbrati eno izmed neodvisnih revizijskih organizacij, ki so registrirane pri Slovenskem inštitutu za revizijo, ter o izbrani revizijski organizaciji in o začetku postopka revizije varnosti obvestiti agencijo v roku 30 dni od zahteve agencije iz prejšnjega odstavka.

3) V primeru, da operater ne ravna v skladu s prejšnjim odstavkom, določi agencija neodvisno revizijsko organizacijo, ki je registrirana pri Slovenskem inštitutu za revizijo, za izvedbo revizije iz prvega odstavka tega člena. Stroške revizije poravna revidiranec.

V 83. in 84. členu ZEKom-1 opredeljuje ukrepe v primeru izjemnih stanj za zagotavljanje razpoložljivosti storitev.

83. člen

1) Operaterji morajo v primeru izjemnih stanj prednostno zagotavljati delovanje tistih delov omrežja, ki so nujni za nemoteno delovanje omrežij nosilcev varnostnega in obrambnega sistema ter sistema zaščite in reševanja. Za čim krajše izpade teh omrežij morajo operaterji po potrebi predvideti tudi nadomestne poti. S tem namenom morajo svoje ukrepe predhodno uskladiti z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja.

2) Operaterji, ki zagotavljajo javno telefonsko omrežje, morajo svoje omrežje prilagoditi tako, da omogoča dodelitev prednosti komunikacijam z določenih omrežnih priključnih točk pred komunikacijami s preostalih omrežnih priključnih točk (v nadaljnjem besedilu:

funkcija prednosti). Komunikacija, ki ji je dodeljena funkcija prednosti v javnem telefonskem omrežju določenega operaterja, to prednost ohrani tudi v javnih telefonskih omrežjih drugih operaterjev. V izjemnih stanjih lahko operaterji omogočijo delovanje omrežnih priključnih točk s prednostjo tudi tako, da omejijo ali prekinejo delovanje preostalih telefonskih priključkov.

3) Vlada z uredbo določi skupine uporabnikov, ki imajo pravico do omrežnih priključnih točk s prednostjo v skladu s prejšnjim odstavkom.

4) Vlada s sklepom določi tudi druge ukrepe in omejitve ali prekinitve delovanja, povezane z zagotavljanjem javnih komunikacijskih omrežij ali storitev ob naravnih in drugih nesrečah ali ob katastrofalnem izpadu omrežja, če je to potrebno zaradi odprave nastalih razmer.

5) Ukrepi, izdani na podlagi četrtega odstavka tega člena, morajo biti določeni v takšnem obsegu in veljavni toliko časa, kolikor je to nujno potrebno za odpravo *izjemnih stanj iz prvega odstavka tega člena.*

84. člen

1) Izvajalci javno dostopnih telefonskih storitev, ki se zagotavljajo po javnih komunikacijskih omrežjih, morajo sprejeti ustrezne tehnične in organizacijske ukrepe, ki omogočajo, da so njihove dejavnosti v primeru izjemnih stanj čim manj motene. Izvajalci javno dostopnih telefonskih storitev morajo te ukrepe izvajati ves čas trajanja okoliščin, zaradi katerih so bili sprejeti.

2) Z ukrepi iz prejšnjega odstavka mora biti zagotovljeno, da se v najkrajšem času zagotovi razpoložljivost javno dostopnih telefonskih storitev. S temi ukrepi se mora omogočiti zlasti neprekinjen dostop do in uporaba številk za klic v sili, predvsem do enotne evropske telefonske številke za klice v sili 112, številke policije 113 in do enotne evropske telefonske številke za prijavo pogrešanih otrok 116 000.

V 109. členu ZEKom-1 opredeljuje neposredno trženje z uporabo elektronskih komunikacij, ki je pomembno na področju neželene elektronske pošte.

109. člen

1) *Uporaba samodejnih klicnih sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja (klicni avtomati), faksimilnih naprav ali elektronske pošte1 za namene neposrednega trženja je dovoljena samo na podlagi naročnikovega predhodnega soglasja.*

2) *Ne glede na določbe prejšnjega odstavka lahko fizična ali pravna oseba, ki od kupca svojih izdelkov ali storitev pridobi njegov elektronski naslov za elektronsko pošto, ta naslov uporablja za neposredno trženje svojih podobnih izdelkov ali storitev, vendar mora kupcu dati možnost, da kadarkoli na brezplačen in enostaven način zavrne takšno uporabo njegovega elektronskega naslova.*

3) *Uporaba drugačnih sredstev za neposredno trženje s pomočjo elektronskih komunikacij kot so določena v prejšnjih dveh odstavkih tega člena, je dovoljena le s soglasjem naročnika.*

4) *Elektronske pošte za potrebe neposrednega trženja s skrito ali prikrito identiteto pošiljatelja, v imenu katerega se sporočilo pošilja, ali brez veljavnega naslova, na katerega lahko prejemnik pošlje zahtevo za prekinitev takega neposrednega trženja, ni dovoljeno pošiljati.*

5.3 Zakon o elektronskem poslovanju na trgu (ZEPT)

Zakon o elektronskem poslovanju na trgu (ZEPT) določa način in obseg elektronskega poslovanja na trgu. S stališča informacijske varnosti je pomemben, ker opredeljuje odgovornost ponudnika storitve za podatke, ki so dostopni prek omrežja.

V členih 6, 8, 9, 10 in 11 ZEPT opredeljuje obveznosti in odgovornosti ponudnikov storitev za pošiljanje komercialnih sporočil, za prenos podatkov v komunikacijskem omrežju in za shranjevanje podatkov.

6. člen

1) *Ponudnik storitev lahko pošilja komercialna sporočila, ki so del storitev informacijske družbe, če:*

   - *prejemnik storitve vnaprej soglaša s pošiljanjem,*

- *je komercialno sporočilo kot tako jasno razpoznavno,*
- *je nedvoumno navedena fizična ali pravna oseba, v imenu katere je komercialno sporočilo poslano,*
- *so jasno in nedvoumno navedeni pogoji za sprejem posebnih ponudb, ki so povezane s popusti, premijami in darili, ki morajo biti kot taki nedvoumno označeni, in*
- *so jasno in nedvoumno ter lahko dostopno navedeni pogoji za sodelovanje v nagradnih tekmovanjih ali igrah na srečo, ki morajo biti kot taki jasno razpoznavni.*

2) *Poleg pogojev iz prejšnjega odstavka mora ponudnik storitev z reguliranim poklicem pri pošiljanju komercialnih sporočil kot dela storitve informacijske družbe, ki jo opravlja, upoštevati tudi morebitna posebna pravila reguliranega poklica v zvezi z neodvisnostjo, dostojanstvom in častjo poklica, poklicno skrivnostjo ter poštenostjo do strank in sodelavcev.*

8. člen

1) *Ponudnik storitev odgovarja za podatke, ki jih zagotovi prejemnik njegove storitve, po določbah tega zakona.*
2) *Ponudnik storitev odgovarja za podatke, ki jih za opravljanje storitve informacijske družbe zagotovi sam, po splošnih pravilih obligacijskega in kazenskega prava.*
3) *Ponudnik storitev ni dolžan nadzirati ali hraniti podatkov, ki jih pošilja ali hrani, ali dejavno raziskovati okoliščin, nakazujočih na protipravnost podatkov, ki jih zagotavlja prejemnik storitve.*
4) *Ponudniki storitev morajo vsem pristojnim organom na njihovo zahtevo najkasneje v roku treh dni od njenega prejema sporočiti podatke, na podlagi katerih je mogoče identificirati prejemnike njihove storitve (ime in priimek, naslov, firma, elektronski naslov). Navedene podatke morajo ponudniki storitev sporočiti zaradi odkrivanja in preprečevanja kaznivih dejanj na podlagi odredbe sodišča, brez odredbe sodišča pa, če tako določa področni zakon.*

9. člen

1) *Kadar se storitev informacijske družbe nanaša na prenos podatkov v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve, ali zagotovitev dostopa do komunikacijskega omrežja prejemniku storitve, ponudnik storitev ni odgovoren za poslane podatke, če:*

- *ne sproži prenosa podatkov,*
- *ne izbere naslovnika in*
- *podatkov, ki jih prenaša, ne izbere ali spremeni.*

2) *Prenos in zagotovitev dostopa iz prejšnjega odstavka vključujeta samodejno, vmesno in prehodno shranjevanje poslanih podatkov, če je namenjeno samo izvajanju prenosa v komunikacijskem omrežju in če se podatki ne shranijo za daljši čas, kolikor je za njihov prenos upravičeno potrebno.*

3) *Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prvega odstavka tega člena, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.*

10. člen

1) *Kadar se storitev informacijske družbe nanaša na prenos podatkov v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve, ponudnik storitev ni odgovoren za samodejno, vmesno in prehodno shranjevanje teh podatkov, če je namenjeno izključno učinkovitejšemu posredovanju podatka drugim prejemnikom storitve na njihovo zahtevo, pod pogojem, da ponudnik storitev:*
   - *podatkov ne spremeni,*
   - *ravna v skladu s pogoji za dostop do podatkov,*
   - *ravna v skladu s pogoji o sprotnem dopolnjevanju podatkov, ki so določeni v splošno priznanih in uporabljenih industrijskih standardih,*
   - *ne posega v zakonito uporabo tehnologij za pridobivanje informacij o rabi podatkov, ki so določene v splošno priznanih in uporabljenih industrijskih standardih in*
   - *brez odlašanja odstrani ali onemogoči dostop do podatka, ki ga hrani, takoj ko je obveščen, da je bil vir podatka odstranjen iz omrežja ali da je bil dostop do njega onemogočen ali da je sodišče ali upravni organ odredil njegovo odstranitev ali omejitev.*

2) Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prejšnjega odstavka, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

11. člen

1) Kadar se storitev informacijske družbe nanaša na shranjevanje podatkov, ki jih zagotovi prejemnik storitve, ponudnik storitev ni odgovoren za podatke, ki jih je shranil na zahtevo prejemnika storitve, ki ne deluje v okviru njegovih pooblastil ali pod njegovim nadzorom, pod pogojem, da ponudnik storitev:

- *ne ve za protipravno dejavnost ali podatek in mu v zvezi z odškodninsko odgovornostjo niso znana dejstva ali okoliščine, iz katerih izhaja protipravnost, ali*
- *nemudoma, ko mu je protipravnost znana, ukrepa tako, da podatke odstrani ali onemogoči dostop do njih.*

2) Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prejšnjega odstavka, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

5.4 Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A)

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A) ureja način, organizacijo, infrastrukturo in izvedbo zajema ter hrambe dokumentarnega gradiva v fizični in elektronski obliki, veljavnost oziroma dokazno vrednost takega gradiva, varstvo arhivskega gradiva in pogoje za njegovo uporabo. Pomembna podrejena predpisa sta Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAG) in Enotne tehnološke zahteve (ETZ). UVDAG

ureja delovanje in notranja pravila oseb, ki hranijo dokumentarno oziroma arhivsko gradivo, hrambo tega gradiva v fizični in digitalni obliki, splošne pogoje, registracijo in certifikacijo opreme in storitev za digitalno hrambo, odbiranje in izročanje arhivskega gradiva javnim arhivom, strokovno obdelavo in vodenje evidenc arhivskega gradiva, varstvo filmskega in zasebnega arhivskega gradiva, uporabo arhivskega gradiva v arhivih ter delo arhivske komisije. ETZ pa določajo zahteve za Notranja pravila organizacij ter pogoje za ponudnike programske opreme in izvajanja storitev elektronske hrambe dokumentarnega ter arhivskega gradiva.

