Zahteve za uspešno vpeljavo standarda BS7799-2 za področje informacijske varnosti

Lucija Zupan,
Hermes SoftLab, d. d., Litijska 51, Ljubljana
lucija.zupan@hermes.si

Povzetek

Večina podjetij je danes stoodstotno odvisnih od informacijske tehnologije. Tesna povezanost informacijske tehnologije in poslovnih procesov prinaša tudi nekatere nove zahteve za varno, zanesljivo in dolgoročno uspešno poslovanje. Podjetja so vse bolj izpostavljena varnostnim tveganjem, iz česar izhaja neobhodna potreba po vzpostavitvi sistema upravljanja informacijske varnosti (v nadaljevanju SUIV). Iniciative uvajanja SUIV v podjetjih se pogosto končajo neuspešno, saj so zanemarjeni ključni vidiki uspešne vpeljave sistema. Pri vpeljavi SUIV se je zato priporočljivo opreti na dobre prakse in standarde, kot je standard BS 7799-2:2002, ki določa vse potrebne korake in postopke za vzpostavitev, implementacijo, nadzor ter stalno izboljševanje sistema. Ker pri implementaciji SUIV upravljamo z obsežno dokumentacijo, se izkaže uporaba orodij za upravljanje dokumentacije SUIV zelo koristna. Na trgu je na voljo več orodij, vendar so namenjeni različnim stvarem. Praktiki ugotavljamo, da je razumevanje namena in obsega varnostne politike zelo različno razumljena. Njen izgled, vsebina in struktura jo prepuščena posameznikom. Pomembno je, da je zastavljena praktično in da je zagotovljena njena razumljivost. Pri vpeljavi SUIV se pogostokrat srečamo tudi z visokimi stroški, kar pri vodstvu povzroči odpor. V takem primeru se mora upravljavec informacijske varnosti posluževati dobrih metrik, da lahko prikaže pozitivne učinke naložbe. V praksi pa se izbira dobrih metrik in zagotavljanje ustreznih vhodnih podatkov pogosto lahko izkaže kot problem.

Ključne besede: informacijska varnost, sistem za upravljanje varnosti informacij, BS7799, certificiranje, orodja za podporo upravljanja SUIV, informacijska varnostna politika, praksa

Abstract

How and why implementing the most integritive Information Security standard BS7799-2 in all sort of organizations

Nowadays, a majority of organizations are onehundred percent dependant on technology. The tight connection between information technology and business procesess also brings new demands for doing (being a) secure, reliable, and long-term sucessful business. Exposure to security threats is becoming an increasingly important issue for businesses. To answer the threats, businesses must implement an information security management system (ISMS). The first attempt at introducing ISMS in a business often results in failure, as they neglect key aspects of a sucessful implementation of ISMS. It is highly recommended to base ISMS implementation on the BS 7799-2:2002 standard, which specifies all the required steps and procedures for specifying, implementing, controlling and continuously improving the system. Because of the extensive documentation, that we must manage during a ISMS implementation, ISMS documentation tools often prove to be very useful. Several such tools exist on the market, with specific purposes. Practitioners are coming to the conclusion, that understanding the purpose and scope of a security policy can be interpreted in different ways. Its outlook, content and structure is up to the individual. It's important however, that it is designed and formulated in a practical and easy to understand way. ISMS implementation is often associated with high costs, which may cause resistance within the businesses' leadership. The information security manager must use quality metricts to convince the leadership, which often proves difficult in practice.

Key words: information secuity, Information Security Management System (ISMS), BS7799, certification, ISMS management tools, information security policy, practice

1 UVOD

Varnost informacijskih sistemov je danes za mnoge organizacije prioriteta številka ena. Do leta 2010 se pričakuje porast računalniških naprav na 14 milijard, kar bo predstavljalo dvakrat več naprav kot prebivalcev (leta 2010 bo po ocenah 7 milijard prebivalcev). Do l. 2005 bo v svetu obstajalo že 35 milijonov oddaljenih uporabnikov (neuslužbenci, ki dostopijo do omrežij; pogodbeniki, prodajalci). V zadnjem času je vse bolj prisoten porast spletnih storitev, t. i. storitev, ki se medsebojno pogovarjajo neodvisno od uporabnikov. Z nenehno rastjo števila računalniških naprav se eksponencialno povečuje tudi

število groženj, s tem pa raste tudi potreba po boljši informacijski varnosti. Pojav elektronskega poslovanja nujno zahteva ne samo vpeljavo varnih elektronskih povezav, temveč tudi številnih organizacijskih pravil ter nenehno usposabljanje zaposlenih, ki so ključni člen pri zagotavljanju varnega elektronskega poslovanja. Varnost informacijskih sistemov bo kmalu na prvem mestu pri izvajanju vseh dejavnosti podjetja. Tega poslanstva pa ne moremo izpolnjevati mimo izpolnitve nekaterih osnovnih pogojev. Z varnostjo informacij se je treba spoprijeti na vseh ravneh poslovanja in se ji posvetiti na dnevni ravni. Ključnega pomena so stalni pregledi sistema in njegovo izboljševanje.

