UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

Rok Bojanc

MODELI ZAGOTAVLJANJA VARNOSTI V POSLOVNIH INFORMACIJSKIH SISTEMIH

Doktorska disertacija

Ljubljana, 2010

Izjava o avtorstvu in objavi elektronske verzije doktorske disertacije in osebnih podatkov, vezanih na zaključek študija

Rok Bojanc izjavljam, da sem avtor te doktorske disertacije in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo doktorske disertacije na spletišču CEK-a.

Tiskana verzija doktorske disertacije je istovetna elektronski verziji, ki sem jo oddal v zbirko polnih besedil zaključnih del EF UL.

Podpisani hkrati izjavljam, da dovolim objavo osebnih podatkov, vezanih na zaključek študija na spletnih straneh in v publikacijah Univerze v Ljubljani.

Ime in priimek doktoranda: Rok Bojanc
Leto in kraj rojstva: 1974, Ljubljana
Datum zagovora: 23. 12. 2010
Predsednica: prof.dr. Metka Tekavčič
Mentorica: prof.dr. Borka Jerman Blažič
Član: prof.dr. Andrej Kovačič

V Ljubljani, dne 23. 12. 2010 Podpis doktoranda:

_____

MODELI ZAGOTAVLJANJA VARNOSTI V POSLOVNIH INFORMACIJSKIH SISTEMIH

Povzetek

Internet in informacijski sistemi so omogočili podjetjem zmanjšanje stroškov, doseganje večje produktivnosti, razvoj tesnejših poslovnih partnerstev in izboljšanje odnosov s strankami. Po drugi strani pa je uporaba interneta pomenila nova tveganja. Ta disertacija pokriva področje ravnanja z informacijsko varnostjo in podaja pregled nad raziskovalnim področjem ekonomike informacijske varnosti. Osredotoča se predvsem na kvantitativno analizo varnostnega tveganja in kvantitativno vrednotenje informacijske varnosti. Disertacija predstavlja tudi analizo dosedanjih teoretičnih in empiričnih spoznanj ter ugotovitev na področju ekonomike informacijske varnosti. Rezultati v tej disertaciji omogočajo vodjem informacijske varnosti odgovoriti na mnoga vprašanja, ki si jih zastavljajo pri svojem delu. Podaja odgovor na ključno vprašanje, kateri varnostni ukrep izbrati za določeno grožnjo. Disertacija podaja metodologijo za kvantitativno merjenje informacijske varnosti. Razviti model omogoča medsebojno kvantitativno vrednotenje investicij v različne varnostne ukrepe. Z investicijami v informacijsko varnost se zmanjšujejo varnostna tveganja, ki pretijo informacijskim sredstvom. Ustreznost in uporabnost modela je preverjena z matematično simulacijo. Model je empirično preizkušen na primeru konkretnega podjetja. Predstavljen je postopek, ki podjetju omogoča pomoč pri odločanju glede ustrezne obravnave tveganja in mu omogoča izbiro ekonomsko optimalnega varnostnega ukrepa. Pri tem so vključene možnosti investicije v tehnični ali proceduralni ukrep ter prenos tveganja na zunanjega izvajalca ali zavarovalnico. V podporo odločanju je predstavljena tudi ustrezna kategorizacija tveganj in ukrepov. Disertacija se zaključuje s priporočilom za standarden kvantitativen pristop na področju investiranja v informacijsko varnost in možnostmi za nadaljnje raziskave in izboljšave modela.

Ključne besede: informacijska varnost, obvladovanje tveganja, investicije v varnostno tehnologijo, preprečevanje spletnega kriminala, ekonomika informacijske varnosti, kvantitativna analiza

MODELS FOR PROVIDING SECURITY IN BUSINESS INFORMATION SYSTEMS

Summary

Internet and information systems have enabled businesses to reduce costs, achieve greater market scope, develop closer business partnerships and improve relationships with customers. On the other hand, the use of the Internet presents new risks. This dissertation covers the area of information security management and provides an overview of the research area of economics of information security. It focuses primarily on quantitative security risks analysis and quantitative information security assessment. The dissertation presents an analysis of current theoretical and empirical insights and findings in the field of economics of information security. The results in this dissertation provide information security managers to answer themselves the many questions especially the ones regarding the use of the right security measure for a certain threat. The dissertation presents a methodology for the quantitative measurement of information security. The developed model enables quantitative evaluation of investments in different security measures. Relevance and usefulness of the model is verified by mathematical simulation. The model is empirically tested for the case of a concrete company. The presented procedure helps organizations taking decision about the appropriate risk treatment and lead to a recommendation by the selection of economically optimal security measure. The investment possibilities in technical and procedural measures, transfer of risk on exterior partner or insurance company are also taken into account. In order to support decision-making is also presented in the appropriate categorization of the risks and measures. The dissertation concluded with a recommendation for a standard qualitative approach regarding investments in information security and opportunities for further research and improvements to the model.

Keywords: information security, risk management, security technology investment, cybercrime prevention, economics of information security, quantitative analysis

Kazalo

Kazalo slik

Kazalo tabel

Uvod

Sodobna informacijska tehnologija omogoča, da podjetja poslujejo hitreje, učinkoviteje in ceneje. Zato podjetja v svoje informacijske sisteme tudi veliko vlagajo (Gordon & Loeb, 2002b). Zaradi povečanja elektronskega poslovanja postajajo podjetja čedalje bolj odvisna od zanesljivosti in stabilnosti delovanja svojih informacijskih sistemov. Do množične uporabe elektronskega poslovanja je prišlo po zaslugi interneta, kot globalnega medija za dostop do informacij in izmenjavo podatkov. Poleg pridobitev pa to predstavlja tudi nove grožnje in nevarnosti za poslovanje podjetij. Zaradi velike odvisnosti podjetij od informacijskih sistemov so grožnje, ki pretijo njihovim informacijskim sredstvom, toliko bolj resne in nevarne (Cagnemi, 2001). Negativne posledice možnega napada na informacijske sisteme so lahko velike in v nekaterih primerih za podjetja celo pogubne. Da se podjetja zavarujejo pred grožnjami, ki pretijo njihovim informacijskim sistemom, morajo vzpostaviti varnostne mehanizme, ki varujejo njihov informacijski sistem.

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. Na začetku je internet predstavljal zaprto omrežje, ki je povezovalo le določene izbrane organizacije in ustanove. Zato tudi ni bilo posebne potrebe po varnosti in načrtovalci omrežij se s samo varnostjo niso preveč ukvarjali. 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 & Blažič, 2007, str. 216).

Podjetje mora določiti, katera informacijska sredstva želi varovati pred grožnjami, ki pretijo elektronskemu poslovanju, in v kolikšnem obsegu jih želi varovati. Informacijska sredstva predstavljajo pravzaprav vse, kar podjetju prinaša vrednost (NIST 800-12, 1995; FIPS 199, 2004). Med informacijska sredstva spadajo fizična infrastruktura (strežniki, omrežna infrastruktura in ostala lastnina), programska oprema, podatki, intelektualna lastnina, znanje, ugled podjetja itd.

Informacijska sredstva v podjetjih so izpostavljena določenim varnostnim tveganjem. Varnostna tveganja so na primer odpoved delovanja storitev, izguba ali kraja podatkov, nepooblaščen vpogled v podatke ali nepooblaščeno spreminjanje podatkov (Schechter & Smith 2003; Young in Yung, 1996). Za uspešno izvedbo varnostnih strategij je ključno, da podjetje pozna grožnje, ki pretijo sredstvom v njihovem podjetju (Whitman, 2003; McClure, Scambrey & Kurtz, 2001). Ker so grožnje pogosto usmerjene na zaupnost, celovitost in razpoložljivost informacijskih sredstev, je osnovni namen informacijske varnosti, da zavaruje ta področja (NIST 800-12, 1995).

Grožnje, ki pretijo informacijskim sredstvom, lahko izkoriščajo ranljivosti v programski opremi, konfiguraciji omrežja, varnostnih procedurah ipd. Večino varnostnih incidentov povzročajo ranljivosti, ki so posledica napak v programski opremi (Arora & Telang, 2005, str. 20). Strokovnjaki ocenjujejo, da je na vsakih 1000 vrstic programske kode približno 20 napak in da število prijavljenih ranljivosti z leti močno narašča (Dacey, 2003). Čeprav so v večini primerov ranljivosti tehnične narave, je velikokrat razlog za varnostni incident človeške narave. 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. Camp in Wolfram (2000) sta ranljivosti sistema predstavila kot posebno tržno "dobrino" (Kannan & Telang, 2004). Da tržišče ranljivosti zares obstaja, se je pokazalo oktobra 2005 v napadu na podjetje 3COM (Espiner, 2005; Ozment, 2004), kjer je bila zlorabljena do takrat še neodkrita ranljivost sistema. Odkritje podobne ranljivosti je objavil tudi Microsoft (Wang, Guo, Simon & Zugenmaier, 2004). Podjetji iDefense in Tipping Point, sta na tržišču ranljivosti prisotni tako, da ranljivosti javno kupujeta (Anderson & Moore, 2006, str. 610).

Ranljivosti v programski opremi proizvajalci rešujejo z varnostnimi popravki, ki so javno objavljeni (Cavusoglu, Cavusoglu & Zhamg, 2006; Donner, 2003). V zadnjih letih se je močno skrajšal čas od odkritja ranljivosti do primera njegove prve zlorabe, zato je treba varnostne popravke nameščati kar se da ažurno (August & Tunca, 2005; Shostack, 2003). Kljub temu nekateri avtorji (Rescorla, 2004) odsvetujejo iskanje ranljivosti in popravkov, ker naj bi po njihovem mnenju javna objava ranljivosti več doprinesla napadalcu kot uporabniku; izjema so primeri, ko sta objava ranljivosti in popravka med seboj časovno usklajena. Za dobro korelacijo med objavo novo odkritih ranljivosti in ustreznih popravkov imajo pomembno vlogo informacijski posredniki (angl. *infomediary:* ***info****rmation inter****mediary***) (Kannan & Telang, 2004). Primer informacijskega posrednika je Computer Emergency Response Team (CERT). Te organizacije zbirajo prijave prostovoljcev, ki odkrijejo kakšno novo ranljivost ter nato obvestijo proizvajalce programske opreme. Šele, ko proizvajalec izdela ustrezen popravek, ranljivost tudi sami javno objavijo.

Uspešno izveden napad na poslovni informacijski sistem podjetja povzroči izgube. V večini primerov so izgube povezane z izgubo prihodka, izgubo produktivnosti, dodatnimi stroški zaradi reševanja in vzpostavitve delujočega stanja informacijskega sistema, izgubo ugleda, prekinitvijo poslovnega procesa, neizpolnjevanjem zakonskih obveznosti, izgubo intelektualne lastnine in manjšim zaupanjem kupcev. Podatkov o dejanski škodi, ki jo povzročajo varnostni incidenti, primanjkuje. Eden izmed bolj ažurnih virov na tem področju je letno poročilo CSI (Computer Security Institute), v katerem podjetja ocenijo stroške različnih kategorij varnostnih incidentov (CSI, 2009).

Podjetja veliko vlagajo v rešitve, povezane z varnostjo in zaščito informacijskih sistemov (Adkins, 2004; CERT, 2008; Tordoff, 2006). V zadnjem času se je precej spremenila tudi miselnost oziroma pogled podjetij na varnost; pred leti je večina podjetij gledala na varnost kot na strošek, danes jih večina gleda na varnost kot na investicijo (Tordoff, 2006). Večanje stopnje varnosti je povezano s stroški, zato je pomembno, da podjetje določi ustrezno stopnjo varnosti, sicer lahko za varnost zapravi občutno več denarja, kot je potrebno. Določitev ustrezne stopnje varnosti ni lahka naloga. Podjetja se pri iskanju ustreznih varnostnih rešitev pogosto srečujejo z naslednjimi vprašanji:

- Kako ustrezno zavarovati podjetje in njegova informacijska sredstva?
- Kolikšna stopnja varnosti zadostuje?
- Kako podjetje ve, ali je stopnja varnosti, ki jo ima, ustrezna?
- Kolikšna je prava vsota denarja, ki naj jo podjetje nameni investicijam v varnost?

Do približno leta 2000 se je na informacijsko varnost in iskanje ustrezne varnostne rešitve gledalo predvsem s tehnološkega vidika, ki tudi zadovoljivo odgovori na prvo zgoraj navedeno vprašanje. Če je grožnja na primer virusni program, se podjetje zaščiti tako, da uvede ustrezno programsko rešitev (protivirusni program), ki virusne programe zazna in preprečuje njihovo delovanje. Pred napadi z interneta se podjetja zaščitijo tako, da postavijo požarni zid, ki blokira dostop iz internetnega omrežja v omrežje podjetja in dovoljuje dostop samo po dovoljenih komunikacijskih protokolih. Pri tem je potrebno upoštevati, da so tehnične rešitve le en del celovitega pristopa obvladovanja informacijske varnosti. Drugi, ravno tako pomemben del, je povezan s človeškim faktorjem (za tovrstne zlorabe se uporablja ime socialni inženiring). Nevarnost virusnih programov se na primer precej zmanjša pri ozaveščenih uporabnikih, ki ne odpirajo sumljivih priponk v e-pošti in so bolj pazljivi pri prenosu spletnih vsebin. Najboljša zaščita pred tovrstnimi zlorabami je izobraževanje in osveščanje uporabnikov.

Pri reševanju varnostnih problemov so podjetjem pogosto v pomoč primeri najboljše prakse, preko katerih lahko sorazmerno hitro in cenovno ugodno izvedejo varovanje svojih sredstev. Zavedati se je treba, da zgolj upoštevanje teh priporočil podjetju ne omogoča vzpostavitve optimalne stopnje varnosti, saj priporočila vključujejo neke standardne postopke, ki veljajo za širok nabor podjetij

in ne upoštevajo specifike posameznega podjetja. Primeri najboljše prakse vsebujejo pravilnike, procedure in tehnologije, ki so potrjene s strani industrijskih standardov, kot so na primer International Standards Organization (ISO) 27001, Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC) in Common Criteria for Information Technology Security Evaluation (CCITSE). Upoštevanje različnih standardov, kot so na primer Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBP), Basel II Accord ali Health Insurance Portability and Accountability Act (HIPAA), podjetja dostikrat izberejo tudi zato, da zadostijo zakonodajnim obveznostim (Garcia & Horowitz, 2006; Schneier, 2004b).

Zgolj tehnični pogled na reševanje varnostnih problemov težko celovito reši problematiko informacijske varnosti. Tehnični pogled sicer podaja tehnološke rešitve za zmanjševanje varnostnih groženj, težko pa utemelji, koliko je potrebno v varnost investirati. To pa je v poslovnem svetu zelo pomembno, saj se podjetja želijo prepričati, da je investicija finančno upravičena, še preden se odločijo zapraviti denar za določene varnostne rešitve. Za pravilen pristop k reševanju problema informacijske varnosti je potrebno vključiti tudi ekonomska stališča (Anderson, 2001; Gordon & Loeb, 2001; Camp, 2006; Longstaff, Chittister, Pethia & Haimes, 2000; Gordon, Loeb & Lucyshyn, 2002; Gordon, Loeb & Lucyshyn, 2003).

V zadnjih nekaj letih je močno naraslo zanimanje strokovne javnosti za področje ekonomike informacijske varnosti. Osrednje področje raziskav je usmerjeno na ravnanje z varnostnim tveganjem, ki vključuje tudi oceno optimalnega vlaganja podjetja v varnost in zaščito. Dosedanje raziskave so dale že veliko zanimivih in uporabnih predlogov, vendar se povečini vse omejujejo na ozko področje svojega raziskovanja.

Zavedati se je potrebno, da je ekonomski pristop precej obsežen in zamuden ter predvsem za mala podjetja velikokrat prezahteven. Zahteva namreč poglobljeno analizo in vrednotenje informacijskih sredstev, analizo groženj za informacijska sredstva, analizo posledic nedelovanja informacijske tehnologije, analizo verjetnosti za uspešno izveden napad, analizo učinkovitosti izvajanja varnostne prakse in tehnologij ter oceno stroškov in pridobitev, ki so posledica vlaganj v informacijsko varnost.

Za vrednotenje investicij v informacijsko varnost je bilo predstavljenih nekaj različnih pristopov (Gordon & Loeb, 2002b; Cavusoglu, 2004, str. 71; Herath & Herath, 2006; Huang, Hu & Behara, 2006; Schechter & Smith, 2003; Cremonini & Nizovtsev 2006; Microsoft, 2004). Večina predstavljenih modelov je osredotočena le na določeno področje (npr. analizo varnostnih tveganj, modeliranje groženj ali vrednotenje investicij v varnost) in ne predstavljajo celovite rešitve. Dobro primerjavo o trenutnem dogajanju podaja Schneier (2004a), ki navaja, da je večina raziskovalcev na področju informacijske varnosti tako osredotočena na svoje ozko raziskovalno področje, da vidijo le posamezna drevesa in ne celotnega gozda.

Pomembno vlogo pri oceni vlaganj v varnost ima kvantitativna analiza varnostnih tveganj, ki predstavlja postopek identifikacije in vrednotenja tveganj, katerim je izpostavljeno podjetje (Gordon & Loeb, 2005; ISO 73, 2002; NIST 800-12, 1995). Z analizo tveganj se poskuša določiti numerične vrednosti posameznim komponentam tveganja (verjetnost, da se dogodek zgodi in možna škoda, ki jo ob uspešnem napadu lahko utrpi podjetje) ter varnostnim rešitvam (donosnost in stroški). V ta namen se uporabijo posebni varnostni kazalci, s katerimi se poskuša tveganja čim bolj natančno ovrednotiti (Sonnenreich, Albanese & Stout, 2006).

Ekonomski pristop k reševanju problema informacijske varnosti v poslovnem okolju je osnova te doktorske disertacije, pri čemer je primarno področje mojega raziskovanja obvladovanje varnostnega tveganja in ocena optimalnega vlaganja v informacijsko varnost.

Namen doktorske disertacije je opraviti raziskavo na področju informacijske varnosti z vidika potrebnih vlaganj za preprečitev varnostnih tveganj in potrditi hipotezo o optimalni oceni vlaganj v ustrezno zaščito s pomočjo kvantitativno ovrednotene informacijske varnosti. Ugotoviti nameravam, ali je mogoče kvantitativno vrednotiti tveganja v informacijski varnosti in ali se s pomočjo takšnega vrednotenja lahko izbire optimalna zaščita, ki zmanjšuje varnostna tveganja. Potrebno je razviti metodologijo in celovit matematični model za kvantitativno merjenje informacijske varnosti, ki podjetjem omogoča kvantitativno vrednotenje različnih možnosti investiranja v informacijsko varnost in zaščito. Z investiranjem v informacijsko varnost se zmanjšujejo varnostna tveganja, ki pretijo informacijskim sredstvom v podjetju. Končni cilj modela je izdelati priporočila, ki podjetjem pomagajo pri izbiri ustreznega vlaganja v varnost.

Glavna hipoteza disertacije ($\mathbf{H_1}$) je:

Kvantitativno ovrednotena potreba po informacijski varnosti omogoča oceniti optimalno količino potrebnih vlaganj v varovanje in izbiro ustrezne zaščite v poslovnih okoljih.

Pri tem izpostavim še naslednje teze:

- Problematike informacijske varnosti se ne da učinkovito reševati le s tehničnim pogledom na problem in tehnološkimi rešitvami.
- Kvantitativno medsebojno vrednotenje različnih tehničnih, proceduralnih zaščit s prenosom tveganja na zunanjega izvajalca so možne poti, ki lahko zagotovijo zmanjšanje varnostnih tveganj na najmanjšo možno mero.
- Kazalci, kot so *donosnost investicije* (ROI), *neto sedanja vrednost* (NPV) in *notranja stopnja donosa* (IRR), lahko zagotovijo celovito vrednotenje varnostnih rešitev.
- Ustrezna metodologija za vrednotenje in izbor varnostnih rešitev v poslovnem okolju, ki sloni na kvantitativnih izračunih, omogoča optimalno rešitev pri izbiri sistema za zmanjšanje varnostnih tveganj.

Poleg potrditve glavne hipoteze in ostalih tez, so **cilji** doktorske disertacije še:

- Predstavitev problematike, s katero se ukvarja relativno novo raziskovalno področje *ekonomika informacijske varnosti*.
- Predstavitev in analiza dosedanjih teoretičnih spoznanj, empiričnih spoznanj ter ugotovitev na področju ekonomike informacijske varnosti.
- Pregled dosedanjih dosežkov na področju modeliranja optimalnega vlaganja v informacijsko varnost ter opis njihovih prednosti in slabosti.
- Predstaviti kategorizacijo varnostnih tveganj, groženj in rešitev v informacijsko-komunikacijskem sistemu, ki je v pomoč vrednotenju rešitev.
- Kvantitativno oceniti izgube, ki jih podjetja lahko utrpijo zaradi zlorab, in primerjati te ocene z do sedaj zbranimi empiričnimi podatki.
- Pokazati primere praktične uporabe razvitega matematičnega modela za konkretno podjetje.

Za potrditev tez in dosego ciljev sem moral opredeliti informacijsko varnost in vse njene ključne elemente, se poglobiti v kvantitativni pristop k obvladovanju varnostnih tveganj, se poglobiti v modeliranje vlaganj v informacijsko varnost, razviti metodologijo merjenja informacijske varnosti ter razviti matematični model za oceno vlaganj v varnost in zaščito v poslovnih informacijskih sistemih, ki temelji na kvantitativni analizi varnostnih tveganj. Glavno hipotezo in ostale teze sem v doktorski disertaciji najprej preizkušal na teoretični ravni, v nadaljevanju pa na matematičnih simulacijah ter na empirični ravni za konkretno podjetje.

Pri raziskovalnem delu, namenjenem dokazovanju navedenih tez, sem uporabil več različnih metod dela. V uvodnem teoretičnem delu sem proučeval literaturo s področja ekonomike informacijske varnosti. Pri tem sem uporabil deskriptivni pristop, v okviru katerega sem uporabil naslednje metode:

- **metodo deskripcije,** s pomočjo katere opišem teorijo, pojme ter ugotovljena dejstva,
- **metodo klasifikacije**, kjer definiram pojme, ki jih razlagam v nadaljevanju in so predmet raziskovanja v nalogi,
- **metodo komparacije**, kjer primerjam dela in raziskave različnih avtorjev,
- **metodo kompilacije**, kjer s povzemanjem spoznanj in sklepov drugih avtorjev v zvezi z izbranim raziskovalnim problemom oblikujem nova stališča.

V nadaljevanju teoretični del nadgradim z analitičnimi metodami in empiričnimi ugotovitvami, ki so objavljene v različnih raziskavah in poročilih (CSI, 2009; DSCI, 2009; DTI, 2006). Na koncu naredim sintezo ugotovitev in analiz preteklih študij in raziskav.

Tekom raziskovalnega dela sem v tuji literaturi naletel na strokovne izraze s področja informacijske varnosti. Za mnoge izmed njih v slovenščini že obstaja primeren izraz, ki se uporablja v strokovnih krogih (Islovar, 2010; Wikipedia,

2010). Pri nekaterih izrazih sem opazil različne prevode v slovenščino. Na primer izraz *integrity* ponekod prevajajo kot *celovitost* (Palsit, 2010; SiQ, 2008), drugod kot *neokrnjenost* (Wikipedia, 2010; Housing, 2010). V teh primerih sem se odločil za uporabo tistega izraza, za katerega sem ocenil, da je v slovenščini bolje sprejet in se širše uporablja. Izkaže se, da izraz *management* 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 in Slovenskega inštituta za standardizacijo sem izraz *information security management* prevajal kot *vodenje informacijske varnosti* ter izraz *risk management* prevajal kot *obvladovanje tveganja*. Odločil sem se tudi za drugačen prevod izraza *asset*, ki sem ga v doktorski dispoziciji prevajal kot *vir*, v doktorski disertaciji pa ga pravilneje prevajam kot *sredstvo*, besedo vir pa uporabljam za prevod izraza *resource*. Srečal sem se tudi z izrazi, za katere v slovenščini nisem našel že uveljavljenega prevoda. Te izraze sem prevedel sam.

V svojem raziskovalnem delu sem združil dosedanja spoznanja in ugotovitve, jih povezal v celoto in uporabil za izhodišče raziskovanja. Doktorska disertacija je strukturirana tako, da vodi od splošnega spoznavanja informacijske varnosti do analize tveganja ter nadaljuje z razvojem matematičnega modela, njegovega preizkušanja in prikaza njegove praktične uporabe.

Doktorsko disertacijo sestavlja devet poglavij. V uvodnem poglavju je predstavljen kratek opis ožjega znanstvenega področja, obravnavani problem, predmet raziskovanja, namen in cilji disertacije, temeljna hipoteza in ostale teze ter opredeljene metode dela doktorske disertacije.

V prvem poglavju so predstavljeni osnovni principi informacijske varnosti ter najpogostejše težave pri reševanju varnostnih vprašanj, s katerimi se srečujejo vodje informacijske varnosti ali varnostni strokovnjaki v poslovnem okolju. Predstavljeni so najpomembnejši standardi na področju informacijske varnosti ter organizacije, ki uveljavljajo standarde. Navedene so omejitve, na katere naletimo, če varnost poskušamo reševati zgolj s tehnologijo, ter analiza potrebe po ekonomskem pristopu k informacijski varnosti. Predstavljeni so začetki ekonomike informacijske varnosti ter prednosti takega pristopa.

Drugo poglavje je namenjeno obvladovanju varnostnih tveganj. Predstavljen je proces ravnanja s tveganji, ki se začne z oceno tveganja in nadaljuje z izbiro ustrezne obravnave tveganja. Poglavje zaključujem s pregledom obstoječih metod in tehnik za obvladovanje varnostnih tveganj.

Tretje poglavje se osredotoča na informacijska sredstva in grožnje. Predstavljeni so zadnji najpomembnejši raziskovalni dosežki na tem področju. Poglavje se začne z analizo informacijskih sredstev v poslovnem okolju in nadaljuje z analizo groženj, ki so usmerjena na ta sredstva. Analiza ranljivosti predstavlja razloge in načine, kako lahko grožnje zlorabijo sredstva. Uspešna grožnja rezultira v varnostni incident, ki za podjetje predstavlja določeno izgubo. Poglavje se zaključuje z

merjenjem izgub v primerih varnostnega incidenta ter empiričnimi rezultati na tem področju.

Četrto poglavje analizira varnostne ukrepe ter predstavlja teoretične modele za določanje optimalne stopnje investicije v informacijsko varnost. Navedeni so načini, kako z ekonomskim pristopom izbiramo ustrezne varnostne ukrepe in merimo njihovo donosnost.

Razvoj matematičnega modela za izbiro optimalne investicije v informacijsko varnost je predstavljen v petem poglavju. Model je zasnovan kot standarden postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro ustrezne rešitve, ki bo zmanjšala določeno varnostno tveganje. Model omogoča podjetjem, da se lahko na podlagi končnih rezultatov in priporočil odločijo, katera izmed varnostnih rešitev je za določen tip grožnje in njihove potrebe optimalna. Za razliko od do sedaj predstavljenih modelov za vrednotenje investicij, pri večini katerih je bil poudarek na iskanju optimalne stopnje investicije (Gordon & Loeb, 2002b; Huang et al., 2006; Cremonini & Nizovtsev 2006), predlagani model omogoča neposredno primerjavo in kvantitativno vrednotenje različnih varnostnih ukrepov. Varnostni ukrepi za zmanjšanje tveganja so lahko uporaba tehnoloških varnostnih rešitev, uvedba varnostnih postopkov, izobraževanja in prenos tveganja na zunanje podjetje (zavarovalnice ali gostovanja storitev). Prenos tveganja na zavarovalnico se šele uveljavlja, saj zavarovalnice povečini še nimajo izdelanih ustreznih produktov, ki bi pokrivali področje informacijske varnosti (Majuca et al. 2006; Böhme & Kataria, 2006; Gordon, Loeb & Sohail, 2003; Ogut, Menon & Ragunathan, 2005). Ključno vodilo pri razvoju modela je bilo, da je model čim bolj vsestranski, da podpira različne vrste groženj ter omogoča vrednotenje različnih varnostnih rešitev. Obenem sem v modelu poskušal čim bolj zajeti realno stanje in upoštevati čim več faktorjev, ki pri določitvi tveganj in izbiri varnostne rešitve vplivajo na poslovanje podjetja. Zavedati se je potrebno, da vsaka varnostna rešitev pomeni na drugi strani tudi omejevanje funkcionalnosti, kar lahko vpliva tudi na poslovanje podjetja. Zato je pomembno, da podjetje oceni, kako bo uvedena varnostna rešitev vplivala na produktivnost in poslovanje podjetja (Sonnenreich, 2006), saj je to lahko ključnega pomena, ali bo na koncu uvedena varnostna rešitev imela pozitiven učinek na poslovanje podjetja (Schneier, 2004a). V model sem vključil tudi klasifikacijo varnostnih tveganj in groženj, ki omogoča boljšo preglednost nad tveganji in izborom ustreznih varnostnih rešitev.

V šestem poglavju se model preverja z matematičnimi simulacijami in tako preizkuša njegovo splošno veljavnost in uporabnost.

V sedmem poglavju je predstavljena praktična uporaba modela na primeru za konkretno podjetje. Izvedeni empirični analizi za varnostni tveganji računalniški virus in ohromitev informacijskih storitev predstavljata empirično potrditev modela.

V zaključku so strnjeni rezultati in glavne ugotovitve doktorske disertacije. Izpostavljen je predviden znanstveni prispevek doktorske disertacije. Navedene so možnosti in predlogi za morebitne nadaljnje raziskave na tem področju ter izboljšave modela.

1 Informacijska varnost

Informacija predstavlja za podjetje vrednost na več različnih načinov (Gordon & Loeb, 2005, str. 5). Lahko pomaga podjetjem do večje produktivnosti, boljšega marketinga in boljših finančnih odločitev. Lahko pomaga nadzorovati aktivnosti in procese ali pomaga pri ravnanju z zaposlenimi. Za zagotavljanje običajnih dnevnih transakcij, povezanih z nakupom in prodajo, je ključno varovanje informacij o ceni, specifikaciji produkta in informacij o nakupu. Pri modelih elektronskega poslovanja podjetja s podjetjem *(*angl. *business to business*, *B2B),* podjetja s potrošnikom *(*angl. *business to consumer*, *B2C)* in podjetij z upravo *(*angl. *business to government*, *B2G)* se vsi sodelujoči zanašajo na varne prenose informacij med partnerjema in varno hrambo zaupnih informacij. Ključna je vzpostavitev zaupanja med partnerjema pri elektronskih transakcijah.

Informacije, vezane na običajne dnevne poslovne transakcije in širok nabor ostalih vrst informacij, predstavljajo ključna strateška sredstva v današnjem podjetju. Primeri takih strateških informacij vsebujejo med drugim tudi: informacije o skrivnih receptih, produkte v razvoju, marketinške načrte, združitve in prevzeme, osebje in demografijo strank. Take strateške informacije so ključne za razvoj in rast podjetja. Vrednost teh informacij je povezana tudi z nivojem varnosti informacij.

Schechter (2004) definira **varnost** kot:

> *"Proces prepoznave dogodkov, ki imajo potencial, da povzročijo škodo in uvedba ukrepov za zmanjšanje tega potenciala."*

Poenostavljeno povedano, varnost je proces varovanja pred poškodbo ali namerno škodo. Varnost tudi določa ukrepe, ki jih proces uvede. Za varovanje informacij in informacijskih sistemov se je uveljavil izraz informacijska varnost (angl. *information security*, *cybersecurity*). **Informacijska varnost** je (Peltier, 2001):

> *"Proces varovanja vrednih informacijskih sredstev pred neavtoriziranim dostopom, uporabo, razkritjem, motnjami, spremembo in uničenjem."*

Različni standardi uporabljajo podobne definicije za informacijsko varnost. Standard ISO/IEC 27002 (2005) definira informacijsko varnost kot:

> *"Ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij, poleg tega tudi ohranjanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost."*

Ameriški zvezni standard 1037C (1996) podaja naslednjo definicijo informacijske varnosti:

> *"Zaščita informacij pred nepooblaščenim razkritjem, prenosom, spremembo ali uničenjem, ne glede na to ali so namerne ali po nesreči."*

Poleg izraza informacijska varnost se pogosto uporablja tudi izraz računalniška varnost (angl. *computer security*, *IT security*). Informacijska varnost je osredotočena na zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij, ne glede na to v kakšni obliki se podatki nahajajo (npr. elektronski, tiskani ...). Računalniška varnost je osredotočena na zagotavljanje razpoložljivosti in ustreznega delovanja računalniškega sistema, ne osredotoča pa se na informacije, ki so shranjene ali pa se obdelujejo na računalniku.

Informacijska varnost je sorazmerno nov pojem. Potreba po zaščiti vrednih informacij pa je stara toliko kot samo človeštvo. Začetki varovanja informacij segajo v čas 50 let p.n.š., ko naj bi Julij Cezar iznašel in uporabljal šifrirni sistem za zaščito vsebine sporočil, če bi slučajno prišli v roke sovražnikom (Singh, 2006). Druga svetovna vojna je prinesla mnogo pomembnih izboljšav na področju varovanja podatkov z mehanskim šifriranjem (enigma) ter kriptoanalizo in tako zaznamovala začetek profesionalnega področja informacijske varnosti. Konec 20. stoletja je zaznamoval hitri napredek telekomunikacij, računalniške strojne in programske opreme ter posledično varovanja podatkov. Informacijska varnost je postala večnivojska, od visokonivojskih politik in postopkov do nizkonivojskih šifrirnih algoritmov. Pokriva mnoga področja, od varovanja omrežja in infrastrukture, varovanja aplikacij in podatkovnih zbirk, varnostnega testiranja, revizije informacijskih sistemov, planiranja neprekinjenega poslovanja, do digitalne forenzike in drugih področij.

Čeprav zamisel o varovanju informacij ni nova, se poslovna praksa na tem področju še vedno precej razvija. Pri tem tehnološki napredek po eni strani spodbuja, po drugi strani pa otežuje njegov napredek (Soo Hoo, 2000). Informacijska doba, ki je omogočila hitro širjenje digitalnih tehnologij in računalniških omrežij, je temeljito spremenila prakso varovanja informacij. Z razvojem tehnologij, ki podjetjem omogočajo obdelavo, hrambo in prenos digitalnih podatkov v širšem smislu, je postalo še toliko bolj pomembno vprašanje, kako ohraniti informacije podjetja ali posameznika varne (Dhillon & Backhouse, 2000, str. 125; Dhillon & Backhouse, 2001, str. 127; Whitman, 2003; Boss, 2007). Po drugi strani uporaba računalniških sistemov in omrežij prinaša razna tveganja, kot so na primer okvara opreme, človeški faktor, odprtost omrežij in druga tveganja, na katera je potrebno biti pozoren.

Učinkovita arhitektura informacijske varnosti je sestavljena iz petih komponent, ki predstavljajo osnovo varnega okolja. Te komponente so (Tudor, 2000):

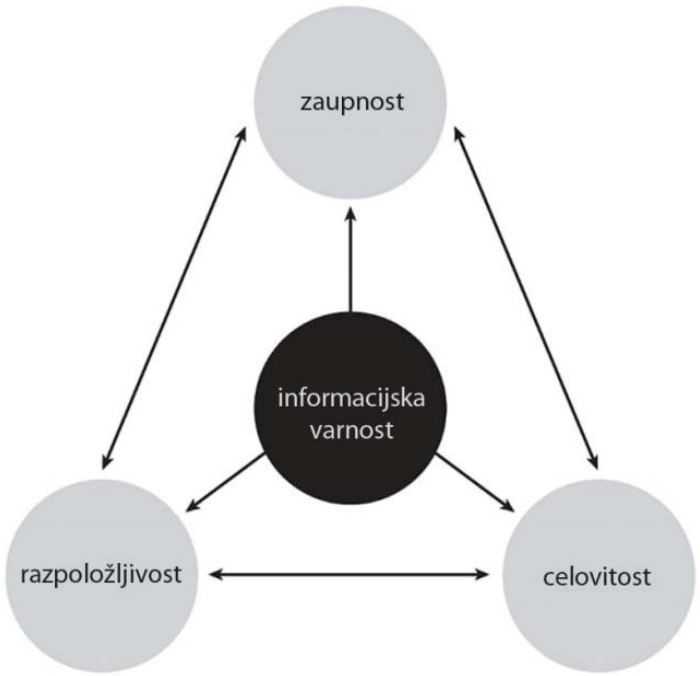
- infrastruktura,
- politike, standardi in postopki,
- izobraževanje in ozaveščanje uporabnikov,
- skladnost,
- ocenjevanje varnosti.

Te komponente morajo biti podprte z ustrezno tehnologijo, metodami in programi, da zagotavljajo, da so informacije zanesljive, razpoložljive in ustrezno dostopne.

1.1 Osnovni principi informacijske varnosti

Že več kot dvajset let osnovne principe informacijske varnosti predstavljajo zaupnost, celovitost in razpoložljivost (angl. *confidentiality*, *integrity* in *availability*) (Pfleeger, 1989)[1]. Po začetnicah ter principov v angleščini se pogosto uporablja naziv CIA triada, kar je shematično prikazano na sliki 1. Poleg osnovnih principov zaupnosti, celovitosti in razpoložljivosti so še drugi principi, ki jih informacijska varnost upošteva.

***Slika 1**: Shematični prikaz CIA triade*



[1] Pfleeger sicer namesto zaupnosti uporablja izraz tajnost (angl. *secrecy*). Izraz zaupnost se je splošno uveljavil kasneje.

Zaupnost informacij

Zaupnost je preprečitev nepooblaščenega ali nenamernega razkritja informacij. Standard ISO/IEC 13335-1 (2004) definira zaupnost kot:

> *"Lastnost, ko informacija ni na voljo ali razkrita nepooblaščenim posameznikom, osebam ali procesom."*

Kot primer zlorabe zaupnosti lahko navedem zlorabo kreditne kartice pri transakcijah preko interneta. Pri postopku te transakcije je potrebno številko kreditne kartice prenesti od kupca k prodajalcu in od prodajalca do omrežja za obdelavo transakcij. Zaupnost podatkov se lahko v tem primeru doseže s šifriranjem številke kartice med prenosom, z zmanjševanjem mest, kjer se podatek lahko hrani (npr. podatkovne baze, dnevniki, varnostne kopije, tiskani računi itd.) ter omejevanjem dostopa do mest, kjer se podatek hrani. V kolikor nepooblaščena oseba na kakršenkoli način pridobi številko kartice, to pomeni zlorabo zaupnosti.

Zaupnost predstavlja jedro vseh varnostnih politik v podjetju, ki določajo, kateri posameznik ima dostop do določenih informacij (DOD, 1985). Zloraba zaupnosti je lahko namerna ali nenamerna (povzročena po nesreči). Na primer razkritje zaupnih podatkov je lahko posledica namernega poskusa zlonamerne osebe ali nenamerna, kot posledica napake v programu ali človeške napake. Informacije se lahko nepooblaščeno pridobi 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.

Za varovanje zaupnosti informacij v elektronski obliki se pri hrambi ali prenosu informacij uporablja šifriranje informacij, ki dovoli dostop do vsebin samo uporabniku z ustreznim šifrirnim ključem. Ker je simetrična kriptografija 1000- do 10.000-krat hitrejša od asimetrične kriptografije (Schneier, 1994), se za šifriranje podatkov uporabljajo simetrični šifrirni algoritmi, npr. Advanced Encryption Standard (v nadaljevanju AES) (FIPS 197, 2001).

Za zagotavljanje zaupnosti in preverjanja pristnosti za e-pošto se najpogosteje uporabljata mehanizma Pretty Good Privacy (v nadaljevanju PGP) in Secure/Multipurpose Internet Mail Extensions (v nadaljevanju S/MIME). Prvo različico PGP je razvil Phil Zimmermann leta 1991 (Singh, 2006). PGP se uporablja za zagotavljanje zasebnosti e-pošte in digitalno podpisovanje datotek. S/MIME je podoben PGP, glavna razlika med njima je v načinu izmenjave ključev. Pri osnovnem PGP si vsak uporabnik sam izmenja ključe z vsemi možnimi prejemniki in tako vzpostavi obroč zaupanja vrednih prejemnikov. S/MIME uporablja za izmenjavo ključev hierarhično potrjena digitalna potrdila, običajno v formatu X.509. Pri S/MIME tako pošiljatelju kot prejemniku ni potrebno predhodno izmenjati ključev, če uporabljata certificiranega izdajatelja digitalnih potrdil, ki mu

zaupata oba. S/MIME je IETF standard postal leta 1999 z različico 3 (RFC 3850, 2004).

Celovitost informacij

Celovitost pomeni, da se podatki ne morejo spremeniti brez avtorizacije. Standard ISO/IEC 13335-1 (2004) definira celovitost kot:

> *"Lastnost varovanja pravilnosti in popolnosti sredstev."*

Primeri zlorabe celovitosti so, če zaposleni namenoma ali pomotoma izbriše pomembne informacije, če računalniški virus okuži računalnik, če lahko zaposleni sam popravlja znesek na svoji plačilni listi, če lahko nepooblaščena oseba spremeni vsebino na spletni strani podjetja itd.

Celovitost temelji na zaupanju informacij in se običajno nanaša na preprečevanje nepravilne ali nepooblaščene spremembe. Celovitost vključuje celovitost informacij (vsebina informacij) in celovitost izvora – verodostojnost (vir informacij) (Farahmand, 2004). Ravnanje s celovitostjo se precej razlikuje od ravnanja z zaupnostjo. Zaupnost podatkov je lahko ogrožena ali pa ne, celovitost pa vključuje pravilnost in verodostojnost informacij. Na celovitost informacij vpliva izvor informacij, kako in od koga so bile pridobljene, kako dobro so bile informacije zaščitene preden so prišle v sedanji sistem in kako dobro so varovane informacije v sedanjem sistemu.

Mehanizmi za varovanje celovitosti informacij so razvrščeni v dva razreda: mehanizmi za preprečevanje zlorabe celovitosti in mehanizmi za odkrivanje zlorabe celovitosti. Mehanizmi za preprečevanje zlorabe celovitosti poskušajo ohraniti celovitost informacij z blokiranjem vseh nepooblaščenih poskusov spreminjanja informacij ali kakršen koli poskus spreminjanja informacij v nepooblaščene namene. Mehanizmi za odkrivanje zlorabe celovitosti ne poskušajo preprečiti kršitve celovitosti, temveč zgolj poročajo, da celovitost informacij ni več vredna zaupanja. Celovitost informacij v elektronski obliki se običajno zagotavlja s kontrolno vsoto, ki se jo dobi z uporabo enosmerne zgoščevalne (angl. *hash*) funkcije npr. SHA-1 (FIPS 180-3, 2008) ali MD5 (RFC 1321, 1992). Za večjo varnost je zaželeno, da je rezultat zgoščevalne funkcije (t. i. izvleček) dodatno šifriran ali pa se uporabi zgoščevalna funkcija s ključem (angl. *Hash-based Message Authentication Code, HMAC*) (Yener, 2003; RFC 2104, 1997).

Razpoložljivost storitev

Razpoložljivost pomeni, da je storitev ali sistem na voljo, ko se potrebuje. Standard ISO/IEC 13335-1 (2004) definira razpoložljivost kot:

> *"Lastnost, ko je nekaj dostopno in uporabno na zahtevo pooblaščene osebe."*

Primer zlorabe razpoložljivosti je ohromitev storitve (angl. *Denial of Service*, v nadaljevanju *DoS*). Ta napad na informacijski sistem ima za cilj onesposobiti delovanje sistema ali storitev. Zloraba razpoložljivosti je lahko tudi nenamerna, kot na primer prekinitev dobave infrastrukturnih storitev (elektrike, vode, telekomunikacijskih storitev itd.) zaradi različnih težav ponudnikov.

Za zaščito razpoložljivosti se v zadnjem času pogosto uvaja upravljanje neprekinjenega poslovanja (angl. *Business Continuity Management - BCM*), ki vključuje dobre prakse in priporočila (BS 25999-1, 2006). Ena izmed rešitev je razpršeno izvajanje storitev na več geografsko ločenih lokacijah.

Verodostojnost

Standard ISO/IEC 13335-1 (2004) definira verodostojnost (angl. *authenticity*) kot:

> *"Lastnost, ki zagotavlja, da je identiteta osebe ali sredstva, tista za katero se izdaja."*

Verodostojnost se nanaša na osebe, procese, sisteme in informacije. Na verodostojnost se pogosto gleda kot na podmnožico celovitosti ali razpoložljivosti (Gordon & Loeb, 2005, str. 10; FISMA, 2002).

Verodostojnost se dokazuje skozi proces **overjanja**. Pri preverjanju verodostojnosti osebe je overjanje povezava identitete na 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 (npr. geslo ali zaupne informacije)?
- Kaj oseba ima (npr. kartico)?
- Kaj oseba je (npr. biometrija, prstni odtis, značilnosti mrežnice)?
- Kje se oseba nahaja (npr. pri določenem terminalu)?

Proces overjanja je sestavljen iz pridobivanja informacij za overjanje s strani osebe, analiziranja podatkov in ugotavljanj ali so podatki povezani s to osebo. Največkrat se za preverjanje uporablja kar uporabniško ime in geslo, na voljo pa so tudi bolj varni mehanizmi, npr. digitalna potrdila (RFC 2459, 1999). Ločimo med enosmernim overjanjem, kjer le sistem preveri pristnost uporabnika, in dvosmernim, ki zahteva, da tudi uporabnik preveri pristnost sistema.

Primera mehanizmov za overjanje sta X.509 in Kerberos. Mehanizem X.509 določa algoritem za preverjanje pristnosti in opredeljuje digitalna potrdila. Kerberos je splošno sprejet protokol za preverjanje pristnosti, ki je bil razvit leta 1980 in se uporablja predvsem v notranjih sistemih odjemalec-strežnik (Stalling, 1999; RFC 1510, 1993). Temelji na Needham-Schroeder avtentikacijskem protokolu (Needham & Schroeder, 1978). Avtentikacijski strežnik je Key Distribution Center

(KDC), ki uporabnikom izdaja vstopnice (angl. *ticket*). Uporabnik ob prvi prijavi v sistem od KDC prejme svojo vstopnico, s katero lahko dostopa do različnih storitev.

Neovrgljivost

Standard ISO/IEC 13335-1 (2004) definira neovrgljivost (angl. *non-repudiation*) kot:

> *"Zmožnost za dokazovanje akcije ali dogodka, ki se je zgodil, na način, da dogodek ali akcija kasneje ne more biti zanikana."*

Neovrgljivost preprečuje zanikanje posredovanega sporočila bodisi s strani pošiljatelja bodisi prejemnika (Farahmand, 2004). Prejemnik lahko dokaže, da je domnevni pošiljatelj dejansko poslal sporočilo. Podobno lahko pošiljatelj dokaže, da je sporočilo dejansko prejel domnevni prejemnik. Pogosto se za neovrgljivost uporabljajo digitalni podpisi, ki uporabljajo asimetrične šifrirne algoritme, npr. RSA (Rivest, Shamir & Adleman, 1978).

Podobno, kot na verodostojnost, se tudi na neovrgljivost pogosto gleda kot na podmnožico celovitosti ali razpoložljivosti (Gordon & Loeb, 2005, str. 10; FISMA, 2002).

Nadzor dostopa

Standard ISO/IEC 13335-1 (2004) definira nadzor dostopa (angl. *access control*) kot:

> *"Zmožnost zagotovitve, da je dostop do sredstev avtoriziran in omejen glede na poslovanje in varnost."*

Da bi dosegli ta nadzor, je potrebno vsako osebo, ki želi pridobiti dostop, predhodno identificirati ali overiti, tako da se lahko pravice za dostop prilagodijo.

Vsako podjetje mora določiti svoje varnostne prioritete. To pomeni, da za vsak poslovni proces določi obseg, v katerem določi zahteve po zaupnosti, celovitosti in razpoložljivosti. Zavedati se je potrebno, da so cilji informacijske varnosti pogosto v nasprotju drug z drugim (Gordon & Loeb, 2005, str. 10). Za spletno knjigarno je na primer najpomembnejša razpoložljivost, da zavaruje poslovanje. To lahko doseže s postavitvijo več strežnikov na različne geografske lokacije. S tem pa tudi poveča možnosti za napade na svoj sistem, s čimer dodatno ogrozi zaupnost in celovitost podatkov. Drugi primer je vladna obveščevalna služba, ki je pripravljena žrtvovati razpoložljivost na račun zaupnosti, s katero varuje svoje skrivnosti (Ioannidis, Pym & Williams, 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.

Razni modeli in standardi različno vključujejo in povezujejo principe informacijske varnosti med seboj. Standard ISO 7498-2 (1989) navaja sledeče varnostne principe za boj proti varnostnim grožnjam:

- overjanje,
- zaupnost podatkov,
- nadzor dostopa,
- celovitost podatkov,
- neovrgljivost.

Standard ISO 13335-1 (2004) navaja, da morajo varnostni cilji, strategije in politike naslavljati sledeče probleme informacijske varnosti:

- zaupnost,
- celovitost,
- razpoložljivost,
- odgovornost (angl. *accountability*),
- verodostojnost,
- zanesljivost (angl. *reliability*).

Parker (2009) je CIA triado razširil v Parkerjevo heksado, da je zaupnosti, celovitosti in razpoložljivosti dodal še nadzor dostopa, verodostojnost ter uporabnost informacij (angl. *utility*).

1.2 Težave pri reševanju varnostnih vprašanj

1.2.1 Zavedanje o informacijski varnosti

Informacijska varnost je področje, za katerega se zanimanje hitro povečuje. Podjetja se čedalje bolj zavedajo, da je varnost eden izmed osnovnih elementov vsakega informacijskega sistema. Farahmand (2004) je mnenja, da informacijska varnost ni ločeno področje od informacijske tehnologije, temveč je vidik, kako je informacijska tehnologija specificirana, načrtovana, razvita, nameščena in vzdrževana. Vidik varnosti mora biti vključen v življenjski cikel produkta ali storitve že od samega začetka. Varnosti se namreč ne da kar enostavno vključiti v sistem, ko je okolje informacijske tehnologije že uvedeno. Informacijska varnost ni lastnost produkta ali storitve, temveč je lastnost okolja.

Schneier (2004a) zato poudarja, da varnost ni produkt, temveč je proces. Produkti dajejo določeno zaščito, vendar je edini način za učinkovito poslovanje in

prepoznavanje potencialnih nevarnosti procesni pristop. Ključno je, da se podjetje zaveda realnih groženj sistema, načrtuje varnostno politiko in uvede varnostne kontrole, ki grožnje preprečujejo.

1.2.2 Mit popolne varnosti

Zavedati se je potrebno, da popolnoma varen sistem ne obstaja. Zlonamerni uporabniki (hekerji[2]) bodo vedno našli naprednejši način za dostop do informacij. Pri tem so tisti, ki napadajo sistem vedno v prednosti pred tistimi, ki sistem branijo (Sunzi, 2009). Branitelj mora braniti vse točke, medtem ko bo napadalec izbral najšibkejšo točko. Branitelj mora biti stalno na preži, napadalec pa bo napadel, ko se bo njemu zdel ustrezen čas. Branitelj lahko brani samo tisto, kar pozna, napadalec pa lahko preuči vse ranljive točke in izbere tisto, ki njemu ustreza.

Michael Howard, manager varnostnega programa znotraj Microsoft Security Engineering Team, je opisal problem informacijske varnosti takole:

> *"Lahko stanujete v najbolj varni soseski, vendar ko enkrat priklopite tisti kabel na internet, takrat se znajdete v najhujši možni soseski."*

Gene Spafford, direktor Computer Operations, Audit and Security Technology (COAST) Purdue University, opisuje, kakšen naj bi bil popolnoma varen sistem (Bowen, 2002, str. 302):

> *"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."*

Kako varen je sistem? Kako varen bi moral biti sistem? To sta dve vprašanji, ki si jih strokovnjaki na področju varovanja informacij neprenehoma zastavljajo (Schechter, 2004). Na vprašanje kakšno stopnjo varnosti želimo imeti, Sandhu (2003) enostavno odgovarja: dovolj dobro varnost. Geer (2004a) ob tem dodaja, da je zelo težko določiti, kaj je dovolj dobro. Popolno varnost se torej lahko razume kot stopnjo varnosti, ki je za podjetje sprejemljiva (Schneier, 2003).

[2] Heker (angl. *hacker*) je splošno gledano tehnično dobro podkovan računalniški zanesenjak. V doktorski disertaciji uporabljam izraz heker za zlonamernega uporabnika, ki poskuša z vdiranjem v računalniške sisteme odkriti zaupne ali občutljive podatke. Za tovrstne zlonamerne uporabnike se pogosto uporablja tudi izraz kreker oziroma vdiralec (angl. *cracker*).

1.2.3 Vpliv kompleksnosti sistemov na varnost

Informacijski sistemi so in bodo čedalje bolj kompleksni (Schneier, 2004a; Perrow, 1999). S stališča kupca je kompleksnost vsekakor dobra. Za njega to pomeni več izbire, več možnosti, več stvari, ki jih lahko naredi. S stališča varnosti pa je to slabo, saj se z večanjem kompleksnosti sistemov njihova varnost zmanjšuje. Razlogov za negativni vpliv kompleksnosti sistemov na varnost je veliko:

- Mnogi hrošči v programski opremi vplivajo na varnost.
- Kompleksni sistemi so zaradi obsežnosti modularni in povečini niso združeni vnaprej. Obsežnost prinaša varnostne luknje, ker varnost velikokrat odpove, ko moduli med seboj sodelujejo.
- Testiranje kompleksnih sistemov je težje. Bolj je sistem kompleksen, več varnostnih napak bo imel. Preverjanje vseh možnih konfiguracij je v kompleksnih sistemih praktično nemogoče.
- Razumevanje kompleksnih sistemov je težje.
- Analiziranje kompleksnih sistemov je težje.

Kompleksni sistemi imajo več pomanjkljivosti, modularna zgradba to samo poveča, težje je testirati, težje je razumeti in težje je analizirati. Schneier (2004a) poudarja, da je varnost celotnega sistema tolikšna kot varnost najšibkejšega člena. To pomeni, da ena ranljivost lahko uniči celoten sistem. Schneier vidi rešitev problema vse manjše varnosti zaradi vse bolj kompleksnih sistemov v vključevanju varnosti v procese.

1.2.4 Pomen človeških virov na informacijsko varnost

Kakšen pomen imajo človeški viri na informacijsko varnost, predstavimo s sledečim primerom. Če bi tehničnega strokovnjaka (npr. sistemskega inženirja) vprašali, zakaj je varnost potrebna, bi navedel različne grožnje, od nedelovanja spletne strani, okvare ali izgube podatkov, ohromitve storitve, do virusov in trojanskih konjev. Na vprašanje kako tveganje zmanjšamo, bi sistemski inženir najprej pomislil na to, kako lahko z varnostno tehnologijo grožnje preprečimo. To je tradicionalna paradigma informacijske varnosti, kjer se najprej ugotovi, kaj so grožnje in nato naredi tehnologijo, da se grožnje preprečijo. Pri tem se predpostavlja, da lahko tehnologija reši informacijsko varnost. Končni rezultat takega pristopa je največkrat varnostni program, ki je običajno drag in omejuje poslovanje. Ta paradigma je napačna. Ne obstaja noben magični računalniški varnostni produkt, ki bi informacijsko okolje enostavno naredil varno.

Informacijska varnost vključuje tehnologijo in ljudi. Gonzalez in Sawicka (2002) ugotavljata, da je sicer tehnološki napredek čedalje bolj impresiven, vendar je vse bolj očitno, da je človeški dejavnik Ahilova peta informacijske varnosti. Tudi Germain (2007) navaja, da je človek še vedno najšibkejši člen varnosti. Raziskava o

zlorabah na bankomatih v Veliki Britaniji je pokazala, da so skoraj vsi incidenti povzročeni zaradi človeške napake, ne zaradi težav s tehnologijo (Anderson, 1993, str. 215). Schneier (1996) se je leta 1994 v svoji knjigi o uporabi kriptografije močno zavzemal, da je visoka stopnja varnosti v naših rokah. Toda šest let pozneje je v svoji drugi knjigi to trditev preklical: *"Če mislite, da lahko tehnologija reši vaše varnostne težave, potem ne razumete niti problemov niti tehnologije."* (Schneier, 2004a, str. xii). Ter nadaljuje: *"Jaz potencialnim strankam povem, da je matematika brezhibna, da so računalniki ranljivi, da so omrežja zanič in da so ljudje brezmejno neumni. Sam sem se naučil veliko o problemih varovanja računalnikov in omrežij, vendar nobeden resnično ne pomaga rešiti človeškega problema."* (Schneier 2004a, str. 255). Varnost je torej predvsem človeški problem, ne tehnološki.

Učinkovito reševanje informacijske varnosti je odvisno od tehničnih rešitev in človeških virov. S tehnične strani mora podjetje uporabiti ustrezno kombinacijo sredstev, kot na primer šifrirne tehnike, požarni zidovi, nadzor dostopa in sistemi za zaznavanje vdorov (angl. *intrusion detection system*, v nadaljevanju *IDS*). Tehnične rešitve so za podjetja najenostavnejše za uvedbo in upravljanje, niso pa vedno najučinkovitejše (Dhillon & Backhouse, 2000, str. 125). Poleg tega so za zagotovitev ustrezne ravni varnosti potrebni še človeški viri, ki znajo te tehnične rešitve pravilno uporabiti za zaščito informacij pred zlorabami (Gordon & Loeb, 2005, str. 10; Boss, 2007).

Straub (1990) je v svoji študiji, ki je zajela 1211 podjetij, ugotovil, da je ozaveščanje (npr. uvedba politik in postopkov) o varnosti bolj učinkovito kot tehnične rešitve. Večinoma se vodstvo podjetij ne zaveda dovolj pomena informacijske varnosti. Čeprav uvedba raznih politik za varovanje informacij narašča (BERR, 2008), večina podjetij še vedno nima uvedenega sistematičnega pristopa k informacijski varnosti, ki bi omogočal uvedbo politik in postopkov (Whitman, 2003). Po drugi strani pa so večkrat tudi pravila in postopki v varnostnih politikah prezapleteni in se jih težko uvede v realno poslovanje (Dhillon & Backhouse, 2000). To pogosto pripelje do neupoštevanja varnosti, ker se zaradi pomanjkanja ozaveščenosti zaposlenih le-ti ne zavedajo dovolj pomena varnosti (Hughes & DeLone, 2007).

Zato je zelo pomembno stalno izobraževanje in ozaveščanje zaposlenih. Zlonamerni uporabniki z raznimi pretvezami, tehnika se imenuje socialni inženiring (angl. *social engeeniring*), od uporabnika pridobijo razne podatke, ki jim omogočajo vdor v sistem. Še posebno pozornost je potrebno nameniti navadnim posameznikom, ne zgolj tehničnim strokovnjakom za varnost, ter vodstvenim kadrom. Ključno je ozavestiti vodstvo podjetja, da se zaveda pomena informacijske varnosti (Dutta & McCrohan, 2002). Vodstvo se mora zavezati k uvedbi učinkovitih varnostnih politik in postopkov ter motivirati posameznike, da spoštujejo in se ravnajo v skladu s politikami (National Cyber Security Alliance, 2005). Še posebej je pomembno, kako posameznik deluje preventivno ter kako je za tako ravnanje motiviran (Boss, 2007). V situaciji, ko posamezniki niso motivirani za spoštovanje

varnostnih pravil, celotna varnost odpove (Campbell, 2000; CERT, 2004; Coren, 2005; Dhillon & Backhouse, 2000).

1.2.5 Vodenje informacijske varnosti

Ker je informacijska varnost sorazmerno nova poslovna funkcija v podjetju, se naziv in vloga managerjev, ki so odgovorni za to funkcijo, razlikuje od podjetja do podjetja (Gordon & Loeb, 2005). V večini podjetij imajo težave z umestitvijo človeških virov, ki delujejo na področju varnosti.

V nekaterih podjetjih ni določenega posebnega delovnega mesta za informacijsko varnost. V takih podjetjih je običajno za celotno področje informacijske tehnologije odgovoren vodja informatike (angl. *Chief Information Officer*, v nadaljevanju *CIO*). Za njega je informacijska varnost zgolj ena od mnogih zadolžitev, med katerimi so tudi vsakodnevne aktivnosti upravljanja računalnikov in omrežij, IT izobraževanja, izbira strojne ter programske opreme itd.

Nekatera podjetja imajo vodjo varnosti (angl. *Chief Security Officer*, v nadaljevanju *CSO*), ki je zadolžen za varovanje vseh sredstev (npr. za poslopje, avtomobile, podatke, programsko opremo ter strojno opremo). Za njega predstavlja informacijska varnost zgolj eno izmed področij, za katera je odgovoren.

Čedalje več podjetij pa ima vodjo informacijske varnosti (ang. *Chief Information Security Officer*, v nadaljevanju *CISO*), ki je primarno zadolžen za informacijsko varnost v podjetju. V večini podjetij je služba za informacijsko varnost znotraj IT oddelka in je CISO odgovoren direktno CIO. Taka organizacija v podjetju lahko pripelje do konflikta interesov. CIO zagovarja razvoj informatike, nove funkcionalnosti, integracijo z ostalim okoljem itd. CISO pa želi čim manj sprememb, saj vsaka sprememba lahko predstavlja novo varnostno tveganje. Germain (2005) zato priporoča, da je CISO izven IT oddelka ter da sta tako CIO kot CISO tudi člana uprave podjetja. V zadnjem času narašča število podjetij, ki vlogo CISO postavlja izven sektorja informatike, tako da CISO odgovarja vodji financ (angl. *Chief Financial Officer*, v nadaljevanju *CFO*) ali celo izvršnemu direktorju (angl. *Chief Executive Officer*, v nadaljevanju *CEO*).

1.2.6 Dilema med varnostjo in uporabnostjo

Informacijska varnost se dotika vsakega zaposlenega v podjetju, saj običajno omejuje njegovo svobodo po prosti uporabi tehnologije v polnem obsegu. V tem tiči osnovni konflikt med varnostjo in uporabnostjo. Varnost in funkcionalnost sistema sta si med seboj nasprotujoči. Če se izboljša varnost sistema, se s tem omeji njegova funkcionalnost (Schneier, 1996). Informacijska varnost zahteva, da se informacije in dostop do njih ustrezno obvladuje in nadzoruje, 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.

1.3 Pregled standardov na področju informacijske varnosti

Farahmand (2004) ugotavlja, da imajo podjetja težave s prepoznavanjem groženj, ki pretijo njihovim informacijskim sredstvom, ter kako se z grožnjami spopasti. Sookdawoor (2005) zato priporoča, da je za ustrezno izvajanje informacijske varnosti, dobro poznati najboljše prakse in jih uporabljati kot vodilo pri uvedbi. V pomoč so lahko mnogi mednarodni standardi s področja informacijske varnosti (ISO 27001, 2005; ISO 13335-1, 2004; NIST 800-27, 2004; NIST 800-30, 2002). Varnostni standardi in priporočila pomagajo posameznikom pri zmanjševanju tveganja in učinkovitejšem upravljanju sistemov in omrežij (Tudor, 2000). Standardi imajo lahko velik vpliv na uvedbo varnostnih tehnologij. Če se standardov ne upošteva pri uvedbi tehnologij, lahko to vpliva tako na stroške kot na obseg tveganja, saj se na ta način lahko porabi več energije za izpolnjevanje varnostnih ciljev podjetja (Farahmand, 2004).

1.3.1 Organizacije

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

- **ISO**: International Organization for Standardization
- **BSI**: British 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

1.3.2 Standardi

Standarde in priporočila s področja informacijske varnosti se lahko razdeli na več področij: obvladovanje tveganja, najboljša praksa, produktno usmerjeni standardi, smernice in procesno usmerjeni standardi.

