Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji

Alenka Brezavšček
Univerza v Mariboru, Fakulteta za organizacijske vede
alenka.brezavscek@fov.uni-mb.si

Stane Moškon
Vris, d. o. o.
stane.moskon@vris.si

Izvleček

Zaradi vse večje odvisnosti izvajanja poslovnih procesov od informacijske tehnologije in zaradi izpostavljenosti informacijskih sistemov različnim varnostnim tveganjem se v organizaciji pojavi potreba po vzpostavitvi ustreznega sistema za upravljanje informacijske varnosti – SUIV. V prispevku so opisane in analizirane štiri faze, ki so potrebne za vzpostavitev SUIV. Podane so smernice za uspešno implementacijo posamezne faze v organizaciji. Take smernice so lahko v veliko pomoč organizacijam, ki se zavedajo pomembnosti zagotavljanja informacijske varnosti in skušajo v svoje poslovanje vpeljati učinkovit SUIV.

Ključne besede: informacijska varnost, upravljanje, SUIV, vzpostavitev, smernice.

Abstract

INFORMATION SECURITY MANAGEMENT SYSTEM – IMPLEMENTATION IN AN ORGANIZATION

Nowadays, information systems in organizations are exposed to different security risks. To ensure business continuity, organizations are forced to implement an information security management system – ISMS. In the paper, the four phases of ISMS implementation are presented and described. Besides, some guidelines and best practices are given to make the implementation process easier. The guidelines would be useful for organizations trying to involve information security concepts in their business.

Keywords: information security, management, ISMS, implementation, guidelines.

1 UVOD

Danes je poslovanje v organizacijah v veliki meri podprto z informacijskim sistemom. Učinkovitost izvedbe poslovnih procesov je pogojena z zadovoljivim delovanjem informacijskega sistema, saj njegovo nedelovanje ali okrnjeno delovanje pogosto vodi v prekinitev izvajanja ključnih poslovnih procesov organizacije. Posledice takega dogodka so lahko za organizacijo kritične in povezane z visokimi stroški. Organizacija, ki želi zagotoviti kontinuirano in ekonomično izvajanje svojih poslovnih procesov, je prisiljena poskrbeti za ustrezno raven varnosti informacijskega sistema. Zagotavljanje varnosti informacijskega sistema v organizaciji je kompleksna aktivnost, ki zahteva sistematičen pristop. V prispevku bodo opisane različne faze, ki so potrebne za vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. Posamezne faze bodo podrobneje analizirane upoštevajoč priporočila iz strokovne literature. Poleg tega bodo na podlagi dolgoletnih izkušenj avtorjev za vsako fazo vzpostavitve SUIV podane smernice za uspešno implementacijo. Take smernice bodo v veliko pomoč organizacijam, ki se zavedajo pomembnosti zagotavljanja informacijske varnosti in skušajo v svoje poslovanje vpeljati učinkovit SUIV.

2 TEORETIČNI VIDIKI ZAGOTAVLJANJA INFORMACIJSKE VARNOSTI

Na podlagi izsledkov iz različne strokovne literature so v nadaljevanju podane podlage s področja zagotavljanja varnosti informacijskih sistemov, ki so nujno potrebne za razumevanje tega prispevka.

2.1 Informacijska varnost, grožnje varnosti, ranljivost informacijskega sistema

Varnost informacijskega sistema (angl. information security) bi lahko definirali kot sposobnost informacijskega sistema, da ob določenih pogojih zadovoljivo opravlja zahtevane funkcije kljub morebitnim negativnim vplivom, ki so posledica različnih neželenih dogodkov (glej npr. Brezavšček in Moškon, 2009).

Take dogodke imenujemo grožnje varnosti (angl. security threats).

V literaturi je mogoče zaslediti različne klasifikacije groženj varnosti. Cunningham et al. (2007) npr. razvrščajo grožnje varnosti v naslednje skupine: človekova dejavnost (npr. sabotaža, vlom, kraja ipd.), grožnje, ki pretijo infrastrukturi (npr. poškodbe poslovne stavbe, odpoved podporne tehnologije, izliv vode ipd.), in grožnje, specifične za informacijsko tehnologijo (programski vsiljivci, logični vdor, odpoved strojne opreme ipd.). Pogosto zasledimo tudi delitev groženj na naslednje tri skupine: izredni dogodki, naključni dogodki in človekova (zlo)namerna dejavnost.

