Proces upravljanja s tveganji v informacijski varnosti

Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru
Kaja Prislan, študentka magistrskega študija, Fakulteta za varnostne vede, Univerza v Mariboru

Namen in cilj prispevka
Namen prispevka je prikazati načine zoperstavljanja grožnjam informacijski varnosti in proučiti obstoj sistemov upravljanja s tveganji v praksi med različnimi organizacijami. Ker so spremembe edina stalnica sodobnega sveta, se le-tem prilagajamo uporabniki, prav tako pa tudi grožnje informacijski tehnologiji. Brez slednje sodobne organizacije ne morejo poslovati, še manj dosegati zastavljene cilje. Edina možnost je obvladovanje groženj in izvajanje procesa upravljanja s tveganji.

Metodologija
Za proučitev trenutnega stanja varnosti informacijskih sistemov v organizacijah je bila izvedena anketa med za analizo narave postopka upravljanja s tveganji v teoriji pa deskriptivna metoda. Za pridobivanje podatkov in oblikovanje spoznanj o pomembnosti informacijske varnosti bom uporabila strokovno literaturo domačih in tujih avtorjev ter internetne vire, ki se nanašajo na področje tematike diplomskega dela.

Ugotovitve in omejitve
Omejitve se kažejo v nerazumevanju problematike in dejstvu, da je ustroj takšnega sistema povsem odvisen od vsake organizacije posebej, zatorej ugotavljamo, da poznamo toliko sistemov, kolikor je organizacij. V teoriji velja, da preden sistem upravljanja s tveganji vzpostavimo, natančno proučimo informacijski sistem, identificiramo njegove ranljivosti, grožnje, verjetnosti napada in posledice, ki bi pri tem nastale. S tveganji pa lahko upravljamo na različne načine. Najpogosteje organizacije izbirajo med neformalnim, splošnim, natančnim ali pa kombiniranim pristopom. Ko je pristop izbran, uvedemo nadzorne mehanizme s katerimi se tveganjem preprosto izognemo, lahko blažimo le posledice, lahko določeno tveganje sprejmemo ali pa vpeljemo ustrezne varnostne mehanizme. Zaradi nenehnih sprememb pa je potrebno takšen sistem stalno evalvirati in izboljševati.

Izvirnost
Strokovni prispevek bo proučil teoretične smernice za vzpostavitev varnega informacijskega sistema in ugotovitve kako to poteka v praksi. Izvirnost se kaže v proučitvi trenutnega stanja v različnih organizacijah. Le-te lahko upoštevajo različne smernice, priporočila in dobre prakse, kamor spada tudi serija standardov ISO 27000. Ugotovitve kažejo, da je v procesu upravljanja informacijske varnosti ključnega pomena zaveza vodstva za vzpostavitev sistema upravljanja s tveganji, prepoznavanje kritičnih področij in ustrezno zavarovanje le-teh.

Ključne besede:informacijski sistem, upravljanje, tveganja, spremembe, varnostne grožnje

1 Uvod

»Ni varnosti na enem področju, če-le ta ni zagotovljena na vseh drugih«.- Edwin Markham (Robinson, 1999)

Vse, kar človek naredi, lahko človek premaga. Vse kar za to potrebujemo, je zadostna količina znanja, časa in denarja. Če je slednjega dovolj se bo vedno našel nekdo, ki bo storil vse, da bi onesposobil potreben del varnostnega sistema. V obdobju agresivne tekmovalnosti med podjetji (v državni in zasebni sferi), so le-te pripravljene storiti in plačati vse, da bi se polastile informacijskega premoženja svoje tekmice ali sovražne organizacije. Informacija pridobljena ali uničena, z vdorom skozi varnostni sistem, organizacijam-storilkam velikokrat omogoča lansiranje produkta na trg, še preden bi ga predstavila prava lastnica. Škoda, ki pri tem nastane za oškodovano organizacijo je lahko nepopravljiva (Robinson, 1999). Znanje je torej kapital organizacije, s katerim je potrebno ravnati skrbno in ga znati čuvati pred tistimi, ki bi ga lahko zlorabili, na drugi strani pa ga tudi preudarno deliti z okoljem (Podbregar, 2008: 189).

Iz tega sledi, da je informacijska varnost eden izmed najpomembnejših aspektov uspešnega delovanja vsake sodobne organizacije, kajti vsako, še tako nepomembno dejavnost v človekovem življenju, spremlja določena stopnja tveganja. Le-ta pa so vseskozi prisotna tudi pri upravljanju in vodenju organizacijske dejavnosti.

Ker pa v tem digitalnem obdobju vsaka organizacija svojo vizijo podpira z informacijskim sistemom mora za dosego strateškega cilja, zagotoviti varno in nemoteno delovanje le-tega. Po mnenju Stoneburnerja, Gougena in Feringe (2002) je ravno informacijsko področje najbolj izpostavljena in ob neprimerni zaščiti najbolj ranljiva točka organizacijske strukture. Organizacije morajo natančno poznati vsakršno grožnjo, ki preti njihovemu varnostnemu sistemu, sicer so posledice tveganja lahko usodne za njeno preživetje.

A vendar popolne informacijske varnosti pred zlonamernimi vdori ni, saj se nasproti nenehno bolj dognanim sistemom varovanja postavljajo vedno bolj domišljeni načini, kako te sisteme premagati. Da bi se zavarovali na čim bolj učinkovit način, je potreben cel nabor ukrepov, od defenzivnih do proaktivnega pristopa (Podbregar, 2008: 190).