Obvladovanje tveganja

- ISO/IEC Guide 73 (2002). Vodič definira slovar obvladovanja tveganja in priporočila za uporabo v ISO standardih. Osredotočen je na terminologijo.
- AS/NZS 4360 (2004). Avstralsko-novozelandski standard podaja splošen pristop k obvladovanju tveganja in je sestavljen iz petih večjih korakov: vzpostavitve konteksta, prepoznavanja tveganja, analize tveganja, ocenitve in rangiranja tveganja, določitve ustreznih ukrepov. Predlaga pregled nad terminologijo in procesom obvladovanja tveganja.
- ISO/IEC 27005 (2008) standard podaja metodologijo obvladovanja tveganja, ki je prvenstveno namenjena pomoči pri uvedbi standarda ISO/IEC 27001(2005).
- Razne metode za obvladovanje tveganja (OCTAVE, CRAMM, EBIOS, MEHARI itd.).[3]

Najboljša praksa

- ISO/IEC 27001 (2005) *"Sistemi vodenja varovanja informacij – Zahteve"* in ISO/IEC 27002 (2005) *"Kodeks za vodenje varovanja informacij"*. Cilj teh dveh standardov je ponuditi model za vzpostavitev, uvedbo, upravljanje, nadzor, pregled, vzdrževanje in izboljšave sistema vodenja varovanja informacij (v nadaljevanju SVVI) (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 preko interneta.
- Information Technology Infrastructure Library (ITIL) je zbirka najboljše prakse s področja obvladovanja IT storitev, ki vključuje tudi področje varnosti.

Produktno usmerjeni standardi

- ISO/IEC 15408 (2008) ali Common Criteria ponuja nabor zahtev za varnostne funkcije v IT produktih in sistemih, ki se jih mora izpolnjevati. "*Common Criteria for Information Technology Security Evaluation*", ki se pogosto označuje kar s "*CC*", je mednarodni standard za pomoč razvijalcem, ocenjevalcem in kupcem varnostnih produktov (Farahmand, 2004).

Smernice

- ISO/IEC 13335-1 (2004) standard je prvi v seriji priporočil ISO/IEC 13335. Ukvarja se z načrtovanjem, upravljanjem in uvedbo informacijske varnosti. Prvi del predstavlja koncepte in modele, ki se lahko uvedejo v različne organizacije.

[3] Metode za obvladovanje tveganja so podrobneje predstavljene v poglavju 2.2.2.

- NIST 800-27 (2004) in NIST 800-30 (2002). 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 navaja 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).

Procesno usmerjeni

- ISO/IEC 21827 (2008) določa ključne karakteristike procesa varnostnega inženiringa v organizaciji.
- CobiT – Control Objectives for IT (ISACA) 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.

1.3.3 Standardi družine ISO 27000

Leta 2000 je International Organisation for Standardisation (ISO) objavila standard ISO/IEC (International Electrotechnical Commission) 17799:2000, *"Kodeks za vodenje varovanja informacij"*. Standard ISO 17799 je bil razvit na osnovi standarda BS7799 organizacije British Standards Institution (BSI). Cilj standarda ISO 17799 je omogočiti podjetjem zmanjšanje tistih IT groženj, ki izhajajo iz fizičnih okvar, zlorab in industrijskega vohunjenja. Namen ISO 17799 je, kot navaja ISO, "*zagotoviti skupno osnovo za razvoj standardov za varovanje organizacij in učinkovito prakso vodenja varnosti in za zagotovitev zaupanja v medorganizacijsko poslovanje*".

Leta 2002 je bila izdana revizija BS 7799 (Part 2). Namen BS 7799-2 je bil uskladitev z ostalimi standardi, ki pokrivajo sisteme vodenja. Postavil je specifikacije za vodenje informacijske varnosti in priporočila za vzpostavitev učinkovitega SVVI.

Standard ISO 27001 je bil objavljen konec leta 2005 kot zamenjava BS7799-2. ISO 27001 je mednarodno sprejet standard najboljše prakse vodenja informacijske varnosti in je kompatibilen z ostalimi upravljavskimi standardi, kot sta družini ISO

9000 in ISO 14000. Standard temelji na seznamu 130 kontrol v 11 poglavjih, ki jih morajo organizacije izpolnjevati. Poglavja so:

- varnostna politika,
- organizacija varovanja informacij,
- upravljanje sredstev,
- varovanje človeških virov,
- fizična zaščita in zaščita okolja,
- upravljanje s komunikacijami in s produkcijo,
- nadzor dostopa,
- nakup, razvoj in vzdrževanje informacijskih sistemov,
- ravnanje z incidenti pri varovanju informacij,
- upravljanje neprekinjenega poslovanja,
- združljivost.

Standardi ISO/IEC 27000 so rezervirani za družino standardov vodenja informacijske varnosti. Nekateri standardi iz družine še niso objavljeni[4].

- ISO/IEC 27000 (2009) podaja pregled družine ISO 27000 standardov in slovar izrazov, ki se uporablja v družini.
- ISO/IEC 27001 (2005) je standard, ki določa zahteve sistema vodenja varovanja informacij (SVVI), in specifikacije po katerih se lahko organizacije certificirajo.
- ISO/IEC 27002 (2005) je kodeks za vodenje varovanja informacij, ki podaja nabor varnostnih kontrol, sprejetih kot dobra praksa.
- ISO/IEC 27003 (predvidena objava v letu 2010) bo podajal pomoč pri uvedbi standarda ISO/IEC 27001.
- ISO/IEC 27004 (2009) je standard, ki predlaga kazalce za pomoč pri izboljšavi učinkovitosti SVVI.
- ISO/IEC 27005 (2008) je standard za obvladovanje varnostnega tveganja.
- ISO/IEC 27006 (2007) je vodič za postopek certificiranja.
- ISO/IEC 27007 (še ni objavljen) bo vodič za revizijo SVVI s poudarkom na vodenju sistema.
- ISO/IEC 27008 (še ni objavljen) bo vodič za revizijo SVVI s poudarkom na varnostnih kontrolah.
- ISO/IEC 27010 (še ni objavljen) bo SVVI vodič za komunikacijo med oddelki
- ISO/IEC 27011 (2008) je SVVI vodič za telekomunikacijske organizacije (standard je tudi objavljen kot ITU X.1051).
- ISO/IEC 27013 (še ni objavljen) bo vodič za integracijo uvedb ISO/IEC 20000-1 (izhaja iz ITIL) in ISO/IEC 27001.
- ISO/IEC 27014 (še ni objavljen) bo pokrival vodenje informacijske varnosti.

[4] Podatki o objavi so z dne 1.1.2010.

- ISO/IEC 27015 (še ni objavljen) bo SVVI vodič za finančne organizacije in zavarovalnice.
- ISO/IEC 27031 (še ni objavljen) bo osredotočen na neprekinjeno poslovanje.
- ISO/IEC 27032 (še ni objavljen) bo vodič za internetno informacijsko varnost.
- ISO/IEC 27033 (še ni objavljen) bo nadomestil večdelni standard ISO/IEC 18028 za IT mrežno varnost.
- ISO/IEC 27034 (še ni objavljen) bo vodič za varnost aplikacij.
- ISO/IEC 27035 (še ni objavljen) bo nadomestil ISO TR 18044 za ravnanje z varnostnimi incidenti.
- ISO/IEC 27036 (še ni objavljen) bo vodič za zunanje izvajanje varnosti.
- ISO 27799:2008 podaja specifične zahteve standarda ISO/IEC 27002 za zdravstveni sektor.

1.3.4 Empirične ugotovitve

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

- Velika potreba po izobraževanju s področja varnosti in ozaveščanja vseh zaposlenih.
- V splošnem se investicije v varnostne projekte 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 ukrepanja. Ključna negativna spoznanja so:

- Neskladnost z informacijsko varnostno politiko, standardi in predpisi.
- Obstaja veliko primerov, kjer varnostna politika ni ustrezno opredeljena.
- Pomanjkanje prizadevanja za merjenje in sledenje varnostnih projektov.
- Če obstajajo varnostne politike, je bilo ugotovljeno, da niso bile redno vzdrževane.
- Pravila in postopki v varnostnih politikah so pogosto prezapleteni in se jih težko uvede v realno poslovanje.
- Nekatere raziskave so pokazale nizko zavezanost najvišjega vodstva v določenih področjih uvedbe varnosti.

Po raziskavi BERR (2008) ima 11 % podjetij uveden standard ISO 27001 (2005), medtem ko je bilo leta 2002 takih podjetij le 5 %. Ista raziskava tudi ugotavlja, da

kar 79 % podjetij ne pozna vsebine standarda ISO 27001. Razveseljujoče je, da kar 40 % podjetij izvaja izobraževalne programe za zaposlene s področja informacijske varnosti.

1.4 Ekonomski pristop k varnosti

1.4.1 Zakaj ekonomski pristop

Pred desetletjem je bilo splošno prepričanje, da internetno okolje ni varno zaradi tehnoloških pomanjkljivosti, pomanjkanja kriptografskih tehnik, overjanja, filtriranja mrežnih paketov itd. Zato so varnostni inženirji pospešeno delali na tehničnem področju in izboljševali kriptografske algoritme (na primer AES), postavljali infrastrukture javnih ključev (angl. PKI), izboljševali požarne pregrade itd. Leta 1999 so se nekateri raziskovalci s področja informacijske varnosti začeli zavedati, da tak pristop ne zadostuje ter da je informacijska varnost področje, ki se ga ne da uspešno rešiti zgolj s tehnologijo, temveč je potrebno upoštevati tudi ekonomijo.

Ross Anderson (2001) trdi, da so neprimerne spodbude za ustvarjanje ne-varnega sistema povzročile toliko škode kot tehnološke pomanjkljivosti. Anderson (1993, str. 215) in Hal Varian (2000) opisujeta, kako varnost spodleti v primeru, da posamezniki, ki varujejo sistem, niso tudi tisti, ki morajo plačati posledice zaradi nedelovanja ali spodletele varnosti. Gordon in Loeb (2005, str. 2) sta mnenja, da odločitve v informacijski varnosti pogosto temeljijo na instinktu v trebuhu, namesto na ekonomski analizi. Vendar se podjetja čedalje bolj zavedajo, da zgolj tehnični vidik ne zadostuje za razumevanje nenehno razvijajočega se varnostnega okolja (Anderson & Moore, 2006, str. 610; Frei, Schatzmann, Plattner & Trammell, 2009).

Izdatki v informacijsko varnost so pod čedalje večjim nadzorom. Varnostni oddelki si prizadevajo za obvladovanje tveganja, povezanega z rastjo elektronskega poslovanja ter za svoje vse večje proračunske potrebe (Su, 2006). Gordon in Loeb (2002a) ugotavljata, da za zaščito zaupnosti, celovitosti in razpoložljivosti informacij podjetja investirajo velike vsote denarja v aktivnosti s področja informacijske varnosti. Ker se investicije v varnost potegujejo za sredstva, ki se lahko porabijo tudi na drugih področjih, finančni direktor (CFO) pogosto zahteva racionalni ekonomski pristop za take izdatke. Varnostni managerji so zato za večje investicije prisiljeni narediti poslovni primer. V preteklosti se je na varnostne investicije pogosto gledalo kot na operativne stroške. Pristop s poslovnim primerom pa so v zadnjih letih spodbudili pogosti varnostni incidenti in s tem povezani stroški kot tudi svetovne gospodarske razmere.

Podjetja, ki se zavedajo pomena informacijske varnosti, se pri odpravi možnih težav osredotočajo na to, kar je ekonomsko optimalno, namesto na to, kar je tehnično mogoče (Schneier, 2004a; Anderson, 2001; Anderson & Schneier, 2005, str. 12). Ekonomski pristop bolje razloži varnostne težave. Danes postajata teorija iger in mikroekonomska teorija tako pomembni za varnostne inženirje, kot sta bili pred četrt stoletja matematika in kriptografija (Anderson & Moore, 2008).

Vodstvenim kadrom z dobrim poznavanjem prava in ekonomije predstavlja uporaba ekonomskega izrazoslovja boljše razumevanje problema, kot pa tehnični jezik informacijske varnosti (Swire, 2001). Managerji lahko na ta način bolje razumejo investicije v varnostne rešitve, ker je povzročena škoda ob varnostnih incidentih predstavljena kot finančna izguba ter ne več zgolj kot tehnična analiza (Bojanc & Jerman-Blažič, 2008a, str. 413).

1.4.2 Prednosti ekonomike informacij

Ko se na informacijsko varnost gleda z ekonomskega vidika, se lahko dobi odgovore na mnoga vprašanja, na katera zgolj tehnologija ne more zadovoljivo odgovoriti (Bojanc & Jerman-Blažič, 2007, str. 216). Večina osnovnih varnostnih vprašanj je vsaj toliko ekonomskih kot tehničnih. Podjetja si pogosto zastavljajo sledeča varnostna vprašanja:

- Kako lahko podjetje postane varno?
- Katera stopnja varnosti je ustrezna?
- Koliko denarja naj podjetje investira v varnost?
- Ali podjetje zapravi dovolj denarja, da hekerjem preprečuje vdor v računalniški sistem?
- Ali podjetje zapravi preveč?
- Ali podjetje zapravi varnostni proračun za ustrezne stvari?

Ekonomski pogled lahko razloži tudi konkretnejša vprašanja s področja informacijske varnosti. Na primer, zakaj so požarni zidovi danes nekaj običajnega, šifriranje e-pošte pa se ni prijelo? Anderson in Schneier (2005, str. 12) ugotavljata, da to ni zaradi relativne učinkovitosti tehnologije, temveč zaradi ekonomskih pritiskov, ki vodijo podjetja v uvedbo. Podjetja redko objavljajo informacije o vdorih v njihov sistem ravno zato, ker ekonomske "spodbude" temu nasprotujejo.

Uporaba ekonomskega pristopa k obvladovanju varnostnih tveganj omogoča podjetjem vpeljavo optimalnih varnostnih rešitev (Gordon & Loeb, 2005). Podjetja lahko na ta način ocenijo posledice, ki nastanejo zaradi neuvedbe določene varnostne rešitve. Podjetja si lahko odgovorijo na vprašanja, koliko pomanjkanje varnostne rešitve stane njihovo poslovanje, kakšen vpliv ima lahko pomanjkanje varnosti na produktivnost ter kakšne so lahko posledice katastrofalnega napada na

podjetje (Sonnenreich, 2006). Podjetja lahko tudi ocenijo, katera izmed rešitev, ki jih imajo na voljo, ima najboljše razmerje med ceno in kakovostjo (Locher, 2005).

1.4.3 Začetki ekonomike informacijske varnosti

Ekonomika informacijske varnosti se je začela skoraj sočasno na različnih koncih (Camp, 2006). Leta 2000 so raziskovalci na Computer Emergency Response Team (v nadaljevanju CERT) predstavili osnutek mehanizma za oceno tveganja. Hierarhični holografski model je predstavljal prvo večplastno ocenjevalno orodje za pomoč pri investicijah v varnost z upoštevanjem tveganja (Longstaff et al., 2000). CERT je v nadaljevanju razvil sistematični mehanizem OCTAVE, ki različno velikim podjetjem pomaga pri oceni tveganja. Le malo pred tem sta Camp in Wolfram (2000) na Harvardski univerzi objavili ekonomske definicije za opredelitev specifične "dobrine", ki je danes splošno veljaven medij pri izmenjavah v različnih teoretičnih varnostnih modelih. Definirali sta trg ranljivosti, ki se je v naslednjih letih potrdil kot veljaven. 3Com je oktobra 2005 od nekega hekerja kupil ničdnevni izkoristek (angl. *zero-day exploit*)[5] (Espiner, 2005). Odkritje ničdnevnega izkoristka potrjuje tudi Microsoft (Wang et al., 2006).

Leta 2001 je Ross Anderson (2001) iz univerze Cambridge objavil članek "*Why Information Security is Hard: An Economic Perspective*", v katerem pojasni težave pri optimalnem razvoju varnostnih tehnologij, pri katerih je nujno potrebno v tehnične modele vključiti ekonomske posledice. 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 nujno s tehničnimi ukrepi ali zgolj štetjem denarja za investicije, temveč s sistematično analizo donosnosti investicije.

Ross Anderson in Hal Varian sta vodila prvo letno konferenco Workshop on the Economics of Information Security (WEIS), ki se od leta 2002 dalje odvija vsako leto. WEIS je konferenca, kjer se srečujejo tehnologi, ekonomisti in odvetniki ter skupaj poskušajo razumeti težave informacijske varnosti (Schneier, 2006). Na WEIS konferencah se obravnava različna področja, med njimi:

- oceno optimalnega vlaganja v varnost in zaščito,
- ranljivosti, varnostne popravke in razkritja varnostnih incidentov,
- modeliranje informacijskih groženj,
- obvladovanje varnostnih tveganj,
- zavarovalništvo in informacijsko varnost,
- varnostne modele in kazalce,

[5] Običajno štetje dni izkoristka je od objave ranljivosti do zlorabe. Ničdnevni izkoristek je taka ranljivost, ki do takrat še ni bila poznana.

- ekonomiko zasebnosti,
- ekonomiko ravnanja z digitalnimi pravicami (angl. *Digital Rights Management - DRM*).

1.4.4 Ekonomika trga IT produktov in storitev

Anderson (2008) v analizi trga IT produktov in storitev z ekonomskega stališča, ugotavlja nekaj pomembnih karakteristik trga.

Prva karakteristika je pomen omrežja, kjer vrednost omrežja narašča s številom uporabnikov. Po Metcalfejevem zakonu je vrednost omrežja enaka kvadratu števila uporabnikov. Ta efekt omrežja vodi k trgu dominantnega podjetja, kjer zmagovalec pobere vse (Anderson 2008, str. 221).

Druga karakteristika so visoki fiksni stroški in majhni mejni stroški (angl. *marginal costs*). V konkurenčnem okolju naj bi bila cena informacije enaka mejnim stroškom proizvodnje. Ta pa je skoraj nič. To razloži, zakaj je na internetu na voljo toliko informacij zastonj. Če dva ali več proizvajalcev ponujajo programsko opremo (na primer operacijski sistem, enciklopedijo ali zemljevide), ki jo lahko razmnožujejo praktično brez stroškov, lahko znižujejo ceno izdelka brez omejitve. To otežuje povrnitev kapitalnih investicij, razen v primeru, če se podjetje zaščiti s patenti, trgovsko znamko, kompatibilnostjo itd. Podjetja so morala prilagoditi poslovni model, v katerem so dobrine na voljo zastonj, denar pa dobijo preko oglaševanja ali drugih virov. Veliko podjetij z visokimi fiksnimi stroški in nizkimi mejnimi stroški se je premaknilo na oglaševalski ali storitveni model (Anderson, 2008).

Tretja karakteristika je drag prehod med ponudniki. Če podjetje želi na primer preiti iz Windows operacijskega sistema na Linux sistem, to predstavlja izobraževanje zaposlenih, reprogramiranje aplikacij itd. Shapiro in Varian (1998) navajata, da je neto sedanja vrednost podjetja, ki razvija programsko opremo, enaka skupnim stroškom zamenjave. Podjetja zato podrobno analizirajo stroške zamenjave. Na primer, če imam predvajalnik iPod, ki je vreden 300 € in sem preko Applove spletne trgovine kupil za 5.000 € glasbe, sem "zaklenjen" na proizvajalca Apple.

Vse te karakteristike vodijo k trgu dominantnih podjetij, kjer imajo prvi na tržišču veliko prednost. Zato je pravočasen prihod na tržišče kritičen. Anderson (2001) pojasnjuje, da je filozofija Microsofta (tj. ponudijo izdelek čim prej ter ga nato s popravki dopolnjujejo in popravljajo) s tega stališča čisto racionalna. Nadalje Anderson ugotavlja, da to ne velja samo za Microsoft, ki ga mnogi imenujejo "veliki zlobni", temveč bi vsako podjetje, ki bi dobilo prevladujoč položaj na trgu operacijskih sistemov, ravnalo enako.

V tej bitki, kdo bo prvi dobil prevlado nad tržiščem, proizvajalci posvečajo varnosti premalo pozornosti že na začetku. Anderson (2001) in drugi so trg varne

programske opreme označili kot trg za limone. Nobelov nagrajenec za ekonomijo George Akerlof (1970, str. 488) je uporabil metaforo prodaje rabljenih avtomobilov za trg nesimetričnih informacij in ga poimenoval trg za limone. Predpostavimo, da ima mesto 100 rabljenih avtomobilov v prodaji, od tega jih je 50 dobrih za ceno 5.000 € in 50 slabih za ceno 1.000 €. Katera je ravnovesna cena za rabljene avtomobile? Če bi bila 3.000 €, se ne bi prodal noben dober avtomobil, ker bi bila za prodajalce ta cena prenizka. Trg za limone je tisti trg, v katerem potrošniki ne morejo ločiti kakovostnih proizvodov od pomanjkljivega blaga ali limon. V takem trgu je proizvajalčeva prevladujoča strategija prodajati limone, ker je za proizvajalca to ceneje, potrošniki pa morajo zato domnevati, da je vsak prodajan proizvod lahko limona (Schechter, 2004). 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 iz trga, zaradi tistih, ki proizvajajo limone po nižji ceni.

Varnost programske opreme je težko izmeriti in uporabniki težko razlikujejo med bolj varnimi in manj varnimi produkti (Anderson, 2001). Stroški dodajanja dobre varnosti v programsko opremo so veliki, medtem ko so stroški zanemarjanja varnosti manjši (Schneier, 2004a). Ker prodajalci ne morejo učinkovito zaračunati stroška za dodatno varnost, uporabniki niso pripravljeni za to plačati. Zato imajo proizvajalci majhen interes za povečanje varnosti svojih proizvodov. Ko neko podjetje pridobi prevladujoč položaj na tržišču, proizvajalec dodaja večjo varnost v svoje produkte, vendar na način, da čim bolj veže stranke na svoje produkte (Anderson, 2003). Kako je mogoče to rešiti? Raziskovalci predlagajo dva pristopa merjenja varnosti programske opreme: tržišče ranljivosti in zavarovanje (Anderson & Moore, 2008).

Večja varnost ni nujno vedno boljša. Prvi primer so banke, ki bi lahko izboljšale varnost tako, da bi varnostniki osebno preiskali vsakega, ki bi vstopil. Vendar pa bi ob taki uvedbi najbrž ostale brez velikega števila svojih strank. Drugi primer so trgovine, ki povečini sprejemajo tveganje kraje kot sprejemljivo. Po raziskavah se največ kraj v trgovinah z oblačili zgodi v garderobah. Varnost bi sicer lahko izboljšali tako, da bi odstranili garderobe, vendar bi lahko to pomenilo precej manjšo prodajo. Zato vsa podjetja iščejo ustrezno stopnjo varnosti za sprejemljive stroške (Schneier, 2004a).

2 Obvladovanje varnostnih tveganj

Standardi navajajo različne definicije za **tveganje** (angl. *risk*) (Mayer, Heymans & Matulevičius, 2007). V nadaljevanju predstavljam pregled in analizo različnih definicij tveganja. Standard za obvladovanje tveganja ISO Guide 73 (2002) podaja sledečo definicijo tveganja:

> *"Tveganje je kombinacija verjetnosti za dogodek in njegove posledice."*

Standard za obvladovanje tveganja AS/NZS 4360 (2004) tveganje definira podobno:

> *"Tveganje je možnost, da se zgodi nekaj, kar bo imelo učinek na cilje."*

Obe definiciji podajata, da je tveganje sestavljeno iz dveh elementov: dogodka oziroma nečesa, kar se zgodi, in posledice.

Standard ISO/IEC 27000 (2009) povzema definicijo tveganja po ISO Guide 73 (2002), dodatno pa definira še tveganje v zvezi z informacijsko varnostjo (angl. *information security risk*):

> *"Možnost, da bo določena grožnja izkoristila ranljivosti sredstva ali skupino sredstev ter povzročila škodo podjetju."*

Varnostni standard ISO/IEC 27001 (2005) samega izraza tveganje ne definira v svojem slovarju, pod identifikacijo tveganja pa standard navaja:

> *"Prepozna tveganja.*
> *1) Prepozna sredstva, ki so zajeta v SVVI, in lastnike teh sredstev.*
> *2) Prepozna grožnje tem sredstvom.*
> *3) Prepozna ranljivosti, ki jih lahko izrabijo te grožnje.*
> *4)Prepozna posledice, ki jih imajo lahko izguba zaupnosti, celovitosti in razpoložljivosti na sredstva."*

ISO 15408 (Common Criteria - CC) definira tveganje še bolj natančno:

> *"Grožnje predstavljajo možnost zlorabe varovanih sredstev. CC okarakterizira grožnjo in povzročitelja grožnje, metodo domnevnega napada, ranljivosti, ki so osnova za napad, in identifikacijo napadenega sredstva. Ocena tveganja za vsako grožnjo oceni verjetnost, da takšna grožnja postane dejanski napad, verjetnost da je takšen napad uspešen in posledice kakršnekoli škode, ki lahko nastane."*

Standarda NIST 800-27 (2004) in NIST 800-30 (2002) ravno tako navajata svojo definicijo tveganja:

> *"Tveganje:*
> *(1) verjetnost, da se bo določen vir grožnje udejanjil ali sprožil, zlasti ranljivost informacijskega sistema,*
> *(2) posledica učinka, če bi se to zgodilo,*
> *(3) metode za obvladovanje varnostnih tveganj."*

Svoje definicije za tveganje podajajo tudi različne metode za obvladovanje tveganja. EBIOS definira tveganje:

> *"Kombinacija grožnje in izgub, ki jih lahko povzroči."*

OCTAVE ponudi sledečo definicijo tveganja:

> *"Tveganje se nanaša na situacijo, kjer bi lahko oseba naredila nekaj neželenega, ali pa naravni pojav, ki lahko povzroči neželene rezultate, kar ima negativen učinek ali posledice. To se razčleni v tri osnovne elemente: sredstva, grožnje in ranljivosti."*

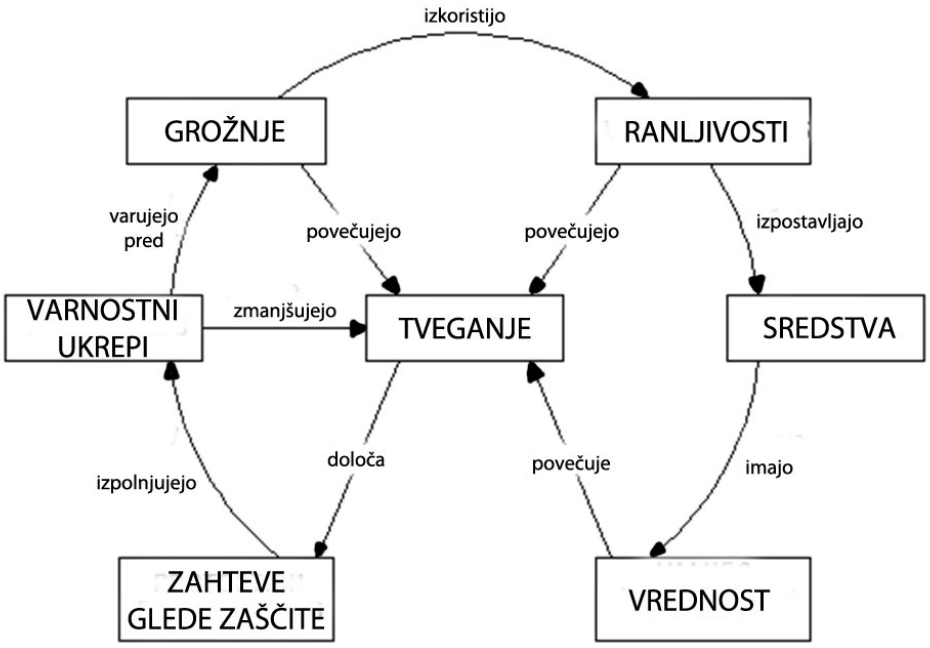
Zelo podobno definicijo tveganja podaja tudi CRAMM:

> *"Kazalec izpostavljenosti, ki mu je podvržen sistem ali podsistem. Ta je določen s kombinacijo:*
> • *stopnjo ogroženosti,*
> • *ranljivostjo,*
> • *morebitno izgubo, ki lahko nastane zaradi takega napada."*

Pri vseh definicijah se tveganje nanaša na negotovost potencialno škodljive ponovitve dogodka. Varnostno tveganje je kombinacija grožnje z eno ali več ranljivostmi, kar pripelje do negativnega učinka, ki škoduje enemu ali več sredstvom. Grožnje in ranljivosti so del vzroka tveganja, učinek pa je posledica tveganja (Mayer et al., 2007). Na primer heker uporabi socialni inženiring na zaposlenem (tj. grožnjo), kar zaradi slabega ozaveščanja zaposlenih (tj. ranljivosti) pripelje do neavtoriziranega dostopa do računalnikov in izgube zaupnosti in celovitosti občutljivih informacij (tj. učinka oziroma posledice).

Obvladovanje tveganja uvaja osnovne varnostne elemente: sredstva, grožnje, ranljivosti, tveganja, ukrepe. Slika 2 prikazuje odvisnosti med varnostnimi elementi, ki sodelujejo pri ravnanju s tveganjem.

Slika 2: *Povezave med elementi, ki sodelujejo pri ravnanju s tveganjem*



Vir: ISO 13335-1, 2004

2.1 Proces obvladovanja tveganja

S tveganjem se podjetja lahko soočajo na različne načine. V grobem ločimo dva pristopa:

- Izogibanje grožnjam oziroma t. i. vojaški model. Pri tem je varnost brezpogojna (absolutna), ugotovi se grožnje in se jim izogne. Sta samo dve stanji, in sicer si varen ali nisi varen.
- Obvladovanje tveganja oziroma t. i. poslovni model. Pri tem je varnost relativna, tveganj je veliko, ravno tako različnih rešitev. Za reševanje tveganja obstaja več načinov.

V literaturi informacijske varnosti se **obvladovanje tveganja** (angl. *risk management*) običajno nanaša na generični proces, ki se ukvarja z ravnanjem, oziroma natančneje z zmanjševanjem tveganja. Standard za obvladovanje tveganja ISO Guide 73 (2002) podaja sledečo definicijo obvladovanja tveganja:

> *"Usklajene dejavnosti za usmerjanje in nadzor organizacije ob upoštevanju tveganja."*

Vodnik za obvladovanje tveganja sistemov informacijske tehnologije NIST 800-30 (2002) definira obvladovanje tveganja kot:

> *"Postopek ugotavljanja tveganja, ocenjevanje tveganja in sprejetje ukrepov za zmanjšanje tveganja na sprejemljivo raven."*

Obvladovanje tveganja je celoten proces obvladovanja izpostavljenosti podjetja negotovosti s posebnim poudarkom na identifikaciji, nadzoru in odpravljanju ali minimiziranju negotovih dogodkov, ki lahko potencialno preprečijo podjetju dosego zastavljenih ciljev (Gordon & Loeb, 2005; NIST 800-12, 1995). Postopek zahteva identifikacijo in oceno informacijskih sredstev podjetja, oceno posledic varnostnih incidentov, oceno verjetnosti uspešnih napadov na informacijske sisteme ter oceno poslovnih stroškov in koristi investicij v varnost (Soo Hoo, 2000).

Danes so mnoga podjetja že spoznala, da je informacijska varnost bolj v domeni vodenja (tj. načrtovanje, usmerjanje, koordinacija, nadzor porabe sredstev za dosego zastavljenega cilja) kot tehnike (Gordon & Loeb, 2005). Podjetja že obvladujejo različne vrste tveganj. Tveganja, povezana z informacijsko varnostjo, so le še ena dodatna vrsta tveganja. Obstaja veliko različnih načinov za obvladovanje tveganja. Kateri se bo izbral v dani situaciji, je odvisno od podrobnosti same situacije. Schechter (2004) ugotavlja, da se napake pri ravnanju s tveganjem neprestano dogajajo, veliko podjetji napačno ravna s tveganji in za napake plača. Podjetja, ki delujejo na področju varnosti, želijo napovedati tveganje za sistem in učinkovitost različnih varnostnih strategij za zmanjševanje teh tveganj. S stališča podjetja je varnost investicija, ki se meri v prihrankih denarnih enot (npr. v evrih). Zato v podjetjih funkcija ravnanja s tveganjem pogosto prevzame nalogo modeliranja varnosti.

Proces ravnanja s tveganjem je sestavljen iz posameznih faz, preko katerih lahko identificiramo ranljivosti informacijskega sistema v podjetju, ovrednotimo trenutno možne varnostne zaščite, sprejmemo odločitve glede še sprejemljivega tveganja in izberemo najbolj ustrezno stroškovno učinkovito zaščito (Farahmand, 2004). Cilj procesa so stroškovno učinkovite zaščite, ki ne stanejo več, kot je pričakovana izguba ob napadu. Proces obvladovanja tveganja običajno sestavljata dve glavni fazi: ocena tveganja ter obravnava tveganja.

2.1.1 Ocena tveganja

Ocena tveganja je proces odločanja, ali obstoječe zaščite zadostujejo za varovanje informacijskih sredstev pred verjetnimi grožnjami (Denning, 1999). Standard ISO Guide 73 (2002) definira oceno tveganja (angl. *risk assessment*) kot:

> *"Celoten proces analize tveganja in vrednotenja tveganja."*

Nadalje podaja definicijo za analizo tveganja (angl. *risk analysis*):

> *"Sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja." (ISO Guide 73, 2002)*

Standard definira tudi vrednotenje tveganja (angl. *risk evaluation*):

> *"Proces primerjave ocenjenega tveganja z danimi kriteriji tveganja, da se določi pomembnost tveganja." (ISO Guide 73, 2002)*

Proces ocene tveganja vključuje identifikacijo sredstev, ki jih je potrebno varovati, grožnje, ki so uperjene na ta sredstva, verjetnost za grožnjo, identifikacijo ranljivosti, ki jih je mogoče izkoristiti ter oceno izgub, ki nastanejo v primeru napada. Poenostavljeno povedano, ocena tveganja je proces določitve potencialne škode za posamezno tveganje ter verjetnosti, da se bo dogodek zgodil (Bojanc & Jerman-Blažič, 2008a, str. 413).

Cilj ocene tveganja je identifikacija in merjenje tveganja z namenom informiranja procesa odločanja. Ocena tveganja potrebuje podatke o informacijskih sredstvih v podjetju, grožnjah, ki so jim sredstva izpostavljena in sistemske ranljivosti, ki jih grožnje lahko zlorabijo. Podrobna analiza parametrov, ki določajo tveganje, je predstavljena v tretjem poglavju.

Soo Hoo (2000) je predstavil formalno ogrodje tveganja, v katerem so tveganja ocenjena z vrednotenjem posledic neželenih dogodkov, napovedovanjem verjetnosti takih dogodkov in tehtanjem prednosti različnih aktivnosti. Tveganje je opredelil kot niz urejenih parov posledic (P) in z njimi povezanih verjetnosti (V) za dogodek.

$$tveganje \propto \{(\mathrm{P}_1,\ \mathrm{V}_1),\ \ldots,\ (P_\mathrm{i},\ \mathrm{V}_\mathrm{i}),\ \ldots,\ (P_\mathrm{n},\ \mathrm{V}_\mathrm{n})\} \quad (1)$$

Pregled literature pokaže na številne raziskave s področja ocene tveganj (Alberts & Dorofee 2002; Bennett & Kailay, 1992, str. 64; Blakley, 2001; Campbell & Sands, 1979, str. 293; Neumann, 2000). Veliko študij, ki preučuje zaznana tveganja se osredotoča na tveganja, kot racionalne odločitve, ki vključujejo oceno posameznika na verjetnost, da se nekaj zgodi, ter njegove dejanske izkušnje (Boss, 2007). Pri tem je izključena subjektivnost, ki ima velik vpliv na posameznike med ocenjevanjem tveganja. Sturrock (2005) navaja, da zaradi subjektivnosti

posamezniki večkrat kot večja tveganja zaznajo dogodke, ki se verjetno nikoli ne bodo zgodili (npr. teroristični napad, napad morskega psa itd.) in manjša tveganja za dogodke, ki se lahko pogosteje zgodijo (npr. 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 subjektivni vpliv spletnega kriminala (Hughes & DeLone, 2007). Dojemanje tveganja je običajno povezano z izkušnjami, ki jih ima posameznik glede varnostnih incidentov ali neposredne izkušnje (Skogan & Maxfield, 1981; Stinchcombe et al., 1980; S. Taylor & Todd, 1995).

2.1.2 Obravnava tveganja

Ko podjetje ugotovi in oceni tveganja, se mora odločiti, kako bo posamezno tveganje obravnavalo (angl. *risk treatment*). Standard ISO Guide 73 (2002) definira obravnavo tveganja kot:

> *"Proces izbora in vpeljave ukrepov za spremembo tveganja."*

Možne obravnave tveganja, shematično prikazana na sliki 3, so (Mehr & Hedges, 1974; Pritchard 1978; NIST 800-30, 2002):

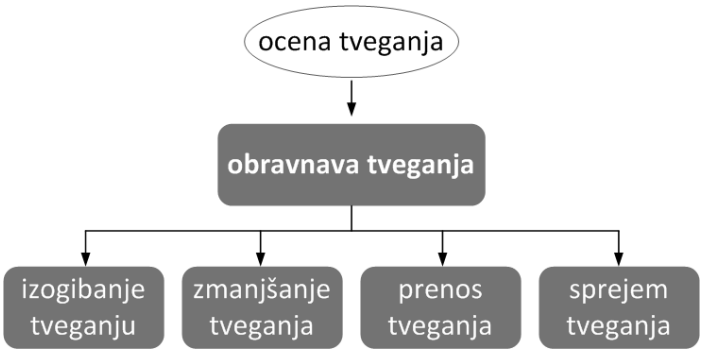
- **Izogibanje** grožnjam in napadom (angl. *risk avoidance*) z omejevanjem izvorov tveganja oziroma izpostavljenostjo sredstev k tveganju. To se večinoma uporabi v primerih, ko resnost učinka tveganja pretehta koristi, ki jih prinaša posamezno sredstvo (na primer odprt dostop do interneta). Podjetje se z izogibanjem tveganim aktivnostim, odpove aktivnosti, vendar pa se zaščiti pred tveganjem, ki bi imelo prevelike posledice.

- **Zmanjšanje** (angl. *risk mitigation* ali *risk reduction*) izpostavljenosti sredstva na tveganje z uvedbo ustreznih tehnologij in orodij (na primer požarnega zidu, protivirusne zaščite) ali uvedbo ustreznih postopkov (npr. 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 preko zunanjega izvajanja storitev (npr. storitve v oblaku) ali z zavarovanjem (Böhme & Kataria, 2006). Ta strategija prenosa postaja v zadnjem času čedalje bolj pomembna.

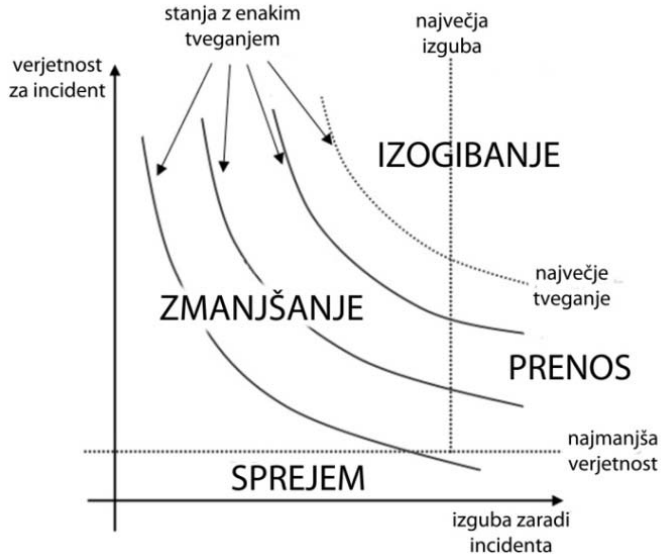
- **Sprejem** tveganja (angl. *risk acceptance*) kot posledico poslovanja. To je smiselna strategija v primeru, ko se tveganju ni mogoče izogniti ali ko so stroški uvedbe zaščitnih ukrepov znatno večji, kot pa skupne izgube zaradi tveganja.

Slika 3: *Različne možnosti obravnave tveganja*



V nekaterih primerih je težko določiti mejo med posameznimi obravnavami. Na primer požarni zid lahko razumemo kot tehniko izogibanja tveganju, ker se s tem podjetje odreče prednosti odprtih omrežij, da bi se izognili tveganju. Izbira ustrezne obravnave tveganja je lahko precej težavna in večkrat pri odločanju zahteva sklepanje kompromisov ali uporabo in kombiniranje dveh strategij (Bosworth & Kabay, 2002). Izbiro ustrezne obravnave tveganja lahko prikažemo na grafu verjetnosti za incident in izgube zaradi incidenta, ki je prikazan na sliki 4.

Slika 4: *Shematični prikaz porazdelitve posamezne obravnave tveganja glede na vrednosti verjetnosti za incident in izgube zaradi incidenta*



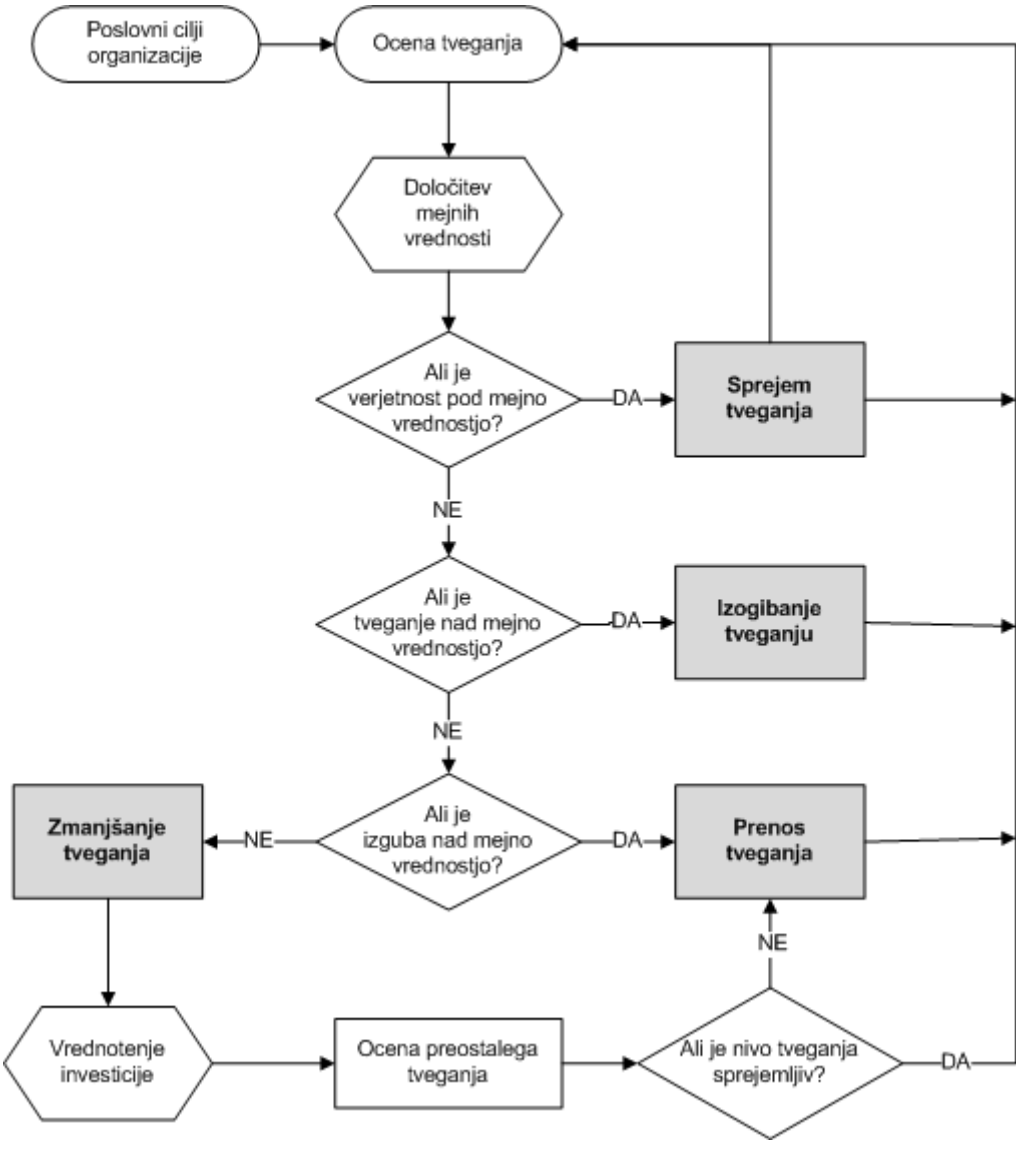
Vir: Bojanc & Jerman-Blažič, An economic modelling approach to information security risk management, 2008a, str. 417.

Parametra verjetnosti za incident in izgube zaradi incidenta sta podrobneje predstavljena v poglavju 3.4. Področje je razdeljeno na štiri enote, ki jih ločujejo tri mejne črte (Bojanc & Jerman-Blažič, 2008a). Prva mejna črta določa najmanjšo smiselno verjetnost za incident, pod to vrednostjo se tveganja sprejmejo. Neko tveganje se lahko na primer sprejme, če je verjetnost manjša kot enkrat v 1000 letih. Druga mejna črta je največja možna izguba zaradi incidenta. Nad to vrednostjo ima učinek lahko katastrofalne posledice. Za to področje je ena možnost

prenos tveganja na zavarovalnico ali zmanjšanje verjetnosti dogodka pod mejno vrednostjo. Tretja mejna črta je največja možna vrednost tveganja, nad katero se podjetje tveganju izogne. Tveganja v preostalem območju se odpravi z zmanjševanjem preko investicij v varnostne ukrepe.

Na podlagi razporeditve posameznih obravnav tveganja glede na verjetnost in izgubo se lahko določi proces izbire ustrezne obravnave tveganja. Primer procesa izbire obravnave tveganja je prikazan na sliki 5.

Slika 5: *Postopek izbire ustrezne obravnave tveganja*



Vir: Bojanc & Jerman-Blažič, An economic modelling approach to information security risk management, 2008a, str. 418.

Včasih je potrebnih več zaščitnih ukrepov za zmanjšanje preostalega tveganja na sprejemljivo raven. V nekaterih primerih, ko je tveganje sprejemljivo, se ne uvede nobenega zaščitnega ukrepa, četudi grožnje obstajajo. V drugih primerih lahko

ranljivosti obstajajo, vendar ni znanih groženj, ki bi jih izkoriščale. Podrobna obravnava tveganja je predstavljena v četrtem poglavju.

2.2 Pregled obstoječih metod in tehnik za obvladovanje tveganja

2.2.1 Primerjava kvantitativne in kvalitativne metode

S pomočjo ravnanja s tveganjem podjetja obvladujejo stroške, povezane z informacijskimi tveganji. Za obvladovanje varnostnega tveganja je na voljo veliko različnih metodologij, ki jih lahko razdelimo v dve osnovni kategoriji: kvantitativne in kvalitativne.

Kvantitativne metode

Kvantitativna analiza tveganja poskuša določiti numerične vrednosti za verjetnost in učinek tveganja ter ovrednotiti stroške in koristi, povezane z uvedbo varnostnih ukrepov. Kvantitativni pristop predpostavlja, da je mogoče vsako tveganje numerično ovrednotiti in izračunati vrednost verjetne škode, če se tveganje uresniči.

V večini primerov se tveganje izračuna s pomočjo pričakovane letne izgube (angl. *Annual Loss Expectancy*, v nadaljevanju *ALE*)[6], ki se za vsako grožnjo določi na podlagi dveh faktorjev (Turn, 1986): verjetnosti dogodka v določenem časovnem intervalu in zneska nastale izgube. Osnovno načelo je, da je uvedba zaščite stroškovno učinkovita, če je strošek zaščitnega ukrepa manjši od izračunane vrednosti ALE. V nasprotnem primeru je potrebno preučiti druge alternative.

Kvalitativne metode

V nasprotju s kvantitativnim pristopom poskuša kvalitativni pristop vrednost sredstev, pričakovano izgubo in stroške uvedbe zaščite izraziti v opisnih spremenljivkah, kot so "visoka", "srednja" ali "nizka". Pristop zagovarja načelo, da posledic nekaterih vrst izgub (na primer okvare ali spremembe podatkov) ni mogoče izraziti z denarnimi vrednostmi (Farahmand, 2004). Kvalitativni pristop se običajno izvaja skozi kombinacijo vprašalnikov in skupnih delavnic.

Tako kvalitativni kot kvantitativni pristop ima svoje prednosti in slabosti (Bojanc & Jerman-Blažič, 2008a). Težava kvantitativne analize je v pomanjkanju

[6] Metoda ALE je podrobneje predstavljena v poglavju 3.4.3.

standardnih metod, ki bi učinkovito izračunavale numerične vrednosti sredstev, izgub, stroške zaščit itd. Prednost kvalitativne metode je v tem, da proces sam zahteva manj človeških virov za točne izračune. Slabost kvalitativnega pristopa pa 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 enostavni • ne zahteva prikaza vrednosti sredstev v denarnih enotah • ne zahteva izračuna pogostosti groženj • enostavneje 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 se ne da enostavno 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

Prednost kvantitativnih metod je njihova zmožnost, da povežejo stroške in vrednosti grožnje med seboj. Povezava je lahko v odstotkih ali sorazmerna glede na sredstvo (Carter, 1987). Čeprav lahko ALE to povezavo izrazi z eno samo vrednostjo, Gardner (1989, str. 479) opozarja, da se je potrebno zavedati, da

izračun dobimo iz podatkov in verjetnosti, ki pogosto nimajo močne empirične podlage. Težave lahko nastopijo takrat, ko slepo verjamemo, da so podatki, s katerimi razpolagamo točni, v resnici pa podatki pogosto niso zelo natančni.

Največji prednosti kvalitativnega pristopa sta porabljen čas in strošek za izvedbo ocene (Farahmand, 2004). Kvantitativni pristop običajno zahteva poglobljeno in obsežno raziskavo o grožnjah, sistemu in podjetju, da se lahko določijo numerične vrednosti za verjetnosti in stroške. V večini primerov je taka raziskava časovno zahtevna in vključuje tudi veliko ljudi v podjetju. Kvalitativne metode se lahko po drugi strani običajno izvedejo v krajšem času z manjšim številom osebja. Vendar pa je potrebno biti pazljiv pri primerjavi kvalitativnih vrednosti (kot so visoko, srednje in majhno tveganje). Za nekoga je lahko določeno tveganje visoko, nekdo drug pa isto tveganje lahko razume kot nizko. Wong in Watt (1990) priporočata upoštevanje spodaj naštetih dejavnikov pri izbiri metode:

- **Stroški**: koliko je podjetje pripravljeno zapraviti?
- **Primernost**: podjetje mora izbrati ustrezno analizo tveganja za svoje okolje.
- **Prilagodljivost**: metoda se mora nanašati na trenutno delovno prakso.
- **Popolnost**: zagotoviti je treba, da metoda zajema vsa možna tveganja.

2.2.2 Metode in tehnike za obvladovanje tveganja

Za vodenje informacijske varnosti obstaja veliko modelov. Najpomembnejši cilj je zagotoviti, da podjetje ohrani sposobnost za opravljanje svoje dejavnosti in pri tem tveganje omeji na sprejemljivo raven. Nobena varnost ne more biti popolnoma učinkovita, zato je pomembno, da se načrtuje okrevanje iz neželenega dogodka in strukturira varnost za omejitev obsega škode. Varnost informacijskih sistemov je večdimenzionalni problem, ki ga je mogoče gledati z različnih vidikov.

Na voljo je veliko različnih metod in tehnik za obvladovanje tveganja. Med najbolj priljubljenimi so sledeče metode:

- EBIOS (2009) metoda, ki je razvita in vzdrževana s strani DCSSI (Central Information Systems Security Division) v Franciji.
- MEHARI (2009) 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) 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 Insight Consulting.

- CORAS (Risk Assessment of Security Critical Systems) (2009) je Evropski projekt razvoja ogrodja ravnanja s tveganjem.
- Facilitated Risk Assessment Process (FRAP), ki ga je razvil Tom Peltier (2005).
- National Security Agency's (NSA) INFOSEC Assessment Methodology (IAM) (Douglas, 2006).

Podroben seznam s kratkim opisom metod in tehnik za obvladovanje in ocenjevanje tveganj objavljata ENISA (ENISA, 2009) in ISO27001 Security (2009).

3 Informacijska sredstva in grožnje

3.1 Analiza sredstev

Standard ISO 13335-1 (2004) podaja sledečo definicijo **sredstva**:

> *"Vse, kar ima določno vrednost za podjetje."*

To definicijo sredstva povzemajo tudi drugi ISO standardi. Standard ISO 27000 (2009) podrobneje definira tudi **informacijsko sredstvo**:

> *"Znanje ali podatek, ki ima določeno vrednost za podjetje."*

Ustrezno upravljanje sredstev je ključnega pomena za uspeh podjetja in velika odgovornost za vse managerje. Prvi korak v procesu analize tveganja je identifikacija informacijskih sredstev podjetja (Bojanc & Jerman-Blažič, 2008a). Količina podatkov, ki jih sodobna podjetja proizvajajo in obdelujejo, čedalje bolj narašča. Zato je pomembno, da podjetje zlahka identificira in izkoristi ključne informacije (Rues, 2003). Zaradi lažje uporabe in preglednosti je smiselno, da so sredstva grupirana, v kolikor je to mogoče. Logična in fizična sredstva lahko združimo v sledeče kategorije:

- **Fizična sredstva**: računalniška strojna oprema, naprave za komunikacijo in hrambo, nosilci podatkov, zgradbe, lokacije …
- **Programska sredstva**: operacijski sistemi, programske aplikacije in storitve, ki obdelujejo, shranjujejo ali posredujejo informacije, razvojna orodja …
- **Podatki**: dokumenti v papirnati ali elektronski obliki (oz. zbirke podatkov) in intelektualna lastnina, ki se uporabljajo za dosego ciljev podjetja.
- **Sistemi**, sposobni za proizvodnjo izdelkov ali opravljanje storitev: informacijski sistemi, ki obdelujejo in hranijo informacije (sistemi so kombinacija informacij, programske in strojne opreme ter katerikoli gostitelj, odjemalec ali strežnik, ki je vključen v sistem), podporni sistemi (na primer ogrevanje, osvetlitev, fizično varovanje, elektrika in klimatske naprave).

- **Človeški viri**: zaposleni v podjetju, ki imajo veščine, znanje in izkušnje, ki jih je težko nadomestiti.
- **Neopredmetena sredstva**: ugled in podoba podjetja, morala zaposlenih, blagovne znamke, produktivnost zaposlenih ...

Za informacijska sredstva, ki so izpostavljena grožnjam, je potrebno poznati njihove vrednosti. Vse informacije v poslovnem okolju imajo vrednost, ki je večja ali enaka nič. Podjetja ne morejo dobro ovrednotiti izgube, če niso predhodno ovrednotena sredstva (Su, 2006). Kot poudarja Crume (2001) je prvo pravilo informacijske varnosti, da nikoli ne zapraviš za zaščito več od vrednosti tistega, kar dejansko varuješ. Zato je pomembno poznati vrednost sredstev.

Vrednost svojih opredmetenih sredstev lahko podjetje dokaj enostavno določi, saj lahko hitro izračuna njihovo vrednost v določenem trenutku. Vrednost sredstev je merjena v denarju, pri čemer se upošteva amortizacija sredstev. Vrednost posameznega sredstva se lahko predstavi tudi kot izgubo, ki jo podjetje utrpi ob izgubi tega sredstva. Težje pa se določi vrednost neopredmetenim sredstvom (Brynjolfsson, Hitt & Yang, 2002, str. 137; Bojanc & Jerman-Blažič, 2008a). Strokovnjaki ocenjujejo, da ima lahko izguba neopredmetenih sredstev večje negativne posledice, kot izguba opredmetenih sredstev (Bresnahan, Brynjolfsson & Hitt, 2002, str. 339; Brynjolfsson & Hitt, 2003, str. 793).

Pri oceni sredstev se sredstva običajno klasificira v diskretne kategorije ali razrede, s katerimi se sredstva razdeli po prioritetah varovanja (FIPS 199, 2004; NIST 800-60, 2008; Microsoft, 2004). Razredi olajšajo definiranje varnostnih tveganj, po drugi strani pa pomagajo podjetjem, da se najprej osredotočijo na najbolj kritična sredstva. Različni modeli za oceno tveganj določajo za sredstva različne razrede. Večje število razredov (na primer 10) je sicer bolj natančno, po drugi strani pa manjše število razredov (na primer 3 ali 4) skrajša čas vrednotenja. Primer trirazredne klasifikacije razredov je: kritično, zmerno, nizko. Tipična sredstva v kritičnem razredu so: finančni podatki, intelektualna lastnina, številke bančnih računov itd. V zmernem razredu so običajno naslednja sredstva: interne poslovne informacije, naročila, računi, načrt omrežja in informacije na interni spletni strani. Sredstva v nizkem razredu pa so: informacije na javni spletni strani, objavljeni prispevki, brošure produktov in dokumentacija (Bojanc & Jerman-Blažič, 2008a).

V zadnjih letih so bile razvite različne metode vrednotenja sredstev, ki pa lahko za ista sredstva podajajo različne vrednosti (Mercuri, 2003; Power, 1999; Campbell, Gordon, Loeb & Zhou, 2003, str. 431; Soo Hoo 2000; Garg, Curtis & Halper, 2003; Cavusoglu, Mishra & Raghunathan, 2004a). Nekateri pristopi gledajo na stroške ustvarjenja (oziroma ponovnega ustvarjenja) ogroženih sredstev, drugi pristopi gledajo stroške, ki nastanejo zaradi varnostnega incidenta, medtem ko tretji poskušajo zajeti vse učinke na prihodke in stroške.

Poore (2000) je objavil pogoje, ki predstavljajo osnovo za vrednotenje informacij, za ravnanje s tveganji:

- **Izključno lastništvo.** Stopnja, do katere je informacija v določenem izključnem lastništvu, se direktno odraža na vrednosti informacije za podjetje, ki jo lasti. Na primer ko neka poslovna skrivnost preneha biti skrivnost, izgubi svojo vrednost.
- **Koristnost**. Koristna informacija je pomembna vsaj toliko, kot je možnost njene uporabe.
- **Stroški ustvarjenja ali ponovnega ustvarjenja.** Ena izmed najlažjih metod za zajemanje vrednosti je, da podjetje ugotovi, kolikšen strošek za podjetje predstavlja ustvarjanje ali pridobitev informacij.
- **Odgovornost**. Če informacije predstavljajo odnos zaupanja, potem lastnik informacije prevzame odgovornost za njeno zaščito.
- **Zamenljivost**. Če informacije predstavljajo vrednost samo po sebi ali kadar ima informacija notranjo vrednost (npr. intelektualna lastnina, glasba), ki se lahko zamenjuje z drugimi sredstvi, je vrednost informacije vsaj tolikšna, kot je vrednost zamenjave.
- **Operativni vpliv.** Podjetje lahko pogosto dodeli vrednost na osnovi ocene vpliva na podjetje, ki bi ga imela napačna uporaba sredstva (npr. neveljavni inventar ali naročanje materialov).

Geer (2004a) je predstavil tri načine, kako se lahko za informacijo določi, koliko je vredna. Vsak od teh načinov predstavlja najnižjo mejo, koliko je informacija vredna. Načini so:

- **Nadomestna vrednost.** Kolikšni so stroški obnovitve podatkov iz stanja nič do stanja podatkov v tem trenutku?
- **Vrednost na črnem trgu.** Koliko je nekdo pripravljen plačati za podatke?
- **Bodoča vrednost.** Koliko bodočega prihodka ali drugih vrednosti ne bo realiziranih v primeru izgube podatkov?

3.2 Analiza groženj

Informacijska sredstva so izpostavljena grožnjam. Standard ISO 27000 (2009) podaja sledečo definicijo **grožnje**:

> *"Potencialni vzrok neželenega incidenta, ki lahko povzroči škodo sistemu ali podjetju."*

Grožnje so viri možnih akcij ali dogodkov, ki lahko povzročijo kršitve informacijske varnosti (Gordon & Loeb, 2005, str. 12). Grožnje lahko opredelimo kot vse, kar

prispeva k spreminjanju, uničenju ter prekinitvi storitev ali drugih stvari, ki podjetju predstavljajo vrednost.

Schechter (2004) navaja, da je varnost proces, ki se začne z zaporedjem dogodkov z nezaželenimi posledicami, ki jih podjetje želi preprečiti. Za povečanje zaščite in vzpostavitev varnostnih strategij in politik mora podjetje jasno identificirati grožnje, ki pretijo njihovim informacijskim sredstvom. V varnostni literaturi se beseda nevarnost ne nanaša na nasprotnika, ki lahko povzroči škodo, ampak na zaporedje dogodkov, ki se začnejo z nasprotnikom (t. i. povzročiteljem grožnje) in končajo z okvaro ali škodo (Fites, Kratz & Brebner, 1989, str. 37; Peltier, 2001, str. 21). Za tako zaporedje dogodkov se v literaturi uporablja tudi izraz "scenarij" grožnje, ki predstavlja (Alberts & Dorofee, 2002; Anderson 1991, str. 301; Fites, Kratz & Brebner 1989; Lewis, 1990; Schechter, 2004):

- V splošnem smislu: zaporedje dogodkov, skozi katere bi naravni ali inteligentni nasprotnik (ali skupina nasprotnikov) lahko povzročil škodo.
- V informacijski varnosti: zaporedje dogodkov, skozi katere naravni ali inteligentni nasprotnik (ali skupina nasprotnikov) lahko uporabi sistem na nepooblaščen način, da povzroči škodo, s katero ogrozi zaupnost, celovitost ali razpoložljivost informacij.

Z razumevanjem dogodkov, ki v scenariju grožnje vodijo do škode, si lahko razjasnimo, kaj je ogroženo in kateri zaščitni ukrepi lahko zmanjšajo tveganje. Raziskovanje scenarijev groženj pomaga razumeti, kaj lahko povzroči izgubo varnosti, kako in zakaj se ti dogodki lahko zgodijo ter kdo jih najverjetneje lahko povzroči.

Literatura informacijske varnosti deli scenarije groženj na tri kategorije, ki temeljijo na tem, kateri varnostni princip je ogrožen: zaupnost, celovitost ali razpoložljivost. Osnovni scenariji za vsako izmed teh treh kategorij so (Schechter, 2004):

- Informacije so izpostavljene nekomu, ki naj ne bi imel dostopa do njih.
- Informacije so spremenjene v nasprotju s politiko.
- Pooblaščeni uporabniki imajo preprečen dostop do informacij ali sredstev takrat, ko se jih potrebuje.

Grožnja je običajno sestavljena iz povzročitelja grožnje in tehnike napada (Mayer et al., 2007). Grožnja se udejanji skozi povzročitelja grožnje, ki uporabi določeno tehniko napada, da doseže neželeni učinek (Farahmand, 2004).

3.2.1 Klasifikacija varnostnih groženj v informacijskih sistemih

Grožnje različno vplivajo na informacijska sredstva. V osnovi so usmerjene na:

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

Za učinkovito analizo varnostnih groženj in določitev ukrepov, s katerimi se podjetje pred grožnjami zavaruje, je potrebno grožnje klasificirati. Klasifikacija je koristna tudi pri poročanju incidentov ustreznim ekipam. Camp in Wolfram (2000, str. 31) opozarjata, da je potrebno pri klasifikaciji upoštevati, da nobena varnostna grožnja ne ostane neklasificirana ter da se nobena varnostna grožnja ne uvrsti v več kot eno klasifikacijo. Pregled literature je pokazal veliko poskusov klasifikacije varnostnih groženj. Lindqvist in Jonsson (1997, str. 154) priporočata naslednje lastnosti za klasifikacijo informacijske varnosti:

- Kategorije naj se med seboj izključujejo, tako da se vsak element uvrsti v največ eno kategorijo. Kategorije so skupaj popolne, tako da je vsak element treba uvrstiti v vsaj eno kategorijo.
- Vsako kategorijo bi morala spremljati jasna in nedvoumna merila, ki opredeljujejo, kateri elementi se uvrstijo v kategorijo.
- Taksonomija mora biti razumljiva in uporabna, tako varnostnim strokovnjakom, kot tudi uporabnikom in skrbnikom z manj znanja in izkušenj.
- Terminologija taksonomije mora biti v skladu z uveljavljeno varnostno terminologijo.