Zagotavljanje informacijske varnosti je odgovorna naloga. Zahteva dobro poznavanje poslovnega okolja, poslovnih zahtev, informacijskega sistema ter varnostnih standardov. Pri zagotavljanju informacijske varnosti je treba vzpostaviti delujoč, živ sistem, ki bo omogočal zagotavljanje ustreznega nivoja varnosti in se ustrezno odzival na spremembe. Standard BS7799 nam omogoča postavitev ogrodja takega sistema in upoštevanje le-tega nam zagotavlja, da smo vključili vse elementarne sestavine, ki se zahtevajo pri zagotavljanju informacijske varnosti. Standard je zelo ohlapen in pušča implementacijsko plat popolnoma odprto. To je tudi eden glavnih razlogov za zmedo, ki nastaja pri definicijah področja, kot tudi pri vzpostavitvi sistemov, ki se medsebojno razlikujejo po obsegu, vsebini, strukturi itn.

Zaradi hitrih tehnoloških, gospodarskih in političnih sprememb je standard v nekaterih svojih delih zastarel. Obetajo se spremembe standarda, vendar strokovna javnost zaenkrat večinoma molči, premiki se dogajajo počasi. V vsakem primeru je potrebno zasnovati SUIV na ta način, da bo preživel mnoge spremembe skozi čas. Zato je še posebej pomembno, da pri tem upoštevamo napotila in najboljšo prakso.

Vsak sistem je unikat, ki mu je treba prilagoditi stopnjo varovanja. Vsak novo izgrajeni sistem zahteva tudi, da ga sprejmejo njihovi zaposleni in se s tem čimbolj vključi v poslovno okolje.

2 ZAHTEVE ZA VARNOST IN ZAŠČITO INFORMACIJ BODO V PRIHODNOSTI VSE VEČJE

Živimo v svetu nenehnega prilagajanja, kjer morajo organizacije dnevno spreminjati svoje poslovanje v skladu z zahtevami poslovnih partnerjev. Zahteve se vse bolj pogosto nanašajo tudi na urejenost področja varnosti in zaščite informacij, saj ni več dovolj, da podjetja ustrezno varujejo samo svoj informacijski sistem, temveč potrebujemo zagotovilo, da ga ustrezno varuje tudi njihov poslovni partner. V tem primeru se podjetja znajdejo pred odločitvijo glede vpeljave ustreznega sistema varovanja, ki lahko vpliva na pridobitev potencialnega posla. Znajdejo se tudi pred mnogimi drugimi izzivi, ki jih predstavlja vpeljava učinkovitega sistema varovanja in zaščite podatkov.

Pri vzpostavitvi sistema za upravljanje informacijske varnosti se je smotrno opreti na standarde. Trenutno so na voljo številni standardi, samo za informacijsko varnost bi jih lahko našteli več kot petdeset. Strokovnjaki so si enotni, da je najbolj celovit standard na področju informacijske varnosti še vedno ISO17799/BS 7799, ki določa upravljavski sistem za področje informacijske varnosti. Drugi del standarda, BS 7799-2:2002 predstavlja specifikacijo oziroma zbirko lastnosti, katerim mora sistem upravljanja ustrezati, če želimo, da je skladen s standardom in da sistem lahko certificiramo.

Poleg tega obstaja več različnih standardov za sisteme vodenja: družina ISO 9000 (sistem kakovosti), družina ISO 14000 (sistem ravnanja z okoljem), družina OHSAS 18000 (sistem varnosti in zdravja pri delu), družina BS 7799 (sistem informacijske varnosti).

Ti sistemi imajo veliko skupnih lastnosti, med katere sodijo:

- temeljijo na načelu neprestanega izboljševanja kakovosti in izboljševanja na področjih, kjer ni mogoče doseči absolutno najvišje vrednosti (oziroma 100 % varnosti),
- pokrivajo področja, kjer so potrebni stalni odzivi na spremenjene zahteve okolja,
- procesi, postopki in nadzorstva upravljavskih sistemov morajo biti dokumentirani, saj nam to zagotavlja, da se res izvajajo in da jih je mogoče nadzirati,
- upravljavski sistemi oziroma sistemi vodenja predstavljajo model organiziranosti, ki teži k zmanjševanju in preprečevanju pomanjkljivosti v poslovanju.