Pri načrtovanju ustrezne stopnje varnosti se moramo vedno vprašati: »Če je neka informacija izgubljena, ali lahko škoduje organizaciji, oz. zagotovi prednost drugi« (Robinson, 1999)? Če je odgovor pritrdilen, je vzpostavitev varnostnih ukrepov za zavarovanje le-te neizogibna. Da pa lahko organizacija zagotovi ustrezno stopnjo varnosti lastnemu informacijskemu sistemu, se mora grožnjam zoperstavljati. To počne v procesu upravljanja s tveganji, s katerim se zagotavlja relativno varno in stabilno delovanje organizacije. Postopek upravljanja s tveganji je povsem odvisen od vsake organizacije posebej, kar pomeni, da poznamo toliko načinov upravljanja s tveganji kolikor imamo organizacij. Slednje lahko v osnovi izbirajo med štirimi različnimi pristopi: (1) neformalen je strokoven pristop brez sistematičnih/strukturiranih metod, (2) splošen pristop pomeni izbiro standardiziranih varnostnih mehanizmov za vse dele informacijskega sistema, (3) natančna analiza vključuje identifikacijo in oceno premoženja, groženj in njihove resnosti skozi preučevanje ranljivosti tega premoženja, (4) kot najbolj koristen se kaže četrti pristop, to je kombinirana tehnika, pri kateri so kritični deli/sistemi podvrženi natančni analizi, medtem ko so ostali manj pomembni/ranljivi sistemi predmet osnovne analize/obravnave (Trček, 2006: 21-22).

V teoriji je v postopek upravljanja s tveganji nujno vključena identifikacija in evalvacija informacijskega premoženja organizacije. V nadaljevanju je potrebno iz preteklih izkušenj ugotoviti in oceniti grožnje, ki pretijo temu premoženju, prav tako pa identificirati njegove

ranljivosti, ki bi lahko bile izkoriščene. Potreben je še izračun verjetnosti, da bo prišlo do tovrstnega napada in posledice, ki bi pri tem nastale.

Za ugotovitev najprimernejših mehanizmov zavarovanja informacijskega sistema je torej natančna analiza sistema neizogibna. Tovrstna analiza oskrbuje management z informacijami na katerih le-ta snuje svoje odločitve. Glavni cilj je zagotoviti ravnovesje med tveganji in ceno za implementacijo preventivnih in zaščitnih ukrepov (Sennewald, 2003). Po analizi sistema, na podlagi ugotovitev, organizacija izbere primeren način obvladovanja teh tveganj. Odločiti se mora za eno od štirih osnovnih strategij za nadzor tveganj (Whitman in Mattord, 2008: 297): (1) izogibanje: uporaba zaščite, ki izključi ali zmanjša preostala nenadzorovana tveganja, (2) prenos: premikanje tveganj na druga območja ali izven organizacijske entitete, (3) blaženje: zmanjšanje škode v primeru, da napadalec uspešno izkoristi ranljivost, (4) odobritev: razumevanje posledic in priznavanje tveganja brez poskusa nadzora ali blažitve. Ko je takšen sistem enkrat vzpostavljen ga je potrebno nenehno preverjati, ocenjevati in izboljševati. Učinkovitost sistema preverjamo tako, da ugotavljamo, če so bili stroški uvedbe nadzorstev manjši od letnih stroškov, ki so se pojavljali zaradi varnostnih incidentov (Pfleeger, 1989: 465).

Sistem upravljanja s tveganji je torej nenehen in cikličen proces, ki ga uporablja vodstvo, management in strokovno osebje, za prepoznavanje ranljivosti v informacijskem sistemu organizacije, z namenom zagotavljanja zaupnosti, integritete in dostopnosti vseh komponent informacijskega sistema (Whitman in Mattord, 2008). Čeprav teorija natančno razlaga, kako naj bi takšen sistem potekal, pa je njegova oblika odvisna od različnih dejavnikov, kot so; velikost organizacije, zainteresiranost vodstva, usposobljen kader in finančna zmogljivost vzpostavitve in vzdrževanje takšnega sistema.

Organizacije si ravno zaradi tega pri vzpostavitvi čim bolj primernega sistema lastni organizacijski strukturi lahko pomagajo z vpeljevanjem standarda ISO 27001 namenjenemu informacijski varnosti, lahko pa se odločijo tudi za pridobitev certifikata, ki tako dokazuje popolnost, strokovnost in zaupnost organizacije. Standard povzema in priporoča sledenje modelu PDCA (Plan, Do, Check, Act), za prilagajanje spremembam. Gre za štiristopenjski program, v katerem spremembo načrtujemo, jo uvedemo nato pa še preverimo uspešnost in zanesljivost uvedenega. Na koncu napravimo še izboljšave in s procesom nadaljujemo od začetka (Tague, 2004). V procesu certificiranja je ključnega pomena zaveza vodstva za vzpostavitev sistema upravljanja s tveganji, prepoznavanje kritičnih področij in ustrezno zavarovanje le-teh. Pri izbiri organizaciji ustreznega varnostnega mehanizma si lahko pomagamo s smernicami standarda ISO 27002 (ISO 27000 Directory). Za vodenje sistema upravljanja s tveganji in natančne analize sistema, pa lahko sledimo priporočilom standarda ISO 27005. Za pridobitev certifikata ISO 27001, se organizacije odločajo z namenom zagotoviti večjo stopnjo varnosti, povečati strokovnost, kredibilnost in zaupnost organizacije, ali pa preprosto zaradi želje poslovnih partnerjev. Druge pa smernice upoštevajo, vendar se za pridobitev certifikata ne odločijo.