Standard ISO 27005 (2008) razvršča grožnje glede na vrsto napada v sledeče kategorije:

- **Fizična škoda:** požar, izliv vode, onesnaženje, uničenje opreme …
- **Naravni dogodki:** potres, izbruh vulkana, poplava …
- **Izguba ključnih storitev:** okvara klimatske naprave, okvara vodovodnega omrežja, izpad elektrike, okvara telekomunikacijske opreme …
- **Težave zaradi sevanja:** npr. elektromagnetno sevanje, toplotno sevanje …
- **Ogrožanje informacij:** prisluškovanje, kraja dokumentov ali opreme, razkritje, pridobitev zavrženih podatkov …
- **Tehnične okvare:** odpoved opreme, preobremenitev informacijskega sistema …
- **Nepooblaščena dejanja:** nepooblaščena uporaba opreme, nelegalno kopiranje programske opreme, okvara podatkov, nelegalna obdelava podatkov …

- **Ogrožanje funkcij:** napačna raba, zloraba pravic, ponareditev pravic, odpoved aktivnosti …

Taksonomija, ki jo je razvil Naval Research Laboratory (Landwehr et al., 1994), razvršča vsako varnostno ranljivost glede na izvor (povzročeno namerno ali nenamerno), čas izvedbe (med razvojem, vzdrževanjem ali obratovanjem) in lokacijo (programska ali strojna oprema). Neumann in Parker (1989) sta v svoji taksonomiji kategorizirala računalniške tehnike zlorab v devet razredov. Taksonomija DARPA's Intrusion Detection Evaluation razvršča napade v štiri skupine (Lipmann, 2000):

- ohromitev storitve (angl. *Denial of Service – DoS*),
- oddaljen dostop do lokalnega okolja (napadalec pridobi dostop do računalnika žrtve),
- pridobitev administratorskih privilegijev (lokalni uporabnik na računalniku lahko pridobi privilegije administratorja ali "root" uporabnika),
- nadzor.

3.2.2 Povzročitelji grožnje

V splošnem se povzročitelje grožnje deli na okoljske (naravne) pojave in človeški faktor. Farahmand (2004) človeški faktor razdeli na avtorizirane uporabnike in neavtorizirane uporabnike.

Okoljski (oz. naravni) pojavi: Nekatere lokacije so bolj dovzetne za določene okoljske vplive in naravne nesreče kot druge. Nekatere vrste nesreč niso geografsko odvisne (npr. požar, udar strele), medtem ko so druge specifične za določena območja (npr. poplave, potresi). Poleg naravnih nesreč so nevarnosti tudi okvare mehanske in električne opreme ter prekinitev napajanja ali instalacijskih vodov (npr. vodovodna instalacija, plinska instalacija, električna instalacija, izpad elektrike).

Avtorizirani (oz. pooblaščeni) uporabniki: Avtorizirani uporabniki lahko predstavljajo grožnjo, kadar presežejo svoja pooblastila ali storijo nenamerno napako (npr. brisanje datotek, fizične nesreče), s čimer vplivajo na delovanje sistema na način, da ta ne opravlja svoje naloge. Kot potencialno grožnjo je potrebno upoštevati zaposlene, ki imajo dostop do sistema ali imajo položaj s posebnimi dovoljenji. Grožnja je lahko tudi neustrezno usposobljeno IT osebje. Glede na zadnje raziskave, postajajo avtorizirani uporabniki čedalje pogostejši povzročitelji grožnje (CSI, 2009). Zato se mora podjetje zavedati, da so osebe z internim znanjem pomemben vir napadov.

Neavtorizirani (oz. nepooblaščeni) uporabniki: Nepooblaščen uporabnik je lahko kdorkoli, ki ne opravlja podpore poslovnim procesom in poskuša prekiniti produktivnost ali delovanje sistema (npr. hekerji, tatovi, partnerska podjetja,

neavtorizirani notranji uporabniki). To lahko stori na odkrit ali prikrit način. Odkrita metoda je lahko sabotaža, ki vpliva na delovanje strojne in pripadajoče opreme. Prikrite metode so bolj subtilna prizadevanja za uničenje, ki se lahko dosežejo z manipulacijo programske opreme, sistema in aplikacij.

Tudi standard ISO 13335-1 (2004) deli povzročitelje na okoljski (oz. naravni) faktor in človeški faktor. Za razliko od Farahmandove razdelitve, standard ISO 13335-1 loči človeški faktor na:

- Namerne grožnje: lahko so zunanji uporabniki (npr. hekerji, tatovi, partnerska podjetja …) ali notranji uporabniki, ki želijo škodovati podjetju.
- Nenamerne napake: lahko jih povzročijo navadni uporabniki (npr. brisanje datotek, fizične nesreče …) ali pa neustrezno usposobljeno IT osebje.

Nekaj primerov groženj različnih povzročiteljev je prikazanih v tabeli 2:

Tabela 2: *Primeri groženj različnih povzročiteljev*

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

Vir: ISO 13335-1, 2004, str.7.

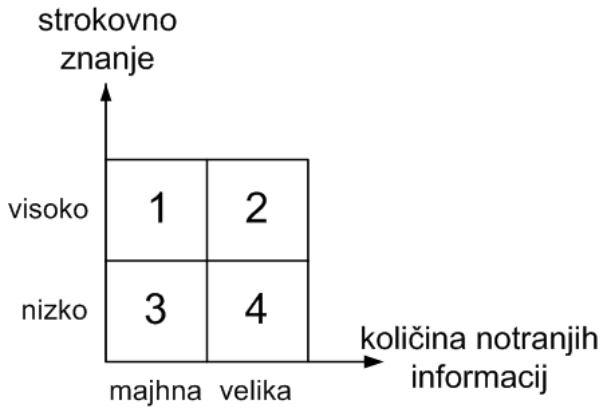
Schneier (2004a) kategorizira ljudi, ki izvajajo zlonamerna dejanja, glede na cilje, dostope, sredstva, izkušnje in tveganja. Najbolj znane vrste zlonamernih ljudi so: hekerji, osamljeni kriminalci, zlonamerni zaposleni, industrijski vohuni, organizirani kriminal in teroristi (Bojanc & Jerman-Blažič, 2008a). Vsaka vrsta zlonamernih ljudi poskuša premagati varnost zaradi različnih motivov, kot so priznanje, reklama, pridobitev prednosti pred konkurenco, osebno zadovoljstvo, finančni dobiček, maščevanje ali terorizem.

Farahmand (2004, str. 12) prikaže razvrstitev zlonamernih ljudi grafično, kot matriko dimenzije 2×2 (slika 6). V matriki upošteva dve lastnosti posameznikov:

- nivo tehničnega znanja napadalca (prikazano na navpični osi),
- količina notranjih informacij, ki jih napadalec morda ima (prikazano na vodoravni osi).

Nestrokovni zunanji zlonamerni uporabnik (kvadrant 3) predstavlja nizko stopnjo grožnje. To je nekdo, ki bi lahko ukradel prenosni računalnik in ga ob priložnosti prodal. Nestrokovni notranji uporabnik (kvadrant 4) predstavlja precej pomembno grožnjo, saj pozna postopke in lahko izkoristi ranljivosti sistema, brez uporabe zahtevnih tehnik ali algoritmov. Tehnično usposobljeni zunanji uporabniki (kvadrant 1) so maloštevilni hekerji. Vendar pa ti posamezniki razvijajo orodja, s katerimi lahko upravlja zelo veliko manj usposobljenih uporabnikov. Zato so ti posamezniki še posebej nevarni. Najnevarnejšo grožnjo pa predstavljajo tehnično usposobljeni notranji uporabniki (kvadrant 2). Farahmand (2004) ugotavlja, da so običajno ravno ti notranji zaposleni odgovorni za največ finančno pomembnih težav z informacijsko varnostjo.

Slika 6: *Matrika klasifikacije napadalcev glede na strokovno znanje in količino notranjih informacij*



Vir: Farahmand, Developing a Risk Management System for Information Systems Security Incidents, 2004, str.12.

3.2.3 Tehnike napadov

Schneier (2002a) ugotavlja, da v informacijski varnosti stare vrste napadov ne zastarijo, novi napadi pa so le še hujši. Najbolj resne težave v informacijski varnosti ne predstavljajo najnovejši napadi, temveč čedalje več ponovitev starih napadov, ki še nadalje povzročajo škodo. En tak primer so napadi s prekoračitvijo pomnilnika (angl. *buffer overflow*), ki so eni izmed najstarejših vrst računalniških napadov. Prvič se jih omenja po letu 1960. V 70-tih letih se je ta tehnika pogosto uporabljala za napade prvih omreženih računalnikov. Leta 1988 je črv Morris s prekoračitvijo pomnilnika onemogočil 10 % gostiteljev na internetu (Wikipedia, 2008; Bluejackel's finds, 2009). Napadi s prekoračitvijo pomnilnika še danes predstavljajo ogromen problem, saj je največ napadov na internetu ravno te vrste in to kljub temu, da so na voljo avtomatični programi, ki lahko poiščejo in odpravijo tovrstne ranljivosti že v času razvoja. Seveda je veliko napadov, ki so bolj prikriti in težji za odpravo, kot napadi s prekoračitvijo pomnilnika, vendar se slednji še vedno veliko uporabljajo in povzročajo škodo.

Pred desetimi leti je bil uspešen napad na spletno stran velika medijska novica, danes se tovrstni napadi dogajajo dnevno in se o njih skorajda ne poroča več. Leta 1999 je trojanski konj BackOrifice povzročil veliko hrupa (Wikipedia, 2009a), danes je veliko trojanskih konjev hujših, vendar se o njih ne poroča. Februarja leta 2000 je napad s porazdeljeno ohromitvijo storitve (angl. *distributed denial-of-service*, v nadaljevanju *DDoS*) onemogočil delovanje veliko znanih spletnih strani, kot so Yahoo, eBay, Amazon.com in CNN. DoS napadi so stari toliko kot sam internet in danes se vsak teden zgodi na tisoče tovrstnih napadov (Schneier, 2002a).

Tehnike napadov se lahko razvrsti v sledeče kategorije:

- **Fizični napadi.** Fizični vdor predstavlja nepooblaščen dostop do varovanih področij, kot so poslovni prostori, strežniška soba ali drugi varovani prostori.
- **Napadi na osebje.** Te tehnike in metode napada se ukvarjajo z izkoriščanjem osebja, ki imajo določeno stopnjo dostopa in privilegije v sistemu. Osebje so lahko navadni uporabniki ali upravljavci sistema (npr. 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.** Z napadi na strojno opremo se lahko doseže, da strojna oprema omejuje ali preprečuje delovanje sistema. Lahko gre za fizični napad na opremo, hrošč podtaknjen v krmilnik strojne opreme ali napad na podporno opremo. Strojna oprema običajno vključuje vsak kos opreme, ki je del informacijskega sistema (npr. strežniki, periferna oprema in komunikacijska oprema) ter podporno opremo, kot so napajalniki, klimatske naprave, rezervno napajanje itd.
- **Napadi na programsko opremo.** Tehnike vdora v programsko opremo so lahko usmerjene na operacijski sistem ali aplikacijske programe. Napadi na programsko opremo 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 postopkov.** Pooblaščeni ali nepooblaščeni uporabniki lahko vdrejo v sistem zaradi pomanjkanja ustreznih kontrol ali neustreznega izvajanja kontrol. Primer zlorabe postopkov je, da bivši zaposleni ohranijo in uporabljajo veljavna gesla za dostop v sistem.

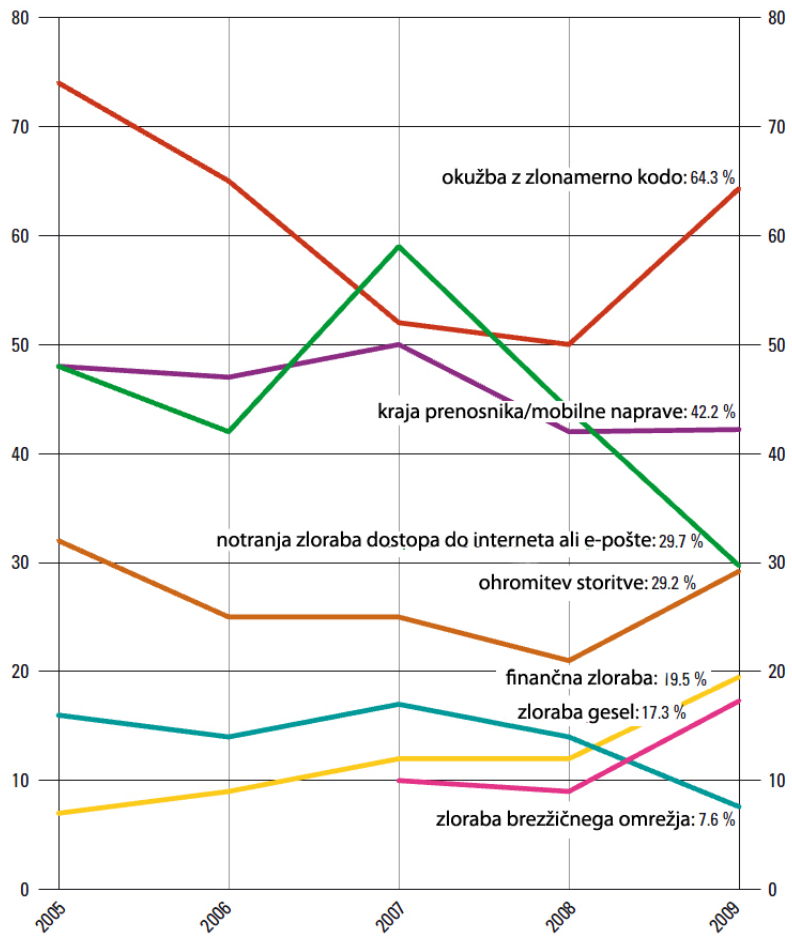
3.2.4 Empirične ugotovitve

Zaskrbljujoče je, da se grožnje na informacijske sisteme povečujejo. Raziskava (Symantec Corporation, 2007) je pokazala opazno povečanje kraje podatkov in

razvoja zlonamerne kode za krajo zaupnih informacij. Podjetja si prizadevajo za večjo varnost sistemov in podatkov, soočajo pa se z naraščanjem števila potencialnih hekerjev (Swartz, 2005) in zaposlenih, ki na varnost ne gledajo kot prednostno nalogo ali se ne zavedajo svoje ogroženosti (Boss, 2007).

Raziskava CSI (2009) beleži grožnje, ki so jih podjetja že izkusila. V zadnjem poročilu CSI so najbolj napredovale naslednje grožnje: finančna zloraba (v letu 2009 19,5 %, v letu 2008 12 %), okužba z zlonamerno kodo (v letu 2009 64,3 %, v letu 2008 50 %), ohromitev storitve (v letu 2009 29,2 %, v letu 2008 21 %), iskanje gesel (v letu 2009 17,3 %, v letu 2008 9 %) in zloraba spletne strani (v letu 2009 13,5 %, v letu 2008 6 %). Po drugi strani pa sta se najbolj zmanjšali grožnji zlorabe brezžičnih omrežij (v letu 2009 7,6 %, v letu 2008 14 %) in zlorabe neposrednega sporočanja (v letu 2009 7,6 %, v letu 2008 21 %). V raziskavi je sodelovalo 443 podjetij. Rezultati so prikazani na sliki 7:

Slika 7: *Katere vrste napadov je podjetje že utrpelo*

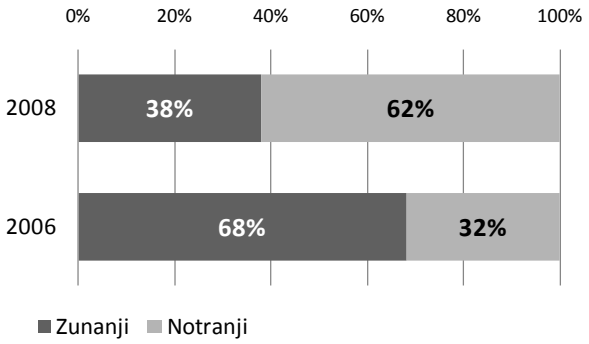


Vir: CSI Computer Crime and Security Survey 2009, str.7.

V zadnjih letih se razmerje med internimi in zunanjimi zlorabami spreminja. Če je bilo še leta 2006 občutno več tistih podjetij, pri katerih je bil najhujši incident

zunanja zloraba, je stanje leta 2008 ravno nasprotno (BERR, 2008). Rezultati so prikazani na sliki 8:

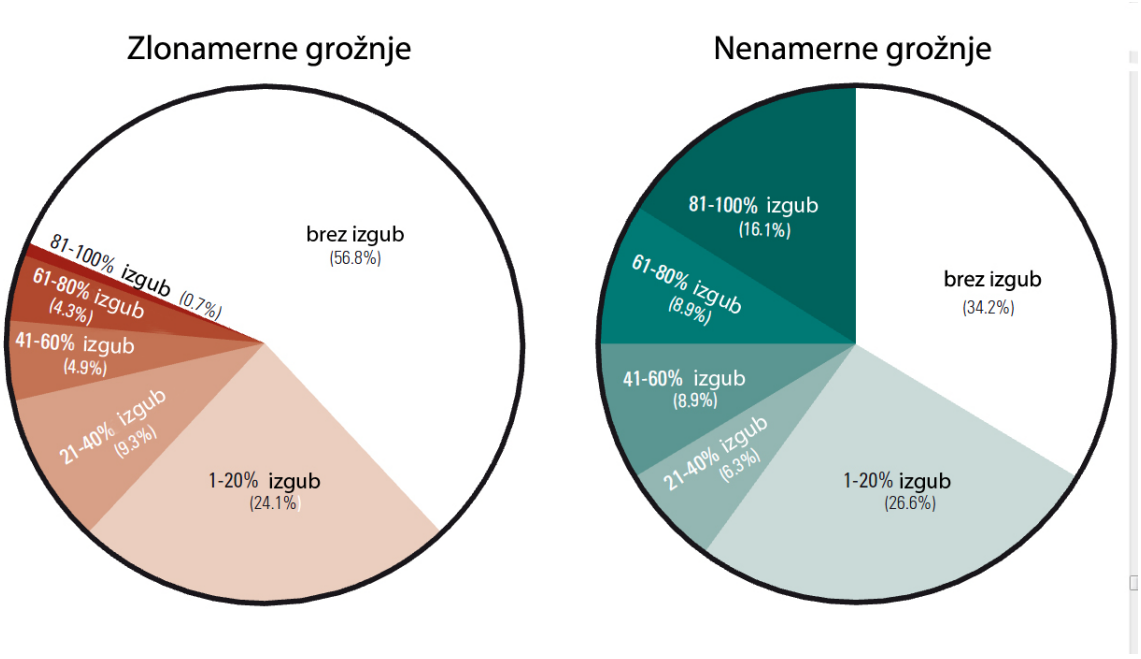
Slika 8: *Ali je najhujši varnostni incident povzročil zunanji ali notranji uporabnik*



Vir: BERR Information Security Breaches Survey 2008, str.23.

Raziskava CSI (2009) je zajela tudi izgube glede na zlonamerne in nenamerne grožnje notranjih uporabnikov. 43 % sodelujočih je izjavilo, da je vsaj nekaj izgub zaradi zlonamernih notranjih uporabnikov. Očitno večjo težavo predstavljajo nenamerne grožnje notranjih uporabnikov, saj je 65 % sodelujočih izjavilo, da so imeli tovrstne izgube. 16 % sodelujočih je celo ocenilo, da nenamerne grožnje predstavljajo skoraj vse njihove izgube. To pomeni, da je pri teh podjetjih zelo pomembno izobraževanje in ozaveščanje uporabnikov. Rezultati so prikazani na sliki 9:

Slika 9: *Odstotek izgub glede na notranje uporabnike*



Vir: CSI Computer Crime and Security Survey 2009, str.12.

Po raziskavi BERR (2008) je 13 % podjetij zaznalo nepooblaščene zunanje uporabnike v njihovem omrežju.

Najpogostejše tehnike napadov so: SQL vrivanje (40 %), naprednejši napadi (15 %), notranji uporabniki (15 %), "phishing" (15 %) in napadi v brezžičnih omrežjih (10 %) (CSI, 2009).

3.3 Ranljivosti sredstev

V medijih se neprestano pojavljajo novice o novih varnostnih grožnjah (Boss, 2007). Običajno gre za opozorila o novo odkritih ranljivostih v operacijskih sistemih in aplikacijski programski opremi (ABC News, 2004) ali novih virusih (Symantec Corporation, 2009). Standard ISO 27000 (2009) podaja sledečo definicijo **ranljivosti**:

> *"Šibkost sredstva ali kontrole, ki jo grožnja lahko zlorabi."*

Ranljivost je šibka točka informacijskega sistema podjetja, ki povečuje verjetnost za uspešen napad na ta sistem (Gordon & Loeb, 2005, str. 13). Na primer puščanje prenosnega računalnika v nezaklenjeni pisarni, 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 povzroči škode; ranljivost je zgolj pogoj (ali niz pogojev), ki lahko omogoči grožnji, da vpliva na sredstva (ISO 13335-1, 2004).

Zlonamerni posamezniki (oziroma hekerji) neprestano iščejo ranljivosti in pregledujejo računalnike, ki so povezani v internet (Coren, 2005). Ko ranljivost najdejo, jo poskušajo zlorabiti. Veliko virusov avtomatizirano opravlja podobne funkcije, pregledujejo ranljive računalnike ter se replicirajo na druge računalnike. Te aktivnosti povzročajo določeno porabo pasovne širine komunikacijske povezave. Ocenjuje se, da samo stroški uporabe pasovne širine v te namene znašajo vsako leto več sto milijonov dolarjev (CERT, 2004; Coren, 2005). Število ranljivosti se je v zadnjih letih močno povečalo, iz 171 v letu 1995 in 1090 v letu 2000, na 8064 ranljivosti v letu 2006 (CERT, 2008). Povečevanje odkritih ranljivosti, ki ostanejo nezakrpane, zagotavlja stalen vir za napade zlonamernih posameznikov. Tu so še posebej izpostavljeni domači uporabniki, ki danes povečini uporabljajo stalno internetno povezavo in imajo povečini slabo varovane računalnike, ki jih napadalci zlorabijo in uporabijo za izhodišče za druge napade, s čimer zmanjšujejo svoje tveganje. Zmanjševanje tveganja (za napadalca) in stroškov za napad (avtomatizacija napadov z raznimi orodji), pa povzroča povečanje števila napadov v omrežju (Schechter, 2004).

Primeri pogostih ranljivosti so (ISO 13335-1, 2004; ISO 27005, 2008):

- slaba skrb za gesla (npr. zapisovanje gesel),
- splošno pomanjkanje zavedanja informacijske varnosti zaposlenih,
- nepravilna uporaba interneta (npr. 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.

Čeprav se večinoma na ranljivost gleda kot na tehnično napako, so določene ranljivosti vezane na človeški faktor. Take ranljivosti so na primer deljenje gesel med uporabniki, uporaba šibkih gesel, nepoznavanje ali neupoštevanje varnostnih politik, odpiranje sumljivih priponk v e-poštnih sporočilih, ogledovanje sumljivih spletnih strani ali prenos programske opreme, ki vsebuje zlonamerno kodo (Bojanc & Jerman-Blažič 2008a).

Večina varnostnih incidentov je povzročenih zaradi ranljivosti kot napake v programski opremi. Splošno se postavlja vprašanje, zakaj proizvajalci programske opreme ne naredijo bolj varnega produkta že na začetku. Razvijalci programske opreme imajo boljša orodja in znanje kot pred desetimi leti, zmožni so napisati bolj varno programsko opremo, vendar zaradi ekonomike razvoja programske opreme nimajo spodbude, da to storijo (Anderson & Moore, 2008). Kot opisujem v poglavju 1.4.4, programska oprema na trgu trpi zaradi informacijske asimetrije, ki je značilna za tržišče limon. Ker je varnost programske opreme težko izmeriti, uporabniki težko razlikujejo med bolj varnimi in manj varnimi produkti, zato za

varnost niso pripravljeni plačati več. Proizvajalci pa zato niso motivirani, da bi vlagali v varnost.

3.3.1 Trg ranljivosti

Eden od mehanizmov za zagotavljanje varnosti je opredeliti ranljivost kot tržno blago, ki je menjalno sredstvo na različnih trgih ranljivosti (Camp, 2006). To pomeni, da proizvajalec ali lastnik ponuja nagrado za prvo osebo, ki odkrije ranljivost. Trg ranljivosti pomaga kupcem in proizvajalcem vzpostaviti dejanske stroške pri iskanju ranljivosti v programski opremi (Camp & Wolfram, 2000). Schechter (2004) je uporabil ta izhodišča in razvil predlog za odprt trg še neodkritih ranljivosti. Tržna cena za najdeno in poročano ranljivost je ocena stroškov iskanja ranljivosti v programski opremi, kjer lahko sodeluje vsak.

iDefense in Tipping Point sta dve podjetji, ki odprto kupujeta ranljivosti, kar priča o tem, da trg ranljivosti dejansko obstaja. Njihov poslovni model je istočasna objava podatkov o ranljivosti svojim strankam in proizvajalcu, na katerega se ranljivost nanaša. Njihove stranke lahko na ta način naredijo varnostne posodobitve (npr. na požarnih pregradah) pred ostalimi.

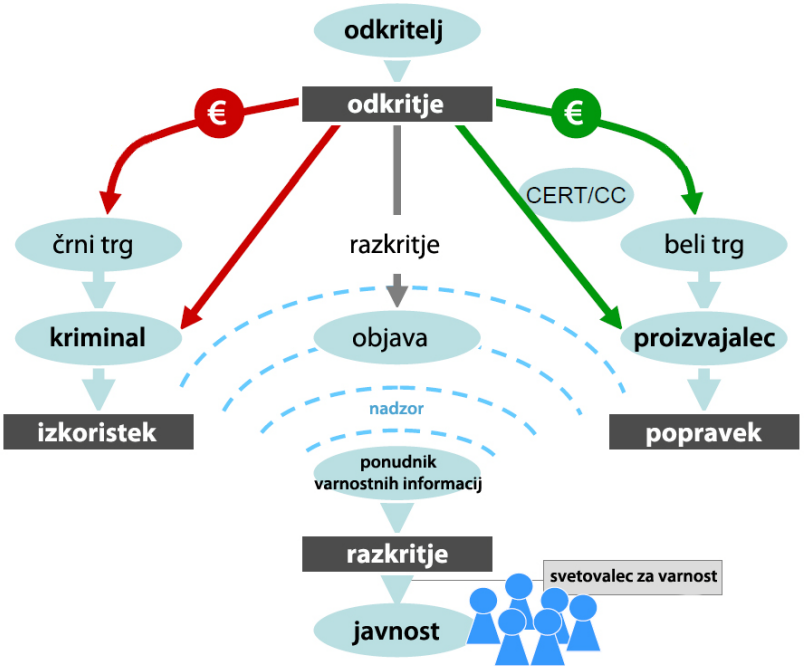
Drugi primer je CERT, ki za odkrite ranljivosti nič ne plača ali zaračuna. CERT deluje kot informacijski posrednik med uporabniki, proizvajalcem in prijaznim odkriteljem, ki prostovoljno in brez finančnih koristi poroča o ranljivosti. Da bi zagotovili, da takšnih javnih obvestil ne izkoriščajo napadalci, CERT kontaktira proizvajalca, da pripravi ustrezen popravek in čaka na primeren čas, preden javno razkrije ranljivost (Bojanc & Jerman-Blažič 2008a).

Za trg ranljivosti je bilo predlaganih nekaj sprememb. Böhme predlaga, da bi proizvajalec plačal za vsako odkrito ranljivost (Böhme, 2006, str. 298), Ozment (2004) pa, da trg ranljivosti deluje kot dražba.

Odkrivanje ranljivosti v programski opremi je povzročilo veliko zanimanja in vroče debate med varnostnimi strokovnjaki (Anderson & Schneier, 2005, str. 12; Kannan & Telang, 2004; Arora & Telang, 2005, str. 20). Pristaši odprtokodnih skupnosti zagovarjajo, da je iskanje in razkrivanje ranljivosti družbeno zaželeno. Anderson (2005) je leta 2002 pokazal, da je varnost odprtih sistemov takšna kot drugje, ter da objava ranljivosti enako pomaga tako napadalcem kot braniteljem. Rescorla (2004) po drugi strani trdi, da v programski opremi z mnogo ranljivosti, odstranitev ene ranljivosti le malo doprinese k verjetnosti, da napadalec ne bo kasneje odkril nove ranljivosti. Razkritje ranljivosti pomaga tudi motivirati proizvajalce, da odpravijo hrošče (Arora, Telang & Xu, 2004). Arora je pokazal, da javno razkritje ranljivosti proizvajalce spodbudi, da se s popravki odzovejo hitreje (Arora et al., 2004). Pri tem napadi na začetku naraščajo, število objavljenih ranljivosti pa se s časom zmanjšuje.

Na sliki 10 so prikazani procesi varnostnega ekosistema in odvisnosti med posameznimi fazami življenjskega cikla ranljivosti (Frei et al., 2009).

Slika 10: *Glavni procesi varnostnega ekosistema glede ranljivosti.*



Vir: Frei, Schatzmann, Plattner & Trammell, Modelling the Security Ecosystem - The Dynamics of (In)Security, 2009, str. 6.

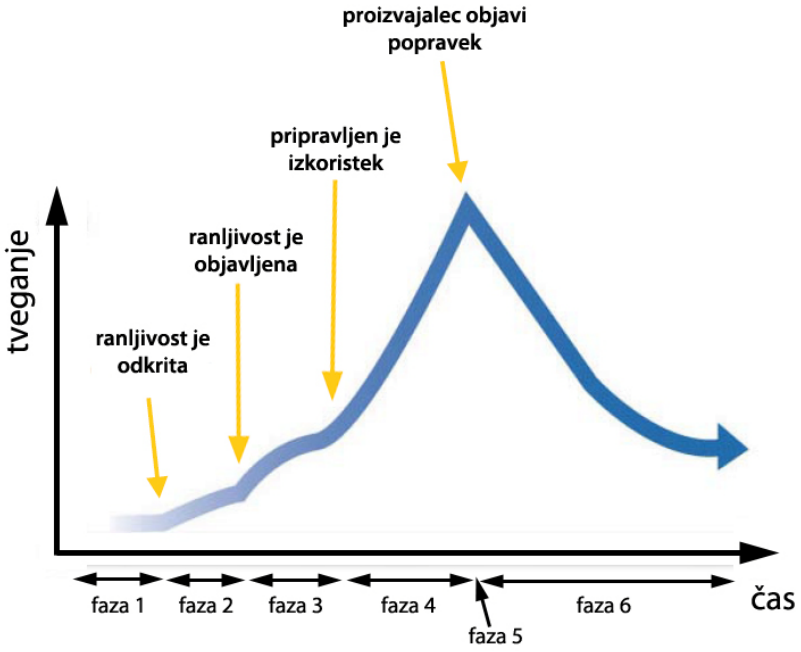
3.3.2 Popravki programske opreme

Za odpravo ranljivosti v programski opremi proizvajalci razvijajo popravke. CERT navaja, da bi lahko z ažurnim nameščanjem popravkov preprečili približno 95 % varnostnih incidentov (Dacey, 2003). Časovno okno med identifikacijo ranljivosti in ugotovitvijo načina za zlorabo, se je v preteklih letih dramatično zmanjšalo. Zato se morajo podjetja prilagoditi in varnostne popravke namestiti takoj, ko jih objavi proizvajalec, da preprečijo škodo zaradi zlonamernih dejanj (August & Tunca, 2005; Cavusoglu, Cavusoglu & Zhamg, 2006). Znano pa je, da številni sistemi tudi več mesecev ali celo let niso posodobljeni, kar lahko povzroči resne posledice in škodo (Shostack, 2003; McGhie, 2003; Register 2003; Moore, Shannon & Brown, 2002). Primer je črv Nimbda, ki je leta 2001, v prvih 24 urah delovanja, okužil 2,2 milijona računalnikov, čeprav je bil popravek te ranljivosti na voljo že skoraj eno leto pred incidentom (Dacey, 2003). Drugi primer je črv SQL Slammer, ki je okužil 90 % ranljivih sistemov, za katerega je bil popravek javno na voljo 6 mesecev prej. 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.

Cavusoglu in Arora sta raziskovala, kako politika razkritja vpliva na čas, da proizvajalec objavi popravek (Cavusoglu, Cavusoglu & Raghunathan, 2004; Arora, Telang & Xu, 2004), Cavusoglu pa je pokazal, da sinhronizacija izida popravka in posodobitvenih ciklov zmanjšuje izgube (Cavusoglu, Cavusoglu &, Zhang 2008, str. 657).

Na sliki 11 so prikazane faze ranljivosti po odkritju. Graf prikazuje tveganje v odvisnosti od časa. Pomembna ugotovitev je, da tveganje nikoli ne pade na nič (Schneier, 2002a, 2002b).

Slika 11: *Faze ranljivosti skozi čas*



Vir: Schneier, 2002a

Faza 1: čas preden je ranljivost odkrita. Ranljivosti so običajno ustvarjene po naključju, kot napaka pri kodiranju in se pogosto nanaša na slabo ravnanje s (sistemskim) spominom. Če se ranljivosti skozi faze razvoja in testiranja programske kode ne odkrije, obstaja verjetnost, da se bo pojavila v splošno objavljeni kodi, ko bo izšla (IBM ISS, 2009). V tem času tveganja ni.

Faza 2: po odkritju ranljivosti, vendar pred njeno javno objavo. Čas odkritja je najzgodnejši čas, ko je zaznano, da ranljivost predstavlja varnostno tveganje. Ranljivosti sicer obstajajo že pred tem časom, vendar do tega trenutka še ni znano, da predstavljajo varnostno tveganje. V tem času je tveganje zelo omejeno.

Faza 3: javna objava ranljivosti. Namen razkritja je, da so varnostne informacije na voljo javnosti v standardizirani in razumljivi obliki. Razkritje je pomemben dogodek v varnostnem ekosistemu (Arbaugh, Fithen & McHugh, 2000, str. 52; Arora et al., 2004; OISA). V tem času je tveganje večje.

Faza 4: pripravljen je izkoristek, ki zlorablja ranljivost. Ranljivost se lahko zlorabi s pomočjo programske opreme (npr. virusa, zaporedja ukazov, nabora podatkov), ki povzroči nepredvideno ali nepričakovano obnašanje v programski opremi ali napravah. Hekerski malčki (angl. *Script Kiddy*), ki nimajo znanja, da sami zlorabijo ranljivost, si pomagajo z raznimi skriptami. V tem času tveganje občutno naraste.

Faza 5: proizvajalec objavi popravek. Razpoložljivi čas popravka je čas, ko proizvajalec javno objavi popravek, ki zagotavlja zaščito pred izkoriščanjem ranljivosti. Nekateri proizvajalci programske opreme objavljajo popravke sproti, takoj, ko so ti na voljo, drugi pa objavljajo popravke v planiranih časovnih intervalih, ki olajšajo načrtovanje namestitve popravka (npr. mesečna ali četrtletna redna objava popravkov). Drugi varnostni mehanizmi, kot so sistemski podpisi za preprečevanje vdora ali protivirusne definicije, se ne štejejo za popravke. V tem trenutku je tveganje največje, a začne takoj po izdaji padati zaradi nameščanja popravkov.

Faza 6: namestitve popravka. Uporabniki programske opreme lahko z namestitvijo popravka v svoj sistem le pridobijo, saj odpravijo ranljivost sistema. Sam postopek, ki traja od časa razpoložljivosti popravka do časa namestitve popravka, se lahko precej razlikuje od podjetja do podjetja. V tem času tveganje počasi pada glede na intenzivnost nameščanja popravkov.

3.4 Varnostni incidenti

Standard ISO 27000 (2009) podaja sledečo definicijo za **informacijsko varnostni incident**:

> *"Eden ali serija neželenih ali nepričakovanih dogodkov v zvezi z informacijsko varnostjo, za katere je zelo verjetno, da bodo ogrozili poslovanje in informacijsko varnost."*

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 tudi povzroči nezanimanje vlagateljev, ki se zanimajo za dolgoročno uspešnost podjetja. Varnostni incidenti zmanjšujejo prihodne denarne tokove, obenem pa lahko tudi znižujejo ceno delnic (Farahmand, 2004).

Varnostni incidenti so različnih vrst. Nekateri incidenti so vezani na zaupnost, kot na primer kraja bančnih računov. Drugi incidenti so vezani na celovitost, kot na primer zlonameren izbris ali sprememba dela podatkovne baze podjetja. Tretji incidenti so vezani na razpoložljivost, kot na primer DoS napadi, ki preprečujejo

uporabo storitev vsem (avtoriziranim in neavtoriziranim) uporabnikom (Gordon & Loeb, 2005, str. 55).

Varnostni incidenti se med seboj ne razlikujejo samo po vrsti, temveč predvsem po obsegu. Nekateri incidenti vplivajo le na del informacij ali informacijskega sistema podjetja. Drugi incidenti imajo vpliv na celotno podjetje ali celo več podjetij. Incident lahko povzroči verižno reakcijo incidentov ali posredne incidente. Na primer izguba zaupnih občutljivih informacij vodi do izgube zaupanja strank.

Dodatna metoda za razvrščanje obsega incidenta je vrednost ogrožene informacije ali sredstva (Gordon & Loeb, 2005, str. 55). Na primer neavtoriziran dostop do skrivne formule podjetja je lahko mnogo dražji, 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. 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 obdobju tistih desetih sekund, v katerih je z geslom mogoč dostop do omrežja (Soo Hoo, 2000).

3.4.1 Verjetnost za incident

Strokovnjaki za informacijsko varnost se še niso poenotili, katera je najboljša ali najbolj ustrezna metoda za oceno verjetnosti incidentov računalniške varnosti. Določene metode, kot so kontrolni seznami in tehnike generiranja scenarijev, zahtevajo od uporabnika le minimalno znanje o varnosti informacijskega sistema (Wood et al., 1987). Če želimo imeti dobro opredeljen obseg za kontrolne sezname, je priporočljivo upoštevati standarde[7].

Ocenjevanje verjetnosti incidentov, ki jih povzroča človek, je lahko subjektivno in zapleteno. Farahmand (2004) upošteva naslednje dejavnike:

- **Motiv**. Kako motiviran je napadalec? Ali je napadalec politično motiviran? 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?

[7] Podroben pregled standardov je v poglavju 1.3.2.

Med letoma 1988 in 1991 je NIST izvedel štiri delavnice, katerih cilj je bil izboljšati modele tveganja za informacijske tehnologije. Oktobra 2001 je NIST objavil vodnik za obvladovanje tveganja za sisteme informacijske tehnologije NIST 800-30 (2002), v katerem priporoča, da se pri ocenjevanju verjetnosti dogodkov uporablja samo tri kvalitativne kategorije:

- Visoka verjetnost. Povzročitelj grožnje je zelo motiviran in dovolj sposoben; obstoječe kontrole so neučinkovite pri preprečevanju napada.
- Srednja verjetnost. Povzročitelj grožnje je motiviran in sposoben; kontrole so uvedene in lahko ovirajo uspešen napad.
- Majhna verjetnost. Povzročitelj grožnje nima motivacije ali sposobnosti; uvedene kontrole preprečujejo ali vsaj bistveno ovirajo napad.

Enake tri kategorije priporoča tudi metoda OCTAVE (Alberts & Dorofee, 2001; Alberts & Dorofee, 2002). Ocene, pridobljene na tak kvalitativen način ni mogoče uporabiti za oceno letne pričakovane izgube (ALE) ali druge kvantitativne meritve stroškov (Schechter, 2004).

Druga možnost je dodelitev kvantitativnih ocen verjetnosti za incident. Vrednosti so zaradi lažje predstave običajno v odstotkih. Kvalitativne ocene se lahko prevedejo v kvantitativne in obratno. Tako se dobi na primer vrednost 0,9 za veliko verjetnost, vrednost 0,5 za srednjo verjetnost in 0,1 za nizko verjetnost. Namesto trinivojske lestvice se lahko uporabi bolj podrobna. Na primer kvantitativna vrednost 0,9 za zelo visoko kvalitativno vrednost, 0,7 za visoko, 0,5 za srednjo, 0,3 za nizko in 0,1 za zelo nizko. Pri tem je nesmiselno pretiravati s preveč podrobno delitvijo, ker gre zgolj za oceno vrednosti.

3.4.2 Izguba ob incidentih

Ekonomske posledice varnostnih incidentov so lahko zelo velike. Raziskave kažejo, da se povprečna letna izguba v zadnjih letih zmanjšuje (CSI, 2009). Dejanske izgube zaradi varnostnih incidentov so večplastne in jih je težko ovrednotiti. Merjenje izgub zaradi varnostnih incidentov zato ni enostavna naloga. Pregled literature kaže na veliko raziskav o stroških, ki so jih povzročili varnostni incidenti (Anderson, 2001; Butler, 2002, str. 232; Cohen, 1991, str. 239; Dobson, 1994, str. 10; Orlandi, 1989; Tarr, 1995, str. 183; Farahmand, 2004).

Vsako podjetje mora razumeti finančne stroške, ki nastanejo v primeru varnostnega incidenta. Stroški varnostnega incidenta se merijo glede na to, kako vplivajo na poslovanje (Farahmand, 2004). Ko podjetje doleti varnostni incident, se posledice lahko močno razlikujejo od podjetja do podjetja. Kadar dve podjetji doleti isti incident, lahko eno podjetje utrpi škodo, medtem ko drugo ne. Eno podjetje ima lahko uvedene učinkovite postopke arhiviranja, medtem ko drugo ne.

Eno podjetje ima lahko učinkovite povezave s svojimi proizvajalci informacijske varnosti in zunanjih izvajalcev, medtem ko drugi ne.

Soo Hoo (2000) zagovarja, da je pri vrednosti posledic varnostnega incidenta potrebno upoštevati dva scenarija: prvega, v katerem se varnostni incident zgodi ter drugega, v katerem se ne. Razlika med obema scenarijema je osnova za vrednotenje posledic. Če na primer sistem naročanja pri proizvajalcu utrpi enotedenski izpad, izguba ni enaka enotedenskemu izpadu poslovanja, ker sistem ni mogel sprejemati naročil. Proizvajalec bi za čas nedelovanja lahko poiskal alternativo za naročanje. Stroške posledic je v tem primeru bolj ustrezno izračunati s primerjavo prihodkov med obema scenarijema.

ISF (2006) predlaga kategorizacijo poslovnih izgub zaradi varnostnih incidentov v kategorije:

- Finančne izgube:
  - izguba prodaje, naročil ali pogodb,
  - izguba fizičnega sredstva,
  - kazni in pravne obveznosti,
  - nepredvideni stroški,
  - manjša kreditna sposobnost,
  - padec vrednosti delnic na borzi,
  - povečanje zavarovalne premije.

- Operativne izgube:
  - izguba nadzora upravljanja,
  - izguba konkurenčnosti,
  - kršitev standardov delovanja.

- Izgube vezane na stranko:
  - zamuda pri dobavi kupcem ali strankam,
  - izguba strank,
  - izguba zaupanja ključnih institucij,
  - zmanjšan ugled,
  - priložnosti ni mogoče pretvoriti v nove stranke.

- Izgube vezane na zaposlene:
  - zmanjšanje morale in produktivnosti zaposlenih,
  - poškodba ali smrt.

Eden izmed osnovnih načinov za kategorizacijo je ločitev na takojšnje in posredne izgube. Takojšnje izgube predstavljajo stroške, ki jih lahko jasno povežemo s posameznimi incidenti. To so običajno stroški, vezani na osebje, strojno opremo in programsko opremo. Tipične takojšnje izgube so na primer izguba prihodka, izguba produktivnosti in povečanje stroškov (nadure, višje zavarovalne premije

itd.). Čeprav se lahko takojšnje izgube po obsegu precej razlikujejo med seboj, imajo skupno lastnost to, da se jih lahko poveže direktno z določenim incidentom (Gordon & Loeb, 2005, str. 56).

V nasprotju s takojšnjimi izgubami, se posrednih izgub ne more z dovolj veliko verjetnostjo povezati direktno s posameznim incidentom (Gordon & Loeb, 2005, str. 56). Kot posredne izgube štejemo predvsem naslednje (Farahmand, 2004; Bojanc & Jerman-Blažič, 2008a):

- podoba blagovne znamke, javni ugled in dobro ime na trgu,
- finančne vrednosti poslov,
- zaupanje javnosti in strank v pravilnost poslovnih transakcij,
- sposobnost obnavljanja prihodkov denarnega toka v ustreznem času,
- sposobnost za reševanje sporov onkraj razumnega dvoma,
- sposobnost za izpolnjevanje pravnih zahtev in zahtev regulatorjev,
- izguba intelektualne lastnine.

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 et al., 2004). Posredne izgube imajo lahko v določenih situacijah veliko daljši negativni vpliv na stranke, dobavitelje, finančni trg, banke in poslovne partnerje kot takojšnje izgube (Camp & Wolfram, 2004; Dynes, Andrijcic & Johnson, 2006; Rowe & Gallaher, 2006).

Za lažji izračun izgub, razdeli Denning (1999) stroške na tri področja, ki so vezana na zlorabe zaupnosti, celovitosti in razpoložljivosti. Prvo področje 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 …).

Drugo področje so stroški zaradi nedostopnosti, ki nastanejo, kadar informacijska sredstva niso na voljo v določenem časovnem obdobju. Bodisi zato, ker so bila sredstva 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 (Denning, 1999):

- izgubo prihodkov zaradi nedelovanja (direktna 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.

Tretje področje so stroški, ki izhajajo iz zlorab zaupnosti. Ti stroški lahko vključujejo (Denning, 1999):

- 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 …).

V kolikor kršitve informacijske varnosti vključujejo nepooblaščen dostop do zaupnih podatkov, je lahko reakcija trga zelo negativna, medtem ko v drugih primerih ni zaznati posebnih reakcij trga (Campbell et al., 2003, str. 431; Hovava & D'Arcy, 2003, Farahmand, 2004). Ta ugotovitev je skladna s poročilom CSI/FBI iz leta 2002, kjer so najbolj resne finančne izgube povezane s krajo zaupnih podatkov. Finančne izgube zaradi kršitev zaupnosti podatkov so večkrat povezane z odškodninami, ki so lahko zelo visoke.

3.4.3 Izračun pričakovane letne izgube zaradi incidentov (ALE)

Leta 1975 je National Bureau of Standards, predhodnik National Institute of Standards and Technology (NIST), objavil Federal Information Processing Standard (FIPS) 65: Smernice za avtomatsko obdelavo podatkov analize tveganja (angl. *Guideline for Automatic Data Process Risk Analysis*). Dokument definira in predlaga uporabo metode ALE za kvantitativno merjenje tveganja informacijske

varnosti. Standard FIPS 65 je bil sicer leta 1995 ukinjen (Withdrawn FIPS, 2010) in merjenje po metodi ALE ni postalo del obvezujočih standardov, je pa metoda ALE v krogih informacijske varnosti postala splošno znana in pogosto uporabljena (Soo Hoo, 2000; Gordon & Loeb, 2005, str. 75). Pričakovana letna izguba (oziroma natančneje pričakovana vrednost izgub) združuje dva ključna elementa povezana s tveganjem: pogostost incidentov in velikost izgube.

Pogostost incidentov pri merjenju ALE pove, kolikokrat na leto lahko podjetje upravičeno pričakuje določen dogodek. Nekaj primerov za pogostost incidentov je prikazanih v tabeli 3:

Tabela 3: *Prikaz pogostosti za incidente pri merjenju ALE*

Pogostost	**Preračunana vrednost na eno leto**	
Nikoli		0
Enkrat na 300 let	1/300	0,00333
Enkrat na 200 let	1/200	0,005
Enkrat na 100 let	1/100	0,01
Enkrat na 50 let	1/50	0,02
Enkrat na 25 let	1/25	0,04
Enkrat na 5 let	1/5	0,2
Enkrat na 2 leti	1/2	0,5
Letno	1/1	1
Dvakrat letno	2/1	2
Enkrat ne mesec	12/1	12
Enkrat na teden	52/1	52
Enkrat na dan	365/1	365

Velikost izgube predstavlja skupno vsoto prihodka, ki je izgubljen zaradi ene ponovitve tveganja. Je denarna vrednost, ki je vezana na en sam dogodek in predstavlja potencialno izgubo, ki bi jo imelo podjetje v primeru incidenta (Bojanc & Jerman-Blažič, 2008a).

ALE se izračuna z množenjem pogostosti incidentov in velikosti izgube. Predpostavimo, da je *n* možnih incidentov, ki se lahko zgodijo v enem letu in vsak možen incident označimo z indeksom *i*. Naj bo *I* predlagana investicija v informacijsko varnost (ali skupina investicij). Investicija v informacijsko varnost vpliva na pogostost incidentov (koliko incidentov se zgodi v danem letu) in na obseg izgube povezane z incidentom. Naj bo *Pi(I)* pogostost, da se incident *i* zgodi v

danem letu ob investiciji *I.* Naj bo *Li(I)* letna izguba v denarni enoti, ki jo podjetje utrpi, če se zgodi incident *i* ob investiciji *I*. ALE vezano na investicijo *I* lahko zapišemo:

$$ALE(I) = \sum_{i=1}^{n} Li(I)\, Pi(I) \tag{2}$$

Na primer, če okužba z računalniškim virusom v podjetju predstavlja 17.500 € izgube in se pričakuje eno okužbo na dve leti (pogostost okužbe je 0,5), znaša ALE 17.500 € × 0,5 = 8.750 €.

Izračun ocen pogostosti incidenta in velikosti izgube je lahko zelo težaven. Določevanje točnih vhodnih vrednosti za ALE je za človeške grožnje občutno težje kot za naravne nesreče (Anderson, 1991; Soo Hoo, 2000). Pri izračunu vrednosti ALE za primere naravnih nesreč (npr. potres, poplava) se lahko predvideva pričakovano ponovitev incidentov na podlagi zgodovinskih podatkov. Ta predvidevanja je potrebno nato prilagoditi aktualnim trendom. Modeli lahko natančno napovedujejo bodoče dogodke na podlagi zgodovinskih podatkov le, kadar so statistična razmerja, na katerih je model zgrajen, skozi čas stacionarna. Kadar se vpliv neodvisnih spremenljivk na odvisne spremenljivke spreminja, bo predvidevanje modela nezanesljivo. To stacionarno zahtevo je težko doseči, kadar gre za modeliranje dogodkov, ki jih povzroča človeški faktor (npr. zlonamerni posamezniki). Za razliko od narave, zlonamerni uporabniki poskušajo izvesti napad na najšibkejšo točko sistema, neprestano izboljšujejo svoja znanja ter onemogočajo poskuse merjenja njihovega obnašanja (Schechter, 2004). In četudi bi se zlonamerni uporabniki obnašali stacionarno, primanjkuje zgodovinskih podatkov za človeške grožnje (NIST 800-12, str. 63).

Izračunavanje ALE že nekaj časa uporabljajo zavarovalnice, trenutno pa to tehniko uporablja večina kvantitativnih analiz tveganj informacijske varnosti. Za razliko od zavarovalniških tveganj, ki se osredotočajo na izgube, ki izhajajo iz zavarovalnih zahtevkov, lahko varnostna tveganja ocenimo zgolj z upoštevanjem kompleksnih kombinacij možnih posledic. Poleg tega varnostna tveganja niso neposredno izražena v povsem denarnih enotah. Farahmand (2004) navaja, da so potencialne izgube pogosto povezane z dejavniki, kot so dobro ime podjetja ali drugimi nedenarnimi sredstvi. Zelo težko je na primer izmeriti obseg izgube zaupanja strank po nekem varnostnem incidentu.

Gordon in Loeb (2005, str. 100) ločita dva tipa managerjev, ki sprejemajo odločitev glede investicije. Managerju, ki ga zanima zgolj pričakovana donosnost investicije (angl. *risk-neutral manager*), popolnoma zadostuje podatek o izračunu pričakovane letne izgube (ALE), da se odloči glede določene investicije. Drugi primer je manager, ki bolj favorizira investicijo z gotovo donosnostjo (angl. *risk-averse manager)*, kot investicijo z negotovo donosnostjo, ki ima 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 incidenta ne bo prišlo.

Uporaba ALE ima nekaj pomanjkljivosti (Gordon & Loeb, 2005, str. 76):

- ALE predpostavlja, da so možne izgube zaradi varnostnih incidentov konstantne skozi čas.
- ALE opredeli tveganje glede na izgube, ki bodo ostale po izvedeni investiciji, ne podaja pa pravila za izbiro najboljše investicije.
- ALE gleda le s strani koristi varnostne investicije in jih ne primerja s stroški izboljšav informacijske varnosti.

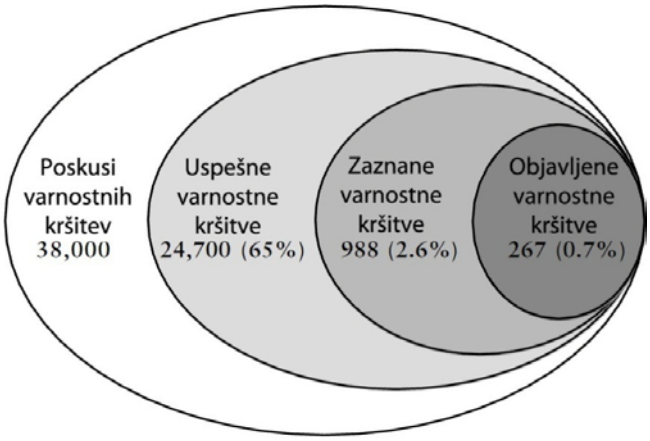
3.4.4 Empirične ugotovitve

Podatke o pravih stroških, povzročenih zaradi varnostnega incidenta, je zelo težko pridobiti. Strokovnjaki za varnost se strinjajo, da je število dejanskih incidentov precej večje, kot prikazujejo uradno objavljeni podatki. Eden od razlogov je, da večina podjetij sistematično ne odkriva, nadzira in beleži varnostnih incidentov. Drugi razlog je, da se podjetja s temi problemi ukvarjajo interno. Podjetja, ki doživijo napad, pogosto o tem raje molčijo, kot da bi napad objavile. 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 in dragih varnostnih incidentov ni nikoli objavljenih (Bojanc & Jerman-Blažič, 2007). V zadnji raziskavi CSI (2009) je bilo le 25 % sodelujočih pripravljenih razkriti podrobnosti o finančnih izgubah, ki so jih utrpeli in to kljub anonimnosti raziskave.

Soo Hoo (2000) navaja podatke iz raziskave, ki jo je leta 1996 objavila organizacija Defense Information Systems Agency (DISA) znotraj programa Vulnerability Analysis and Assessment Program. Poročilo ocenjuje, da ostaja 96 % odstotkov uspešnih kršitev nezaznanih in izmed vseh zaznanih je poročanih le 27 %. Podatki so predstavljeni na sliki 12. Navedeni podatki so sicer že precej zastareli, vendar vseeno odražajo neko dimenzijo glede števila poskusov kršitev in javno objavljenimi podatki.

Trenutno najbolj ažurne podatke o varnostnih incidentih podajajo letna poročila različnih raziskav (CSI, 2009; DSCI, 2009; BERR, 2008; CERT, 2008; DTI, 2006). Ta poročila so povzetek raziskav, v katerih podjetja poročajo o letnih stroških, ki so nastali zaradi različnih varnostnih incidentov. Empirični podatki so na voljo tudi pri organizacijah, ki se ukvarjajo s svetovanjem na področju informacijske varnosti, kot so CERT, SecurityFocus, IBM ISS X-Force, Secunia, Vupen, SecurityTracker, iDefense in TippingPoint. Podatki o varnostnih zlorabah so na voljo tudi pri Milw0rm, Packetstorm, SecurityVulns in Metasploit.

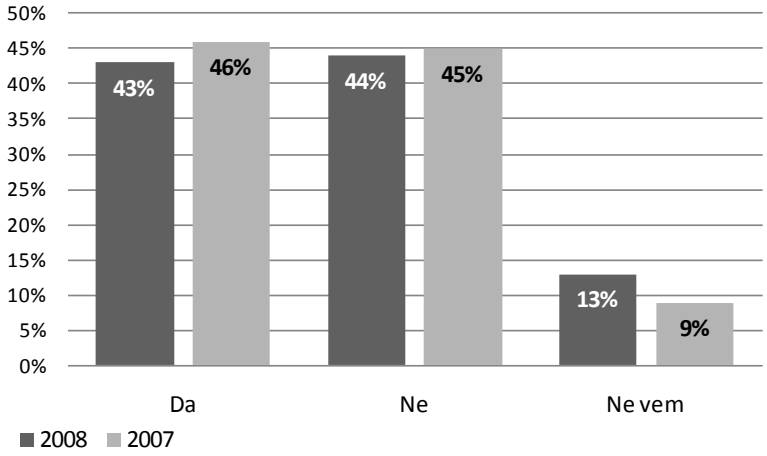
Slika 12: *Rezultati raziskave analiza ranljivosti in ocenitve tveganja*



Vir: Soo Hoo, How Much Is Enough? A Risk-Management Approach to Computer Security, 2000, str. 31.

Po rezultatih raziskave CSI (2008) je v letih 2007 in 2008 skoraj polovica podjetij v posameznem letu doživela varnostni incident. Zanimivo je, da se je v zadnjem letu malo povečalo število podjetij, ki so doživela incident, in podjetij, ki ga niso doživela, zmanjšalo pa se je število tistih, ki ne vedo za svoje stanje. Rezultati so prikazani na sliki 13.

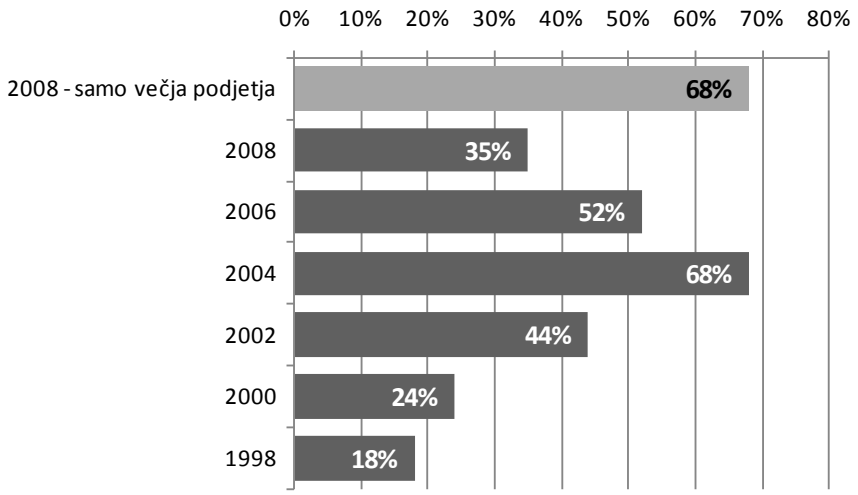
Slika 13: *Doživeti varnostni incidenti*



Vir: CSI Computer Crime and Security Survey 2008, str.13.

Po raziskavi BERR (2008), ki je zajela podjetja v Veliki Britaniji, se povprečno število podjetij, ki so doživela varnostni incident, v zadnjih letih zmanjšuje – iz 68 % v letu 2004 na 35 % v letu 2008. Pri večjih podjetjih je število podjetij, ki so doživela varnostni incident občutno večje – 68 %. Rezultati so prikazani na sliki 14.

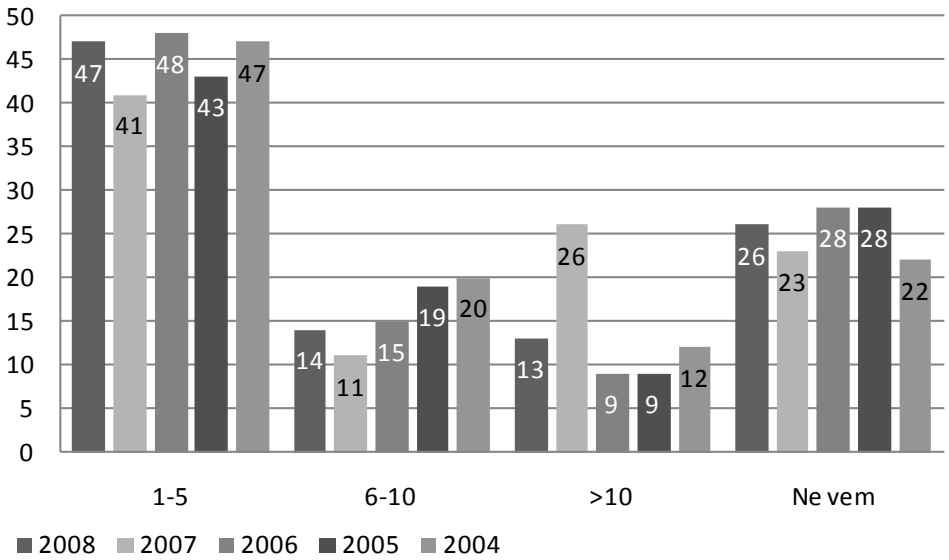
Slika 14: *Delež podjetij, ki so v zadnjem letu imela zlonameren varnostni incident*



Vir: BERR Information Security Breaches Survey 2008, str.22.

Slika 15 prikazuje število incidentov, ki jih utrpijo podjetja v posameznem letu. Že več let zaporedoma utrpi večina podjetij od enega do pet incidentov na leto (CSI, 2008). Ti rezultati veljajo le za podjetja, ki so imela vsaj en incident.

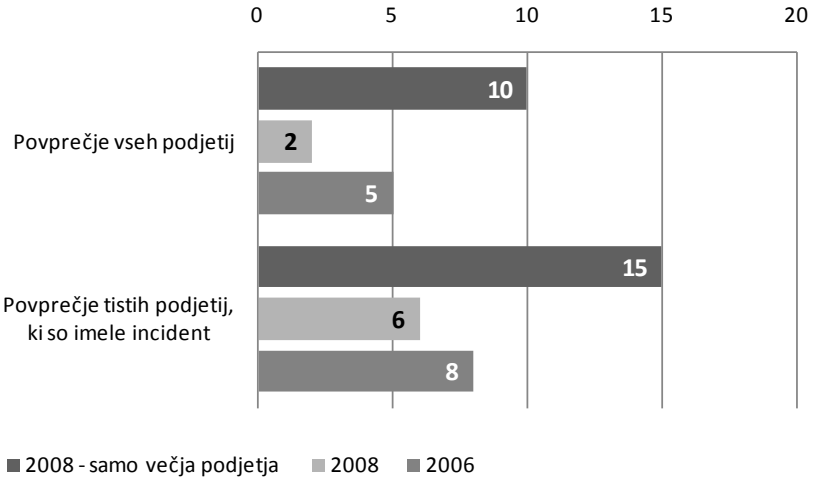
Slika 15: *Število incidentov v odstotkih*



Vir: CSI Computer Crime and Security Survey 2008, str.13.

Podobne rezultate prikazuje raziskava BERR (2008). Podjetja, ki utrpijo varnostni incident, doživijo v povprečju 6 incidentov na leto, večja podjetja pa kar 15 incidentov letno. Rezultati so prikazani na sliki 16.

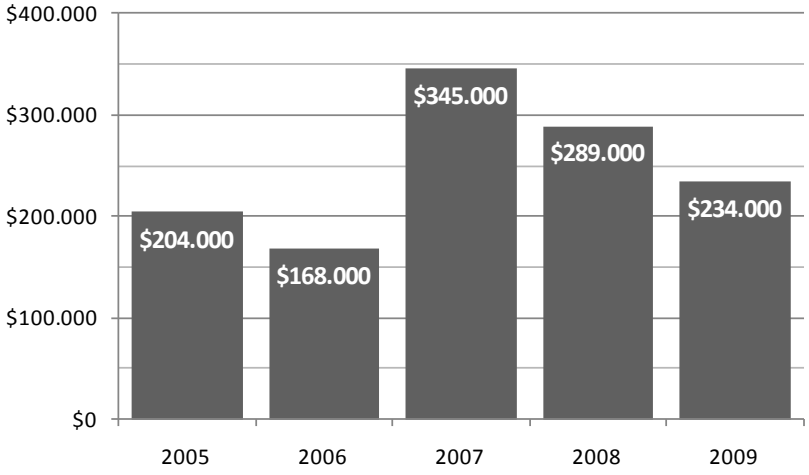
Slika 16: *Povprečno število zlonamernih incidentov v zadnjem letu*



Vir: BERR Information Security Breaches Survey 2008, str.22.