Zakonske zahteve za skladnost z BS7799-2 v Sloveniji so trenutno najbolj zavezujoče za banke. Julija 2004 je Banka Slovenije objavila, da mora banka pri svojem poslovanju upoštevati slovenska standarda SIST BS7799-2:2003 in SIST ISO/IEC 17799:2003 (Ur. L. RS št. 83/04 z dne 29. 07. 2004). Poleg tega za banke velja tudi mednarodni standard Basel II, ki banke tesneje kot standard BS 7799-2:2002 zavezuje k ureditvi področja informacijske varnosti prek zagotavljanja ustreznega nivoja tveganj in zmanjšanja operativnih tveganj [18]. Za ostale panoge posebna zakonska določila

glede skladnosti s standardom ne obstajajo, vendar pa podjetja sama opažajo veliko potrebo po varnem in zaupanja vrednem poslovanju. Na področju zakonske ureditve se pričakujejo ostrejše zahteve ter bolj celovito pokritje področja predvsem za banke in zdravstvene institucije. Zdravstvene institucije uvajajo elektronski zdravstveni zapis, ki bo vseboval kritične podatke o pacientih, v naslednjem koraku pa se bodo ti podatki pretakali med zdravstvenimi organizacijami. Neizogibno bo treba temu področju posvetiti večjo skrb in prilagoditi tudi regulativo [15].

Pomemben vidik pri varovanju informacij predstavlja veljavna zakonodaja, vendar je upoštevanje samo zakonskih določil premalo za doseganje ustreznega nivoja varnosti [19]. Upoštevati je treba tudi zahteve poslovnih partnerjev, odjemalcev in zaposlenih. Ob vstopu Slovenije v Evropsko unijo se bo brez dvoma tudi na področju informacijske varnosti in poslovanja med organizacijami začelo obdobje prilagajanja in sprememb. Pri sklepanju partnerstev v tujini bo treba upoštevati tudi poslovne zahteve in zakonodajo v državi, iz katere partner izhaja. Pri tem bo treba upoštevati predvsem sledeča zakonska področja: zakonodaja v zvezi z šifriranjem podatkov, zakonodaja v zvezi z varovanjem kritične (informacijske) infrastrukture, politika digitalnega podpisovanja in mednarodni sodni postopki za kriminaliteto na spletu. Organizacije morajo v skladu s tem razširiti obseg pri načrtovanju svoje strategije, kar pomeni, da morajo upoštevati številne mednarodne in državne zakone in pravila. Tako bodo lahko zagotovile usklajenost s pravno-zakonodajnimi načeli, pravili in smernicami v tujih državah.

3 KORISTI UVEDBE STANDARDA BS7799-2 V ORGANIZACIJO

Danes je podjetjem več ali manj že jasno, da se je pri vpeljavi sistema informacijske varnosti smiselno opreti na standard BS 7799-2:2002. Bistvene prednosti opiranja na standard, pred uporabo neformalnih pristopov k zagotavljanju informacijske varnosti so predvsem:

- Standard omogoča osnovo za vpeljavo najboljših praks.
- Je upravljalsko, tehnološko in organizacijsko neodvisno orodje ter dovolj splošen, da je primeren za vse vrste organizacij.
- S standardom zagotovimo celovito pokrivanje področja informacijske varnosti (zmanjšamo možnost, da bi spregledali pomembna področja).
- Standard BS7799 omogoča sistematičen in konsistenten pristop ne samo pri vpeljavi, temveč tudi pri vzdrževanju SUIV.
- Uporaba standarda za varovanje informacij omogoča osnovo za ugotavljanje odstopanj in predvideva tudi vire za varovanje.
- Opiranje zgolj na izkušnje posameznikov ni več potrebno, saj se pri zapisovanju politike in nadzorstev, ki zagotavljajo ustrezen nivo varnosti, lahko naslonimo na standard.

Še dva praktična nasveta, kako pridobiti čimveč koristi od standarda [17]:

- Priporočljivo je graditi na tem, kar imamo v podjetju že vzpostavljeno. Če imamo vzpostavljen npr. sistem za vodenje kakovosti ISO9000, ga lahko uporabimo kot ogrodje. Najmanj kar bo pomagal odkriti, je, ali nadzor dokumentov obstoječega standarda zadostuje za certificiranje.
- Certificirajte se. Mnogo organizacij se odloči samo za skladnost s standardom. Ampak to je sivo, nejasno področje. Zakaj bi šli čez vse težave, ki jih prinaša vzpostavitev SUIV, ne da bi svoj uspeh ovekovečili pred zunanjim svetom (našim strankam, poslovnim partnerjem)? Certificiranje pomeni boljši fokus, večjo osredotočenost na cilje in zato tudi večjo možnost uspeha. Čeprav lastni stroški certificiranja za dobo treh let znašajo okrog 3000 EUR (BSQVI poročilo), se certificiranje lahko obrestuje.