Grožnje varnosti pretijo informacijskemu sistemu in njegovim delom (t. i. dobrinam, angl. assets). Če so v informacijskem sistemu navzoče določene ranljivosti (angl. vulnerabilities), lahko grožnja, ki se uresniči, prizadene informacijski sistem oz. njegovo dobrino. Ranljivost je torej vsaka pomanjkljivost informacijskega sistema in njegovih dobrin, ki jo lahko izrabi določena grožnja ali skupina groženj.

2.2 Cilji zagotavljanja informacijske varnosti

Glavni cilj informacijske varnosti je zagotavljanje razpoložljivosti, celovitosti in zaupnosti informacijskega sistema in njegovih dobrin.

Zagotavljanje razpoložljivosti (angl. availability) pomeni zagotavljanje dostopnosti do informacijskega sistema oz. njegovih dobrin v vsakem trenutku, ko ga/jih potrebujejo pooblaščeni uporabniki. Zagotavljanje razpoložljivosti se nanaša na vse glavne dele informacijskega sistema: sistemska oprema, programska oprema, podatki/informacije in človek.

Zagotavljanje celovitosti (angl. integrity) pomeni preprečevanje nepooblaščenih sprememb. Tako kot zagotavljanje razpoložljivosti se tudi zagotavljanje zaupnosti nanaša na vse dele informacijskega sistema.

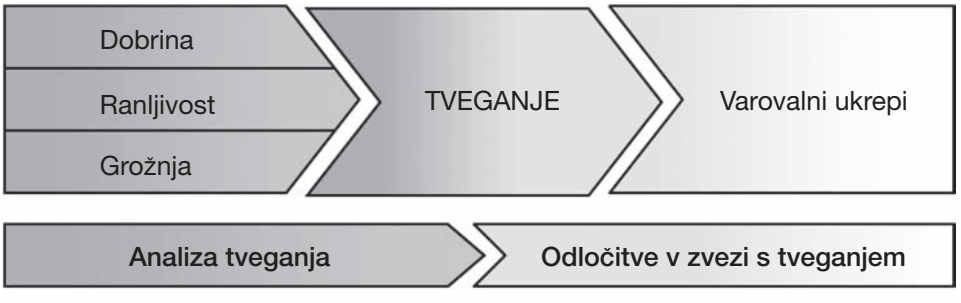
Zagotavljanje zaupnosti (angl. confidentiality) pomeni preprečevanje nepooblaščenega razkritja podatkov oz. informacij. Zagotoviti želimo, da so podatki in informacije dostopni izključno pooblaščenim osebam.

2.3 Upravljanje varnostnih tveganj

Proces upravljanja varnostnih tveganj (angl. information security risk management) je ciklični proces, ki sestoji iz tehle faz:

- sistematična izvedba analize, s katero prepoznamo vsa varnostna tveganja, katerim je izpostavljen informacijski sistem organizacije;
- sprejem ustreznih odločitev glede ugotovljenih varnostnih tveganj (definiranje stopnje tveganja, ki je še sprejemljivo za organizacijo, definiranje varovalnih ukrepov, s katerimi bomo tveganja, ki so nad mejo sprejemljivosti, znižali na sprejemljivo raven);
- realizacija sprejetih odločitev;
- spremljanje ustreznosti uvedenih varovalnih ukrepov in kontinuirano ugotavljanje novih varnostnih tveganj.

Prvi dve fazi procesa upravljanja varnostnih tveganj sta shematsko ponazorjeni na sliki 1.



Slika 1: **Prvi dve fazi procesa upravljanja varnostnih tveganj**

Posebno pomembna faza v procesu upravljanja varnostnih tveganj je prva, ki jo imenujemo analiza tveganja (na sliki 1 je ponazorjena s temnejšim senčenjem). V okviru take analize prepoznamo in ovrednotimo vsa tveganja, povezana z varnostjo informacijskega sistema. V kontekstu informacijske varnosti lahko tveganje definiramo kot kombinacijo verjetnosti, da se grožnja uresniči, in vseh negativnih posle-

dic, ki lahko nastanejo pri tem (BSI, 2006; ISO, 2008). Stopnjo tveganja lahko izračunamo po preprosti formuli

