Kvantitativni model za upravljanje informacijskovarnostnih tveganj

Rok Bojanc
ZZI, d. o. o., Pot k sejmišču 33, 1231 Ljubljana Črnuče
rok.bojanc@zzi.si; http://www.zzi.si

Izvleček

Upravljanje informacijskovarnostnih tveganj postaja čedalje bolj pomemben proces v sodobnem poslovanju podjetij. Predlagani model za upravljanje informacijskovarnostnih tveganj temelji na kvantitativni analizi varnostnih tveganj, kar omogoča organizacijam vpeljavo optimalnih varnostnih rešitev. Model je zasnovan kot standardni postopek, ki organizacijo vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro ustrezne rešitve, ki zmanjšuje določeno varnostno tveganje. Pri analizi varnostnih tveganj model kvantitativno ovrednoti informacijska sredstva organizacije, njihove ranljivosti ter grožnje, ki pretijo informacijskim sredstvom. Vrednosti parametrov tveganja so podlaga za izbiro ustrezne obravnave tveganja in vrednotenje različnih varnostnih ukrepov, ki zmanjšujejo varnostna tveganja. Za posamezen varnostni ukrep določimo kazalnike donosnosti, ki omogočajo primerjavo različnih varnostnih ukrepov. Pri tem so vključene možnosti investicije v tehnološke varnostne rešitve, uvedbe organizacijskih postopkov, izobraževanja ter prenos tveganja na zunanjega izvajalca ali zavarovalnico. Model je bil preverjen z različnimi praktičnimi izračuni iz realnega poslovnega okolja.

Ključne besede: informacijska varnost, upravljanje tveganja, ocena tveganja, sistem upravljanja informacijske varnosti, kvantitativno vrednotenje, optimalna investicija.

Abstract

Quantitative Model for Information Security Risk Management

Information security risk management is becoming increasingly important process in modern businesses. The proposed model for managing information security risks is based on quantitative analysis of security risks, which enables organizations to introduce optimal security solutions. The model is designed as a standard procedure leading the organization from the initial input data selection to the final recommendations for the selection of appropriate solutions, which reduces a certain security risk. In the process of analyzing the security risks the model quantitatively evaluates the information assets, their vulnerability and threats to information assets. The values of risk parameters are the basis for selecting appropriate risk treatment and for evaluating of various security measures that reduce security risks. Economic indicators are determined for each security measure so as to compare of various security measures to each other. This includes the possibility of investment in technology security solutions, the introduction of organizational procedures, training and transfer of risk to an outsourcing provider or to the insurance agency. The model was tested using empirical examples with data from real business environment.

Keywords: information security, risk management, risk assessment, information security management system, quantitative evaluation, optimal investment.

1 UVOD

Danes podjetja poslujejo hitreje, učinkoviteje in ceneje kot kadar koli. Pri tem pomembno vlogo igrajo sodobne informacijske tehnologije, ki podpirajo njihove poslovne procese. 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. Obenem pa smo priča razmahu novih groženj in nevarnosti za poslovanje podjetij. Negativne posledice mogočega napada na informacijske sisteme so lahko velike in v nekaterih primerih lahko privedejo celo do stečaja podjetja.

Informacijski varnosti v preteklosti niso posvečali 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 bil internet zaprto omrežje, ki je povezovalo le določene izbrane organizacije in ustanove. Zato

tudi ni bilo posebne potrebe po varnosti in načrtovalci omrežij se z 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 & Jerman-Blažič, 2008).

Da se podjetja zavarujejo pred grožnjami, ki pretijo njihovim informacijskim sistemom, morajo vzpostaviti varnostne mehanizme, ki varujejo njihov informacijski sistem. Za uspešno izvedbo varnostnih strategij je ključno, da podjetje pozna grožnje, ki pretijo sredstvom v njihovem podjetju. Obenem se mora podjetje odločiti, katera informacijska sredstva želi varovati pred grožnjami ter v kolikšnem obsegu jih želi varovati. Pogosta varnostna tveganja v podjetju so npr. odpoved delovanja storitev, izguba ali kraja podatkov, nepooblaščen vpogled v podatke ali nepooblaščeno spreminjanje podatkov.

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, postavljali infrastrukture javnih ključev (angl. Public Key Infrastructure, PKI), izboljševali požarne pregrade itd. Raziskovalci s področja informacijske varnosti pa čedalje bolj opozarjajo, da tak pristop ne zadostuje. Informacijska varnost je namreč področje, ki se ga ne da uspešno rešiti zgolj s tehnologijo, temveč je treba upoštevati tudi ekonomski pogled (Anderson & Schneier, 2005). Podjetja, ki upoštevajo ta pogled, se tako pri odpravi mogočih težav na področju informacijske varnosti osredinjajo na to, kar je ekonomsko optimalno, namesto na to, kar je tehnično mogoče (Schneier, 2004). Ko na informacijsko varnost gledamo z ekonomskega vidika, lahko dobimo odgovore na mnoga vprašanja, na katera ne more zadovoljivo odgovoriti samo tehnologija. Taka varnostna vprašanja so npr.: Kako lahko podjetje postane varno? Katera stopnja varnosti je ustrezna? Koliko denarja naj podjetje investira v varnost? Ali podjetje vlaga dovolj denarja, da hekerjem preprečuje vdor v računalniški sistem? Ali podjetje vlaga preveč? Ali podjetje ustrezno vlaga sredstva za varnost?

Uporaba ekonomskega pristopa k obvladovanju varnostnih tveganj omogoča podjetjem vpeljavo optimalnih varnostnih rešitev. Podjetja lahko tako ocenijo posledice, ki nastanejo zaradi neuvedbe določene varnostne rešitve, ter ocenijo, katera izmed rešitev, ki jih imajo na voljo, ima najboljše razmerje med ceno in kakovostjo. Vodstvenim kadrom z dobrim poznavanjem prava in ekonomije predstavlja uporaba ekonomskega izrazoslovja boljše razumevanje problema kot pa tehnični jezik informacijske varnosti. Menedžerji lahko tako bolje razumejo investicije v varnostne rešitve, ker je povzročena škoda ob varnostnih incidentih predstavljena kot finančna izguba.

K uveljavitvi ekonomskega pogleda na informacijsko varnost je pomembno prispevalo zavedanje, da je treba na informacijsko varnost gledati kot na investicijo in ne samo kot na strošek. Ravno varno informacijsko okolje ustvarja dodano vrednost za podjetje in njegove partnerje. Enega izmed prvih okvirov analitičnega odločanja za ocenjevanje različnih politik informacijske varnosti je predstavil Soo Hoo (2000). Gordon in Loeb (2002) sta predstavila ekonomski model za oceno optimalne investicije v informacijsko varnost, ki temelji na izenačevanju mejnih finančnih koristi informacijske varnosti in mejnih finančnih stroškov zaščite. Butler (2002) predlaga metodo analize stroškov in koristi za primerjavo alternativnih varnostnih rešitev z že uvedenimi rešitvami in tako preverja, ali je mogoča bolj stroškovno učinkovita rešitev. Ryan in Ryan (2006) zagovarjata, da se korist investicije meri kot razlika med pričakovano izgubo v primeru investiranja in neinvestiranja. Bojanc in Jerman-Blažič (2008) sta predstavila izhodišča za ekonomski pristop k modeliranju upravljanja z informacijsko varnostnimi tveganji. Na teh izhodiščih so Bojanc, Jerman-Blažič in Tekavčič (2012) predstavili splošen matematični model za kvantitativno vrednotenje investicij v različne varnostne ukrepe in iskanje optimalne varnostne rešitve. Alternativna metoda, ki poskuša analizirati vlaganja v informacijsko varnost, je t. i. teorija iger (Cavusoglu, Mishra & Raghunathan, 2004). Avtorji trdijo, da tradicionalni odločitveno-analitični pristopi za vrednotenje informacijskotehnoloških investicij v varnost obravnavajo varnostne tehnologije kot črno škatlo in ne upoštevajo, da se investicija v informacijsko varnost razlikuje od drugih splošnih informacijskotehnoloških 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, pri čemer ima napadalec motiv za napad in povzroči podjetju določeno škodo. 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: 86) sta z uporabo teorije iger poiskala, kolikšni so stroški in koristi izmenjave informacij o varnostnih incidentih.

Predstavljeni model podpira analitičen pristop reševanja problematike informacijskovarnostnih tveganj, pri čemer uporablja kvantitativno vrednotenje parametrov tveganja. Prednost takega pristopa je, da omogoča vrednotenje različnih obravnav tveganja in medsebojno primerjavo različnih vrst varnostnih ukrepov. Ti ukrepi so lahko tehnološke rešitve, organizacijski ukrepi, izobraževanja, zavarovanje, zunanje izvajanje storitev ter drugi. Rezultat modela so priporočila, kateri izmed predlaganih ukrepov je najbolj ustrezen za uvedbo v podjetju. Članek povzema matematično formulacijo teoretičnega modela za iskanje optimalnih investicij v informacijsko varnost (Bojanc, Jerman-Blažič & Tekavčič, 2012), vendar je ustrezno prirejen in poenostavljen za preprostejšo uporabo v podjetjih. Obenem pa daje članek večji poudarek samemu procesu upravljanja informacijskovarnostnih tveganj.