Opisali smo koristi opiranja na standard. V nadaljevanju navajamo tudi koristi uvedbe standarda BS7799-2 za varovanje in zaščito informacij. Notranje koristi so predvsem:

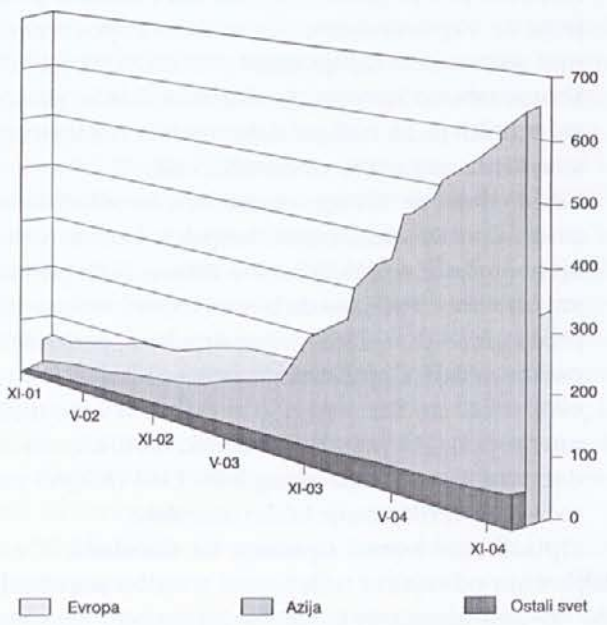
- povečanje produktivnosti (ljudje delajo bolj učinkovito, v bolj urejenih in strukturiranih okvirih, kar tudi zmanjšuje možnost za odkrivanje »na novo« in podvajanje dela ter olajšuje izmenjavanje informacij);
- revizije omogočajo nepristranski zunanji pogled na poslovanje, odkrivanje priložnosti za izboljšanje;
- standard vpeljuje discipline, kot so ocenjevanje tveganja in hranjenje zapisov, ki jih lahko izkoristimo za povečanje urejenosti poslovanja nasploh;
- povečanje zanesljivosti delovanja celotnega informacijskega sistema;
- omogoča hitro in učinkovito uvajanje novih sodelavcev.

Med zunanje koristi štejemo:

- povečanje zaupanja poslovnih partnerjev in drugih interesnih skupin,

- povečanje ugleda,
- povečanje prednosti pred tekmeci,
- izboljšanje osnov za marketing in trženje storitev,
- izpolnjevanje zakonskih zahtev,
- izpolnjevanje zahtev poslovnih partnerjev in odjemalcev.

Vse več podjetij v svetu se odloča za certificiranje. V zadnjih 12 mesecih je število držav z certificiranimi podjetji po BS7799-2 naraslo na 37 (med njimi tudi Slovenija). Rast števila certificiranih podjetij v svetu ponazarja slika 1 [13].



Slika 1: **Rast števila certificiranih po BS7799-2 v svetu**
(Vir: Gammassi, 2005)

4 PRIHODNOST STANDARDA

Standard mora biti, če hoče biti uporaben, pragmatičen in koristen, prilagodljiv ter mora upoštevati spremembe, ki jih prinašajo tehnološki napredek in drugi trendi v poslovnem svetu. Obetajo se spremembe standarda, s tem pa tudi potrebe po spremembi in dopolnjevanju že vzpostavljenih sistemov varovanja. Kaj pravijo strokovnjaki, ki zasledujejo spreminjanje standarda o njegovi prihodnosti, si lahko preberete v nadaljevanju [13].

Revizija standarda ISO/IEC 17799

ISO/IEC 17799:2000 je trenutno v postopku pregledovanja, ki bo predvidoma sredi leta 2005. Največja sprememba, ki se pričakuje, je v ureditvi, načrtovanju nadzorstev za jasnejšo razlikovanje med zahtevami, smernicami za vzpostavitev in nadaljnje informacije. Pričakuje se tudi racionalizacija standarda z dodajanjem nekaj novih nadzorstev in boljšo obrazložitvijo obstoječih.

Razvoj tretjega dela standarda

Mnogi se sprašujejo, če bo obstajal tudi tretji del standarda. Junija/julija 2002 se je začelo razmišljati o razvoju tretjega dela standarda. Iniciativa je bila osnovana na dejstvu, da je ISO 9001 sestavljen iz štirih delov, standard BS7799-2:2002 pa je zelo soroden ISO 9001:2000. Novi tretj del standarda bi potemtakem skrbel za proces neprestanega izboljševanja SUIV (podoben namen je imel ISO 9004). Drugi razlog za smiselnost vpeljave tretjega dela standarda so strokovnjaki videli v potrebi po integraciji SUIV z ostalimi sistemi vodenja.

Nadgradnja BS7799-2:2002

Tehnologija nezadržno napreduje in se spreminja, zaradi tega je pričakovati, da obstoječi standard v prihodnosti ne bo pokrival vseh potreb in zahtev v praksi. Praktiki že ugotavljajo določene pomanjkljivosti standarda ter tudi nekoherentnosti med posameznimi nadzorstvi znotraj njega. Iz tega razloga lahko pričakujemo, da se bo tudi standard BS7799-2 v prihodnjih letih dopolnil in nadgradil.