Organizacije si torej lahko pomagajo z mnogimi dobrimi praksami in si tako olajšajo proces upravljanja s tveganji. Le-ta je v teoriji zelo izčrpen, mnogokrat zapleten in zamuden. Zaradi različnosti in kompleksnosti organizacijskih in informacijskih struktur, pa se načini vzpostavitve in vodenja zaščitnih ukrepov med organizacijami razlikujejo. Avtorja sva se, zaradi tega odločila narediti pregled teh sistemov v različnih slovenskih organizacijah. V vzorec 20 organizacij sva zajela tako tiste najmanjše organizacije, podizvajalce in tiste največje, samostojne, tako v državni kot v zasebni sferi. Z usmerjenimi intervjuji sva želela pridobiti vpogled v dejavnike, ki vplivajo na načine zavarovanja informacijskih sistemov, prav tako pa ugotoviti, kako posamezna podjetja dojemajo lasten položaj v sferi nenehnih ogrožanj in kako le-ta vplivajo na njihovo poslovanje.

2 Ugotovitve

O pomenu informacijskega sistema v večini organizacij (70%) ugotavljajo, da je konkurenčno prednost in uspešnost na globalnem trgu moč doseči le s kakovostnim, k uporabniku usmerjenim informacijskim sistemom. Prav tako menijo, da brez informacijskega sistema ne morejo doseči v organizaciji zastavljenih ciljev. Ostale organizacije pa menijo, da je informacijski sistem sicer pomemben del njihove strukture, vendar ni ključnega pomena za njihovo delovanje. Visok delež odvisnosti od informacijske tehnologije, kaže na pomembnost zaupnih, razpoložljivih in neokrnjenih informacijskih sistemov.
Večji delež organizacij (60%) ugotavlja, da je za njihovo uspešno in nemoteno delovanje kritična zaščita podatkov. Pri tem preseneča dejstvo, da so nekatera podjetja opredelila kot pomembno tudi strojno opremo informacijskega sistema. Z vidika zaščite podatkov in integritete je to vsekakor smiselno, vendar meniva, da je za uspeh organizacije kritična predvsem zaščita podatkov ob jasni predpostavki, da je na delu strojne in programske opreme izvedeno vse, kar zagotavlja stabilen, varen učinkovit in zmogljiv IS.
Iz prejšnjega odgovora o kritičnem premoženju za uspeh organizacije sledi tudi zavarovanje najpomembnejših elementov in s tem povezani stroški. Glavni stroški delovanja in obnavljanja informacijskega sistema nastajajo na nivoju podatkov. Zakaj? Ob katastrofi je možno nadomestiti strojno in programsko opremo relativno hitro. Obnova podatkov, identifikacija zadnje še dobre varnostne kopije, izgubljeni podatki med varnostnim kopiranjem do katastrofe in nepričakovani problemi pri restavraciji podatkov pa privedejo do razmer, ki ne zagotavljajo takojšnjega uspešnega nadaljevanja s poslovnimi procesi nad / z ustreznimi podatki. Tako ni presenetljivo, da se je delež »kritičnih« na strani podatkov v primerjavi z odgovori na prejšnje vprašanje pomembno povečal (70%).
Če prej ugotavljamo, da je najdražje in najtežje zavarovati podatke, pa se skoraj 2/3 vprašanih v tem primeru nagiba k cenovni nesprejemljivosti programske opreme informacijskega sistema. Res je, da v primeru navezanosti na eno okolje (npr. Windows) in odvisnosti od specialne programske opreme (uporaba npr. ASPja namesto PHPja) pride do odvisnosti od programja skupine oz. podjetja, vendar so to relativno poznani postopki prehoda in so v praksi mnogokrat izvedeni. Pri podatkih pa predstavlja glavni problem dejstvo prenosa oz. transformacije podatkov iz starega sistema v novega. To samo po sebi niti ni problematično, vendar praksa kaže, da pri prenosu prihaja do nenamernih, neželenih napak, s tem pa se integriteta podatkov bistveno zmanjša. Tako imamo dve možnosti ukrepanja: dopustiti napake v informacijskem sistemu in podatkom ne zaupati v celoti ali pa porabiti mnogo sredstev (časa, denarja, znanja) za zagotovitev primerne integritete na podatkovni strani, kar pa v končni fazi pomeni za podjetje visoke stroške. Žal v raznih primerih vse premalo poudarka namenimo prenosu podatkov in njihovemu ustreznemu obnavljanju, pereče pa je tudi, da stroškov prenosa pri zamenjavi, nadgradnji ali obnovi sistema pogosto niti ne znamo pravilno ovrednotiti.
Ker je bilo pri prejšnjih odgovorih čutiti rahlo nepozornost in ozko razmišljanje o menjavi elementov informacijskega sistema pa je sedaj razvidno, da se podjetja za varovanje svojega premoženja poslužujejo različnih načinov – od najpreprostejših in najpogostejših do najzahtevnejših. Tako vidimo, da 70% podjetij za zavarovanje informacijskega premoženja uporablja glavne elemente zavarovanja podatkov in zagotavljanja informacijske varnosti. »Moti« le dejstvo, da na prvo mesto postavljajo poslovno zavarovanje. Zakaj bi nekaj zavaroval, če lahko preprečim škodo s preprostimi ukrepi? (npr. backup) Strežniki z varnostnimi kopijami, redno arhiviranje, ustrezna raba gesel, zagotavljanje razpoložljivosti delovanja strojne opreme,... so preprosti in poceni ukrepi, ki pa se jih poslužuje premalo podjetij. Na tem nivoju, kljub

miselnosti, da so tehnični elementi informacijske varnosti ustrezno urejeni, pa praksa kaže, da je na tem mestu še dovolj rezerve in možnosti za izboljšanje informacijske varnosti. To lahko dosežemo z relativno nizkimi stroški in poznanimi, zanesljivi rešitvami. Pri dodatnem, naknadnem preverjanju smo ugotovili, da se podjetja nekaterih omenjenih elementov sicer poslužujejo, vendar zaradi dolge rabe in nevsiljivosti v informacijske sisteme nanje preprosto ne pomislijo več v povezavi z varnostjo sistema, pač pa kot integralni del celovitega informacijskega sistema. To kaže na višanje kulture poznavanja problematike informacijske varnosti z vidika zaščite in ohranjanja razpoložljivosti podatkovnih virov v informacijskih sistemih.