Članek je sestavljen iz petih razdelkov. Uvodu, v katerem je na kratko predstavljena problematika informacijske varnosti, sledi predstavitev upravljanja varnostnih tveganj, ki je glavni proces upravljanja sistema informacijske varnosti. V tretjem razdelku je predstavljen matematični model za upravljanje varnostnih tveganj. Model je zasnovan kot standarden postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro optimalnega ukrepa, ki zmanjšuje določeno varnostno tveganje. Četrti razdelek vsebuje rezultate praktičnega izračuna, s katerim na podlagi realnih podatkov preverjamo ustreznost in pravilnost modela. Četrtemu razdelku sledi sklep.

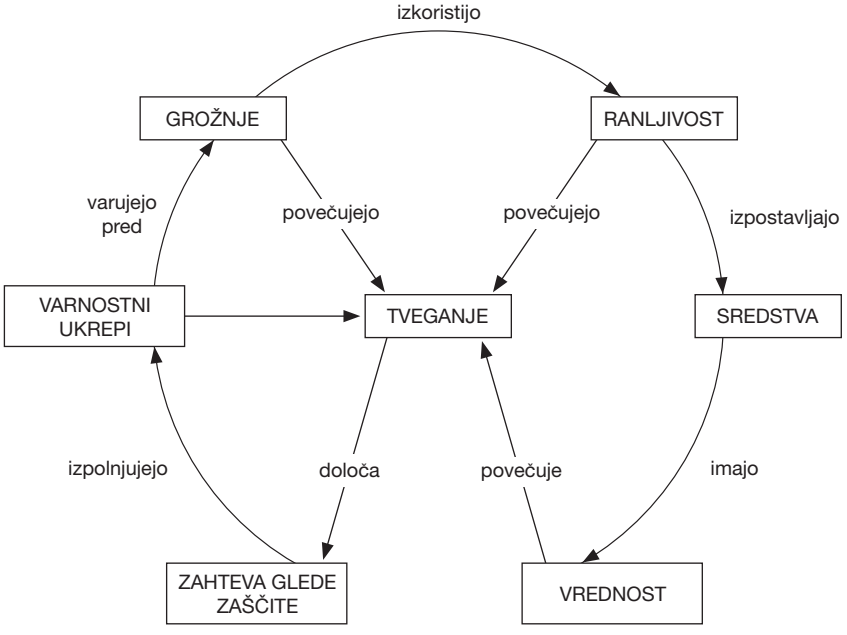
2 UPRAVLJANJE VARNOSTNIH TVEGANJ

Kako varen je informacijski sistem? Kako varen bi moral biti? To sta vprašanji, ki si jih strokovnjaki na področju varovanja informacij neprenehoma zastavljajo. Preprost odgovor na vprašanje, kakšno stopnjo varnosti želimo imeti, je: dovolj dobro varnost (Sandhu, 2003). Žal pa je zelo težko določiti, kaj je dovolj dobro (Geer, 2004). Popolno varnost lahko razumemo kot stopnjo varnosti, ki je sprejemljiva za podjetje (Schneier, 2003). To stopnjo podjetje lahko ugotovi s pomočjo upravljanja tveganj.

Upravljanje informacijske varnosti temelji na obvladovanju varnostnih tveganj. Tveganje je v splošnem opredeljeno kot kombinacija verjetnosti, da se zgodi neželen dogodek, in negativnih posledic, ki lahko nastanejo pri tem (ISO Guide 73, 2002). Na področju informacijske varnosti tveganje lahko natančneje opredelimo kot možnost, da bo določena grožnja izkoristila ranljivosti sredstva ali skupino sredstev ter povzročila škodo podjetju (ISO/IEC 27000, 2009). Tveganje je tako kombinacija grožnje in ranljivosti informacijskega sredstva, kar pripelje do negativnega učinka, ki škoduje enemu ali več informacijskim sredstvom. Grožnje in ranljivosti so del vzroka tveganja, učinek pa je posledica tveganja (Mayer idr., 2007). Npr. heker uporabi socialni inženiring na zaposlenem (tj. grožnjo), kar zaradi slabe ozaveščenosti zaposlenih (tj. ranljivosti) pripelje do neavtoriziranega dostopa do računalnikov in izgube zaupnosti ter celovitosti občutljivih informacij (tj. učinka oz. posledice).

Upravljanje 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. 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 varnostne rešitve. Upravljanje tveganja uvaja glavne varnostne elemente: sredstva, grožnje, ranljivosti, tveganja in ukrepe. Slika 1 prikazuje odvisnosti med varnostnimi elementi, ki sodelujejo pri upravljanju s tveganjem.

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 dodatna vrsta tveganja. Proces upravljanja s tveganjem je sestavljen iz posameznih faz, preko katerih lahko identificiramo ranljivosti informacijskega sistema v podjetju, ovrednotimo trenutno mogoče varnostne zaščite, sprejmemo odločitve



Slika 1: **Povezave med elementi, ki sodelujejo pri upravljanju s tveganjem** (Vir: ISO 13335-1, 2004)

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.

Obstaja veliko različnih načinov za obvladovanje tveganja. Katerega bomo izbrali v danih okoliščinah, je odvisno od podrobnosti le-teh. Za upravljanje s tveganji je na voljo veliko različnih metodologij in tehnik. ENISA (2009) med najbolj priljubljene metode in tehnike uvršča EBIOS, MEHARI, OCTAVE, CRAMM, CORAS, FRAP in IAM. Metode in tehnike za ocenjevanje tveganja lahko razdelimo v dve glavni kategoriji: kvantitativne in kvalitativne. Oba pristopa imata svoje prednosti in slabosti (Bojanc & Jerman-Blažič, 2008).

Kvantitativna metoda 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 uresniči tveganje. Ključna prednost kvantitativne metode je, da podpira analizo stroškov in koristi ter da so rezultati predstavljeni tako, ki ga razume vodstvo. Po drugi strani pa kvantitativni pristop običajno zahteva poglobljeno in obsežno raziskavo o grožnjah, sistemu in podjetju, da lahko določimo numerične vrednosti za verjetnosti in stroške. Največja težava kvantitativnega pristopa je pomanjkanje dobrih statističnih oz. zgodovinskih podatkov, ki so potrebni za oceno parametrov tveganja. Statistični podatki so običajno razpoložljivi za tveganja, pri katerih so grožnje naravne nesreče (npr. potres, poplava). Precej težje pa je pridobiti statistične podatke za človeške grožnje.[1]

Kvalitativni pristop poskuša izraziti vrednost sredstev, pričakovano izgubo in stroške uvedbe zaščite v opisnih spremenljivkah, kot so »visoka«, »srednja« ali »nizka«. Pristop zagovarja načelo, da posledic nekaterih vrst izgub (npr. okvare ali spremembe podatkov) ni mogoče izraziti z denarnimi vrednostmi. Kvalitativne metode lahko izvedemo v krajšem času z manjšim številom osebja, pri čemer jih običajno izvajamo v kombinaciji vprašalnikov in

[1] Eden od razlogov je, da večina podjetij sistematično ne odkriva, nadzira in zapisuje varnostnih incidentov. Drugi razlog je, da podjetja, ki doživijo napad, o tem pogosto raje molčijo, kot da bi objavile napad. V primeru javnega razkritja varnostnega incidenta lahko tvegajo zmanjšanje svojega ugleda, izgubo zaupanja strank ali – kar je še huje – razkrivajo svoje ranljivosti drugim hekerjem. Zato veliko resnih varnostnih incidentov ni nikoli objavljenih (Bojanc & Jerman-Blažič, 2008). V zadnji raziskavi CSI (2010) je bilo kljub anonimnosti raziskave le 25 odstotkov sodelujočih pripravljenih razkriti podrobnosti o finančnih izgubah, ki so jih utrpeli.

skupnih delavnic. Največji prednosti kvalitativnega pristopa sta porabljeni čas in strošek za izvedbo ocene. Slabost kvalitativnega pristopa je splošnost in netočnost rezultatov, ki so posledica relativnih vrednosti vhodnih podatkov. Običajno je za manjša podjetja z omejenimi človeškimi viri primernejši kvalitativni pristop.