V 5. in 6. členu ZVDAGA opredeljuje načelo celovitosti in dostopnosti dokumentarnega gradiva.

5. člen

Hramba dokumentarnega gradiva mora zagotavljati nespremenljivost in integralnost dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenost dokumentarnega gradiva oziroma njegove vsebine ter dokazljivost izvora dokumentarnega gradiva (provenience).

6. člen

Dokumentarno gradivo oziroma reprodukcija njegove vsebine mora biti ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom ali uporabnicam (v nadaljnjem besedilu: uporabnikom).

V 23. členu ZVDAGA opredeljuje pogoje za varno hrambo dokumentarnega gradiva.

23. člen

1) Dokumentarno gradivo se hrani v ustreznih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi ter zagotavlja dostopnost, kar pomeni varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe, in celovitost, kar obsega nespremenljivost in neokrnjenost ter urejenost tega gradiva.

V 31. in 33. členu ZVDAGA opredeljuje pravno veljavnost elektronskega gradiva glede na opravljanje storitve skladno z notranjimi pravili, ki jih potrdi državni arhiv.

31. člen

Na podlagi zakona se vsaka enota varno hranjenega gradiva v digitalni obliki šteje za enako posamezni enoti izvirnega gradiva, če sta bila zajem in varna hramba opravljena v skladu s tem zakonom, njegovimi podzakonskimi predpisi, pri državnem arhivu potrjenimi notranjimi pravili ter če drug zakon ne določa drugače.

33. člen

1) *Če oseba, ki hrani gradivo, hrambe nima urejene z notranjimi pravili, se enota hranjenega gradiva v digitalni obliki šteje za enako posamezni enoti izvirnega gradiva, če izpolnjuje pogoje varne hrambe v enaki meri kot enota izvirnega gradiva.*
2) *Prejšnji odstavek se uporablja tudi:*
   - *v primeru hrambe v skladu z od nadzornega organa potrjenimi notranjimi pravili, če gre za primer, ki ga pravila ne urejajo;*
   - *v primeru, da oseba, ki hrani gradivo, ima notranja pravila, vendar v konkretnem primeru hrambe teh pravil ni spoštovala.*

V 72. členu ZVDAGA opredeljuje pogoje za storitev hrambe dokumentarnega gradiva s strani ponudnikov.

72. člen

1) *Ponudniki storitev zajema in hrambe dokumentarnega gradiva v digitalni obliki ter ponudniki spremljevalnih storitev morajo za varstvo arhivskega gradiva v digitalni obliki uporabljati samo pri državnem arhivu v skladu s 85. členom tega zakona certificirano opremo in storitve.*

5.5 Zakon o tajnih podatkih (ZTP)

Zakon o tajnih podatkih (ZTP) določa osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov. Z vidika informacijske varnosti so pomembni tudi podzakonski akti, izdani na podlagi ZTP:

- Uredba o varovanju tajnih podatkov,
- Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih,
- Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov.

V 13. členu ZTP opredeljuje stopnje tajnosti.

13. člen

Tajni podatki iz 5. člena tega zakona imajo glede na možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, ki utegnejo nastati, če bi bili razkriti nepoklicani osebi, eno od naslednjih stopenj tajnosti:

1. *STROGO TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo.*
2. *TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije.*
3. *ZAUPNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije.*
4. *INTERNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa.*

V organih se smejo za določanje stopenj tajnosti podatkov uporabljati samo stopnje, določene v prejšnjem odstavku.

V 31., 38. in 39. členu ZTP opredeljuje dostop do tajnih podatkov in njihovo varovanje.

31. člen

Pravico dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov stopnje tajnosti, določene v dovoljenju.

Nihče ne sme dobiti tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog ali funkcije.

38. člen

V vsakem organu in organizaciji se mora v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi, vzpostaviti sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza določeni stopnji tajnosti in onemogoča njihovo razkritje nepoklicanim osebam.

Postopki in ukrepi iz prejšnjega odstavka morajo obsegati:

- *splošne varnostne ukrepe;*
- *varovanje oseb, ki imajo dostop do tajnih podatkov;*
- *varovanje prostorov;*
- *varovanje dokumentov in medijev, ki vsebujejo tajne podatke;*
- *varovanje komunikacij, po katerih se prenašajo tajni podatki;*
- *način označevanja stopenj tajnosti;*
- *varovanje opreme, s katero se obravnavajo tajni podatki;*
- *način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov;*
- *kontrolo in evidentiranje dostopov do tajnih podatkov;*
- *kontrolo in evidentiranje pošiljanja in distribucije tajnih podatkov.*

Predstojnik organa in organizacije je dolžan enkrat letno zagotoviti dodatno usposabljanje oseb, ki opravljajo naloge na področju obravnavanja in varovanja tajnih podatkov stopnje tajnosti ZAUPNO in višje.

Predstojnik organa in organizacije mora izdati akt, s katerim zagotovi izvajanje ukrepov in postopkov iz prvega in drugega odstavka tega člena.

Akt iz prejšnjega odstavka predpiše za sodišča s splošno pristojnostjo in specializirana sodišča predsednik Vrhovnega sodišča Republike Slovenije, za državna tožilstva pa generalni državni tožilec Republike Slovenije.

Vlada podrobneje predpiše program in način usposabljanja oseb iz tretjega odstavka tega člena.

39. člen

Tajne podatke se mora v organih hraniti na način, ki zagotavlja, da imajo dostop do teh podatkov samo osebe, ki imajo dovoljenje za dostop do tajnih podatkov, in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.

Tajni podatki se lahko pošljejo izven prostorov organa samo ob upoštevanju predpisanih varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme oseba, ki ima dovoljenje za dostop do tajnih podatkov in je do teh podatkov upravičena.

Postopki in ukrepi varovanja pošiljanja tajnih podatkov izven prostorov organa se predpišejo glede na stopnjo tajnosti teh podatkov.

Organi tajnih podatkov ne smejo prenašati ali posredovati po nezaščitenih komunikacijskih sredstvih.

Vlada podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov.

5.6 Zakon o varstvu potrošnikov (ZVPot)

Določila Zakona o varstvu potrošnikov se uporabljajo le za razmerja med podjetji in potrošniki (fizičnimi osebami). V 45.a členu ZVPot opredeljuje pravila neposrednega trženja prek elektronskih poti. Bistvena zahteva za pošiljanje komercialnih sporočil je soglasje prejemnika, kar je enako kot pri ZEPT, le da se ZEPT uporablja tudi za razmerja med samimi podjetji (podjetje – podjetje), ZVPot pa za razmerja med potrošniki in podjetji (potrošnik – podjetje).

45.a. člen

1) *Podjetje lahko uporablja sistem klicev brez posredovanja človeka, faksimile napravo, elektronsko pošto in drugo obliko elektronskega komuniciranja samo z vnaprejšnjim soglasjem posameznega potrošnika, ki mu je sporočilo namenjeno.*

4) *Če potrošnik pri kateremkoli stiku, vzpostavljenem s sredstvom za komunikacijo, ki omogoča osebna sporočila, izjavi, da ne želi več prejemati sporočil na takšen način, mu podjetje ne sme več pošiljati nobenih sporočil, ki so namenjena sklenitvi pogodbe za dobavo kateregakoli blaga ali katerekoli storitve.*

5.7 Zakon o varstvu osebnih podatkov (ZVOP-1)

Zakon o varstvu osebnih podatkov (ZVOP-1) določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi

osebnih podatkov. ZVOP-1 opredeljuje osebni podatek kot kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če jo lahko neposredno ali posredno identificiramo, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

V 14. in 24. členu ZVOP-1 opredeljuje varovanje osebnih podatkov.

14. člen

1) *Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru iz 5. točke 13. člena tega zakona.*

2) *Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.*

24. člen

1) *Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:*

   - *varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;*
   - *varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;*
   - *preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;*
   - *zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;*

- *omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.*

2) *V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.*

3) *Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.*

4) *Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.*

V 72. in 73. členu ZVOP-1 opredeljuje pravice in dolžnosti posameznika in upravljavca osebnih podatkov pri neposrednem trženju z uporabo elektronskih komunikacij.

72. člen

1) *Upravljavec osebnih podatkov lahko uporablja osebne podatke posameznikov, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti, tudi za namene ponujanja blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih sredstev (v nadaljnjem besedilu: neposredno trženje) v skladu z določbami tega poglavja, če drug zakon ne določa drugače.*

2) *Za namene neposrednega trženja lahko upravljavec osebnih podatkov uporablja le naslednje osebne podatke, ki jih je zbral v skladu s prejšnjim odstavkom: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa. Na podlagi osebne privolitve posamez-*

nika lahko upravljavec osebnih podatkov obdeluje tudi druge osebne podatke, občutljive osebne podatke pa le, če ima za to osebno privolitev posameznika, ki je izrecna in praviloma pisna.