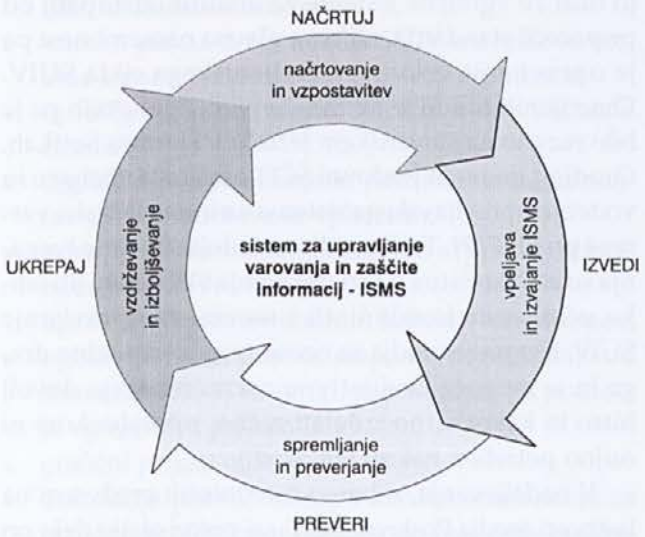
5 VPELJAVA SISTEMA ZA UPRAVLJANJE VAROVANJA IN ZAŠČITO INFORMACIJ

Ko govorimo o varovanju in zaščiti informacij, imamo v mislih predvsem tri lastnosti, ki jih je treba zagotoviti:

- **Zagotavljanje zaupnosti** pomeni zaščito informacij v kakršnikoli obliki (pisni, ustni, elektronski in neelektronski) pred vsakršnim nepooblaščenim vpogledom med njenim shranjevanjem, obdelavo ali prenašanjem. To lahko dosežemo npr. z implementacijo mehanizmov za preverjanje gesel, uporabo pametnih kartic, vgradnjo biometričnih kontrol ali čisto običajnih ključavnic.
- **Zagotavljanje celovitosti** pomeni zagotavljanje točnosti in popolnosti informacij med njenim shranjevanjem, prenašanjem in obdelovanjem. Informacije ne smejo biti nepooblaščeno spremenjene, kar zagotavljamo z mehanizmi za preverjanje vhodno/izhodnih podatkov, uporabo preverjalnih vsot itd.

- **Zagotavljanje razpoložljivosti** pomeni zagotavljanje dostopnosti informacij in storitev pooblaščenim uporabnikom, kadar jih ti potrebujejo in kjer jih potrebujejo. To lahko zagotovimo z uporabo hladne/vroče lokacije, varnostnimi kopijami, zagotovljenimi redundantnimi podatkovnimi kapacitetami na rezervnih lokacijah, postopki okrevanja po nesreči, načrtovanjem neprekinjenega poslovanja.

Za potrebe varnega poslovanja v sodobnem poslovnem okolju morajo podjetja vzpostaviti in implementirati sistem za upravljanje varnosti informacij, ki ga je treba nadalje stalno nadzorovati ter izboljševati. Opisani pristop je edino zagotovilo, da sistem resnično zmanjšuje tveganja. Varnost informacij je treba zgraditi z uporabo različnih upravnih, procesnih in poslovnih nadzornih postopkov [8]. Varnost informacijskih sistemov je treba zagotoviti na začetku izgradnje novega sistema. Izkazalo se je, da so stroški implementacije na začetku projekta do trikrat nižji od stroškov implementacije v zreli fazi delovanja sistema. Tak sistem mora temeljiti na ciljih varovanja ter ustrezni izbiri strategije v odvisnosti od načina in obsega poslovanja, velikosti podjetja, razpoložljivih resursih, organizacijski strukturi in kulturi ter zrelosti organizacije. Bistvo vpeljave sistema upravljanja varnosti informacij je vpeljava sistema za upravljanje tveganj.



Slika 2: **Model PDCA za upravljanje informacijskih tveganj**
(Vir: BS7799-2:2002)

Standard BS7799-2 vpeljuje pomemben princip, imenovan PDCA (Plan – Načrtuj, Do – Izvedi, Check – Preveri, Act – Ukrepaj), ki zagotavlja učinkovito obvladovanje tveganj (slika 2).

Opisani princip pokriva vse faze delovanja SUIV, od njegove vzpostavitve do zrele faze delovanja. V nadaljevanju so naštete zahtevane aktivnosti, ki se morajo izvajati v vsaki od posameznih faz.