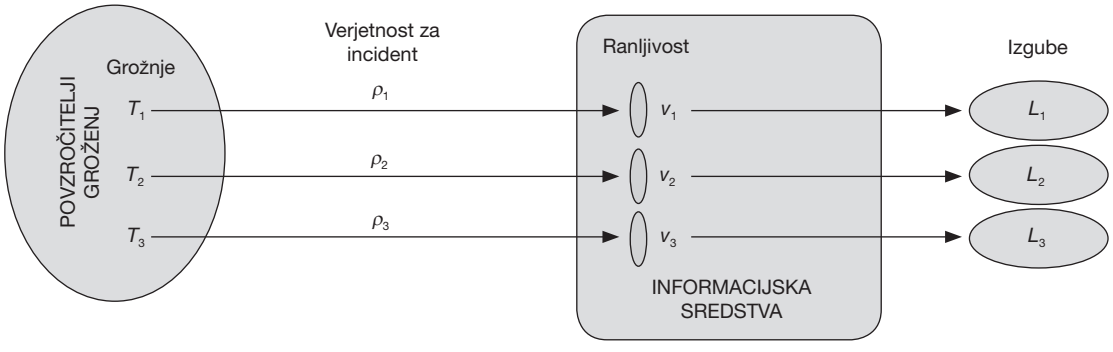
3 MODEL UPRAVLJANJA INFORMACIJSKOVARNOSTNIH TVEGANJ

Za učinkovito upravljanje tveganj informacijske varnosti je uporabljen matematični model, ki uporablja kvantitativni pristop (Bojanc, Jerman-Blažič & Tekavčič, 2012). Model je sestavljen iz štirih faz. Prva faza je ocena tveganja, v kateri za vsako informacijsko sredstvo določimo ter ovrednotimo ranljivosti in grožnje, verjetnost za nastanek incidenta ter izgube v primeru varnostnega incidenta. Druga faza je obravnava tveganja, pri čemer za vsako ovrednoteno tveganje določimo ustrezno obravnavo tveganja glede na njene kvantitativne parametre. Tretja faza je izbira in vrednotenje varnostnih ukrepov ter ocena njihovega učinka na zmanjšanje tveganja. Zadnja faza pomeni medsebojno primerjavo varnostnih ukrepov in ekonomsko analizo donosnosti posameznega ukrepa.

3.1 Ocena tveganja

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 izpostavljena sredstva, in sistemske ranljivosti, ki jih lahko zlorabijo grožnje. Preprosteje povedano je ocena tveganja proces določitve potencialne škode za posamezno tveganje ter verjetnosti, da se bo dogodek zgodil (Bojanc & Jerman-Blažič, 2008).

V predlaganem modelu v postopku ocene tveganj za vsako informacijsko sredstvo določimo ter ovrednotimo 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. Shematični prikaz parametrov za oceno tveganja je prikazan na sliki 2. Povzročitelji groženj vsebujejo nabor možnih groženj (T), ki imajo neželene učinke na sistem. Grožnje so usmerjene na ranljivosti (v) informacijskih sredstev. Grožnje, ki so izvedene uspešno, so varnostni incident (ρ), ki podjetju povzroči izgubo (L). Zaradi preglednosti so povezave med grožnjami in ranljivostmi na sliki 2 prikazane samo linearno. Model podpira tudi primere, v katerih je ena grožnja usmerjena na več ranljivosti ter več groženj usmerjenih na eno ranljivost.



Slika 2: **Shematični prikaz parametrov za oceno tveganja**

3.1.1 Identifikacija in vrednotenje groženj ter ranljivosti

Informacijska sredstva so izpostavljena grožnjam. Grožnjo lahko opredimo kot potencialni vzrok neželenega incidenta, ki lahko povzroči škodo sistemu ali podjetju (ISO 27000, 2009). Grožnje so vse, kar prispeva k spreminjanju, uničenju ter prekinitvi storitev ali drugih stvari, ki pomenijo vrednost za podjetje. Nabor mogočih groženj se neprestano spreminja in je podjetjem poznan le delno.

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: 20). Strokovnjaki ocenjujejo, da je na vsakih tisoč vrstic programske kode približno dvajset napak in da število prijavljenih ranljivosti z leti 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. Grožnje različno vplivajo na informacijska sredstva. V glavnem so grožnje usmerjene na:

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

Standard ISO 27005 (2008) Information Security Risk Management razvršča grožnje glede na vrsto napada v te 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 napake: odpoved opreme, nepravilno delovanje programske opreme,
- nepooblaščena dejanja: nepooblaščena uporaba opreme, nelegalno kopiranje programske opreme, okvara podatkov, nelegalna obdelava podatkov,
- ogrožanje funkcij: napačna raba, zloraba pravic, ponareditev pravic, odpoved aktivnosti.

Za izračun vrednosti tveganja potrebujemo podatek o verjetnosti grožnje. *Verjetnost grožnje T* zato 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. Pri vrednotenju verjetnosti grožnje T se je treba zavedati, da na verjetnost vpliva veliko faktorjev, in sicer kolikšna je vrednost informacijskih sredstev podjetja za napadalca, katere vire ima napadalec na voljo, ali je informacija o stopnji varnosti v podjetju na voljo napadalcu (informacija napadalcu o visoki stopnji varnosti lahko odvrne napadalca, saj zahteva več napadalčevih virov na razpolago) idr. Vsaka grožnja izkorišča določeno ranljivost in je usmerjena na zlorabo zaupnosti, celovitosti ali razpoložljivosti.

Informacijska sredstva imajo ranljivosti, preko katerih lahko grožnje zlorabijo sredstva. Ranljivost sredstva lahko opredelimo kot šibkost sredstva ali nadzora, ki ga lahko zlorabi grožnja (ISO 27000, 2009) ter tako povečuje verjetnost za uspešen napad na ta sistem (Gordon & Loeb, 2005: 13); npr. puščanje prenosnega računalnika v nezaklenjeni namesto v zaklenjeni pisarni znatno poveča ranljivost prenosnega računalnika za grožnjo kraje. Verjetnost, da bo prenosnik dejansko ukraden, je odvisna od grožnje in ranljivosti. Ranljivost sama po sebi ne povzroči škode; ranljivost je samo pogoj (ali niz pogojev), ki lahko omogoči grožnji, da vpliva na sredstva (ISO 13335-1, 2004).

Ranljivost v sredstva opredelimo 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, $v = 1$ pa, da so informacijska sredstva popolnoma ranljiva.

3.1.2 Verjetnost za varnostni incident

Nekatere izvedene grožnje so za povzročitelja grožnje uspešne in povzročijo varnostni incident, medtem ko druge grožnje niso uspešne. Varnostni incident lahko opredelimo kot neželen ali nepričakovan dogodek v zvezi z informacijsko varnostjo ali serijo takšnih dogodkov, za katere je zelo verjetno, da bodo ogrozili poslovanje in informacijsko varnost (ISO 27000, 2009).

Varnostni incidenti so različnih vrst. Nekateri incidenti so vezani na zaupnost, kot npr. kraja bančnih računov. Drugi incidenti so vezani na celovitost, kot npr. zlonameren izbris ali sprememba dela podatkovne baze podjetja. Tretji incidenti so vezani na razpoložljivost, kot npr. napadi DoS (angl. Denial-of-Service), ki preprečujejo uporabo storitev vsem (avtoriziranim in neavtoriziranim) uporabnikom.

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; npr. izguba zaupnih občutljivih informacij lahko vodi do izgube zaupanja strank.

Verjetnost za varnosti incident ρ $(0 \leq \rho \leq 1)$ določimo kot produkt med verjetnostjo za pojav grožnje T in ranljivostjo v.

$$\rho = T \cdot v \qquad (1)$$

3.1.3 Izguba v primeru varnostnega incidenta

V primeru varnostnega incidenta podjetje utrpi finančno izgubo $L > 0$, ki je merjena v denarnih enotah (npr. evro). Natančno finančno izgubo zaradi varnostnega incidenta je težko oceniti. Dokaj preprosto lahko izračunamo takojšnjo (oz. neposredno izgubo), ki vključuje izgubo prihodkov, izgubo produktivnosti, stroške, povezane z zamenjavo opreme, in sanacijo škode. Precej težje pa je oceniti in ovrednotiti posredno izgubo zaradi varnostnega incidenta. Za lažji izračun izgub razdelimo izgubo na posamezne faktorje:

$$L = L_S + L_r + L_i + L_p + L_{SLA} + L_{posredne} \qquad (2)$$

Podrobna opredelitev in matematična izpeljava posameznih faktorjev, ki nastopajo v enačbi (2) je v Bojanc, Jerman-Blažič in Tekavčič (2012), tukaj je vsebina faktorjev predstavljena le opisno.

Strošek zamenjave opreme L_s je strošek nakupa nove opreme. To vrsto izgub je najpreprosteje ovrednotiti, saj so podatki običajno že na razpolago ali pa jih lahko dokaj preprosto pridobimo. V primeru okvare opreme se lahko ta strošek občutno zmanjša ob investiciji v garancijske storitve, ki jih ponujajo proizvajalci ali razni vzdrževalci opreme.

Strošek popravila L_r so stroški dela zaposlenih ali zunanjih izvajalcev, ki so potrebni, da odpravimo posledice incidenta in ponovno vzpostavimo normalno delovanje sistema ali storitve.

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

Izguba produktivnosti podjetja L_p je zmanjšanje produktivnosti v času nedelovanja sistema ali storitve. V določenih primerih sta lahko izguba prihodkov in izguba produktivnosti medsebojno povezani, zato je treba paziti, da v takih primerih izgube ne vrednotimo dvojno.

Izguba zaradi nespoštovanja zakonskih predpisov ali pogodbenih obveznosti L_{SLA} je odvisna od pogodbe oz. zakonodaje. Za primer poglejmo podjetje, ki strankam ponuja določeno storitev in ima s strankami sklenjeno pogodbo SLA (angl. Service Level Agreement). Če je razpoložljivost storitve, ki jo ponuja podjetje, pod mejo, določeno v SLA, pomeni to za podjetje strošek, saj mora strankam povrniti del plačila.