3) *Upravljavec osebnih podatkov mora neposredno trženje izvajati tako, da posameznika ob izvajanju neposrednega trženja obvesti o njegovih pravicah iz 73. člena tega zakona.*

4) *Če namerava upravljavec osebnih podatkov posredovati osebne podatke iz drugega odstavka tega člena drugim uporabnikom osebnih podatkov za namene neposrednega trženja ali pogodbenim obdelovalcem, je dolžan o tem obvestiti posameznika in pred posredovanjem osebnih podatkov pridobiti njegovo pisno privolitev. Obvestilo posamezniku o nameravanem posredovanju osebnih podatkov mora vsebovati informacijo, katere podatke namerava posredovati, komu in za kakšen namen. Stroške obvestila krije upravljavec osebnih podatkov.*

73. člen

1) *Posameznik lahko kadarkoli pisno ali na drug dogovorjen način zahteva, da upravljavec osebnih podatkov trajno ali začasno preneha uporabljati njegove osebne podatke za namen neposrednega trženja. Upravljavec osebnih podatkov je dolžan v 15 dneh ustrezno preprečiti uporabo osebnih podatkov za namen neposrednega trženja ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.*

2) *Stroške vseh dejanj upravljavca osebnih podatkov v zvezi z zahtevo iz prejšnjega odstavka krije upravljavec.*

5.8 Kazenski zakonik RS (KZ-1)

Kazenski zakonik opredeljuje tudi kazniva dejanja, povezana z informacijsko varnostjo, predvsem vdor v informacijski sistem in nepooblaščeno spreminjanje podatkov.

V 143. členu KZ-1 opredeljuje zlorabo osebnih podatkov.

143. člen

1) *Kdor brez podlage v zakonu ali v osebni privolitvi posameznika, na katerega se osebni podatki nanašajo, osebne podatke, ki se obdelu-*

jejo na podlagi zakona ali osebne privolitve posameznika, posreduje v javno objavo ali jih javno objavi, se kaznuje z denarno kaznijo ali zaporom do enega leta.

2) *Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.*

3) *Kdor na svetovnem medmrežju ali drugače javno objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.*

4) *Kdor prevzame identiteto druge osebe ali z obdelavo njenih osebnih podatkov izkorišča njene pravice, si na njen račun pridobiva premoženjsko ali nepremoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.*

5) *Kdor stori dejanje iz prvega odstavka tega člena tako, da posreduje v javno objavo ali javno objavi občutljive osebne podatke, se kaznuje z zaporom do dveh let.*

6) *Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.*

7) *Pregon iz četrtega odstavka tega člena se začne na predlog.*

V 221. in 237. členu KZ-1 opredeljuje napad na informacijski sistem.

221. člen

1) *Kdor neupravičeno vstopi ali vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.*

2) *Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.*

3) *Poskus dejanja iz prejšnjega odstavka je kazniv.*

4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

237. člen

1) Kdor pri gospodarskem poslovanju neupravičeno vstopi ali vdre v informacijski sistem ali ga neupravičeno uporablja tako, da uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema ali neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.

2) Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je storilec hotel sebi ali komu drugemu pridobiti tako premoženjsko korist ali drugemu povzročiti tako premoženjsko škodo, se kaznuje z zaporom do petih let.

V 306. členu KZ-1 opredeljuje izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje.

306. člen

1) Kdor orožje, razstrelilne snovi ali pripomočke, s katerimi se lahko napravijo, ali strupe, za katere ve, da so namenjeni za kaznivo dejanje, izdela ali si jih pridobi ali jih hrani ali komu omogoči, da pride do njih, se kaznuje z zaporom do treh let.

2) Kdor napravi ali komu odstopi ponarejen ključ, odpirač ali kakšen drug pripomoček za vlom, čeprav ve, da je namenjen za kaznivo dejanje, se kaznuje z zaporom do enega leta.

3) Enako kot v prejšnjem odstavku se kaznuje, kdor z namenom storitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem.

ZAKLJUČEK IN NAPOTKI

Informacijska varnost je področje, za katero se zanimanje hitro povečuje. Podjetja se čedalje bolj zavedajo, da je varnost eden izmed osnovnih elementov vsakega informacijskega sistema. Pri tem se zastavljata ključni vprašanji, kako varen je informacijski sistem in kako varen bi moral biti informacijski sistem. Zavedati se moramo, da popolnoma varen sistem ne obstaja. Podjetje mora izbrati takšno stopnjo varnosti, ki je zanj sprejemljiva in po nekaterih kazalcih optimalna. Določitev ustrezne stopnje varnosti in optimalnih vlaganj za dosego te stopnje pa je zahtevna naloga, ki se izvaja skozi proces obvladovanja varnostnih tveganj.

Proces obvladovanja tveganja pomaga podjetjem sprejeti odločitev glede potrebnih investicij v varnostne ukrepe, ki so za poslovanje podjetja najučinkovitejši. Cilj procesa je identifikacija in merjenje tveganja z namenom informiranja procesa odločanja, ki omogoča izbiro stroškovno učinkovite zaščite. To je zaščita, ki ne stane več, kot je pričakovana izguba ob napadu. Osnovna strategija obvladovanja tveganja je zmanjšanje izpostavljenosti sredstva tveganju z uvedbo ustreznih tehnologij, orodij ali postopkov. S tem se zmanjša verjetnost za škodljive dogodke ali omeji škoda, ki jo lahko povzroči dogodek. Vlaganja v rešitve, povezane z informacijsko varnostjo, so torej neizogibna za vsa podjetja, ki so tako ali drugače vključena v proces elektronskega poslovanja. S stališča podjetja je varnost investicija, ki se meri v prihrankih denarnih enot.

Osebe, ki so v podjetjih odgovorne za investicije, seveda najbolj zanima, kam vlagati in predvsem koliko. Preden se investira v določen izdelek ali storitev, je dobro vedeti, ali je investicija finančno upravičena. Informacijska varnost pri tem ni nobena izjema. V predstavljeni študiji smo spoznali, da problematike informacijske varnosti ne moremo učinkovito rešiti le s tehničnim pogledom na problem in tehnološkimi rešitvami, temveč je treba na informacijsko varnost gledati kot na proces, v katerem se upoštevajo ekonomska načela. Zavedati se moramo, da je ekonomski pristop ocenjevanja optimalnih vlaganj v informacijsko varnost obsežen in zamuden projekt, saj zahteva poglobljeno analizo in vrednotenje informacijskih sredstev in z njimi povezanih groženj, posledic nedelovanja informacijske tehnologije, verjetnosti uspešno izvedenega napada,

učinkovitosti izvajanja varnostne prakse ter oceno stroškov in pridobitev, ki so posledica vlaganj v informacijsko varnost.

Sklenemo lahko, da ocena optimalnega obsega vlaganj v informacijsko varnost in izbira ustrezne varnostne zaščite zahtevata, da podjetja potrebo po informacijski varnosti kvantitativno ovrednotijo. Kvantitativno je treba ovrednotiti ranljivosti in grožnje, ki so povezane z nekim informacijskim sredstvom, ter ukrepe, ki ta tveganja zmanjšajo. To dokazujemo z rezultati preverjanja veljavnosti treh hipotez.

> **Hipoteza 1** – Z uporabo standardiziranega modela ocene vlaganj je mogoče določiti optimalni varnostni ukrep za zmanjšanje informacijsko-varnostnih tveganj.

S preverjanjem **hipoteze 1** smo želeli ugotoviti, ali lahko obstaja neki standardni postopek, s katerim lahko ovrednotimo tveganja in kvantitativno primerjamo različne varnostne ukrepe za zmanjšanje tveganja. Za preverjanje hipoteze 1 smo uporabili kvantitativni matematični model za vrednotenje vlaganj v informacijsko varnost glede na ocene tveganja in verjetnosti, da se bo varnostni incident zgodil (Bojanc, 2010). Model omogoča kvantitativno vrednotenje sredstev, groženj, ranljivosti, tveganj in ukrepov za zmanjšanje tveganja. Izbrani model je osredotočen na izbiro optimalnega ukrepa za določeno tveganje.

Ker se problematika informacijske varnosti ne more učinkovito reševati zgolj s tehničnimi rešitvami, je ključno, da postopek vrednotenja omogoča izbiro različnih vrst rešitev. Da v poslovnem okolju organizacije dejansko uporabljajo kombinacijo različnih vrst ukrepov, so pokazale tudi različne raziskave (CSI, 2011; DSCI, 2009; BERR, 2008). Težava nastopi, ko želimo različne ukrepe spraviti na skupni imenovalec, ki omogoča medsebojno primerjanje različnih vrst rešitev. Prednost predstavljenega postopka izbire je ravno v tem, da je dovolj splošen, da omogoča standardno vrednotenje poljubnega varnostnega ukrepa in da ni omejen le na določene vrste ukrepov. To omogoča, da z izbranim modelom lahko kvantitativno vrednotimo različne možnosti investiranja v informacijsko varnost, od tehničnih ukrepov do organizacijsko-procesnih ukrepov, zunanjega izvajanja, izobraževanj zaposlenih, zavarovanja itd.

Postopek izbire stroškovno optimalnega ukrepa smo v nadaljevanju preverili tudi na empirični ravni za konkretno podjetje, pri čemer smo pri izbiri možnih ukrepov izbrali tako preventivne, korektivne kot organizacijske varnostne rešitve ter jih uspešno kvantitativno primerjali med seboj. Obenem smo naredili pregled različnih metod in standardov za vrednotenje in izbiro varnostnih rešitev. S predstavljenim postopkom izbire stroškovno optimalne varnostne rešitve za zmanjšanje varnostnih tveganj, ki sloni na kvantitativnem modelu, ter s prikazom praktičnega primera uporabe izbranega postopka v poslovnem okolju ocenjujemo, da je hipoteza 1 potrjena.

> **Hipoteza 2** – Za določitev stroškovno optimalnega varnostnega ukrepa za določeno grožnjo je treba upoštevati in primerjati različne kazalce za merjenje donosnosti vlaganj.

S preverjanjem **hipoteze 2** smo želeli ugotoviti, ali se lahko stroškovno optimalen varnostni ukrep določi zgolj na podlagi vrednosti enega kazalca za merjenje donosnosti vlaganj ali pa je treba za izbiro ustreznega ukrepa donosnost vlaganja meriti z več različnimi kazalci in jih primerjati med seboj. Za preverjanje hipoteze 2 smo donosnost investicije merili s kazalci donosnost investicije (ROI), neto sedanje vrednosti (NPV) in notranje stopnje donosa (IRR).