Po rezultatih raziskave CSI (2009) so se povprečne izgube zaradi varnostnih incidentov v letu 2009 zmanjšale za 20 % glede na leto 2008, vendar so še vedno višje kot v letih 2005 in 2006. Rezultati so prikazani na sliki 17. Največje izgube predstavljajo grožnje, kot so zloraba brezžičnih omrežij (povprečna izguba $770,000 na podjetje, ki je utrpelo incident), kraja mobilnih naprav (povprečna izguba $710,000) in finančna zloraba (povprečna izguba $450,000).

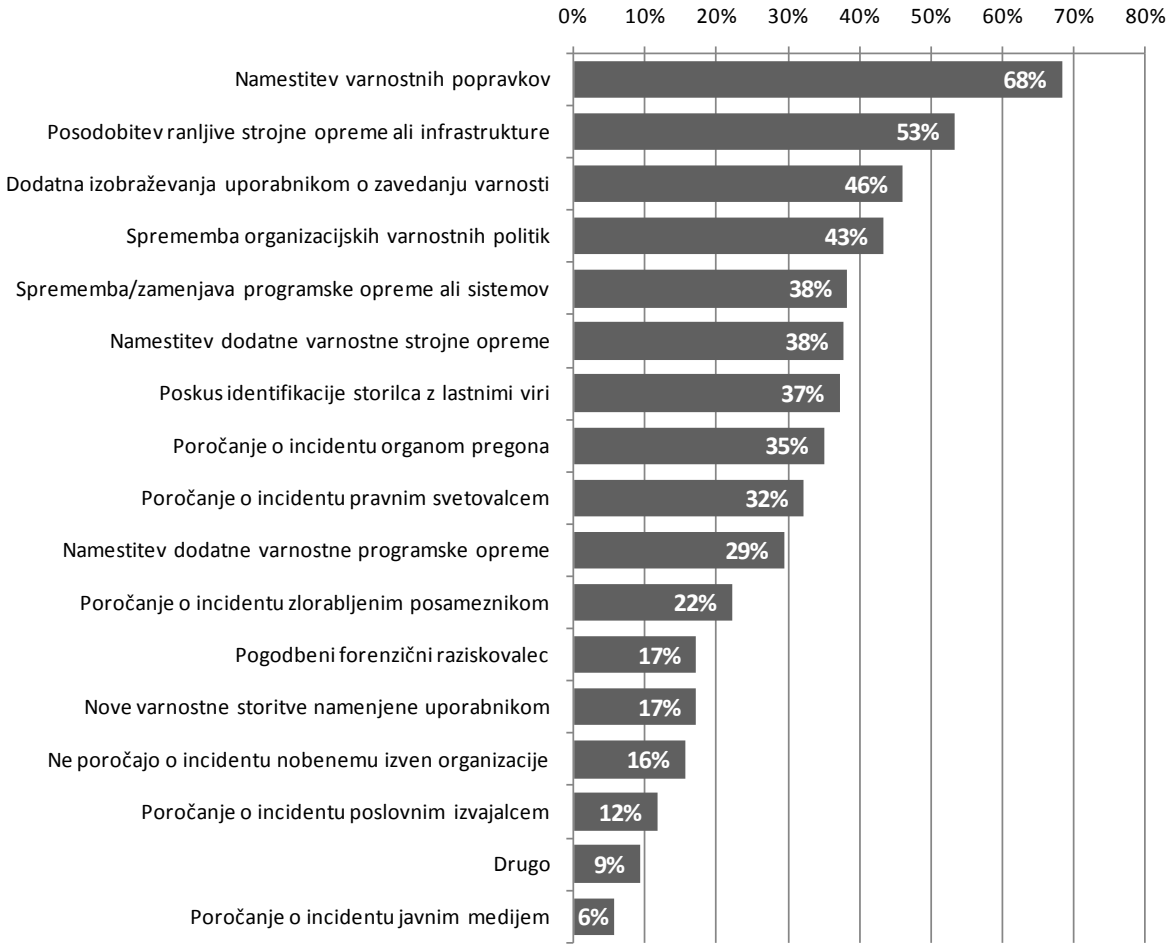
Slika 17: *Povprečna izguba podjetja*



Vir: CSI Computer Crime and Security Survey 2009, str.10.

V primeru, da se zgodi varnostni incident, večina podjetij najprej popravi ugotovljene ranljivosti na strojni in programski opremi ter izvede izobraževanje zaposlenih o informacijski varnosti (CSI, 2009). Rezultati so prikazani na sliki 18.

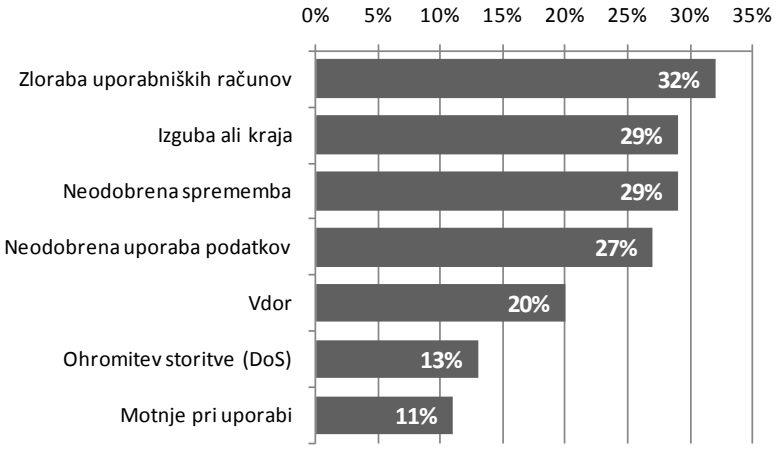
Slika 18: *Izvedene aktivnosti po varnostnem incidentu*



Vir: CSI Computer Crime and Security Survey 2009

Po raziskavi DSCI-KPMG, opravljeni med podjetji v Indiji, so najbolj pogosti incidenti: zloraba uporabniških računov, izguba ali kraja ter nepooblaščena sprememba ali uporaba podatkov (DSCI, 2009). Rezultati so prikazani na sliki 19.

Slika 19: *Varnostni incidenti*



Vir: DSCI- KPMG Survey 2009, str. 20.

Posledice varnostnih incidentov so za podjetja lahko hude. Podjetja, ki so utrpela incident, izgubijo povprečno v dveh dneh po dogodku približno 2,1 % njihove tržne vrednosti. Varnostni proizvajalci pa pridobijo povprečno 1,36 % od vsake take objave incidenta (Cavusoglu, Mishra, Raghunthan, 2002). Po raziskavi Gartner Group, dve od petih podjetij, ki doživijo katastrofalni dogodek ali daljši izpad delovanja sistema, ne more več nadaljevati poslovanja. Od tistih, ki pa uspejo nadaljevati s poslovanjem, jih ena tretjina propade v obdobju dveh let (Eklund, 2000).

4 Varnostni ukrepi

4.1 Vrste varnostnih ukrepov

Schechter (2004) podaja sledečo definicijo za **varnostni ukrep**:

> *"Politika, proces, algoritem ali drug ukrep, ki se uporablja za preprečevanje ali omejevanje škode povzročene iz enega ali več scenarijev groženj."*

Varnostne ukrepe se pogosto imenuje tudi *protiukrepi*, *kontrole* ali *zaščitni ukrepi*. Varnostni ukrepi so aktivnosti, postopki ali mehanizmi, ki preprečujejo ali zmanjšujejo škodo, povzročeno z realizacijo enega ali več scenarijev groženj. Varnostni ukrepi so lahko fizične ovire, senzorji, programska oprema, algoritmi, izboljšave obstoječih politik ali postopkov. Lahko izvajajo eno ali več naslednjih funkcij: odkrivanje, odvračanje, preprečevanje, omejevanje, popravljanje, okrevanje, nadzor in ozaveščenost (ISO 13335-1). Lahko varujejo pred grožnjami, zmanjšujejo ranljivosti, zmanjšujejo učinek nezaželenih incidentov, odkrivajo nezaželene incidente in olajšajo okrevanje. Primerna izbira varnostnih ukrepov je bistvenega pomena za učinkovito informacijsko varnost.

Informacijska varnost je kombinacija **preventivnih**, **korektivnih** in **detekcijskih** ukrepov (NIST 800-14, 1996). Preventivni ukrepi zmanjšujejo število uspešnih incidentov in s tem verjetnost za incident. Korektivni in detekcijski ukrepi zmanjšujejo posledice napadov na ogroženih sistemih. V tabeli 4 je prikazanih nekaj primerov različnih vrst varnostnih ukrepov.

Izbrana obravnava tveganja (poglavje 2.1.2) pomembno vpliva na možne vrste zaščite. Pri nekaterih ravnanjih so smiselne vse vrste zaščit, pri drugih ne. Relacije med izbiro obravnave tveganja in vrstami zaščit so prikazane v tabeli 5.

Tabela 4: *Primeri različnih vrst varnostnih ukrepov.*

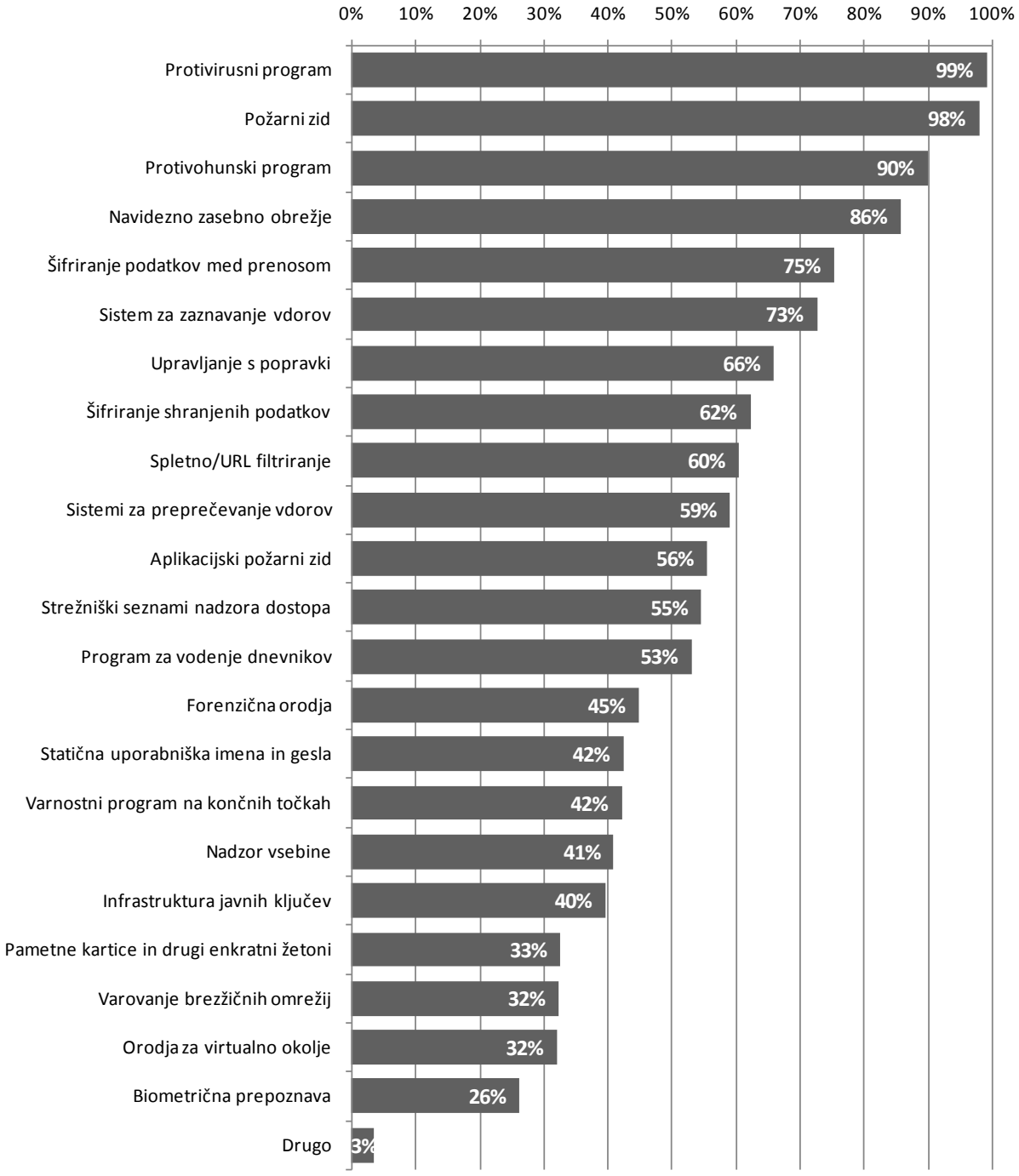
Preventivni varnostni ukrepi	Korektivni varnostni ukrepi	Detekcijski varnostni ukrepi
varnostna politika kriptografija (šifriranje za potrebe zaupnosti, digitalni podpisi) varna arhitektura omrežja in aplikacij ažurno posodabljanje programske opreme s popravki požarni zid sistemi za preprečevanje vdorov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

Tabela 5: *Ustreznost izbire vrste zaščite glede na izbrano obravnavo tveganja*

Izbrana strategija	Preventivni ukrep	Korektivni ukrep	Detekcijski ukrep
Zmanjšanje tveganja z investicijo	da	da	da
Prenos tveganja	delno	da	ne
Izogibanje tveganja	da	ne	delno
Sprejem tveganja	ne	ne	delno

Po raziskavi CSI (2009) sta v zadnjih dveh letih protivirusna programska oprema in požarni zid najpogosteje uporabljena varnostna ukrepa. V zadnjem letu so največji porast zabeležili pri naslednjih ukrepih: protivohunska programska oprema (angl. *anti-spyware*), šifriranje shranjenih podatkov in varovanje končnih točk (angl. *endpoint security*). Rezultati so prikazani na sliki 20.

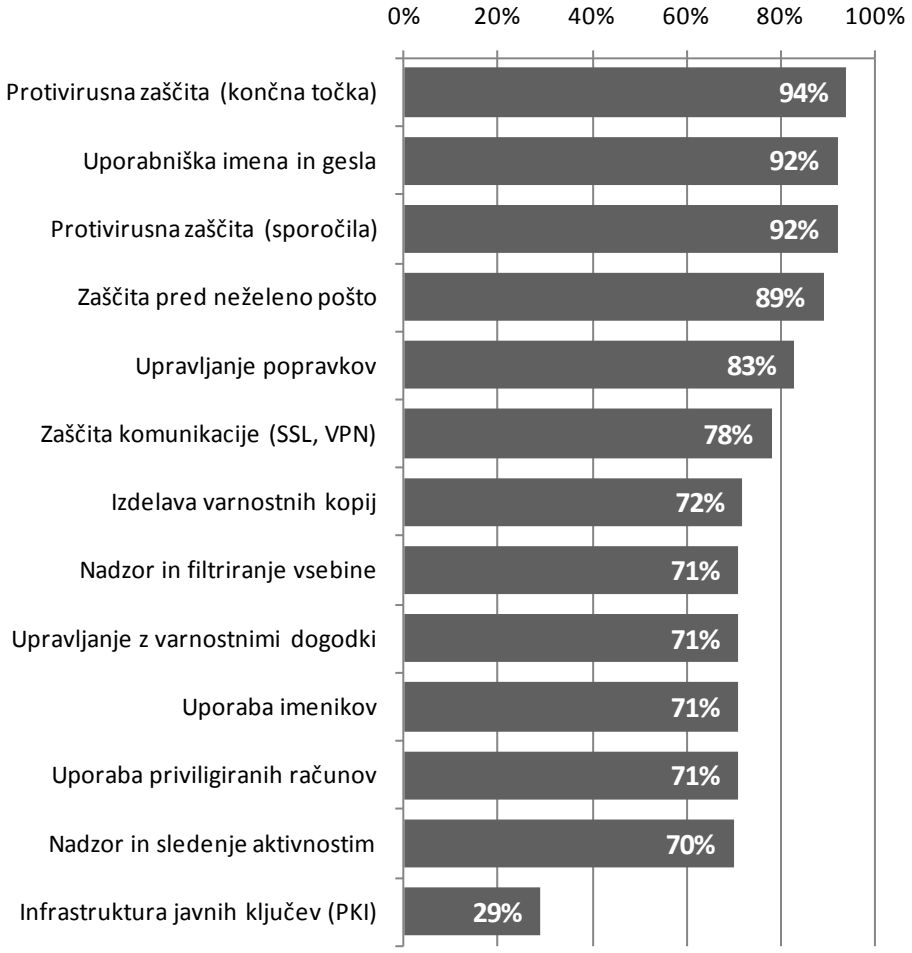
Slika 20: *Vrste uporabljenih varnostnih ukrepov v odstotkih glede na delež sodelujočih podjetij*



Vir: CSI Computer Crime and Security Survey 2009.

Tudi po raziskavi DSCI-KPMG (2009) je protivirusna programska oprema najpogosteje uporabljen varnostni ukrep, sledi uporaba uporabniških imen in gesel ter pregledovanje e-pošte pred virusi. Rezultati so prikazani na sliki 21.

Slika 21: *Najbolj pogosto uporabljeni varnostni ukrepi*

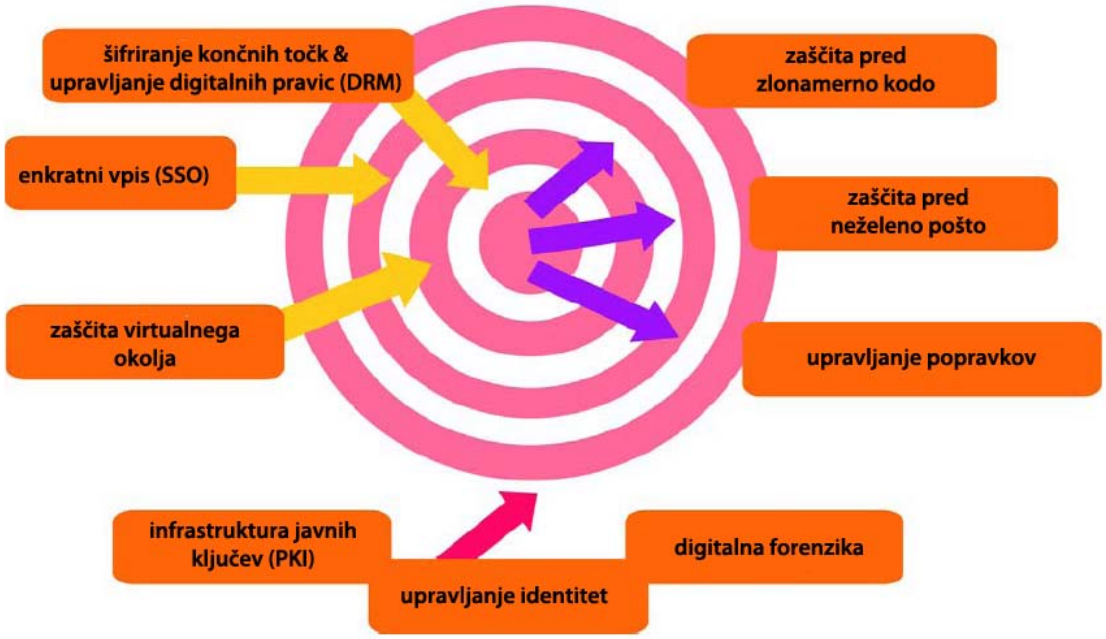


Vir: DSCI- KPMG Survey 2009, str. 36.

Raziskava BERR (2008) ugotavlja, da ima velika večina podjetij v Veliki Britaniji že uvedene najbolj pogoste varnostne ukrepe. 99 % podjetij izdeluje varnostne kopije kritičnih podatkov, 98 % podjetij uporablja programsko opremo, ki pregleduje sistem za vohunsko programsko opremo (angl. *spyware*), 97 % podjetij uporablja filtre za neželeno elektronsko pošto, 97 % podjetij ščiti svoje spletne strani s požarnim zidom, 95 % podjetij pregleduje dohodno e-pošto pred virusi in 94 % podjetij šifrira njihova brezžična omrežja. 55 % podjetij ima dokumentirano varnostno politiko, leta 2002 je bilo takih podjetij le 27 %.

Trend priljubljenosti varnostnih ukrepov se skozi čas spreminja. Na sliki 22 so prikazani aktivni ukrepi, katerih uporaba se povečuje (puščice, ki gredo v center), ukrepi, ki so že dosegli pomembnost in bodo v prihodnje manj aktualni (puščice gredo iz centra) in ukrepi, ki morajo šele pridobiti na uporabi (puščica na obrobju).

Slika 22: *Trendi uporabe varnostnih ukrepov*



Vir: DSCI- KPMG Survey 2009, str. 37.

Varnostne tehnologije odpovedo zaradi različnih razlogov, zato varnostni strokovnjaki priporočajo kombinacijo več ukrepov za zaščito pred pričakovanimi grožnjami (Anderson, 2008). Tudi Schechter (2004) priporoča, da se varnostni ukrepi lahko kombinirajo med seboj, saj so praviloma ukrepi bolj učinkoviti v kombinaciji, kot ločeno. Tak pristop je znan kot varovanje v globino (angl. *Defense-in-Depth*), kjer se podjetje pred grožnjami varuje s kombinacijo človeških, procesnih in tehnoloških zaščit. Model globinske obrambe je prikazan na sliki 23.

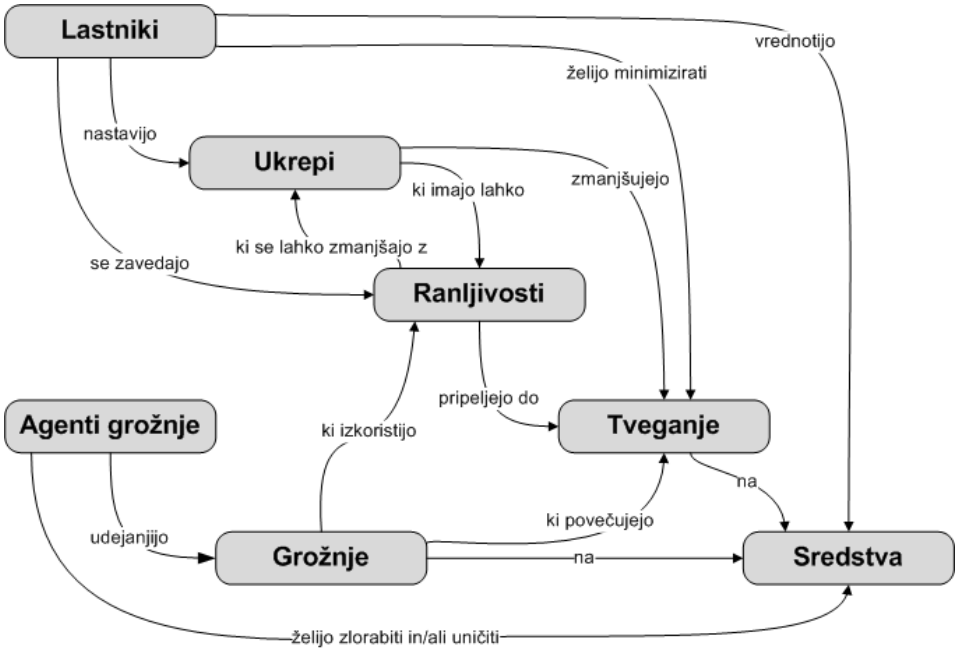
Slika 23: *Model globinske obrambe*

Vir: Microsoft Security Risk Management Guide, 2004, str.46.

Glede na dejstvo, da je varnostna arhitektura globinske obrambe potrebna za varno okolje podjetja, je ključno vprašanje, kako varnostni ukrepi sodelujejo med seboj ter ali se med seboj dopolnjujejo. Ali je na primer učinkovitost varnostne arhitekture s požarnim zidom in IDS sistemom večja, ko sta rešitvi v paketu, ali ko se vsak ukrep uporabi posamično? Pomembno je, da podjetja natančno ocenijo vrednost varnostnega mehanizma in ob tem upoštevajo že obstoječe ukrepe.

Pri uvedbi varnostnega ukrepa je potrebno upoštevati, da lahko nasprotnik prebije zaščito, ki jo daje ukrep ali jo preprosto zaobide. Vsak varnostni ukrep lahko privede do uvedbe dodatnih, bolj podrobnih scenarijev groženj. Ti novi podrobni scenariji lahko privedejo do uvajanja novih varnostnih ukrepov (Schechter, 2004). Tudi Schneier (2003, str. 14; 2004c, str. 290) opozarja, da je pri uvedbi ukrepov potrebno biti pozoren tudi na nova tveganja, ki jih ukrepi lahko prinašajo. Ta povratna zanka je predstavljena na sliki 24.

Slika 24: *Prikaz odvisnosti med tveganjem, sredstvi, ranljivostmi, grožnjami in ukrepi*



Vir: ISO 15408-1, 1999, str.13.

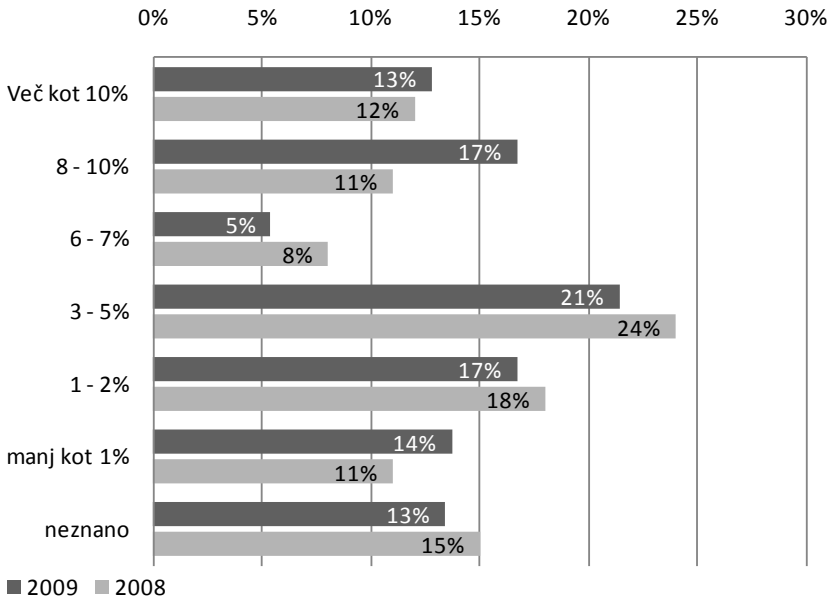
Učinkovitost ukrepa je ocena, kako dobro ukrep blaži tveganja. Ocena učinkovitosti varnostnih ukrepov je lahko težavna. Še posebej, če ukrepi zahtevajo spremembe v vedenju delavcev ter njihovega dostopa do informacij. Merjenje učinkovitosti varnostnih ukrepov že obstaja za nekatere posebne tehnologije, kot so požarni zid, protivirusna programska oprema in IDS sistemi, vendar pa so te ocene težko primerljive med seboj. Trenutno ne obstaja nobena formalna metodologija, ki bi primerjala stopnjo varnosti enega sistema z drugim. Težavnost merjenja je tudi v tem, da je problem odvisen od ljudi z različnimi spodbudami in nenehno spreminjajočimi se tehnologijami.

V kolikor so na voljo pretekli podatki, se ti lahko analizirajo in uporabijo za pridobitev ocen učinkovitosti. V nasprotnem primeru je potrebno za oceno učinkovitosti uporabiti mnenje strokovnjaka. Pri tem se zastavlja vprašanje, ali je s subjektivno oceno varnostnega strokovnjaka sploh mogoče dobiti smiselne in uporabne faktorje. Butler (2002) zagovarja, da je s strani varnostnih strokovnjakov mogoče zagotoviti grobe kvantitativne ocene za učinkovitost varnostnih ukrepov.

4.2 Investicije v varnost

Zmanjševanje tveganja z investicijami v varnostne tehnologije je primarna obravnava tveganja (Bojanc & Jerman-Blažič, 2008a). Namen investicije je zmanjšanje verjetnosti in posledice varnostnih incidentov. V podjetjih investicije v varnost niso zelo visoke. Po raziskavi CSI (2009, 2008) se v povprečju le okoli 3-5 % IT proračuna podjetja nameni informacijski varnosti. Podobne rezultate podaja tudi raziskava DSCI-KPMG (DSCI, 2009). Rezultate CSI raziskave so prikazani na sliki 25.

Slika 25: *Delež IT proračuna namenjen informacijski varnosti*



Vir: CSI Computer Crime and Security Survey 2009 in 2008.

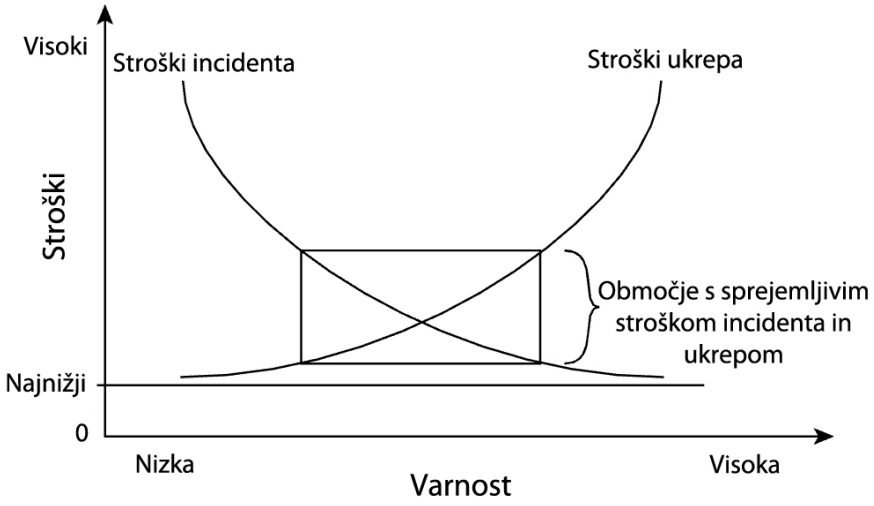
Raziskava BERR (2008) je med podjetji v Veliki Britaniji zaznala občuten porast deleža IT proračuna namenjenega informacijski varnosti, in sicer leta 2002 le 2 % IT proračuna, medtem ko leta 2008 že 7 %. Po drugi strani 21 % podjetij za varnost porabi manj kot 1 % IT proračuna. Za izobraževanje in ozaveščenost v informacijsko varnost se porabi manj kot 1 % proračuna (CSI, 2008).

Odločitev o tem, kako je najbolje vlagati sredstva v informacijsko varnost, ni enostavna. Težava združuje več negotovosti glede groženj, ranljivosti, posledic uspešnega napada in učinkovitosti ukrepov. Posledice neustrezne odločitve o investicijah v informacijsko varnost postanejo hujše, ko podjetje shranjuje čedalje več vrst informacij, ki jim narašča občutljivost in vrednost. Načini za dostop do informacij se širijo, tako da vključujejo čedalje večje število mobilnih in oddaljenih naprav. Pomembno je, da se podjetje zaveda, da zaščitni ukrepi zmanjšujejo tveganja le na sprejemljivo raven ter da 100 % varnost ni in ne sme biti cilj.

Pri zmanjševanju nevarnosti je koristno razumevanje motivov in ciljev napadalcev, kar pa zahteva kulturno in politično znanje, ki pogosto ni znotraj podjetja. Zastavlja se vprašanje, kako v podjetju določiti ustrezne ukrepe za povečanje informacijske varnosti in najbolj učinkovito razporediti sredstva. Za pomoč pri tem odločanju obstajajo modeli in orodja. Ključno pa je razumeti, kateri modeli so najbolj primerni za določene vrste podpore odločanju (Rue, Pfleeger & Ortiz, 2007).

Pri določitvi optimalnega zneska v informacijsko varnost je potrebno najti optimalno razmerje med stroški in varnostjo, kar je prikazano na sliki 26. Stroški informacijske varnosti imajo dve veji, ki sta med seboj povezani, in sicer "stroški ukrepa" in "stroški incidenta". Strošek ukrepa je denar, ki ga podjetje porabi za investicijo, s katero se želi izogniti problemu. Strošek incidenta pa je denar, ki ga podjetje porabi, ko pride do problema. Če podjetje ne porabi nič za stroške ukrepa, bo to imelo za posledico povečano porabo stroškov incidenta zaradi sanacije stanja, medtem ko bodo zelo veliki stroški ukrepa močno zmanjšali stroške incidenta. Iskanje optimalne stopnje varnosti, ki upošteva stroške incidenta in stroške ukrepa, ni enostavna naloga. Pogosto se za določitev optimalne stopnje informacijske varnosti uporabi analizo stroškov in koristi, ki je predstavljena v poglavju 4.4.1.

Slika 26: *Iskanje optimalne rešitve med tveganjem in stroški*



Vir: Kaplan, A Matter of Trust, v Tipton & Krause (ur.), Information Security Management Handbook, 6th edition, 2007, str.304.

4.2.1 Zmanjšanje tveganja preko zavarovalnice

Ena od obravnav, s katero se podjetje lahko odzove na varnostna tveganja, je prenos tveganja na zavarovalnice. Četudi pred tem že uporabijo druge tehnične rešitve za zmanjšanje tveganja, lahko podjetja s sklenitvijo zavarovanja še dodatno zmanjšajo tveganje. Zavarovanje ne zmanjšuje verjetnosti za varnostni incident, temveč zmanjšuje izgube ob morebitnem incidentu. Zavarovanje običajno zahteva minimalne investicije. Pozitivna stran uporabe zavarovanja je tudi ta, da spremenljive stroške tveganja prevede v fiksne stroške, ki jih je mogoče zajeti v proračun (Schneier, 2004a).

Obvladovanje tveganja skozi zavarovanje raziskujejo mnogi avtorji (Baer, 2003; Conrad, 2005; Farahmand, Navathe, Sharp & Enslow, 2005, str. 203; Geer, 2004a; Gordon, Loeb & Sohail, 2003; Haimes & Chittester, 2005; Soo Hoo, 2000; Baer & Parkinson, 2007). Pri zavarovanju informacij se izgube krijejo iz dveh razredov tveganja (Gordon et al., 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 napadi virusov in napake programske opreme itd.
- Tveganja tretje stranke pokriva 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.

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).

Tudi zavarovalnice imajo potencialni vpliv na odločitev, ki jo sprejemajo vodje informacijske varnosti (Farahmand, 2004). V preteklosti je bilo kar nekaj poskusov opredelitve zavarovalniškega sektorja v informacijski varnosti, pri tem zavarovalnice pokrivajo naslednja področja (Gordon et al., 2003; Schneier, 2001; Agger et al., 2003):

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

Vendar pa je potrebno biti previden pri izjavah zavarovalnic glede plačevanja zahtevkov za navedena pokritja (Gordon et al., 2003). Farahmand (2004) trdi, da obstaja kompromis med zneskom, ki ga podjetja vlagajo v zaščito pred možnimi varnostnimi grožnjami in zneskom, ki ga podjetja porabijo za zavarovanje pred informacijskimi grožnjami.

Po raziskavi CSI 2007 le 29 % podjetij uporablja zavarovanje informacij (CSI, 2007). To je predvsem zato, ker zavarovalnice nimajo dobrih aktuarskih podatkov, na podlagi katerih izračunavajo premije. Nekateri raziskovalci celo trdijo, da so zavarovalne police, ki jih trenutno ponujajo zavarovalnice, skoraj neuporabne (Majuca, Yurcik & Kesan, 2006).

Skozi čas se bodo zavarovalnice naučile, kako natančneje vrednotiti tveganja. Trenutno stanje je, da je informacijsko-zavarovalniški trg nerazvit in slabo izkoriščen (Anderson & Moore, 2008). Eden od razlogov je soodvisnost tveganja tako v lokalnih kot globalnih oblikah (Böhme & Kataria, 2006). IT infrastruktura podjetja je povezana z drugim okoljem, zato napaka v drugih okoljih lahko vpliva na lokalno podjetje. Napadalci dostikrat zlorabijo ranljivost v programu, ki ga uporablja veliko podjetij. Medsebojna odvisnost nekaterih tveganj je lahko neprivlačna za zavarovalnice. To velja predvsem za tista tveganja, ki so povezana globalno in ne lokalno. To so običajno napadi črvov in virusov ter sistemska tveganja (kot je bil na primer Y2K) (Anderson & Moore, 2008).

V Sloveniji zavarovalnice že ponujajo nekatere zavarovalniške produkte, ki pokrivajo posamezna tveganja s področja informacijske varnosti. Že dalj časa je na voljo zavarovanje pred krajo strojne opreme v obliki vlomskega zavarovanja, ki zajema krajo v poslovnih prostorih in na terenu (npr. prenosni računalniki). Zavarovalnice v Sloveniji običajno krijejo stroške popravila ali zamenjavo fizične opreme ter stroške demontaže in montaže te opreme. Za kritje stroškov vzpostavitve delovanja IT sistema se je potrebno posebej zavarovati. Tehnično okvaro in nenamerno poškodbo strojne opreme pokriva strojelomno zavarovanje. Namerno uničenje strojne opreme (npr. vandalizem, demonstracije) pokriva požarno zavarovanje. Možno je zavarovanje pred nenamerno izgubo podatkov, kjer 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. 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 …).

Za zavarovalnice v Sloveniji in v svetu še vedno ostaja glavni problem to, da je varnostna tveganja zelo težko izmeriti. Ko bodo zavarovalne družbe pridobile

izkušnje in dobre aktuarske podatke, bodo cene in zavarovalne police postale bolj zanimive (Bojanc & Jerman-Blažič, 2008a).

4.2.2 Zunanje izvajanje informacijske varnosti

Podjetje se lahko odloči za zunanje izvajanje določenih aktivnosti informacijske varnosti. Z zunanjim izvajanjem podjetje pridobi zunanje strokovno znanje in znižanje začetne kapitalne investicije (predvsem tiste, ki so vezane na strojno opremo, programsko opremo in osebje). Zunanji izvajalec za svoje aktivnosti seveda zaračuna, zato je potrebna ocena, ali je ceneje te aktivnosti izvajati znotraj podjetja. Odločitev o tem, ali se odločiti za zunanje izvajanje ali aktivnosti izvajati znotraj podjetja, izhaja iz analize stroškov in koristi. Gordon in Loeb (2005, str. 87) navajata nekaj strateških pomislekov, ki jih je dobro preučiti, preden se podjetje odloči za zunanje izvajanje informacijske varnosti. Ti pomisleki so:

- razlika v kvaliteti izvajanja informacijske varnosti,
- želja po ohranitvi notranjega ocenjevanja kvalitete informacijske varnosti,
- dostop do zaupnih informacij (deljenje zaupnih informacij z zunanjim izvajalcem odpira novo grožnjo za podjetje),
- koristi izvajanja varnosti znotraj podjetja (deljenje znanja).

V letu 2009 je zaznati občutno zmanjšanje zunanjega izvajanja informacijske varnosti (CSI, 2009). 71 % podjetij ne uporablja zunanjega izvajanja nobenih varnostnih funkcij, medtem ko je bilo leta 2008 takih 59 %.

4.3 Teoretični modeli določitve optimalne stopnje varnostne investicije

Izračun optimalnih investicij v informacijsko varnost je relativno nov pogled, saj so se v preteklosti varnostni strokovnjaki osredotočali skoraj izključno na tehnološke rešitve, ne da bi to povezali s finančnimi stroški, potrebnimi za izvajanje ukrepov (Ioannidis et al., 2009). Za pomoč pri odločanju o razporeditvi sredstev za informacijsko varnost so bili predlagani različni modeli, ki vsak zase vzame drugačen pristop. Dosedanje pristope določanja optimalne stopnje varnostne investicije lahko razvrstimo v nekaj skupin.

4.3.1 Analitični modeli

Analitični modeli temeljijo na analizi stroškov in koristi. Potencialno tveganje zaradi varnostnih incidentov identificirajo glede na povzročeno škodo in verjetnost. Gordon in Loeb (2002b) sta predstavila ekonomski model za ocenitev

optimalne investicije v informacijsko varnost, ki temelji na izenačevanju mejnih finančnih koristi informacijske varnosti in mejnih finančnih stroškov zaščite. Soo Hoo (2000) je predstavil okvir analitičnega odločanja za ocenjevanje različnih politik IT varnosti in razvil okvir za modeliranje tveganja za izbiro zaščitnih ukrepov. Namesto, da primerja varnostne ukrepe na individualni ravni, modelira skupino zaščitnih ukrepov ali politik in išče za vsako politiko kompromis med stroški in koristmi. Longstaff (2000) predlaga hierarhični holografski model (HHM) za oceno varnostnih tveganj in oceno učinkovitosti ravnanja s tveganji. Bodin predlaga uporabo analitičnega hierarhičnega procesa (AHP) za pomoč podjetju pri odločanju o investicijah v informacijsko varnost (Bodin, Gordon & Loeb, 2005, str. 97). Njihov pristop lahko analizira odločitvene scenarije z več kriteriji in lahko medsebojno primerja finančne in nefinančne ter kvantitativne in kvalitativne kriterije. Butler (2002) predlaga metodo analize stroškov in koristi, imenovano SAEM, za primerjavo alternativnih varnostnih konceptov. SAEM primerja alternativne koncepte informacijske varnosti z že uvedenim konceptom in tako preveri ali je možna bolj stroškovno učinkovita rešitev. Xie in Mead (2004) podajata splošni okvir za analizo stroškov in koristi za zagotavljanje sprejemljive ocene za mala podjetja. Primere zlorab razvršča v kategorije groženj za katere obstajajo javno objavljena poročila o tveganjih in finančnih podatkih.

4.3.2 Model teorije iger

Alternativna metoda, ki poskuša analizirati optimalne investicije v informacijsko varnost, je tako imenovana teorija iger (Cavusoglu, Mishra & Raghunathan, 2004a). Avtorji 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, da se pri varnosti podjetja srečujejo s strateškimi nasprotniki, ki iščejo priložnosti, da izkoristijo ranljivosti v sistemih. Zato lahko na informacijsko varnost gledamo kot na neke vrste igro med podjetji in napadalci. Teorija iger gleda interakcijo med potencialnim napadalcem in podjetjem in skuša pojasniti primere vdorov v podjetje, kjer ima napadalec motiv za napad in povzroči podjetju določeno škodo.

Teorija iger se uporablja za analizo težav, v katerih je rezultat odvisen od interakcije med strategijami igralcev (Rasmusen, 1998). Varnostne investicije po eni strani zmanjšujejo ranljivosti, ki jih zlonamerni uporabnik poskuša zlorabiti, po drugi strani pa tudi naredijo cilj za zlonamernega uporabnika manj zanimiv.

Cremonini in Martini (2005) predlagata izboljšanje ocene donosnosti investicije v informacijsko varnost z novim indeksom, ki se imenuje donosnost napada (angl. *Return-On-Attacts, ROA*).

Gal-Or in Ghose (2005, str. 86) sta z uporabo teorije iger poiskala, kolikšni so stroški in kolikšne so koristi izmenjave informacij. Opisala sta situacijo, v kateri dve podjetji A in B s konkurenčnimi proizvodi izbereta optimalne stopnje varnostnih investicij in izmenjavo informacij. A in B sočasno izbereta cene, igra pa jima pomaga, da se odločita, koliko podatkov o varnostnih incidentih izmenjujeta. Na splošno obstajajo močne spodbude za izmenjavo informacij o varnostnih incidentih, pri čemer spodbude naraščajo z velikostjo podjetja, velikostjo panoge in povečanjem konkurence.

Metode iz teorije iger so za svoje modele uporabili tudi drugi raziskovalci (Garcia & Horowitz, 2006; Gal-Or & Ghose, 2005; Horowitz in Garcia 2005; Irvine, Thompson & Allen, 2005, str. 61).

4.3.3 Različni drugi modeli

Andrijcic in Horowitz (2004) sta predstavila vhodno-izhodni model za oceno makroekonomskih učinkov kraje intelektualne lastnine na gospodarstvo. Model temelji na modelu vpliva terorizma na gospodarstvo ZDA, ki sta ga razvila Santos in Haimes (2004). Makroekonomski vhodno-izhodni modeli so bili predlagani za oceno občutljivosti gospodarstva ZDA na napade v posameznih sektorjih in posledice premajhnih investicij v informacijsko varnost (Garcia & Horowitz, 2006).

Beautement (2008) je vzel za vzor makroekonomski model, s katerim centralne banke uravnavajo inflacijo in nezaposlenost (Ruge-Murcia, 2001; Ruge-Murcia, 2003) ter ga prevedel v investicije v informacijsko varnost, pri čemer primerja zahteve po celovitosti in razpoložljivosti. Ta model so Ioannidis, Pym in Williams (2009) nadgradili z raziskavo, ki primerja celovitost in razpoložljivost za različne vrste organizacij, kot so vojska, finance, proizvodnja.

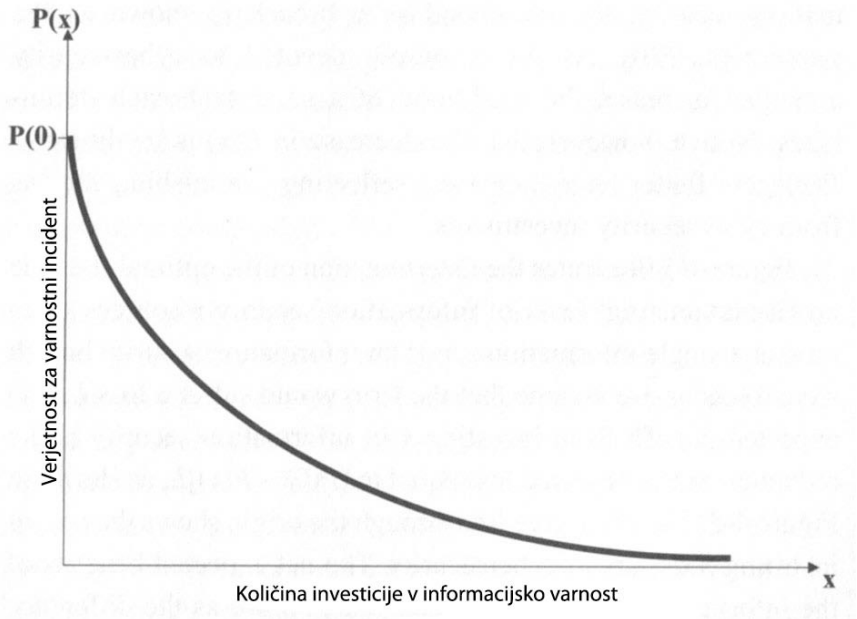
Nekateri avtorji so uporabili teorijo realnih možnosti, ki je bila sicer najprej razvita kot tehnika za pomoč odločanju na področju kapitalskih naložb (Childs, Ott & Triantis, 1998, str. 305). Teorija realnih možnosti je bila uporabljena pri raziskovanju ponovne uporabe programske opreme (Favaro, Favaro & Favaro, 1998) in raziskovanju stabilnosti programske arhitekture (Bahsoon & Emmerich, 2004, str. 443).

4.3.4 GLEIS model

En izmed prvih predstavljenih analitičnih matematičnih modelov je model GLEIS, ki sta ga za določitev optimalne investicije v informacijsko varnost predlagala Gordon in Loeb (2005, 2002b). Upoštevala sta tri parametre, in sicer izgubo zaradi varnostnega incidenta, verjetnost pojava grožnje in ranljivost (ki jo definirata kot verjetnost, da je realizirana grožnja uspešna). Učinek je izražen v denarnih enotah, za katere se pričakuje, da bodo izgubljene, če pride do incidenta.

Pri tem sta uvedla funkcijo verjetnosti za varnostni incident, ki povezuje možno izgubo, verjetnost, da pride do izgube in produktivnost investicije. Na sliki 27 je prikazana odvisnost funkcije verjetnosti za incident od količine investicij v informacijsko varnost. Na grafu os x predstavlja obseg izdatka, ki ga podjetje nameni aktivnostim informacijske varnosti. *P(x)* predstavlja verjetnost, da bo v tem časovnem obsegu prišlo do kršitve zaradi varnostnega incidenta. Če ni namenjenih nobenih investicij za informacijsko varnost, je verjetnost za incident *P(0)* kar vrednost na y osi. Z večanjem količine investicij, namenjenih za informacijsko varnost, se verjetnost za incident zmanjšuje. Zmanjševanje *P(x)* ni linearno, temveč konkavno.

Slika 27: *Graf funkcije varnostnega incidenta*



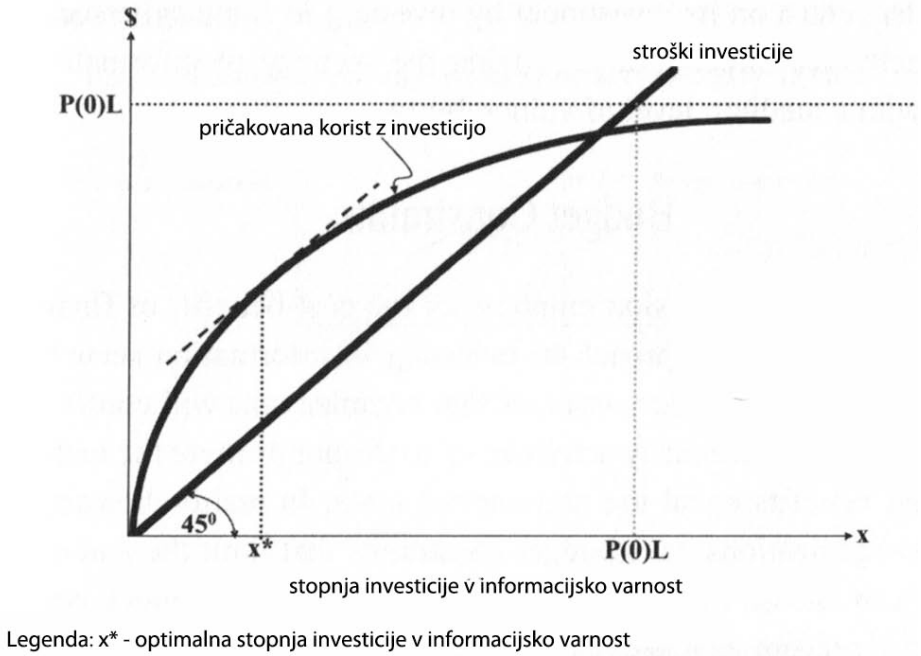
Vir: Gordon & Loeb, Managing Cyber-Security Resources, 2005, str. 82.

Na sliki 28 je prikazana določitev optimalne količine investicije *x** za zaščito določenega informacijskega sredstva. V kolikor pride do incidenta, podjetje utrpi izgubo *L*. Pričakovana korist investicije *x* je zmanjšanje pričakovane izgube, ki je enaka:

$$\left[P(0)-P(x)\right]\cdot L \tag{3}$$

45 stopinjska črta skozi izhodišče prikazuje stroške investicije v denarni enoti. Pričakovana neto korist investicije v informacijsko varnost je prikazana kot razlika med krivuljama in je največja pri x*, kjer je mejna pričakovana korist zaradi investicije v denarni enoti enaka stroškom investicije.

Slika 28: *Koristi in stroški investicije v informacijsko varnost v GLEIS modelu*



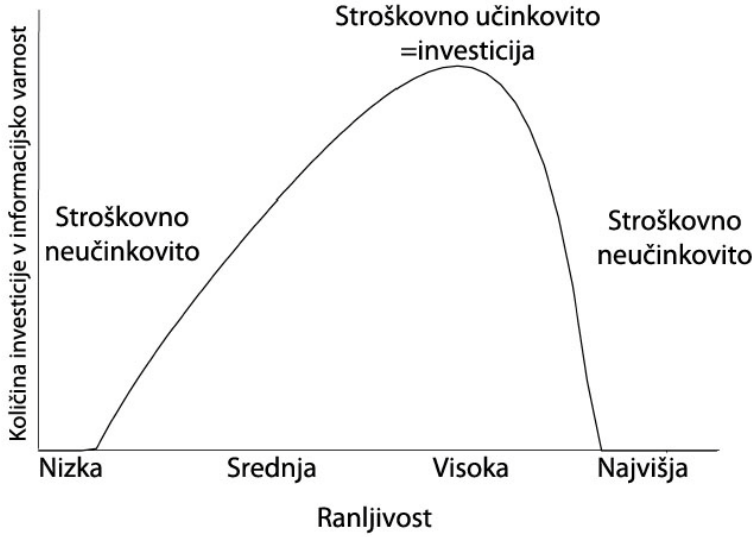
Vir: Gordon & Loeb, Managing Cyber-Security Resources, 2005, str. 83.

Iz modela GLEIS izhajata dve pomembni ugotovitvi. Prva je, da naj podjetja za dosego največje donosnosti namenijo le manjši del tiste vrednosti, ki bi jo lahko izgubili ob možnem incidentu. Model ocenjuje, da je pod določenimi pogoji neekonomično investirati v aktivnosti informacijske varnosti, ki stanejo več kot 37 % pričakovane izgube. Dejansko želijo podjetja v večini primerov investirati v znesku, ki je občutno manjši od tega tretjinskega pravila. Kasneje je Willemson (2006) skonstruiral situacijo, kjer je lahko investicija večja od tega tretjinskega pravila, in sicer v višini 50 % pričakovanih izgub, če se omejitve nekoliko omili, pa celo do 100 % pričakovanih izgub.

Drugi rezultat GLEIS modela se nanaša na situacije, kjer ena grožnja lahko povzroči dve možni izgubi. Za podjetje ni vedno najboljše, da svoje investicije usmeri v varovanje večje ranljivosti izmed obeh. V nekaterih primerih je zaščita večje ranljivosti dražja od prihrankov stroškov. Zato lahko podjetje dobi večjo donosnost z investicijo v nekatere ukrepe, ki so usmerjeni na izboljšanje varnosti pri ranljivostih srednjega nivoja, kar prikazuje tudi slika 29.

GLEIS model je postal osnova za mnoga nadaljnja teoretična (Willemson, 2006; Huang, Hu & Behara, 2005a; Huang, Hu & Behara, 2005b) in empirična raziskovanja (Tanaka, 2005, str. 185; Tanaka, Matsuura & Sudoh, 2005, str. 37; Tanaka, Liu & Matsuura, 2006).

Slika 29: *Učinkovitost investicije v informacijsko varnost glede na stopnjo ranljivosti sredstev*



Vir: Gordon & Loeb, The Economics of Information Security Investment, 2002, str. 450.

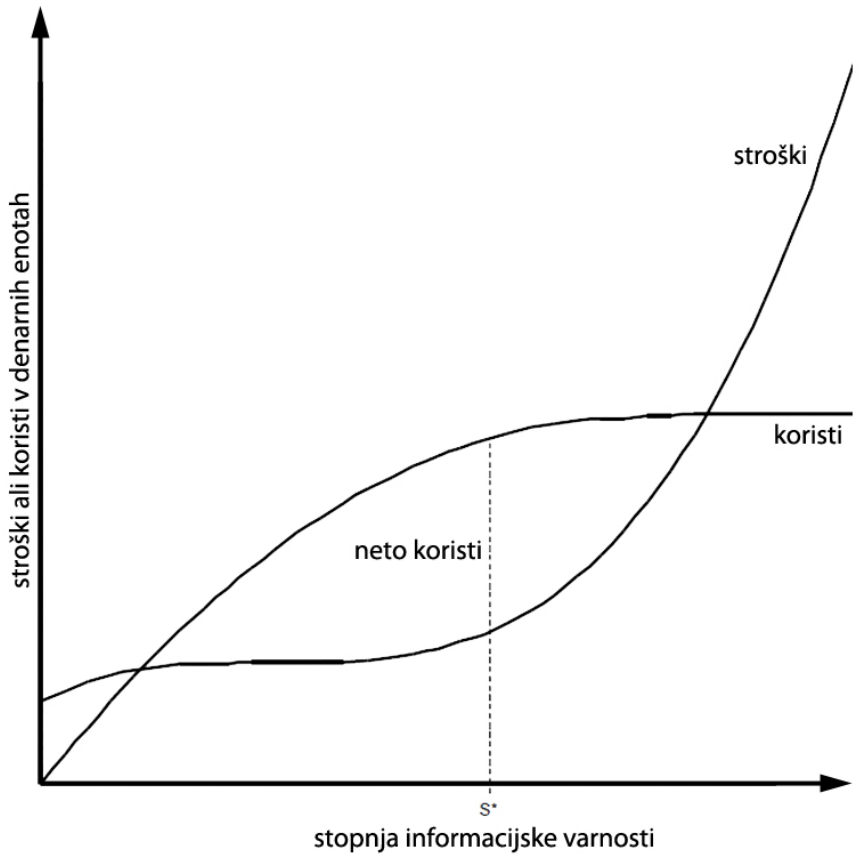
4.4 Kvantitativno vrednotenje stroškov in koristi investicij v informacijsko varnost

4.4.1 Primerjava stroškov in koristi

Eno izmed ključnih vprašanj informacijske varnosti je, koliko naj podjetje investira v aktivnosti informacijske varnosti. Geer (2002) zagovarja, da se varnostne investicije ne smejo meriti zgolj s tehničnimi kazalci oziroma skozi količino zapravljenega denarja, temveč skozi sistematično analizo stroškov varnostne rešitve in koristi zaradi njene uvedbe (Schechter, 2002). Ta metoda je tudi primerna za finančno odločanje managerjev (Nemzow 1997, str. 127).

Analiza stroškov in koristi primerja stroške določene aktivnosti s koristmi, ki jih aktivnost prinaša (Gordon & Loeb, 2002b; Gordon & Loeb, 2006; Schechter, 2002). Predpostavimo, da lahko ocenimo pričakovane skupne koristi in pričakovane skupne stroške za različne nivoje aktivnosti informacijske varnosti. Dokler koristi dodatne aktivnosti informacijske varnosti presegajo stroške, je uvedba aktivnosti smiselna. Cilj podjetja mora biti uvedba varnostnih ukrepov do točke, kjer so koristi minus stroški maksimalni. Uvedba aktivnosti informacijske varnosti preko te točke pomeni, da so mejni stroški večji od mojnih koristi dodatne varnosti. Z drugimi besedami, neto koristi (tj. koristi minus stroški) uvedbe mejne informacijske varnosti preko največje točke, so negativne. Za podjetje nima smisla, da se za varnostno rešitev zapravi več, kot znašajo možne izgube v primeru incidenta. Grafični prikaz neto koristi je na sliki 30.

Slika 30: *Merjenje koristi in stroškov informacijske varnosti*



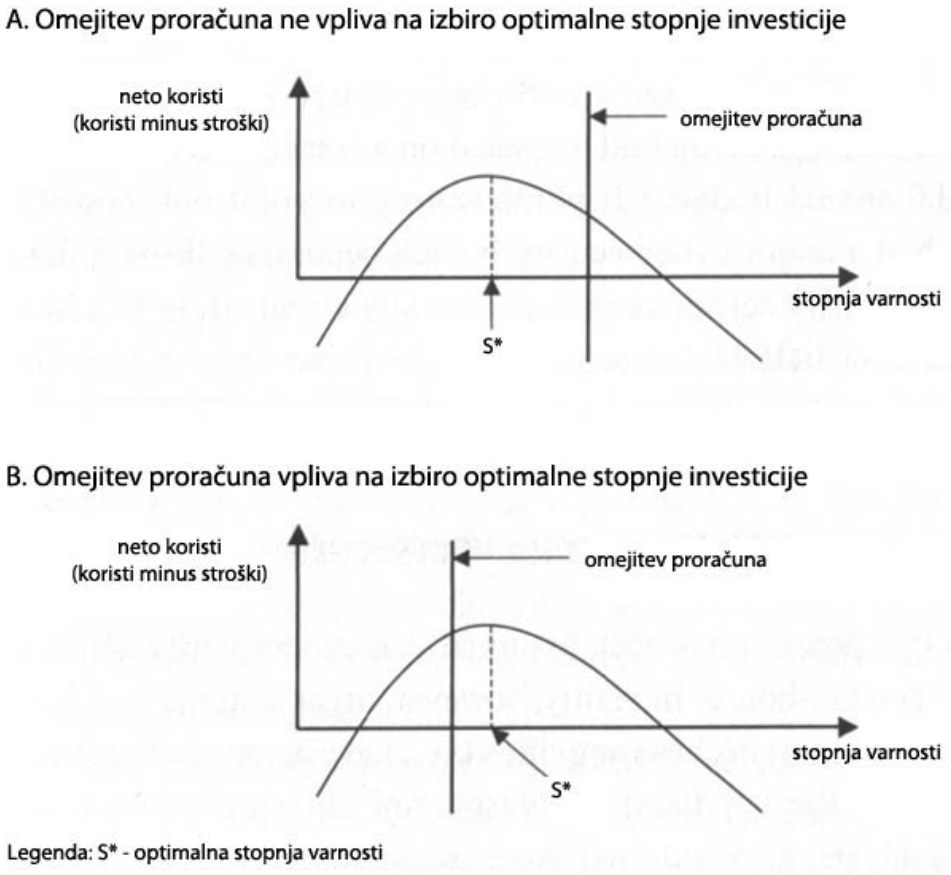
Legenda: S* - optimalna stopnja varnosti, kjer so neto koristi (razlika med koristmi in stroški) največje

Vir: Gordon & Loeb, Economic Aspects of Information Security, 2003, str. 9.

Podjetje lahko nadaljuje z investicijami vse dokler mejne koristi niso enake mejnim stroškom. Če so stroški in koristi aktivnosti informacijske varnosti izenačeni, je s tehničnega stališča uvedba aktivnosti nevtralna. Poleg tega večja stopnja informacijske varnosti ni vedno boljša za podjetje, saj je med stroški in koristmi informacijske varnosti vedno potreben kompromis (Gordon & Loeb, 2005, str. 21).

V realnosti imajo podjetja vedno omejen proračun, ki omejuje količino, ki se lahko nameni investicijam v informacijsko varnost. Proračun je opredeljen kot odstotek od IT proračunskih sredstev za informacijsko varnost. Omejitve proračuna preprečujejo managerjem uporabo čisto ekonomskih principov (Gordon & Loeb, 2005, str. 85). Omejitev proračuna je grafično prikazana na sliki 31. V primeru A je omejitev proračuna nad optimalno stopnjo varnostne aktivnosti, zato lahko managerji investirajo vse do optimalne stopnje, kjer so neto koristi največje. V primeru B pa je omejitev proračuna pod optimalno stopnjo varnostne aktivnosti, zato managerji ne morejo investirati do optimalne stopnje, ker za to nimajo zadosti finančnih sredstev.

Slika 31: *Vpliv omejitve proračuna na investicijo v informacijsko varnost*



Vir: Gordon & Loeb, Managing Cyber-Security Resources, 2005, str. 85.

4.4.1.1 Stroški uvedbe ukrepa

V splošnem lahko vse stroške, povezane z varnostnim ukrepom, razdelimo na operativne stroške in kapitalske investicije (Gordon & Loeb, 2005, str. 28). Dejanski strošek vlaganja v varnost je mogoče dobiti zelo preprosto.

Operativni stroški vključujejo izdatke, od katerih se pričakuje korist v eni periodi izvajanja (pri tem je ena perioda običajno fiskalno leto). Ti stroški so v bistvu načrtovana poraba v določenem obdobju. Operativni stroški predstavljajo letno vzdrževanje (posodobitve in varnostne popravke), izobraževanje uporabnikov in skrbnikov omrežja ter nadzor rešitve (Mizzi, 2005). Primer operativnih stroškov je nameščanje varnostnih popravkov (ki vključujejo stroške osebja) za odpravo varnostnih vdorov, ki so se zgodili tekom leta.

V nasprotju z operativnimi stroški, ki se računajo kot izdatek v enem obdobju, so kapitalske naložbe izdatki, ki prinesejo podjetju korist v obdobju več zaporednih obdobjih. Ker kapitalske naložbe izgubljajo svojo ekonomsko vrednost, se del investicije, ki je bil izgubljen v določeni periodi, zaračuna tej periodi kot operativni strošek. Primer kapitalske naložbe je nabava novega sistema za zaznavanje vdorov v omrežje (z vključenimi povezanimi stroški osebja), ki pomaga podjetju

zmanjševati verjetnost varnostnih vdorov v določenem prihodnjem obdobju (npr. 2- do 3-letnem) z zaznavanjem napadov na sistem.