Zgoraj predpostavljeno in naknadno ugotovljeno se pokaže pri odgovorih na vprašanje o načinu shranjevanja kritičnih informacij. Dejansko vsa podjetja uporabljajo poseben način hranjenja kritičnih informacij in njim ustrezno zaščito (varnostne kopije, dvojne lokacije, arhiviranje, posebni strežniki ipd.). Izbrani načini so sicer različni; tudi po dodatni analizi se ne pokaže, da podjetja, ki so po ustroju in velikosti podobna uporabljajo primerljive načine, vendar pa zagotavljajo ustrezno varovanje informacijskega premoženja podjetja.

Za zagotavljanje najpomembnejših vidikov informacijske varnosti organizacije uporabljajo osnovne načine zaščite (gesla, kriptiranje zapisov, varnostne kopije ipd.), poznane že dolgo, ko problematika informacijske varnosti še ni bila tako pereča kot danes. Sodobne, naprednejše tehnike (politika neprekinjenega poslovanja, SSL, TLS tehnologija, digitalna potrdila ipd.) in predvsem višje nivoje zašite podatkov in s tem boljšo zanesljivost, razpoložljivost in neokrnjenost pa uporabljajo le nekatera, tehnološko naprednejša podjetja. Pri podrobnem pregledu podatkov skrb vzbuja dejstvo, da podjetja, ki bi v osnovi morala spoštovati zakon (npr. o varstvu osebnih podatkov) nimajo vzpostavljenih ustreznih mehanizmov zaščite za ustrezno stopnjo informacijske varnosti glede na znane faktorje tveganja.

Sodelujoče organizacije uporabljajo zelo različne pristope pri upravljanju s tveganji na področju informacijske varnosti. Žal se celovito kaže, da se k informacijski varnosti v podjetjih še vedno preveč stihijsko pristopa, večinoma se organizacije poslužujejo enega pristopa (kombiniranega le 1/3 vprašanih), kar kaže na predpostavko, da podjetja ne pristopajo dovolj celovito in metodično k problematiki informacijske varnosti. Poleg kombiniranega, najpogosteje uporabljajo še splošnega in neformalnega, saj le-ta zahtevata najmanj truda, časa in finančnih virov. Skrb vzbujajoče pa je tudi dejstvo, da kar 5% izprašanih organizacij s tveganji sploh ne upravlja.

Necelovit in ne ustrezen pristop se kaže tudi pri oceni sistema upravljanja s tveganji. Le 35% organizacij je lasten sistem ocenilo kot dobrega, ostala večina pa kot nezadostnega ali slabega. Zaskrbljujoče je tudi dejstvo, da se med nekvalitetnimi pojavljajo tudi organizacije, katerih informacijski sistemi so povezani z življenjsko pomembnimi komponentami. V razgovoru se hitro izkaže, da se v celovito zagotavljanje informacijske varnosti vodstvo angažira premalo, s tem ni ustrezne podpore in tudi ne primernih rešitev in mehanizmov „prisile“ zaposlenih za odgovorno ravnanje. Skrbi podatek, da le nekatera podjetja svoje upravljaje s tveganji izvajajo na nivoju mednarodnih standardov. Zakaj? Informacijski sistemi in njihovo vključevanje v internetno omrežje so del globalnih komunikacij in omogočajo globalni dostop, torej tveganja na varnost informacijskega sistema obstajajo na globalni ravni, zato je izvajanje ukrepov informacijske varnosti danes ne le potreba, pač pa nuja.

Problematike informacijske varnosti v podjetju bi se morali zavedati vsi. Vzpostavitev, delovanje in vzdrževanje sistema pa je običajno na strani ustrezne tehnične službe ali zunanjih pogodbenih partnerjev z močno podporo vodstva. Vse izprašane organizacije navajajo, da za potrebe informacijske varnosti skrbi strokovno osebje, ki je del službe oz. oddelka za informatiko ali pa vodstva in zaposlenih.

Pri obravnavi groženj je potrebno razumeti, da so najmanj očitne najbolj nevarne. Če se proti

virusom, napakam opreme, vdorom s tehničnimi sredstvi, ki so najpogostejše grožnje, ki jih organizacije navajajo, preprosto in relativno poceni zoperstavimo (antivirusni programi, ustrezno kopiranje podatkov, požarni zid), pa se največja grožnja za izgubo podatkov večinoma pojavlja človeški faktor. Mnogokrat se zaradi neznanja in nezavedanja kaj za poslovni sistem pomenijo tajni podatki in neodgovorno posredovanje vpletenih zgodi, da je največji odtok pomembnih podatkov ravno skozi t.i. „človeški“ kanal.

Že iz prejšnjega odgovora nakazano, pa se ozek pogled na problematiko kaže tudi v primeru najbolj kritičnih groženj informacijskemu sistemu. Tu lahko ugotovimo, da je pogled na področje še vedno preozko (organizacije kot najbolj kritične grožnje v največji meri navajajo vdore in napake sistema, viruse, okvare podatkov in nedostopnost sistema) in da bo v obravnavanju sistemov zagotavljanja informacijske varnosti potrebno spremeniti pogled iz tehničnega razumevanja informacijske varnosti na “uporabniški” vidik informacijske varnosti. Ugotavljava namreč, da so tehnični aspekti informacijske varnosti v večini podjetij dobro urejeni, preprosto pa se gleda, da so največje grožnje sistemom iz škodljive programske opreme. Vendar se ta v sodobnih sistemih aktivira šele, ko jim to na nek način dopusti uporabnik (z dostopom do okuženih vsebin, “radovednim” odpiranjem datotek, ki so okužene, ipd.). Prav tako se tu zopet pozablja na zaposlene v stiku z okoljem in njihovo nekritično posredovanje informacij v okolico.