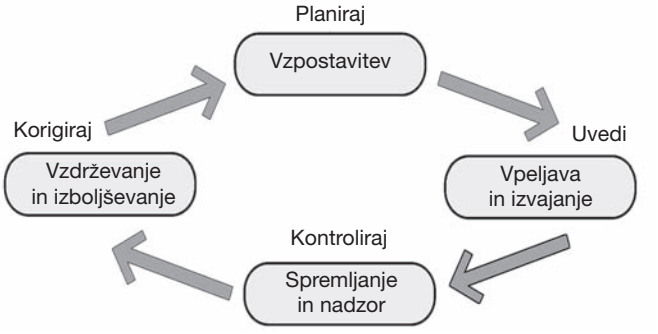
$$R = P \cdot C$$

pri čemer pomeni R stopnjo tveganja, P pogostost oz. verjetnost uresničitve grožnje na časovno enoto in C skupne stroške (neposredne in posredne), ki zaradi tega lahko nastanejo. Ker je vrednosti parametrov P in C v praksi pogosto težko natančno oceniti, se namesto kvantitativnega ocenjevanja navadno zadovoljimo s kvalitativno oceno varnostnega tveganja (npr. nizko, srednje, visoko tveganje). Tako oceno lahko določimo, če poznamo kvalitativne ocene za verjetnost uresničitve posamezne grožnje, stopnjo ranljivosti informacijskega sistema in vrednost dobrine, ki jo lahko prizadene grožnja. Metodologije, ki se v ta namen uporabljajo, so po navadi razmeroma preproste (glej npr. BSI, 2006; ISO, 2008; Jones in Ashenden, 2005; Peltier, 2005; Landoll, 2006).

Poznavanje varnostnih tveganj in njihovih ocen predstavlja podlago za planiranje ustreznih varovalnih ukrepov, s katerimi znižamo stopnjo tveganja in posledično dvignemo raven varnosti informacijskega sistema (glej desno stran slike 1).

2.4 Sistem za upravljanje informacijske varnosti

Organizacija, ki želi v svojem okolju vzpostaviti želeno raven informacijske varnosti, mora vzpostaviti ustrezen SUIV. SUIV v organizaciji mora temeljiti na procesnem pristopu »planiraj–uvedi–kontroliraj–korigiraj«, ki ga uvaja standard ISO/IEC 27001 (glej BSI, 2005). Procesni pristop »planiraj–uvedi–kontroliraj–korigiraj« je shematično prikazan na sliki 2.



Slika 2: **Procesni pristop vzpostavitve SUIV, ki ga vpeljuje standard ISO/IEC 27001**

Podlago SUIV v organizaciji predstavlja ustrezna dokumentacija. Dokumente, ki z različnih vidikov definirajo SUIV in jih je treba izdelati v organizaciji, bi lahko predstavili v obliki piramide, ki je ponazorjena na sliki 3.

Slika 3: **Piramida dokumentov, ki definirajo SUIV v organizaciji**
Vir: Avoine (2007)

Bistvenega pomena za uspešno vzpostavitev SUIV v organizaciji je tudi opredelitev odgovornosti za informacijsko varnost. Določiti je treba tim za informacijsko varnost, ki bo zagotovil, da se določila, navedena v dokumentih s slike 3, dejansko tudi izvajajo v praksi. Priporočljivo je, da so člani takega tima skrbniki oz. predstavniki glavnih poslovnih procesov organizacije. Vodja tima naj bo neposredno podrejen najvišjemu vodstvu organizacije, ki mora podpirati uvedbo SUIV ter v ta namen zagotoviti ustrezna sredstva.

Zavedati pa se moramo, da so ljudje ključni faktor za uspešnost uvedbe SUIV. Če želimo, da bo SUIV v organizaciji učinkovit in bodo doseženi zastavljeni cilji, je treba zavest zaposlenih dvigniti na tako raven, da se bo vsak zaposleni v organizaciji zavedal pomena zagotavljanja informacijske varnosti in svoje odgovornosti pri tem. Za doseganje tega cilja je treba v organizaciji vzpostaviti ustrezen sistem izobraževanja in ozaveščanja zaposlenih, ki ga je treba izvajati kontinuirano in dosledno.

2.5 Standardi, priporočila in dobre prakse

Pri zasnovi in vzpostavitvi SUIV si v organizaciji lahko pomagajo z različnimi standardi, priporočili in primeri dobrih praks, ki so se uveljavili v praksi. Poleg omenjenega ISO/IEC 27001 so na tem področju na voljo še številni dokumenti. Nekateri so bolj splošne narave in obravnavajo področje zagotavljanja informacijske varnosti v širšem smislu, drugi pa so bolj specializirani in se osredinjajo le na kak ožji segment zagotavljanja varnosti (npr. planiranje neprekinjenega poslovanja). Strnjen pregled tovrstnih dokumentov je podan v Brezavšček in Zupan (2006).