Posredne izgube $L_{posredne}$ pomenijo zmanjšan ugled podjetja, prekinitev poslovnih procesov, zakonske sankcije, izgubo intelektualne lastnine in izgubo zaupanja strank. Ta izguba je lahko precej večja kot takojšnja izguba ter ima lahko daljnoročne negativne učinke na stranke, dobavitelje, partnerje, finančne trge, banke, zavarovalnice.

Varnostni incidenti lahko povzročijo nedelovanje storitev ali informacijskega sistema. Trajanje nedelovanja je sestavljeno iz časa detekcije t_d, v katerem zaznamo varnostni incident, in časa trajanja popravila t_r, v katerem ponovno vzpostavimo v normalno delovanje informacijski sistem ali storitve. Čas t_d štejemo od trenutka, ko se zgodi incident, do trenutka, ko ga zaznamo. Posamezni faktorji v enačbi (2) lahko vsebujejo bodisi t_r, t_d ali oboje. Časovni parameter t_r vsebujejo faktorji L_r, L_i in L_p, časovni parameter t_d vsebujeta faktorja L_i in L_p, medtem ko faktorji L_s, L_{SLA} in $L_{posredne}$ nimajo časovne odvisnosti (Bojanc, Jerman-Blažič & Tekavčič, 2012). Tako lahko faktorje izgub v enačbi (2) zapišemo tako, da jih ločimo glede na časovna parametra:

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 \qquad (3)$$

Faktor L_1 združuje podatke o L_r, L_i in L_p, faktor L_2 podatke o L_i in L_p ter faktor L_3 podatke o L_s, L_{SLA} in $L_{posredne}$. Faktor L_3 je izražen v denarnih enotah (npr. evro), faktorja L_1 in L_2 pa v denarnih enotah na časovno enoto (npr. evro/uro).

3.1.4 Izračun stopnje tveganja

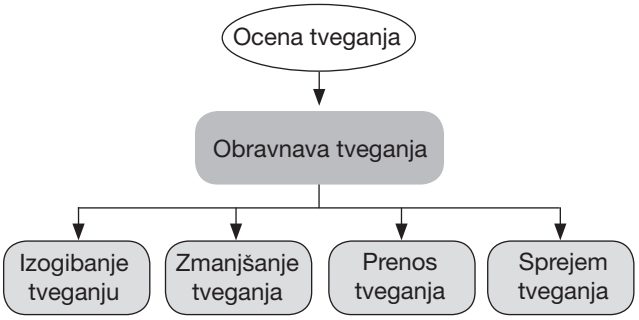
S postopkom ocene tveganja za vsako informacijsko sredstvo ugotovimo in ovrednotimo ranljivosti in grožnje. Rezultat ocene tveganja je izračunani parameter *varnostno tveganje R*, ki pomeni pričakovano finančno izgubo zaradi pričakovanega varnostnega incidenta in je izražen v enakih denarnih enotah kot izguba L (npr. evro). Varnostno tveganje je določeno kot produkt med ocenjeno verjetnostjo za varnostni incident ρ in izgubo zaradi varnostnega incidenta L ter ga ob upoštevanju zapisa izgube (3) in verjetnosti za incident (1) lahko zapišemo:

$$R = \rho \cdot L = T \cdot v \cdot [L_1 \cdot t_r + L_2 \cdot t_d + L_3] \qquad (4)$$

3.2 Izbira ustrezne obravnave tveganja

Za vsako zaznano in ovrednoteno varnostno tveganje je na voljo več možnosti, kako podjetje obravnava to tveganje. Glede na opravljeno oceno tveganja ima podjetje na izbiro obravnave, ki so shematično prikazane na sliki 3:

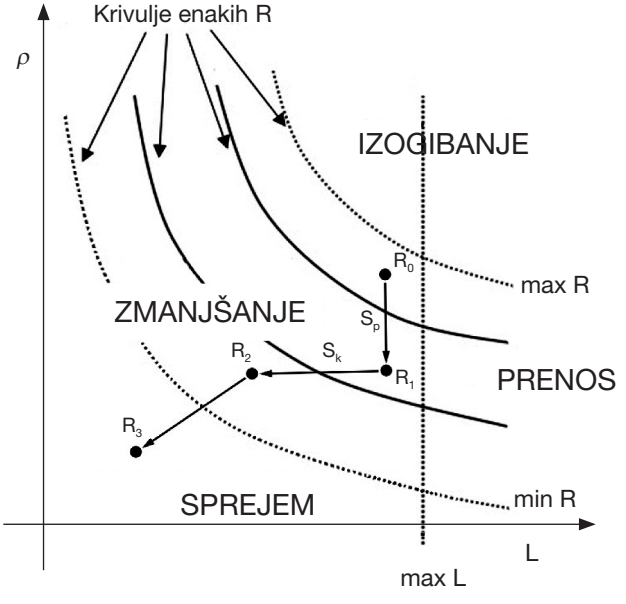
- *zmanjšanje* izpostavljenosti sredstva na tveganje z uvedbo ustreznih tehnologij in orodij (npr. požarnega zidu, protivirusne zaščite) ali uvedbo ustreznih postopkov (npr. varnostne politike, politike gesel, nadzora dostopa itd.): s tem zmanjšamo verjetnost za škodljive dogodke ali omejimo izgubo, ki jo povzroči dogodek. Zmanjšanje tveganja je pogosto glavna strategija obvladovanja tveganja;
- *prenos* tveganja na drugo stranko – lahko preko zunanjega izvajanja storitev (npr. storitve v oblaku) ali z zavarovanjem: strategija prenosa postaja v zadnjem času čedalje bolj pomembna;
- *izogibanje* grožnjam in napadom z omejevanjem izvorov tveganja oz. z izpostavljenostjo sredstev k tveganju večinoma uporabimo v primerih, ko resnost učinka tveganja pretehta koristi, ki jih prinaša posamezno sredstvo (npr. odprt dostop do interneta). Podjetje se z izogibanjem tveganim aktivnostim odpove aktivnosti, vendar pa se zaščiti pred tveganjem, ki bi imelo prevelike posledice;
- *sprejem* tveganja kot posledico poslovanja je smiselna strategija v primeru, ko se ni mogoče izogniti tveganju ali ko so stroški uvedbe zaščitnih ukrepov znatno večji kot skupne izgube zaradi tveganja.



Slika 3: **Različne možnosti obravnave tveganja**

Zavedati se je treba, da izbrana obravnava tveganja lahko privede do novih tveganj, ki jih je treba ravno tako oceniti in obravnavati (Schneier, 2003: 14). V nekaterih primerih je težko določiti mejo med posameznimi obravnavami, npr. požarni zid lahko razumemo kot zmanjšanje tveganja ali pa tudi kot izogibanje tveganju, ker se s tem podjetje odreče prednosti odprtih omrežij, da bi se izognilo tveganju. Zato je izbira ustrezne obravnave tveganja lahko precej težavna in večkrat pri odločanju zahteva sklepanje kompromisov ali uporabo in kombiniranje dveh strategij.

Izbiro ustrezne obravnave tveganja lahko prikažemo na grafu verjetnosti za incident in izgube zaradi incidenta $\rho = \rho(L)$, ki je prikazan na sliki 4. Krivulje na grafu predstavljajo točke z isto vrednostjo tveganja R, ki pa se med seboj razlikujejo v vrednostih ρ in L. Notranje krivulje pomenijo nižje vrednosti tveganja, zunanje krivulje pa višje. Izbrana obravnava tveganja, ki zmanjšuje vrednost tveganja R, prestavi točko tveganja na nižjo krivuljo tveganja. Obravnava tveganja s_p zmanjšuje verjetnost za incident ρ in je na grafu prikazana kot vertikalen premik navzdol iz točke R_0 v R_1. Obravnava tveganja s_k zmanjšuje izgubo in je na grafu prikazana kot horizontalni premik proti levi s točke R_1 na R_2.



Slika 4: **Grafični prikaz porazdelitve posamezne obravnave tveganja glede na vrednosti *L*, *ρ* in *R*** (Vir: Bojanc & Jerman-Blažič, 2012)

Vsaka izmed štirih mogočih obravnav tveganja pomeni določeno področje na grafu. Določiti je treba mejne vrednosti parametrov tveganja, ki so mejne črte, ki področje grafikona razdelijo na štiri enote, katere ustrezajo posameznim obravnavam tveganja (Bojanc & Jerman-Blažič, 2008). 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.