Na podlagi prejšnjih odgovorov lestvica najbolj ranljivih komponent informacijskega sistema ne preseneča. Različnost odgovorov (kot najbolj ranljiva se kaže programska oprema, nato strojna oprema, dokumentacija in komunikacije) in njihove kombinacije potrjujejo spoznanje, da je razumevanje informacijske varnosti v podjetjih zelo raznoliko, pogled na to področje pa široko. Dejstvo je, da je zavedanje o ranljivosti sistema še vedno pogosto videno iz delovanje sistema samega, ne pa iz poslovnega vidika pri katerem se ugotavlja, da je največja vrednost poslovnega sistema v podatkih iz katerih na podlagi poznavanja sistema in okolice črpamo potrebna znanja, ki zagotavljajo strateški boj sistema z tekmeci. Z izgubo podatkov tekmecem posredujemo obilico podatkov, ki jih v kombinaciji s svojimi podatki uporabijo za širše razumevanje problema in na ta način pridobijo znanje in razumevanje, ki jih naš poslovni sistem zaradi manjšega nabora podatkov nima.

Presenetljivo so v kar Ľ organizacij prepričani v neverjetne posledice v primeru napake ali odtujitvi pomembnih informacij. Sama napaka ali luknje v varovanju IS verjetno težko povzročijo smrt osebja, odgovornega za informacijsko varnost, vendar v sistemih kritične infrastrukture, vojski, policiji in podobno, posledice izgube podatkov lahko dejansko pripeljejo do smrti, kar še bolj nakazuje pomembnost razvijajočega se področja informacijske varnosti.

Organizacije, kot psihološke učinke nedostopnosti storitev v največji meri navajajo izgubo kredibilnosti, med poslovnimi partnerji in uporabniki. Kot posledice, ki bi temu sledile pa razumejo še izgubo posla, sramoto in slabo voljo. Izguba kredibilnosti zelo pogosto pomeni izgubo poslov, zato se večina poslovnih subjektov v primeru izgube podatkov odloči, da s tem ne seznanja javnosti. Tako je dejansko stanje ogroženosti in že zlorabljenih sistemov v nekem okolju mnogokrat nemogoče oceniti, s tem pa se ne identificirajo grožnje v okolju. To posledično vodi, da se podjetja pripravljajo na zagotavljanje celovite informacijske varnosti le z lastnim poznavanjem problematike, kar pa je drago, zahtevno in malo učinkovito.

Pri ocenjevanju pogostosti napadov na informacijski sistem skoraj polovica (45%) organizacij navaja, da so napadi na njihov sistem redki. Četrtina izprašanih trdi, da napadov na sistem sploh nimajo, ostale organizacije pa beležijo pogostejše napade na njihov informacijski sistem. Vendar pa je ocenjevanje pogostosti napadov na informacijski sistem je v informacijski varnosti kritično. Podjetja namreč delujejo le na podlagi detektiranih napadov na sistem, ob tem pa mnogokrat pozabljajo, da mnogo napadov na sistem ni detektiranih. Le ti pa pomenijo mnogo večjo grožnjo