Izračun kazalca ROI je preprost in ga lahko uporabimo tako za oceno, ali je investicija finančno upravičena, kot tudi za primerjavo investicijske vrednosti več različnih varnostnih rešitev. Po drugi strani pa ROI zgolj pove, kakšna je donosnost investicije v odstotkih za določeno časovno obdobje. Ker je rezultat v odstotkih, to nič ne pove o dejanski višini donosa, poleg tega ROI ne upošteva časovne komponente. NPV upošteva spremembo vrednosti denarja v času z uporabo diskontne stopnje, pri tem pa vse prihodnje stroške in koristi prevede na sedanjo vrednost. Rezultat je prikazan v denarnih enotah, pri čemer pozitiven NPV pomeni, da je investicija finančno upravičena. Kazalec IRR določa diskontno stopnjo, pri kateri je NPV enak nič.

Skupna težava teh kvantitativnih kazalcev je, da lahko zaradi številske vrednosti dobimo lažen vtis, da je izračun natančen. Zavedati se moramo, da je rezultat

kljub številski vrednosti zgolj ocena, pri kateri je natančnost odvisna od točnosti vhodnih podatkov.

Ker na donosnost investicije vsak izmed teh kazalcev gleda s svoje perspektive, lahko pričakujemo določene razlike pri uporabi posameznega kazalca kot podatek, ki naj pomaga pri odločanju. Če merimo zgolj to, ali je neka rešitev donosna ali ne, lahko pričakujemo, da bodo vsi trije kazalci dali pozitiven ali vsi trije negativen rezultat. Do razlik pa lahko pride pri primerjavi izračunov kazalcev za več različnih investicij, še zlasti se to rado zgodi pri dolgoročnih investicijah. Opravljena empirična raziskava je to potrdila, saj so za primer grožnje z računalniškim virusom posamezni kazalci različno razvrstili določene rešitve med seboj.

Obstoječe teoretične raziskave, opravljene empirične raziskave in preverjena uporaba matematičnega modela potrjujejo, da je kazalce ROI, NPV in IRR pri odločitvi o izbiri optimalnega varnostnega ukrepa dobro kombinirati in primerjati med seboj, kar potrjuje hipotezo 2.

> **Hipoteza 3 –** Čeprav uvedbe varnostnih ukrepov podjetju ne prinašajo neposredne finančne koristi, je za odločanje o investicijah v varnostne rešitve mogoče učinkovito uporabiti ekonometrične metode za analizo stroškov in koristi.

S preverjanjem **hipoteze 3** smo želeli ugotoviti, kako učinkovita je analiza stroškov in koristi na področju obravnave informacijskih varnostnih tveganj in izbire ustreznih ukrepov. Za preverjanje hipoteze 3 smo podrobneje preučili, kako lahko pri posamezni investiciji v varnostno rešitev opredelimo koristi, ki jih ima podjetje zaradi investicije, ter tudi same stroške investicije.

V splošnem velja, da je uvedba rešitve smiselna, če so koristi investicije večje od stroškov investicije. Z ekonomskega stališča je optimalna investicija v varnost takrat, ko je razlika med koristmi in stroški največja.

V raziskavi ugotavljamo, da je ocena stroškov investicije dokaj preprosta, saj jo dobimo, če seštejemo vse stroške, ki so povezani z nakupom, testiranjem, uvedbo, vzdrževanjem, izobraževanjem uporabnikov in skrbnikov, nadzorom

itd. Seštevanje navedenih elementov običajno ni zahtevno, saj so ti podatki bolj ali manj že v denarnih enotah.

Precej težje pa je opredeliti, oceniti ali meriti koristi zaradi same investicije v varnostni ukrep (Soo Hoo, 2000). Kot smo spoznali, varnostne rešitve same po sebi ne prinašajo finančnih koristi, ki jih je mogoče izmeriti, zato je treba koristi investicije v varnostni ukrep meriti posredno. Koristi investicije v informacijsko varnost so lahko različne, od zmanjšanja verjetnosti ponovitve incidenta, povečanja produktivnosti drugih investicij informacijske varnosti do zmanjševanja izgub, če pride do incidenta (Gordon & Loeb, 2005, str. 74).

Najpogosteje se za oceno koristi uporablja ocena možne izgube, ki se ji z investicijo izognemo. Ta prihranek stroškov zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta pa je običajno zelo težko točno oceniti (Gordon & Loeb, 2005, str. 21). Največja težava je, ker gre za ocenjevanje prihrankov stroškov, povezanih z nekimi potencialnimi varnostnimi incidenti, ki se še niso zgodili. Poleg tega je dejanske koristi težje opaziti, če je informacijska varnost v podjetju učinkovita in uspešna.

Ker je uporaba analize stroškov in koristi kompleksna in zahtevna, jo podjetja na področju informacijske varnosti v praksi ne uporabljajo pogosto (Gordon & Loeb, 2005). Priporočila, ki jih monografija podaja, temeljijo na ekonomskem principu analize stroškov in koristi. V raziskavi pa smo pokazali, da je uporaba analize stroškov in koristi ne samo mogoča, temveč tudi potrebna, če želi podjetje izračunati donosnosti investicij v informacijsko varnost. Uporabo analize stroškov in koristi na področju investicij v informacijsko varnost smo predstavili najprej na teoretični ravni v predstavljenem postopku za izbiro optimalne investicije, nato pa še na primeru praktične uporabe v podjetju. S tem smatramo hipotezo 3 za potrjeno.

Namen raziskave je tudi prikazati pomen razmeroma novega raziskovalnega področja ekonomika informacijske varnosti za varno e-poslovanje med podjetji in organizacijami. Ugotavljamo, da je ekonomska obravnava investicij v informacijsko varnost prispevala nekaj pomembnih znanstvenih rezultatov.

Prvič, vlaganja v informacijsko varnost lahko na ta način presojamo z vidika njihove ekonomske upravičenosti. Pri procesu ekonomskega vrednotenja vlaganj v informacijsko varnost je treba kvantitativno ovrednotiti tako ranljivosti in grožnje, ki so povezane z nekim informacijskim sredstvom, kot tudi ukrepe, ki ta tveganja zmanjšujejo. Pri investiciji v varnostno rešitev je treba primerjati koristi, ki jih ima podjetje zaradi investicije, ter same stroške investicije. Če so koristi investicije večje od stroškov investicije, je uvedba rešitve smiselna. Seveda nima nobenega smisla uvesti neko rešitev, za katero porabimo več, kot je največja možna izguba. Za presojo ekonomske upravičenosti posamezne investicije se običajno uporabijo kazalci ROI, NPV ali IRR.

Drugič, s pomočjo ekonomskega pristopa se lahko oceni, katera izmed rešitev, ki jih ima podjetje na voljo, ima najboljše razmerje med ceno in kakovostjo. Ekonomska obravnava investicij namreč omogoča neposredno medsebojno primerjavo posameznih ukrepov in izbiro optimalne investicije. Za vsakega izmed ukrepov se primerjajo koristi njegove uvedbe in stroški, povezani z uvedbo. Z ekonomskega stališča je optimalna investicija v varnost tista, pri kateri je razlika med koristmi in stroški največja. Za to vrednotenje se uporabijo kazalci ROI, NPV ali IRR, ki omogočajo primerjavo posameznih ukrepov med seboj. Vsak od teh kazalcev osvetli optimalnost izbire z drugega zornega kota in pomaga, da je odločitev res optimalna.

V monografiji smo poleg tega predstavili model za ekonomsko vrednotenje investicij v varnostne ukrepe, ki omogoča neposredno primerjavo različnih vrst varnostnih ukrepov od tehnoloških varnostnih rešitev, uvedbe organizacijskih postopkov, izobraževanja ali prenosa tveganja na zunanje podjetje.

Tretjič, ekonomska obravnava informacijske varnosti omogoča poiskati optimalno stopnjo varnosti določenega sistema. Varnostne rešitve je v določenem okolju smiselno uvajati do točke, kjer se mejni stroški uvedbe ukrepa izenačijo s prihrankom ob varnostnem incidentu. Optimalna stopnja uvedbe varnostnih ukrepov pa je dosežena v točki, kjer je razlika med koristmi in stroški največja. Uvedba dodatnih varnostnih ukrepov prek te točke pomeni, da so mejni stroški uvedbe dodatnega ukrepa večji od mejnih koristi, ki jih pridobimo s tem dodatnim ukrepom.

Na koncu naj še opozorimo, da kvantitativni pristop k reševanju investicij v informacijsko varnost sicer omogoča ekonomsko vrednotenje rešitev, zavedati pa se moramo tudi omejitev tega pristopa. Rezultati kvantitativnega vrednotenja so namreč zelo odvisni od natančnosti in verodostojnosti vhodnih podatkov. Za določene grožnje trenutno primanjkuje dobrih zgodovinskih podatkov, na podlagi katerih se lahko vhodni podatki natančno določijo z verjetnostnimi parametri. Pričakujemo pa lahko, da bo v prihodnje na voljo vse več statističnih podatkov, kar bo pozitivno vplivalo na uporabo kvantitativnih pristopov.

LITERATURA IN VIRI

Akerlof, G. (1970). The Market for 'Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), 488–500.

Alberts, C., & Dorofee, A. (2001, 30. januar). An introduction to the OCTAVE method. *Computer Emergency Response Team (CERT)*. Najdeno 9. septembra 2006 na spletnem naslovu http://www.cert.org/octave/methodintro.html

Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Boston: Addison-Wesley.

Anderson, A. (1991). Comparing risk analysis methodologies. The *Seventh International Conference on Information Security, IFIP/Sec '91* (str. 301–311). Maryland Heights: Elsevier.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science, 314*(5799), 610–613.

Anderson, R., & Moore, T. (2008). Information Security Economics – and Beyond. *Deontic Logic in Computer Science, 5076,* 49–72. Najdeno 21. maja 2009 na spletnem naslovu http://www.cl.cam.ac.uk/~rja14/Papers/econ_ crypto.pdf

Anderson, R., & Schneier, B. (2005). Economics of Information Security. *IEEE Security and Privacy, 3*(1), 12–13.