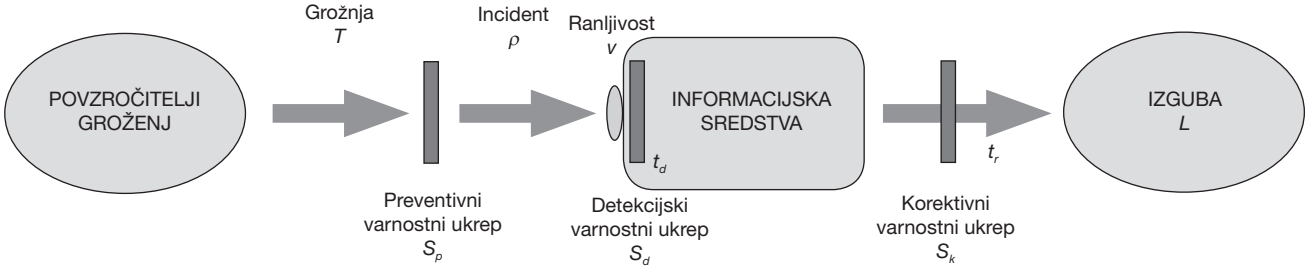
Ustrezno obravnavo tveganja določimo tako, da za posamezno tveganje vrednosti R in L primerjamo z mejnimi vrednostmi R_{max}, L_{max} in R_{min}. Prva mejna črta določa najmanjšo smiselno verjetnost za incident ($R < R_{min}$). Pod to vrednostjo je tveganje zanemarljivo nizko, zato uvajanje varnostnega ukrepa ni finančno upravičeno in sprejmemo tveganja. Druga mejna črta je največja mogoča vrednost tveganja ($R > R_{max}$), nad katero se podjetje izogne tveganju. Tretja mejna črta je največja mogoča izguba zaradi incidenta ($L > L_{max}$). Nad to vrednostjo ima zaradi visoke izgube učinek lahko katastrofalne posledice in je priporočljivo oblikovati prenos tveganja. Schneier (2003: 23) pravi, da zares velike posledice niso sprejemljive ne glede na pogostost. Tveganja v preostalem območju ($L < L_{max}$) odpravimo z zmanjševanjem preko investicij v varnostne ukrepe.

Mogoče so tudi kombinacije teh obravnav; npr. podjetje najprej izvede varnostne ukrepe, ki zmanjšajo izgubo, ter preostanek tveganja prenese na zavarovalnico. Pri tem je treba ugotoviti, ali je investicija v varnostni ukrep manjša od zmanjšanja premije, ki jo plačujemo zavarovalnici.

3.3 Izbira in vrednotenje varnostnih ukrepov

Varnostni ukrepi so aktivnosti, postopki ali mehanizmi, ki preprečujejo ali zmanjšujejo škodo, povzročeno z realizacijo ene ali več groženj. Varnostni ukrepi so lahko fizične ovire, senzorji, programska oprema, algoritmi, izboljšave obstoječih politik ali postopkov. Lahko izvajajo eno ali več funkcij, kot so odkrivanje, odvračanje, preprečevanje, omejevanje, popravljanje, okrevanje, nadzor in ozaveščenost. 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. Kot je prikazano na sliki 5, se pred grožnjami zavarujemo z uvedbo varnostnih ukrepov, ki jih lahko glede na učinek na parametre R, ρ in L razvrstimo v:

- *preventivne varnostne ukrepe* s_p, ki zmanjšujejo verjetnost za varnostni incident ρ (npr. požarni zid, protivirusna zaščita),
- *korektivne varnostne ukrepe* s_k, ki zmanjšujejo izgubo L v primeru incidenta (npr. vzdrževalne pogodbe, načrt neprekinjenega poslovanja, varnostne kopije podatkov, redundantni sistem, uvedba različnih standardov),
- *detekcijske varnostne ukrepe* s_d, ki zmanjšujejo čas, v katerem zaznamo incident t_d in omogočamo zbiranje podatkov o grožnjah (npr. sistem za odkrivanje vdorov, IDS – Intrusion Detection System).



Slika 5: **Učinek uvedbe varnostnih ukrepov na zmanjšanje tveganja** (Vir: Bojanc, Jerman-Blažič & Tekavčič, 2012)

Učinek varnostnih ukrepov je prikazan tudi grafično na sliki 4. Uvedeni preventivni ukrep s_p prestavi stanje na grafu vertikalno navzdol (iz R_0 na R_1) na nižjo krivuljo tveganja, uvedba korektivnih s_k in detekcijskih ukrepov s_d pa prestavi stanje na grafu horizontalno proti levi na nižjo krivuljo tveganja (iz R_1 na R_2).

Vsak varnostni ukrep $s(\alpha, C)$ opredeljujeta dva kvantitativna parametra: učinkovitost ukrepa α in strošek ukrepa C. *Učinkovitost varnostnega ukrepa* α predstavlja vpliv varnostnega ukrepa na zmanjšanje tveganja. *Strošek ukrepa* C je denarna investicija v varnostni ukrep, ki vsebuje vse izdatke, vezane na uvedbo varnostnega ukrepa, od enkratnega izdatka v kapitalske naložbe do operativnih stroškov. Kapitalske naložbe so npr. nabava novega sistema za zaznavanje vdorov v omrežje, ki pomaga podjetju

zmanjševati verjetnost varnostnih vdorov v določenem (npr. triletnem) prihodnjem obdobju. Operativni stroški vključujejo letno vzdrževanje (posodobitve in varnostne popravke), izobraževanje uporabnikov in skrbnikov omrežja ter nadzor delovanja rešitve.

Pri uvedbi varnostnih ukrepov je treba upoštevati tudi proračun podjetja, namenjen za varnostne investicije C_{IT_budget}, ki ga ne sme presegati strošek varnostnih ukrepov v določenem proračunskem obdobju. Če je cena ukrepa višja kot znaša proračun, uvedba tega ukrepa ni mogoča. Po raziskavi CSI (2010) je v povprečju 6 odstotkov proračunskih sredstev podjetja namenjenih za informacijsko varnost.

Uvedba preventivnega varnostnega ukrepa $s_p(\alpha_p, C_p)$ zmanjšuje verjetnost za varnostni incident ρ. Obstaja precej različnih funkcij verjetnosti za varnostni incident ρ, v predstavljenem modelu je uporabljena funkcija, ki je med raziskovalci precej priljubljena (Gordon & Loeb, 2002; Matsuura, 2008):

$$\rho = T \cdot v^{\alpha_p C_p + 1} \qquad (5)$$

Izguba L zaradi varnostnega incidenta se lahko zmanjša z investicijo v korektivni varnostni ukrep $s_k(\alpha_k, C_k)$, ki zmanjšuje čas popravila t_r, ali v detekcijski varnostni ukrep $s_d(\alpha_d, C_d)$, ki zmanjšuje čas za detekcijo t_d. Poseben primer korektivnega ukrepa je prenos tveganja na zavarovalnico. V tem primeru je strošek C mesečna ali letna premija, ki jo podjetje plačuje zavarovalnici; v primeru incidenta pa zavarovalnica izplača podjetju kompenzacijo za kritje izgube v vrednosti I. Izgubo L v enačbi 3 ob uvedbi teh ukrepov lahko zapišemo:

$$L = L_1 \cdot t_r^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^0 \cdot e^{-\alpha_d C_d} + L_2 - I \qquad (6)$$

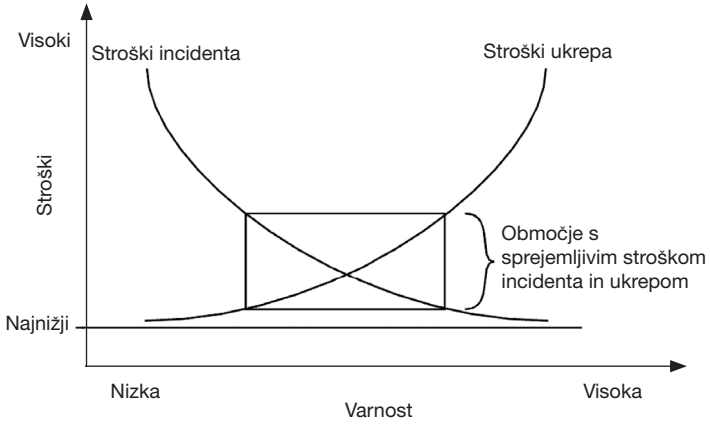
Enačba 4 za varnostno tveganje R ob upoštevanju uvedbe varnostnih ukrepov, ki zmanjšujejo verjetnost za incident (enačba 5) ali izgubo v primeru incidenta (enačba 6), izračunamo kot:

$$R = T \cdot v^{\alpha_p C_p + 1}[L_1 \cdot t_r^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^0 \cdot e^{-\alpha_d C_d} + L_3 - I \qquad (7)$$

Nova vrednost tveganja R po uvedbi varnostnih ukrepov je grafično prikazana na sliki 4, na kateri nova vrednost tveganja leži na nižji krivulji tveganja R kot prvotna vrednost tveganja.

