Upravljanje informacijske varnosti – strateški in operativni vidik

Daša Selan, študentka magistrskega študija, Fakulteta za varnostne vede, Univerza v Mariboru
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru

Namen

Z naraščanjem uporabe informacijskih tehnologij narašča tudi nevarnost za njeno zlorabo. Tako postaja vse pomembnejša varnost informacijskih tehnologij, posledično pa njeno organiziranje in upravljanje. Zato prispevek prikazuje upravljanje informacijske varnosti na dveh nivojih, predstavlja jasno segmentacijo opravil na področju informacijske varnosti z operativnega in strateškega vidika ter določa naloge in odgovornosti posameznikov za celovito zagotavljanje informacijske varnosti.

Metodologija

Uporabljali bomo metodo deskripcije in poizvedovanja. Predvidevamo, da se, tako vodstvo in management, kot ostali zaposleni v organizacijah, še vedno premalo zavedajo pomena zagotavljanja in upravljanja informacijske varnosti. V povezavi s tem menimo, da pristojnosti in odgovornosti za učinkovito zagotavljanje informacijske varnosti sploh niso opredeljene, če pa že so, zadevajo samo enega ali dva zaposlena znotraj službe za informatiko.

Ugotovitve

Varnost informacijskih tehnologij in rabe informacij je potrebno umestiti v strateške plane vsake organizacije, pripraviti program informacijske varnosti in skladno s predvideno organizacijsko strukturo upravljanja informacijske varnosti opredeliti delovna mesta, ki so neposredno ali posredno odgovorna za zagotavljanje informacijske varnosti. Tako bi organizacije z dejavnostmi na strateškem in operativnem nivoju poskrbele za zaupnost, celovitost in razpoložljivost informacij.

Omejitve

Izhajajoč iz teoretičnih predpostavk področja priporočila niso bila preverjena in vrednotena v slovenski praksi. Zato je potrebno pri uvajanju koncepta ravnati v skladu z priporočili, vendar se ne zanašati, da je možne vse elemente prenesti direktno.

Praktična uporabnost

Priporočila o obravnavanju informacijske varnosti v organizaciji z vidika upravljanja predstavljajo možnost za zagotavljanje ustrezne stopnje, pri čemer ni potrebno podrobneje členiti posameznih elementov posameznemu podjetj in preiskušati novih rešitev.

Izvirnost/pomembnost prispevka

Informacijska varnost ni le tehnični izziv, ampak predvsem izziv celotne organizacije in vodenja le-te, ki zajema upravljanje, poročanje in odgovornosti. Pri zagotavljanju informacijske varnosti je pomembna ustrezna podpora vodstva, vzpostavljen, tako strateški kot operativni nivo upravljanja informacijske varnosti, tehnologija primerna kompleksnosti informacijske podprtosti ter zavedanje pomembnosti ustrezne informacijske varnosti. Prispevek prikazuje

potrebno segmentacijo odgovornosti in postopkov za zagotavljanje celovite korporativne informacijske varnosti.

Ključne besede: informacijska varnost, upravljanje, strateški nivo, operativni nivo, odgovornosti

1 Uvod

Področje informacijske varnosti postaja v zadnjih letih vedno bolj pomembno. Čeprav se varnost informacij najpogosteje obravnava le kot tehnično vprašanje, zadeva tudi upravljanje, ki med drugim vključuje tudi obvladovanje tveganj, spremljanje rezultatov, upravljanje incidentov, poročanje in nenazadnje odgovornost.
Za zagotavljanje primerne informacijske varnosti pa so potrebni opredeljeni nivoji in naloge pri upravljanju informacijske varnosti v organizaciji. Naloge je potrebno razdeliti na različnih nivojih organizacije, iz česar izhajajo pristojnosti in odgovornosti za uspešno zagotavljanje zaupnosti, celovitosti in razpoložljivost informacij v organizaciji (Bernik, 2008). Zaupnost, celovitost in razpoložljivost pa so osnovni cilji informacijske varnosti.