sistemov z vidika – če ne poznaš problema ga ne odpravljaš...
Potrditev zgornjih ugotovitev je zapis najpogostejših napadov. Dejansko podjetja navajajo tista, ki jih je najlažje detektirati oz. v primeru napada pomenijo nek resen incident za informacijski sistem organizacije (virusi, trojanski konji, črvi, spam, ipd.). Stalno spremljanje delovanja sistema, neželen nadzor podatkov in ostali težje zaznavni napadi na informacijski sistem pa niso omenjeni.
Ocenjevanje škode v primeru takšnih napadov seveda situacijo postavi v drugačno perspektivo. Več kot tretjina organizacij navaja, da je škoda, ki pri tem nastane sprejemljiva. Druga tretjina meni, da je škoda velika oz. nepopravljiva, seveda pa je manjši delež trdil, da je škoda pri tem neopazna. Dokler o napadih govorimo, ugotavljamo, da so le ti možni, najhujši poseg v integriteto informacijskega sistema pa je okužba z virusi ali črvi, ob omembi informacijske varnosti ne postanemo pozorni. Ko pa pride do dejanskega napada na informacijski sistem, izgube podatkov, okrnjenosti integritete in prekinitve delovanja pa se pričnemo zavedati dejanskega stanja – informacijska varnost je pomemben del našega vsakdanjika, varnost informacijskega sistema pa pomemben aspekt poslovanja organizacije.
Pri ugotavljanju nadzorstev je razvidno, da se večina organizacij v največji možni meri izogiba tveganjem. V nadaljevanju precej manj uporabljajo prenos in blaženje tveganj, zgolj delno in še to le nekatere organizacije pa uporabljajo odobritev tveganj. Rezultati so na podlagi prejšnjih opažanj razumljivi in pričakovani.
Kot kaže splošno stanje informacijske varnosti, se nekatera podjetja še ne zavedajo njenega pomena in tudi ne uporabljajo mehanizmov za vzpostavitev, nadzor in izboljšavo le-te. Le polovica organizacij lasten sistem informacijske varnosti stalno izboljšuje, ostale izprašane pa ga le po potrebi ali pa sploh ne. Prva splošna priporočila bi tako podjetjem šla, naj pričnejo uporabljati PDCA krog, s tem začnejo na bazičnih elementih informacijske varnosti, skozi stalno evalvacijo pa naj jo izboljšujejo, do potrebne stopnje glede na znane faktorje tveganj.
Seveda pa je za zagotavljanje visoke stopnje informacijske varnosti potrebno vključiti vse uporabnike (zaposlene + zunanje) informacijskega sistema organizacije. Udeležene v raziskavi navajajo, da na potrebe po izboljšanju varnosti najpogosteje opozarjajo zaposleni v organizaciji, nato uporabniki, informatiki, partnerska podjetja in revizorji. Tako se morajo vsi na nek način prizadevati za varen informacijski sistem in visoko stopnjo celovite informacijske varnosti sistema. To je še posebej pomembno pri odpiranju informacijskih virov partnerskim organizacijam za vzpostavitev elektronskega poslovanja in medsebojne virtualne organiziranosti.
Podjetja oz. zaposleni imajo mnogo predlogov, kje pričeti z izboljševanjem (shranjevanje podatkov na oddaljeni lokaciji, upravljanje s tveganji, večja varnost na lokalnem nivoju, redno posodabljanje sistema, izboljšanje medsebojne komunikacije, uvajanje formalne varnostne politike, ipd.), vendar pa večina ukrepov potrebuje vsaj minimalne investicije, ki pa jih poslovni subjekti v času soočanja s krizo nimajo. Zato je potrebno čim prej (takoj) pričeti z ozaveščanjem zaposlenih, opozarjanjem na potencialne nevarnosti in grožnje in vložiti napore v zavedanje zaposlenih o potrebi po skrbnem ravnanju z informacijami. Ta ukrep je ob dobrem managementu in podpori vodstva možno uvesti ob minimalni investiciji. Tako se skupna varnost izboljša in namesto investiranja v odpravo posledic izgub podatkov bo sredstva možno nameniti za vzpostavitev manjkajočih ali neustreznih zgoraj omenjenih sistemov.
Organizacije so kot predlog za povečevanje informacijske varnosti navajale tudi postopek certificiranja. Na tem področju je najbolj učinkovita, preverjena in zanesljiva serija standardov ISO 27000, namenjena izključno vzpostavljanju informacijske varnosti in vodenju procesa upravljanja s tveganji.
Skladno z zavedanjem prednosti formaliziranja kakovosti informacijske zaščite večina

organizacij (60%) navaja, da pri zagotavljanju varnih informacijskih sistemov upoštevajo smernice, ki jih nalaga standard ISO 27005. Ostale teh smernic ne vpeljujejo v zaščito lastnih sistemov. Dejstvo, da več kot polovica organizacij spremlja in izpolnjuje navodila tovrstnega standarda, kaže, da se zavedajo prednosti dobrih praks in priporočil. Standard ISO 27005 organizacijam daje usmeritve, kako zagotoviti varen informacijski sistem v procesu upravljanja s tveganji, pri tem pa ji pušča veliko manevrskega prostora pri vzpostavljanju lastne stopnje zaščite. Glede na to, da pri tem ni potreben postopek certificiranja za sledenje tem smernicam, bi lahko le-te upošteval večji delež organizacij. Razumevanje njihovih koristi pa ni odvisno od velikosti ali dejavnosti, temveč meniva, da je njihovo upoštevanje in vpeljevanje v sistem upravljanja s tveganji odvisno predvsem od ozaveščenosti in volje zaposlenih ter njihovega vodstva.

Glede na dejstvo, da se večina organizacij dobro zaveda resnosti sodobnih informacijskih groženj in potrebe po vzpostavitvi učinkovite varnosti za zagotovitev neprekinjenega poslovanja, se lahko le peščica organizacij (15%) pohvali s certifikatom ISO 27001. Le-ta je namenjen zagotavljanju varnosti informacijskih sistemov in je znak zaupnosti, strokovnosti in popolnosti organizacije. Njegova uvedba, je tako kot pri prejšnjemu, povsem neodvisna od vrste dejavnosti in velikosti organizacije, temveč so na tem mestu drugi odločilni dejavniki, ki pogojujejo zavezo za pridobitev certifikata. Ker pa je to relativno nov proces v slovenskih organizacijah, meniva, da je pomanjkanje informacij o njegovi prednostih in koristih eden izmed teh dejavnikov.

Organizacije, ki certifikat za standard ISO 27001 imajo, navajajo, da so ga uvedle v preteklih štirih letih, največ v letu 2009. To potrjuje dejstvo, da se organizacije šele seznanjajo s to prakso in je porast njegove uvedbe v organizacijske sfere mogoče pričakovati v prihodnjih letih.

Udeleženke v raziskavi, kot prednost standarda navajajo večje zadovoljstvo uporabnikov, vodstva, zaposlenih in poslovnih partnerjev. To nakazuje, da je eden izmed razlogov uvedbe standarda in certificiranja tudi zahteva poslovnih partnerjev, saj se z uradnim potrdilom poveča kredibilnost in zaupnost organizacije. Najverjetneje pa se tudi uporabniki lažje odločajo za uporabo varnostno certificiranih sistemov. Kot prednost so organizacije navedle tudi možnost, da si organizacije same določijo ustrezen nivo varnosti in pri tem niso omejene z ozkimi okvirji. Stopnjo varnosti lahko tako prilagodijo dejavnosti in velikosti organizacije, posamezna področja pa zavarujejo glede na njihove ranljivosti.