3.4 Ocena donosnosti ukrepov in izbira optimalnega ukrepa

Odločitev o tem, kako najbolje vlagati sredstva v informacijsko varnost, ni preprosta in se tudi razlikuje od organizacije do organizacije. Pri določitvi optimalnega zneska investicij v informacijsko varnost je treba najti optimalno razmerje med stroški in varnostjo, kar je prikazano na sliki 6. Stroški informacijske varnosti imajo dve komponenti, ki sta povezani med seboj, in sicer »stroški ukrepa« in »stroški incidenta«. Strošek ukrepa je denar, ki ga podjetje porabi za investicijo, s katero se želi izogniti problemu. Ta komponenta se povečuje z večanjem varnosti sistema. Strošek incidenta je denar, ki ga podjetje porabi, ko pride do problema. Ta komponenta se zmanjšuje z večanjem varnosti sistema. 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 preprosta naloga. Za določitev optimalne stopnje informacijske varnosti pogosto uporabimo analizo stroškov in koristi.



Slika 6: **Iskanje optimalne rešitve med višino stroškov varnostnega incidenta in stroški ukrepa** (Vir: Kaplan, 2007: 304).

Analiza stroškov in koristi primerja stroške določene aktivnosti s koristmi, ki jih prinaša aktivnost. Predpostavimo, da lahko ocenimo pričakovane skupne koristi in pričakovane skupne stroške za različne ravni aktivnosti informacijske varnosti. Dokler *koristi B* dodatne aktivnosti informacijske varnosti presegajo *stroške C*, je uvedba aktivnosti smiselna.

$$B > C \qquad (8)$$

Cilj podjetja je uvedba varnostnih ukrepov do točke, na kateri so neto koristi (tj. koristi minus stroški) maksimalne. Uvedba varnostnih ukrepov preko te točke pomeni, da so mejni stroški višji od mejnih koristi dodatne varnosti. Z drugimi besedami, neto koristi uvedbe varnostnih ukrepov preko najvišje točke so negativne. Za podjetje nima smisla, da za varnostno rešitev zapravi več, kot znašajo mogoče izgube v primeru incidenta.

Gordon in Loeb (2002) ocenjujeta, da naj bi optimalni strošek za varnostni ukrep znašal od 0 do 37 odstotkov mogoče izgube zaradi varnostnega incidenta. Drugi raziskovalci so to ugotovitev razširili in našli okoliščine, v katerih je upravičeno, da strošek ukrepa znaša celo do 100 odstotkov mogoče izgube (Willemson, 2006). Te ugotovitve so uspešno preverili na empiričnih primerih (Tanaka, Matsuura & Sudoh, 2005; Tanaka, Liu & Matsuura, 2006).

Izračun stroškov vlaganja *C* v informacijsko varnost je opisan v prejšnjem razdelku. Za razliko od stroškov, ki jih je mogoče dobiti dokaj preprosto, pa je precej težje opredeliti, oceniti ali meriti koristi. Varnostne rešitve (npr. požarni zid, protivirusni program in sistemi IDS) same po sebi namreč ne prinašajo finančne koristi, ki jih je mogoče izmeriti. Koristi investicije v informacijsko varnost so lahko različne, npr. zmanjšanje verjetnosti ponovitve incidenta, povečanje učinkovitosti ostalih investicij informacijske varnosti ali zmanjševanju izgub v primeru incidenta.

V splošnem se na koristi zaradi vlaganja v informacijsko varnost gleda kot na prihranek stroškov incidenta zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta. Te koristi je običajno zelo težko točno napovedati. Največja težava je, ker gre za ocenjevanje prihrankov stroškov, vezanih na potencialne varnostne incidente, ki se še niso zgodili. Bolj kot je informacijska varnost uspešna, težje je opaziti dejanske koristi.

Koristi *B* zaradi investicije v varnostni ukrep so enake zmanjšanju tveganja na račun uvedbe ukrepa, kar lahko zapišemo kot razliko med vrednostmi tveganja pred uvedbo ukrepa R_0 in vrednostmi tveganja po uvedbi varnostnega ukrepa $R(C)$:

$$B = R_0 - R(C) \qquad (9)$$

Za oceno ekonomske upravičenosti uvedbe varnostnega ukrepa v praksi najpogosteje uporabljamo kazalnike donosnost investicije (angl. Return on Investment – ROI), neto sedanja vrednost (angl. Net Present Value – NPV) in notranja stopnja donosa (angl. Internal Rate of Return – IRR) ali kombinacija teh kazalnikov.

Donosnost investicije (ROI) določa, koliko podjetje dobi glede na porabljeni znesek denarja. Kazalnik je izražen kot odstotek vrnjene investicije v določenem času. ROI je enak sedanji vrednosti neto koristi v določenem časovnem obdobju, deljen z začetnim stroškom investicije *C*. Pozitivna vrednost ROI pomeni, da je vlaganje ekonomsko upravičeno.

$$ROI = \frac{B - C}{C} \qquad (10)$$

Izračun ponazorimo s preprostim primerom. Recimo, da je tveganje okužbe z virusom v organizaciji ocenjeno na 8.750 evrov. Z uvedbo varnostnega ukrepa v vrednosti 1.600 evrov tveganje zmanjšamo na 3.400 evrov. K stroškom nakupa ukrepa je treba prišteti še 450 evrov letnih stroškov za vzdrževanje in upravljanje varovanja. Za prvo leto uporabe znaša tako ROI:

$$ROI = \frac{8.750 - 3.400 - 1.600 - 450}{1.600 + 450} = 160\ \% \qquad (11)$$

Izračun ROI lahko navedemo za različne varnostne ukrepe, ki so predstavljeni v razdelku 3.3. Pri tem za posamezne varnostne ukrepe ustrezno prilagodimo enačbo tveganja 7. Če varnostno tveganje rešujemo z vlaganjem v preventivni varnostni ukrep s_p, ki zmanjša ranljivost sredstva, lahko enačbo 10 za ROI zapišemo:

$$ROI = \frac{T \cdot v\,(1 - v^{\alpha_p C_p}) \cdot L - C_p}{C_p} \qquad (12)$$

Če pa tveganje rešujemo z vlaganjem v korektivni varnostni ukrep s_k, ki zmanjšuje izgubo, lahko enačbo 10 za ROI zapišemo:

$$ROI = \frac{TvL_1 t_r^0 (1 - e^{-\alpha_k C_k}) - C_k}{C_k} \qquad (13)$$

Poseben primer je prenos tveganja na zavarovalnico, pri čemer enačbo 10 poenostavimo v:

$$ROI = \frac{TvI - C}{C} \qquad (14)$$

Zavedati se je treba, da ROI pove samo odstotek donosnosti investicije v določenem časovnem obdobju, ničesar pa ne pove o obsegu donosa. Tako lahko 124-odstotna donosnost na prvi pogled zgleda precej mikavno, vprašanje pa je, ali bi raje imeli 124-odstotno donosnost projekta v višini 10.000 evrov ali »samo« 60-odstotno donosnost projekta v višini 300.000 evrov.

Za dolgoročnejša vlaganja v informacijsko varnost je zato primernejša uporaba kazalnika *neto sedanja vrednost (NPV)*, ki upošteva tudi vrednost denarja v času, ki ga kazalnik ROI ne upošteva:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + k)^t} \qquad (15)$$

V enačbi 15 je k diskontna stopnja, n pa časovno obdobje. Diskontna stopnja k se običajno razume kot povprečni strošek kapitala. Izbor ustrezne diskontne stopnje je za izračun kazalnika NPV zelo pomemben. Model NPV preko diskontne stopnje uravnava tveganje, pri tem večja diskontna stopnja pomeni manjšo vrednost kazalnika NPV.

Kazalnik NPV je merjen v denarnih enotah, vlaganje pa je ekonomsko upravičeno, če je NPV enak ali večji od nič. Bistvo pristopa NPV je primerjava diskontiranih denarnih tokov, vezanih na prihodnje koristi in stroške z začetnimi stroški investicije, pri čemer so celotne koristi in stroški izraženi v denarni enoti. Zaradi lažjega izračunavanja se pogosto privzame, da so prihodnje koristi in stroški, z izjemo stroškov začetne investicije, realizirani na koncu posameznega obdobja. S tem ko denarne tokove diskontiramo, ustrezno vključimo časovno komponento, tako da so zneski koristi in stroškov v različnih časovnih obdobjih primerljivi.

NPV pogosto uporabljamo v primerih, ko med seboj primerjamo različne alternative, npr. organizacija izbira med dvema varnostnima rešitvama, pri čemer za prvo rešitev plača 15.000 evrov vnaprej, za drugo pa plačuje tri leta po 5.000 evrov na leto. Obe rešitvi staneta 15.000 evrov, vendar je druga rešitev ugodnejša, saj lahko organizacija investira preostali denar za določen čas v druge namene. Tako je dejanski strošek druge investicije manjši od 15.000 evrov.