Omeniti velja predvsem tele dokumente, katerih uporaba se je v praksi najbolj uveljavila:

- COBIT – zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije (glej npr. ISACA, n. d.);
- ITIL – zbirka najboljše prakse za upravljanje informacijskih storitev (glej npr. ITIL, n. d.);
- serija standardov ISO/IEC 27000, med katerimi so že na voljo:
  - 27001 – specifikacije za sistem za upravljanje informacijske varnosti (ISO 27001 je leta 2005 nadomestil britanski standard BS7799-2),
  - 27002 – kodeks dobre prakse na področju varovanja informacij (nastal leta 2007, ko se je BS ISO/IEC 17799:2005 preimenoval v ISO 27002),
  - 27005 – pokriva področje upravljanja varnostnih tveganj (izšel leta 2008),
  - 27006 – smernice za institucije, ki so pooblaščene za izvajaje revizije in certificiranje sistemov za upravljanje informacijske varnosti (izšel leta 2007).

Kar nekaj standardov v tej zbirki pa je trenutno še v pripravi in jih lahko pričakujemo v bližnji prihodnosti (glej npr. ISO, n. d.).

3 VZPOSTAVITEV SISTEMA ZA UPRAVLJANJE INFORMACIJSKE VARNOSTI V PRAKSI

Iz navedb v razdelku 2 lahko sklepamo, da je vzpostavitev želene ravni informacijske varnosti v organizaciji kompleksen proces, ki zahteva sistematičen in dolgoročen pristop. Pomembno je, da so cilji jasno postavljeni in da so vse aktivnosti za doseganje ciljev in zahtevane ravni informacijske varnosti usmerjene in načrtovane. Kot smo že omenili, je treba definirati in vzpostaviti SUIV, ki mora temeljiti na procesnem pristopu »planiraj–uvedi–kontroliraj–korigiraj«, ki ga prikazuje slika 2. V skladu s tem procesnim pristopom sestoji vzpostavitev SUIV v organizaciji iz štirih faz:

- 1. faza: načrt vzpostavitve SUIV,
- 2. faza: uvedba SUIV,
- 3. faza: vzpostavitev sistema kontrol in nadzorstev nad delovanjem SUIV,
- 4. faza: analiza odstopanj SUIV in izvajanje korektivnih ukrepov.

V nadaljevanju so podrobneje opisane posamezne faze vzpostavitve SUIV v organizaciji. Pri tem so upoštevana različna priporočila iz strokovne literature (glej npr. Kumar Puthuseeri, 2006; Atsec, 2007; BSI, 2005). V okviru opisa posamezne faze so podane tudi nekatere smernice in priporočila, ki bodo organizacijam v pomoč za uspešnejšo izvedbo posamezne faze vzpostavitve SUIV. Navedene smernice so plod avtorjevih dolgoletnih izkušenj pri vzpostavljanju SUIV v konkretnih organizacijah. So rezultat dobre prakse in v ničemer ne odstopajo od priporočil v strokovni literaturi.

3.1 Načrt vzpostavitve SUIV

V tej fazi je treba zagotoviti jasno definiranje ciljev in zahtevane ravni informacijske varnosti. Izhajati je treba iz osnovne zahteve, da mora informacijski sistem zagotavljati in podpirati učinkovito izvajanje vseh in še posebno ključnih poslovnih procesov v organizaciji. Natančno in jasno je treba opredeliti varnostna tveganja z namenom preprečiti nedelovanje oz. okrnjeno delovanje informacijskega sistema. Izvedba analize in ocene tveganj je podlaga za določitev okvira SUIV. Le-ta je v vsaki organizaciji drugačen glede na njeno specifičnost, pomembnost in odvisnost informacijskega sistema za izvajanje poslovnih procesov. Ključni del prve faze vzpostavitve SUIV pa je izdelava načrta vzpostavitve in, kar je najpomembneje, sprejem in potrditev načrta s strani najvišjega vodstva organizacije.