5.1 Načrtovanje in vzpostavitev SUIV

V okviru faze načrtovanja in vzpostavitve SUIV je treba določiti obseg SUIV in varnostno politiko. Nadalje je potrebno določiti pristop k ocenjevanju tveganja, poiskati relevantna tveganja in izvesti oceno tveganj. Na podlagi ocene tveganj je treba poiskati in ovrednotiti možna ravnanja s tveganji ter izbrati ustrezna nadzorstva za zmanjševanje tveganj. Izbrana nadzorstva z obstoječimi nadzorstvi tvorijo izjavo o primernosti nadzorstev (angl. *Statement of Applicability*). V fazi vzpostavitve je treba pridobiti tudi odobritev vodstva. Standard opredeljuje zahteve za odgovornost vodstva organizacije, pregled upravljavskega sistema SUIV s strani vodstva in odgovornost za njegovo izboljševanje.

5.2 Vpeljava in izvajanje SUIV

V fazi vpeljave najprej oblikujemo načrt ravnanja s tveganji, ki vključuje prednostno listo za upravljanje varnostnih tveganj vključno s terminskim planom uvedbe (v priporočilu se navede čas, v katerem je treba nadzorstva implementirati), seznam priporočenih nadzorstev, ki evidentirana tveganja zmanjša na sprejemljiv nivo. Načrt za ravnanje s tveganji izvedemo tako, da seznam priporočenih nadzorstev predamo poslovnim lastnikom, ki odločijo, katera nadzorstva se bodo implementirala in kdaj [9]. Razlog za potrebo po vpletenosti poslovnih lastnikov je v tem, da je implementacija nadzorstev povezana s finančnimi sredstvi in ostalimi resursi. Če so določena nadzorstva povezana z visokimi finančnimi sredstvi, je priporočljivo podati tudi alternativna nadzorstva, saj tako zagotovimo, da bodo implementirane vsaj alternativne, čeprav tveganje ne bo popolnoma odpravljeno [15]. Pomembno se je zavedati predvsem dejstva, da je odločitev o implementaciji priporočenih nadzorstev v rokah poslovnih lastnikov in ne informatikov [9].

Po vpeljavi sistema izvedemo usposabljanja za ozaveščanje zaposlenih. Ko sistem pride v polno de-

lovanje, ga moramo ustrezno voditi in izvajati ustrezne postopke.

5.3 Spremljanje in preverjanje SUIV

Faza spremljanja in preverjanja vključuje izvajanje nadzorovalnih postopkov (postopki za hitro ugotavljanje napak obdelave podatkov, varnostnih pomanjkljivosti in incidentov), redno pregledovanje učinkovitosti SUIV, pregledovanje preostalih in sprejemljivih tveganj, redno izvajanje notranjih presoj SUIV, izvajanje vodstvenih pregledov (vodstvo se mora prepričati o tem, ali je izvajanje procesov v skladu s pričakovanim in je zapisano ter če se odpravljanje varnostnih pomanjkljivosti izvaja v skladu z opredeljenimi prioritetami), beleženje dejanj in dogodkov, ki lahko vplivajo na SUIV.

5.4 Vzdrževanje in izboljševanje SUIV

Faza vzdrževanja in izboljševanja vključuje uvedbo prepoznanih možnih izboljšav, vpeljavo korektivnih in preventivnih ukrepov (medtem, ko korektivni ukrepi izničujejo vzroke neskladja s standardom, ki so se pojavili pri delovanju sistema SUIV, preventivni ukrepi skušajo odpravljati bodoča neskladja), prek komuniciranja in posvetovanje doseči potrebni nivo strinjanja vseh vpletenih, skrb za to, da izboljšave dosežejo zadane cilje SUIV.

5.5 Dokumentacija SUIV

V okviru vzpostavitve SUIV je treba pripraviti dokumentacijo. V grobem dokumentacija SUIV sestoji iz:

- krovnih varnostnih politik in ciljev,
- definicije obsega SUIV,
- poročila o ocenah tveganj in načrta ravnanja s tveganji,
- izjave o primernosti nadzorstev,
- področnih varnostnih politik,
- dokumentiranih postopkov in delovnih navodil,
- zapisov in dnevnikov, ki se ustvarjajo pri delovanju SUIV.

Dokumentacijo mora pred izdajo pregledati in potrditi pristojno osebje. Dokumentacija mora biti zapisana zgoščeno, razumljivo in mora biti enolično označena, da je mogoče spremljati različne različice dokumentacije. Dostop do dokumentacije mora imeti vedno samo osebje kateremu je namenjena. Dokumentacijo je treba stalno pregledovati in vzdrževati v skladu z zaznanimi potrebami po spremembah, ki so osnovane na analizi tveganja.

6 UPORABA ORODIJ ZA PODPORO SISTEMU INFORMACIJSKE VARNOSTI ISO/IEC 17799 IN BS 7799-2

Dokumentacija, ki se zahteva v okviru standarda BS7799-2 je lahko v katerikoli obliki, vendar je vzdrževanje in ustrezno menjavanje papirnih različic zahtevna in zamudna naloga, saj moramo zagotavljati, da zaposleni uporabljajo zadnje veljavne različice. Pogosto dostopanje do dokumentacije zahteva urejeno in jasno zapisano dokumentacijo in konsistenten pristop k izvedbi zagotavljanja dostopa do nje. Vzpostavitev in upravljanje takšnega sistema za varovanje informacij v skladu s standardom BS 7799 je bistveno lažje, hitrejše in cenejše z uporabo orodij, ki omogočajo upravljanje dokumentacije v zvezi z varovanjem informacij v skladu z zahtevami standarda ter olajšajo postopek morebitnega certificiranja [14].