Anderson, R. (1993). Why cryptosystems fail. *The 1st ACM conference on Computer and communications security* (str. 215–227). Fairfax: ACM.

Anderson, R. (2001). Why information security is hard: An economic perspective. *The 17th Annual Computer Security Applications Conference (ACSAC '01)*, 358. Los Alamitos: IEEE Computer Society.

Anderson, R. (2005). Open and Closed Systems are Equivalent. *MIT Press 2005*, 127–142.

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). New York: John Wiley and Sons.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). Measuring the Cost of Cybercrime. *The 11th Workshop on the Economics of Information Security (WEIS 2012)*. Berlin: Germany.

Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2007). Security economics and the internal market. *Report to the European Network and Information Security Agency (ENISA)*.

Andrijcic, E., & Horowitz, B. (2004). A Macro-Economic Framework or Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Workshop on the Economics of Information Security (WEIS 2004)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207

Arora, A., Krishnan, R., Nandkumar, A., Telang, R., & Yang, Y. (2004a). Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis. *Workshop on the Economics of Information Security (WEIS 2004)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207

Arora, A., & Telang, R. (2005). Economics of Software Vulnerability Disclosure. *IEEE Security and Privacy, 3*(1), 20–25.

Arora, A., Telang, R., & Xu, H. (2004b). Optimal policy for software vulnerability disclosure. *Workshop on the Economics of Information Security (WEIS 2004)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207

August, T., & Tunca, T. (2005). *Network Software Security and User Incentives*. Stanford: Stanford University.

AV-Test release latest results. (2008, 2. september). *Virus Bulletin*. Najdeno 25. septembra 2009 na spletnem naslovu http://www.virusbtn.com/news/2008/09_0

Baer, W., & Parkinson, A. (2007). The Role of CyberInsurance in Managing IT Security. *IEEE Security and Privacy, 6*, 50–56.

Baer, W. (2003). *Rewarding IT security in the marketplace.* Santa Monica: RAND Corporation.

Baryshnikov, Y. (2012). It Security Investment And Gordon-Loeb's 1/e Rule. *The 11th Workshop on the Economics of Information Security (WEIS 2012).* Berlin: Germany.

Bennett, S. P., & Kailay, M. P. (1992). An application of qualitative risk analysis to computer security for the commercial sector. *Eighth Annual IEEE Computer Security Applications Conference.* Najdeno 15. septembra 2009 na spletnem naslovu http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=443

Berinato, S. (2004, 1. september). Best Practices: The 2004 Global Information Security Survey. *CSO ONLINE.COM.* Najdeno 17. oktobra 2006 na spletnem naslovu http://www.csoonline.com/article/219573/Best_Practices_The_2004_Global_Information_Security_Survey_?page=1

BERR. (2008). *BERR 2008 Information Security Breaches Survey, Technical Report*. Najdeno 10. marca 2009 na spletnem naslovu http://www.berr.gov.uk/

Besterfield, D. H. (2002). *Total Quality Management* (3rd ed.). New York: Prentice Hall.

BIS. (2013). *2013 Information Security Breaches Survey, Technical Report*. Najdeno 10. aprila 2014 na spletnem naslovu https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

Bishop, M. (2003). *Computer Security: Art and Science.* Boston: Addison-Wesley.

Blakley, B. (2001). An imprecise but necessary calculation. *Secure Business Quarterly: Special Issue on Return on Security Investment, 1*(2), 1–3.

Bluejackel's finds. (2009, 5. september). *The first internet virus: Morris Worm.* Najdeno 18. novembra 2009 na spletnem naslovu http://bluejackal.tumblr.com/post/179742558/the-first-internet-virus-morris-worm-in-1988

Böhme, R., & Kataria, G. (2006). Models and Measures for Correlation in Cyber-Insurance. *Workshop on the Economics of Information Security (WEIS 2006).* Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Böhme, R., & Moore, T. (2009). The Iterated Weakest Link – A Model of Adaptive Security Investment. *The 8th Workshop on the Economics of Information Security (WEIS 2009)*. London: England.

Bojanc, R. (2010). *Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih* (doktorska disertacija). Ljubljana: Ekonomska fakulteta.

Bojanc, R., & Jerman-Blažič, B. (2007). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces, 30*(4), 216–222.

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413–422.

Bojanc, R., & Jerman-Blažič, B. (2012). Quantitative model for economic analyses of information security investment in an enterprise information system. *Organizacija, 45*(6), 276–288.

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, *25*(3), 25–37.

Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012a). Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach. *Information Processing & Management, 48*(6), 1031–1052.

Bojanc, R., Mörec, B., Tekavčič, M., & Jerman-Blažič, B. (2012b). Model določitve optimalnega obsega vlaganj v informacijsko varnost. *IB revija, 46*(3/4), 53–61.

Boss, S. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior.* Pittsburgh: University of Pittsburgh.

Bosworth, S., & Kabay, M. (2002). *Computer Security Handbook* (4th ed.). New York: John Wiley and Sons.

Bowen, R. (2002). *Apache Administrator's Handbook.* Indianapolis: Sams Publishing.

Brealey, R. A., & Myers, S. C. (2000). *Principles of Corporate Finance* (6th ed.). New York: McGraw-Hill.

Brecht, M., & Nowey, T. (2012). A Closer Look at Information Security Costs. *The 11th Workshop on the Economics of Information Security (WEIS 2012)*. Berlin: Germany.

Brent, R. J. (2007). *Applied cost-benefit analysis.* Cheltenham: Edward Elgar Publishing.

British Standards Institution (BSI). Najdeno 12. januarja 2010 na spletnem naslovu http://www.bsigroup.com

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report, 11*(1), 26–31.

Butler, S. A. (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach. *The 24th International Conference on Software Engineering (ICSE '02)* (str. 232–240). New York: ACM Press.

Butler, S. A., Chalasani, P., Jha, S., Raz, O., & Shaw, M. (1999). The Potential of Portfolio Analysis in Guiding Software Decisions. *The First Workshop on Economics-Driven Software Engineering Research (EDSER-1)*. Najdeno 6. avgusta 2009 na spletnem naslovu http://www.cs.cmu.edu/afs/cs/project/vit/ftp/pdf/SoftDec.pdf

Cagnemi, M. P. (2001). Top Technology Issues. *Information Systems Controls Journal, 4*(6).

Camp, L. J. (2006). The State of Economics of Information Security. *A Journal of Law and Policy for the Information Society, 2*(2), 1–14.

Camp, L. J., & Wolfram, C. (2000). Pricing Security. *The CERT Information Survivability Workshop* (str. 31–39). Boston: CERT.

Camp, L. J., & Wolfram, C. (2004). Pricing Security. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 17–34). Heidelberg: Springer.

Campbell, K., Gordon, L., Loeb, M., & Zhou L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security, 11*(3), 431–448.

Campbell, R. P., & Sands, G. A. (1979). A Modular Approach to Computer Security Risk Management. *1979 National Computer Conference* (str. 293–303). New York: IEEE Computer Society.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). Economics of IT security management: Four improvements to current security practices. *Communications of the AIS, 14*, 65–75.

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2006). Economics of Security Patch Management. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security Patch Management: Share the Burden or Share the Damage? *Management Science, 54*(4), 657–670.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). A Model for Evaluating IT Security investments. *Communications of the ACM, 47*(7), 87–92.

Computer Emergency Response Team (CERT). (2005). *OCTAVE-S Implementation Guide*. Najdeno 14. aprila 2014 na spletnem naslovu http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6795

Computer Emergency Response Team (CERT). (2008). *CERT Statistics 1988–2008*. Najdeno 13. septembra 2009 na spletnem naslovu http://www.cert.org/stats

Computer Emergency Response Team Coordination Center (CERT/CC). Najdeno 4. septembra 2007 na spletnem naslovu http://www.cert.org/certcc.html

Computer Security Institute (CSI). Najdeno 11. septembra 2008 na spletnem naslovu http://www.gocsi.com/

Computer Security Institute (CSI). (2007). CSI Survey 2007. *The 12th Annual Computer Crime and Security Survey.* Najdeno 10. oktobra 2007 na spletnem naslovu http://www.gocsi.com/forms/csi_survey.jhtml

Computer Security Institute (CSI). (2008). CSI Survey 2008. *The 13th Annual Computer Crime and Security Survey.* Najdeno 2. junija 2009 na spletnem naslovu http://www.gocsi.com/survey

Computer Security Institute (CSI). (2009). CSI Survey 2009. *The 14th Annual Computer Crime and Security Survey.* Najdeno 2. marca 2010 na spletnem naslovu http://www.gocsi.com/survey

Computer Security Institute (CSI). (2011). 2010/2011 Computer Crime and Security Survey. *The 15th Annual Computer Crime and Security Survey.* Najdeno 17. januarja 2012 na spletnem naslovu http://www.gocsi.com/survey

Conrad, J. R. (2005). Analyzing the Risks of Information Security Investmens with Montecarlo Simulations. *Workshop on the Economics of Information Security (WEIS 2005).* Najdeno 15. novembra 2006 na spletnem naslovu http://infosecon.net/workshop/schedule.php

Counterpane. (2000). *Counterpane Internet Security, Lloyd's of London: Counterpane Internet Security announces industry's first broad insurance coverage backed by Lloyd's of Londonfor e-commerce and Internet security.* Najdeno 7. februarja 2007 na spletnem naslovu http://www.counterpane.com/pr-lloyds.html

CRAMM (CCTA Risk Analysis and Management Method). (2003). *User Guide version 5.0.* Milton Keynes: Siemens, Insight Consulting.

Crume, J. (2001). *Inside Internet Security*. Boston: Addison Wesley.

Dacey, F. R. (2003). Effective Patch Management is Critical to Mitigating Software Vulnerabilities. *United Stated General Accounting Office, GAO-03-1138T.* Washington DC: United Stated General Accounting Office.

Demetz, L., & Bachlechner, D. (2012). To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool. *The 11th Workshop on the Economics of Information Security (WEIS 2012).* Germany: Berlin.

Denning E. D. (1999). *Information Warfare and Security.* Boston: Addison-Wesley.