Prva faza vzpostavitve SUIV vključuje tele aktivnosti:

- izvedba analize in ocene varnostnih tveganj za vse ključne poslovne procese v organizaciji,
- na podlagi ocene tveganj sledi določitev okvira SUIV,
- izdelava načrta vzpostavitve SUIV v organizaciji,
- sprejem odločitve vodstva organizacije za pristop k projektu SUIV.

Smernice in priporočila za izvedbo prve faze vzpostavitve SUIV v organizaciji so:

- Za vzpostavitev SUIV je pomemben procesni pristop. V organizaciji moramo najprej jasno ločevati vodstvene, glavne in podporne procese. Med glavnimi procesi pa je treba ugotoviti, kateri procesi ali podprocesi so še posebno odvisni od informacijske tehnologije. Te procese opredelimo kot ključne procese, saj bi daljše nedelovanje informacijske podpore lahko povzročilo zastoj teh procesov in s tem veliko poslovno škodo.
- Celoten proces vzpostavitve SUIV v organizaciji mora izhajati iz analize in ocene varnostnih tveganj. Po posameznih procesih, še posebno po glavnih in ključnih, moramo najprej ugotoviti stopnjo tveganja, ki je rezultat ocene verjetnosti, da se bo uresničila grožnja varnosti, in škode, ki bo nastala pri tem. Poleg tega nam ocena varnostnih tveganj podaja izhodišče, na kaj moramo biti še posebno pozorni pri vzpostavitvi SUIV.
- Poleg ocene tveganj je treba za ključne procese ugotoviti časovni okvir, v katerem mora biti po uresničitvi grožnje varnosti ponovno vzpostavljena informacijska podpora. Če se tega okvira ne uspemo držati, bo nastala poslovna škoda še večja.
- Vodstvo organizacije mora sprejeti načrt vzpostavitve SUIV v organizaciji in zagotoviti sredstva za njegovo uvedbo.

3.2 Uvedba SUIV

Na osnovi sprejetega načrta vzpostavitve SUIV sledi uvedba SUIV v organizacijo. Krovni dokument izvedbe celotnega projekta vzpostavitve SUIV in vodilo za njegovo uvedbo je politika varovanja podatkov in informacij, ki ga sprejema in potrjuje najvišje vodstvo organizacije. Ker je politika okvirni dokument, je treba izdelati in potrditi izvedbene dokumente na več ravneh, do najnižje ravni, ki zagotavlja operativno izvajanje vseh potrebnih aktivnosti za doseganje zahtevane ravni informacijske varnosti (glej sliko 3). Sprejeti izvedbeni dokumenti so podlaga za aktivnosti uvajanja SUIV, kar pomeni informiranje in izobraževanje vseh zaposlenih kot tudi zunanjih sodelavcev in pogodbenih partnerjev organizacije.

Uvedba SUIV vključuje tele aktivnosti:

- izdelava in sprejem politike varovanja podatkov in informacij s strani najvišjega vodstva organizacije,
- izdelava, potrditev in sprejem izvedbenih dokumentov SUIV,
- uvedba SUIV (politike in izvedbenih dokumentov),
- seznanjanje in izobraževanje vseh zaposlenih, zunanjih sodelavcev in pogodbenih partnerjev organizacije, ki pri svojem delu uporabljajo informacijsko podporo.

Smernice in priporočila za izvedbo druge faze vzpostavitve SUIV v organizaciji so:

- Krovni dokument SUIV je politika varovanja podatkov in informacij.
- Politiko varovanja podatkov in informacij sprejema najvišje vodstvo organizacije, ki mora podporo celotnemu projektu vzpostavitve SUIV zagotavljati tudi dejansko (ne samo načelno).
- Politika varovanja podatkov in informacij mora vključevati izsledke analize in ocene varnostnih tveganj.
- Na podlagi politike varovanja podatkov in informacij je treba izdelati načrt izvedbenih dokumentov.
- Izvedbeni dokumenti naj bodo v več ravneh. Priporočamo štiri: poleg ustanovne listine je treba izdelati in sprejeti varnostne politike, organizacijska navodila in zapise oz. izvedbena navodila.
- Sprejemanje novih izvedbenih dokumentov oz. sprememb obstoječih mora biti natančno določeno s posebnim organizacijskim predpisom. Natančno morajo biti opredeljene tudi odgovorne osebe za posamezna področja.
- Vsi na novo sprejeti izvedbeni dokumenti kot tudi spremembe obstoječih morajo biti objavljeni in dostopni po ustreznih strukturah v organizaciji.
- Informiranje in izobraževanje mora biti izvedeno na več ravneh v organizaciji in mora vključevati vse zaposlene skladno z načrtom izobraževanja.
- Informiranje mora biti izvedeno tudi za zunanje sodelavce in pogodbene izvajalce, ki so kakor koli povezani z informacijskim sistemom organizacije.