2 Upravljanje informacijske varnosti

Informacijska varnost je vedno spreminjajoča in razvijajoča se aktivnost, ki pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem (Von Solms, 2009). Glavni elementi informacijske varnosti, poznani kot CIA model, so zaupnost (ang. confidentiality), celovitost (ang. integrity) in razpoložljivost (ang. availability). Informacijska varnost ni le tehnični izziv, ampak tudi izziv celotne organizacije in vodenja le-te, ki zajema tvegani management, poročanje in odgovornosti.
Upravljanje informacijske varnosti je postal bistven element celotnih aktivnosti organizacije. Opisuje dejavnosti, ki se nanašajo na varovanje informacij in sredstev informacijske infrastrukture pred tveganji izgube, zlorabe, razkritja ali poškodbe. Poleg tega je tudi nadzor, ki ga mora organizacija izvajati, da zagotovi pametno obvladovanje morebitnih tveganj. Najbolj pa vse elemente upravljanja informacijske varnosti zajame naslednja definicija: "Upravljanje informacijske varnosti je podmnožica upravljanja organizacije, ki zagotavlja strateške usmeritve, doseganje ciljev organizacije, ustrezno upravljanje s tveganji, odgovorno uporabo organizacijskih sredstev in spremljanje rezultatov programa varnosti organizacije." (IT Governance Institute, 2007)
Upravljanje informacijske varnosti določa *okvir* - *program*, v katerem predvideva skrb za vpeljavo, vzdrževanje in nenehno izboljševanje področja upravljanja informacijske varnosti. Program za upravljanje informacijske varnosti služi kot poslovni načrt za zaščito digitalnih sredstev. Navadno je enostaven in učinkovit. Najbolj učinkovit program je tisti, ki je preprost in vključuje vse zaposlene, ki se jih predvideva pri upravljanju informacijske varnosti in tudi tiste, ki so samo uporabniki informacij. Vsak program upravljanja informacijske varnosti bi moral, z namenom ugotovitve doseganja posameznega cilja, imeti definirane meje sprejetja, zavrnitve in odločnosti, ki bi jih lahko razumeli tudi tisti, ki se z informacijsko varnostjo ne ukvarjajo neposredno (npr. uporabniki informacij ali informacijske tehnologije).
Rezultati učinkovitega upravljanja informacijske varnosti morajo vključevati:

- strateško usklajevanje informacijske varnosti z institucionalnimi cilji;
- tvegani management – ugotavljanje, upravljanje in ublažitev nevarnosti;
- upravljanje virov;
- merjenje uspešnosti – opredelitev, poročanje in uporaba podatkov meritev upravljanja informacijske varnosti.

Upravljanje informacijske varnosti je v organizaciji prepleteno z upravljanjem informacijskih tehnologij. Oboje pa združujemo pod upravljanje celotne organizacije.
Bistvena sestavina - element upravljanja informacijske varnosti pa je tudi *informacijska varnostna politika*. Informacijska varnostna politika je združenje pravil in praks, ki določajo, kako naj organizacija upravlja, ščiti in prenaša informacije. Pomembno je predvsem to, da varnostna politika deluje v kombinaciji z veljavno zakonodajo, ki določa poslovanje na področju varovanja informacij. Z varnostno politiko so določena minimalna obvezujoča pravila in predpisi, ki se nanašajo na splošne principe ravnanja, dostopa, obdelave, shranjevanja, prenosa in uničenja informacijskih podatkov znotraj organizacije. Pravila in predpisi veljajo za vse zaposlene, zunanje sodelavce in druge, ki imajo stik z informacijskimi viri podjetja.