Department of Defense (DoD). (1985). Trusted Computer System Evaluation Criteria (TCSEC). *U.S. Department of Defense, DoD 5200.28-STD*. Najdeno 25.

marca 2010 na spletnem naslovu http://csrc.nist.gov/publications/history/dod85.pdf

Digital Signature diagram. (2008). V *Wikimedia Commons*. Najdeno 2. marca 2010 na spletnem naslovu http://commons.wikimedia.org/wiki/File:Digital_ignature_diagram.svg?

DSCI. (2009). *DSCI-KPMG Survey 2009. State of Data Security and Privacy in the Indian Industry*. Najdeno 2. marca 2010 na spletnem naslovu http://www.dsci.in

DTI. (2006). *Information security breaches survey 2006.* Najdeno 27. novembra 2007 na spletnem naslovu http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

Dynes, S., Andrijcic, E., & Johnson M. E. (2006). Costs to the U.S. Economy of Information Infrastructure Failures: Estimates from Field Studies and Economic Data. *Workshop on the Economics of Information Security (WEIS 2006).* Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

EBIOS. (2011, 25. oktober). *EBIOS 2010 – Expression of Needs and Identification of Security Objectives.* Najdeno 14. aprila 2014 na spletnem naslovu http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

Eloff, J. H. P., & Eloff, M. M. (2005). Information Security Architecture. *Computer Fraud & Security, 2005*(11), 10–16.

ENISA. (2014). *Inventory of Risk Management / Risk Assessment Methods.* Najdeno 14. aprila 2014 na spletnem naslovu http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html

Enotne Tehnološke Zahteve 2.1 (ETZ). *Arhiv RS.* Najdeno 14. aprila 2014 na spletnem naslovu http://www.arhiv.gov.si/si/zakonodaja_in_dokumenti/predpisi_s_podrocja_arhivske_dejavnosti_v_sloveniji/

Espiner, T. (2005, 14. oktober). Symantec flaw found by TippingPoint bounty hunters. *ZDNET UK*. Najdeno 8. novembra 2007 na spletnem naslovu http://news.zdnet.co.uk/internet/security/0,39020375,39230317,00.htm

European Committee for Standardization (CEN). Najdeno 10. junija 2014 na spletnem naslovu https://www.cen.eu/Pages/default.aspx

European Telecommunications Standards Institute (ETSI). Najdeno 10. junija 2014 na spletnem naslovu http://www.etsi.org/

Farahmand, F. (2004). *Developing a Risk Management System for Information Systems Security Incidents.* Atlanta: Georgia Institute of Technology.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2003). Managing vulnerabilities of information systems to security incidents. *The 5th International Conference on Electronic Commerce* (str. 348–354). New York: ACM Press.

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. H. (2004). Evaluating Damages Caused by Information Systems Security Incidents. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 85–94). Heidelberg: Springer.

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. H. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management 6*(2–3), 203–225.

Federal Information Processing Standards (FIPS) publication 180-3. (2008). Secure Hash Standard. National Institute of Standards and Technology (NIST).

Federal Information Processing Standards (FIPS) publication 197. (2001). Advanced Encryption Standard. National Institute of Standards and Technology (NIST).

Federal Information Security Management Act (FISMA). (2002, 24. oktober). Najdeno 21. aprila 2009 na spletnem naslovu http://csrc.nist.gov/groups/SMA/fisma/index.html

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering.* New York: John Wiley & Sons, Inc.

Frei, S., Schatzmann, D., Plattner, B., & Trammell, B. (2009). Modelling the Security Ecosystem – The Dynamics of (In)Security. *Workshop on the Economics of Information Security (WEIS 2009).* Najdeno 28. oktobra 2009 na spletnem naslovu http://weis09.infosecon.net/programme.html

Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research, 16*(2), 86–208.

Gansler, J. S., & Lucyshyn, W. (2005). Improving the Security of Financial Management Systems: What Are We to Do? *Journal of Accounting and Public Policy, 24*(1), 1–9.

Garcia, A., & Horowitz, B. (2006). The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Gardner, P. E. (1989). Evaluation of Five Risk in Aiding Management Decisions. *Computers & Security, 8*(6), 479–485.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of it security breaches. *Information Management & Computer Security, 11*(2),74–83.

Garson, G. D. (2006). *Public Information Technology and E-Governance: Managing the Virtual State.* Sudbury: Jones and Barlett Publishers.

Geer, D. (2001). Return on security investment: Calculating the security investment equation. *Secure Business Quarterly, 1*(2).

Geer, D. (2002). Making choices to show ROI. *Secure Business Quarterly, 1*(2), 1–5.

Geer, D. (2004, 20. oktober). Q&A: Dan Geer on security of information when economics matters. *SearchDataManagement.com*. Najdeno 4. decembra 2007 na spletnem naslovu http://searchdatamanagement.techtarget.com/news/interview/0,289202,sid91_gci1139680,00.html

Germain, J. M. (2007, 18. marec). TraceSecurity CTO Jim Stickley: Robbing Banks With Impunity. *TechNews World.* Najdeno 12. septembra 2008 na spletnem naslovu http://www.technewsworld.com/story/56547.html

Gonzalez, J., & Sawicka, A. (2002). A Framework for Human Factors in Information Security. *2002 WSEAS International Conference on Information Security*. Najdeno 19. oktobra 2009 na spletnem naslovu http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf

Gordon, A. L. (2004). *Managerial Accounting: Concepts and Empirical Evidence* (6th ed.). New York: McGraw-Hill.

Gordon, A. L., & Loeb, P. M. (2001). Using information security as a response to competitor analysis systems. *Communications of the ACM, 44*(9), 70–75.

Gordon, A. L., & Loeb, P. M. (2002a). Return on Information Security Investments: Myths vs. Reality. *Strategic Finance,* november 2002, 26–31.

Gordon, A. L,. & Loeb, P. M. (2002b). The Economics of Information Security Investment. *Communications of the ACM, 5*(4), 438–457.

Gordon, A. L., & Loeb, P. M. (2003, 6. marec). Economic Aspects of Information Security. *University of Maryland Institute for Advanced Computer Studies*. Najdeno 7. decembra 2006 na spletnem naslovu http://www.umiacs.umd.edu/docs/umiacspresentation.pdf

Gordon, A. L., & Loeb, P. M. (2005). *Managing Cybersecurity Resources: A Cost-Benefit Analysis.* New York: McGraw Hill.

Gordon, A. L., & Loeb, P. M. (2006). Budgeting process for information security expenditures. *Communications of the ACM, 49*(1), 121–125.

Gordon, A. L., & Richardson, R. (2004, 13. april). The New Economics of Information Security. *Bank Systems & Technology*. Najdeno 6. novembra 2007 na spletnem naslovu http://www.banktech.com/aml/showArticle.jhtml?articleID= 18901266

Gordon, A. L., Loeb, P. M., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.

Haimes, Y. Y., & Chittester, C. (2005). A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems. *Journal of Homeland Security and Emergency Management, 2*(2).

Horowitz, B., & Garcia, A. (2005). A growing trend towards underinvestment in internet security. *Verdasys, Inc.* Charlottesville, Virginia: University of Virginia.

Hovava, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements of the market value of firms. *Risk Management and Insurance Review, 6*(2), 97–121.

How a digital timestamp works. (2010). Najdeno 22. oktobra 2014 na spletnem naslovu https://www.digistamp.com/technical/how-a-digital-time-stamp-works/

Hoyle, D. (2009). *ISO 9000 Quality Systems Handbook – updated for the ISO 9001:2008 standard* (6th ed.). Using the standards as a framework for business improvement. Oxford: Taylor & Francis.

Huang, C. D., Hu, Q., & Behara S. R. (2005a). Investment in information security by a riskaverse firm. *The 2005 Softwars Conference*. Las Vegas, NV.

Huang, C. D., Hu, Q., & Behara S. R. (2005b). In search for optimal level of information security investment in risk-averse firms. *The Third Annual Security Symposium*. Tempe, Arizona: Arizona State University.

Hughes, L. A., & DeLone, G. J. (2007). Viruses, worms, and Trojan horses – Serious crimes, nuisance, or both? *Social Science Computer Review, 25*(1), 78–98.

iDefense. Najdeno 28. januarja 2009 na spletnem naslovu http://labs. idefense.com

Information Systems Audit and Control Association (ISACA). Najdeno 13. oktobra 2009 na spletnem naslovu http://www.isaca.org

Information Systems Security Association (ISSA). Najdeno 13. oktobra 2009 na spletnem naslovu http://www.issa.org

Information Technology Infrastructure Library (ITIL). Najdeno 2. februarja 2010 na spletnem naslovu http://www.itil-officialsite.com/home/home.asp

International Organization for Standardization (ISO). Najdeno 27. marca 2008 na spletnem naslovu http://www.iso.org

Internet Engineering Task Force (IETF). Najdeno 13. oktobra 2009 na spletnem naslovu http://www.ietf.org

Internet Security Alliance (ISA). Najdeno 13. oktobra 2009 na spletnem naslovu http://www.isalliance.org

Internet Society (ISOC). (2012). *A Brief History of the Internet*. Najdeno 15. oktobra 2012 na spletnem naslovu http://www.isoc.org/internet/history/brief.shtml

Ioannidis, C., Pym, D., & Williams, J. (2009). Investments and trade-offs in the economics of information security. V R. Dingledine & P. Golle (ur.), *Financial Cryptography and Data Security* (str. 148–166). Heidelberg: Springer.

Ioannidis, C., Pym, D., & Williams, J. (2011). Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach. *The 10th Workshop on the Economics of Information Security (WEIS 2011)*. Fairfax: Virginia.

ISAMM. (2008). Najdeno 4. aprila 2012 na spletnem naslovu http://www.telindus.com

Islovar (*slovar informatike)*. Najdeno 17. februarja 2010 na spletnem naslovu http://www.islovar.org/iskanje_enostavno.asp

ISO 31000:2009. Risk management – Principles and guidelines. Geneva: International Organization for Standardization (ISO).

ISO 9001:2008. Quality management systems – Requirements. Geneva: International Organization for Standardization (ISO).

ISO Guide 73:2009. Risk management – Vocabulary. Geneva: International Organization for Standardization (ISO).

ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1:

Concepts and models for information and communications technology security management. Geneva: International Organization for Standardization (ISO).