3.3 Vzpostavitve sistema kontrol in nadzorstev nad delovanjem SUIV

Z načrtovanjem kontrol in kontrolnega okolja SUIV je treba začeti že v prvi fazi vzpostavitve SUIV. Poleg tega je treba v vsej strukturi dokumentov, ki obravnavajo zagotavljanje informacijske varnosti, definirati kontrole in kontrolno okolje za nadzor nad delovanjem SUIV. V procesu informiranja in usposabljanja je treba s temi kontrolami seznanjati vse zaposlene. Poleg tega je treba določiti postopke in odgovorne osebe za izvajanje teh kontrol, kakor tudi nadzor nad delovanjem teh oseb.

Vzpostavitev sistema kontrol in nadzorstev nad delovanjem SUIV v organizaciji vključuje te aktivnosti:

- vzpostavitev kontrol in kontrolnega okolja,
- izvajanje kontrol in nadzorstev,
- nadzor nad delovanjem kontrol.

Smernice in priporočila za izvedbo tretje faze vzpostavitve SUIV v organizaciji so:

- Kontrole in kontrolno okolje mora biti določeno na vseh ravneh vzpostavitve SUIV.
- Kontrole morajo biti določene tako, da zagotavljajo učinkovit nadzor nad delovanjem SUIV.
- Določeni morajo biti postopki in odgovorne osebe za izvajanje kontrol in nadzorstev.
- Določene morajo biti sankcije v primeru ugotovitve neskladnosti ali nespoštovanja SUIV. Zaposleni naj bodo seznanjeni z njimi.
- Sankcije naj bodo večstopenjske (od opozoril do prekinitve delovnega razmerja).
- Postopki za izvedbo sankcij naj bodo jasni in dogovorjeni vnaprej.

3.4 Analiza odstopanj SUIV in izvajanje korektivnih ukrepov

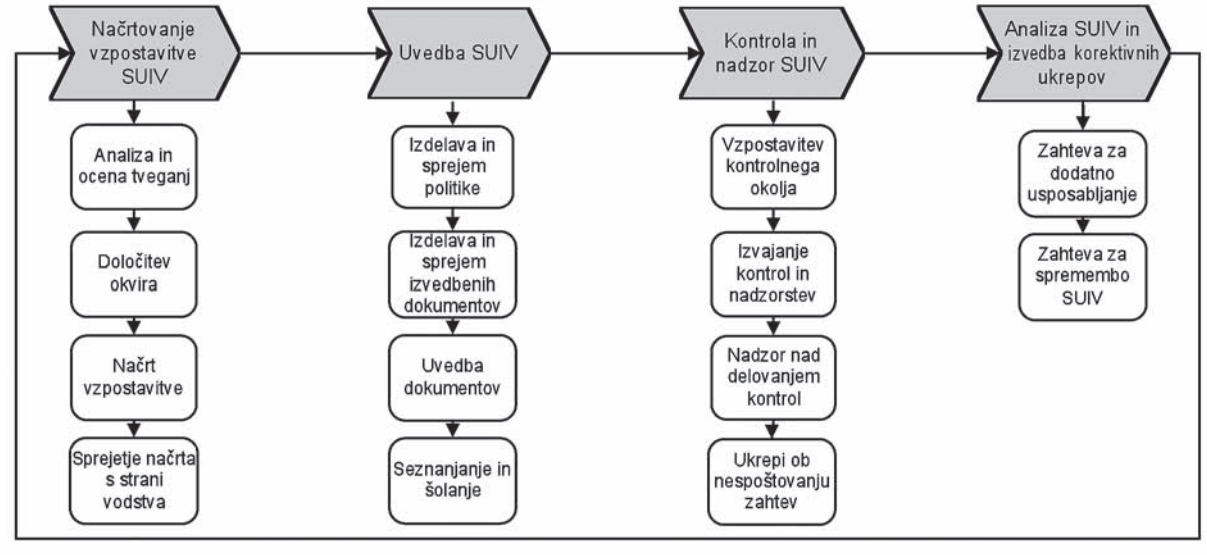
Zadnja faza vzpostavitve SUIV v organizaciji je analiza odstopanj in izvajanje korektivnih ukrepov. Analiza odstopanj lahko pokaže, ali udeleženci v poslovnih procesih organizacije niso ustrezno seznanjeni z zahtevami SUIV oz. jih ne razumejo ali se ne zavedajo resnosti posledic njihovega nespoštovanja. V tem primeru je treba zagotoviti dodatno usposabljanje ali ustreznejši način informiranja. Če analize pokažejo, da je treba spremeniti določila v posameznih dokumentih SUIV, mora biti določen postopek izvedbo teh sprememb.