V poglavju 1.2.6 izpostavim dilemo med varnostjo in uporabnostjo. Večja varnost skoraj vedno pomeni zmanjšanje udobja, kar zmanjšuje produktivnost (Schneier, 2003). Stroški zaščitnih ukrepov morajo vključevati tudi vpliv na produktivnost, saj je ta podatek včasih zelo pomemben, lahko celo tako zelo pomemben, da odloča o tem, ali se določeno storitev še izvaja ali ukine.

4.4.1.2 Koristi uvedenega varnostnega ukrepa

Za razliko od stroškov, ki se določijo sorazmerno enostavno, pa je precej težje opredeliti, oceniti ali meriti koristi (Soo Hoo, 2000). Varnostne rešitve (npr. požarni zid, protivirusni program in IDS sistemi) same po sebi namreč ne prinašajo finančne koristi, ki jih je mogoče izmeriti.

Koristi investicije v informacijsko varnost so lahko različne (Gordon & Loeb, 2005, str. 74). Najbolj pogosta korist je zmanjšanje verjetnosti ponovitve incidenta. Druga možna korist je povečanje produktivnosti ostalih investicij informacijske varnosti. Nekatere investicije niso namenjene zmanjševanju verjetnosti incidenta temveč zmanjševanju izgub, če pride do incidenta.

V splošnem se na koristi zaradi vlaganja v informacijsko varnost gleda kot na prihranek stroškov zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta (Gordon & Loeb, 2006). Te koristi je pogosto zelo težko točno napovedati (Gordon & Loeb, 2005, str. 21). Največja težava je, ker gre za ocenjevanje prihrankov stroškov vezanih na potencialne varnostne incidente, ki se še niso zgodili. Bolj kot je informacijska varnost uspešna, težje je opaziti dejanske koristi. Zaradi tega veliko podjetij pri odločanju o razporeditvi sredstev za investicije v informacijsko varnost ne uporablja analize stroškov in koristi.

Analitično lahko koristi zaradi investicije v informacijsko varnost dobimo kot razliko vrednosti ALE pred in vrednosti ALE po izvajanju varnostnega ukrepa.

$$koristi = ALE_{brez\ investicije} - ALE_{z\ investicijo} \tag{4}$$

4.4.1.3 Alternativni pristopi

Geer (2002) opozarja, da je analiza stroškov in koristi racionalna, a težka. Težka je predvsem zato, ker je potrebno stroške in koristi umeriti v skupno valuto (npr. v evro). 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 se reši človeško življenje?"

Geer (2002) zato predlaga, da se v primerih, ko stroški in koristi niso enostavno primerljivi, raje primerja stroške in učinkovitost rešitve (analiza stroškovne

učinkovitosti). Merjenje stroškov in koristi zahteva, da se vsi vpleteni strinjajo o tem, koliko je korist vredna. To je običajno težko. Merjenje stroškov in učinkovitosti pa nasprotno zahteva, da vpleteni soglašajo, da bodo zapravili X evrov, poleg tega pa še ocenijo, koliko vrednosti lahko dobijo za teh X evrov. 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 zapraviti X €?" namesto pristopa "Ali bi raje imel korist X ali Y evrov?" (Geer, 2004a). Pri stroškovni učinkovitosti gre za maksimiranje učinkovitosti odhodka, kadar je koristi težko ovrednotiti (Farahmand, 2004).

Schechter (2002) uvaja nov kazalec, in sicer "strošek vdora v sistem" (angl. *Cost to Break*), kjer koristi varnostne rešitve ocenjuje preko napadalčevega vložka za vdor v sistem (Schechter & Smith, 2003; Mizzi, 2005).

Nekatera podjetja, ki se izogibajo pristopu stroškov in koristi za razporeditev sredstev namenjenih informacijski varnosti, uporabljajo najboljše prakse ali pristop industrijskih standardov. Zagovorniki takega pristopa to argumentirajo s tem, da je merjenje stroškov in koristi nemogoče, zato naj bi bilo najenostavneje uvesti aktivnosti informacijske varnosti, ki jih je uvedlo že veliko drugih podjetij. Tak pristop managerjem daje občutek varnosti skozi številke. V kolikor podjetje uvede tak pristop, bo za varnost zapravilo preveč ali ostalo odprto za določena nepotrebna tveganja.

Gordon in Loeb (2005) kljub vsem tem pomislekom zagovarjata analizo stroškov in koristi. Razdelitev sredstev za informacijsko varnost mora temeljiti na ekonomskem principu analize stroškov in koristi na enak način, kot se upravljajo sredstva za ostale aktivnosti v podjetju.

4.4.2 Donosnost investicije

Donosnost investicije (angl. *Return on Investment*, v nadaljevanju *ROI*) je priljubljen finančni kazalec za primerjavo poslovnih investicij (Blakley, 2001; Butler et al., 1999; Jacobson, 2000; Geer, 2001; Soo Hoo, 2001). ROI preprosto določa, koliko podjetje dobi glede na porabljen znesek denarja. Za uporabo kazalca ROI v informacijski varnosti uporabljajo nekateri avtorji bolj specifične izraze, kot sta donosnost varnostne investicije (angl. *Return on Security Investment*, *ROSI*) (Sonnenreich, 2006) ali donosnost informacijsko varnostne investicije (angl. *Return on Information Security Investment*, *ROISI*) (Mizzi, 2005). Ti izrazi zgolj poudarijo, da gre za merjenje donosnosti v ukrepe informacijske varnosti, medtem ko je izračun in rezultat enak za vse.

Kazalec ROI se nanaša na izračun finančnega donosa od investicij v varnost, ki upošteva finančne koristi in stroške te investicije. ROI je izražen kot neto dobiček, deljen z investicijo:

$$ROI = \frac{koristi - stroški}{stroški} \tag{5}$$

Oziroma če upoštevamo enačbo (4):

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

Kazalec je izražen kot odstotek vrnjene investicije v določenem času. ROI je enak sedanji vrednosti nakopičenih neto prejemkov (koristi) v določenem časovnem obdobju, deljen z začetnim stroškom investicije (Bojanc & Jerman-Blažič, 2008a).

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.

Stopnja donosa je koristna pri določitvah, 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. Stopnja donosa je čedalje bolj priljubljen kazalec, ker je poznan finančnim direktorjem (CFO) in drugim, ki skrbijo za proračun podjetij in odobravajo izdatke (Schechter, 2004).

Navedimo preprost primer: če so stroški novega strežnika za spletno trgovino 10.000 €, pričakovani prihodki v obdobju štirih let pa so 50.000 €, znaša ROI za štiriletno obdobje 400 %.

Še en primer ROI izračuna: vrednost ALE je za tveganje okužbe z virusom ocenjena na 8.750 €. Po nakupu in uvedbi protivirusne zaščite v vrednosti 1.600 € je vrednost ALE ocenjena na 3.400 €. Letni stroški vzdrževanja in delovanja zaščite so 450 €, tako da je ROI v prvem letu:

(8.750 € - 3.400 € - 1.600 € - 450 €) / (1.600 €+ 450 €) = 160 %

Medtem ko ROI pove odstotek donosa zaradi investicije v določenem časovnem obdobju, ne pove ničesar o velikosti investicije. 124 % donosnost lahko na začetku zgleda zelo privlačno, vendar ali bi bilo bolje imeti 124 % donosa na investicijo 10.000 € ali 60 % donosa na investicijo 300.000 € (Bojanc & Jerman-Blažič, 2008a)?

Neto sedanja vrednost

V primeru dolgoročnih finančnih investicij predstavlja časovni atribut problem pri izračunu ROI. Zato se v takih primerih namesto ROI raje uporablja kazalec neto sedanja vrednost (angl. *Net Present Value*, v nadaljevanju *NPV*) (Bojanc, 2008).

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 NPV pristopa je primerjava diskontiranih denarnih tokov vezanih na bodoče koristi in stroške z začetnimi stroški investicije, pri čemer so celotne koristi in stroški izraženi v denarni enoti. Zaradi lažjega izračunavanja se pogosto privzame, da so bodoče koristi in stroški, z izjemo stroškov začetne investicije, realizirani na koncu posameznega obdobja. S tem, ko se denarne tokove diskontira, se ustrezno vključi časovno komponento, 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 odšteje začetne stroške 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:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+k)^t} \tag{7}$$

Diskontna stopnja k se običajno razume kot povprečni strošek kapitala. Izbor ustrezne diskontne stopnje je za izračun kazalca NPV zelo pomemben. NPV model preko diskontne stopnje uravnava tveganje, pri tem večja diskontna stopnja pomeni manjšo vrednost kazalca NPV (Gordon & Loeb, 2005, str. 43).

NPV model podaja managerjem enostavna odločitvena pravila, ali odobrijo ali zavrnejo določeno investicijo v informacijsko varnost (Gordon & Loeb, 2005, str. 34). Pravila so:

- odobritev investicije v informacijsko varnost, če je vrednost neto sedanja vrednost večja od nič,
- zavrnitev investicije v informacijsko varnost, če je vrednost neto sedanja vrednost manjša od nič,
- neopredeljenost do investicije v informacijsko varnost, če je vrednost neto sedanja vrednost enaka nič.

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 kot sedanja vrednost pričakovanih stroškov ter da projekt ustvarja izgubo. V kolikor je NPV enak nič, pomeni, da sta sedanja vrednost pričakovanih koristi in

sedanja vrednost pričakovanih stroškov enaki. Projekt je zato donosen, če je vrednost NPV večja od nič. Višja vrednost NPV je vedno boljša, medtem ko nizka vrednost NPV in še posebej negativna vrednost NPV predstavlja nesprejemljive investicije (Su, 2006).

NPV je zelo uporabna pri vrednotenju različnih alternativ. Podjetje na primer izbira med dvema varnostnima rešitvama, kjer 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 pa je druga rešitev boljša, saj lahko podjetje za določen čas vlaga denar na druga področja. 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 pride do pričakovanega donosa (Bojanc & Jerman-Blažič 2008a).

Notranja stopnja donosa

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).

$$\sum_{t=0}^{n} \frac{B_t - C_t}{\left(1 + IRR\right)^t} = 0 \tag{8}$$

Kazalec IRR je še posebej uporaben v primerih, če se stroški večletne investicije radikalno spreminjajo iz leta v leto. Tako kot NPV model, tudi IRR model omogoča managerjem enostavno odločanje glede investicij v informacijsko varnost (Gordon & Loeb, 2005, str. 35):

- odobritev investicije v informacijsko varnost, če je vrednost notranja stopnja donosa večja od *k*,
- zavrnitev investicije v informacijsko varnost, če je vrednost notranja stopnja donosa manjša od *k*,
- neopredeljen do investicije v informacijsko varnost, če je vrednost notranja stopnja donosa enaka *k*.

Pri tem je *k* enak diskontni stopnji, ki se običajno upošteva kot organizacijski povprečni strošek kapitala (najmanjša stopnja, ki jo mora projekt vrniti, da se vrednost podjetja ne bo zmanjšala).

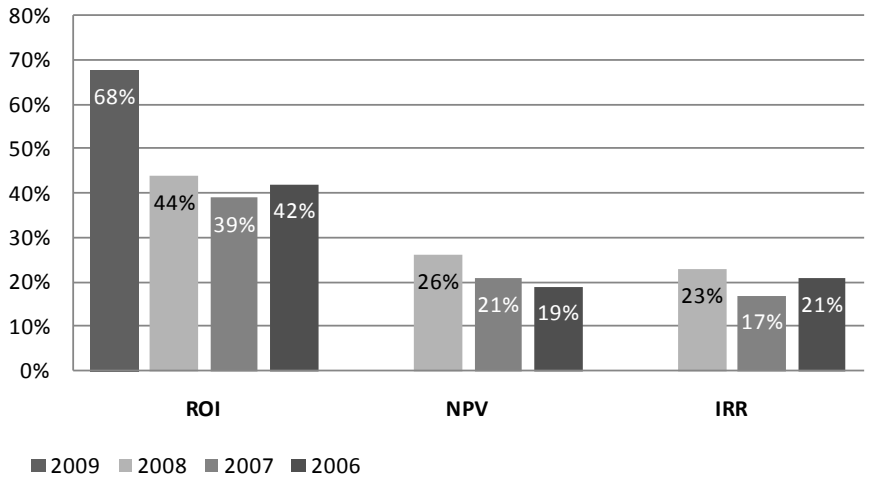
Odločitev glede uporabe kazalcev ROI, NPV ali IRR je prepuščena podjetjem in posameznikom, odgovornim za vrednotenje varnostnih investicij. Vsak od teh finančnih kazalcev ima svoje prednosti in slabosti. Pogosto so rezultati enaki pri

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 pri 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. Gordon in Loeb (2002a) ugotavljata, da bi morala podjetja namesto ROI raje 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 z večjo neto korist, kot pa v rešitev z višjo stopnjo donosa (Schechter, 2004).

Čeprav ima ROI svoje pomanjkljivosti v primerjavi z NPV in IRR (Gordon & Loeb, 2002a), je po raziskavah CSI (2009, 2008, 2007) še vedno najbolj priljubljen kazalec v praksi. Po podatkih iz raziskave (CSI, 2007) 39 % podjetij uporablja ROI, 21 % uporablja NPV in 17 % uporablja IRR. V letu 2008 je 44 % podjetij uporabljalo ROI za varnostni kazalec, 26 % NPV in 23 % IRR (CSI, 2008). V letu 2009 je zaznati porast uporabe ROI kot varnostnega kazalca na 67,8 % (v letu 2008 44 %), uporaba NPV in IRR pa se je temu ustrezno zmanjšala (CSI, 2009). Rezultat je prikazan na sliki 32.

Slika 32: *Delež uporabe ROI, NPV in IRR za varnostni kazalec*



Vir: CSI Computer Crime and Security Survey 2008, str. 10 in 2009, str.3.

V večini primerov sta NPV in IRR boljša kazalca za razliko od preprostega ROI izračuna (Gordon & Richardson, 2004). V primeru različnih odločitev ima običajno NPV rezultat večjo težo kot IRR rezultat (Gordon, 2004; Brealey & Myers, 2000). Kljub temu dejstvu veliko managerjev za vrednotenje bodočih investicij uporablja ROI, ker je za uporabo najenostavnejši. Da bi dobili jasno in popolno sliko o bodočih investicijah, je večkrat potrebno upoštevati vse tri kazalce (Bojanc & Jerman-Blažič, 2008a).

5 Model optimalne investicije v informacijsko varnost

Predstavljen matematični model za oceno optimalne investicije v informacijsko varnost temelji na kvantitativni analizi varnostnih tveganj. Model vključuje identifikacijo informacijskih sredstev, groženj ter ranljivosti. Za ključne poslovne procese se določi želeno stopnjo varnosti. Skozi oceno tveganja se določi verjetnost za varnostni incident ter posledice oziroma izgubo ob uspešnem incidentu. Za varnostno tveganje se določi optimalno obravnavo tveganja. Pri izbiri možnih ukrepov za zmanjšanje tveganja se oceni vpliv posameznih ukrepov na zmanjšanje tveganja. Z uporabo ekonomskih kazalcev se oceni ekonomska učinkovitost posameznega ukrepa, ki omogoča neposredno primerjavo, in kvantitativno vrednotenje različnih možnih varnostnih ukrepov med seboj.

V tabeli 6 so prikazane aktivnosti, ki so zajete v modelu ter pregled vhodnih in izhodnih podatkov za vsako aktivnost.

Tabela 6: *Aktivnosti zajete v modelu z vhodnimi in izhodnimi podatki*

Aktivnost		Vhodni podatki	Izhodni podatki
1	določitev želene stopnje varnosti za poslovne procese	ključni poslovni procesi P v podjetju	varnostne zahteve za vsak proces $S_P{}^C$, $S_P{}^I$ in $S_P{}^A$
2	določitev želene stopnje varnosti za informacijska sredstva, ki so vključena v procese	seznam informacijskih sredstev a_i ki sodelujejo v procesu P varnostne zahteve za procese $S_P{}^C$, $S_P{}^I$ in $S_P{}^A$	varnostne zahteve za vsako informacijsko sredstvo $S_a{}^C$, $S_a{}^I$ in $S_a{}^A$
3	identifikacija in vrednotenje ranljivosti	informacijska sredstva a	ranljivosti sredstev v
4	identifikacija in vrednotenje groženj	ranljivost v informacijska sredstva a	verjetnost grožnje T

se nadaljuje

nadaljevanje

aktivnost		vhodni podatki	izhodni podatki
5	verjetnost za varnostni incident	ranljivost v verjetnost grožnje T	verjetnost za incident ρ
6	identifikacija in ocena izgub v primeru incidentov	incident parametri za določitev velikosti izgub	izguba zaradi incidenta L čas popravila t_{r0} čas detekcije t_{d0}
7	ocena varnostnega tveganja	verjetnost za incident ρ izguba v primeru incidenta L	varnostno tveganje R
8	določitev obravnave tveganja	ρ, L, R, R_{min}, L_{max}, R_{max}, C_{IT_budget}	izbira ustrezne obravnave tveganja: investicija, prenos, sprejem, izogibanje
9	izbira varnostnega ukrepa	možni varnostni ukrepi	produktivnost izbranih ukrepov α stroški izbranih ukrepov C
10	vpliv izbranega ukrepa na zmanjšanje tveganja	produktivnost ukrepa α stroški ukrepa C odškodnina zavarovalnice I	varnostno tveganje po uvedbi ukrepa, ki zmanjšuje verjetnost za incident ρ varnostno tveganje po uvedbi ukrepa, ki zmanjšuje izgube L
11	ocena koristi B zaradi uvedbe ukrepa	varnostno tveganje pred uvedbo ukrepa R_0 varnostno tveganje po uvedbi ukrepa $R(C)$	pridobitev B
12	ekonomsko vrednotenje varnostnega ukrepa	pridobitev B negativni vpliv uvedenega ukrepa na poslovanje δ posredni pozitiven učinek uvedbe ukrepa μ stroški ukrepa C diskontna stopnja k časovno obdobje n	ROI NPV IRR
13	izbira poslovno-ekonomsko optimalnega varnostnega ukrepa	ROI NPV IRR poslovne zahteve po varnosti S_a	poslovno-ekonomsko optimalen varnostni ukrep

5.1 Varnostne zahteve poslovnih procesov

Postopek identifikacije informacijskih sredstev, groženj ter ranljivosti se začne z določitvijo varnostnih zahtev na nivoju poslovnih procesov. Definiramo **poslovni proces *P***, za katerega podjetje določi **želeno stopnjo varnosti S_P.** Stopnja varnosti ($0 \leq S_P \leq 1$) predstavlja poslovne varnostne zahteve, pri tem vrednost 0 predstavlja proces, ki ga ni potrebno varovati, vrednost 1 pa proces, ki zahteva najstrožje varovanje. Želena stopnja varnosti določa, kako je potrebno varovati posamezen poslovni proces in ni odvisna od tega, ali podjetje že ima uvedene ukrepe, ki zagotavljajo ustrezno varnost ali ne.

Za podrobnejšo določitev želene stopnje varnosti se želena stopnja varnosti ločeno določi za zaupnost S_P^C, celovitost S_P^I in razpoložljivost S_P^A procesa. Želena stopnja varnosti S_P za posamezen poslovni proces je v tem primeru trojček števil S_P^C, S_P^I in S_P^A:

$$S_P = (S_P^C, S_P^I, S_P^A) \tag{9}$$

$$S_P^j \in [0,1], \forall j = C, I, A \tag{10}$$

Skupna vrednost želene stopnje varnosti za poslovni proces je enaka največji vrednosti elementov trojčka:

$$\overline{S_P} = \max(S_P^C, S_P^I, S_P^A) \tag{11}$$

Če je v podjetju prisotnih *n* poslovnih procesov, lahko posamezen poslovni proces označimo kot P_i , $i = 1,...,n$. Za vsak poslovni proces se določijo želene stopnje varnosti za zaupnost, celovitost in razpoložljivost, ki predstavljajo varnostne zahteve za posamezen poslovni proces:

$$S_{Pi} = (S_{Pi}^C, S_{Pi}^I, S_{Pi}^A) \tag{12}$$

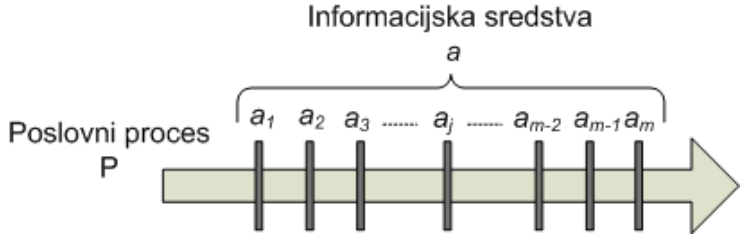
Ker je v podjetju običajno prisotnih veliko poslovnih procesov, se model osredotoča le na ključne poslovne procese.

V vsakem procesu sodelujejo **informacijska sredstva *a***. Če v procesu *P* sodeluje *m* informacijskih sredstev lahko zapišemo:

$$a_j \in P, \forall j = 1,...,m \tag{13}$$

Relacija je prikazana tudi na sliki 33.

Slika 33: *Shematični prikaz informacijskih sredstev, ki sodelujejo v poslovnem procesu*



Želene stopnje varnosti glede zaupnosti S_a^C, celovitosti S_a^I in razpoložljivosti S_a^A informacijskih sredstev, ki sodelujejo v poslovnem procesu P (9), se privzamejo iz varnostnih zahtev poslovnega procesa:

$$S_{a_j}^C = S_P^C, \forall j = 1,\ldots,m \tag{14}$$

$$S_{a_j}^I = S_P^I, \forall j = 1,\ldots,m \tag{15}$$

$$S_{a_j}^A = S_P^A, \forall j = 1,\ldots,m \tag{16}$$

Želena stopnja varnosti S_{aj} za posamezno informacijsko sredstvo j je trojček števil S_{aj}^C, S_{aj}^I in S_{aj}^A:

$$S_{a_j} = \left(S_{a_j}^C, S_{a_j}^I, S_{a_j}^A\right), \forall j = 1,\ldots,m \tag{17}$$

Posamezno informacijsko sredstvo lahko sodeluje v enem ali več procesih. Tako se dobi dvodimenzionalna relacija med procesi in informacijskimi sredstvi, ki je shematično prikazana na sliki 34.

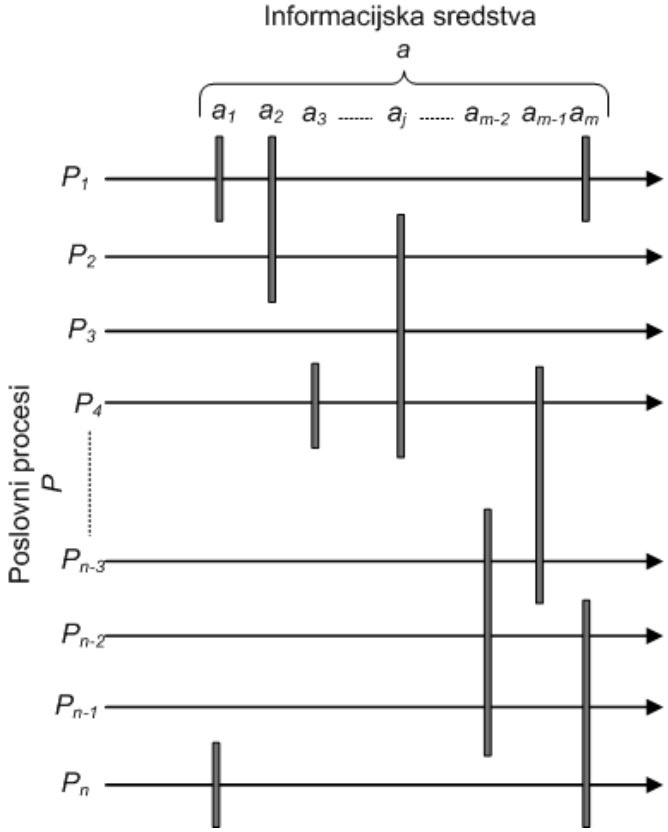
Ker so za vsak proces lahko želene stopnje varnosti za zaupnost, celovitost in razpoložljivost različne (12), se pri tistih sredstvih, ki so vključeni v več poslovnih procesov, lahko pojavijo za stopnje varnosti različne vrednosti. V tem primeru se za posamezne stopnje varnosti vsakega sredstva določi tista stopnja varnosti procesa, ki je najvišja. Za informacijsko sredstvo a, ki je vključeno v poslovne procese od P_1 do P_n, lahko zapišemo:

$$S_a^C = \max(S_{P_1}^C,\ldots,S_{P_n}^C) \tag{18}$$

$$S_a^I = \max(S_{P_1}^I,\ldots,S_{P_n}^I) \tag{19}$$

$$S_a^A = \max(S_{P_1}^A,\ldots,S_{P_n}^A) \tag{20}$$

Slika 34: *Shematični prikaz relacije med informacijskimi sredstvi in procesi*



Cilj tega postopka je vsako informacijsko sredstvo ovrednotiti glede na želeno stopnjo varnosti za zaupnost, celovitost in razpoložljivost.

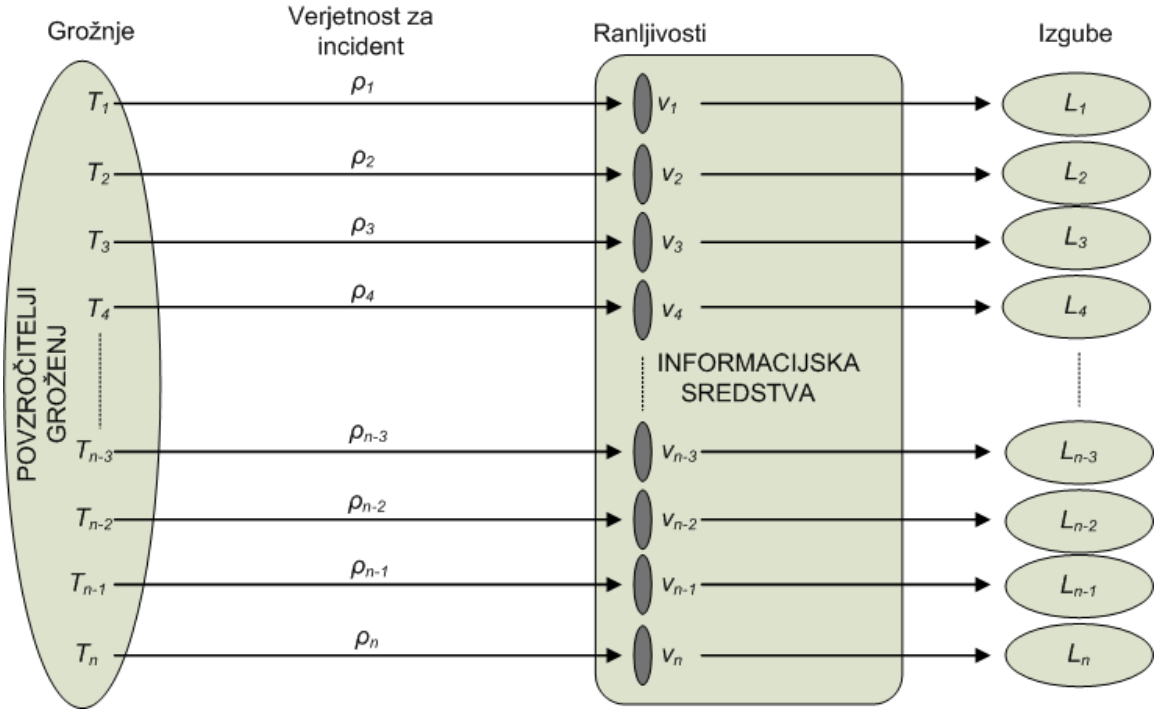
V kolikor podjetje ne potrebuje podrobne razdelitve stopenj varnosti na zaupnost, celovitost in razpoložljivost, lahko uporablja zgolj eno skupno vrednost. Tudi za stopnje varnosti sredstev velja enako, kot za stopnje varnosti poslovnih procesov (11):

$$\overline{S_a} = \max(S_a^C, S_a^I, S_a^A) \tag{21}$$

5.2 Ocena tveganja

V postopku ocene tveganj se za vsako informacijsko sredstvo določijo ter ovrednotijo ranljivosti in grožnje, ki so vezane na to sredstvo. Izhodni podatek ocene tveganja je parameter tveganja, ki ga opredeljujeta verjetnost za varnostni incident ter posledica varnostnega incidenta. Na sliki 35 je prikazan model analize tveganja.

Slika 35: *Modeliranje analize tveganja*



5.2.1 Identifikacija in vrednotenje ranljivosti

Informacijska sredstva imajo ranljivosti, preko katerih lahko grožnje zlorabijo sredstva. **Ranljivost *v*** sredstva definiramo kot verjetnost ($0 < v < 1$), da bo izvedena grožnja uspešno zlorabila sredstvo, na katerega je usmerjena. Mejna vrednost $v = 0$ bi pomenila, da so informacijska sredstva popolnoma varna[8], $v = 1$ pa, da so informacijska sredstva popolnoma ranljiva, ne glede na to, kateri varnostni ukrep se uvede. Taki vrednosti v praksi nista smiselni, zato sta iz obsega izpuščeni. Če za informacijsko sredstvo *a* obstaja *n* ranljivosti *v*, lahko zapišemo:

$$v_i \in a, \forall i = 1, \ldots, n \tag{22}$$

Pri tem je podjetje omejeno le na ranljivosti, ki jih pozna. Napadalec lahko pozna tudi ranljivosti, ki jih podjetje ne. V modelu predpostavimo, da je ena ranljivost lahko vezana zgolj na zaupnost v^C, celovitost v^I ali razpoložljivost v^A in ne more biti kombinacija teh opcij. V nadaljevanju bo pri splošni navedbi ranljivosti uporabljena oznaka *v*, v kolikor bo potrebno posebej ločiti, bo navedeno v^C, v^I ali v^A.

[8] Kot sem navedel v poglavju 1.2.2, se je potrebno zavedati, da popolne varnosti ni.

5.2.2 Identifikacija in vrednotenje verjetnosti groženj

Zbirka groženj se neprestano spreminja s časom in je le delno znana (ISO 13335-1, 2004). **Verjetnost grožnje *T*** definiramo kot verjetnost za izveden dogodek, ki ima neželene učinke na informacijska sredstva. Verjetnost grožnje ($0 \leq T \leq 1$) je število napadov na enoto časa. Izbira ustrezne enote časa je poljubna. Za nadaljnjo obdelavo in primerjavo je priročna enota na primer en dan, lahko pa je seveda večja ali manjša. V tabeli 7 je prikazan poenostavljen primer različnih enot časa, če je povprečno število določenega incidenta eden na leto.

Tabela 7: *Prikaz verjetnosti za en dogodek v različnih enotah časa*

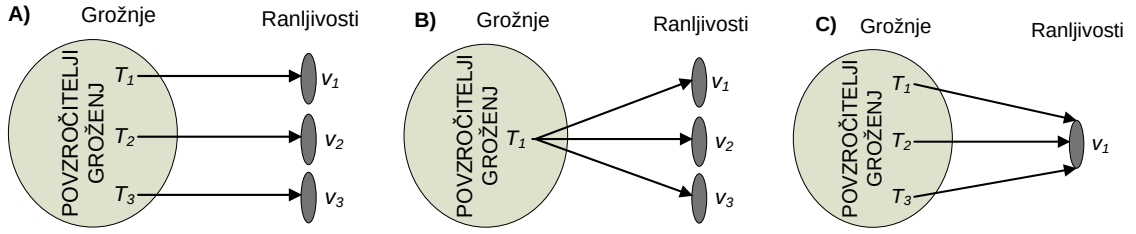
Enota časa	Verjetnost
na leto	1
na mesec	0,0833
na dan	0,0027
na uro	$1{,}14 \times 10^{-4}$
na minuto	$1{,}90 \times 10^{-6}$
na sekundo	$3{,}17 \times 10^{-8}$

Pri vrednotenju verjetnosti grožnje T se je potrebno zavedati, da na verjetnost vpliva veliko faktorjev, 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 napadalcu o visoki stopnji varnosti lahko napadalca odvrne, saj zahteva več napadalčevih virov na razpolago) idr. Vsaka grožnja izkorišča določeno ranljivost in je usmerjena na zlorabo zaupnosti, celovitosti ali razpoložljivosti. Z drugimi besedami, grožnja T lahko zlorabi v^C, v^I ali v^A. Model vključuje več možnih scenarijev relacij med ranljivostmi in grožnjami:

- Ena grožnja napada natanko eno ranljivost (T:v = 1:1).
- Ena grožnja napada več ranljivosti (T:v = 1:∞). Pri tem so vse ranljivosti vezane le na eno izmed varnostnih zahtev (zaupnost, celovitost ali razpoložljivost).
- Več groženj napada eno ranljivost (T:v = ∞:1). Pri tem so vse grožnje vezane le na eno izmed varnostnih zahtev (zaupnost, celovitost ali razpoložljivost).

Relacija med grožnjami in ranljivostmi je shematično prikazana na sliki 36.

Slika 36: *Shematični prikaz relacije med grožnjami in ranljivostmi*



5.2.3 Verjetnost za varnostni incident

Nekateri izvedeni neželeni dogodki so za povzročitelja grožnje uspešni in povzročijo varnostni incident, medtem ko drugi dogodki niso uspešni. Verjetnost, da bo izvedena grožnja uspešna, je določena z ranljivostjo sredstva *v.*

Naj ***ρ*** predstavlja **verjetnost za varnostni incident** (*0 ≤ ρ ≤1*), ki je odvisna od verjetnosti grožnje *T* in ranljivosti sredstva *v*. Verjetnost za varnostni incident določimo kot produkt med verjetnostjo za grožnjo in ranljivostjo.

$$\rho(T, v) = T \cdot v \tag{23}$$

Funkcija ρ izpolnjuje tudi robne pogoje sistema. Verjetnost za incident je nič, v kolikor ni nobenega napada (verjetnost za napad je nič):

$$\rho(0, v) = 0 \tag{24}$$

Verjetnost za incident je nič, v kolikor sistem nima nobene ranljivosti (ranljivost sistema je nič):

$$\rho(T, 0) = 0 \tag{25}$$

Predpostavimo, da verjetnost za napad T in ranljivost v povečujeta verjetnost za incident ρ. Obnašanje funkcije ρ opišemo z:

$$\frac{\partial \rho}{\partial T} > 0 \tag{26}$$

$$\frac{\partial \rho}{\partial v} > 0 \tag{27}$$

5.2.4 Izguba v primeru varnostnega incidenta

V primeru varnostnega incidenta podjetje utrpi finančno **izgubo *L***. Izguba *L > 0* je merjena v denarnih enotah. Predpostavimo, da je *L* sicer lahko zelo velika

vrednost, vendar v modelu vedno ostaja končna. To pomeni, da model ne vsebuje primerov možnih izgub v primerih katastrofe.

Pri vrednotenju izgub je potrebno ločiti izgube, ki nastanejo takoj ob incidentu in posredne izgube, ki imajo lahko dolgoročne posledice.

$$L = L_{takojšnje} + L_{posredne} \tag{28}$$

Po raziskavah (Campbell et al, 2003, str. 431; Hovava & D'Arcy, 2003) imajo posredne izgube velike dolgoročne učinke na tržno vrednost podjetja večinoma le pri zlorabah zaupnosti. Zato se lahko podjetje pri določevanju posrednih izgub omeji le na izgube, vezane na zlorabo zaupnosti. Enačbo (28) lahko ob upoštevanju tega dopolnimo z:

$$L = \begin{cases} L_{takojšnje} + L_{posredne} & ; v^C > 0 \\ L_{takojšnje} & ; v^C = 0 \end{cases} \tag{29}$$

Za kvantitativno vrednotenje takojšne izgube razdelimo na:

$$L_{takojšnje} = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} \tag{30}$$

Pri tem oznake pomenijo:

- L_s - strošek zamenjave opreme zaradi kraje, uničenja, izgube ali okvare
- $L_r(t)$ - strošek popravila (vzpostavitev delujočega stanja)
- $L_i(t)$ - izguba prihodkov podjetja
- $L_p(t)$ - izguba produktivnosti podjetja
- L_{SLA} - izguba zaradi nespoštovanja zakonskih predpisov ali pogodbenih obveznosti

Strošek zamenjave opreme L_s predstavlja strošek nakupa nove opreme. To vrsto izgub je najenostavneje ovrednotiti, saj so podatki običajno že na razpolago ali pa se lahko dokaj enostavno pridobijo. V primeru okvare opreme se lahko ta strošek občutno zmanjša ob investiciji v garancijo, ki jo ponujajo proizvajalec ali razni vzdrževalci opreme.

Strošek popravila $L_r(t)$ lahko ovrednotimo kot:

$$L_r(t) = n \cdot p \cdot t_r \tag{31}$$

Pri tem je:

- n – število zaposlenih, ki odpravlja problem
- p – povprečna plača zaposlenih, ki odpravljajo problem (v primeru zunanjega izvajanja odprave problema je to urna postavka izvajalca)

- t_r – čas popravila (redni čas in nadure)

Izgubo prihodkov podjetja $L_i(t)$ lahko ovrednotimo kot:

$$L_i(t) = EF_I \cdot i \cdot t_{NA} \tag{32}$$

Pri tem je:

- EF_I – vpliv incidenta na prihodek $(0 \leq EF_I \leq 1)$
- i – povprečni prihodek na časovno enoto
- t_{NA} – čas nedelovanja

Izgubo produktivnosti podjetja $L_p(t)$ lahko ovrednotimo kot:

$$L_p(t) = m \cdot EF_p \cdot p' \cdot t_{NA} \tag{33}$$

Pri tem je:

- m – število zaposlenih, ki imajo moteno produktivnost
- EF_P – vpliv incidenta na produktivnost $(0 \leq EF_P \leq 1)$
- p' – povprečna plača zaposlenih, ki imajo moteno produktivnost
- t_{NA} – čas nedelovanja

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 s strankami sklenjeno SLA pogodbo. V primeru, da je razpoložljivost storitve, ki jo ponuja podjetje, pod mejo določeno v SLA, predstavlja to za podjetje strošek, saj mora strankam povrniti del plačila.

Z upoštevanjem (30), (31), (32) in (33) lahko izgube (28) zapišemo:

$$L = L_s + L_r^0 \cdot t_r + L_i^0 \cdot t_{NA} + L_p^0 \cdot t_{NA} + L_{SLA} + L_{posredne} \tag{34}$$

Pri tem se zaradi poenostavitve dodatno uvedejo faktorji:

$$L_r^0 = n \cdot p \tag{35}$$

$$L_i^0 = EF_i \cdot i \tag{36}$$

$$L_p^0 = m \cdot EF_p \cdot p' \tag{37}$$

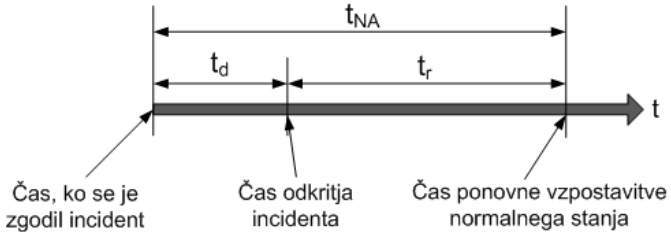
Pri enačbah (31), (32) in (33) nastopata dva časovna parametra, **čas popravila** t_r in **čas nedelovanja** t_{NA}. Čas nedelovanja je sestavljen iz **časa detekcije** t_d, v katerem se odkrije, da je prišlo do incidenta, in časa, ki je potreben, da se delovanje

sistema ponovno vzpostavi t_r. Čas t_d se šteje od trenutka, ko se je incident zgodil, do odkritja incidenta. Tako lahko zapišemo:

$$t_{NA} = t_d + t_r \tag{38}$$

Odvisnost med časi t_{NA}, t_r in t_d je prikazana na sliki 37.

Slika 37: *Shematični prikaz časov nedelovanja t_{NA}, detekcije t_d in popravila t_r*



Razlago za časa t_r in t_{NA} ponuja tudi ITILv3. Čas t_r je po ITIL standardu povprečen čas za popravilo sredstva ali storitve po odpovedi (angl. *Mean Time To Repair, MTTR*). Čas t_{NA} je po ITIL standardu povprečen čas za ponovno vzpostavitev storitve po odpovedi (angl. *Mean Time to Restore Service, MTRS*). ITIL definira tudi parameter povprečni čas med incidenti (angl. *Mean Time Between Incidents, MTBI*), ki je obratno sorazmeren z verjetnostjo za incident.

V modelu je uporabljenih nekaj poenostavitev, da model ni preveč kompleksen. Prva poenostavitev je, da se začne reševanje takoj, ko se incident odkrije. Druga je, da lahko obstajajo incidenti, kjer je $t_r > 0$ in $t_d > 0$, vendar ne povzročijo nedelovanja storitve $t_{NA} = 0$. Varnostni incident na primer lahko povzroči stroške popravila, vendar sistema ne ohromi do take mere, da ne bi deloval. Zato se loči dve situaciji: čas nedelovanja in čas nepopolnega delovanja. Pri prvi storitve ne delujejo, pri drugi pa sicer delujejo, vendar stanje še ni sanirano. V modelu se ti dve situaciji poenoti tako, da se za primere nepopolnega delovanja postavi $EF_i = 0$.

Z upoštevanjem enačbe (38), lahko izgube (34) zapišemo:

$$L = \left(L_r^0 + L_i^0 + L_p^0\right) \cdot t_r + \left(L_i^0 + L_p^0\right) \cdot t_d + L_s + L_{SLA} + L_{posredne} \tag{39}$$

Enačbo (39) lahko zapišemo še bolj poenostavljeno:

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 \tag{40}$$

Pri tem oznake pomenijo:

$$L_1 = L_r^0 + L_i^0 + L_p^0 \tag{41}$$

$$L_2 = L_i^0 + L_p^0 \tag{42}$$

$$L_3 = L_s + L_{SLA} + L_{posredne} \tag{43}$$

5.2.5 Varnostno tveganje

Na podlagi ocenjene verjetnosti za varnostni incident in izgubo, lahko izračunamo **varnostno tveganje *R***:

$$R = \rho \cdot L \tag{44}$$

Tveganje *R* predstavlja pričakovano finančno izgubo zaradi varnostnega incidenta. *R* je merjen v enakih denarnih enotah kot *L*. Če upoštevamo funkciji verjetnost za incident ρ (23) in izgubo *L* (40) dobimo:

$$R = T \cdot v \cdot L = T \cdot v \cdot \left[L_1 \cdot t_r + L_2 \cdot t_d + L_3 \right] \tag{45}$$

Tveganje je enako kot grožnja usmerjeno na zaupnost, celovitost in razpoložljivost.

5.3 Izbira in vrednotenje varnostnih ukrepov

5.3.1 Določitev ustrezne obravnave tveganja

Za vsako varnostno tveganje je na voljo več možnosti, kako podjetje to tveganje obravnava. Glede na opravljeno oceno tveganja, ima podjetje na izbiro sledeče obravnave, ki so podrobneje opredeljene v poglavju 2.1.2:

- **zmanjšanje** varnostnega tveganja z investicijo v uvedbo ustrezne zaščite, ki je lahko preventivna, korektivna ali detekcijska,
- **prenos** varnostnega tveganja (npr. na zavarovalnico ali ponudnika storitev),
- **izogibanje** tveganja z omejevanjem ali zaustavitvijo storitve,
- **sprejem** tveganja kot del poslovanja, brez uvedbe dodatnih zaščit.

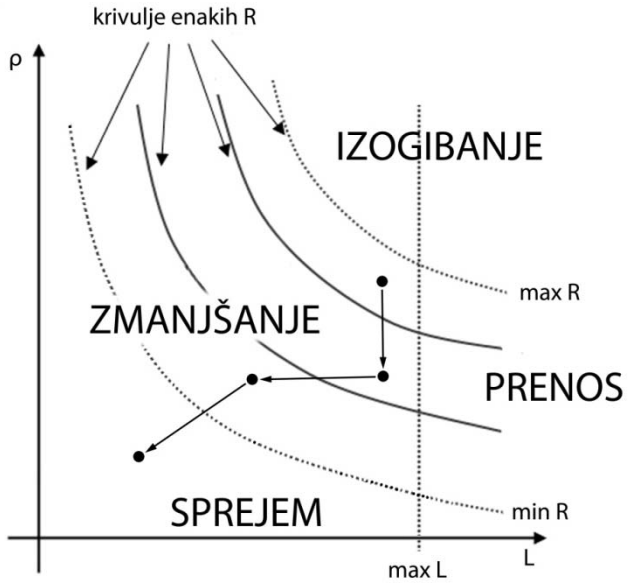
Za izbiro ustrezne obravnave je potrebno določiti *mejne vrednosti parametrov tveganja*. Te vrednosti so:

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

Posamezno tveganje lahko prikažem na grafu $\rho = \rho(L)$, kot je prikazano na sliki 38. Pri tem se vzame za osnovo graf na sliki 4 na strani 38, ki se ga ustrezno dopolni.

Krivulje na grafu predstavljajo točke z isto vrednostjo tveganja. Varnostni ukrep *s,* ki zmanjšuje tveganje *R,* prestavi točko tveganja na nižjo krivuljo tveganja *R*. Če ukrep zmanjša verjetnost za incident *ρ*, je premik na grafu vertikalno navzdol. Če pa ukrep zmanjšuje izgubo, je premik na grafu horizontalno proti levi.

***Slika 38**: Grafični prikaz krivulj tveganja v odvisnosti od ρ in L*



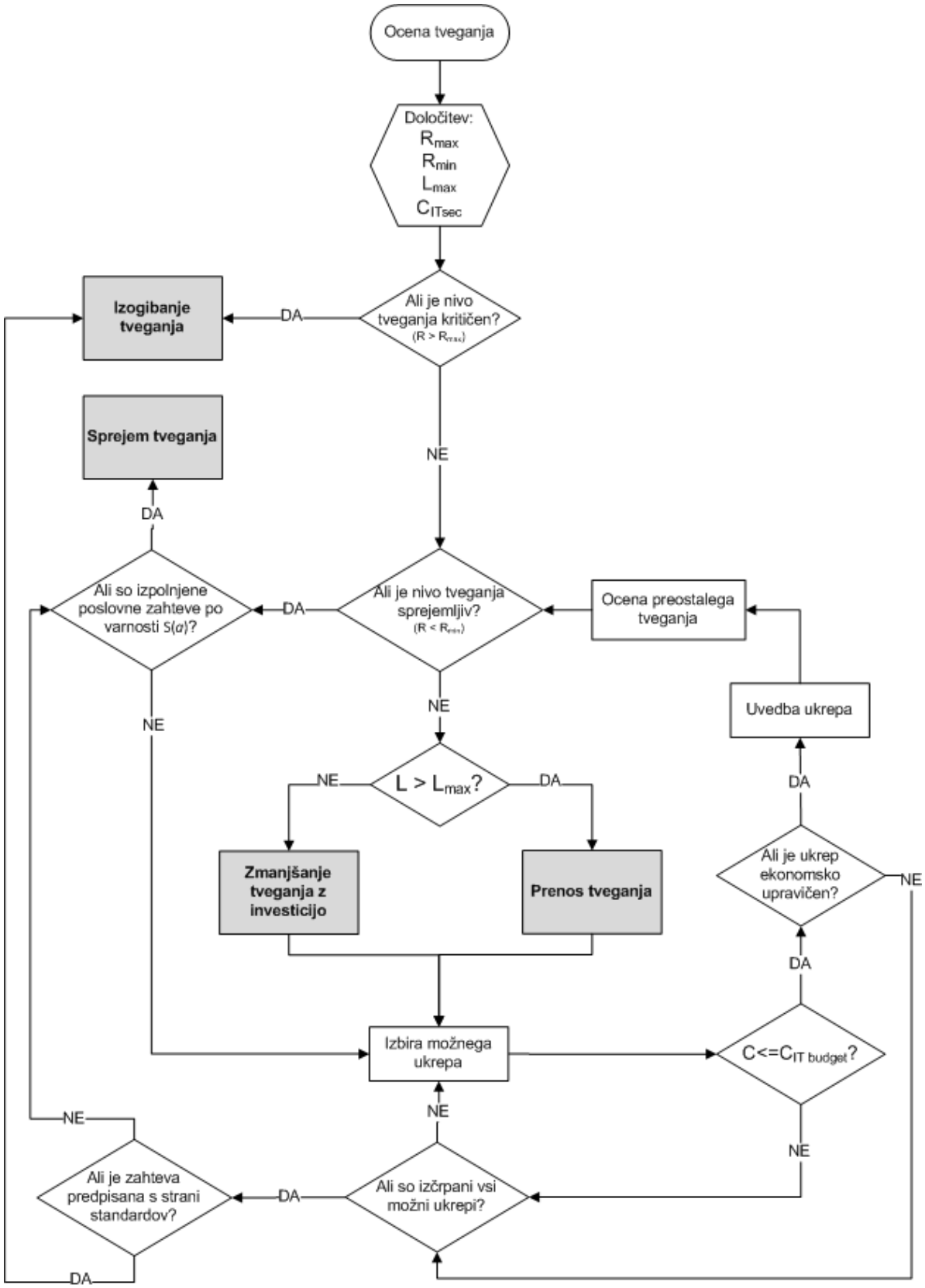
Ustrezno obravnavo tveganja se izvede tako, da se vrednosti *R* in *L* primerja z mejnimi vrednostmi R_{max} , L_{max} in R_{min}. Rezultati ocene so:

- $R > R_{max}$ - zaradi zelo visokega tveganja je priporočljivo izogibanje tveganju.
- $R < R_{min}$ - tveganje je zanemarljivo nizko, zato uvajanje varnostnega ukrepa ni finančno upravičeno.
- $L > L_{max}$ - zaradi visoke izgube je priporočljiv prenos tveganja. Schneier (2003, str. 23) pravi, da zares velike posledice niso sprejemljive ne glede na pogostost.
- $L < L_{max}$ - priporoča se zmanjšanje tveganja z investicijo v varnostni ukrep, kot je zapisano v enačbi (45).

Možne so tudi kombinacije teh obravnav. Na primer podjetje najprej izvede varnostne ukrepe, ki zmanjšajo izgubo, ter preostanek tveganja prenese na zavarovalnico. Pri tem je potrebno ugotoviti, ali je investicija v varnostni ukrep manjša od zmanjšanja premije, ki se jo plačuje zavarovalnici.

Izbira ustrezne obravnave varnostnega tveganja je proces, ki je prikazan na sliki 39.

Slika 39: *Proces izbire ustrezne obravnave tveganja glede na parametre R_{min} , R_{max} , L_{max} in C_{ITsec_budget}*



Pri tem procesu vzamemo za osnovo proces prikazan na sliki 5 na strani 39 in ga ustrezno nadgradimo. Skozi proces potekajo izbire obravnav, vezane na parametre. Poleg parametrov R_{min} , R_{max} in L_{max} se v procesu odločanja upošteva še poslovne zahteve po varnosti $S(a)$ ter proračun podjetja za investicije v informacijsko varnost C_{ITsec_budget}. Cena ukrepov C v določenem obdobju ne sme presegati proračuna. Če je cena ukrepa večja kot znaša proračun, uvedba tega ukrepa ni mogoča. V kolikor pri zmanjšanju tveganja ni na voljo nobenega ustreznega ukrepa, je potrebno zmanjšanje tveganja zamenjati za sprejem ali izogibanje tveganju.

5.3.2 Vrste varnostnih ukrepov

Pred varnostnimi incidenti se podjetje zavaruje z **varnostnimi ukrepi *s***. Podjetje lahko izbira med številnimi varnostnimi ukrepi. Glede na njihov vpliv na zmanjšanje parametrov R, ρ in L jih lahko razvrstimo v tri vrste:

- **preventivni varnostni ukrepi s_p**, ki zmanjšujejo verjetnost za varnostni incident ρ[9],
- **korektivni varnostni ukrepi s_k**, ki zmanjšujejo čas za popravilo t_r in izgubo L zaradi uspešnega incidenta,
- **detekcijski varnostni ukrepi s_d**, ki zmanjšujejo čas za odkritje incidenta t_d ter omogočijo pridobitev informacije o grožnjah.

Od preventivnih varnostnih ukrepov, ki zmanjšujejo verjetnost za incident, se korektivni varnostni ukrepi ločijo po tem, da zmanjšujejo izgubo v primeru uspešnega incidenta. Detekcijski varnostni ukrepi omogočajo podrobnejšo analizo varnostnih dogodkov, zaznavajo incidente in na njih opozarjajo. V kolikor incidenta ne odkrije detekcijska zaščita, ga lahko podjetje odkrije tudi preko posledic ali drugih sledi, ki jih je pustil zlonamerni uporabnik. Primera preventivnih varnostnih ukrepov sta:

- požarni zid in
- protivirusna zaščita.

Izraza preventivna in korektivna zaščita se nanašata na to, ali se je zgodil varnostni incident. V določenih drugih literaturah sta izraza vezana glede na čas (Purcell, 2007). Preventivna zaščita je tam omenjena kot zaščita, ki se uvede preden pride do varnostnega incidenta, korektivna zaščita pa, ko se je varnostni incident že zgodil. V nasprotju s tem, se v predlaganem modelu tudi korektivna zaščita določi preden se varnostni incident zgodi. Njen namen pa je zmanjševanje posledic incidenta. Primeri korektivnih varnostnih ukrepov so:

[9] Ob tem se privzame, da podjetja lahko investirajo le v zmanjšanje ranljivosti ter da ne morejo investirati v zmanjšanje groženj.

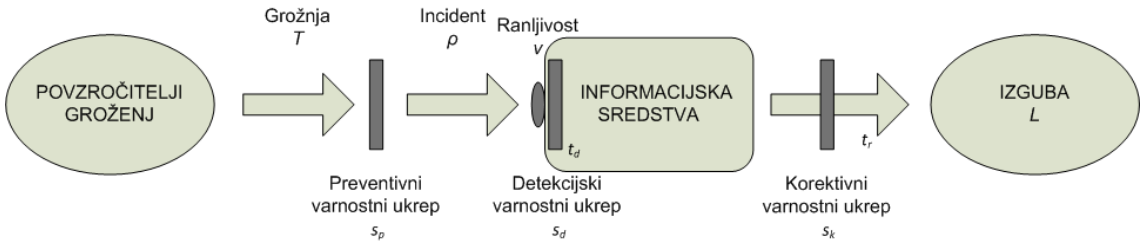
- vzdrževalna pogodba s proizvajalci vpliva na strošek zamenjave opreme L_s,
- načrt neprekinjenega poslovanja ali varnostno kopiranje podatkov vpliva na strošek popravila L_r, izgubo prihodkov podjetja L_i in izgubo produktivnosti zaposlenih L_p,
- uvedba redundančnega sistema vpliva na izgubo prihodkov podjetja L_i in izgubo produktivnosti zaposlenih L_p,
- medijsko oglaševanje ali uvedba različnih standardov (npr. ISO) vpliva na posredne izgube $L_{posredne}$.

Uporaba detekcijske zaščite omogoča podjetju, poleg zmanjšanja izgub, tudi realnejše vrednotenje verjetnosti za napad T in verjetnosti za incident ρ. V kolikor podjetje ne uporablja detekcijske zaščite, so te vrednosti zgolj približna ocena, ki pa je lahko tudi precej drugačna od realne situacije. Napačne predpostavke pa lahko vodijo do neoptimalne izbire varnostnih ukrepov. Primer detekcijskega varnostnega ukrepa je sistem IDS.

5.3.3 Karakteristike varnostnih ukrepov

Model analize tveganja z varnostnimi ukrepi je prikazan na sliki 40. Povzročitelji groženj izvajajo grožnje oziroma napade na sistem. Napadi so usmerjeni na ranljivost informacijskega sredstva. Pred napadi se podjetje zavaruje s preventivnimi ukrepi, ki zmanjšujejo verjetnost za varnostni incident. V primeru incidenta, pa lahko korektivni varnostni ukrep zmanjša nastalo izgubo.

Slika 40: *Modeliranje analize tveganja*



Varnostni ukrep *s* definiramo s parametroma strošek ukrepa C in produktivnost ukrepa α.

$$s = s(C, \alpha) \tag{46}$$

Strošek ukrepa *C* definiramo kot denarno investicijo v varnostni ukrep, ki vsebuje vse stroške, vezane na uvedbo varnostnega ukrepa.

$$0 \le C \le C_{IT\,\mathrm{sec}\,budget} \tag{47}$$

C_{ITsec_budget} je proračun podjetja namenjen za varnostne investicije, ki ga je potrebno upoštevati pri uvedbi varnostnih ukrepov. Strošek C varnostnih ukrepov ne sme

presegati C_{ITsec_budget} v določenem proračunskem obdobju. V kolikor se v časovnem obdobju, na katerega je določen proračun, uvede n varnostnih ukrepov, mora veljati:

$$0 \le \sum_{i=1}^{n} C_i \le C_{ITbudget} \tag{48}$$

Po raziskavi CSI (2009) je v povprečju 3-5 % sredstev podjetja namenjenih za IT varnost. Če je cena ukrepa višja kot znaša proračun, uvedba tega ukrepa ni mogoča.

Investicija v varnostni ukrep C je sestavljena iz različnih stroškov:

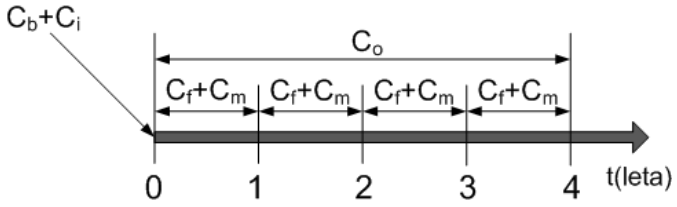
$$C = C_b + C_i + C_f + C_m + C_o \tag{49}$$

Pri tem so nekateri stroški enkratni, nekateri pa se periodično ponavljajo:

- C_b - enkraten strošek nabave opreme
- C_i - enkraten strošek uvedbe, testiranja, izobraževanja
- C_f - strošek nadgradenj in popravkov
- C_m - strošek vzdrževanja
- C_o - ostali stroški povezani z uvedbo ukrepa

Na sliki 41 je prikazana časovna porazdelitev stroškov, porazdeljenih na štiri leta.

Slika 41: *Prikaz stroškov pri uvedbi ukrepa*



Vrednosti C_i in C_m sta časovno odvisni. Za obe lahko zapišemo, da je vrednost enaka številu opravljenih ur pomnoženo z urno postavko:

$$C_i(t) = p \cdot t_i \tag{50}$$

Pri tem je:

- p – povprečna urna postavka zaposlenega, ki skrbi za uvedbo (v primeru zunanjega izvajanja je to urna postavka izvajalca)
- t_i – skupen čas uvedbe ukrepa

$$C_m(t) = p \cdot t_m \tag{51}$$

Pri tem je:

- p – povprečna urna postavka zaposlenega, ki skrbi za vzdrževanje
- t_m – skupen čas porabljen za vzdrževanje

Grobo oceno glede skupnih stroškov investicije v varnostni ukrep dobimo z uporabo GLEIS modela, ki je predstavljen v poglavju 4.3.4 (Gordon & Loeb, 2002b; Gordon & Loeb, 2005). Po tem modelu naj investicija v varnostni ukrep ne bi presegala dobre tretjine možne izgube L (39).

$$C < 0{,}37 \cdot L \tag{52}$$

Produktivnost varnostnega ukrepa $\alpha(t) > 0$ predstavi vpliv varnostnega ukrepa na zmanjšanje tveganja. Določevanje parametra α je lahko zelo težavno, saj kvantitativnih podatkov, na podlagi katerih bi podali oceno parametra α, pravzaprav ni.

Produktivnost ukrepa ima lahko različne vrednosti glede na posamezne varnostne zahteve. Zato lahko parameter α za posamezni varnostni ukrep razdelimo na produktivnost glede zaupnosti α^C, produktivnost glede celovitosti α^I in produktivnost glede razpoložljivosti α^A.

Zaradi vedno novih groženj produktivnost varnostnega ukrepa $\alpha(t)$, s časom konveksno pada, v kolikor ni dodatnih investicij v varnostne ukrepe.

$$\frac{\partial \alpha(t)}{\partial t} < 0 \quad , \quad \frac{\partial^2 \alpha(t)}{\partial t^2} > 0 \tag{53}$$

Zaradi tega mora podjetje neprestano investirati v varnostne ukrepe, če želi zmanjšati ali vsaj ohraniti tveganje na istem nivoju.

5.3.4 Vpliv uvedbe varnostnega ukrepa na zmanjšanje verjetnosti za incident

Verjetnost za varnostni incident $\rho(t)$ se lahko zmanjša z uvedbo preventivnega varnostnega ukrepa $s_p(\alpha_p, C_p)$, ki zmanjšuje ranljivost sredstev. Funkcijo ρ (23) dopolnimo tako, da dodamo odvisnost od investicije v varnostni ukrep C_p, ki zmanjšuje verjetnost za varnostni incident:

$$\rho = \rho(T, v, C_p) \tag{54}$$

Robna pogoja (24) in (25) razširimo v:

$$\rho(0, v, C_p) = 0 \tag{55}$$

$$\rho(T,0,C_p)=0 \tag{56}$$

Dodamo še dva nova robna pogoja. V kolikor ne investiramo v varnostni ukrep, je verjetnost za incident enaka produktu verjetnosti za napad *T* in ranljivosti *v*, kot določa (23)*:*

$$\rho(T,v,0)=T\cdot v \tag{57}$$

Verjetnost za incident limitira proti nič, v kolikor je investicija neskončna:

$$\lim_{C_p\to\infty}\rho(T,v,C_p)=0 \tag{58}$$

Verjetnost za incident zmanjšuje preventivni varnostni ukrep s_p, kar lahko opišemo:

$$\frac{\partial\rho}{\partial C_p}<0 \quad , \quad \frac{\partial^2\rho}{\partial {C_p}^2}>0 \tag{59}$$

Na voljo je več možnih funkcij verjetnosti za incident *ρ*, ki ustrezajo robnim pogojem od (55) do (59). V modelu je uporabljen razred funkcij, ki je med raziskovalci najbolj zanimiv (Matsuura, 2008, str. 2; Gordon & Loeb; 2002b):

$$\rho(T,v,C_p)=T\cdot v^{\alpha_p C_p+1} \tag{60}$$

Ob upoštevanju enačbe (60) lahko tveganje v enačbi zapišem (44):

$$R=T\cdot v^{\alpha_p C_p+1}\cdot L \tag{61}$$

Poleg izbrane funkcije verjetnosti za varnostni incident, so v raziskovalni literaturi uporabljene tudi druge vrste funkcij. Gordon in Loeb (2002b) sta poleg funkcije (60) predlagala tudi naslednjo funkcijo:

$$\frac{Tv}{(\chi C_p+1)^{\beta}};\chi>0,\beta\in R \tag{62}$$

Eno izmed možnih funkcij verjetnosti za varnostni incident je predstavil Willemson (2006):

$$\begin{cases} Tv(1-\dfrac{C_p}{b})^k & ;0\le C_p<b, b>0, k>2 \\ 0 & ;C_p\ge b \end{cases} \tag{63}$$

Z enačbo (61) lahko preverimo, kolikšna je minimalna stopnja tveganja, ki jo lahko dosežemo z določeno investicijo v preventivni varnostni ukrep. V kolikor želimo

imeti najmanjše tveganje R za določeno investicijo v preventivni varnostni ukrep C_p, upoštevamo pogoja:

$$\frac{\partial R(C_p)}{\partial C_p} = 0 \quad , \quad \frac{\partial^2 R(C_p)}{\partial {C_p}^2} > 0 \tag{64}$$

Če v pogoj (64) vstavimo enačbo (61), lahko zapišemo:

$$\frac{\partial R}{\partial C_p} = \alpha_p \cdot T \cdot \ln v \cdot v^{\alpha_p C_p^* + 1} \cdot L = 0; C_p^* \to \infty \tag{65}$$

Pri tem s C_p^* označimo vrednost stroškov investicije, pri kateri je tveganje najmanjše. Preverimo še, ali je dobljeni ekstrem zares minimum:

$$\left.\frac{\partial^2 R}{\partial {C_p}^2}\right|_{C_p^* \to \infty} = {\alpha_p}^2 \cdot T \cdot \left(\ln v\right)^2 \cdot v^{\alpha_p C_p + 1} \cdot L > 0 \tag{66}$$

Rezultat (66) velja za vse vrednosti C_p, zato je C_p^* zares minimum. To pomeni, da lahko tveganje popolnoma izničimo le ob neskončni investiciji v preventivno zaščito. To se sklada z že navedeno trditvijo, da 100 % varnosti ni mogoče doseči.