2.1 Razdelitev upravljanja informacijske varnosti

Upravljanje informacijske varnosti lahko razdelimo na dva dela.
Management odgovornosti vključuje sredstva, financiranje in strateško zastopanje, potrebno za sodelovanje v programu informacijske varnosti. Navezuje se predvsem na vodilne zaposlene v organizaciji. Podpora vodstva je eden najpomembnejših dejavnikov za uspeh programa varnosti.
Management izvajanja je temelj informacijske varnosti in zajema bistvene elemente: obvladovanje tveganj, informacijsko varnostno politiko, postopke, standarde, smernice, izhodišča, klasifikacije, izobraževanja in organizacijo. Varnostni ukrepi se izvajajo in vzdržujejo tako, da pokrivajo tri soodvisna načela prisotna v vseh programih: zaupnost celovitost in razpoložljivost.
Pojma management odgovornosti in management izvajanja že lahko podata osnovo za razdelitev upravljanja na dva nivoja ter podlago za določitev odgovornosti zaposlenih na področju informacijske varnosti. Lahko rečemo, da management odgovornosti pomeni nivo strateškega managementa. Iz tabele 1 je razvidno, da strateški management nadzira in daje navodila. Management izvajanja pa lahko pomeni nivo operativnega managementa, ki izvaja naloge po navodilih strateškega managementa. Ves čas pa se moramo zavedati, da je strateški management vedno "več" kot operativni management (Pironti 2007).

Tabela 1: Primerjava med strateškim in operativnim managementom (Bergsma, 2010).

Strateški management	**Operativni management**
Nadzor/pregled	Izvajanje
Izdaja dovoljenje za odločanje	Izvajanje odločanja
Uvedbena politika	Izvajalna politika
Odgovarjanje	Odgovornost
Strateško načrtovanje	Projektno načrtovanje
Dodelitev virov	Uporaba virov

Če razdelitev upravljanja informacijske varnosti opravimo še na organizacijskem nivoju, bi strateški management lahko uvrstili v vodstvo organizacije. Operativni management bi pa

organizacijsko sodil v sektor informacijskih tehnologij, saj je po opisanih lastnostih iz tabele 1 podrejen strateškemu managementu.

2.1.1 Upravljanje informacijske varnosti na strateškem nivoju

Strateški management se začne čisto na vrhu organizacijske strukture in vključuje vse zaposlene v organizaciji. Je sistem, s katerim organizacija upravlja in nadzira informacijsko varnost. Temelji na izvajanju pravih stvari. Poleg tega strateški management specificira odgovornost posameznikov in priskrbi nadzor za preprečitev tveganja. Strateški management skrbi za strategijo ter jo objektivno in dosledno, glede na cilje in potrebe organizacije, uvrsti v organizacijsko ureditev. Skrbi, da so politike in postopki v skladu z organizacijskimi cilji ter, da je operativno okolje ustrezno nadzorovano.

2.1.2 Upravljanje informacijske varnosti na operativnem nivoju

Operativni management je sistem, ki se ukvarja z izvajanjem odločitev za ublažitev oziroma preprečitev tveganja. Temelji na pravilnem izvajanju stvari. Poleg tega skrbi za izvrševanje potrebnih kontrol, na podlagi katerih strateškemu managementu lahko priporoči varnostno strategijo. Največji izziv operativnega managementa v vseh organizacijah je delati prave stvari na pravi način.

3 Organizacijska struktura pri upravljanju informacijske varnosti

Upravljanje informacijske varnosti je podmnožica upravljanja podjetja, ki:

- določa strateške usmeritve;
- določa uporabo organizacijskih virov;
- zagotavlja, da so cilji doseženi;
- primerno in odgovorno upravlja tveganja;
- spremlja uspeh ali neuspeh programa varnosti podjetja.

Nenačrtovana in neusklajena lokalizacija oblasti v organizacijah predstavlja velike izzive za celotno institucionalno skladnost z varnostjo, avtorskimi pravicami, zasebnostjo, identiteto in drugimi predpisi, ki urejajo področje informacijske varnosti. Glede na širino in globino celotne informacijske dejavnosti neusklajenost povzroča težavo za vodje informatike in je lahko tudi neučinkovita. S pristopom od zgoraj navzdol, najvišje vodstvo zagotavlja podporo in usmeritve navzdol, skozi ravni upravljanja na srednjem nivoju in nazadnje tudi na najnižji ravni, ki zajema vse zaposlene.
Z upravljanjem informacijske varnosti bi se v vsaki organizaciji, ne glede na njeno velikost, morali ukvarjati (po Malik, 2006; Brotby, 2009):