Aktivnosti zadnje faze vzpostavitve SUIV so:

- ugotavljanje učinkovitosti SUIV,
- organiziranje dodatnega usposabljanja in izobraževanja, če je potrebno,
- uvajanje sprememb SUIV, če je potrebno.

Smernice in priporočila za izvedbo te faze vzpostavitve SUIV v organizaciji so:

- V primeru ugotovitve neskladnosti morajo biti jasno določeni postopki za spremembo ali dopolnitev SUIV.
- V primeru ugotovitve nepoznavanja določil SUIV med zaposlenimi naj se izvede dodatno usposabljanje in izobraževanje.



Slika 4: **Model vzpostavitve SUIV v organizaciji**

Celotni model vzpostavitve SUIV v organizaciji je prikazan na sliki 4. Prikazane so vse štiri faze vzpostavitve in navedene glavne aktivnosti znotraj posamezne faze.

Iz slike 4 je razvidno, da je vzpostavitev SUIV v organizaciji proces, ki se pravzaprav nikoli ne konča. Tega se je treba zavedati. Po naših izkušnjah organizacije vse prevečkrat pristopajo k vzpostavitvi SUIV kot k enkratni projektni nalogi, kar zagotovo ne more prinesti želenih rezultatov.

4 SKLEP

Skrb za zagotovitev ustrezne ravni informacijske varnosti bi morala biti eden izmed primarnih ciljev vsake organizacije, ki želi zagotoviti učinkovitost izvajanja svojih poslovnih procesov. Za dosego tega cilja je treba v organizaciji vzpostaviti ustrezen sistem za upravljanje informacijske varnosti – SUIV. V prispevku so predstavljene štiri faze vzpostavitve takega sistema. Podane so tudi smernice za uspešno izvedbo posamezne faze, ki temeljijo na izsledkih strokovne literature, predvsem pa na izkušnjah iz prakse. Smernice bodo dobrodošla usmeritev tako za organizacije, ki šele razmišljajo o uvedbi SUIV, kakor tudi za tiste, ki že uvajajo SUIV v svoje poslovanje.

Učinkovitost uvedbe SUIV v organizacijo je odvisna od številnih dejavnikov. Naj za konec strnemo le nekaj glavnih ugotovitev:

- Odločitev za vzpostavitev SUIV v organizaciji mora sprejeti najvišje vodstvo organizacije, ki mora v ta namen zagotoviti tudi potrebna finančna sredstva.
- Vodstvo organizacije mora jasno razumeti kontekst varnostnih tveganj in sprejeti odločitev, katera tveganja je treba zniževati in katera tveganja se lahko sprejmejo.
- Zagotoviti je treba zadovoljivo informiranost vseh zaposlenih. V ta namen je učinkovita uporaba intraneta, prek katerega lahko objavljamo vse sprejete dokumente in sprejete spremembe na področju zagotavljanja varnosti informacijskega sistema.
- Določiti je treba lastništvo nad krovno varnostno politiko in tudi nad izvedbenimi dokumenti. Lastniki dokumentov so odgovorni za zagotavljanje skladnosti dokumentov s spremembami v organizaciji ali zunaj nje.
- Uvesti je treba stalne oblike izobraževanja in ozaveščanja na področju informacijske varnosti za vse zaposlene v organizaciji in tudi za zunanje sodelavce. Posebno pozornost velja posvetiti zunanjim sodelavcem, dijakom in študentom. Le-ti imajo lahko visoko raven informacijskega znanja, zato lahko organizaciji povzročijo veliko škodo, če ne poznajo in ne spoštujejo določil za zagotavljanje informacijske varnosti.
- Nujno je treba vzpostaviti ustrezne kontrole in nadzorstva ter izvajati sankcije za nespoštovanje sprejetih določil, saj v nasprotnem primeru ne bo doseženo dosledno izvajanje SUIV.