5.3.5 Vpliv uvedbe varnostnega ukrepa na zmanjšanje izgub

Izgubo, ki nastane zaradi varnostnih incidentov, se lahko zmanjša z investicijo C_k v korektivni varnostni ukrep s_k in z investicijo C_d v detekcijski varnostni ukrep s_d.

Korektivni varnostni ukrepi zmanjšujejo čas popravila in nedelovanja ter posledično izgubo, katero podjetje utrpi v primeru incidenta:

$$t_r = t_r(s_k) = t_r(\alpha_k, C_k) \tag{67}$$

Določimo še robne pogoje. Prvi določa vrednost časa popravila t_r v primeru, da se v varnostni ukrep ne investira:

$$t_r(0) = t_r^0 \tag{68}$$

V kolikor je investicija v varnostni ukrep neskončna, čas popravila limitira proti nič:

$$\lim_{C_k \to \infty} t_r(C_k) = 0 \tag{69}$$

Funkcija t_r je na celotnem intervalu $0 \le C_k \le C_{ITsec\_budget}$ padajoča in konveksna:

$$\frac{\partial t_r}{\partial C_k} < 0 \quad \frac{\partial^2 t_r}{\partial C_k^{\,2}} > 0 \quad , \tag{70}$$

Funkcija, ki ustreza tem robnim pogojem, je:

$$t_r = t_r^{\,0} e^{-\alpha_k C_k} \tag{71}$$

pri tem je t_r^0 čas popravila brez uvedene zaščite. Tveganje v enačbi (45) lahko ob upoštevanju (71) zapišemo:

$$R = T \cdot v \cdot \left[L_1 \cdot t_r^{\,0} e^{-\alpha_k C_k} + L_2 \cdot t_d + L_3 \right] \tag{72}$$

Za **detekcijske varnostne ukrepe** lahko zapišemo:

$$t_d = t_d(s_d) = t_d(\alpha_d, C_d) \tag{73}$$

Za funkcijo t_d veljajo enaki robni pogoji kot za funkcijo t_r v primeru investicije v korektivni ukrep. Po vzoru enačb (68), (69) in (70) lahko zapišemo:

$$t_d(0) = t_d^0 \tag{74}$$

$$\lim_{C_d \to \infty} t_d(C_d) = 0 \tag{75}$$

$$\frac{\partial t_d}{\partial C_d} < 0 \quad \frac{\partial^2 t_d}{\partial C_d^{\,2}} > 0 \quad , \tag{76}$$

Funkcija, ki ustreza tem robnim pogojem, je:

$$t_d = t_d^{\,0} e^{-\alpha_d C_d} \tag{77}$$

pri tem je t_d^0 čas zaznave incidenta brez uvedenega varnostnega ukrepa. Tveganje v enačbi (45) lahko ob upoštevanju (77) zapišemo:

$$R = T \cdot v \cdot \left[L_1 \cdot t_r + L_2 \cdot t_d^{\,0} e^{-\alpha_d C_d} + L_3 \right] \tag{78}$$

Po enačbi (38) vplivata čas popravila (71) in čas detekcije (77) na čas nedelovanja t_{NA}. Ob upoštevanju zgornjih enačb lahko zapišemo:

$$t_{NA} = t_r^{\,0} e^{-\alpha_k C_k} + t_d^{\,0} e^{-\alpha_d C_d} \tag{79}$$

Podobno kot pri preventivnem ukrepu, lahko tudi za korektivni ali detekcijski ukrep preverimo, kolikšna je minimalna stopnja tveganja, ki jo lahko dosežemo z določeno investicijo v korektivni varnostni ukrep. V kolikor želimo imeti najmanjše

tveganje R za določeno investicijo v korektivni varnostni ukrep C_k (izračun za detekcijski varnostni ukrep je zelo podoben), upoštevamo pogoja:

$$\frac{\partial R(C_k)}{\partial C_k} = 0\,,\ \frac{\partial^2 R(C_k)}{\partial {C_k}^2} > 0 \tag{80}$$

Če v pogoj (80) vstavimo enačbi (45) in (71), lahko zapišemo:

$$\frac{\partial R}{\partial C_k} = \frac{\partial T \cdot v \cdot L_1 {t_r}^0 e^{-\alpha_k C_k}}{\partial C_k} = -Tv\alpha L_1 {t_r}^0 e^{-\alpha {C_k}^*} = 0; {C_k}^* \to \infty \tag{81}$$

Pri tem s C_k^* označimo vrednost stroškov investicije, pri kateri je tveganje najmanjše. Preverimo še, ali je dobljeni ekstrem zares minimum:

$$\left.\frac{\partial^2 R}{\partial {C_k}^2}\right|_{C_k^* \to \infty} = Tv{\alpha_k}^2 L_1 {t_r}^0 e^{-\alpha_k C_k} > 0 \tag{82}$$

Rezultat (82) velja za vse vrednosti C_k , zato je C_k* zares minimum. To pomeni, da lahko tveganje popolnoma izničimo le ob neskončni investiciji v preventivno zaščito. To se sklada z že navedeno trditvijo, da 100 % varnosti ni mogoče doseči.

5.3.6 Vpliv prenosa tveganja

Eden izmed možnih varnostnih ukrepov je prenos tveganja na zavarovalnico ali na zunanjega izvajalca.

5.3.6.1 Prenos tveganja na zavarovalnico

V primeru prenosa tveganja na zavarovalnico je investicija C mesečna premija, ki jo podjetje plača kot zavarovanje, v primeru incidenta pa zavarovalnica izplača odškodnino I. Ker prenos tveganja zmanjšuje izgube ob varnostnem incidentu, na samo verjetnost pa nima vpliva, gre v tem primeru za posebno vrsto korektivnega varnostnega ukrepa, ki se zaradi specifike obravnava drugače.

V enačbo (30) zato dodamo še parameter $I(C) \geq 0$, ki predstavlja odškodnino, ki jo podjetje prejme v primeru incidenta. Izgube ob varnostnem incidentu lahko zapišemo:

$$L = L_s + L_r(t_r) + L_i(t_{NA}) + L_p(t_{NA}) + L_{SLA} + L_{posredne} - I \tag{83}$$

Izgube lahko zapišemo še krajše, če izpostavimo časovne faktorje kot v (40):

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 - I \tag{84}$$

Enačbi (83) in (84) lahko v celoti nadomestita enačbi (30) in (40). V primerih, ko se podjetje ne odloči za investicijo v zavarovanje je $I = 0$.

5.3.6.2 Zunanje izvajanje storitev

Drugi možnosti prenosa tveganja sta uporaba zunanjega izvajanja storitev (angl. *outsourcing*) ali gostovanja storitev (angl. *hosting*), kjer podjetje svoj informacijski sistem (ali del sistema) prenese k ponudniku. V primeru incidenta sta $L_s = 0$ in $L_r = 0$, saj podjetje nima investicij v lastno opremo. Še vedno podjetje utrpi izgubo zaradi zmanjšanja prihodkov in produktivnosti $L_i \geq 0$ in $L_p \geq 0$. V kolikor ima podjetje s ponudnikom podpisano ustrezno pogodbo o zagotavljanju storitev (angl. *Service Level Agreement, SLA*), je lahko v pogodbi določeno, da v primeru incidenta podjetje dobi odškodnino $I \geq 0$. Na zunanje izvajanje storitev se lahko gleda tudi kot na preventivno zaščito, v kolikor ima podjetje, ki svoje storitve ponuja, ustrezno infrastrukturo. Pri tem je pogoj podpisan SLA.

5.4 Ekonomsko optimalen varnostni ukrep

5.4.1 Izračun koristi zaradi investicije v varnostni ukrep

Z upoštevanjem (71), (77) in (84) lahko izgube v primeru varnostnega incidenta (40) zapišemo:

$$L = L_1 \cdot {t_r}^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot {t_d}^0 \cdot e^{-\alpha_d C_d} + L_3 - I \tag{85}$$

Če upoštevamo funkciji za verjetnost za varnostni incident ρ (60) in izgubo L (85), dobimo splošen zapis tveganja, ki vsebuje različne vrste možnih varnostnih ukrepov:

$$R = T \cdot v^{\alpha_p C_p + 1} \cdot L = T \cdot v^{\alpha_p C_p + 1} \left[L_1 \cdot {t_r}^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot {t_d}^0 \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{86}$$

Izračunamo **koristi** ***B***, ki jih investicija v varnostni ukrep prinaša. Koristi investicije v varnostni ukrep so enake zmanjšanju tveganja na račun uvedbe ukrepa. Tako lahko zapišemo:

$$B = R_0 - R(C) - \delta + \mu \tag{87}$$

Pri tem so:

- $R_0 = R(C = 0)$ - varnostno tveganje pred uvedbo varnostnega ukrepa.
- $R(C)$ - varnostno tveganje po uvedbi varnostnega ukrepa.

- δ - negativni vpliv uvedenega ukrepa na poslovanje. Pričakujemo, da uvedba večje stopnje varnosti zmanjšuje funkcionalnosti sistema, kar vpliva na produktivnost in poslovanje. Večja varnost pomeni omejitev funkcionalnosti, po drugi strani pa dodatne funkcionalnosti odpirajo nove varnostne luknje. Zelo pomembno je, da tveganje dobro razumemo, poudarja Schneier (2003, str. 25), sicer je lahko ocena za δ zelo slaba.
- μ - posredni pozitiven učinek uvedbe ukrepa (na primer večji ugled in status, reference, samozavest, povezava in dopolnitev z obstoječimi zaščitami, izpolnjevanje zakonskih obveznosti, nižja zavarovalna premija …).

Vrednosti δ in μ je v večini primerov težko oceniti. V grobem lahko upoštevamo, da sta parametra δ in μ linearno odvisna od stroška varnostnega ukrepa C in zapišemo:

$$\delta = k_1 \cdot C \tag{88}$$

$$\mu = k_2 \cdot C \tag{89}$$

5.4.2 Ekonomsko vrednotenje varnostnega ukrepa

Ko imamo za izbrano investicijo oceno koristi in stroškov, ocenimo donosnost izbranega ukrepa, oziroma ali je njegova uvedba ekonomsko upravičena. V ta namen uporabimo ROI, NPV in IRR, ki so po raziskavah najpogosteje uporabljeni kazalci v praksi (CSI, 2009, 2008, 2007).

Donosnost investicije (ROI) primerja koristi investicije s stroški, rezultat pa je donosnost investicije v odstotkih:

$$ROI = \frac{B - C}{C} \tag{90}$$

Pozitivna vrednost ROI pomeni, da je investicija ekonomsko upravičena. Če v (90) vstavim (87), dobim:

$$ROI = \frac{R_0 - R(C) - \delta + \mu - C}{C} \tag{91}$$

Za dolgoročne investicije je primernejša **neto sedanja vrednost (NPV)**, ki upošteva tudi časovni faktor:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+k)^t} \tag{92}$$

Pri tem je *k* diskontna stopnja, *n* pa časovno obdobje. NPV je merjen v denarnih enotah, investicija pa je ekonomsko upravičena, v kolikor je NPV > 0.

Notranja stopnja donosa (IRR) omogoča najti tisto diskontno stopnjo, pri kateri je NPV enak nič, oziroma pri kateri se sedanja vrednost prilivov in sedanja vrednost odlivov izenačita.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t} = 0 \tag{93}$$

Pri primerjavi dveh ali več varnostnih rešitev med seboj je pogosto potrebno upoštevati več kazalcev, ne samo enega, saj lahko posamezni kazalci favorizirajo različne rešitve (Bojanc & Jerman-Blažič, 2008a). Definiramo **ekonomsko optimalno varnostni ukrep**, ki ima med izbranimi varnostnimi rešitvami največje vrednosti za ROI, NPV in IRR.

$$s_{eko} = s\big|_{\max(ROI),\max(NPV),\max(IRR)} \tag{94}$$

Ekonomsko optimalen varnostni ukrep je tisti, ki ima pri izračunu kazalcev največje vrednosti. Zavedati se je potrebno, da kazalci niso vedno med seboj usklajeni. Tako na primer ROI favorizira eno rešitev, NPV drugo, IRR lahko celo tretjo. V takih primerih je potrebno pri izbiri ustreznega ukrepa upoštevati še druge parametre in se odločiti subjektivno. Podrobnejša analiza razlik med uporabljenimi kazalci je podana v poglavju 4.4.2.

5.4.3 Primerjava posameznih obravnav tveganja

Izračun kazalca ROI se lahko prilagodi različnim obravnavam tveganja, navedenih v poglavju 2.1.2. Izračun NPV in IRR je podoben kot izračun za ROI, le da je zaradi časovnega faktorja zapis manj pregleden.

V kolikor je izbrana obravnava tveganja investicija v **preventivni varnostni ukrep**, lahko za ROI enačbo (91) zapišemo:

$$ROI = \frac{R_0 - R(C_p) - \delta + \mu - C_p}{C_p} \tag{95}$$

Če vstavim vrednosti za *R* (61), dobimo:

$$ROI = \frac{T \cdot v\left(1 - v^{\alpha_p C_p}\right) \cdot L - \delta + \mu - C_p}{C_p} \tag{96}$$

Pri tem je izguba L enaka enačbi (40).

V kolikor je izbrana obravnava tveganja investicija v **korektivni varnostni ukrep**, lahko za ROI enačbo (91) zapišem:

$$ROI = \frac{R_0 - R(C_k) - \delta + \mu - C_k}{C_k} \tag{97}$$

$$ROI = \frac{TvL_1 t_r{}^0 \left(1 - e^{-\alpha_k C_k}\right) - \delta + \mu - C_k}{C_k} \tag{98}$$

V enačbi (98) sem upošteval enačbo za tveganje (72).

V kolikor je izbrana obravnava tveganja investicija v **detekcijski varnostni ukrep**, lahko za ROI enačbo (91) zapišemo:

$$ROI = \frac{R_0 - R(C_d) - \delta + \mu - C_d}{C_d} \tag{99}$$

$$ROI = \frac{TvL_2 t_d{}^0 \left(1 - e^{-\alpha_d C_d}\right) - \delta + \mu - C_d}{C_d} \tag{100}$$

V enačbi (100) smo upoštevali enačbo za tveganje (78).

Pri **prenosu tveganja** na zavarovalnico, je uveden korektivni varnostni ukrep, saj s prenosom tveganja nanjo ne zmanjšujemo možnosti za incident, temveč le blažimo posledice. Enačba (98) se poenostavi v:

$$ROI = \frac{TvI + \mu - C}{C} \tag{101}$$

Ker pri prenosu na zavarovalnico ne gre za poseg v sistem podjetja, je zanemarjen faktor zmanjšanja produktivnosti ($\delta \approx 0$), oziroma omejitve funkcionalnosti zaradi uvedenega varnostnega ukrepa. Strošek C predstavlja znesek mesečne premije, ki se plačuje zavarovalnici.

5.4.4 Upoštevanje želene stopnje varnosti

V modelu smo za iskanje ekonomsko optimalnega varnostnega ukrepa upoštevali kvantitativne rezultate koristi uvedbe ukrepa ter njegove stroške. V kolikor primerjamo med seboj ukrepe, ki zmanjšujejo isto tveganje, sta korist in strošek uvedbe ukrepa res zadostna podatka za odločitev o ekonomsko optimalnem ukrepu.

Če pa primerjamo med seboj ukrepe, ki zmanjšujejo različna tveganja, je potrebno, poleg koristi in stroškov, upoštevati še poslovne zahteve po želeni stopnji varnosti, ki se določijo za posamezne poslovne procese in sredstva (poglavje 5.1). Želene stopnje varnosti namreč določajo prioriteto in pomembnost posameznih tveganj in posledično ukrepov.

Za boljše razumevanje problema poglejmo enostaven primer. Podjetje se odloča za investicijo med dvema varnostnima ukrepoma s_A in s_B. Ukrep s_A zmanjšuje varnostno tveganje R_A, ukrep s_B pa varnostno tveganje R_B. Podatki o posameznih tveganjih A in B so v tabeli 8:

Tabela 8: *Primerjava rešitev z različnima poslovnima zahtevama*

	Rešitev A	**Rešitev B**
Začetno tveganje brez uvedenega ukrepa (R_0)	10.000 €	20.000 €
Tveganje z uvedenim ukrepom (R)	5.000 €	10.000 €
Cena ukrepa (C)	2.500 €	2.500 €
Želena stopnja varnosti (poglavje 5.1)	0,9	0,3
Izračunan ROI	100 %	300 %

Glede na naveden rezultat, bi se podjetje brez odlašanja odločilo za ukrep B, ki daje občutno večjo donosnost. Po drugi strani je tveganje A za podjetje bolj pomembno od tveganja B, želena stopnja varnosti (v tabeli 8 niso navedene ločene želene stopnje varnosti za zaupnost, celovitost ali razpoložljivost) je namreč trikrat večja za ukrep A, kot za ukrep B.

Zato uvedemo **poslovno-ekonomski optimalni varnostni ukrep**, ki združuje kvantitativno oceno za ekonomsko optimalen varnostni ukrep in podatek o želeni stopnji varnosti. Vrednotenje s kazalci ROI, NPV ali IRR dopolnimo z želeno stopnjo varnosti:

$$ROI_{pos-eko} = S_a \cdot ROI \tag{102}$$

$$NPV_{pos-eko} = S_a \cdot NPV \tag{103}$$

$$IRR_{pos-eko} = S_a \cdot IRR \tag{104}$$

Pri tem je S_a želena stopnja varnosti, ki je (po enačbi (17)) določena s poslovno zahtevo po varnosti informacijskega sredstva, ki je izpostavljeno tveganju. Z množenjem želene stopnje varnosti s kazalci ROI, NPV in IRR v enačbah (102), (103) in (104) ustvarimo povezavo med kvantitativnim izračunom donosnosti ukrepa in pomembnostjo tega ukrepa s poslovnega stališča. Tako ima lahko neki ukrep sicer veliko donosnost, vendar ima na račun nizke želene stopnje varnosti rezultat poslovno-ekonomskega kazalca manjšo vrednost. V zgornjem primeru,

prikazanem v tabeli 8, sta poslovno-ekonomska izračuna ROI za oba varnostna ukrepa enaka in znašata 0,9.

Kazalec poslovno-ekonomski optimalni varnostni ukrep ni namenjen finančnemu vrednotenju, temveč primerjavi različnih ukrepov za različna tveganja med seboj. Za primere, ko več možnih ukrepov zmanjšuje isto tveganje, so poslovne varnostne zahteve enake in je primerjava kazalcev poslovno-ekonomskega optimalnega ukrepa enaka primerjavi kazalcev ROI, NPV ali IRR.

Poslovne zahteve določajo tudi to, koliko preostalega tveganja si podjetje lahko privošči. Zato mora biti pri izbiri ukrepa upoštevano tudi to, ali je izpolnjen pogoj za minimalno preostalo tveganje, ki pomaga tudi pri izbiri obravnave tveganja (poglavje 5.3.1). Velja pogoj:

$$preostalo\ tveganje\,(R) < \frac{R_{\min}}{S_a} \tag{105}$$

To pomeni da je R_{min} zares najmanjša vrednost tveganja samo za najvišje poslovne zahteve, za nižje poslovne zahteve pa je navidezno višji.

5.4.5 Ocena potrebne investicije za dosego optimalne varnosti

V tem poglavju naredimo oceno, kolikšen strošek predstavlja ekonomsko optimalna investicija v varnostni ukrep. Ta ocena je lahko koristna, v kolikor želimo dobiti cenovni okvir, oziroma za določen ukrep preveriti, kako blizu je optimalni investiciji.

Za oceno stroška optimalne investicije lahko uporabimo dve metodi. Pri prvi metodi iščem največjo neto koristi glede na investicijo, pri drugi metodi pa najnižje celotne stroške glede na investicijo.

5.4.5.1 Metoda največjih neto pridobitev

Pri tej metodi ocenimo, kdaj je neto pridobitev ukrepa (razlika med koristmi in stroški) največja. Pri tem iščemo vrednost investicije v varnostni ukrep *s**, ki je prikazana na sliki 30. Najprej opravimo izračun za **preventivni ukrep**. Če zapišemo razliko med koristmi in stroški, dobimo:

$$B(C_p) - C_p = \eta TvL \cdot (1 - v^{\alpha_p C_p}) - \delta + \mu - C_p \tag{106}$$

Za parametra δ in μ predpostavimo, da sta linearno odvisna od stroška varnostnega ukrepa C_P:

$$\delta = k_1 \cdot C_p \tag{107}$$

$$\mu = k_2 \cdot C_p \tag{108}$$

Ker iščemo največjo neto pridobitev, velja:

$$\frac{\partial(B(C_p) - C_p)}{\partial C_p} = 0 \tag{109}$$

$$\frac{\partial^2(B(C_p) - C_p)}{\partial {C_p}^2} < 0 \tag{110}$$

Zapišemo lahko:

$$\frac{\partial(B(C_p) - C_p)}{\partial C_p} = \frac{\partial(\eta TvL \cdot (1 - v^{\alpha_p C_p}) - (k_1 - k_2 + 1)C_p)}{\partial C_p} = 0 \tag{111}$$

$$-\alpha_p \eta TvL v^{\alpha_p {C_p}^*} \cdot \ln v - (k_1 - k_2 + 1) = 0 \tag{112}$$

$$v^{\alpha_p {C_p}^*} = -\frac{k_1 - k_2 + 1}{\alpha_p \eta TvL \cdot \ln v} \tag{113}$$

Pri tem je C_p* optimalna vrednost investicije. Ker daje izraz *ln(v)* negativno vrednost za vsak *v*, lahko izraz preuredimo tako, da ima vedno pozitivno vrednost:

$$\ln v < 0, \forall v \rightarrow -\ln v = \ln \frac{1}{v} > 0, \forall v \tag{114}$$

Enačbo (113) zapišemo:

$$v^{\alpha_p {C_p}^*} = \frac{k_1 - k_2 + 1}{\alpha_p \eta TvL \cdot \ln \frac{1}{v}} \tag{115}$$

Tako dobimo za C_p*:

$${C_p}^* = \frac{1}{\alpha_p} \log_v \left[\frac{k_1 - k_2 + 1}{\alpha_p \eta TvL \cdot \ln \frac{1}{v}} \right] \tag{116}$$

Preverimo, če je dobljeni rezultat zares maksimum:

$$\frac{\partial^2(B(C_p) - C_p)}{\partial {C_p}^2} = -{\alpha_p}^2 \eta TvL v^{\alpha_p C_p} \cdot \ln^2 v \tag{117}$$

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. Tudi tu predpostavljamo linearno odvisnost parametrov δ in μ od C_k kot je navedeno v (107) in (108). Koristi korektivnega varnostnega ukrepa zapišemo:

$$B(C_k) = \eta T v L_1 t_r^0 (1 - e^{-\alpha_k C_k}) - \delta + \mu \tag{118}$$

Za največjo neto pridobitev zapišemo:

$$\frac{\partial (B(C_k) - C_k)}{\partial C_k} = \frac{\partial (\eta T v L_1 t_r^0 (1 - e^{-\alpha_k C_k}) - (k_1 - k_2 + 1) C_k)}{\partial C_k} = 0 \tag{119}$$

$$\alpha_k \eta T v L_1 t_r^0 e^{-\alpha_k C_k^*} - (k_1 - k_2 + 1) = 0 \tag{120}$$

$$e^{-\alpha_k C_k^*} = \frac{k_1 - k_2 + 1}{\alpha_k \eta T v L_1 t_r^0} \tag{121}$$

$$C_k^* = \frac{1}{\alpha_k} \ln \left[\frac{\alpha_k \eta T v L_1 t_r^0}{k_1 - k_2 + 1} \right] \tag{122}$$

Tudi tu preverimo, ali je dobljeni rezultat zares maksimum:

$$\frac{\partial^2 (B(C_k) - C_k)}{\partial {C_k}^2} = -{\alpha_k}^2 \eta T v L e^{-\alpha_k C_k} < 0, \forall C_k \tag{123}$$

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

Za detekcijski varnostni ukrep lahko (122) priredimo v:

$$C_d^* = \frac{1}{\alpha_d} \ln \left[\frac{\alpha_d \eta T v L_2 t_d^0}{k_1 - k_2 + 1} \right] \tag{124}$$

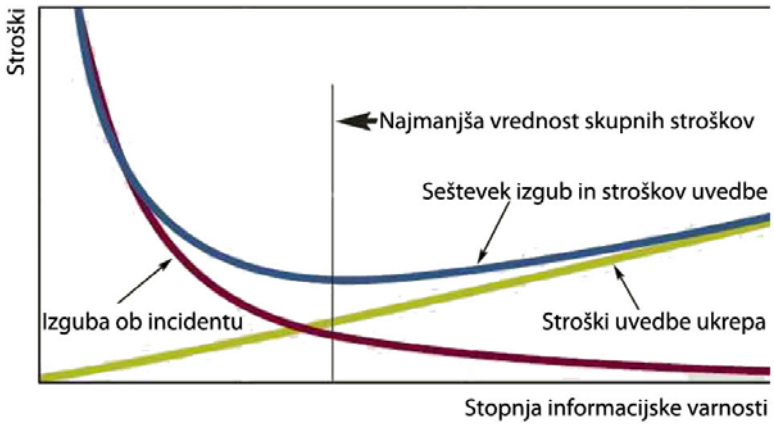
5.4.5.2 Metoda najmanjših stroškov

Pri metodi **najmanjših skupnih stroškov** predpostavimo, da so vsi skupni stroški C_T, ki jih ima podjetje zaradi varnostnega incidenta, vsota stroškov zaradi varnostnega incidenta R ter stroška varnostnega ukrepa C (slika 26 na strani 81). Pri tem upoštevamo kot strošek tudi δ in μ, za katera velja enačba (107) in (108).

$$C_T = R(C) + C + \delta - \mu \tag{125}$$

Zato iščemo pri katerem C ima funkcija C_T najmanjšo vrednost, kar je prikazano na sliki 42.

Slika 42: *Odvisnost stroškov od stopnje informacijske varnosti*



Ker iščemo najmanjšo vrednost stroškov, velja:

$$\frac{\partial C_T}{\partial C} = 0 \tag{126}$$

$$\frac{\partial^2 C_T}{\partial C^2} > 0 \tag{127}$$

Zapišemo enačbo (125) za **preventivni varnostni** ukrep:

$$C_T = \eta T v^{\alpha_p C_p + 1} \cdot L + C_p + \left(k_1 - k_2\right) C_p \tag{128}$$

Zapišemo lahko:

$$\frac{\partial C_T}{\partial C_p} = \frac{\partial (\eta T v^{\alpha_p C_p + 1} \cdot L + \left(1 + k_1 - k_2\right) \cdot C_p)}{\partial C_p} = 0 \tag{129}$$

$$\alpha_p \eta T L v^{\alpha_p C_p^*} \cdot \ln v + \left(1 + k_1 - k_2\right) = 0 \tag{130}$$

$$\alpha_p \eta T L v^{\alpha_p C_p^*} \cdot \ln v = -1 - k_1 + k_2 \tag{131}$$

$$v^{\alpha_p C_p^*} = \frac{-1 - k_1 + k_2}{\alpha_p \eta T L \cdot \ln v} = \frac{1 + k_1 - k_2}{\alpha_p \eta T L \cdot \ln \frac{1}{v}} \tag{132}$$

$$\alpha_p C_p^* = \log_v \left(\frac{1 + k_1 - k_2}{\alpha_p \eta T L \cdot \ln \frac{1}{v}} \right) \tag{133}$$

$$C_p^* = \frac{1}{\alpha_p} \log_v \left(\frac{1 + k_1 - k_2}{\alpha_p \eta T L \cdot \ln \frac{1}{v}} \right) \tag{134}$$

Enačba (134) daje enak rezultat kot (116). Preverimo, če je dobljeni rezultat zares minimum:

$$\frac{\partial^2 C_T}{\partial C_p^{\ 2}} = \alpha_p^{\ 2} \eta T L v^{\alpha_p C_p + 1} \cdot \ln^2 v \tag{135}$$

Zgornji rezultat daje pozitivno vrednost za vsak ukrep, zato je C_p* zares minimum.

Izračun optimalne investicije za **korektivni in detekcijski varnostni ukrep** je podoben kot za preventivni ukrep, pri čemer dobimo enake rezultate, kot pri metodi največjih neto pridobitev:

$$C_k^{\ *} = \frac{1}{\alpha_k} \ln\left[\frac{\alpha_k \eta T v L_1 t_r^0}{1 + k_1 - k_2}\right] \tag{136}$$

$$C_d^{\ *} = \frac{1}{\alpha_d} \ln\left[\frac{\alpha_d \eta T v L_2 t_d^0}{1 + k_1 - k_2}\right] \tag{137}$$

5.5 Scenariji kompleksnejših relacij med grožnjami, ranljivostmi in ukrepi

V preteklih poglavjih je bilo prikazano, da ena grožnja napada natanko eno ranljivost, varnostni ukrep pa zmanjšuje tveganje za eno samo grožnjo. V tem poglavju so prikazani štirje različni scenariji, ki vsebujejo kompleksnejše relacije med grožnjami, ranljivostmi in ukrepi.

- Scenarij 1: več groženj, kjer vsaka grožnja napada svojo ranljivost. Pred vsemi grožnjami se zaščitimo z enim varnostnim ukrepom.
- Scenarij 2: ena grožnja napada več ranljivosti. Pred grožnjo se zaščitimo z varnostnim ukrepom.
- Scenarij 3: na eno ranljivost je usmerjenih več groženj. Pred vsako grožnjo se zavarujemo s svojim varnostnim ukrepom.
- Scenarij 4: pred eno grožnjo, ki napada eno ranljivost, se zavarujemo z več varnostnimi ukrepi.

Pri vseh scenarijih izračunamo tveganje R_0 brez uvedbe ukrepa in tveganje R po uvedbi ukrepa. Za izračun ekonomsko optimalnega ukrepa zaradi enostavnosti uporabimo ROI, ker so zapisi rezultatov za NPV in IRR manj pregledni. V nadaljnjih izračunih se sklicujemo na naslednje enačbe: tveganje brez uvedenega varnostnega ukrepa (45), tveganje ob uvedenem varnostnem ukrepu (86) in ROI vrednotenje varnostnega ukrepa (91). Zato jih zapišemo ponovno:

$$R_0 = T \cdot v \cdot L \tag{138}$$

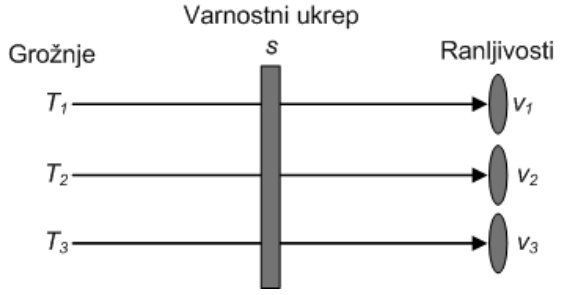
$$R = T \cdot v^{\alpha_p C_p + 1} \left[L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{139}$$

$$ROI = \frac{R_0 - R(C) - \delta + \mu - C}{C} \tag{140}$$

5.5.1 Scenarij 1: En varnostni ukrep varuje pred več različnimi grožnjami

Vsaka grožnja napada svojo ranljivost. Varnostni ukrep lahko varuje pred eno ali več grožnjami. Parametri, vezani na grožnje, ranljivosti in izgube, so specifični za vsako grožnjo oziroma ranljivost. Parametri, vezani na ukrep, veljajo za vse grožnje, z izjemo produktivnosti varnostnega ukrepa *α*, ki se določa za vsako grožnjo posebej, saj je vpliv varnostnega ukrepa na zmanjšanje posameznega tveganja lahko različen.

Slika 43: *Prikaz odvisnosti med grožnjami, ranljivostmi in ukrepi za scenarij 1*



V kolikor je *n* število vseh groženj oziroma ranljivosti, lahko tveganje brez uvedenega ukrepa zapišemo:

$$R_0 = \sum_{i=1}^{n} T_i \cdot v_i \cdot L_i \tag{141}$$

Za **preventivni ukrep** lahko tveganje zapišemo:

$$R = \sum_{i=1}^{n} T_i \cdot v_i^{\alpha_{pi} C_p + 1} \cdot L_i \tag{142}$$

Korist posameznega varnostnega ukrepa je tako:

$$B = \sum_{i=1}^{n} (T_i \cdot v_i \cdot L_i - T_i \cdot v_i^{\alpha_{pi} C_p + 1} \cdot L_i) - \delta + \mu \tag{143}$$

ROI za posamezen varnostni ukrep izračunamo:

$$ROI = \frac{\sum_{i=1}^{n}\left[T_i \cdot L_i \cdot v_i\left(1 - v_i^{\alpha_{pi}C_p}\right)\right] - \delta + \mu - C_p}{C_p} \tag{144}$$

V kolikor je izbran **korektivni ukrep**, lahko na podoben način zapišemo enačbe (142), (143) in (144):

$$R = \sum_{i=1}^{n} T_i \cdot v_i \cdot \left(L_{1i} \cdot t_{ri}{}^{0} e^{-\alpha_{ki}C_k} + L_{2i} \cdot t_d{}_i^{0} + L_{3i}\right) \tag{145}$$

$$B = \sum_{i=1}^{n}\left[T_i v_i\left(L_{1i} t_{ri}{}^{0} + L_{2i} t_d{}_i^{0} + L_{3i}\right) - T_i v_i\left(L_{1i} t_{ri}{}^{0} e^{-\alpha_{ki}C_k} + L_{2i} t_d{}_i^{0} + L_{3i}\right)\right] - \delta + \mu \tag{146}$$

$$B = \sum_{i=1}^{n} T_i \cdot v_i \cdot L_{1i} \cdot t_{ri}{}^{0}\left(1 - e^{-\alpha_{ki}C_k}\right) - \delta + \mu \tag{147}$$

$$ROI = \frac{\sum_{i=1}^{n}\left[T_i \cdot v_i \cdot L_{1i} \cdot t_{ri}{}^{0}\left(1 - e^{-\alpha_{ki}C_k}\right)\right] - \delta + \mu - C_k}{C_k} \tag{148}$$

V kolikor je izbran **detekcijski ukrep**, lahko podobno kot pri korektivnem ukrepu zapišemo:

$$R = \sum_{i=1}^{n} T_i \cdot v_i \cdot \left(L_{1i} \cdot t_{ri}{}^{0} + L_{2i} \cdot t_d{}^{0} e_i^{-\alpha_{di}C_d} + L_{3i}\right) \tag{149}$$

$$B = \sum_{i=1}^{n}\left[T_i v_i\left(L_{1i} t_{ri}{}^{0} + L_{2i} t_d{}_i^{0} + L_{3i}\right) - T_i v_i\left(L_{1i} t_{ri}{}^{0} + L_{2i} t_d{}^{0}{}_i e^{-\alpha_{di}C_d} + L_{3i}\right)\right] - \delta + \mu \tag{150}$$

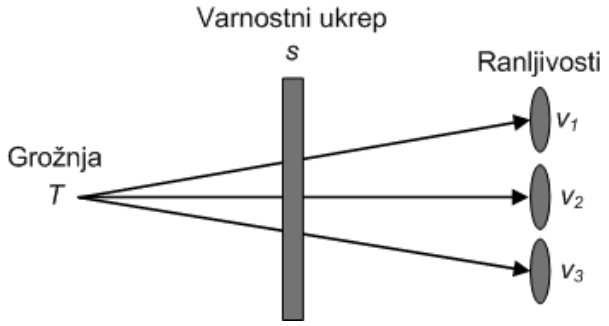
$$B = \sum_{i=1}^{n} T_i \cdot v_i \cdot L_{2i} \cdot t_{di}{}^{0}\left(1 - e^{-\alpha_{di}C_d}\right) - \delta + \mu \tag{151}$$

$$ROI = \frac{\sum_{i=1}^{n}\left[T_i \cdot v_i \cdot L_{2i} \cdot t_{di}{}^{0}\left(1 - e^{-\alpha_{di}C_d}\right)\right] - \delta + \mu - C_d}{C_d} \tag{152}$$

5.5.2 Scenarij 2: Ena grožnja je usmerjena na več ranljivosti

Parametri, vezani na ranljivosti in izgube, so specifični za vsako ranljivost. Parametri, vezani na grožnjo in ukrep, so enaki za vse ranljivosti.

Slika 44: *Prikaz odvisnosti med grožnjami, ranljivostmi in ukrepi za scenarij 2*



V kolikor je *m* število vseh ranljivosti, ki jih grožnja napada, lahko tveganje brez uvedenega ukrepa zapišemo:

$$R_0 = \sum_{i=1}^{m} T \cdot v_i \cdot L_i \tag{153}$$

V kolikor je izbran **preventivni ukrep**, lahko tveganje zapišemo:

$$R = \sum_{i=1}^{m} T \cdot v_i^{\alpha_{pi} C_p + 1} \cdot L_i \tag{154}$$

Zapišemo izračun pridobitev, ki bi nastale z uvedbo posameznega varnostnega ukrepa, in izračun ROI kazalca:

$$B = \sum_{i=1}^{m} (T \cdot v_i \cdot L_i - T \cdot v_i^{\alpha_{pi} C_p + 1} \cdot L_i) - \delta + \mu \tag{155}$$

$$ROI = \frac{T \cdot \sum_{i=1}^{m} \left[L_i \cdot v_i \left(1 - v_i^{\alpha_{pi} C_p} \right) \right] - \delta + \mu - C_p}{C_p} \tag{156}$$

V kolikor je izbran **korektivni ukrep**, lahko na podoben način zapišemo:

$$R = \sum_{i=1}^{m} T \cdot v_i \cdot \left(L_{1i} \cdot t_{ri}^{\,0} e^{-\alpha_{ki} C_k} + L_{2i} \cdot t_d^{\,0} + L_{3i} \right) \tag{157}$$

$$B = \sum_{i=1}^{m} T \cdot v_i \cdot L_{1i} \cdot t_{ri}^{\,0} \left(1 - e^{-\alpha_{ki} C_k} \right) - \delta + \mu \tag{158}$$

$$ROI = \frac{T \cdot \sum_{i=1}^{m} \left[v_i \cdot L_{1i} \cdot t_{ri}^{\,0} \left(1 - e^{-\alpha_{ki} C_k} \right) \right] - \delta + \mu - C_k}{C_k} \tag{159}$$

V kolikor je izbran **detekcijski ukrep**, lahko podobno kot pri korektivnem ukrepu zapišemo:

$$R = \sum_{i=1}^{m} T \cdot v_i \cdot \left(L_{1i} \cdot {t_{ri}}^0 + L_{2i} \cdot {t_d}^0 e_i^{-\alpha_{di} C_d} + L_{3i} \right) \tag{160}$$

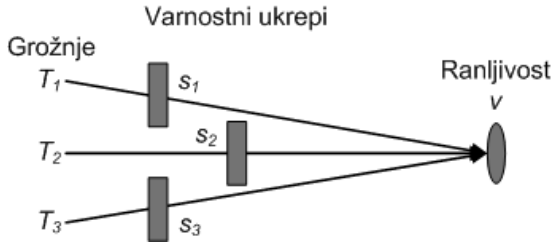
$$B = \sum_{i=1}^{m} T \cdot v_i \cdot L_{2i} \cdot {t_{di}}^0 \left(1 - e^{-\alpha_{di} C_d} \right) - \delta + \mu \tag{161}$$

$$ROI = \frac{T \cdot \sum_{i=1}^{m} \left[v_i \cdot L_{2i} \cdot {t_{di}}^0 \left(1 - e^{-\alpha_{di} C_d} \right) \right] - \delta + \mu - C_d}{C_d} \tag{162}$$

5.5.3 Scenarij 3: Na eno ranljivost usmerjenih več groženj, vsako grožnjo preprečuje svoj varnostni ukrep

Parametri, vezani na grožnje in ukrepe, so specifični za vsako grožnjo oziroma ukrep posebej. Parametri, vezani na ranljivost in izgubo, se ne spreminjajo.

Slika 45: *Prikaz odvisnosti med grožnjami, ranljivostmi in ukrepi za scenarij 3*



V kolikor je *p* število vseh groženj, ki ogrožajo ranljivost, lahko tveganje brez uvedenega ukrepa zapišemo:

$$R_0 = \sum_{i=1}^{p} T_i \cdot v \cdot L \tag{163}$$

V kolikor je izbran **preventivni ukrep**, lahko tveganje zapišemo:

$$R = \sum_{i=1}^{p} T_i \cdot v^{\alpha_{pi} C_{pi} + 1} \cdot L \tag{164}$$

Zapišemo izračun pridobitev, ki bi nastale z uvedbo posameznega varnostnega ukrepa, in izračun ROI kazalca:

$$B = \sum_{i=1}^{p} (T_i \cdot v \cdot L - T_i \cdot v^{\alpha_{pi} C_{pi} + 1} \cdot L) - \delta + \mu \tag{165}$$

$$B = v \cdot L \cdot \sum_{i=1}^{p} \left[T_i \cdot \left(1 - v^{\alpha_{pi} C_{pi}} \right) \right] - \delta + \mu \tag{166}$$

$$ROI = \frac{v \cdot L \cdot \sum_{i=1}^{p} \left[T_i \cdot \left(1 - v^{\alpha_{pi} C_{pi}} \right) \right] - \delta + \mu - C_p}{C_p} \tag{167}$$

V kolikor je izbran **korektivni ukrep**, lahko na podoben način zapišemo:

$$R = \sum_{i=1}^{p} \cdot T_i \cdot v \cdot \left(L_1 \cdot {t_r}^0 e^{-\alpha_{ki} C_{ki}} + L_2 \cdot {t_d}^0 + L_3 \right) \tag{168}$$

$$B = \sum_{i=1}^{p} T_i \cdot v \cdot L_1 \cdot {t_r}^0 \left(1 - e^{-\alpha_{ki} C_{ki}} \right) - \delta + \mu \tag{169}$$

$$ROI = \frac{v \cdot L_1 \cdot {t_r}^0 \cdot \sum_{i=1}^{p} \left[T_i \cdot \left(1 - e^{-\alpha_{ki} C_{ki}} \right) \right] - \delta + \mu - C_k}{C_k} \tag{170}$$

V kolikor je izbran **detekcijski ukrep**, lahko podobno kot pri korektivnem ukrepu zapišemo:

$$R = \sum_{i=1}^{p} T_i \cdot v \cdot \left(L_1 \cdot {t_r}^0 + L_2 \cdot {t_d}^0 e^{-\alpha_{di} C_{di}} + L_3 \right) \tag{171}$$

$$B = \sum_{i=1}^{p} T_i \cdot v \cdot L_2 \cdot {t_d}^0 \left(1 - e^{-\alpha_{di} C_{di}} \right) - \delta + \mu \tag{172}$$

$$ROI = \frac{v \cdot L_2 \cdot {t_d}^0 \cdot \sum_{i=1}^{p} \left[T_i \cdot \left(1 - e^{-\alpha_{di} C_{di}} \right) \right] - \delta + \mu - C_d}{C_d} \tag{173}$$

5.5.4 Scenarij 4: Eno grožnjo preprečuje več varnostnih ukrepov

Parametri, vezani na ukrepe, so specifični za vsak ukrep posebej. Parametri, vezani na grožnjo, ranljivost in izgubo, so enaki.

Slika 46: *Prikaz odvisnosti med grožnjami, ranljivostmi in ukrepi za scenarij 4*

Število vseh ukrepov, ki so uvedeni za zaščito ene grožnje, je *q*. Zapišemo tveganje brez uvedenega ukrepa:

$$R_0 = T \cdot v \cdot L \tag{174}$$

V kolikor je izbran **preventivni ukrep**, lahko tveganje zapišemo:

$$R = \sum_{i=1}^{q} T \cdot v^{\alpha_{pi} C_{pi} + 1} \cdot L \tag{175}$$

Zapišemo izračun pridobitev, ki bi nastale z uvedbo posameznega varnostnega ukrepa, in izračun ROI kazalca:

$$B = T \cdot v \cdot L - \sum_{i=1}^{q} (T \cdot v^{\alpha_{pi} C_{pi} + 1} \cdot L) - \delta + \mu \tag{176}$$

$$B = T \cdot v \cdot L \cdot \left[1 - \sum_{i=1}^{q} (v^{\alpha_{pi} C_{pi}}) \right] - \delta + \mu \tag{177}$$

$$ROI = \frac{T \cdot v \cdot L \cdot \left[1 - \sum_{i=1}^{q} (v^{\alpha_{pi} C_{pi}}) \right] - \delta + \mu - \sum_{i=1}^{q} C_{pi}}{\sum_{i=1}^{q} C_{pi}} \tag{178}$$

V kolikor je izbran **korektivni ukrep**, lahko na podoben način zapišemo:

$$R = \sum_{i=1}^{q} T \cdot v \cdot \left(L_1 \cdot {t_r}^0 e^{-\alpha_{ki} C_{ki}} + L_2 \cdot {t_d}^0 + L_3 \right) \tag{179}$$

$$B = T \cdot v \cdot L_1 \cdot {t_r}^0 \cdot \left[1 - \sum_{i=1}^{q} e^{-\alpha_{ki} C_{ki}} \right] - \delta + \mu \tag{180}$$

$$ROI = \frac{T \cdot v \cdot L_1 \cdot {t_r}^0 \cdot \left[1 - \sum_{i=1}^{q} e^{-\alpha_{ki} C_{ki}} \right] - \delta + \mu - \sum_{i=1}^{q} C_{ki}}{\sum_{i=1}^{q} C_{ki}} \tag{181}$$

V kolikor je izbran **detekcijski ukrep**, lahko podobno kot pri korektivnem ukrepu zapišemo:

$$R = \sum_{i=1}^{q} T \cdot v \cdot \left(L_1 \cdot {t_r}^0 + L_2 \cdot {t_d}^0 e^{-\alpha_{di} C_{di}} + L_3 \right) \tag{182}$$

$$B = T \cdot v \cdot L_2 \cdot t_d{}^0 \cdot \left[1 - \sum_{i=1}^{q} e^{-\alpha_{di} C_{di}} \right] - \delta + \mu \tag{183}$$

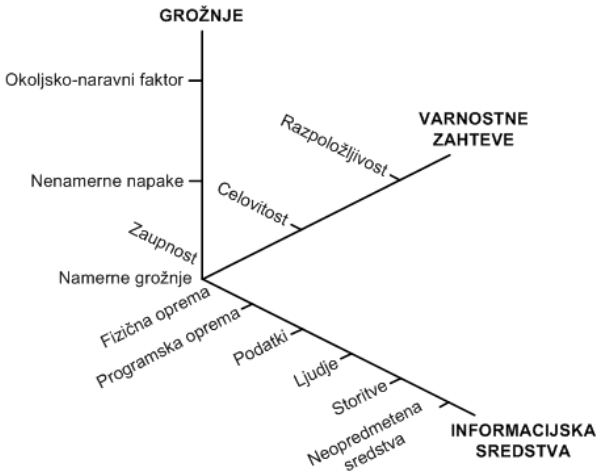
$$ROI = \frac{T \cdot v \cdot L_2 \cdot t_d{}^0 \cdot \left[1 - \sum_{i=1}^{q} e^{-\alpha_{di} C_{di}} \right] - \delta + \mu - \sum_{i=1}^{q} C_{di}}{\sum_{i=1}^{q} C_{di}} \tag{184}$$

5.6 Grafična klasifikacija tveganj in varnostnih ukrepov

V poglavju 5.5 je prikazanih nekaj primerov kompleksnejših relacij med grožnjami, ranljivostmi in ukrepi. Prikazane kompleksnejše relacije podajajo celovit pogled na varnostni sistem, po drugi strani pa lahko relacije med grožnjami, ranljivostmi in ukrepi hitro postanejo nepregledne. Za preglednejši prikaz varnostnega okolja uvedemo grafično klasifikacijo tveganj in varnostnih ukrepov.

Klasifikacijo prikažemo grafično, pri čemer osi na grafu predstavljajo informacijska sredstva, varnostne zahteve ter grožnje, kot je prikazano na sliki 47. Pri informacijskih sredstvih vzamemo kategorije, navedene v poglavju 3.1, ki so: fizična oprema, programska oprema, podatki, ljudje, storitve in neopredmetena sredstva. Varnostne zahteve ločimo na zaupnost, celovitost in razpoložljivost (poglavje 1.1). Grožnje ločimo na okoljsko-naravni faktor, namerne grožnje in nenamerne napake (poglavje 3.2.2).

Slika 47: *Model za grafično klasifikacijo tveganj in ukrepov.*



Klasifikacijski model je dimenzije 6×3×3, pri tem je potrebno upoštevati, da vse kombinacije na grafu niso smiselne. Vrednost tveganja na grafu predstavimo z

velikostjo točke. Ker je lahko tak prikaz velikosti vrednosti v nekaterih primerih manj pregleden, lahko v takih primerih poleg grafičnega načina klasifikacijo prikažemo tudi tabelarično in vrednost za posamezna polja navedemo v tabeli.

5.6.1 Klasifikacija tveganj

Na grafu se za posamezno tveganje prikaže, na katera informacijska sredstva je grožnja usmerjena, kaj zlorablja ter kakšne vrste je grožnja. Nekatere grožnje delujejo na manjšem področju, druge na širšem. Velikost točke na grafu simbolizira vrednost *R*. Na sliki 48 in v tabeli 9 je prikazana grafična in tabelarična klasifikacija za računalniški virus. V tabeli so vrednosti prikazane s stopnjami od 1 do 3 (pri čemer je 1 najmanjša stopnja in 3 največja), poleg vrednosti pa je v tabeli tudi navedena varnostna zahteva, ki je ogrožena (CIA). Na primer vrednost I3 pomeni, da je ogrožena celovitost z vrednostjo 3.

Slika 48: *Prikaz grafične klasifikacije za računalniški virus*

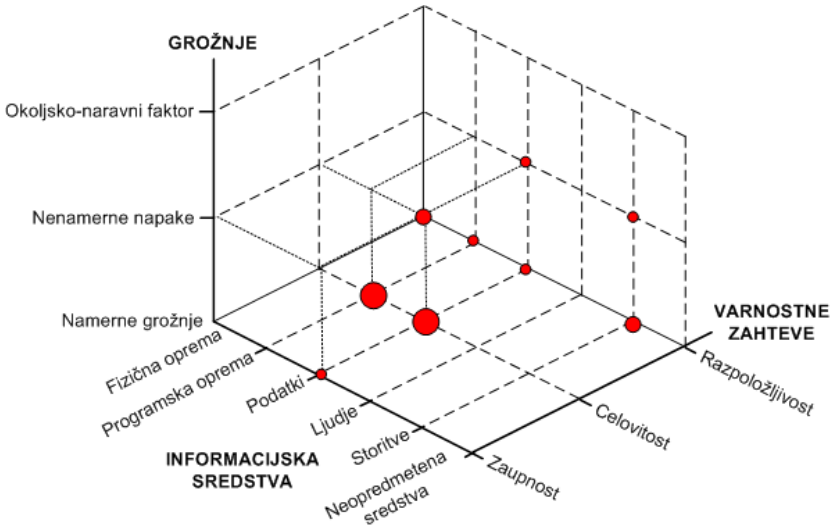
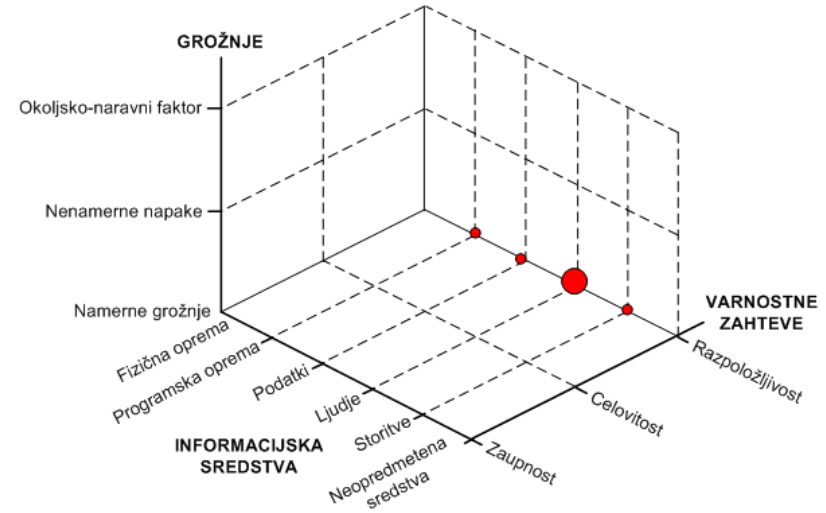


Tabela 9: *Prikaz tabelarične klasifikacije za računalniški virus.*

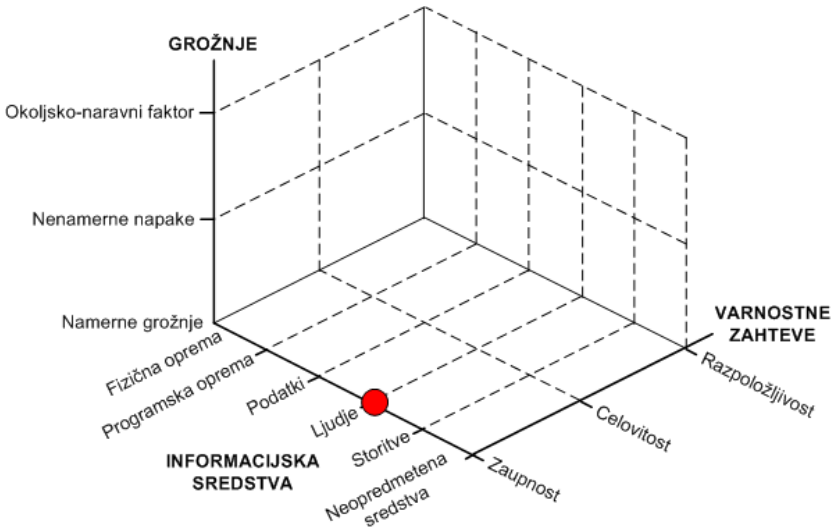
Grožnje \ Sredstva	Fizična oprema	Programska oprema	Podatki	Ljudje	Storitve	Neopredmetena sredstva
Okoljsko-naravni faktor						
Nenamerne napake			I2 A1		A1	
Namerne grožnje		I3 A1	C1 I3 A1		A2	

Na slikah 49, 50, 51 in 52 so prikazane grafične klasifikacije za naslednje grožnje: neželena pošta, "phishing", nepooblaščena sprememba spletne strani in odpoved delovanja storitev.

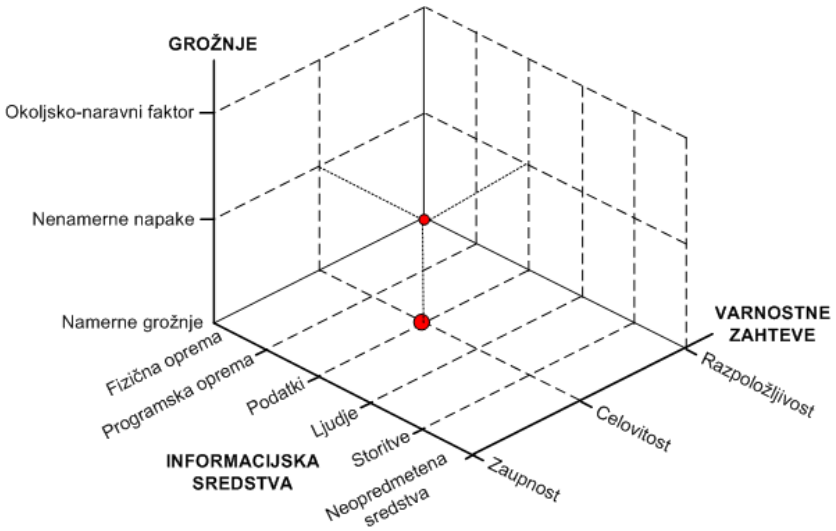
Slika 49: *Prikaz grafične klasifikacije za neželeno pošto*



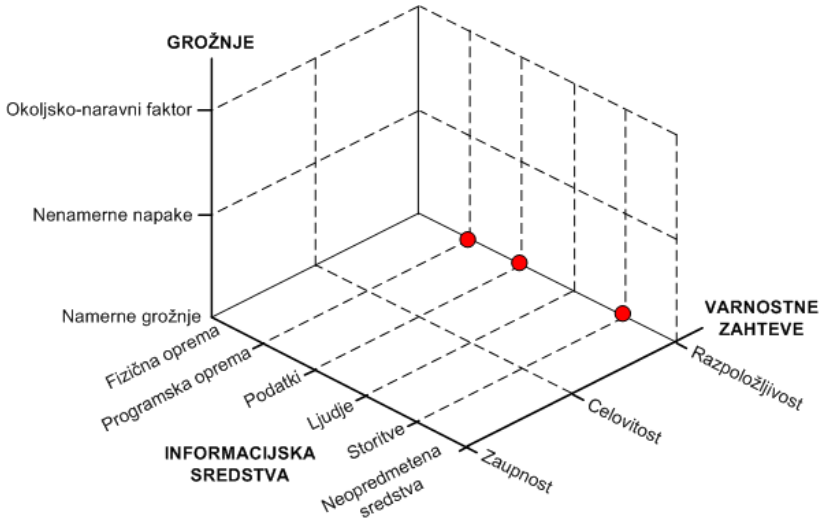
Slika 50: *Prikaz grafične klasifikacije za "phishing"*



Slika 51: *Prikaz grafične klasifikacije za nepooblaščeno spremembo vsebine spletne strani*



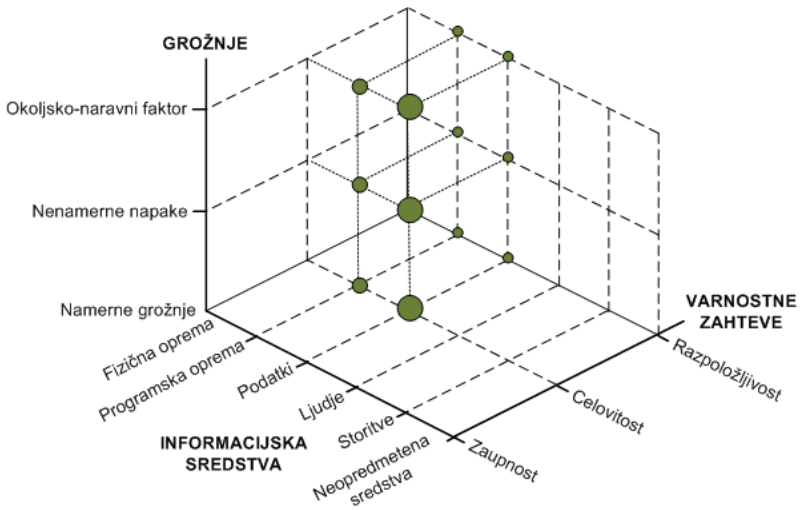
Slika 52: *Prikaz grafične klasifikacije za odpoved delovanja storitev*



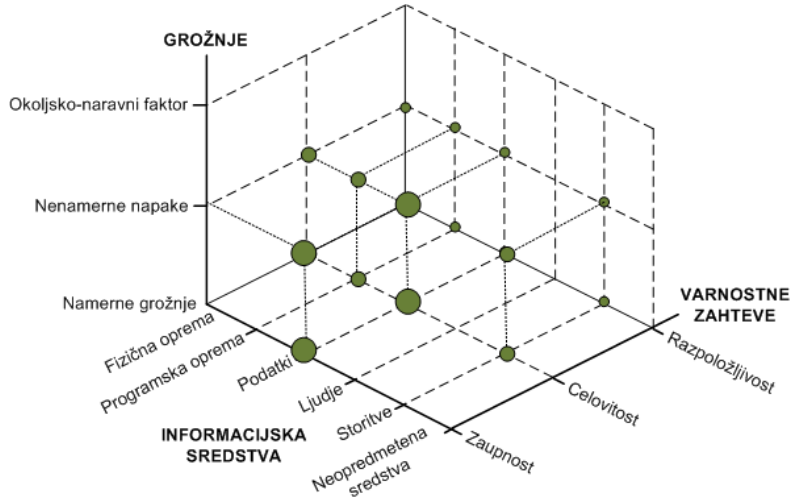
5.6.2 Klasifikacija varnostnih ukrepov

Na podoben način, kot smo prikazali klasifikacijo tveganj, lahko klasificiramo tudi varnostne ukrepe. Namen te klasifikacije je dobiti prikaz na obseg, ki ga posamezen varnostni ukrep zajema. Na slikah 53, 54, 55 in 56 so prikazane grafične klasifikacije za naslednje ukrepe: varnostno kopiranje podatkov, nadzor dostopa, alarmni sistem in požarni zid. Tak pristop med drugim omogoča grafično primerjavo tveganja brez uvedbe ukrepa in tveganja po uvedbi ukrepa (prikažemo koristi uvedbe ukrepa).

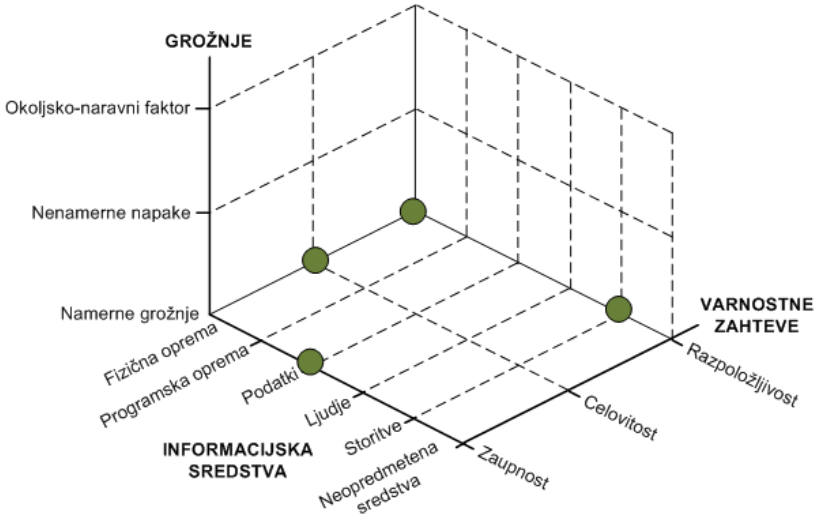
Slika 53: *Prikaz grafične klasifikacije za varnostno kopiranje podatkov*



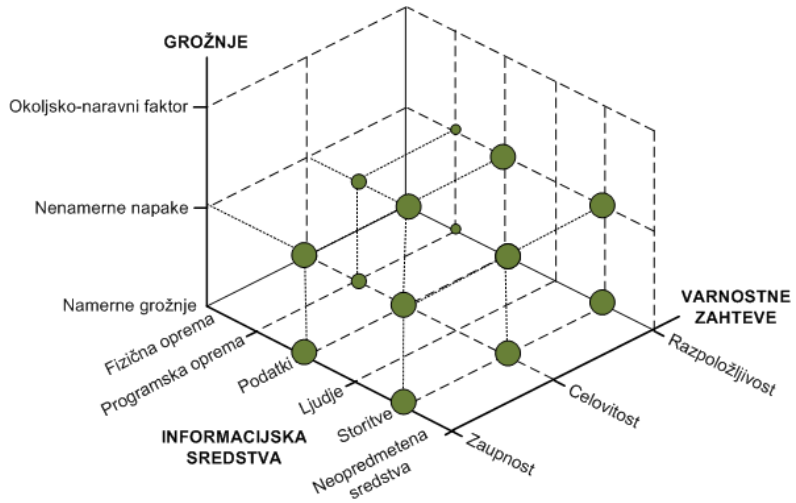
Slika 54: *Prikaz grafične klasifikacije za nadzor dostopa*



Slika 55: *Prikaz grafične klasifikacije za alarmni sistem*



Slika 56: *Prikaz grafične klasifikacije za požarni zid*

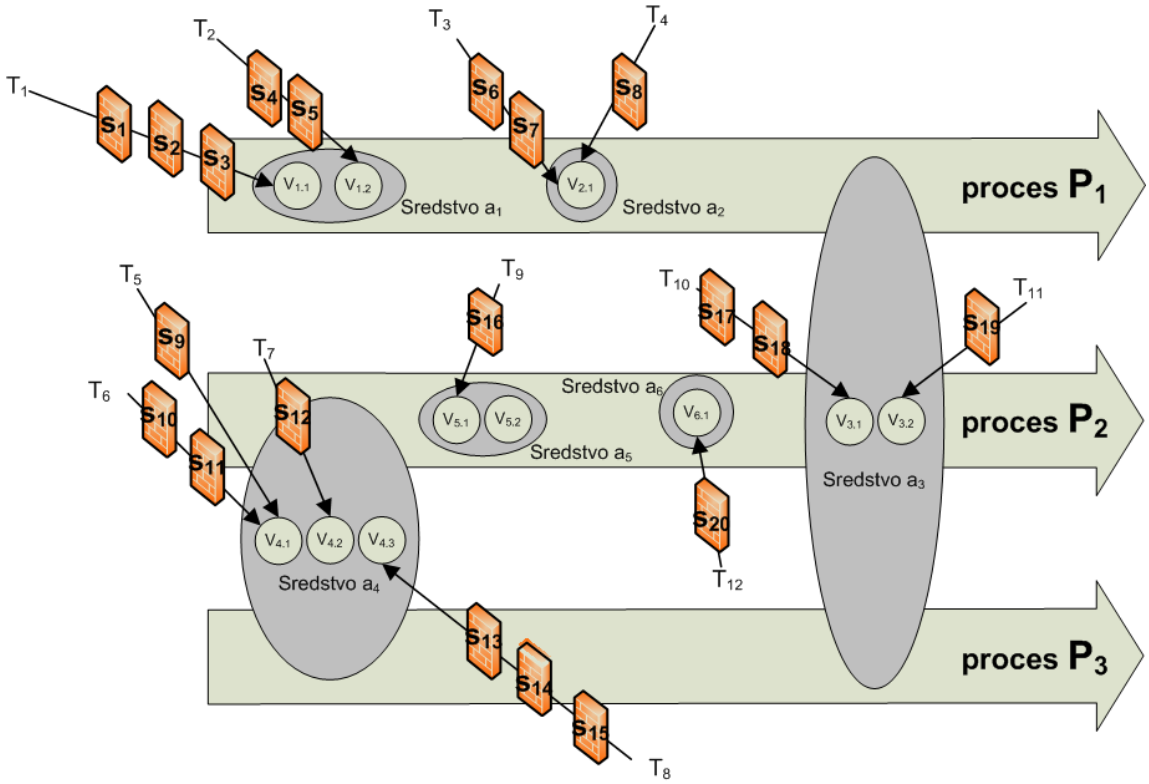


6 Matematična simulacija modela

6.1 Simulacijski model

Splošno veljavnost in vsestransko uporabnost modela preverimo z matematično simulacijo, pri kateri primerjamo teoretične rezultate ekonomskega vrednotenja varnostnih ukrepov s simulacijo poslovnega okolja. Cilj simulacije je potrditi skladnost teoretičnih izračunov modela z naključno simulacijo izbire varnostnih ukrepov in naključnim naborom varnostnih incidentov. Model simulacije zajema statično okolje, prikazano na sliki 57.