ISO/IEC 15408:2008. Information technology – Security techniques – Evaluation criteria for IT security. Geneva: International Organization for Standardization (ISO).

ISO/IEC 21827:2008. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM). Geneva: International Organization for Standardization (ISO).

ISO/IEC 22301:2012. Societal security – Business continuity management systems – Requirements. Geneva: International Organization for Standardization (ISO).

ISO/IEC 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva: International Organization for Standardization (ISO).

ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization (ISO).

ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management. Geneva: International Organization for Standardization (ISO).

ISO/IEC 27003:2010. Information technology – Security techniques – Information security management system implementation guidance. Geneva: International Organization for Standardization (ISO).

ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization (ISO).

ISO/IEC 31010:2009. Risk management – Risk assessment techniques. Geneva: International Organization for Standardization (ISO).

ISO/TR 31004:2013. Risk management – Guidance for the implementation of ISO 31000. Geneva: International Organization for Standardization (ISO).

Jacobson, R. V. (2000). What is a rational goal for security? *Security Management, 44*(12), 144–151.

Jerman-Blažič, B. (2011). Kako je internet prišel v Slovenijo. *Isoc-drustvo.si*. Najdeno 30. oktobra 2011 na spletnem naslovu http://www.isoc-drustvo.si/prihod-interneta/

Kannan, K., & Telang, R. (2004). An Economic Analysis of Market for Software Vulnerabilities. *Workshop on the Economics of Information Security (WEIS 2004)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207

Kaplan, R. (2007). A Matter of Trust. V H. F. Tipton & M. Krause (ur.). *Information Security Management Handbook*, 6th edition (str. 295–310). Boca Raton, Florida: Auerbach Publications.

Kazenski zakonik (KZ-1). *Uradni list RS* št. 50/2012-UPB2.

Kwon, J., & Johnson, M. E. (2012). Security Resources, Capabilities And Cultural Values: Links To Security Performance And Compliance. *The 11th Workshop on the Economics of Information Security (WEIS 2012)*. Berlin: Germany.

Locher, C. (2005). Methodologies for Evaluating Information Security Investments – What Basel II can Change in the Financial Industry. *13th European Conference on Information Systems in a Rapidly Changing Economy (ECIS 2005)*. Regensburg, Germany: University of Regensburg.

Longstaff, T. A., Chittister, C., Pethia, R., & Haimes, Y. Y. (2000). Are We Forgetting the Risks of Information Technology? *Computer, 33*(12), 43–51.

Magerit. (2012). *Magerit V.3: methodology of risk analysis and management of information systems*. Najdeno 14. aprila 2014 na spletnem naslovu http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.U0mxFfl_sek

Majuca, R., Yurcik, W., & Kesan J. P. (2006). The evolution of cyberinsurance. V *ACM Computing Research Repository (CoRR)*. Najdeno 27. maja 2008 na spletnem naslovu http://arxiv.org/ftp/cs/papers/0601/0601020.pdf

Matsuura, K. (2008). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. *Workshop on the Economics of Information Security (WEIS 2008)*. Najdeno 2. septembra 2008 na spletnem naslovu http://weis2008.econinfosec.org/program.htm

Mayer, N., Heymans, P., & Matulevičius, R. (2007). Design of a modelling language for information system security risk management. *The 1st International Conference on Research Challenges in Information Science (RCIS '07)*. Najdeno 16. septembra 2008 na spletnem naslovu http://www.nmayer.eu/publis/RCIS07-CR_NMA-PHE-RMA.pdf

McGhie, L. (2003). Software patch management – the new frontier. *Secure Business Quarterly, 3*(2), 1–4.

McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley.

Mehari. (2010). *Mehari: Information risk analysis and management methodology*. Najdeno 14. aprila 2014 na spletnem naslovu http://www.clusif.asso.fr/en/production/mehari/

Mehr, R. I., & Hedges, B. A. (1974). *Risk Management: Concepts and Applications*. Homewood, Illinois: Richard D. Irwin, Inc.

Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM, 46*(6), 15–18.

Metcalfe's law. (2013). V *Wikipedia*. Najdeno 5. februarja 2013 na spletnem naslovu http://en.wikipedia.org/wiki/Metcalfe's_law

Ministrstvo za notranje zadeve Republike Slovenije. (b.l.). *Osnove varnih časovnih žigov*. Najdeno 2. septembra 2010 na spletnem naslovu http://www.si-tsa.si/osnove.php

Mizzi, A. (2005). Return on Information Security Investment. Are you spending enough? Are you spending too much? *InfosecWriters*. Najdeno 14. oktobra 2008 na spletnem naslovu http://www.infosecwriters.com/text_resources/pdf/ROISI.pdf

Mizzi, A. (2010). Return on information security investment-the viability of an antispam solution in a wireless environment. *International Journal of Network Security, 10*(1), 18–24.

Moore, T., & Anderson, R. (2011). Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research. *Harvard Computer Science Technical Report TR-03-11 in The Oxford Handbook of the Digital Economy*. Oxford: Oxford University Press.

Moore, D., Shannon, C., & Brown, J. (2002). Code-red: a case study on the spread and victims of an internet worm. *The Second ACM SIGCOMM Workshop on Internet Measurement* (str. 273–284). Marseille: Internet Measurement Conference.

Morris worm. (2008). V *Wikipedia*. Najdeno 27. maja 2008 na spletnem naslovu http://en.wikipedia.org/wiki/Morris_worm

Munger, M. C. (2000). *Analyzing Policy*. New York: W.W. Norton.

National Institute of Standards and Technology (NIST). Najdeno 16. aprila 2009 na spletnem naslovu http://www.nist.gov

Neumann, P. G. (2000). *Computer-Related Risks*. Boston: Addison-Wesley.

NIST Special Publication 800-12. (1995). An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology (NIST).

NIST Special Publication 800-14. (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology (NIST).

NIST Special Publication 800-27. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. National Institute of Standards and Technology (NIST).

NIST Special Publication 800-30. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST).

Oakland, J. S. (2003). *Total Quality Management: Text with Cases* (3rd ed.). Oxford: Butterworth-Heinemann Ltd.

OECD. (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Najdeno 4. aprila 2014 na spletnem naslovu http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm

Overill, R. E. (2008). ISMS insider intrusion prevention and detection. *Information Security Technical Report, 13*(4), 216–219.

Palsit d.o.o. – O podjetju. Najdeno 3. februarja 2010 na spletnem naslovu http://www.palsit.com/slo/podjetje.php

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Power, R. (1999, oktober). CSI special report: How to quantify financial losses from infosec breaches. *Computer Security Institute, Alert Newsletter*, (št. 199), str. 1 in 12.

Pravilnik o načinu posredovanja hranjenih podatkov o prometu telefonskih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju. *Uradni list RS* št. 103/2009.

Pravilnik o opremi in vmesnikih za zakonito prestrezanje informacij. *Uradni list RS* št. 89/2013.

Pritchard, J. (1978). *Risk Management in Action*. Manchester: NCC Publications.

Raba interneta v Sloveniji (RIS). (2013). *Zakonodaja (informacijska varnost)*. Najdeno 13. marca 2013 na spletnem naslovu http://www.ris.org/index.php?fl=2&lact=1&bid=10708&parent=26

Rescorla, E. (2004). Is Finding Security Holes a Good Idea? *Workshop on the Economics of Information Security (WEIS 2004)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207

RFC 1321. (1992). The MD5 Message-Digest Algorithm. Internet Engineering Task Force (IETF). Najdeno 10. novembra 2009 na spletnem naslovu www.ietf.org/rfc/rfc1321.txt

RFC 2104. (1997). HMAC: Keyed-Hashing for Message Authentication. Internet Engineering Task Force (IETF). Najdeno 24. marca 2010 na spletnem naslovu www.ietf.org/rfc/rfc2104.txt

RFC 2196. (1997). Site Security Handbook. Internet Engineering Task Force (IETF). Najdeno 10. novembra 2009 na spletnem naslovu www.ietf.org/rfc/rfc2196.txt

RFC 2459. (1999). Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Internet Engineering Task Force (IETF). Najdeno 10. novembra 2009 na spletnem naslovu www.ietf.org/rfc/rfc2459.txt

RFC 3161. (2001). Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP). Internet Engineering Task Force (IETF). Najdeno 4. aprila 2014 na spletnem naslovu www.ietf.org/rfc/rfc3161.txt

RFC 3447. (2003). Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. Internet Engineering Task Force (IETF). Najdeno 4. aprila 2014 na spletnem naslovu www.ietf.org/rfc/rfc3447.txt

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120–126.

Rowe, R. B., & Gallaher, P. M. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Schechter, S. (2004). *Computer Security Strength & Risk: A Quantitative Approach*. Cambridge, Massachusetts: Harvard University.

Schneier, B. (1996). *Applied Cryptography* (2nd ed.). New York: John Wiley & Sons, Inc.

Schneier, B. (2001). Insurance and the Computer Industry. *Communications of the ACM, 44*(3), 114–115.

Schneier, B. (2002). Network Monitoring and Security. *Counterpane Internet Security, Inc*. Najdeno 19. Junija 2007 na spletnem naslovu http://bt.counterpane.com/presentation3.pdf

Schneier, B. (2003). *Beyond Fear: Think Sensibly about Security in an Uncertain World.* New York: Copernicus Books.

Schneier, B. (2004a). *Secrets & Lies, Digital Security in a Networked World.* New York: Wiley Publishing.

Schneier, B. (2004b). Evaluating Security Systems: A Five-step Process. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 289–293). Heidelberg: Springer.

Shapiro, C., & Varian H. (1998). *Information Rules*. Boston: Harvard Business School Press.

Shostack, A. (2003). Quantifying patch management. *Secure Business Quarterly, 3*(2), 1–4.

SI-CA. (2006). *Digitalni podpis*. Najdeno 4. aprila 2014 na spletnem naslovu http://www.si-ca.si/kripto/kr-podp.htm

SiQ. (2008, 29. januar). *Trendi razvoja varnostne politike informacijskega sistema in standarda ISO/IEC 27001:2005*. Najdeno 3. februarja 2010 na spletnem naslovu http://www.siq.si/o_institutu/novice/novica/article/496/index.html

SIST ISO 31000:2011. Obvladovanje tveganja – Načela in smernice. Ljubljana: Slovenski inštitut za standardizacijo (SIST).