Skrb za informacijsko varnost mora biti motiv vsakega zaposlenega v organizaciji. Le v takem okolju bo mogoča uspešna uvedba SUIV. Vsekakor pa se mora vodstvo organizacije zavedati, da je vzpostavitev SUIV kontinuiran proces, ki ni nikoli končan. Ob takem zavedanju bo vzpostavitev SUIV zagotovo prinesla želene rezultate.

5 LITERATURA

[1] Atsec (2007). *ISMS Implementation Guide*. Atsec information security corporation. Pridobljeno 20. 12. 2009 s svetovnega spleta: http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf.

[2] Avoine G. idr. (2007). *Computer system security: basic concepts and solved exercises*, EPFL, Lausanne.

[3] Brezavšček, A. & Zupan, L.(2006). Standardi in priporočila na področju informacijske varnosti, *Uporabna informatika*, Vol. 14, No. 2, str. 91–97.

[4] Brezavšček, A. & Moškon, S. (2009). Smernice za vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. *Nove tehnologije, novi izzivi, 28. mednarodna konferenca o razvoju organizacijskih znanosti*, *28th International Conference on Organizational Science Development*, 25.–27. marec 2009, Portorož, Slovenija, Moderna organizacija, Kranj, str. 202–209.

[5] BSI. (2005). British standard. BS ISO/IEC 27001:2005, *Information technology, security techniques, information security, management systems*, British Standards Institution, cop., London, 2005.

[6] BSI. (2006). British standard. BS 7799-3:2006, *Information security management systems. Part 3, Guidelines for information security risk management*, British Standards Institution, cop., London.

[7] Cunningham, B. et al. (2007). *The best damn IT security management book period*, Syngress Publishing, Inc., Burlington, ZDA.

[8] ISACA. (n. d.). *Spletna stran organizacije ISACA*. Pridobljeno 20. 12. 2009 s svetovnega spleta: www.isaca.org/cobit.

[9] ISO. (2008). International standard ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management; Technologies de l'information – Techniques de sécurité – Gestion du risue en sécurité de l'information*, International Organization for Standardization, cop., Geneva.

[10] ISO. (n.d.). *Spletna stran ISO 27000*. Pridobljeno 20. 12. 2009 s svetovnega spleta: http://www.27000.org.
[11] ITIL. (n.d.). *Spletna stran ITIL*. Pridobljeno 20. 12. 2009 s svetovnega spleta: http://www.itil-officialsite.com.
[12] Jones, A. & Ashenden, D.(2005). *Risk management for computer security: protecting your network and information assets*, Elsevier, Amsterdam.
[13] Kumar Puthuseeri, V. (2006). *ISMS Implementation Guide*. Pridobljeno 20. 12. 2009 s svetovnega spleta: http://www.infosecwriters.com/text_resources/pdf/ISMS_VKumar.pdf.
[14] Landoll, D. J. (2006). *The security risk assessment handbook: a complete guide for performing security risk assessments*, Auerbach Publications, Boca Raton.
[15] Peltier, T. R. (2005). *Information security risk analysis*, Auerbach Publications, Boca Raton.

▪

Alenka Brezavšček je leta 2000 doktorirala na Fakulteti za organizacijske vede Univerze v Mariboru, kjer je od leta 1994 tudi redno zaposlena. Habilitirana je v naziv docentka in je nosilka več različnih predmetov na vseh treh stopnjah bolonjskega študija. Njeno raziskovalno delo obsega predvsem študij stohastičnih modelov zanesljivosti in razpoložljivosti kompleksnih sistemov ter zagotavljanja varnosti informacijskih sistemov. Je avtorica oz. soavtorica več izvirnih znanstvenih člankov in referatov, objavljenih v domači in tuji strokovni literaturi. Poleg tega je članica tima urednikov spletnega slovarja Islovar, pri katerem deluje na področju informacijske varnosti.

▪

Stane Moškon je leta 1997 magistriral na Fakulteti za organizacijske vede Univerze v Mariboru. Je nosilec mednarodne licence CISA (Certified Information System Auditor), CISM (Certified Information Security Manager) in slovenske licence preizkušeni revizor informacijskih sistemov. Zaposlen je v podjetju Vris, d. o. o., kjer se že več let ukvarja z varnostjo in revizijo informacijskih sistemov. Na Fakulteti za organizacijske vede Univerze v Mariboru ima naziv gostujočega strokovnjaka.