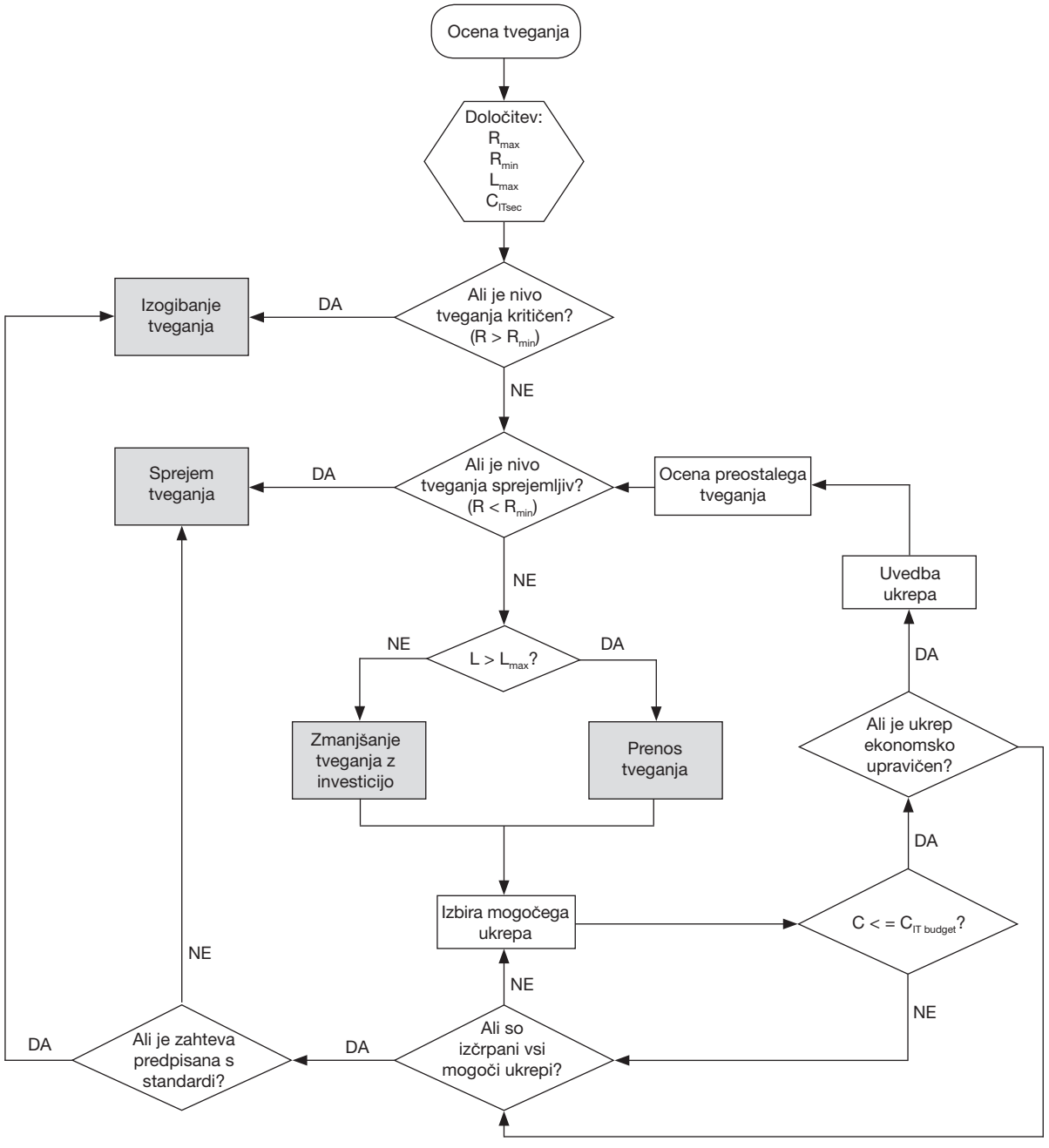
Da bi ugotovili, kolikšna je dejanska stopnja donosnosti projekta, lahko uporabimo kazalnik *notranja stopnja donosa (IRR)*. IRR je enak tisti diskontni stopnji, pri kateri je NPV = 0 oz. pri kateri se izenačita sedanja vrednost prejemkov in sedanja vrednost izdatkov.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0 \qquad (16)$$

Odločitev glede uporabe kazalnikov ROI, NPV ali IRR je prepuščena podjetjem in posameznikom, odgovornim za vrednotenje varnostnih investicij. Vsak od teh finančnih kazalnikov ima svoje prednosti in slabosti. Pogosto so rezultati enaki pri uporabi vseh treh kazalnikov, včasih pa se pri odločanju pokažejo razlike. Zato je pri primerjavi dveh ali več alternativnih varnostnih rešitev pogosto treba upoštevati več kazalnikov. Čeprav ima ROI določene pomanjkljivosti v primerjavi z NPV in IRR, je ROI še vedno najbolj priljubljen kazalnik v praksi. Po raziskavi CSI (2010) uporablja kazalnike ROI 54 odstotkov vprašanih, 22 odstotkov jih uporablja NPV, 17 odstotkov pa IRR.

3.5 Proces upravljanja tveganja

Proces upravljanja informacijskovarnostnih tveganj je prikazan na sliki 7. Proces se začne z oceno tveganja in nadaljuje z izbiro ustrezne obravnave tveganja, ki temelji na določitvi mejnih parametrov tveganja R_{min}, R_{max}, L_{max}. Izbira varnostnega ukrepa je odvisna tudi od višine proračuna podjetja za investicije v informacijsko varnost C_{IT_budget}, ki ga cena ukrepov C v določenem proračunskem obdobju ne sme presegati. Če pri zmanjšanju tveganja ni na voljo nobenega ustreznega ukrepa, je treba zmanjšanje tveganja zamenjati za drugo obravnavo (npr. sprejem ali izogibanje) tveganja.



Slika 7: **Proces upravljanja informacijskovarnostnih tveganj** (Vir: Bojanc, Jerman-Blažič in Tekavčič, 2012)

4 PRAKTIČNO PREVERJANJE MODELA

Model upravljanja tveganj je praktično preverjen v raziskavi v realnem okolju, pri čemer je sodelovalo srednje veliko podjetje s področja informacijske tehnologije v Sloveniji. Namen raziskave je uporaba modela v praksi in ocena njegove praktične uporabnosti. Izračuni, v katerih smo preizkušali model, so narejeni na podlagi realnih podatkov in za različne grožnje (virusi, neželena pošta, neavtorizirana sprememba spletne strani, phishing, napad DoS). V nadaljevanju je prikazan izračun za grožnjo okužbe z računalniškim virusom, ki je po raziskavi CSI najpogostejša grožnja (CSI, 2010). Da izračun ni preobširen, je v članku naveden pregled praktične uporabe, celotni izračun pa je prikazan v Bojanc, Jerman-Blažič in Tekavčič (2012).

Pri tveganju okužbe z računalniškim virusom pojem virus razumemo v širšem pomenu, tako da pod tem izrazom upoštevamo 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 naj se odločijo za katero drugo rešitev. 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 mogoči ukrep upoštevajo sedanjo rešitev.

V prvem koraku pridobimo kvantitativne podatke za oceno tveganja. Ranljivost je verjetnost, da bo računalniški virus okužil sredstvo, na katerega je usmerjen. Ker ocenjujemo stanje, v katerem ni nobene tehnične zaščite zoper grožnje, je ranljivost enaka ozaveščenosti zaposlenih, da v primeru, ko dobijo virus, tega ne aktivirajo. Podjetje ocenjuje, da bi glede na trenutno ozaveščenost in v okolju brez protivirusne zaščite, virus preko okužene datoteke aktivirali dve tretjini zaposlenih ($\nu = 0{,}66$). Verjetnost grožnje je ocena pogostosti prejema okuženih datotek ali drugega načina okužbe in je ocenjena na enkrat na teden ($T = 1/7$ dni = 0,143/dan). Verjetnost za incident je:

$$\rho = T \cdot \nu = 0{,}143 \cdot 0{,}66 = 0{,}0952 \ / \ dan \qquad (17)$$

Parametri izgube v primeru varnostnega incidenta so ocenjeni: $L_1 = 41{,}53$ evrov/uro, $L_2 = 18{,}41$ evrov/uro, $L_3 = 0$, $t_{r0} = 8$ ur, $t_{d0} = 2$ uri. Skupna izračunana izguba je tako: $L = 369{,}07$ evrov. Varnostno tveganje ocenimo na:

$$R = \rho \cdot L = 0{,}0952 \ / \ dan \cdot 369{,}07 \ € = 35{,}15 \ € \ / \ dan \qquad (18)$$

Za reševanje tveganja okužbe z računalniškim virusom so izbrani tile mogoči 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, pri čemer 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, posredniku SMTP in delovnih postajah (poleg virusov pregleduje tudi za neželeno pošto). Omogoča centralno posodabljanje, potrebno je letno podaljševanje naročnine za virusne definicije;
- ukrep Č: vsakoletno izobraževanje in ozaveščanje uporabnikov s spletnimi izobraževanji;
- ukrep D: izdelava varnostnih kopij sistemov, kar zmanjšuje čas okrevanja okuženih sistemov (to velja le v primeru, če podatki na varnostnih kopijah niso okuženi z virusom). V nasprotju z drugimi ukrepi, ki so preventivni, je ta ukrep korektiven, ker blaži posledice v primeru incidenta;
- ukrep E: kombinacija protivirusne zaščite in izobraževanja uporabnikov (ukrepa B in Č).

Pri izračunu so namenoma izbrani preventivni in korektivni tehnološki ukrepi, izobraževanje uporabnikov ter kombinacija več ukrepov, da tako demonstriramo zmogljivost modela za medsebojno vrednotenje različnih vrst varnostnih ukrepov. Ocena karakteristik za stroške in učinkovitost izbranih ukrepov je zbrana v tabeli 1. V izračunu je časovno obdobje za investicijo štiri leta.