SIST ISO/IEC 27001:2013. Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve. Ljubljana: Slovenski inštitut za standardizacijo (SIST).

SI-TSA. (2014). *Izdajatelj varnih časovnih žigov SI-TSA*. Najdeno 4. aprila 2014 na spletnem naslovu http://www.si-tsa.si

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions.* Beverly Hills: Sage Publications.

Slovenian Computer Emergency Response Team (SI-CERT). (2013). *Zakonodaja RS, ki se nanaša na informacijsko varnost.* Najdeno 13. marca 2013 na spletnem naslovu https://www.cert.si/si/zakonodaja/

Slovenian Computer Emergency Response Team (SI-CERT). (2013a). *Slovenian Police cracks down on a gang netting almost 2 million € from companies via e-banking hacks.* Najdeno 12. avgusta 2013 na spletnem naslovu

https://www.cert.si/slovenian-police-cracks-down-on-a-gang-netting-almost-2-million-e-from-companies-via-e-banking-hacks/

Slovenski inštitut za standardizacijo (SIST). Najdeno 1. oktobra 2012 na spletnem naslovu http://www.sist.si

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment (ROSI) – A Practical Quantitative Model. *Journal of Research and Practice in Information Technology, 38*(1), 45–56.

Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach To Computer Security*. Palo Alto, CA: Stanford University.

Sookdawoor, O. (2005). *An Investigation of Information Security Policies and Practices in Mauritius.* Unisa, South Africa: University of South Africa.

Splošni akt o varnosti omrežij in storitev. *Uradni list RS* št. 75/2013.

Splošni akt o zavarovanju hranjenih podatkov. *Uradni list RS* št. 75/2013.

Splošni akt o zbiranju, uporabi in dajanju podatkov o razvoju trga elektronskih komunikacij. *Uradni list RS* št. 62/2013.

Stinchcombe, A. L., Adams, R., Heimer, C. A., Scheppele, K. L., Smith, T. W., & Taylor, D. G. (1980). *Crime and punishment-changing attitudes in America*. San Francisco: Jossey-Bass Publishers.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255–273.

Strickland, J. (2008, 26. avgust). *Worst Computer Viruses of All Time.* Najdeno 1. oktobra 2012 na spletnem naslovu http://computer.owstuffworks.com/worst-computer-viruses.htm

Sturrock, S. (2005, 16. junij). Psycho (but not) logical fears flying vs. driving. *Palm Beach Post*. Najdeno 24. februarja 2009 na spletnem naslovu http://findarticles.com/p/articles/mi_8163/is_20050616/ai_n51874341/?tag=content;col1

Su, X. (2006). *An Overview of Economic Approaches to Information Security Management*. Technical Report TR-CTIT-06-30. Enschede: Centre for Telematics and Information Technology, University of Twente.

Swartz, J. (2005, 29. december). 2005 worst year for breaches of computer security. *USA Today*. Najdeno 17. februarja 2009 na spletnem naslovu http://www.usatoday.com/tech/news/computersecurity/2005-12-28-computer-security_x.htm

Swire, P. P. (2001, 24. september). What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory. *The Computer Research Repository (CoRR)*. Najdeno 17. februarja 2009 na spletnem naslovu http://arxiv.org/abs/cs.CR/0109089

Tanaka, H. (2005). A Firm Level Empirical Analysis of Information Security Investment. *20th Annual Conference of Japan Association for Social Informatics* (str. 185–188). Kyoto: Kyoto University.

Tanaka, H., Liu, W., & Matsuura, K. (2006). An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy, 24*(1), 37–59.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561–570.

The SANS (SysAdmin, Audit, Network, Security) Institute Online. Najdeno 16. aprila 2009 na spletnem naslovu http://www.sans.org

TippingPoint. Najdeno 29. januarja 2009 na spletnem naslovu http://tippingpoint.com

Tordoff, P. (2006). UK Information Security Breaches Survey. *ENISA quarterly, 2*(2), 15–17.

Tudor, J. K. (2000). Information Security Arcitecture – An Integrated Approach to Security in the Organization. New York: Auerbach.

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. *Uradni list RS* št. 77/00, 2/01 in 86/06.

Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov. *Uradni list RS* št. 71/2006 in 138/2006.

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih. *Uradni list RS* št. 48/2007 in 86/2011.

Uredba o varovanju tajnih podatkov. *Uradni list RS* št. 74/2005, 7/2011 in 24/2011.

Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAG). *Uradni list RS* št. 86/2006.

Varian, H. R. (2000, 1. junij). Managing online security risks. *The New York Times*. Najdeno 3. junija 2011 na spletnem naslovu http://www.nytimes.com/library/financial/columns/060100econ-scene.html

Wang, Y., Beck, D., Jiang, X., & Roussev, R. (2006). Automated web patrol with strider honeymonkeys: Finding web sites that exploit browser vulnerabilities. *MSR-TR-2005-72*. Redmond: Microsoft Research.

Willemson, J. (2006). On the Gordon&Loeb Model for Information Security Investment. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

Willemson J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. *The 5th International Conference on the Availability, Reliability, and Security (ARES '10),* 258–261.

Withdrawn Federal Information Processing Standards Publications (FIPS) Listed by Number. Najdeno 20. aprila 2010 na spletnem naslovu http://www.itl.nist.gov/fipspubs/withdraw.htm

Xie, N., & Mead N. R. (2004). SQUARE Project: Cost/ Benefit Analysis Framework for Information Security Improvement Projects in Small Companies. *CMU/SEI-2004-TN-045*. Pittsburgh: Carnegie Mellon University.

Yener, B. (2003). Internet Security. V J. G. Proakis (ur.), *Encyclopedia of Telecommunications, Vol 2* (str. 1152–1157). New York: John Wiley and Sons.

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). *Uradni list RS* št. 98/2004-UPB1.

Zakon o elektronskem poslovanju na trgu (ZEPT). *Uradni list RS* št. 96/2009-UPB2.

Zakon o elektronskih komunikacijah (ZEKom-1). *Uradni list RS* št. 109/2012, 110/2013.

Zakon o tajnih podatkih (ZTP). *Uradni list RS* št. 50/2006-UPB2, 9/2010, 60/2011.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A). *Uradni list RS* št. 30/2006, 51/2014.

Zakon o varstvu osebnih podatkov (ZVOP-1). *Uradni list RS* št. 94/2007-UPB1.

Zakon o varstvu potrošnikov (ZVPot). *Uradni list RS* št. 98/2004-UPB2, 126/2007, 86/2009, 78/2011.

SEZNAM UPORABLJENIH KRATIC IN IZRAZOV

Kratica	Slovenski izraz	Angleški izraz
AES	napredni standard za šifriranje	Advanced Encryption Standard
AKOS	Agencija za komunikacijska omrežja in storitve Republike Slovenije	Agency for Communication Networks and Services of the Republic of Slovenia
ALE	pričakovana letna izguba	Annual Loss Expectancy
B2B	poslovanje med podjetji	Business-to-Business
B2C	poslovanje podjetja s potrošnikom	Business-to-Consumer
B2G	poslovanje podjetja z državo	Business-to-Government
BCM	obvladovanje neprekinjenega poslovanja	Business Continuity Management
BSI	Britanski inštitut za standardizacijo	British Standards Institute
CBR	razmerje med stroški in koristi	Cost-benefit ratio
CEN	Evropski komite za standardizacijo	European Committee for Standardization
CERT	Odzivni center za obravnavo incidentov	Computer Emergency Response Team
CIA	zaupnost, celovitost, razpoložljivost	Confidentiality, Integrity, Availability
CSI	Inštitut za računalniško varnost (ZDA)	Computer Security Institute
DoS	ohromitev storitve	Denial of Service
ENISA	Evropska agencija za varnost omrežij in informacij	European Union Agency for Network and Information Security
ETSI	Evropski inštitut za telekomunikacijske standarde	European Telecommunications Standards Institute
FIPS	zvezni standard za obdelavo informacij (ZDA)	Federal Information Processing Standard

Kratica	Slovenski izraz	Angleški izraz
HMAC	avtentikacijska koda sporočila z zgoščevanjem	Hash-based Message Authentication Code
IDS	sistem za zaznavanje vdorov	Intrusion Detection System
IKT	informacijska in komunikacijska tehnologija	Information and Communication Technology
IRR	notranja stopnja donosa	Internal Rate of Return
ISO	Mednarodna organizacija za standardizacijo	International Organization for Standardization
ITIL	knjižnica IT-infrastrukture	Information Technology Infrastructure Library
KZ	Kazenski zakonik	Criminal Code
MD5	zgoščevalna funkcija MD5	Message-Digest Algorith 5
NIST	Državni inštitut za standarde in tehnologijo (ZDA)	National Institute of Standards and Technology
NPV	neto sedanja vrednost	Net Present Value
PDCA	planiraj, naredi, preveri, ukrepaj	Plan, Do, Check, Act
ROI	donosnost investicije	Return on Investment
SHA	varni zgoščevalni algoritem	Secure Hash Algorith
SI-CERT	Nacionalni odzivni center za obravnavo incidentov	Slovenian Computer Emergency Response Team
SiQ	Slovenski institut za kakovost in meroslovje	Slovenian Institute of Quality and Metrology
SIST	Slovenski inštitut za standardizacijo	Slovenian Institute for standardization
SLA	sporazum o ravni storitve	Service Level Agreement
SVIV (ISMS)	sistema vodenja informacijske varnosti	Information Security Management System
TSA	overitelj časovnih žigov	Time Stamp Authority
ZEKom	Zakon o elektronskih komunikacijah	Electronic Communications Act

Kratica	Slovenski izraz	Angleški izraz
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu	Electronic Commerce and Electronic Signature Act
ZEPT	Zakon o elektronskem poslovanju na trgu	Electronic Commerce Market Act
ZTP	Zakon o tajnih podatkih	Secret Information Act
ZVDAGA	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih	Protection of Documents and Archives and Archival Institutions Act
ZVOP	Zakon o varstvu osebnih podatkov	Personal Data Protection Act
ZVPot	Zakon o varstvu potrošnikov	Consumer Protection Act