Na tržišču se pojavlja kopica orodij, ki omogočajo podporo vzpostavitve SUIV. V grobem jih delimo na dve skupini: orodja za izdelavo ocene tveganja in izbor nadzorstev ter orodja za upravljanje dokumentacije SUIV in celotnega upravljavskega procesa. V prvo skupino orodij spadajo analitična orodja, kot je CRAMM, RA Software, Cobra in mnogo drugih. Načeloma je za uporabo teh specializiranih orodij v organizaciji treba zaposliti strokovnjaka, ki se bo usposobil za uporabo tovrstnega orodja, saj zahteva dobro poznavanje orodja in izgradnjo kompleksnih modelov tveganja. V drugo skupino spadajo orodja, ki imajo tudi že vgrajene sisteme za analizo odstopanj od priporočil standarda, njihova glavna namembnost pa je upravljanje celotnega življenjskega cikla SUIV. Omenjenih orodij je na tržišču manj, eno prvih pa je bilo razvito na slovenskem tržišču v Hermes SoftLab. Orodje z imenom Poslovni ŠČIT omogoča vpeljavo in vodenje upravljavskega sistema za informacijsko varnost po BS 7799. Tudi orodja za izdelavo ocene tveganja so zelo koristna v fazi delovanja SUIV in bi jih lahko učinkovito kombinirali s sistemi za upravljanje SUIV. Ker pa so orodja za oceno tveganj navadno draga in je mogoče kvalitativno oceno tveganja dovolj hitro in kakovostno izdelati ročno, uporabnikom ni nujno potreben nakup teh orodij.

V nadaljevanju se bomo osredotočili predvsem na lastnosti orodja Poslovni ŠČIT, saj precej olajša delo pri upravljanju SUIV. Orodje Poslovni ŠČIT je primerno za vse vrste organizacij in oblike informacij, je popolnoma usklajeno z zahtevami standarda BS7799 (nadzor dokumentacije in upravljanje sprememb, upravljanje

korektivnih in preventivnih ukrepov) ter podpira vse faze pri vzpostavitvi in delovanju upravljavskega sistema. Vsebuje ogrodje za enostavnejšo vzpostavitev in upravljanje SUIV dokumentacije, orodja za analizo odstopanj ter tabele za analizo in upravljanje tveganja, smernice pri analizi tveganja in vzpostavitvi ustreznih nadzorstev. Lahko služi tudi kot osnova za dvig varnostne zavesti zaposlenih ter kot osnova za izobraževanje in usposabljanje zaposlenih s področja informacijske varnosti [12].

6.1 Zgradba in druge lastnosti orodja Poslovni ŠČIT

Poslovni ŠČIT sestavljata dva osnovna sklopa. Prvi omogoča izvedbo analize odstopanj od standarda, drugi pa je namenjen upravljanju dokumentov kot pomoč pri vzpostavitvi upravljavskega sistema za varovanje informacij.

Poslovni ŠČIT vsebuje že nekatere vnaprej pripravljene SUIV dokumente oziroma predloge, ki se nanašajo na informacijska sredstva in ocenjevanje tveganja, klasifikacijo zaupnosti dokumentov in sklop, ki se nanaša na upravljanje SUIV dokumentacije. Klasifikacija zaupnosti dokumentov je skladna z oznakami britanskega ministrstva za trgovino in industrijo (DTI). V praksi se je kot koristen pokazal vgrajen katalog z opredeljenimi grožnjami in ranljivostmi informacijski varnosti, s katerim si lahko bistveno pomagamo pri izdelavi ocene tveganja. Katalog so pripravili BSI strokovnjaki [10].

Glavne lastnosti orodja so:

- vnos in prikaz dokumentov SUIV ter njihove vsebine s pomočjo drevesno organiziranih kazal,
- upravljanje z dokumenti SUIV in njihovimi različicami
- digitalno podpisovanje in potrjevanje dokumentov s strani vodstva in vpletenih,
- upravljanje varnostnih incidentov (prijava, obravnava, korektivni ukrepi),
- upravljanje preventivnih in korektivnih ukrepov,
- ugotavljanje stopnje odstopanja organizacije od standarda BS 7799 (angl. gap analysis) s pomočjo vgrajenih vprašalnikov,
- grafični prikaz odstopanja.
- določanje pravic dostopa do dokumentacije za različne profile uporabnikov do različnih poslovnih področij in različnih nivojev zaupnosti
- poslovni ŠČIT je dostopen prek medmrežja ali intraneta (odjemalec za dostop potrebuje internet brskalnik).