Tabela 1: **Ocena stroškov in učinkovitosti varnostnih ukrepov**

Ukrep	Strošek nabave in nadgradnje opreme	Stroški vzdrževanja	Učinkovitost ukrepa α (v 10^{-3})
A	Začetni stroški 1.766 evrov	Letno vzdrževanje 693 evrov	0,7691
B	Začetni stroški 1.481 evrov, letna nadgradnja 835 evrov (razen prvo leto)	Letno vzdrževanje 138 evrov	2,1018
C	Začetni stroški 6.484 evrov, letna nadgradnja 1.100 evrov	Letno vzdrževanje 277 evrov	1,1607
Č	Začetni stroški 1.646 evrov, nadgradnja 1.600 evrov (razen prvo leto)	Ni letnega vzdrževanja.	1. leto: 0,1482 2. leto: 0,2320 3. leto: 0,3157 4. leto: 0,3995
D	Začetni stroški 3.297 evrov	Letno vzdrževanje 1.387 evrov	0,1284
E	Začetni stroški 3.127 evrov, nadgradnja 2.435 evrov (razen prvo leto)	Letno vzdrževanje 138 evrov	1. leto: 0,9571 2. leto: 1,0062 3. leto: 1,0553 4. leto: 1,1044

Vrednotenje posameznih ukrepov je prikazano v tabeli 2, rezultati izračunov ROI, NPV in IRR pa v tabeli 3. Pri izračunu je upoštevana diskontna stopnja 2,7 odstotka.

Tabela 2: **Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov**

	Ukrep A			Ukrep B			Ukrep C		
Leto	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**
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 Č			Ukrep D			Ukrep E		
Leto	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**
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 3: **Izračun kazalnikov ROI, NPV in IRR za posamezne ukrepe**

Ukrep	ROI	NPV	IRR
A	111 %	4.591 evrov	89 %
B	437 %	18.522 evrov	390 %
C	151 %	16.571 evrov	87 %
Č	255 %	15.173 evrov	209 %
D	53 %	4.191 evrov	48 %
E	134 %	13.634 evrov	166 %

Praktični izračun lepo demonstrira uporabnost modela za vrednotenje in medsebojno primerjavo različnih vrst varnostnih ukrepov. Prva zanimiva ugotovitev je, da dajo vsi ukrepi pri vseh izračunanih kazalnikih pozitiven rezultat. Najbolj ekonomsko optimalna izbira je ukrep B, na drugem mestu je ukrep Č; ukrep E, ki je kombinacija ukrepov B in Č, pa je šele na četrtem mestu. Očitno v tem primeru cena skupnih ukrepov ne upraviči dodatne varnosti. Omeniti je treba še, da izračun za ukrep B, enako kot drugi ukrepi, vsebuje tudi nabavno ceno in uvedbo ukrepa. Če upoštevamo, da ima podjetje že uveden ta ukrep, odpadeta stroška za ukrep B, kar pomeni še boljši rezultat pri vseh kazalnikih.

5 SKLEP

Informacijska varnost je področje, za katerega se hitro povečuje zanimanje. Podjetja se čedalje bolj zavedajo, da je varnost eden izmed temeljnih 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 treba, da popolnoma varen sistem ne obstaja. Podjetje mora izbrati takšno stopnjo varnosti, ki je sprejemljiva zanj. Določitev ustrezne stopnje je zahtevna naloga, ki se izvaja v procesu upravljanja varnostnih tveganj.

Proces upravljanja tveganja pomaga podjetjem sprejeti odločitev glede potrebnih investicij v varnostne ukrepe, ki so za poslovanje podjetja najučinkovitejši. Temeljna 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. S stališča podjetja je varnost investicija, ki se meri v prihrankih denarnih enot.

Osebe, ki so v podjetjih odgovorne za investicije, seveda najbolj zanima, kam vlagati in predvsem koliko. Preden investiramo v določen produkt ali storitev, je dobro vedeti, ali je investicija finančno upravičena. Informacijska varnost pri tem ni nobena izjema. Zavedati pa se je treba, da je ekonomski pristop k upravljanju varnostnih tveganj in ocenjevanja optimalne investicije v informacijsko varnost obsežen projekt. Zahteva namreč poglobljeno analizo in vrednotenje informacijskih sredstev, analizo groženj, usmerjenih na informacijska sredstva, analizo posledic nedelovanja informacijske tehnologije, analizo verjetnosti za uspešno izveden napad ter oceno stroškov in koristi, ki so posledica vlaganj v informacijsko varnost.

V članku je predstavljen celovit model za upravljanje informacijskovarnostnih tveganj, ki omogoča oceno vlaganj v varnost in zaščito v poslovne informacijske sisteme. Razviti model temelji na kvantitativni analizi varnostnih tveganj in omogoča vrednotenje različnih možnosti investiranja v informacijsko varnost. Model je zasnovan kot standardni postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro optimalnega ukrepa, ki zmanjšuje določeno varnostno tveganje. Največja prednost modela je, da 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. Pri procesu ocene optimalnega obsega vlaganj v informacijsko varnost je treba kvantitativno ovrednotiti tako ranljivosti in grožnje, ki so vezane na neko informacijsko sredstvo, kot tudi ukrepe, ki zmanjšujejo ta tveganja. Kvantitativno vrednotenje teh parametrov je namreč podlaga za presojo ekonomske upravičenosti posamezne investicije s pomočjo kazalnikov ROI, NPV ter IRR. Model je bil praktično uporabljen in preverjen za konkretno podjetje, kar potrjuje njegovo pravilnost in učinkovitost. Zavedati pa se moramo, da so rezultati modela zelo odvisni od natančnosti vhodnih podatkov. Za določene grožnje trenutno primanjkuje dobrih zgodovinskih podatkov, na podlagi katerih lahko natančno določimo vhodne podatke. Pričakujemo lahko, da bo v prihodnje vse več razpoložljivih statističnih podatkov, kar bo pozitivno vplivalo na uporabo kvantitativnih pristopov.

5 LITERATURA IN VIRI

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

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

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

[4] Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2012). Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach, Information Processing & Management, 22 str., [URL: http://dx.doi.org/10.1016/j.ipm.2012.01.001].

[5] 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.

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

[7] Computer Security Institute (CSI). (2010). CSI Survey 2010/2011. The 15th Annual Computer Crime and Security Survey. Dosegljivo na http://www.gocsi.com/survey.

[8] 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.

[9] 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.

[10] ENISA. (2009). Inventory of risk assessment and risk management methods. Dosegljivo na: http://rm-inv.enisa.europa.eu/rm_ra_methods.html.

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

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

[13] Geer, D. (2004, 20. oktober). Q&A: Dan Geer on security of information when economics matters. SearchDataManagement.com. Dosegljivo na http://searchdatamanagement.techtarget.com/news/interview/0,289202,sid91_gci1139680,00.html.

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

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

[16] 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).

[17] International Organization for Standardization (ISO). (2008). ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization (ISO).

[18] International Organization for Standardization (ISO). (2009). ISO/IEC Guide 73:2009. Risk management – Vocabulary. Geneva: International Organization for Standardization (ISO).

[19] 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).
[20] 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.
[21] 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). Dosegljivo na http://weis2008.econinfosec.org/program.htm.
[22] 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). Dosegljivo na http://www.nmayer.eu/publis/RCIS07-CR_NMA-PHE-RMA.pdf.
[23] Ryan, J. & Ryan, D. (2006) Expected benefits of information security investments. Computers & Security, 25, 579–588.
[24] Sandhu, R. (2003). Good-Enough Sercurity: Toward a Pragmatic Business-Driven Discipline. IEEE Internet Computing, 5(3), 66–68.
[25] Schneier, B. (2003). Beyond Fear: Think Sensibly about Security in an Uncertain World. New York: Copernicus Books.
[26] Schneier, B. (2004). Secrets & Lies, Digital Security in a Networked World. New York: Wiley Publishing.
[27] Soo Hoo, K. J. (2000). How Much Is Enough? A Risk-Management Approach To Computer Security. Palo Alto, CA: Stanford University.
[28] 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). Dosegljivo na http://weis2006.econinfosec.org/prog.html.
[29] 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.
[30] Willemson, J. (2006). On the Gordon&Loeb Model for Information Security Investment. Workshop on the Economics of Information Security (WEIS 2006). Dosegljivo na http://weis2006.econinfosec.org/prog.html.

▪

Rok Bojanc je zaposlen v ZZI, d. o. o., kot vodja storitev informacijske tehnologije in informacijske varnosti. Na področju informacijske tehnologije deluje že več kot petnajst let, izkušnje je pridobival na različnih področjih — od predavatelja, sistemskega inženirja, arhitekta do vodje projektov. Je avtor in soavtor več člankov in priročnikov s področja informacijske varnosti, elektronskega poslovanja, računalniških omrežij in strežniških sistemov. Pogosto predava na konferencah in seminarjih.