Organizacije občutijo, povišanje stopnje varnosti po uvedbi standarda ISO 27001. Z upoštevanjem priporočil, ki jih oblikujejo strokovnjaki za informacijsko-varnostnega področja, te navedbe niso presenetljive. Pravzaprav bi bilo presenetljivo dejstvo, da bi se po dolgotrajnem trudu in naporu izpolnjevanja zahtev standarda, varnost poslabšala ali stagnirala. Standard je namenjen izboljšanju varnostne stopnje informacijskih sistemov in ob navedbah organizacij, svoj namen tudi izpolnjuje.

Organizacije prav tako navajajo izboljšanje oz. povečanje poslovanja po uvedbi standarda in njegovem certificiranju. Standard je znak kakovosti in kredibilnosti in najverjetneje se poslovni partnerji veliko raje odločajo za sodelovanje s podjetji, ki imajo zagotovilo o učinkovitem in stabilnem informacijskem sistemu. Tudi uporabniki kakovost organizacije in njenih storitev pogojujejo s formalnimi potrdili. Povišanje varnosti in uspešnosti organizacije sta tako posledici, ki sledita uvedbi standarda ISO 27001 in njegovi certifikaciji.

Organizacije, ki standarda (še) niso uvedle navajajo, da je njihova varnost tudi brez tega zadostna oz. učinkovita in ne čutijo potrebe po certificiranju. Med razloge za ne-uvedbo navajajo tudi pomanjkanje finančnih virov. Postopek certificiranja od organizacije sicer terja določene finančne stroške, vendar so le-ti dolgoročno z višjo stopnjo varnosti vsekakor povrnjeni. Neozaveščenost oz. pomanjkanje informacij o prednosti in kakovosti standarda prav tako vpliva na odločitev o

njegovi uvedbi. Druge v raziskavo vključene organizacije pa navajajo, da je njihova organizacijska struktura na ta standard nepripravljena in bi bila potrebna njegova reorganizacija, ali pa je premajhna za vpeljevanje tako visokih zahtev. Pomanjkanje ustreznega kadra je prav tako lahko ovira pri izbiri in vpeljavi ISO 27001. Razlogi za ne-uvedbo so torej najrazličnejši in variirajo od organizacije do organizacije. Lahko bi rekli, da je pogoj oz. odločitev za vpeljevanje in certificiranje odvisna od velikosti podjetja, njegove organizacijske strukture in finančnih virov.
Kar polovica organizacij brez certifikata ISO 27001 navaja, da je odločitev o uvedbi tovrstnega standarda v največji meri odvisna od volje in zaveze vodstva. Njihova odločitev pa je najverjetneje pogojena z drugimi dejavniki, ki jih navajajo ostale izprašane organizacije. Vodstvo bo odločitev za vpeljevanje standarda in postopek certificiranja, sprejelo kadar bo na voljo imelo zadostno količino finančnih virov, njihova organizacijska struktura pa bo na to ustrezno pripravljena. Tudi ponudba in ozaveščenost o prednosti takšnega standarda odigra veliko vlogo za odločitev o njegovi uvedbi. Iz tega je razvidno, da je uvedba standarda v največji meri odvisna od volje vodstva organizacije, le-ta pa je pogojena z ostalimi dejavniki v organizacijski strukturi, ki smo jih ugotovili že pri prejšnjem vprašanju.
Mnenja organizacij o potrebnosti certifikata v njihovi informacijski strukturi je deljena. Skoraj polovica organizacij (47%) meni, da takšnega standarda ne potrebujejo. Najverjetneje se razlogi za to skrivajo v zadostni varnostni infrastrukturi informacijskega sistema in pomanjkanja ozaveščenosti o sami prednosti in kakovosti takšnega standarda. Poslovanje takšne organizacije je torej zadovoljivo in ne čuti potrebe po izboljšavi in formalni potrditvi lastne varnostne strukture. Ostale organizacije pa menijo, da bi takšen standard potrebovale. Najverjetneje so te bolje informirane o koristih, ki jih uvedba takšnega standarda lahko prinese, prav tako pa si želijo bolj kakovosten, varen, stabilen in kredibilen informacijski sistem.
Organizacije, ki menijo da bi jim uvedba takšnega standard koristila (41%) in bi bila potrebna menijo, da bi se stanje varnosti po njegovi uvedbi izboljšalo. S tem so se strinjale že organizacije, ki ta standard imajo saj so po uvedbi standarda ISO 27001 občutile večjo stopnjo varnosti in zaščite na lastnem informacijskem sistemu. Da to predvidevajo tudi organizacije, ki standarda nimajo, vendar menijo, da bi ga potrebovale, kaže na visoko stopnjo ozaveščenosti in informiranosti o koristih certificiranja zaščite informacijskega sistema. Ostale organizacije pa se le-tega ne zavedajo, zatorej menijo, da se njihova varnost po uvedbi ne bi izboljšala. Razlog za takšno mnenje je poleg neobveščenosti lahko tudi zadostna ali najvišja možna stopnja zaščite informacijskih sistemov. Meniva, da je to manj verjetna možnost, saj so spremembe v informacijskem okolju nenehne, kar otežuje spremljanje groženj in posodabljanje lastnih informacijskih sistemov. Grožnje le-tem so navadno vedno korak pred ukrepi, ki jim grozijo.
Večina (59%) izprašanih organizacij, ki certifikata ISO 27001 ne posedujejo, ga prav tako tudi v prihodnosti nima namena uvesti in certificirati. Razlogi za to so že bili našteti, najverjetneje pa je odločilnega pomena pomanjkanje finančnih virov in zadostna varnostna struktura. Morda se bo v prihodnosti z razvojem teh organizacij in pojavom novih, bolj naprednih in sofisticiranih groženj tovrstna miselnost spremenila. Organizacije, ki so pred tem že navedle potrebo po tovrstnem standardu pa izražajo tudi namen po njegovi uvedbi v prihodnosti. Za to potrebujejo priprave tako na ravni zaposlenih kot organizacijsko-informacijske strukture, kar pomeni, da takšnega standarda ne moremo v strukturo vpeljati čez noč. Potrebna je temeljita usposobljenost celotne organizacijske sfere, da bo lahko takšen standarda dosegel svoj namen.