Slika 57: *Simulacijski model s procesi, sredstvi, ranljivostmi, grožnjami in varnostnimi ukrepi*



Model vključuje:

- procese *P*,
- sredstva *a,*
- ranljivosti *v.*

V vsakem procesu sodeluje več sredstev. Nekatera sredstva (a_3 in a_4) so vključena v več procesov. Sredstva imajo lahko eno ali več ranljivosti *v*, ki so na sliki 57 prikazane znotraj sredstva. Vrednosti za **ranljivosti** so prikazane v tabeli 10. Prva številka v indeksu ranljivosti označuje sredstvo, na katerega se ranljivost nanaša, druga številka v indeksu pa, za katero zaporedno ranljivost posameznega sredstva gre. Vrednosti so izbrane naključno.

Tabela 10: *Vrednosti ranljivosti v simulacijskem modelu*

Ranljivost	**Vrednost *v***
$V_{1.1}$	0,3
$V_{1.2}$	0,4
$V_{2.1}$	0,05
$V_{3.1}$	0,1
$V_{3.2}$	0,05
$V_{4.1}$	0,9
$V_{4.2}$	0,75
$V_{4.3}$	0,1
$V_{5.1}$	0,15
$V_{5.2}$	0,9
$V_{6.1}$	0,75

Poleg procesov, sredstev in ranljivosti, vsebuje model simulacije tudi:

- seznam možnih groženj *T,* z vsemi potrebnimi parametri,
- statične povezave med grožnjami in ranljivostmi,
- popis možnih izgub *L* za posamezno grožnjo,
- seznam možnih ukrepov *s* z vsemi potrebnimi parametri.

Grožnje *T* napadajo ranljivosti, pri tem lahko eno ranljivost napada več groženj. Zaščito pred grožnjami predstavljajo varnostni ukrepi *s*, pri čemer lahko sredstva pred posamezno grožnjo varuje več možnih ukrepov. V simulaciji predpostavimo, da podjetje pozna vse možne grožnje, ne ve pa, kateri in koliko napadov groženj bo izvedenih v določenem časovnem obdobju. Glede na vrednost ranljivosti ogroženega sredstva se lahko napad realizira v incident, ki za podjetje pomeni izgubo.

Verjetnosti za napad posamezne grožnje so prikazane v tabeli 11. Vrednosti so izbrane naključno.

Tabela 11: *Verjetnosti za napad posamezne grožnje v simulacijskem modelu*

Grožnja	Vrednost *T*
T_1	0,0071
T_2	0,0355
T_3	0,00137
T_4	0,1
T_5	0,025
T_6	0,95
T_7	0,5
T_8	0,0025
T_9	0,1
T_{10}	0,00137
T_{11}	0,00274
T_{12}	0,005

Podatki o **izgubah** v primeru enkratnega incidenta so prikazani v tabeli 12. Vrednosti so izbrane naključno.

Tabela 12: *Podatki o izgubah v primeru varnostnega incidenta za simulacijski model*

Incident povzroči grožnja	L_s	L_r	L_i	L_p	L_{SLA}	L_{pos}	t_r	t_d
T_1	0	23,53	6,62	35,29	0	0	8	2
T_2	0	30	100	250	0	1000	4	2
T_3	0	11,76	0	0	0	0	8	2
T_4	0	11,76	0	11,76	0	1000	16	0
T_5	0	47,06	331	58,8	0	0	6	1
T_6	0	11,76	0	470	0	0	0,000417	0,00375
T_7	0	8	20	300	0	0	0,0003	0,01
T_8	450	20	0	120	2500	0	5	10
T_9	0	50	450	60	0	0	10	5
T_{10}	0	15	0	10	0	0	40	4
T_{11}	0	15	700	100	0	0	8	4
T_{12}	8000	30	0	10	0	0	25	8

Karakteristike **možnih ukrepov** so prikazane v tabeli 13. Navedeni so stroški in ocena produktivnosti ukrepa, vrsta ukrepa (preventivni, korektivni ali detekcijski ukrep), negativni vpliv uvedenega ukrepa na poslovanje (parameter δ) ter posredni pozitivni učinek uvedbe ukrepa (parameter μ). V stolpcu "Vrsta ukrepa" pomeni črka p-preventivni ukrep, k-korektivni ukrep in d-detekcijski ukrep.

Tabela 13: *Podatki o karakteristikah možnih ukrepov za simulacijski model*

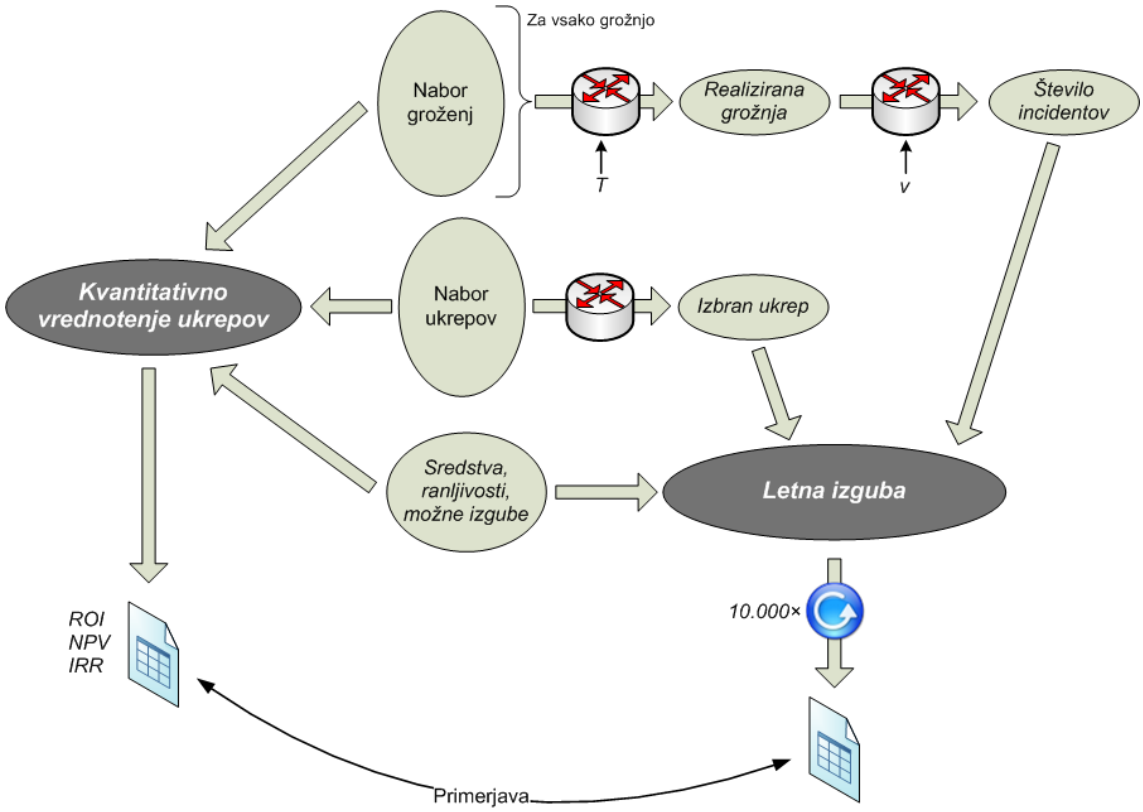
Varnostni ukrep	C_p	C_i	C_f	C_m	C_o	α	Vrsta ukrepa	δ	μ
s_1	1.000	424	0	59	0	0,00088	p	1.500	2.000
s_2	2.100	282	1.050	12	0	0,00015	p	2.000	0
s_3	6.400	565	2.600	24	0	0,00084	k	1.000	500
s_4	2.000	47	2.000	0	0	0,00065	p	0	0
s_5	4.100	329	3.050	12	0	0,0018	p	1.500	0
s_6	941	282	0	0	0	0,0409	p	0	0
s_7	2.000	471	500	24	0	0,00065	k	0	1.000
s_8	2.000	500	500	30	0	0,00065	k	0	0
s_9	2.000	300	1.000	140	0	0,00165	p	0	0
s_{10}	600	424	300	12	0	0,002567	p	0	0
s_{11}	900	376	500	12	0	0,001018	d	0	0
s_{12}	1.500	612	800	24	0	0,001119	k	0	0
s_{13}	600	400	300	15	0	0,0025	p	0	0
s_{14}	900	400	500	15	0	0,0011	p	0	0
s_{15}	1.500	600	800	150	0	0,0015	d	0	0
s_{16}	9.000	1.500	1.000	50	500	0,00011	p	0	0
s_{17}	2.000	47	500	12	0	0,00063	p	0	500
s_{18}	1.755	471	0	24	0	0,00179	d	0	0
s_{19}	2.000	471	500	24	0	0,005	k	0	0
s_{20}	6.500	2.000	2.000	30	0	0,00085	k	0	1.000

Na podlagi vhodnih podatkov o grožnjah, ranljivostih, izgubah in možnih ukrepih se s pomočjo teoretičnega modela izračunajo vrednosti ROI, NPV in IRR za posamezen varnostni ukrep.

6.2 Postopek simulacije

Simulacija se izvede s programom Microsoft Excel, pri čemer se uporabi VBA (Visual Basic for Applications). Postopek simulacije je prikazan na sliki 58. Ena ponovitev simulacije predstavlja časovno obdobje enega leta. Na začetku tega obdobja podjetje investira v en varnostni ukrep (lahko tudi ne investira in prihrani denar). Varnostni ukrep, v katerega podjetje investira, se v simulaciji izbere naključno izmed vnaprej določenega nabora možnih ukrepov (podatki o ukrepih so zbrani v tabeli 13). Pri tem se upošteva, da ima podjetje omejeno vsoto denarja ($IT_{sec\ budget}$), ki jo lahko nameni v investicijo varnostne rešitve. Naključna izbira varnostnega ukrepa je bistvenega pomena, ker na ta način primerjam rezultate teoretičnega izračuna s simulacijo naključnih dogodkov.

Slika 58: *Postopek izvedbe simulacije*



Sredstvom v podjetju pretijo grožnje (nabor možnih groženj je določen vnaprej, vrednosti so prikazane v tabeli 11), ki se v časovnem obdobju enega leta lahko udejanjijo enkrat, večkrat ali nikoli. Za vsako grožnjo simulacija določi število ponovitev izvedbe posamezne grožnje. Število ponovitev grožnje v časovnem obdobju je naključno, pri čemer se upošteva vrednost T. Za generiranje naključnih števil, kjer je generirana vrednost večja ali enaka a in manjša od b, uporabim Excel funkcijo RAND na naslednji način:

$$= RAND() \cdot (b - a) + a \tag{185}$$

Za vsako grožnjo se naključno generirano število primerja z vrednostjo *T*. Do napada pride, v kolikor je dobljeno naključno število manjše od *T*.

Za vsak napad se glede na podatek o ranljivosti (vrednosti so navedene v tabeli 10) naključno določi, ali se incident zgodi ali ne. V primeru izvedenega napada se postopek generiranja naključnega števila z enačbo (185) ponovi in dobljeno naključno število primerja z vrednostjo *v*. Incident se zgodi v primeru, da je naključno število manjše od *v*.

Pri generiranju naključnih števil je potrebno upoštevati problem generatorja naključnih števil. Schneier (1996) opozarja, da je dober generator naključnih števil zelo težko narediti. V starejših verzijah programa Microsoft Excel so bili znani določeni problemi pri statističnih izračunih, ki pa so bili odpravljeni v Excelu 2003 in novejših verzijah (Knüsel, 2005). Ocenjujem, da za potrebe te simulacije funkcija naključnega generiranja števil zadostuje, kar potrjujejo tudi rezultati simulacije.

Postopek naključnega generiranja števil po posameznih grožnjah, ki določa število napadov in incidentov, se ponovi 365-krat, kar predstavlja časovno obdobje enega leta. Seštevek dobljenih vrednosti za incidente predstavlja število incidentov po posameznih grožnjah v obdobju enega leta. V kolikor je pri posamezni ponovitvi simulacije izbran preventivni ukrep, je pri grožnji, na katero je vezan izbrani ukrep, število napadov manjše kot običajno, pri drugih grožnjah ostaja enako.

Na podlagi naključne investicije v ukrep in naključnega nabora incidentov v obdobju enega leta se izračunajo letne izgube. Število incidentov posamezne grožnje se pomnoži z izgubo, ki nastane zaradi incidenta. V kolikor je pri posamezni ponovitvi simulacije izbran korektiven ukrep, je pri grožnji, na katero je vezan izbrani ukrep, izguba manjša kot običajno, pri drugih grožnjah ostaja enaka.

Za obdobje enega leta se za izbran ukrep izračuna seštevek koristi in vseh izgub za vse grožnje. Ta podatek predstavlja, kolikšno letno izgubo ima podjetje ob izbiri izbranega ukrepa zaradi izvedenih napadov. Simulacija se večkrat ponovi. Glede števila ponovitev simulacije ocenim, da je ustrezno število ponovitev 10.000 ali več. Število vseh možnih kombinacij groženj in ukrepov je 252, kar pomeni, da se ob 10.000 ponovitvah, vsak ukrep za posamezno grožnjo v povprečju izbere 40-krat. Pri manjšem številu ponovitev bi lahko bili rezultati preveč razpršeni. To je potrdila tudi večkratna izvedba simulacije z le 1.000 ponovitvami, pri kateri so se rezultati simulacije precej razlikovali med posameznimi izvedbami simulacije.

Za vsak izbrani ukrep se pogleda povprečno skupno letno izgubo zaradi vseh incidentov. Skupne izgube so lahko velike, ker se v simulaciji uvede zgolj en ukrep, incidenti pa se zgodijo zaradi 12 možnih groženj. Ukrepi se razvrstijo glede na velikost skupnih izgub. Ukrep z najmanjšo izgubo je na vrhu, ukrep z največjo izgubo je na koncu. To razvrstitev se primerja z izračunanimi teoretičnimi vrednostmi ROI, NPV in IRR za posamezen ukrep. Pri razvrstitvah za ROI, NPV in IRR je ukrep z največjo vrednostjo ROI, NPV ali IRR najvišje, ukrep z najmanjšo

vrednostjo (možne so tudi negativne vrednosti) ROI, NPV ali IRR pa na koncu. V kolikor razvrstitev ukrepov pri izračunu naključnih dogodkov sovpada z razvrstitvijo ukrepov pri teoretičnem izračunu modela, lahko privzamemo, da teoretični model podaja pravilne rezultate. Ujemanje pomeni, da ima ukrep, ki je imel v simulaciji najmanjšo izgubo, tudi pri teoretičnem izračunu največjo vrednost ROI, NPV in IRR. Pri tem se je potrebno zavedati, da ne gre za primerjavo popolnoma identičnih podatkov. Izračuni ROI, NPV in IRR vrednotijo, kako je posamezen ukrep ekonomsko učinkovit, s simulacijskim izračunom pa se dobi podatek, kolikšno skupno izgubo ima podjetje, če izbere natanko en ukrep. Ne glede na to omejitev, lahko privzamemo, da podobna razvrstitev vrstnega reda ukrepov potrjuje pravilnost teoretičnega modela.

6.3 Rezultati simulacije

Za vsak ukrep se izračunajo vrednosti ROI, NPV in IRR. Pri tem izračunu je za diskontno stopnjo upoštevana letna obrestna mera 0,05 in investicijsko obdobje petih let. Simulacijo ponovimo 10.000-krat. Dobljeni rezultati izračuna povprečnih skupnih stroškov, ROI, NPV in IRR za vsak ukrep, so prikazani v tabeli 14.

Drugi stolpec "Seštevek vseh stroškov ukrepa" sešteje stroške uvedbe posameznega ukrepa in izgube ob vseh ponovitvah incidentov, ki so nastali, ko je bil v 10.000 ponovitvah simulacije izbran posamezen ukrep. Tretji stolpec "Število ponovitev ukrepa" pove, kolikokrat je bil v 10.000 ponovitvah simulacije izbran posamezen ukrep. Četrti stolpec "Povprečni stroški za izbran ukrep" predstavlja povprečne stroške (seštevek stroška uvedbe ukrepa in vseh izgub zaradi incidentov), ki v obdobju enega leta nastanejo ob izbiri posameznega ukrepa. Visoke vrednosti tega stolpca v tabeli so posledica vrednosti parametrov T in v, ki so namenoma izbrani tako, da je število možnih ponovitev groženj in incidentov v obdobju enega leta dokaj veliko. Redki dogodki v izbranem simulacijskem modelu ne dajejo dobrih rezultatov. Pomemben podatek predstavlja vrednost tega stolpca za podatek "ni investicije". Ta podaja povprečne stroške, ki nastanejo v obdobju enega leta, če podjetje ne investira v varnostni ukrep. Groba ocena je, da simulacija predlaga uvedbo tistih ukrepov, ki imajo povprečne stroške manjše od vrednosti povprečnih stroškov za "ni investicije".

Tabela 14: *Rezultati simulacije za posamezen ukrep*

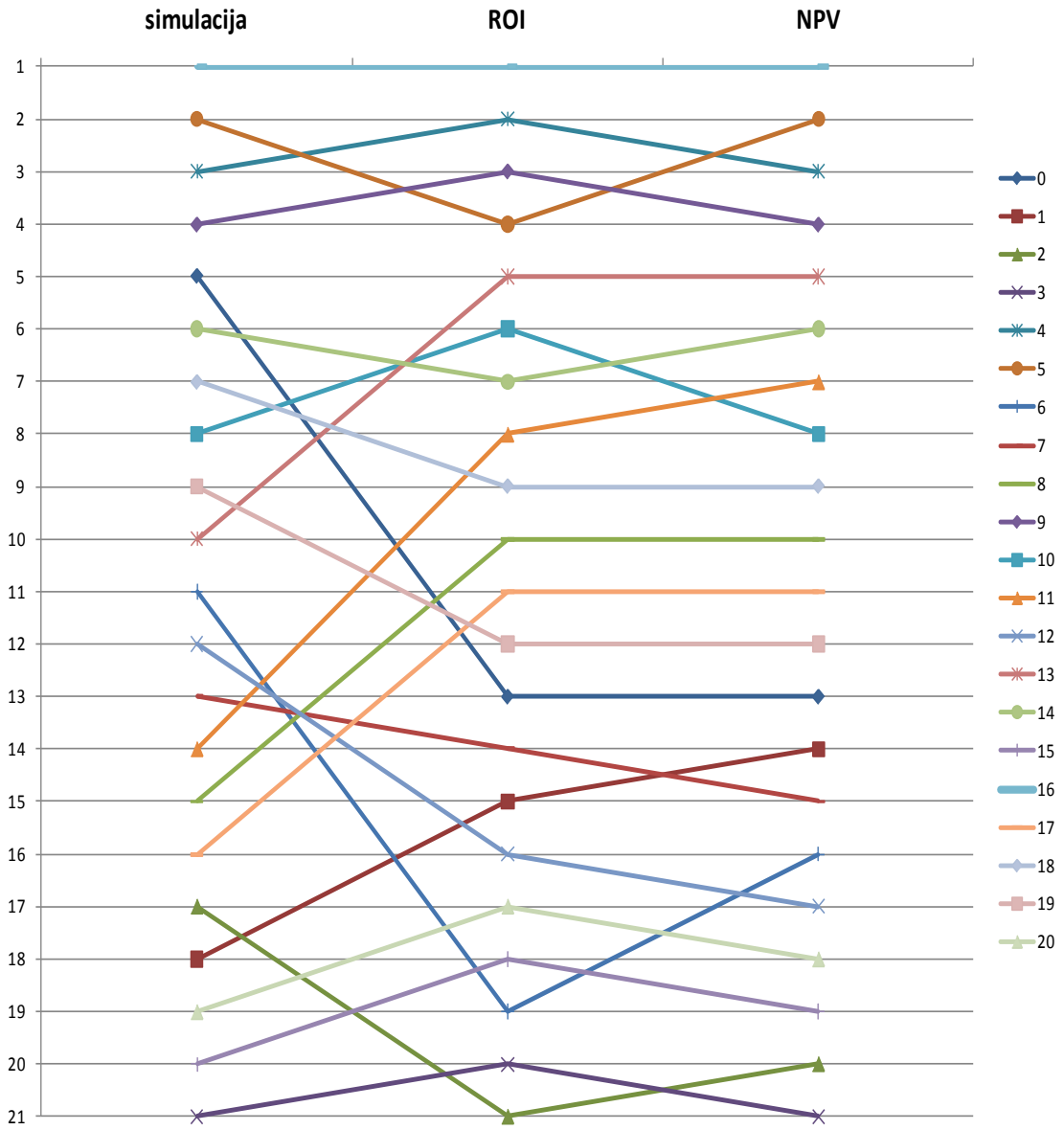
Varnostni ukrep	Seštevek vseh stroškov ukrepa (v 10.000 ponovitvah)	Število ponovitev ukrepa (skupno 10.000 ponovitev)	Povprečni stroški za izbran ukrep	ROI	NPV	IRR
ni investicije	48.265.724	476	101.399			
s_1	52.325.087	495	105.707	-19 %	-994,3	-27 %
s_2	50.136.429	478	104.888	-229 %	-14678,0	
s_3	50.179.150	464	108.145	-103 %	-17443,3	
s_4	44.796.680	483	92.747	533 %	46249,6	607 %
s_5	41.829.621	462	90.540	337 %	50322,6	323 %
s_6	49.428.926	474	104.280	-99 %	-1212,8	
s_7	49.360.243	473	104.356	-15 %	-1071,2	-16 %
s_8	51.152.877	488	104.821	11 %	327,3	10 %
s_9	46.397.511	469	98.929	349 %	38102,5	418 %
s_{10}	48.058.979	463	103.799	87 %	2095,8	72 %
s_{11}	51.325.941	490	104.747	66 %	2169,4	65 %
s_{12}	48.927.071	469	104.322	-25 %	-1683,5	
s_{13}	49.158.457	472	104.149	131 %	3414,9	109 %
s_{14}	49.128.240	482	101.926	67 %	2300,5	67 %
s_{15}	52.234.412	492	106.168	-61 %	-7796,3	
s_{16}	41.607.505	495	84.056	536 %	91462,2	228 %
s_{17}	47.712.162	455	104.862	9 %	146,8	8 %
s_{18}	49.783.600	486	102.435	37 %	862,9	18 %
s_{19}	47.361.454	456	103.863	6 %	20,5	5 %
s_{20}	50.646.526	478	105.955	-30 %	-5186,7	-31 %

Ustreznost teoretičnega modela se preveri s primerjavo vrstnega reda optimalnih ukrepov simulacije in vrstnega reda ukrepov po izračunih ROI, NPV in IRR. Vrstni red ukrepov pri simulaciji sledi rezultatom povprečnih stroškov za posamezen ukrep, pri čemer velja za najbolj optimalen ukrep tisti z najnižjo vrednostjo povprečnega stroška. Rezultati za ROI, NPV in IRR so razvrščeni glede na vrednosti za posamezen ukrep, pri čemer velja za najbolj optimalen ukrep tisti z največjo vrednostjo ROI, NPV ali IRR. Primerjava razvrstitve ukrepov je v tabeli 15 in na sliki 59. Na sliki predstavljajo številke v legendi identifikacijo posameznih ukrepov. Ukrep z oznako 0 pomeni, da ni investicije v ukrep. V primeru, ko ni investicije v ukrep, se za vrednosti ROI, NPV in IRR privzame 0 oziroma 0 %.

Tabela 15: *Primerjava razvrstitve posameznih ukrepov med simulacijo in izračuni ROI, NPV in IRR*

vrstni red (najbolj optimalen ukrep)	Simulacija	ROI	NPV	IRR
1	16	16	16	4
2	5	4	5	9
3	4	9	4	5
4	9	5	9	16
5	0	13	13	13
6	14	10	14	10
7	18	14	11	14
8	10	11	10	11
9	19	18	18	18
10	13	8	8	8
11	6	17	17	17
12	12	19	19	19
13	7	0	0	0
14	11	7	1	7
15	8	1	7	1
16	17	12	6	20
17	2	20	12	
18	1	15	20	
19	20	6	15	
20	15	3	2	
21	3	2	3	

Slika 59: *Grafična primerjava razvrstitve posameznih ukrepov med simulacijo in izračunoma ROI in NPV*



Iz primerjave razvrstitve je razvidno, da se vrstni red ukrepov v simulaciji in teoretičnem izračunu ROI, NPV in IRR precej dobro ujema. Prisotne so sicer nekatere razlike, vendar so razlike prisotne že med samimi izračuni ROI, NPV in IRR. Iz prikazanega lahko zaključimo, da matematična simulacija potrjuje pravilnost in ustreznost teoretičnega modela.

7 Empirična analiza modela

Skozi empirično analizo predstavljen matematični model za oceno optimalne investicije v informacijsko varnost praktično preizkusimo v realnem okolju. Cilj empirične analize je potrditev ustreznosti matematičnega modela za praktično uporabo v poslovnem okolju. Empirična analiza je opravljena v sodelovanju s srednje velikim slovenskim podjetjem, ki deluje na področju informacijske tehnologije. Zajeti podatki so pridobljeni iz različnih virov v podjetju (javni podatki o podjetju, interni podatki, seznam informacijskih sredstev, ocena tveganja idr). V izračunih empirične analize so uporabljeni tudi občutljivi podatki podjetja, ki so klasificirani kot interno ali zaupno. Podatki s tovrstno oznako v disertaciji niso objavljeni, oziroma so delno prikriti ali prilagojeni, da ne razkrijejo identitete podjetja. Podatki podjetja, ki so uporabljeni v empirični analizi, so bili večinoma zajeti jeseni 2009.

V empirični analizi sta obravnavana računalniški virus in ohromitev informacijskih storitev. Ti grožnji sta dovolj splošni, da sta lahko aktualni v vsakem poslovnem okolju. Pri analizi groženj so uporabljeni sledeči podatki podjetja:

- Letni prihodek podjetja znaša 3.000.000 €. Če privzamem, da storitve podjetja delujejo v režimu 24×7×365, je povprečni prihodek 342,47 € na uro (i = 342,47 €/uro).
- V podjetju je zaposlenih 40 ljudi.
- Povprečna bruto plača sistemskega administratorja je 2.000 €/mesec. Mesečno opravi zaposleni v povprečju 173 delovnih ur[10], zato znaša bruto plača 11,56 € na uro (p = 11,56 €/uro).
- Za diskontno stopnjo, v izračunih NPV in IRR, je bila poenostavljeno vzeta letna obrestna mera, po kateri podjetje lahko dobi posojilo za financiranje investicije (k = 2,7 %[11]).

[10] Od 365 dni v letu jih je 260 v delovnem tednu. To pomeni mesečno 21,7 delovnih dni ali ob 8 urnem delovniku 173 delovnih ur. Prazniki in dopusti izračuna ne spremenijo, ker so plačani.

Podjetje se pri analizi tveganja ni odločilo za ločevanje podatkov na elemente zaupnosti, celovitosti in razpoložljivosti (CIA). Za vse grožnje velja sledeča ocena parametrov za obravnavo tveganja, ki so predstavljeni v poglavju 5.3.1:

- Največje tveganje je ocenjeno na trimesečni prihodek podjetja. Letni prihodek je 3.000.000 €, trimesečni je tako 750.000 € (R_{max} = 750.000 €/leto).
- Največja izguba je ocenjena na letni prihodek podjetja, ki znaša 3.000.000 € (L_{max}).
- Tveganja, ki so na letni ravni manjša od dveh delovnih ur, so ocenjena za sprejemljiva in se upošteva, da je uvedba varnostnega ukrepa v tem primeru dražja (najmanjše tveganje R_{min} = 2 × 11,56 € ≈ 23,12 €/leto).

Podjetje ima definirane ključne procese, ki so pomembni pri opravljanju njihove dejavnosti. V tabeli 16 so prikazani ključni procesi in želena stopnja varnosti za vsak proces (nekateri procesi so zaradi zahteve po zaupnosti preimenovani). Želena stopnja varnosti je tronivojska, pri čemer so v tabeli prikazane vrednosti: v-visoka, s-srednja in n-nizka.

Tabela 16: *Prikaz ključnih poslovnih procesov in želene stopnje varnosti za vsak proces*

Poslovni proces	Želena stopnja varnosti
Razvoj projektov po naročilu	v
Razvoj internih projektov	s
Izvajanje storitev za zunanje stranke	v
Skrbništvo projektov po naročilu	v
Skrbništvo projektov za neznanega kupca	v
Podporni proces prodaja	s
Podporni proces nabava	n
Podporni proces zagotavljanje delovanja infrastrukture	v

V analizi tveganja so bila uporabljena informacijska sredstva, ki so po kategorijah, prikazana v tabeli 17. Zaradi zaupnosti niso prikazane posamezne podkategorije in sredstva. Pri vsaki kategoriji so navedene tudi varnostne zahteve, ki so podrobneje določene na nivoju podkategorij.

[11] Trimesečni EURIBOR + 2,00 odstotnih točk (NLB). Vrednost trimesečni EURIBOR na dan 31.12.2009 je 0,7.

Tabela 17: *Prikaz kategorij informacijskih sredstev in želene stopnje varnosti za njihove podkategorije*

Informacijsko sredstvo	želena stopnja varnosti
Fizična oprema	
Mrežna in telekomunikacijska oprema	v, s, n
Strežniška računalniška oprema	v, s, n
Delovne postaje	n
Prenosni računalniki	n
Monitorji	n
Periferna računalniška oprema	n
Nosilci zapisa	s, n
Infrastrukturna oprema	v, s, n
Pohištvena oprema	v, n
Razna oprema	n
Prostori	v, s, n
Programska oprema	
Aplikacijska programska oprema	v, s, n
Sistemska programska oprema	v, s, n
Razvojna orodja	n
Podatki in informacije	
Javni podatki	s, n
Interni podatki	v, s, n
Zaupni podatki	v, s, n
Strogo zaupni podatki	v
Storitve	
Infrastrukturne storitve	v, n
Interne IT storitve	v, s, n
Storitve za zunanje stranke	v
Izobraževanja	n
Človeški viri	
Interno osebje	v
Zunanji izvajalci, dobavitelji, ponudniki	v
Neotipljiva sredstva	s

7.1 Analiza modela za tveganje okužbe z računalniškim virusom

Pri tveganju okužbe z računalniškim virusom se pojem virus razume v širšem pomenu, tako da pod tem izrazom upoštevam tudi črve in trojanske konje. Podjetju se v kratkem izteče naročnina za protivirusni program, ki ga trenutno uporabljajo za zaščito delovnih postaj in strežnikov. Želijo preveriti, ali naj obdržijo sedanji protivirusni program in podaljšajo naročnino, ali pa se odločijo za katero drugo rešitev.

Vsi zaposleni pri delu dnevno uporabljajo računalniško opremo, zato okužba z virusom lahko vpliva na vse poslovne procese. Računalniški virus ogroža naslednja sredstva, ki so prikazana po kategorijah v tabeli 18.

Tabela 18: *Prikaz informacijskih sredstev, ki jih lahko ogroža računalniški virus*

Informacijsko sredstvo	Želena stopnja varnosti
Programska oprema	
Aplikacijska programska oprema	v, s, n
Sistemska programska oprema	v, s, n
Podatki in informacije	
Javni podatki	s, n
Interni podatki	v, s, n
Zaupni podatki	v, s, n
Strogo zaupni podatki	v
Storitve	
Infrastrukturne storitve	v, n
Interne IT storitve	v, s, n
Storitve za zunanje stranke	v

7.1.1 Ocena tveganja

Uporabniki se lahko z računalniškim virusom okužijo na različne načine, lahko pri prenosu okuženih datotek preko interneta, pri ogledu internetnih strani z zlonamerno kodo, pri sprejemu e-pošte z okuženo datoteko in preko programov za takojšnje sporočanje (angl. *instant messaging*). Večinoma se virusi aktivirajo tako, da uporabnik zažene ali odpre okuženo datoteko, v nekaterih primerih pa za okužbo zadostuje zgolj prikaz spletne vsebine, ki vsebuje zlonamerno kodo. Ker podjetje želi preučiti tako obstoječo zaščito kot tudi nove zaščite, privzamemo

stanje, da trenutno ni uvedena nobena zaščita pred tveganjem okužbe z računalniškim virusom in kot en možen ukrep vzamemo sedanjo rešitev.

Ranljivost je verjetnost, da bo računalniški virus okužil sredstvo, na katerega je usmerjen. Ker ocenjujemo stanje, kjer ni nobene tehnične zaščite zoper grožnje, je ranljivost enaka ozaveščenosti zaposlenih, da v primeru, ko dobijo virus le-tega ne aktivirajo. Podjetje ocenjuje, da bi glede na trenutno ozaveščenost in v okolju brez protivirusne zaščite, virus preko okužene datoteke aktivirala dve tretjini zaposlenih:

- $v = 0{,}66$

Ocena pogostosti prejema okuženih datotek ali drugega načina okužbe je ocenjena na enkrat na teden:

- $T = 1/7$ dni $= 0{,}143$ /dan

Verjetnost za incident v enačbi (23) je:

- $\rho = T \cdot v = 0{,}143 \cdot 0{,}66 = 0{,}0952 / dan$

Ocenimo izgube v primeru varnostnega incidenta. Zaradi okužbe z virusom ni potrebno zamenjati opreme, zato stroška zamenjave ni:

- $L_s = 0$

Čas odprave posledic incidenta je ocenjen na en delovnik (t_r = 8 ur), pri tem delo odpravljata dva sistemska administratorja (n = 2). Odprava posledic vsebuje čiščenje virusne okužbe na nivoju programske opreme ter morebitna povrnitev okuženih dokumentov iz varnostnih kopij. Strošek popravila v enačbi (31) zaradi okužbe z virusom je:

- $L_r{}^0(t)$ = 23,12 €/uro, $t_r{}^0$ = 8 ur

Čas nedelovanja je ocenjen na 10 ur, okužba se ugotovi in posreduje odgovornim osebam v dveh urah (t_{NA} = 10 ur, t_d = 2 uri). Ocenjeno je, da okužba z virusom bistveno ne vpliva na prihodek podjetja (EF_I = 0,02). Izguba prihodkov podjetja v enačbi (32) zaradi okužbe z virusom je:

- $L_i{}^0(t)$ = 0,02 × 342 €/uro = 6,85 €/uro, $t_{NA}{}^0$ = 10 ur, $t_d{}^0$ = 2 uri

Vpliv incidenta na produktivnost pri okuženih uporabnikih je ocenjen na četrtino časa nedelovanja (EF_P = 0,25). V primeru enega incidenta je ocenjeno, da bi se okužila desetina zaposlenih (m = 4). Izguba produktivnosti zaposlenih v enačbi (33) zaradi okužbe z virusom je:

- $L_p{}^0(t)$ = 11,56 €/uro, $t_{NA}{}^0$ = 10 ur, $t_d{}^0$ = 2 uri

Zaradi okužbe z virusom ni izgub zaradi nespoštovanja SLA:

- $L_{SLA} = 0$

Zaradi okužbe z virusom so posredne izgube zanemarljive:

- $L_{posredne} = 0$

Ob upoštevanju enačb (40), (41), (42) in (43) dobimo:

- L_1 = 41,53 €/uro
- L_2 = 18,41 €/uro
- $L_3 = 0$
- L = 369,07 €

Varnostno tveganje v enačbi (45) ocenimo na:

- $R = \rho \cdot L = 0,0952 / dan \cdot 369,07€ = 35,15€ / dan$

Vrednost tveganja je takšna, da je ustrezna obravnava zmanjšanje tveganja z investicijo v varnostni ukrep.

7.1.2 Vrednotenje možnih ukrepov za zmanjšanje tveganja

Za reševanje tveganja okužbe z računalniškim virusom se izberejo naslednji možni ukrepi:

- Ukrep A: Osnovna protivirusna zaščita za delovne postaje, ki ne zahteva letnega podaljševanja naročnine za virusne definicije. Podjetje potrebuje licence za 40 delovnih postaj.
- Ukrep B: Protivirusna zaščita za delovne postaje in strežnike s centralnim posodabljanjem in analizo, kjer je potrebno letno podaljševanje naročnine za virusne definicije. Podjetje potrebuje licence za 40 delovnih postaj. To rešitev podjetje uporablja že sedaj.
- Ukrep C: Protivirusna zaščita, ki pregleduje promet na požarnem zidu, SMTP posredniku in delovnih postajah (poleg virusov pregleduje tudi za neželeno pošto). Omogoča centralno posodabljanje, potrebno je letno podaljševanje naročnine za virusne definicije.
- Ukrep D: Vsakoletno izobraževanje uporabnikov preko spletnih izobraževanj.
- Ukrep E: Izdelava varnostnih kopij sistemov, kar zmanjšuje čas okrevanja okuženih sistemov. V nasprotju z ostalimi ukrepi, ki so preventivni, je ta ukrep korektiven, ker blaži posledice v primeru incidenta.
- Ukrep F: kombinacija izobraževanja in protivirusne zaščite (ukrepa B in D).

Ocena karakteristik stroškov izbranih ukrepov v enačbi (49) je prikazana v tabeli 19. V izračunu je časovno obdobje za investicijo 4 leta.

Tabela 19: *Ocena stroškov varnostnih ukrepov za zmanjšanje tveganja virusov*

Ukrep	Strošek nabave opreme C_p	Strošek uvedbe, testiranja, izobraževanja C_i	Strošek nadgradenj in popravkov C_f	Strošek vzdrževanja C_m	Ostali stroški C_o
A	nakup opreme za 40 računalnikov: 1.350 €	namestitev: 30 min/računalnik = 20 ur predhodno testiranje: 16 ur (skupaj 36 ur = 416 €)	0	mesečno 5 ur (letno 60 ur = 693 €)	0
B	nakup opreme za 40 računalnikov: 1.204 €	namestitev: 16 ur, testiranje: 8 ur (skupaj 24 ur = 277 €)	letna naročnina za protivirusne definicije: 835 €	mesečno 1 ura (12 ur letno = 138 €)	0
C	nakup požarnega zidu in opreme za 40 delovnih postaj: 5.930 €	namestitev: 32 ur, testiranje: 16 ur (skupaj 48 ur = 555 €)	letna naročnina za protivirusne definicije: 1.100 €	mesečno 2 uri (letno 24 ur = 277 €)	0
D	strošek spletnega izobraževanja za 40 zaposlenih: 1.600 €	strošek interne organizacije izobraževanja: 4 ure = 46 €	letno ponavljanje izobraževanja: 1.600 €	0	0
E	strošek nakupa programske opreme: 650 € strojne opreme: 2000 € (skupaj = 2.650 €)	namestitev: 40 ur, testiranje: 16 ur (skupaj 56 ur = 647 €)	0	mesečno 10 ur (letno: 120 ur = 1387 €)	0
F	2.804 €	324 €	2.435 €	138 €	0

Parameter produktivnosti varnostnih ukrepov A, B in C določimo s pomočjo zbranih podatkov o učinkovitosti protivirusnih rešitev (AV-Test, 2008), ki ocenijo za koliko odstotkov se zmanjša ranljivost. Iz zbranih podatkov se dobijo vrednosti 65,5 % za ukrep A, 94,4 % za ukrep B in 97,8 % za ukrep C. Pri ukrepu D (in posledično tudi pri ukrepu F) se zaradi vsakoletnega ponavljanja produktivnost vsako leto zvišuje. Ocena podjetja je, da je učinkovitost izobraževanja za prvo leto 25 %, nato se vsako leto tveganje zmanjša za 20 % preostalega tveganja. Če se izobraževanja ne bi ponavljala, bi produktivnost ukrepa z leti padala. Za ukrep E (korektivni ukrep) je parameter α ocenjen na podlagi prihranka pri času povrnitve podatkov. Čas t_r se zmanjša na 6 ur. Produktivnost ukrepa F pa je dobljena s kombinacijo produktivnosti za ukrep B in D.

Za preventivne ukrepe A, B, C, D in F se produktivnost ukrepa α lahko izračuna:

$$v = (1-u) \cdot v_0 \tag{186}$$

Pri tem je parameter u učinkovitost protivirusne rešitve, pridobljena iz zbranih podatkov (AV-Test, 2008). v_0 je ranljivost pred uvedbo zaščite. Povezavo med produktivnostjo ukrepa α in učinkovitostjo posameznih protivirusnih rešitev dobim z uporabo enačb (60) in (186) na sledeč način:

$$\alpha = \frac{\ln(1-u)}{C \cdot \ln v} \tag{187}$$

Pri tem so C povprečni letni stroški.

Za korektiven ukrep E velja:

$$t_r = t_{r0} \cdot e^{-\alpha \cdot C} \tag{188}$$

in

$$\alpha = -\frac{\ln(t_{r0}/t_r)}{C} \tag{189}$$

Za ukrep F dobim vrednost produktivnosti α_F kot kombinacijo produktivnosti α_B ukrepa B in α_D ukrepa D.

$$\alpha_F = 1-(1-\alpha_B)\cdot(1-\alpha_D) \tag{190}$$

Iz enačb izračunamo vrednosti za produktivnost varnostnih ukrepov, ki so prikazane v tabeli 20:

Tabela 20: *Ocena parametra produktivnosti varnostnih ukrepov za zmanjšanje tveganja virusov*

Rešitev	Vrednost α (v 10^{-3})
A	0,7691
B	2,1018
C	1,1607
D[12]	0,1482 / 0,2320 / 0,3157 / 0,3995
E	0,1284
F	0,9571 / 1,0062 / 1,0553 / 1,1044

[12] Učinkovitost se zaradi ponovitev izobraževanj vsako leto povečuje. Navedeni podatki so za vsako leto posebej.

Ocena negativnega vpliva uvedenega ukrepa na poslovanje δ je smiselna za ukrepe A, B in C. Pri teh ukrepih se produktivnost zmanjša za 3 minute dnevno (počasnejše delovanje sistema). To znese za vse zaposlene: 40 × 3 minute = 120 minut/dan. Povprečno zaposleni opravi 260 delovnih dni, kar skupno znese 520 ur (6.011 €/leto).

Ocena posrednega pozitivnega učinka uvedbe ukrepa μ je smiselna za ukrepa C in E. Pri ukrepu C se poleg protivirusne zaščite pridobi požarni zid, zato je μ = 1.000 €. Pri ukrepu E pa izvedene varnostne kopije koristijo še za druga tveganja μ = 500 €.

Vrednotenje posameznih ukrepov je prikazano v tabeli 21, rezultati izračunov ROI, NPV in IRR pa v tabeli 22.

Tabela 21: *Ekonomsko vrednotenje posameznih ukrepov za zmanjšanje tveganja virusov*

	Ukrep A			**Ukrep B**			**Ukrep C**		
Leto	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)
0		1.766			1.481			6.484	
1	2.391	0	693	6.099	0	138	7.535	1.100	277
2	2.391	0	693	6.099	835	138	7.535	1.100	277
3	2.391	0	693	6.099	835	138	7.535	1.100	277
4	2.391	0	693	6.099	835	138	7.535	1.100	277

	Ukrep D			**Ukrep E**			**Ukrep F**		
Leto	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)
0		1.646			3.297			3.127	
1	3.207	0	0	2.887	0	1.387	6.279	0	138
2	5.131	1.600	0	2.887	0	1.387	6.386	2.435	138
3	6.671	1.600	0	2.887	0	1.387	6.473	2.435	138
4	7.903	1.600	0	2.887	0	1.387	6.542	2.435	138

Tabela 22: *Izračuni ROI, NPV in IRR ukrepov za zmanjšanje tveganja virusov*

Ukrep	**ROI**	**NPV**	**IRR**
A	111 %	4.591 €	89 %
B	437 %	18.522 €	390 %
C	151 %	16.571 €	87 %
D	255 %	15.173 €	209 %
E	53 %	4.191 €	48 %
F	134 %	13.634 €	166 %

Prva zanimiva ugotovitev je, da dajejo vsi ukrepi pozitiven rezultat. Najbolj ekonomsko optimalna izbira je ukrep B, na drugem mestu pa ukrep D. Ukrep F, ki je kombinacija ukrepov B in D, pa je šele na četrtem mestu. Očitno v tem primeru cena skupnih ukrepov ne upraviči dodatne varnosti. Omeniti je potrebno še, da izračun za ukrep B, enako kot ostali ukrepi, vsebuje tudi nabavno ceno in uvedbo ukrepa. Če se upošteva, da podjetje ta ukrep že ima uveden, ta stroška za ukrep B odpadeta, kar pomeni še boljši rezultat pri vseh kazalcih.

7.2 Analiza modela za tveganje napada z ohromitvijo storitve

Podjetje se zaveda nevarnosti organiziranega napada skupine ali posameznikov z namenom ohromitve storitve (DoS). Zoper to grožnjo želijo poiskati najboljšo rešitev.

DoS napad je primarno usmerjen na poslovne procese, ki predstavljajo delovanje storitev za zunanje stranke in so prikazani v tabeli 23.

Tabela 23: *Prikaz poslovnih procesov, ki so lahko ogroženi zaradi DoS napada*

Poslovni proces	Želena stopnja varnosti
Izvajanje storitev za zunanje stranke	v
Podporni proces zagotavljanja delovanja infrastrukture	v

Skozi te procese DoS napad ogroža sredstva, ki so prikazana po kategorijah v tabeli 24.

Tabela 24: *Prikaz informacijskih sredstev, ki jih lahko ogroža DoS*

Informacijsko sredstvo	Želena stopnja varnosti
Podatki in informacije	
Javni podatki	s, n
Storitve	
Interne IT storitve	v, s, n
Storitve za zunanje stranke	v

7.2.1 Ocena tveganja

Ranljivost je verjetnost, da bo izveden DoS napad povzročil nedelovanje storitev za zunanje stranke. Podjetje ocenjuje, da bi bil, glede na trenutno zaščito, vsak tretji napad uspešen.

- $v = 0{,}33$

Podjetje zadnja štiri leta preko IDS sistema nadzira in beleži napade preko spleta. V tem času podjetje ni zaznalo izvedenega DoS napada. Zato ocenjuje, da je pogostost tovrstnih napadov manjša od enega napada na štiri leta. Ker je interes, da se pri izračunu upošteva največje možno tveganje, je pogostost za incident ocenjena na enega v štirih letih:

- $T = 1/(365 \times 4)\ /dan = 6{,}85\times10^{-4}\ /dan$

Verjetnost za incident v enačbi (23) je:

- $\rho = T \cdot v = 6{,}85 \cdot 10^{-4} \cdot 0{,}33 = 2{,}28 \cdot 10^{-4}\ /\ dan$

Naredi se oceno izgub v primeru varnostnega incidenta. Zaradi DoS napada ni potrebno zamenjati opreme, zato stroška zamenjave ni:

- $L_s = 0$

Čas odprave posledic incidenta je ocenjen na 6 ur, delo odpravljajo štirje sistemski administratorji ($n = 4$). Strošek popravila v enačbi (31) zaradi DoS napada je:

- $L_r{}^0(t) = 46{,}24$ €/uro, $t_r{}^0 = 6$ ur

Zaradi DoS napada je potrebno sistem ponovno spraviti v normalno delovanje. Čas nedelovanja je ocenjen na 7 ur, napad se detektira v eni uri ($t_{NA} = 7$ ur, $t_d = 1$ ura). Ocena je, da DoS napad popolnoma onemogoči storitve ($EF_I = 1$). Izguba prihodkov podjetja v enačbi (32) zaradi DoS napada je:

- $L_i{}^0(t) = 342{,}47$ €/uro, $t_{NA}{}^0 = 6$ ur, $t_d{}^0 = 1$ ura

Ocena je, da vpliv incidenta na produktivnost pri uporabnikih znaša polovico časa nedelovanja ($EF_P = 0{,}5$). DoS napad vpliva na produktivnost četrtine zaposlenih ($m = 10$). Čas nedelovanja je ocenjen na 7 ur. Izguba produktivnosti zaposlenih v enačbi (33) zaradi DoS napada je:

- $L_p{}^0(t) = 57{,}8$ €/uro, $t_{NA}{}^0 = 7$ ur

Podjetje v trenutno sklenjenih SLA pogodbah nima obveze po plačilu strankam zaradi nedelovanja, ali poplačilu škode, ki jo stranka utrpi zaradi nedelovanja.

Verjetno bi podjetje v primeru takega incidenta strankam pri mesečnem obračunu odštelo sorazmeren delež zaradi časa nedelovanja.

- L_{SLA} = 200 €

Ocena je, da se v primeru DoS napada število novo pridobljenih strank zmanjša za 5 %, obstoječe stranke naj ne bi odšle k drugemu ponudniku.

- $L_{posredne}$ = 1.250 €

Ob upoštevanju enačb (40), (41), (42) in (43) dobimo:

- L_1 = 446,51 €/uro
- L_2 = 400,27 €/uro
- L_3 = 1.450,93
- L = 4.530,27 €

Varnostno tveganje v enačbi (45) ocenimo na:

- $R = \rho \cdot L = 2,28 \cdot 10^{-4} / dan \cdot 4530,27€ = 1,03€ / dan = 377,52€ / leto$

Vrednost tveganja je takšna, da je ustrezna obravnava zmanjšanje tveganja z investicijo v varnostni ukrep.

7.2.2 Vrednotenje možnih ukrepov za zmanjšanje tveganja

Proti DoS napadu se izbere naslednja možna ukrepa:

- Ukrep A: Aplikacijski požarni zid, z vgrajenim sistemom za preprečevanje vdorov (angl. *intrusion prevention system, IPS)*, ki preprečujejo DoS napade.
- Ukrep B: Vzpostavitev redundančnega sistema na drugi fizični lokaciji, ki ob primeru napada na primarno lokacijo, prevzame delovanje storitev. Poenostavljeno privzamem, da v primeru preklopa med lokacijama ni časovne zakasnitve glede nedelovanja.

Ocena karakteristik stroškov izbranih ukrepov v enačbi (49) je prikazana v tabeli 25. V izračunu je časovno obdobje za investicijo 4 leta. Parameter produktivnosti varnostnih ukrepov določimo s pomočjo zbranih podatkov o učinkovitosti ukrepov, ki ocenijo, za koliko odstotkov se zmanjša ranljivost. Za preventivni ukrep A izberemo enako vrednost kot pri ukrepu C za grožnjo računalniški virus. Za korektivni ukrep B upoštevamo, v enačbi (189), da imajo sistemski administratorji 1 uro dela, da stvari vzpostavijo v prvotno stanje, čeprav storitve nemoteno delujejo. Ocena parametra produktivnosti je prikazana v tabeli 26.

Tabela 25: *Ocena stroškov varnostnih ukrepov za zmanjšanje tveganja napada z ohromitvijo storitve*

Ukrep	Strošek nabave opreme C_p	Strošek uvedbe, testiranja, izobraževanja C_i	Strošek nadgradenj in popravkov C_f	Strošek vzdrževanja C_m	Ostali stroški C_o
A	nakup opreme: 2000 €	uvedba in testiranje: 40 ur = 462 €	naročnina na posodobitve: 1.100 €	mesečno 2 uri, (letno 24 ur = 277 €)	0
B	strošek nakupa programske in strojne opreme: 35.000 €	namestitev: 120 ur, testiranje: 40 ur, (skupaj 160 ur = 1.850 €)	0	mesečno 16 ur, (letno: 192 ur = 2.220 €)	mesečni najem lokacije 300 € (letno 3.600 €)

Tabela 26: *Ocena parametra produktivnosti varnostnih ukrepov za zmanjšanje tveganja napada z ohromitvijo storitve*

Rešitev	Vrednost α (v 10^{-3})
A	1,1607
B	0,119

Nobena rešitev nima negativnega vpliva uvedenega ukrepa na poslovanje (δ). Ocena posrednega pozitivnega učinka uvedbe ukrepa μ je smiselna za obe rešitvi. Pri ukrepu A podjetje z rešitvijo pridobi še požarni zid, zato je ocena μ = 1.500 €. Pri ukrepu B se redundančna lokacija lahko uporabi tudi za druge aktivnosti (npr. testiranje okrevalnih načrtov, migracije na nove verzije, enostavnejše zagotavljanje delovanja idr.) Podjetje oceni vse te koristi z μ = 5.000 €.

Vrednotenje posameznih ukrepov je prikazano v tabeli 27, rezultati izračunov ROI, NPV in IRR pa v tabeli 28.

Tabela 27: *Ekonomsko vrednotenje posameznih ukrepov za zmanjšanje tveganja napada z ohromitvijo storitve*

	A			B		
Leto	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)	Koristi (€)	Stroški nabave in nadgradnje (€)	Stroški vzdrževanja (€)
0		2.462,43			36.849,71	
1	1.835,31	0,00	277,46	5.340,31	0,00	5.819,65
2	1.835,31	1.100,00	277,46	5.340,31	0,00	5.819,65
3	1.835,31	1.100,00	277,46	5.340,31	0,00	5.819,65
4	1.835,31	1.100,00	277,46	5.340,31	0,00	5.819,65

Tabela 28: *Izračun ROI, NPV in IRR ukrepov za zmanjšanje tveganja napada z ohromitvijo storitve*

Ukrep	ROI	NPV	IRR
A	7 %	322,82 €	10 %
B	-64 %	-38.644,3 €	-

Ukrep A daje pri vseh kazalcih pozitiven rezultat, zato je njegova vpeljava smiselna. Glede na to, da je rezultat pri vseh kazalcih le malo večji od nič, je potrebno biti pri dokončni odločitvi glede investicije previden, saj je potrebno upoštevati tudi morebitno nenatančnost vhodnih podatkov. Ukrep B daje pri vseh kazalcih precej velik negativen rezultat, zato njegova uvedba ni smiselna. Investicija v ukrep B je finančno prevelika, če se z ukrepom zaščiti zgolj pred DoS napadom. V kolikor bi podjetje v nadaljnji analizi ocenilo, da ta varnostni ukrep varuje tudi pred drugimi grožnjami ali prinaša dodatne koristi (ki se jih upošteva preko parametra μ), bi se lahko rezultat za ukrep B popravil.

Zaključek

Pregled glavnih ugotovitev

Informacijska varnost je področje za katerega 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 je potrebno, da popolnoma varen sistem ne obstaja. Podjetje mora izbrati takšno stopnjo varnosti, ki je za podjetje sprejemljiva. Določitev ustrezne stopnje pa je zahtevna naloga, ki se izvaja skozi proces obvladovanja varnostnih tveganj.

Obvladovanje tveganja je celoten proces obvladovanja izpostavljenosti podjetja negotovosti, s posebnim poudarkom na identifikaciji, nadzoru in odpravljanju ali minimiziranju negotovih dogodkov, ki lahko podjetju potencialno preprečijo dosego zastavljenih ciljev. Postopek vključuje identifikacijo in oceno informacijskih sredstev podjetja, ki jih je potrebno varovati, analizo groženj, ki so uperjene na ta sredstva, oceno verjetnosti za grožnje, identifikacijo ranljivosti, ki jih je mogoče izkoristiti, oceno posledic varnostnih incidentov, verjetnosti uspešnih napadov na sisteme ter poslovnih stroškov in koristi investicij v varnost. Cilj procesa je identifikacija in merjenje tveganja z namenom informiranja procesa odločanja, ki omogoča izbiro stroškovno učinkovite zaščite. To je zaščita, katera ne stane več, kot je pričakovana izguba ob napadu.

Osnovna strategija obvladovanja tveganja je zmanjšanje izpostavljenosti sredstva tveganju z uvedbo ustreznih tehnologij, orodij ali ustreznih postopkov. S tem se zmanjša verjetnost za škodljive dogodke ali omeji škoda, ki jo 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. Zbirka

potencialnih groženj se s časom neprestano spreminja in je le delno znana. Strokovnjaki za informacijsko varnost se zato zavedajo, da je potrebno v rešitve, povezane z informacijsko varnostjo, neprestano vlagati, saj lahko le na ta način zmanjšujejo ali vsaj ohranjajo tveganje na istem nivoju. 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 (Bojanc, 2008). Proces obvladovanja tveganja pomaga podjetjem sprejeti odločitev glede potrebnih investicij v varnostne ukrepe, ki so za poslovanje podjetja najučinkovitejši. Preden se zapravi denar za določen produkt ali storitev, je dobro vedeti, ali je investicija finančno upravičena. Informacijska varnost pri tem ni nobena izjema. Kolikšna je prava vsota denarja, ki naj se ga nameni investicijam v varnost? Kolikšno izgubo lahko povzroči pomanjkanje varnosti? Kakšen vpliv bodo imeli uvedeni varnosti ukrepi na produktivnost? To so le tri vprašanja, s katerimi se strokovnjaki s področja informacijske varnosti običajno srečujejo pri iskanju ustrezne varnostne rešitve. Odgovori seveda niso enostavni.

Za ravnanje z varnostnim tveganjem je možno uporabiti kvantitativne ali kvalitativne metode. Kvantitativne metode poskušajo določiti numerične vrednosti za verjetnost in učinek tveganja ter ovrednotiti stroške in koristi vezane na uvedbo posameznega varnostnega ukrepa. Namen uvedenega varnostnega ukrepa je zmanjšanje tveganja do točke, kjer se mejni stroški uvedbe ukrepa izenačijo s prihrankom ob varnostnem incidentu. Uvedeni varnostni ukrepi lahko bodisi zmanjšujejo izgubo zaradi incidenta ali ranljivost sredstva in s tem posledično verjetnost za incident. Lahko tudi preprečijo nastanek incidenta. Za razliko od kvantitativnih metod, poskušajo kvalitativne metode določiti le relativne vrednosti pri oceni tveganja. Obe vrsti metod imata svoje prednosti in slabosti. Kvantitativne metode slonijo na znanstvenem pristopu, vendar nimajo standardne metode za učinkovito določitev numeričnih vrednosti. Kvalitativne metode so povečini manj obremenjujoče za človeške vire in časovni obseg aktivnosti, vendar so rezultati bolj splošni. Ne glede na vrsto izbrane metode je pomembno, da proces obvladovanje tveganja omogoči izbiro in primerjavo posameznih ukrepov med seboj ter da omogoča oceno ekonomske donosnosti za posamezen ukrep. Zaradi težavnega izračuna kvantitativnih metod se trenutno v praksi večinoma uporabljajo kvalitativne metode. Omejitve kvalitativnih metod in prednosti kvantitativnih metod pa predstavljajo izziv in spodbudo za raziskovanje in iskanje kvantitativne rešitve, ki bi omogočala ustrezno in zanesljivo vrednotenje varnostnih tveganj.

Na navedenih izhodiščih razvijem temeljno hipotezo H_1: kvantitativno ovrednotena potreba po informacijski varnosti omogoča oceniti optimalno količino potrebnih vlaganj v varovanje in izbiro ustrezne zaščite v poslovnih okoljih.

Poleg temeljne hipoteze izpostavim še naslednje teze: a) problematiko informacijske varnosti se ne da učinkovito reševati le s tehničnim pogledom na

problem in tehnološkimi rešitvami, b) kvantitativno medsebojno vrednotenje različnih tehničnih, proceduralnih zaščit s prenosom tveganja na zunanjega izvajalca so možne poti, ki lahko zagotovijo zmanjšanje varnostnih tveganj na najmanjšo možno mero, c) kazalci, kot so donosnost investicije (ROI), neto sedanja vrednost (NPV) in notranja stopnja donosa (IRR), lahko zagotovijo celovito vrednotenje varnostnih rešitev in d) ustrezna metodologija za vrednotenje in izbor varnostnih rešitev v poslovnem okolju, ki sloni na kvantitativnih izračunih, omogoča optimalno rešitev pri izbiri sistema za zmanjšanje varnostnih tveganj.

Za ugotovitev veljavnosti tez analiziram in študiram področje ekonomike informacijske varnosti z vidika potrebnih vlaganj za preprečitev varnostnih tveganj. Skozi raziskovanje ugotavljam, ali je mogoče ustrezno kvantitativno vrednotiti tveganja v informacijski varnosti. Še posebej sem se posvetil razvitim kvantitativnim modelom za vrednotenje potrebnih investicij, izbiri optimalne rešitve in preverjanja modela z empiričnimi izračuni.

Za potrditev tez in dosego ciljev sem disertacijo zasnoval na dveh ravneh. V prvem, teoretičnem delu disertacije, s katerim se ukvarjam od prvega do četrtega poglavja, sem predstavil problematiko, s katero se ukvarja raziskovalno področje ekonomike informacijske varnosti, pregledal dosedanje dosežke, obstoječo literaturo ter tekoče raziskave na področju ekonomike informacijske varnosti. Podajam pregled razvoja informacijske varnosti od prvih poskusov kvantitativnega vrednotenja tveganja z ALE do razvoja raziskovalnega področja ekonomike informacijske varnosti v zadnjem desetletju. Opravil sem pregled in analizo nekaj najvidnejših in najpomembnejših zbranih teoretičnih spoznanj in empiričnih podatkov, ki so objavljeni v različnih člankih, raziskavah in poročilih. Analiziral sem različne analitične pristope in matematične modele. Še posebej sem se posvetil razvitim kvantitativnim modelom za vrednotenje investicij in rezultatom opravljenih empiričnih raziskav.

V drugem delu disertacije, ki zajema poglavja od pet do sedem, sem razvil lastno metodologijo in celovit matematični model za oceno vlaganj v varnost in zaščito v poslovne informacijske sisteme, ki temelji na kvantitativni analizi varnostnih tveganj. Razviti model omogoča kvantitativno vrednotenje različnih možnosti investiranja v informacijsko varnost in podaja priporočila za izbiro optimalnega vlaganja v varnost. Model sem najprej preveril na teoretični ravni, v nadaljevanju na matematičnih simulacijah ter na empirični ravni za konkretno podjetje. V pomoč vrednotenju varnostnih rešitev sem predstavil kategorizacijo varnostnih tveganj in varnostnih ukrepov.