- CEO (ang. chief executive officer): vodstvo (generalni direktor), ki ima temeljno odgovornost za zaščito interesov organizacije;
- Vodstvo sektorja informacijskih tehnologij (direktor informacijskih tehnologij): razvija strategije, zagotavlja integracijo in prevzema odgovornost v zvezi z upravljanjem informacijske varnosti na strateškem nivoju;
- Operativni management: odgovoren je za obravnavanje vseh tveganj in izvajanje zahtev vodstva – upravljanje informacijske varnosti na operativnem nivoju;
- CISO (ang. chief information security officer)/ CSO (ang. chief security officer): znotraj organizacije je direktor za varnost odgovoren za vzpostavitev in vzdrževanje podjetniške vizije, strategije in programa, ki zagotavlja ustrezno zaščito informacij.

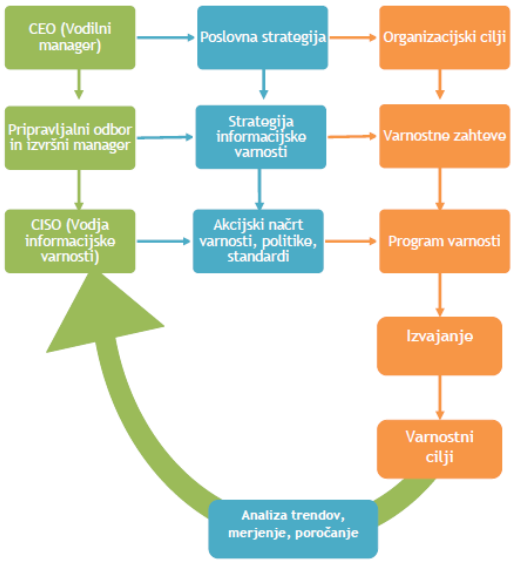
Poleg tega vzpostavi ovir in program upravljanja informacijske varnosti ter prevzame odgovornost za ustrezno izvajanje in skrb za posodobitev vseh dokumentov, ki se navezujejo na področje informacijske varnosti.

Poleg zaposlenih, ki so neposredno povezani z managementom informacijske varnosti ima svoje pristojnosti in odgovornosti najvišje vodstvo organizacije (direktor in njegovi najbližji sodelavci) ter drugi zaposleni, ki so samo uporabniki informacij in informacijske tehnologije (Parizo, 2010). Uporabniki so lahko zaposleni v organizaciji ali drugi uporabniki informacijski virov neke organizacije (npr. pogodbeni zunanji izvajalci, kupci, dobavitelji,…).

3.1 Človeški viri pri upravljanju informacijske varnosti

Vsaka organizacija mora zagotoviti, da se uslužbenci, pogodbeni zunanji izvajalci in tretje stranke (v to skupino uvrščamo npr. dobavitelje, kupce in podobno), ki imajo dostop do organizacijskih informacijskih virov, zavedajo svojih obveznosti in razumejo ter sprejemajo pristojnosti, odgovornosti in dolžnosti, ki so povezane z dostopom, obdelovanjem, sporočanjem in upravljanjem informacij in informacijskih virov organizacije. Vsem uslužbencem, pogodbenikom in tretjim strankam je potrebno zagotoviti ustrezno raven ozaveščenosti, izobraževanja in usposabljanja glede postopkov varovanja in pravilne uporabe informacij in informacijskih virov (Saksida, 2010). Uslužbenci, pogodbeniki in tretje osebe morajo biti s svojimi odgovornostmi in vlogami v zvezi z varovanjem informacij, ustrezno seznanjeni še preden se jim dovoli dostop do informacij ali informacijskih virov, ki jih organizacija hrani ali z njimi posluje.
Z ločevanjem nalog in odgovornosti na posameznike organizacija zmanjšuje možnost zlorab in drugih oblik ogrožanja informacijske varnosti (npr. nepooblaščeno spreminjanje podatkov). Tako, kot samo upravljanje informacijske varnosti, bi tudi zaposlene v organizaciji lahko razdelili na tri nivoje:

- strateški nivo – ugotavljajo kako pomembne so informacije in njihova zaščita;
- taktični nivo – opredelijo politike in postopke za zaščito informacij;
- operativni nivo – zagotovijo izvajanje določil.