3 Sklep

Informacijski sistem je osnovna komponenta vsake organizacije, ki nudi podporo pri doseganju

zastavljenih ciljev. Lahko bi rekli, da je uspeh organizacij v veliki meri odvisen od njihovega informacijskega sistema. Kvaliteta takšnega sistema torej diktira kvaliteto organizacije. To dejstvo potrjujejo tudi ugotovitve izpeljane iz raziskave, v kateri večina organizacij navaja, da brez informacijskega sistema ne morejo doseči vizije oz. zastavljenih ciljev. V povezavi s tem uspešnost organizacije pogojujejo predvsem uspešno, na informacijskem sistemu, zavarovani in shranjeni podatki. Ker je od podatkov oz. dokumentacije odvisen posel organizacij, le-te največ finančnih virov, pri zavarovanju informacijskega kapitala namenijo ravno dokumentaciji. Pri tem pa za zavarovanje podatkov in ostalega premoženja najpogosteje uporabljajo standardizirane varnostne ukrepe in mehanizme, le peščica najbolj naprednih in razvitih organizacij pa se poslužuje tudi tehnično bolj sofisticiranih ukrepov. Le- ti niso odvisni od velikosti in ustroja neke organizacije, temveč v največji meri od njenih potreb in zmogljivosti. Od slednjega pa je odvisna tudi sama oblika sistema vzpostavljanja informacijske varnosti oz. upravljanja s tveganji prav tako pa tudi formaliziranje kvalitete informacijske varnosti. Postopek certificiranja je tako v največji meri odvisen od volje in zaveze vodstva, le-to pa svoje odločitve oblikuje na podlagi finančnih, kadrovskih in časovnih zmožnosti organizacij. In le peščica organizacij ima zadostne vire, ki jim omogočijo to formaliziranje. Dejstvo pa je, da dolgoročno to vodi v manjše stroške v primeru varnostnih incidentov. Ker so zmogljivosti večine organizacij na takšnem področju relativno nizke se za zagotovitev informacijske varnosti ne odločijo za formaliziranje in se tako največkrat poslužujejo enega samega pristopa. Sicer velik delež organizacij uporablja kombiniran pristop, vendar pa prevladujeta predvsem splošen in neformalen, ki zahtevata najmanj časa, znanja in finančnih virov. Najverjetneje je ravno, zaradi varčevanja na tem področju to privedlo do dejstva, da večina organizacij lasten sistem informacijske varnosti ocenjuje kot slab ali nezadosten. Na tem področju imajo organizacije še dovolj prostora za izboljšave in dobro je dejstvo, da se tega tudi zavedajo. Ne zavedajo pa se resnosti tveganj na področju informacijske varnosti, saj kot največje grožnje njihovim informacijskim sistemom, še vedno razumejo tiste najpogostejše in najočitnejše. Pri tem pa zanemarjajo človeški faktor, ki najpogosteje privede do možnosti uresničitve teh groženj. Posledice, ki uspešnim napadom sledijo, pa organizacije največkrat občutijo kot sramoto in izgubo kredibilnosti. Ker pa le-temu največkrat sledi tudi izguba posla, svoje oškodovanosti največkrat javnosti sploh ne priznajo. Iz tega torej izhaja, kot navajajo tudi organizacije, da so napadi na njihove informacijske sisteme zelo redki, pri tem pa zanemarjajo grožnje, ki jih njihova nezadostna stopnja zaščite sploh ne zazna. Zaščita torej zazna najpogostejše in največkrat najmanj nevarne grožnje, kar je skladno tudi z dejstvom, da organizacije navajajo, da je škoda, ki pri napadih na sistem nastane sprejemljiva. Zaključujeva, da je nezadostna stopnja zaščite vzrok in povod vsem nerazumevanjem in napačnim predstavam o resnosti in nevarnosti sodobnih groženj informacijskim sistemom. Največ kar lahko organizacije na tem mestu naredijo takoj, je izobraževanje in ozaveščanje zaposlenih ter uporabnikov informacijskega sistema. S tem se dviga stopnja varnostne kulture in tudi dejanska stopnja informacijske varnosti. Namesto okrevanju po varnostnih incidentih lahko dolgoročno, zaradi tega privarčevane stroške okrevanja, porabijo za bolj sofisticirane oblike zaščite.

4 Literatura

ISO 27000 Directory. The ISO27001 Certification Process. Pridobljeno 10.4.2010, na http://www.27000.org/ismsprocess.htm

Pfleeger, C.P. (1989). Security in Computing. Englewood Cliffs: Prentice-Hall.

Sennewald, C.A. (2003). Effective Security Management- 4th edition. Burlington: Elsevier Science.

Podbregar, I. (2008). Vohunska dejavnost in gospodarstvo. Ljubljana: Fakulteta za varnostne vede.

Robinson, R.R. (1999). Issues in security management; thinking criticaly about security. Woburn: Butterworth. Heinemann.

Stoneburner, G., Goguen, A. in Feringa, A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Pridobljeno 25.11.2009, na http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Tague, N.R. (2004). The Quality Toolbox; second edition. Pridobljeno 10.4.2010, na http://www.asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html

Trček, D. (2006). Managing Infomation Systems Security and Privacy. Berlin: Springer.

Whitman, M.E in Mattord, H.J. (2008). Management of Information Security. Boston: Course Technology Cengage Learning.