Pri raziskovalnem delu, namenjenem dokazovanju navedenih tez, sem uporabil več različnih metod dela. V uvodnem teoretičnem delu sem, pri proučevanju literature s področja ekonomike informacijske varnosti, uporabil metodo deskripcije s pomočjo katere opišem teorijo, pojme ter ugotovljena dejstva, metodo klasifikacije, kjer definiram pojme, ki jih razlagam v nadaljevanju in so predmet raziskovanja,

metodo komparacije, kjer primerjam dela in raziskave različnih avtorjev in metodo kompilacije, kjer s povzemanjem spoznanj in sklepov drugih avtorjev v zvezi z izbranim raziskovalnim problemom oblikujem nova stališča. Teoretični del sem v nadaljevanju nadgradil z analitičnimi metodami in empiričnimi ugotovitvami, ki so objavljene v različnih raziskavah in poročilih (CSI, 2009; DSCI, 2009; DTI, 2006).

V prvem poglavju sem opredelil informacijsko varnost, navedel ključne težave pri reševanju varnostnih težav in predstavil problematiko, s katero se ukvarja ekonomika informacijske varnosti. Prednost ekonomskega pristopa je v celovitejšem pogledu na informacijsko varnost, ki upošteva stroške incidentov in finančne koristi uvedenih ukrepov. S pomočjo ekonomskega pristopa se lahko oceni, katera izmed rešitev, ki jih ima podjetje na voljo, ima najboljše razmerje med ceno in kakovostjo, kar omogoča vpeljavo optimalnih varnostnih rešitev.

Ključnega pomena za določitev optimalnih varnostnih rešitev je zavedanje, da je informacijska varnost proces in ne produkt (Schneier, 2004a). Vsak poslovni proces je potrebno obvladovati in nadzorovati (ISO 9001, 2008). Ravnanje z informacijsko varnostjo sem opredelil v drugem poglavju. S pomočjo ocene tveganja, se tveganja ugotovijo in ovrednotijo, podjetje se lahko odloči, ali obstoječe zaščite zadostujejo za varovanje informacijskih sredstev pred verjetnimi grožnjami ali je potrebno vpeljati nove. Kvantitativna ocena tveganja omogoča določiti natančne finančne vrednosti za posamezna tveganja. To pa so informacije, ki jih pri svojem odločanju potrebujejo managerji. Potrebne investicije so lahko na ta način tudi hitreje odobrene, saj je njihov vpliv zaradi kvantitativne ocene hitro in enostavno primerljiv.

V tretjem in četrtem poglavju sem opredelil ključne elemente informacijske varnosti, ki so: sredstva, grožnje, ranljivosti in varnostni ukrepi. Pri tem sem analiziral dosedanja raziskovanja in teoretične modele, pri čemer sem pri analizi posameznih elementov poudaril prispevek kvantitativnih pristopov. Obe poglavji se zaključujeta s pregledom rezultatov različnih empiričnih raziskav. Raziskave navajajo vrednosti finančnih izgub, število doživetih varnostnih incidentov v posameznem letu ter vrste varnostnih incidentov in njihov delež glede na vse incidente. Navedeni podatki so konkretne vrednosti, ki kažejo na to, da je za varnostna tveganja možno pridobiti kvantitativne podatke in te podatke tudi uporabiti v nadaljnjih kvantitativnih izračunih za varnostna tveganja.

Z dosežki, v opravljenih teoretičnih in empiričnih raziskavah, sem podprl veljavnost temeljne hipoteze H_1, da je mogoče s kvantitativnim vrednotenjem informacijske varnosti pridobiti ustrezne podatke, ki se jih potrebuje za obvladovanje varnostnih tveganj. V poglavju 4.3 skozi dosežke teoretičnih raziskav potrjujem hipotezo tudi v tem, da je mogoče kvantitativno oceniti količino potrebnih vlaganj. Za končno teoretično in empirično potrditev hipoteze sem izdelal matematični model za oceno vlaganj v varnost in zaščito v poslovnih informacijskih sistemih, ki temelji na kvantitativni analizi varnostnih tveganj.

Model je zasnovan kot postopek, ki poteka od vnosa vhodnih podatkov o sredstvih, grožnjah in ranljivostih, do končnih priporočil za izbiro ustrezne rešitve, ki zmanjšuje določeno varnostno tveganje. Model omogoča neposredno primerjavo in kvantitativno vrednotenje različnih varnostnih ukrepov, od tehnoloških varnostnih rešitev, uvedbe organizacijskih postopkov, izobraževanja ali prenosa tveganja na zunanje podjetje. Izhodni podatek modela je donosnost posameznega ukrepa merjena z ROI, NPV in IRR ter primerjava posameznih ukrepov med seboj. Model direktno potrjuje temeljno hipotezo, pri tem pa je potrebno pravilnost matematičnega modela še preveriti. Preverjanje modela sem izvedel dvonivojsko, in sicer z matematično simulacijo in empirično analizo na primeru konkretnega podjetja.

Pri preverjanju modela z matematično simulacijo (šesto poglavje) sem primerjal teoretične rezultate ekonomskega vrednotenja varnostnih ukrepov z naključno simulacijo izbire varnostnih ukrepov in naključnim naborom varnostnih incidentov. Na podlagi vhodnih podatkov o grožnjah, ranljivostih, izgubah in možnih ukrepih, sem s teoretičnim modelom izračunal vrednosti ROI, NPV in IRR za posamezno uvedbo varnostnega ukrepa. Simulacija naključno izbere en varnostni ukrep in oceni letno izgubo glede na naključne ponovitve varnostnih incidentov. Na ta način se varnostne ukrepe razvrsti glede na velikost povprečne letne izgube. To razvrstitev se primerja z izračunanimi teoretičnimi vrednostmi ROI, NPV in IRR za posamezen ukrep. Rezultat simulacije je pokazal precej dobro ujemanje razvrstitve izračunov teoretičnega modela z rezultati naključnih dogodkov simulacije. Ujemanje pomeni, da ima ukrep, ki je imel v simulaciji najmanjšo izgubo tudi pri teoretičnem izračunu, največjo vrednost ROI, NPV in IRR. Med rezultatom simulacije in teoretičnim izračunom so sicer prisotna manjša odstopanja, vendar so razlike v razvrstitvi prisotne že med samimi izračuni ROI, NPV in IRR. Iz prikazanega lahko zaključim, da matematična simulacija potrjuje pravilnost in ustreznost modela.

Pri preverjanju modela z empirično analizo (sedmo poglavje) sem uporabil podatke konkretnega srednje velikega slovenskega podjetja, ki deluje na področju informacijske tehnologije. Cilj empirične analize je potrditev ustreznosti matematičnega modela za praktično uporabo v poslovnem okolju. Model sem, z uporabo realnih podatkov podjetja, praktično preizkusil z analizo varnostnih tveganj za okužbo z računalniškim virusom in za napad z ohromitvijo storitve. S predlaganim matematičnim modelom sem uspešno izbral in določil, kateri varnostni ukrep je za določeno grožnjo najbolj optimalen. Empirična analiza je potrdila praktično uporabnost modela v poslovnem okolju.

Ocenjujem, da sta, tako preverjanje modela s simulacijo, kot preverjanje z empirično analizo, potrdila veljavnost in pravilnost matematičnega modela. S tem sem v doktorski disertaciji pokazal, da je informacijsko varnost mogoče reševati s kvantitativnim pristopom. Na podlagi predstavitve raziskovalnega področja ekonomike informacijske varnosti, razvitega modela za kvantitativno vrednotenje

varnostnih ukrepov in potrditve predlaganega modela z empirično analizo in matematično simulacijo, lahko zaključim, da kvantitativno ovrednotena potreba po informacijski varnosti lahko oceni optimalno količino potrebnih vlaganj v varovanje in izbiro ustrezne zaščite v poslovnih okoljih, kar potrjuje tudi zastavljeno temeljno hipotezo H_1.

Tezo a) potrjujem večinoma skozi prvo poglavje, deloma tudi v nadaljevanju disertacije. V preteklosti se je na informacijsko varnost gledalo zgolj s tehničnega stališča, kar se je izkazalo za pomanjkljiv pristop, ki ne more zadovoljivo rešiti problema informacijske varnosti. Za uspešno reševanje varnostnih vprašanj je potrebno zavzeti procesni pristop in obvladovati varnostna tveganja.

Bruce Schneier (2003) pojasnjuje, kako deluje varnost: "*Najpomembnejše je, da o varnosti ne razmišljamo kot o nečem popolnem, ampak kot o razumnem kompromisu tako na osebni kot globalni ravni.*" Ter dodaja: "*Ekonomija - ne tehnologija - določa katera varnostna tehnologija bo uporabljena.*" Zanašanje samo na tehnologijo je napačno, ker tehnologija ne zmore braniti vsega. Zato je ključno pri iskanju ustreznih odgovorov, da se ne omejimo zgolj na tehnični pogled informacijske varnosti. Tehnični pogled sicer podaja tehnološke rešitve za zmanjševanje varnostnih groženj, težko pa utemelji, koliko je potrebno v varnost investirati. Večina osnovnih varnostnih vprašanj je vsaj toliko ekonomskih kot tehničnih, zato je za pravilen pristop k reševanju problema informacijske varnosti potrebno tehnološke poglede združiti z ekonomskimi stališči, o čemer govorim v poglavju 1.4. Fokus informacijske varnosti se tako prestavi iz tehnično izvedljivega na ekonomsko optimalno.

V disertaciji sem razjasnil, da problematike informacijske varnosti ne moremo učinkovito rešiti le s tehničnim pogledom na problem in tehnološkimi rešitvami, temveč je potrebno na informacijsko varnost gledati kot na proces, v katerem se upošteva tudi ekonomska načela. Pri iskanju ekonomsko optimalne investicije v varnostno rešitev je potrebno primerjati koristi, ki jih ima podjetje zaradi investicije, ter same stroške investicije. Dokler so koristi investicije večje od stroškov investicije, je uvedba rešitve smiselna. Seveda pa nima nobenega smisla uvesti neke rešitve, za katero zapravimo več, kot je največja možna izguba. Z ekonomskega stališča je optimalna investicija v varnost takrat, ko je razlika med koristmi in stroški največja. Na podlagi zgoraj navedenih ugotovitev ocenjujem, da se problematiko informacijske varnosti ne da učinkovito reševati le s tehničnim pogledom na problem in tehnološkimi rešitvami, kar potrjuje tezo a).

Pri potrjevanju teze b), se opiram predvsem na ugotovitve v četrtem poglavju. Zmanjševanje in prenos tveganja sta dve možni obravnavi tveganja, ki sta povezani z investicijami (poglavje 2.1.2). V osnovi lahko možne varnostne ukrepe glede na način zmanjševanja tveganja razdelim na preventivne, korektivne in detekcijske. Vsaka od teh skupin pa lahko vsebuje različne ukrepe, od tehničnih ukrepov do organizacijsko-procesnih ukrepov, izobraževanj zaposlenih, zavarovanja itd.

(poglavje 4.1). Pri iskanju možnih rešitev varnostnih tveganj se je potrebno zavedati omejitev zgolj tehničnih rešitev, spodbujati uvedbo na standardih temelječih organizacijsko-procesnih rešitev (poglavje 1.3), upoštevati pomen človeškega faktorja (poglavje 1.2.4) in alternativnih ravnanj s tveganji, kot sta prenos tveganja na zavarovalnico (poglavje 4.2.1) ali prenos tveganja na zunanjega izvajalca (poglavje 4.2.2).

Uporabo različnih vrst ukrepov v praksi, potrjujem z več raziskavami (CSI, 2009; DSCI, 2009; BERR, 2008). V poglavju 5.3 sem pokazal, kako se lahko kvantitativno ovrednoti različne varnostne ukrepe. Predstavljeni model je dovolj splošen, da omogoča vrednotenje poljubnega varnostnega ukrepa in ni omejen le na določene vrste ukrepov. S pomočjo kazalcev ROI, NPV in IRR se lahko kvantitativno ovrednotene ukrepe primerja med seboj in ugotovi, kateri ukrep je v določeni situaciji najbolj optimalen. Kombinacija različnih vrst varnostnih ukrepov je uporabljena tudi v empirični analizi (sedmo poglavje). Ocenjujem, da je pravilen pristop k reševanju varnostnih tveganj kvantitativno medsebojno vrednotenje različnih tehničnih, proceduralnih zaščit in prenosom tveganja na zunanjega izvajalca. Tak pristop lahko zagotovi zmanjšanje varnostnih tveganj na najmanjšo možno mero, kar potrjuje tezo b).

Za preverjanje teze c) sem v modelu za vrednotenje investicij v varnostne ukrepe uporabil kazalce ROI, NPV in IRR. V poglavju 4.4.2 sem opredelitev smiselnost uporabe teh kazalcev ter potrdil uporabo teh kazalcev na osnovi opravljenih empiričnih raziskav (CSI, 2007, 2008, 2009).

Kazalec ROI je primeren tako za oceno, ali je investicija finančno upravičena, kot tudi za primerjavo več različnih produktov ali storitev med seboj. Osnovno vprašanje, na katerega poskuša ROI odgovoriti, je: "Katera izmed opcij mi da največ za moj denar?" Za izračun ROI se potrebuje finančne vrednosti koristi ter stroškov investicije. V poglavju 4.4.1 ugotavljam, da je ocena stroškov investicije dokaj enostavna, saj se sešteje vse stroške, ki so povezani z nakupom, testiranjem, uvedbo, vzdrževanjem, izobraževanjem uporabnikov in skrbnikov, nadzorom itd. Ker so ti podatki bolj ali manj že v denarnih enotah, to ne predstavlja velikega problema. Ocena koristi zaradi investicije v varnostni ukrep je težja naloga. Običajno se za oceno koristi uporablja ocena možne izgube, ki se ji z investicijo izogne. Za kvantitativno oceno možne izgube se pogosto uporablja metoda ALE, ki predstavlja skupni denarni znesek, ki ga podjetje lahko izgubi v izbranem časovnem obdobju. Pričakovano korist zaradi investicije se lahko izračuna kot razliko med ALE brez investicije v varnostni ukrep in ALE z investicijo.

Zavedati se je potrebno, da ROI ni magična metoda, ki omogoča analitično izbrati optimalno varnostno rešitev. ROI samo pove, kakšna je donosnost investicije v odstotkih za določeno časovno obdobje. Izračun kazalca je enostaven, ima pa tudi nekaj pomanjkljivosti. Ocena je tako točna, kolikor so točni vhodni podatki. Ker je rezultat v odstotkih, to nič ne pove o dejanski višini donosa. Pomanjkljivost je tudi,

da ne upošteva časovne komponente. Zato se, še posebej v primerih dolgoročne investicije, poleg ROI pogosto upoštevajo še drugi kazalci za vrednotenje investicij, med katerimi sta najpogostejša NPV in IRR. NPV upošteva spremembo vrednosti denarja v času z uporabo diskontne stopnje. Pri tem vse prihodnje stroške in koristi prevede na sedanjo vrednost. Rezultat je 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 se zaradi številčne vrednosti lahko dobi lažno prepričanje, da je izračun natančen. Zavedati se je potrebno, da je rezultat kljub številčni vrednosti zgolj ocena, pri kateri je natančnost odvisna od točnosti vhodnih podatkov. Omenjene metode se med seboj razlikujejo, zato jih je dobro pri odločitvi kombinirati in primerjati (Bojanc, 2008; Bojanc & Jerman-Blažič, 2008).

Obstoječe teoretične raziskave, opravljene empirične raziskave in preverjena uporaba matematičnega modela potrjujejo, da kazalci ROI, NPV, IRR lahko zagotovijo celovito vrednotenje varnostnih rešitev in s tem potrjujejo tudi tezo c).

Za potrditev teze d) sem v doktorski disertaciji izdelal metodologijo za kvantitativno vrednotenje informacijske varnosti (peto poglavje). V doktorski disertaciji sem izvedel pregled nad metodami za vrednotenje in izbiro varnostnih rešitev (poglavja 2.2 in 4.3). Večina metod za obvladovanje tveganja se osredotoča na iskanje rešitev za tista tveganja, ki najbolj ogrožajo podjetje, pri čemer je glavni cilj teh metod, da tveganje spravijo na zadovoljivo nizko raven. Težava takega pristopa je, da metoda zgolj poišče ukrep, ki varnostno tveganje zadovoljivo zmanjša in se ne ukvarja s tem ali je ukrep ekonomsko upravičen. Ravno tako te metode običajno ne ponujajo primerjave različnih ukrepov med seboj in ne iščejo ukrepa, ki za svojo ceno ponuja največjo varnost. Za razliko od teh metod se v disertaciji predstavljeni matematični model osredotoča na izbiro optimalnega ukrepa za določeno tveganje.

Pri modelu sem poskušal zajeti čim več pomembnih faktorjev in se s tem čim bolj približati realnemu okolju. Obenem sem pri tem pazil, da model vseeno ne bi postal preveč kompleksen in posledično malo uporaben. Glede tega Varian (1997) navaja: "*Model naj bi razkril bistvo o tem kaj se dogaja, zato je potrebno model zmanjšati na samo tiste elemente, ki so potrebni, da se to doseže.*" Predpostavljanje, da bi bolj zapleten ekonomski model izboljšal razumevanje problematike, je napačno. Tudi v praksi se izkaže, da pogosto preprostejši modeli omogočajo boljše razumevanje kot kompleksnejši modeli.

S predstavljeno metodologijo za vrednotenje in izbor varnostnih rešitev v poslovnem okolju, ki sloni na kvantitativnih izračunih in omogoča izbiro optimalne rešitve za zmanjšanje varnostnih tveganj, ocenjujem, da je teza d) potrjena.

Znanstveni prispevek doktorske disertacije

Predviden prispevek doktorske disertacije k znanosti je večnivojski in zajema teoretični, metodološki in praktični prispevek.

Teoretični znanstveni prispevek predstavljajo opredeljene teoretične in empirične ugotovitve glede informacijske varnosti, obvladovanje varnostnih tveganj, kvantitativno vrednotenje informacijske varnosti in ocene optimalnih vlaganj v informacijsko varnost. Opravljen je kritični pregled, analiza in združitev dosedanjih teoretičnih ugotovitev v pregledno celoto in povezovanje z rezultati objavljenih empiričnih raziskav.

Metodološki prispevek se kaže v predlaganem modelu, postopku in celostnem pristopu k reševanju problematike. V preteklosti podjetja varnosti niso namenjala veliko sredstev, saj se je na varnost gledalo predvsem kot na strošek in ne kot na investicijo. To stanje se z leti popravlja, še vedno pa ostaja težava težko izračunljivih in predstavljivih tveganj. Investicijam v informacijsko varnost se namenja čedalje več pozornosti, saj okolje po eni strani zahteva čedalje več vlaganj v varnost in zaščito (CSI, 2007, 2008, 2009), po drugi strani pa trenutne gospodarske razmere silijo podjetja, IT managerje in vodje informacijske varnosti v racionalizacijo in optimizacijo teh investicij. Še pred nekaj leti so podjetja na investicije v informacijsko varnost večinoma gledala kot na določene nujne stroške in vodje informacijske varnosti niso imeli preveč težav z odobritvijo teh investicij. Danes pa, predvsem zaradi svetovne gospodarske krize in ozaveščenosti na področju ravnanja z informacijsko varnostjo, vrhnji managerji večinoma zahtevajo izdelan poslovni primer, preden odobrijo investicijo. Investicije v varnostne ukrepe morajo biti zato še bolj preudarne in pretehtane. Prav tu pa primanjkuje konkretnih metod in kazalcev za vrednotenje investicij v varnostne rešitve. Modeli in postopki, ki omogočajo managerjem tveganja predstaviti v finančnih vrednostih so zato zelo dobrodošli. To pomeni, da si tisti, ki potrjujejo (oziroma odobrijo) investicije in predvsem njihov finančni učinek, tudi nazorneje predstavljajo pričakovane rezultate in njihov vpliv na poslovanje.

Izdelava modela, ki omogoča vrednotenje investicij v informacijsko varnost in medsebojno primerjavo različnih vrst varnostnih rešitev, je osrednji prispevek doktorske disertacije. Model je izdelan do take mere, da omogoča teoretično kvantitativno vrednotenje posameznih elementov varnostnega tveganja. Rezultat matematičnega modela je ocena donosnosti posameznega ukrepa ter medsebojno vrednotenje in primerjava donosnosti različnih varnostnih ukrepov med seboj. Poseben prispevek predstavlja predlagana metoda za kategorizacijo varnostnih tveganj in groženj in njena možna uvedba v proces obvladovanja varnostnih tveganj.

Praktični prispevek predstavlja simulacijsko okolje, s katerim se preverja veljavnost in uporabnost modela. Okolje simulira grožnje in izbiro varnostnega ukrepa, s čimer se približamo realnemu stanju v poslovnem okolju. Empirični prispevek je preizkus predlaganega modela na primerih različnih groženj v nekem konkretnem podjetju.

Ker je vprašanje iskanja ekonomsko optimalnih varnostnih ukrepov čedalje bolj pereč problem, lahko predstavljeni model in metodologija veliko pripomore k reševanju tovrstne problematike tako na teoretičnem kot praktičnem področju. Na teoretičnem področju je lahko osnova za nadaljnja raziskovanja na področju ekonomike informacijske varnosti, na praktičnem področju pa lahko model in metodologijo uporabljajo podjetja za vrednotenje tveganj in izbiro optimalnih varnostnih rešitev v njihovem poslovnem okolju.

Moja opravljena raziskovanja in dosežki ter objave v revijah s SCI in SSCI omogočajo drugim avtorjem nadaljevati raziskovalno delo in nadgrajevati moje ugotovitve. To dokazuje več člankov, v katerih se tuji avtorji (Fruhwirth & Mannisto, 2009; Qi, Wang & Li, 2009; Huang, Ding & Hu, 2008; Zoric, Helme, Kvalheim & Sundve, 2010; Smith & Kruger, 2010; Sheen, 2010a; Sheen, 2010b; Hajjem, Benabdallah & Ben Abdelaziz, 2010; El-Gayar & Fritz, 2010) sklicujejo na moje dosežke in jih uporabljajo za osnove svojih raziskovanj. Nadgrajevanje mojih dosežkov s strani drugih avtorjev, dokazuje velik prispevek mojih raziskovanj k znanosti.

Kot pomemben rezultat teoretičnega, metodološkega in praktičnega dela ocenjujem zaključne ugotovitve, ki združujejo spoznanja doktorske disertacije, potrjujejo zastavljene teze in cilje ter odpirajo široke možnosti za nadaljnje raziskave in izpopolnjevanje modela.

Možnosti za nadaljnje delo

Raziskava v doktorski disertaciji obravnava nekaj pomembnih varnostnih vprašanj, s katerimi se danes soočajo podjetja in nudi vodjem informacijske varnosti koristne informacije in napotke, kako obravnavati ta vprašanja.

Doktorska disertacija odpira številne možnosti za nadaljnje kvantitativne in ekonomske raziskave na področju informacijske varnosti ter izpopolnjevanje modela. Nadaljnje delo na izboljšavah matematičnega modela lahko vključuje združevanje in kombiniranje več varnostnih ukrepov ter vpliv večjega števila ukrepov na skupno varnost v podjetju. Tak pogled pozitivno vpliva na določitev posrednega pozitivnega učinka uvedbe ukrepa μ in prinaša celovitejši kvantitativen pogled nad stanjem varnosti v podjetju. Tovrsten pristop se lahko nadgradi v kvantitativni kazalec "*stopnja varnosti podjetja*", ki vključuje vsa

tveganja in varnostne ukrepe. Uporaba tega kazalca omogoča povezavo z želenimi stopnjami varnosti (poglavje 5.1).

Možna izboljšava modela je tudi nadgradnja verjetnosti za grožnje, z upoštevanjem povezave med nivojem varnosti v podjetju in napadalčevem poznavanju tega nivoja varnosti. Upošteva se lahko, koliko internih informacij napadalec ima in ali lahko informacije pridobi (poglavje 3.2.2). Če je nivo varnosti v podjetju visok in napadalec to informacijo ima, je manjša verjetnost, da pride do grožnje (Cremonini & Martini, 2005). Nadalje se lahko upošteva vpliv detekcijske zaščite na izboljšanje natančnosti določitve produktivnosti α preventivnega ukrepa. Schneier (2003) opozarja, da vsaka varnostna rešitev prinaša nova tveganja, kar se lahko vključi v proces obvladovanja tveganja. Model se lahko nadgradi tudi z upoštevanjem časovne odvisnosti določenih parametrov (npr. ranljivosti, izgube, produktivnosti ukrepa idr.).

Literatura in viri

1. ABC News online. (2004, 20. avgust). New Microsoft security flaws found. Najdeno 25. septembra 2009 na spletnem naslovu http://www.abc.net.au/news/newsitems/200408/s1181192.htm
2. Adkins, R. (2004). An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from an Information Security Breach. *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=20
3. Akerlof, G. (1970). The Market for 'Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), 488–500.
4. 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
5. Alberts, C. & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Boston: Addison-Wesley.
6. Anderson, A. (1991). Comparing risk analysis methodologies. The *Seventh International Conference on Information Security, IFIP/Sec '91* (str. 301–311). Maryland Heights: Elsevier.
7. Anderson, R. & Moore, T. (2006). The Economics of Information Security. *Science, 314* (5799), 610–613.
8. 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
9. Anderson, R. & Schneier, B. (2005). Economics of Information Security. *IEEE Security and Privacy, 3*(1), 12-13.
10. Anderson, R. (1993). Why cryptosystems fail. *The 1st ACM conference on Computer and communications security* (str. 215-227). Fairfax: ACM.
11. 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.
12. Anderson, R. (2003). Cryptography and Competition Policy – Issues with 'Trusted Computing'. *Workshop on the Economics of Information Security (WEIS 2003)*. Najdeno 15. novembra 2006 na spletnem naslovu *http://www.cpppe.umd.edu/rhsmith3/agenda.htm*
13. Anderson, R. (2005). Open and Closed Systems are Equivalent. *MIT Press 2005*, 127–142.
14. Anderson, R. (2008). *Security Engineering: a Guide to Building Dependable Distributed Systems. Second Edition.* New York: John Wiley and Sons.

15. 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
16. Arbaugh, W. A., Fithen W. L. & McHugh J. (2000). Windows of vulnerability: A case study analysis. *Computer, 33* (12), 52-59.
17. Arora, A. & Telang, R. (2005). Economics of Software Vulnerability Disclosure. *IEEE Security and Privacy, 3*(1), 20-25.
18. Arora, A., Krishnan, R., Nandkumar, A., Telang, R. & Yang, Y. (2004). 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
19. Arora, A., Telang, R. & Xu, H. (2004). 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
20. August, T. & Tunca, T. (2005). *Network Software Security and User Incentives*. Stanford: Stanford University.
21. AV-Test release latest results. (2008, 2. september). *Virus Bulletin.* Najdeno 25. septembra 2009 na spletnem naslovu http://www.virusbtn.com/news/2008/09_02
22. Baer, W. & Parkinson, A. (2007) . The Role of CyberInsurance in Managing IT Security *IEEE Security and Privacy, 6*, 50-56.
23. Baer, W. (2003). *Rewarding IT security in the marketplace.* Santa Monica: RAND Corporation.
24. Bahsoon R. & Emmerich W. (2004). Evaluating architectural stability with real options theory. *The 20th IEEE International Conference on Software Maintenance (ICSM '04)* (str. 443–447), Washington: IEEE Computer Society.
25. Beautement A., Coles R., Griffin R., Ioannidis C., Monahan B., Pym D., Sasse A. & Wonham M. (2008). Modelling the Human and Technological Costs and Beneffits of USB Memory Stick Security. *Workshop on the Economics of Information Security (WEIS 2008).* Najdeno 2. septembra 2008 na spletnem naslovu http://weis2008.econinfosec.org/program.htm
26. 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
27. 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
28. BERR. (2008). BERR 2008 Information Security Breaches Survey, Technical Report. Najdeno 10. marca 2009 na spletnem naslovu http://www.berr.gov.uk/

29. Bishop, M. (2003). *Computer Security: Art and Science.* Boston: Addison-Wesley.
30. Blakley, B. (2001). An imprecise but necessary calculation. *Secure Business Quarterly: Special Issue on Return on Security Investment, 1*(2), 1-3.
31. Bluejackel's finds. (2009, 5. September). The first internet virus: Morris Worm. *Bluejackel's finds*. Najdeno 18. novembra 2009 na spletnem naslovu http://bluejackal.tumblr.com/post/179742558/the-first-internet-virus-morris-worm-in-1988
32. Bodin, L., Gordon, L. & Loeb M. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, *48*(2), 78–83.
33. 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
34. Böhme, R. (2006). A Comparison of Market Approaches to Software Vulnerability Disclosure. *Lecture Notes in Computer Science, 3995*, 298-311.
35. Bojanc, R. & Jerman-Blažič, B. (2007). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces, 30*(4), 216-222.
36. Bojanc, R. & Jerman-Blažič, B. (2008a). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*, 413-422.
37. Bojanc, R. & Jerman-Blažič, B. (2008b). Standard Approach for Quantification of the ICT Security Investment for Cybercrime Prevention. *Second International Conference on the Digital Society (ICDS),* 7-14. Najdeno 7. februarja 2008 na spletnem naslovu http://doi.ieeecomputersociety.org/10.1109/ICDS.2008.37
38. Bojanc, R. (2008). Ekonomika informacijske varnosti. *Varnostni forum, 11*. Nova Gorica: Palsit.
39. Boss, S. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior*. Pittsburgh: University of Pittsburgh.
40. Bosworth, S & Kabay, M. (2002). *Computer Security Handbook. Fourth edition.* New York: John Wiley and Sons.
41. Bowen, R. (2002). *Apache Administrator's Handbook.* Indianapolis: Sams Publishing
42. Brealey, R. A. & Myers, S. C. (2000). Principles of Corporate Finance, 6th edition. New York: McGraw-Hill.
43. Bresnahan, T., Brynjolfsson, E. & Hitt, L. (2002). Information Technology, Workplace Organization, and the Demand for Skilled Labor: Firm-Level Evidence. *Quarterly Journal of Economics, 117*(1), 339-376.
44. British Standards Institution (BSI). (1999). *BS 7799*, London: British Standards Institution (BSI).
45. British Standards Institution (BSI). (2006). *BS 25999-1:2006 Business Continuity Management. Code of Practice*. London: British Standards Institution (BSI).
46. *British Standards Institution (BSI)*. Najdeno 12. januarja 2010 na spletnem naslovu http://www.bsigroup.com

47. *British Standards Institution (BSI).* Najdeno 4. septembra 2007 na spletnem naslovu ttp://www.bsigroup.com
48. Brynjolfsson, E. & Hitt L. (2003). Computing Productivity: Firm-Level Evidence. *Review of Economics and Statistics, 85*(4), 793-808.
49. Brynjolfsson, E., Hitt, L. & Yang, S. (2002). Intangible Assets: Computers and Organizational Capital. *Brookings Papers on Economic Activity, 1*, 137-181.
50. 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.
51. 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
52. Cagnemi, M. P. (2001). Top Technology Issues. *Information Systems Controls Journal, 4*(6).
53. Camp, L. J. & Wolfram C. (2004). Pricing Security. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 17-34). Heidelberg: Springer.
54. Camp, L. J. & Wolfram, C. (2000). Pricing Security. *The CERT Information Survivability Workshop* (str. 31–39). Boston: CERT
55. 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.
56. Campbell, C. M. (2000, 6. oktober). Hacking Rises Despite Increased Security Spending. *PC World*. Najdeno 11. februarja 2009 na spletnem naslovu http://www.pcworld.idg.com.au/article/78513/hacking_rises_despite_increased_security_spending/
57. 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.
58. 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.
59. Carter, R. (1987). The Threat to Computer Systems-Learning the Rules of Risk. *Accountancy, 99*(1125), 124-125.
60. Cavusoglu, H. (2004). Economics of IT Security. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 71-84). Heidelberg: Springer.
61. Cavusoglu, H., Cavusoglu, H. & Raghunathan, S. (2004). Emerging Issues in Responsible Vulnerability Disclosure. *Workshop on Information Technologies and Systems (WITS'04)*. Washington DC: George Mason University.
62. Cavusoglu, H., Cavusoglu, H. & Zhamg, 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

63. Cavusoglu, H., Cavusoglu, H. & Zhang, J. (2008). Security Patch Management: Share the Burden or Share the Damage? *Management Science, 54*(4), 657-670.
64. Cavusoglu, H., Mishra, B. & Raghunthan, S. (2002). *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers*. Dallas: The University of Texas.
65. Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). A Model for Evaluating IT Security investments. *Communications of the ACM, 47*(7), 87–92.
66. Center for Internet Security (CIS). Najdeno 10. septembra 2008 na spletnem naslovu http://www.cisecurity.org
67. Childs, P. D., Ott, S. H. & Triantis, A. J. (1998). Capital Budgeting for Interrelated Projects: A Real Options Approach. *Journal of Fiancial and Quantitative Analysis, 33*(3), 305–335.
68. Cohen, F. (1991). A Cost Analysis of Typical Computer Viruses and Defenses. *Computers & Security, 10*, 239-250.
69. Computer Emergency Response Team (CERT). (2004). E-Crime Watch Survey Summary of Findings. Najdeno 4. septembra 2007 na spletnem naslovu http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf
70. Computer Emergency Response Team (CERT). (2008). CERT Statistics 1988-2008. Najdeno 13. septembra 2009 na spletnem naslovu http://www.cert.org/stats
71. Computer Emergency Response Team Coordination Center (CERT/CC). Najdeno 4. septembra 2007 na spletnem naslovu http://www.cert.org/certcc.html
72. 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.
73. 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
74. 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
75. Computer Security Institute (CSI). Najdeno 11. septembra 2008 na spletnem naslovu http://www.gocsi.com/
76. 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.
77. *CORAS*. Najdeno 25. septembra 2009 na spletnem naslovu http://coras.sourceforge.net/index.html
78. Coren, M. (2005, 24. januar). Experts: Cyber-crime bigger threat than cyber-terror. *CNN*. Najdeno 3. junija 2008 na spletnem naslovu http://edition.cnn.com/2005/TECH/internet/01/18/cyber.security/index.html

79. 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
80. Cremonini, M. & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-on-Attack (ROA). *Workshop on the Economics of Information Security (WEIS 2005).* Najdeno 15. novembra 2006 na spletnem naslovu http://infosecon.net/workshop/schedule.php
81. Cremonini, M. & Nizovtsev, D. (2006). Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. *Workshop on the Economics of Information Security (WEIS 2006).* Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html
82. Crume, J. (2001). *Inside Internet Security*. Boston: Addison Wesley.
83. 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.
84. Denning E. D. (1999). *Information Warfare and Security.* Boston: Addison-Wesley.
85. Department of Defense (DoD). (1985). Trusted Computer System Evaluation Criteria (TCSEC). DoD 5200.28-STD. *U.S. Department of Defense*. Washington, DC. Najdeno 25. marca 2010 na spletnem naslovu http://csrc.nist.gov/publications/history/dod85.pdf
86. Dhillon, G. & Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM, 43*(7), 125-128.
87. Dhillon, G. & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-organizational Perspectives. *Information Systems Journal, 11*(2), 127-153.
88. Dobson, J. (1994). Messages, Communication, Information Security and Value. *The New Security Paradigms Workshop* (str. 10-18). Little Compton: IEEE.
89. Donner, M. (2003). Patch Management - Bits, Bad Guys, and Bucks! *Secure Business Quarterly, 3*(2), 1-4.
90. Douglas, J. L. (2006). *The Security Risk Assessment Handbook. A Complete Guide for Performing Security Risk Assessments.* Boca Raton, Florida: Auerbach Publications.
91. 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
92. 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.
93. Dutta, A. & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-71.
94. 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

95. *EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).* Najdeno 24. septembra 2009 na spletnem naslovu http://www.ssi.gouv.fr/site_article45.html
96. Eklund, B. (2000). Business Unusual, *netWorker, 5*(4), 20-25.
97. El-Gayar, O.F. & Fritz, B.D. (2010). A web-based multi-perspective decision support system for information security planning. *Decision Support Systems, 50*(1), 43-54
98. ENISA. (2009). Inventory of risk assessment and risk management methods. Najdeno 15. aprila 2009 na spletnem naslovu http://rm-inv.enisa.europa.eu/rm_ra_methods.html
99. 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
100. *Euribor Historical Data*. Najdeno 24. novembra 2009 na spletnem naslovu http://www.euribor.org/html/content/euribor_data.html
101. Farahmand, F. (2004). *Developing a Risk Management System for Information Systems Security Incidents.* Atlanta: Georgia Institute of Technology.
102. Farahmand, F., Navathe, S., Sharp, G. & Enslow, P. (2004). Evaluating Damages Caused by Information Systems Security Incidents. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 85-94). Heidelberg: Springer.
103. Farahmand, F., Navathe, S., Sharp, G. & Enslow, P. (2005). A Management Perspective on Risk of Security Threats to Information Systems*. Information Technology and Management 6*(2-3), 203-225.
104. Favaro, J., Favaro, K. & Favaro, P. (1998). Value based software reuse investment. *Annals of Software Engineering, 5*, 5-52.
105. 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
106. *Federal Standard 1037C.* (1996, 7. avgust). Najdeno 12. junija 2008 na spletnem naslovu: http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm
107. Fites, P., Kratz, M. & Brebner, A. (1989). Control and Security of Computer Inforamtion Systems. Rockville, MD: Computer Sccience Press, Inc.
108. 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
109. Fruhwirth, C. & Mannisto, T. (2009). Improving CVSS-based vulnerability prioritization and response with context information. *2009 3rd International Symposium on Empirical Software Engineering and Measurement, ESEM 2009 , št. članka 5314230,* (str. 535-544). Lake Buena Vista, FL: IEEE Computer Society.
110. Gal-Or, E. & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research, 16*(2), 86-208.

111. 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
112. Gardner, P. E. (1989). Evaluation of Five Risk in Aiding Management Decisions. *Computers & Security, 8*(6), 479-485.
113. Garg A., Curtis, J. & Halper, H. (2003). Quantifying the financial impact of it security breaches. *Information Management & Computer Security, 11*(2),74–83.
114. Geer, D. (2001). Return on security investment: calculating the security investment equation. *Secure Business Quarterly, 1* (2).
115. Geer, D. (2002). Making choices to show ROI. *Secure Business Quarterly, 1*(2), 1–5.
116. Geer, D. (2004a, 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
117. Geer, D. (2004b). *Security of Information When Economics Matters.* Waltham, MA: Verdasys.
118. Germain, J. M. (2005, 13. avgust). Your Next Job Title: CISO? *CIO Today*. Najdeno 14. maja 2009 na spletnem naslovu http://www.cio-today.com/story.xhtml?story_id=0320013PMOQO&page=1
119. 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
120. *Glossary of IT Terms*. Najdeno 16. februarja 2010 na spletnem naslovu http://www.seattle.gov/informationsecurity/glossary_A.htm
121. 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
122. 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.
123. Gordon, A. L. & Loeb, P. M. (2002a). Return on Information Security Investments: Myths vs. Reality. *Strategic Finance,* november 2002, 26-31.
124. Gordon, A. L. & Loeb, P. M. (2002b). The Economics of Information Security Investment. *Communications of the ACM, 5*(4), 438-457
125. 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*

126. Gordon, A. L. & Loeb, P. M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis, New York: McGraw Hill.
127. Gordon, A. L. & Loeb, P. M. (2006). Budgeting process for information security expenditures. *Communications of the ACM, 49*(1), 121–125.
128. 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
129. Gordon, A. L. (2004). *Managerial Accounting: Concepts and Empirical Evidence*, 6th edition. New York: McGraw-Hill.
130. Gordon, A. L., Loeb, P. M. & Lucyshyn, W. (2002). An economics perspective on the sharing of information related to security breaches: Concepts and empirical evidence. *Workshop on the Economics of Information Security (WEIS 2002)*. Najdeno 15. novembra 2006 na spletnem naslovu *http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/*
131. Gordon, A. L., Loeb, P. M. & Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy 22* (6).
132. 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
133. 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).
134. Hajjem, L., Benabdallah, S. & Ben Abdelaziz, F. (2010). A dynamic resource allocation decision model for IT security. *2010 2nd International Conference on Engineering System Management and Applications, ICESMA 2010* , št. članka 5542666
135. Herath, H. & Herath, T. (2006). Justifying Spam and E-mail Virus Security Investments: A Case Study. *Workshop on the Economics of Information Security (WEIS 2006).* Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html
136. Horowitz, B. & Garcia, A. (2005). A growing trend towards underinvestment in internet security. *Verdasys, Inc.* Charlottesville, Virginia: University of Virginia,
137. Housing. (2010). Upravljanje z informacijsko varnostjo. Najdeno 3. februarja 2010 na spletnem naslovu http://www.housing.si/sl/ISMS_vpeljava/
138. 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.
139. Huang, C. D., Hu, Q. & Behara S. R. (2005). In search for optimal level of information security investment in risk-averse firms. *The Third Annual Security Symposium*. Tempe, Arizona: Arizona State University.
140. Huang, C. D., Hu, Q. & Behara S. R. (2005a). Investment in information security by a riskaverse firm. *The 2005 Softwars Conference.* Las Vegas, NV.
141. Huang, C. D., Hu, Q. & Behara S. R. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks. *Workshop on the Economics of*

Information Security (WEIS 2006). Najdeno 15. novembra 2006 na spletnem naslovu http://weis2006.econinfosec.org/prog.html

142. Huang, J. W., Ding, Y. S.,& Hu, Z. H. (2008). Knowledge based model for holistic information security risk analysis. *International Symposium on Computer Science and Computational Technology, ISCSCT 2008 1, št. članka 4731381,* (str. 88-91). Shanghai: IEEE Computer Society.
143. 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.
144. *IBM ISS X-Force*. Najdeno 27. januarja 2009 na spletnem naslovu http://xforce.iss.net
145. IBM ISS. (2009). The Lifecycle of a Vulnerability. *IBM Internet Security Systems.* Najdeno 24. septembra 2009 na spletnem naslovu http://www.iss.net/Archive/Website/2009%20documents%20folder/whitepapers/ISS_Vulnerability_Lifecycle_Whitepaper.pdf
146. *iDefense*. Najdeno 28. januarja 2009 na spletnem naslovu http://labs.idefense.com
147. *Information Systems Audit and Control Association (ISACA).* Najdeno 13. oktobra 2009 na spletnem naslovu http://www.isaca.org
148. *Information Systems Security Association (ISSA)*. Najdeno 13. oktobra 2009 na spletnem naslovu http://www.issa.org
149. *Information Technology Infrastructure Library* (ITIL). Najdeno 2. februarja 2010 na spletnem naslovu http://www.itil-officialsite.com/home/home.asp
150. *Information Technology Security Evaluation Criteria (ITSEC).* (1991). Najdeno 25. marca 2010 na spletnem naslovu http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf
151. International Organization for Standardization (ISO). (1989). *ISO/IEC 7498-2:1989*. Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. Geneva: International Organization for Standardization (ISO).
152. International Organization for Standardization (ISO). (2004). *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).
153. International Organization for Standardization (ISO). (2005). *ISO/IEC 27001:2005*. Information technology - Security techniques - Information security management systems – Requirements. Geneva: International Organization for Standardization (ISO).
154. International Organization for Standardization (ISO). (2005). *ISO/IEC 17799:2005*. Information technology - Security techniques - Code of practice for information security management. Geneva: International Organization for Standardization (ISO).

155. International Organization for Standardization (ISO). (2005). *ISO/IEC 27002:2005*. Information technology - Security techniques - Code of practice for information security management. Geneva: International Organization for Standardization (ISO).
156. International Organization for Standardization (ISO). (2007). *ISO/IEC 27006:2007*. Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. Geneva: International Organization for Standardization (ISO).
157. International Organization for Standardization (ISO). (2008). *ISO/IEC 9001:2008*. Quality management systems – Requirements. Geneva: International Organization for Standardization (ISO).
158. International Organization for Standardization (ISO). (2008). *ISO/IEC 15408:2008*. Information technology - Security techniques - Evaluation criteria for IT security. Geneva: International Organization for Standardization (ISO).
159. International Organization for Standardization (ISO). (2008). *ISO/IEC 21827:2008*. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM). Geneva: International Organization for Standardization (ISO).
160. International Organization for Standardization (ISO). (2008). *ISO/IEC 27005:2008*. Information technology - Security techniques - Information security risk management. Geneva: International Organization for Standardization (ISO).
161. International Organization for Standardization (ISO). (2008). *ISO/IEC 27011:2008*. Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Geneva: International Organization for Standardization (ISO).
162. International Organization for Standardization (ISO). (2009). *ISO/IEC Guide 73:2009*. Risk management – Vocabulary. Geneva: International Organization for Standardization (ISO).
163. International Organization for Standardization (ISO). (2009). *ISO/IEC 27000:2009*. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Geneva: International Organization for Standardization (ISO).
164. International Organization for Standardization (ISO). (2009). *ISO/IEC 27004:2009*. Information technology - Security techniques - Information security management - Measurement. Geneva: International Organization for Standardization (ISO).
165. *International Organization for Standardization (ISO)*. Najdeno 27. marca 2008 na spletnem naslovu http://www.iso.org
166. Internet Engineering Task Force (IETF). (1992). *RFC 1321*. The MD5 Message-Digest Algorithm. Najdeno 10. november 2009 na spletnem naslovu www.ietf.org/rfc/rfc1321.txt
167. Internet Engineering Task Force (IETF). (1993). *RFC 1510*. The Kerberos Network Authentication Service (V5). Najdeno 10. november 2009 na spletnem naslovu www.ietf.org/rfc/rfc1510.txt

168. Internet Engineering Task Force (IETF). (1997). *RFC 2104.* HMAC: Keyed-Hashing for Message Authentication. Najdeno 24. marca 2010 na spletnem naslovu www.ietf.org/rfc/rfc2104.txt
169. Internet Engineering Task Force (IETF). (1997). *RFC 2196*. Site Security Handbook. Najdeno 10. november 2009 na spletnem naslovu www.ietf.org/rfc/rfc2196.txt
170. Internet Engineering Task Force (IETF). (1999). *RFC 2459*. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Najdeno 10. november 2009 na spletnem naslovu www.ietf.org/rfc/rfc2459.txt
171. Internet Engineering Task Force (IETF). (2004). *RFC 3850*. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling. Najdeno 10. november 2009 na spletnem naslovu www.ietf.org/rfc/rfc3850.txt
172. *Internet Engineering Task Force (IETF)*. Najdeno 13. oktobra 2009 na spletnem naslovu http://www.ietf.org
173. *Internet Security Alliance (ISA)*. Najdeno 13. oktobra 2009 na spletnem naslovu http://www.isalliance.org
174. 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.
175. Irvine, C. E., Thompson, M. F. & Allen, K. (2005). CyberCIEGE: Gaming for information assurance. *IEEE Security and Privacy Magazine* (maj-junij), 61-64.
176. ISF. (2006). The Standard of Good Practice for Information Security. *Information Security Forum*. Najdeno 21. novembra 2006 na spletnem naslovu: http://www.isfsecuritystandard.com/index_ns.htm
177. *Islovar* (*slovar informatike).* Najdeno 17. februarja 2010 na spletnem naslovu http://www.islovar.org/iskanje_enostavno.asp
178. *ISO27001 Security.* Najdeno 18. maja 2009 na spletnem naslovu http://www.iso27001security.com
179. Jacobson, R. V. (2000). What is a rational goal for security? *Security Management, 44*(12), 144-151.
180. 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
181. 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.
182. Knüsel, L. (2005). On the Accuracy of Statistical Distributions in Microsoft Excel 2003. *Computational Statistics and Data Analysis (CSDA), 48*, 445-449.
183. Landwehr, C. E., Bull, A. R., McDermott, J. P. & Choi, W. S. (1994). A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys (CSUR), 26*(3), 211-254.

184. Lewis, N. (1990).Workshop framework response. *The 3rd International Computer Security Risk Management Model Builders Workshop.* Santa Fe: National Institute of Standards and Technology (NIST).
185. Lindqvist, U. & Jonsson, E. (1997). How to systematically classify computer security intrusions. *IEEE Symposium on Security and Privacy* (str. 154 –163). Oakland, CA: IEEE Computer Society.
186. Lipmann, R., Haines, J. W., Fried, D. J., Korba, J. & Das, K. (2000). The 1999 DARPA off-line Intrusion Detection Evaluation. *Computer Networks: The International Journal of Computer and Telecommunications Networking, 34*(4), 579-595.
187. 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
188. Longstaff, T. A., Chittister, C., Pethia, R. & Haimes, Y. Y. (2000). Are We Forgetting the Risks of Information Technology? *Computer, 33*(12), 43-51.
189. 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.
190. 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
191. 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
192. McClure, S., Scambray, J., Kurtz, G. (2001). *Hacking Exposed*, Third Edition. New York: McGraw-Hill
193. McGhie, L. (2003). Software patch management - the new frontier. *Secure Business Quarterly, 3*(2), 1-4.
194. *Mehari (Information risk analysis and management methodology)*. Najdeno 24. septembra 2009 na spletnem naslovu http://www.clusif.asso.fr/en/production/mehari/
195. Mehr, R. I. & Hedges, B. A. (1974). *Risk Management: Concepts and Applications.* Homewood, Illinois: Richard D. Irwin, Inc.
196. Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM, 46*(6), 15–18.
197. *Metasploit*. Najdeno 29. januarja 2009 na spletnem naslovu http://www.metasploit.com
198. Microsoft. (2004). *Microsoft Security Risk Management Guide*. Najdeno 14. marca 2007 na spletnem naslovu

http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx.

199. *Milw0rm*. Najdeno 27. januarja 2009 na spletnem naslovu http://www.milw0rm.com
200. Mizzi, A. (2005). Return on Information Security Investment. Are you spending enough? Are you spending too much? Najdeno 14. oktobra 2008 na spletnem naslovu http://www.infosecwriters.com/text_resources/pdf/ROISI.pdf
201. 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
202. National Institute of Standards and Technology (NIST). (1995). *NIST Special Publication 800-12*. An Introduction to Computer Security: The NIST Handbook. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsSPs.html
203. National Institute of Standards and Technology (NIST). (1996). *NIST Special Publication 800-14*. Generally Accepted Principles and Practices for Securing Information Technology Systems. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsSPs.html
204. National Institute of Standards and Technology (NIST). (2001). *Federal Information Processing Standards (FIPS) publication 197.* Advanced Encryption Standard. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsFIPS.html
205. National Institute of Standards and Technology (NIST). (2002). *NIST Special Publication 800-30*. Risk Management Guide for Information Technology Systems. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsSPs.html
206. National Institute of Standards and Technology (NIST). (2004). *Federal Information Processing Standards (FIPS) publication 199*. Standards for Security Categorization of Federal Information and Information Systems. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsFIPS.html
207. National Institute of Standards and Technology (NIST). (2004). *NIST Special Publication 800-27*. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsSPs.html
208. National Institute of Standards and Technology (NIST). (2008). *Federal Information Processing Standards (FIPS) publication 180-3*. Secure Hash Standard. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsFIPS.html
209. National Institute of Standards and Technology (NIST). (2008). *NIST Special Publication 800-60*. Mapping Types of Information and Information Systems to Security Categories. Najdeno 16. aprila 2009 na spletnem naslovu http://csrc.nist.gov/publications/PubsSPs.html

210. *National Institute of Standards and Technology (NIST)*. Najdeno 16. aprila 2009 na spletnem naslovu http://www.nist.gov
211. Needham R. & M. Schroeder. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM, 21*(12), 993 - 999
212. Nemzow, M. (1997). Business Continuity Planning. *International Journal of Network Management, 7*(3), 127-136.
213. Neumann, P. G. & Parker, D. B. (1989). A Summary of Computer Misuse Techniques. *The 12th National Computer Security Conference* (str. 396-407). Baltimore, Maryland: National Institute of Standards and Technology (NIST).
214. Neumann, P. G. (2000). *Computer-Related Risks*. Boston: Addison-Wesley.
215. *NLB*. Najdeno 24. novembra 2009 na spletnem naslovu http://www.nlb.si/obrestne-mere
216. Ogut, H., Menon, N. & Ragunathan, S. (2005). Cyber insurance and IT security investment: Impact of independent risk. *Workshop on the Economics of Information Security (WEIS 2005).* Najdeno 15. novembra 2006 na spletnem naslovu http://infosecon.net/workshop/schedule.php
217. Orlandi, E. (1989). Computer Security Economics. ICCST (str. 107-111). Zurich: IEEE.
218. Ozment, A. (2004). Bug auctions: Vulnerability markets reconsidered. *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
219. *Packetstorm*. Najdeno 28. januarja 2009 na spletnem naslovu http://www.packetstormsecurity.org
220. Palsit. (2005). *Prevod standarda BS ISO/IEC 27001:2005*. Information technology - Security techniques - Information security management systems – Requirements. Šempeter pri Gorici: Palsit.
221. Palsit. (2005). *Prevod standarda BS ISO/IEC 27002:2005*. Information technology - Security techniques - Code of practice for information security management. Šempeter pri Gorici: Palsit.
222. Palsit. (2010). O podjetju. Najdeno 3. februarja 2010 na spletnem naslovu http://www.palsit.com/slo/podjetje.php
223. Parker, B. D. (2009). Toward a New Framework for Information Security. V S. Bosworth, M.E.Kabay & E. Whyne (ur.), *The Computer Security Handbook*, 5th edition. New York: John Wiley & Sons
224. Paxson, V. (1998). Bro: A system for detecting network intruders in real-time. The *7th Usenix Security Symposium*. San Antonio, Texas.
225. Peltier, T. (2001). *Information Security Policies, Procedures & Standards.* Boca Raton, FL: Auerbach Publications.
226. Peltier, T. (2005). *Information Security Risk Analysis* (2nd edition). Boca Raton, FL: Auerbach Publications.
227. Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

228. Pfleeger, C. P. (1997). *Security in Computing*. Upper Saddle River, New Jersey: Prentice Hall.
229. Poore, R. S. (2000). Valuing information assets for security risk management. *Information Systems Security, 9*(4), 13–23.
230. Power, R. (1999, oktober). CSI special report: How to quantify financial losses from inforsec breaches. Computer Security Institute, Alert newsletter (št. 199), str. 1 in 12.
231. Pritchard, J. (1978). *Risk Management in Action*. Manchester: NCC Publications.
232. Purcell, J. (2007, 12. februar). Security Control Types and Operational Security. *GIAC Research in The Common Body of Knowledge.* Najdeno 18.aprila 2007 na spletnem naslovu http://www.giac.org/resources/whitepaper/operations/207.php
233. Qi, Y., Wang, Y. & Li, D. (2009). Measuring performance of Chinese corporate social responsibility by information management and modeling for investment analysis. *4th International Conference on Cooperation and Promotion of Information Resources in Science and Technology*, COINFO 2009, *št. članka* 5361833, (str. 122-126). Lake Buena Vista, FL: IEEE Computer Society
234. Rasmusen, E. (1998). *Games and Information*. Malden: Blackwell Publishers.
235. Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot: Ashgate Publishing Ltd.
236. 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
237. 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.
238. 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
239. Rue, R., Pfleeger, S. & Ortiz, D. (2007). A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. *Workshop on the Economics of Information Security (WEIS 2007).* Najdeno 25.septembra 2007 na spletnem naslovu http://weis07.infosecon.net/program.htm
240. Rues, R. (2003). Corporate Open Source Information Leakage. *Infocon magazine, Issue 1*. Najdeno 27. marca 2008 na spletnem naslovu http://www.iwar.org.uk/infocon/corporate-open-source.htm
241. Ruge-Murcia J. F. (2001). The inflation bias when the central bank targets the natural rate of unemployment. *Elsevier, 48*(1), 91-107.
242. Ruge-Murcia J. F. (2003). Inflation targeting under asymmetric preferences. *Journal of Money, Credit, and Banking, 35*(5), 763-785.

243. Sandhu, R. (2003). Good-Enough Sercurity: Toward a Pragmatic Business-Driven Discipline. *IEEE Internet Computing, 5*(3), 66-68.

244. Santos, J. R. & Haimes, Y. Y. (2004). *Modeling the demand reduction inputoutput (I-O) inoperability due to terrorism of interconnected infrastructures*. Charlottesville, Virginia: University of Virginia.

245. Schechter, S. & Smith, M. (2003). How Much Security is Enough to Stop a Thief? *Financial Cryptography* (str. 73–87). Berlin Heidelberg: Springer Verlag.

246. Schechter, S. (2002). Quantitatively differentiating system security. *Workshop on the Economics of Information Security (WEIS 2002)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/

247. Schechter, S. (2004). *Computer Security Strength & Risk: A Quantitative Approach.* Cambridge, Massachusetts: Harvard University.

248. Schneier, B. (1996). *Applied Cryptography, Second Edition.* New York: John Wiley & Sons, Inc.

249. Schneier, B. (2001). Insurance and the Computer Industry. *Communications of the ACM, 44*(3), 114-115.

250. Schneier, B. (2002a). Network Monitoring and Security. *Counterpane Internet Security, Inc*. Najdeno 19. junija 2007 na spletnem naslovu http://bt.counterpane.com/presentation3.pdf

251. Schneier, B. (2002b). No, We Don't Spend Enough. *Workshop on the Economics of Information Security (WEIS 2002)*. Najdeno 15. novembra 2006 na spletnem naslovu http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/

252. Schneier, B. (2003). *Beyond Fear: Think Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

253. Schneier, B. (2004a). *Secrets & Lies, Digital Security in a Networked World.* New York: Wiley Publishing.

254. Schneier, B. (2004b). Security and Complaince. *IEEE Security and Privacy, 2*(3), 96.

255. Schneier, B. (2004c). Evaluating Security Systems: A Five-step Process. V J. Camp & R. Lewis (ur.), *Economics of Information Security* (str. 289-293). Heidelberg: Springer.

256. *Secunia*. Najdeno 28. januarja 2009 na spletnem naslovu http://secunia.com

257. *SecurityFocus*. Najdeno 27. januarja 2009 na spletnem naslovu http://www.securityfocus.com

258. *SecurityTracker*. Najdeno 27. januarja 2009 na spletnem naslovu http://www.securitytracker.com

259. *SecurityVulns*. Najdeno 27. januarja 2009 na spletnem naslovu http://securityvulns.com

260. Shapiro, C. & Varian H. (1998). *Information Rules.* Boston: Harvard Business School Press.

261. Sheen, J.N. (2010a). Information security investment decision-making based on fuzzy economics. *WSEAS Transactions on Systems, 9*(6), 669-678
262. Sheen, J.N. (2010b). Information security investment decision by fuzzy economic. *3rd International Conference on Information Sciences and Interaction Sciences, ICIS 2010*, št. članka 5534680, 648-653.
263. Shostack, A. (2003). Quantifying patch management. *Secure Business Quarterly, 3*(2), 1-4.
264. Siemens, Insight Consulting. (2003). *CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0*. Milton Keynes: Siemens.
265. Singh, S. (2006). *Knjiga šifer.* Tržič: Učila international.
266. 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.palsit.com/slo/podjetje.php
267. Skogan, W. G. & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions.* Beverly Hills: Sage Publications.
268. Smith, E.H. & Kruger, H.A. (2010). A framework for evaluating IT security investments in a banking environment. *The 2010 Information Security for South Africa Conference, ISSA 2010* , št. članka 5588343
269. 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.
270. Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach To Computer Security*. Palo Alto, CA: Stanford University.
271. Soo Hoo, K. J., Sudbury, A. W. & Jaquith, A. R. (2001). Tangible ROI through secure software engineering. *Secure Business Quarterly: Special Issue on Return on Security Investment, 1*(2).
272. Sookdawoor, O. (2005). *An Investigation of Information Security Policies and Practices in Mauritius.* Unisa, South Africa: University of South Africa.
273. Stalling, W. (1999). *Network Security Essentials.* Upper Saddle River, New Jersey Prentice: Hall.
274. Standards Association of Australia. (2004). *AS/NZS 4360*. Risk Management. Strathfield: Standards Association of Australia.
275. 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.
276. Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255 - 273.
277. 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

278. 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.

279. Sunzi. (2009). *Umetnost vojne*. Ljubljana: Mladinska knjiga.

280. 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

281. 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

282. Symantec Corporation. (2007, 19. marec). Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain. *Symantec Corporation*. Najdeno 12. septembra 2008 na spletnem naslovu: http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01

283. Symantec Corporation. (2009). Latest Virus Threats. *Symantec Corporation.* Najdeno 24. avgusta 2009 na spletnem naslovu: http://www.symantec.com/business/security_response/threatexplorer/threats.jsp

284. 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.

285. 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

286. 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.

287. Tarr, C. J. (1995). Cost effective perimeter security. *European Convention on Security and Detection* (str. 183 –187). Brighton: IEEE.

288. Taylor, S. & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570.

289. *The SANS (SysAdmin, Audit, Network, Security) Institute Online*. Najdeno 16. aprila 2009 na spletnem naslovu http://www.sans.org

290. *TippingPoint*. Najdeno 29. januarja 2009 na spletnem naslovu http://tippingpoint.com

291. Tordoff, P. (2006). UK Information Security Breaches Survey. *ENISA quarterly, 2*(2). 15-17,

292. Tudor, J. K. (2000). *Information Security Arcitecture – An Integrated Approach to Security in the Organization.* New York: Auerbach.

293. Turn, R. (1986). Security and Privacy Requirements in Computing. *ACM Fall Joint Computer Conference* (str. 1106-1114). Dallas: ACM.

294. Varian, H. R. (1997). How to build an economic model in your spare time. V M. Szenberg (ur.), *Passion and Craft: Economists at Work* (str. 256-271). Michigan: University of Michigan Press.

295. Varian, H. R. (2000, 1. junij). Managing online security risks. *The New York Times*.

296. *Vupen*. Najdeno 27. januarja 2009 na spletnem naslovu http://www.vupen.com/english

297. Wang, H. J., Guo, C., Simon, D. R. & Zugenmaier, A. S. (2004). Shield: Vulnerability-driven networkfilters for preventing known vulnerability exploits. ACM *SIGCOMM Computer Communication Review, 34*(4), 193-204.

298. 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.

299. Whitman, E. M. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, 46*(8), 91-95.

300. Wikipedia. (2008). Morris worm. Najdeno 27. maja 2008 na spletnem naslovu http://en.wikipedia.org/wiki/Morris_worm

301. Wikipedia. (2009a). Back Orifice. Najdeno 9. januarja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/Back_Orifice

302. Wikipedia. (2009b). Basel II Accord. Najdeno 15. maja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/Basel_II_Accord

303. Wikipedia. (2009c). Gramm-Leach-Bliley Act (GLBP). Najdeno 15. maja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act

304. Wikipedia. (2009d). Health Insurance Portability and Accountability Act (HIPAA). Najdeno 15. maja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

305. Wikipedia. (2009e). Sarbanes-Oxley (SOX). Najdeno 15. maja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/Sarbanes-Oxley

306. Wikipedia. (2010). Informacijska varnost. Najdeno 3. februarja 2010 na spletnem naslovu http://sl.wikipedia.org/wiki/Informacijska_varnost

307. 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

308. 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

309. Wong, K. & Watt, S. (1990). *Managing Information Security: A Non-technical Management Guide*. Maryland Heights: Elsevier Advanced technology.

310. Wood, C. C., et. al. (1987). *Computer Security; A comprehensive Control Checklist*. New York: John Wiley & Sons.

311. *Workshop on the Economics of Information Security (WEIS).* Najdeno 10. decembra 2006 na spletnem naslovu http://www.infosecon.net

312. 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.

313. Yener, B. (2003). Internet Security. V J. G. Proakis (ur.), *Encyclopedia of Telecommunications, Vol 2* (str. 1152-1157). New York: John Wiley and Sons.

314. Young, A. & Yung, M. (1996). Cryptovirology: Extortion-based security threats and countermeasures. *The IEEE Symposium on Security and Privacy* (str. 129–140). Washinghton, DC: IEEE Computer Society

315. Zoric, J., Helme, A., Kvalheim, H. & Sundve, E. (objava v letu 2010). Justifying Information Security Investments in Web Software (Quantitative techno-business modeling approach). *Future Network & Mobile Summit 2010*. Florence: European Commission and eMobility