Slika 1: Primer koncepta upravljanja informacijske varnosti (IT Governance Institute, 2007)

Skozi nivoje zaposleni uravnavajo (podajajo navodila), izvajajo in nadzirajo (kontrolirajo) informacijsko varnost. Njihove pristojnosti in odgovornosti opredeljujejo smernice, politike, organizacijski standardi in postopki. Ti dokumenti upravljajo in odrejajo izvedbo informacijske varnosti na vseh nivojih, vendar so po večini namenjeni nižjim nivojem organizacije.

3.2 Koncept upravljanja informacijske varnosti

Koncept upravljanja informacijske varnosti, prikazan na spodnji sliki prikazuje, kakšen je najboljši princip delovanja pri učinkovitem zagotavljanju informacijske varnosti (Von Roessing, 2010). Koncept zajema zaposlene (razdeli jih na tri nivoje), strategije (celotne organizacije in na področju informacijskih tehnologij), dokumente (potrebne za izvajanje). Pozornost daje tudi samemu izvajanju, varnostnim ciljem in nazadnje analiziranju procesa ter poročanju o tem odgovornim.

4 Zaključek

Da bi podjetja lahko vzpostavila in vzdrževala celosten sistem informacijske varnosti, s katerim bi imela pregled nad dogajanjem v samem podjetju, kakor tudi pregled nad vhodnimi iz izhodnimi parametri, ter sočasno bila v koraku s časom in trendi, morajo imeti močno podporo vodstva pri uresničevanju zadanega cilja. Sistem je potrebno prilagoditi glede na potrebe varovanja samih podatkov, ter glede na število zaposlenih in nenazadnje finančnimi zmožnostmi posameznega podjetja. Razpoložljivost s finančnimi in človeškimi viri ter izobraževanje zaposlenih sta, ne glede na velikost organizacije, dva izmed pomembnih dejavnikov zagotavljanja zaupnosti, celovitosti in razpoložljivosti organizacij, za katera mora poskrbeti in zanj odgovarjati glavni direktor.
Upoštevajoč te dejavnike, se organizacija spopade s sledečo nalogo: zaposlenim v podjetju je potrebno predstaviti nov sistem, ter ga prikazati na tak način, da ga bodo znali in uspeli uporabljati.
Sam proces, od načrtovanja novega sistema informacijske varnosti, pa vse tja do točke, ko je sistem v polnem delovanju, pa je dolgotrajen. Morebitne napake strateškega managementa, ki jih napravi pri načrtovanju sistema, najhitreje opazi operativni management, zatorej sta potrebna dobra komunikacija in sodelovanje, da se nepravilnosti in ovire odpravijo. Nekatere napake pa se pojavijo šele kasneje, ko sistem zaživi.

5 Literatura

Bergsma, K. (2010). *Information security governance*. Članek dobljen 30.3.2010 na: https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance.

Bernik, I. (2008). Organizacijski vidiki informacijske varnosti. V J. Šifrer (ur.), *Zbornik povzetkov: 9. slovenski dnevi varstvoslovja* (str. 66-67). Ljubljana: Fakulteta za varnostne vede.

Brotby, W. K. (2009). *Information security management metrics: a definitive guide to effective security monitoring and measurement*. Boca Raton: CRC.

IT Governance Institute (2006). *Information Security Governance: Guidance for Boards of Directors and Executice Management 2nd Edition.* Rolling Meadows, USA: IT Governance Institute.

Malik, W. J. (2006). Information Securtiy Governance. *Infromation Systems Control Journal*, *3*, 23.

Parizo, E. B. (2010). *Information security 2011: Next-gen threats demand layered defense*. Članek dobljen 12. 2. 2011 na http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1525229,00.html

Pironti, J. (2007). Developing Metrics for Effective Information Security Governance. *Infromation Systems Control Journal*, 2, 33-37.

Saksida, M. (2010). *Politika varovanja informacij s poudarkom na upravljanju s človeškimi viri*. (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede Univerza v Mariboru.

Von Roessing, R. M. (2010). *The Business Model for Information Security*. Rolling Meadows, USA: ISACA.

Von Solms, S. H. (2009). *Information security governance*. New York, London: Springer.