Prednosti uporabe orodja:

- olajša proces vzpostavitve SUIV v podjetju,
- olajša proces certificiranja,
- s pomočjo uporabe orodja lahko zmanjšamo stroške implementacije SUIV,
- s pomočjo uporabe orodja lahko zmanjšamo časovno obdobje, potrebno za certificiranje po BS7799,
- omogoča sledenje incidentov in ustvarjanje zapisov glede incidentov,
- rezultati, ki jih pridobimo s pomočjo orodja za analizo odstopanja, omogočajo osnovo za hitre izboljšave,
- olajša proces vzdrževanja vzpostavljenega SUIV, nadgradnje in stalnega procesa izboljšav.

6.2 Analiza stopnje odstopanja organizacije od standarda ISO17799 (angl. *Gap Analysis*) s pomočjo pametnih vprašalnikov

Analiza odstopanj je sestavljena iz desetih vprašalnikov, ki pokrivajo naslednja področja: politiko informacijske varnosti, organiziranost varovanja, razvrstitev in nadzor sredstev, varovanje v zvezi z osebjem, fizično in okolno varovanje, upravljanje s komunikacijami in obratovanjem, obvladovanje dostopa, razvijanje in vzdrževanje sistema, ravnanje z neprekinjenim poslovanjem, usklajenost [3].

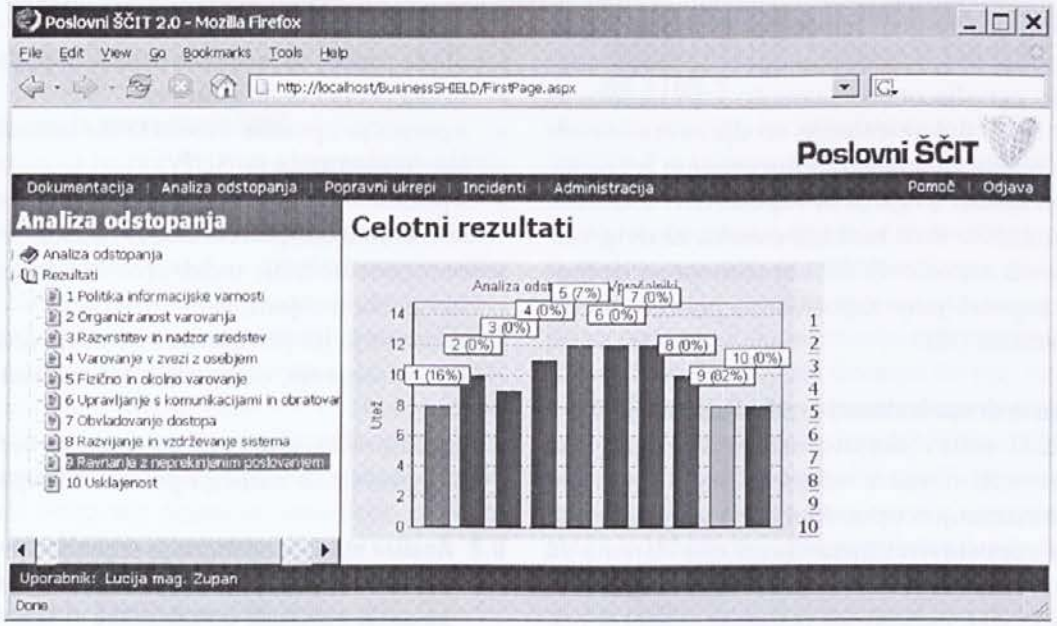
Grafični prikaz rezultatov analize odstopanj omogoča uporabnikom Poslovnega ŠČITA celovit pregled nad varnostjo informacij in podlago za analizo ter ukrepanje.

Grafični prikaz (slika 3) rezultatov analize odstopanj je zasnovan tako, da barva stolpca (rdeča, zelena in različni odtenki oranžne barve) določa odstopanje od standarda, višina pa predstavlja pomembnost posameznega vprašanja.

Z rezultati analize odstopanja na nivoju celotne organizacije ali njenih delov pridobimo nazorno sliko stanja na področju informacijske varnosti in so v prvi vrsti namenjeni vodstvu organizacije. Rezultati so v pomoč tudi pri opredelitvi izboljšav obstoječega sistema in kot vodilo pri opredelitvi najbolj pomanjkljivih področij.

7 NAPAKE IN TEŽAVE PRI VPELJAVI SISTEMA UPRAVLJANJA VAROVANJA V ORGANIZACIJO

Najpogostejša napake pri implementaciji SUIV so nezadostno in sprotno izobraževanje na področju varnosti [9]. Treba se je zavedati, da je varnost neprekinjena dejavnost, za katero morajo biti odgovorni vsi zaposleni. Po besedah Humpreysa (soavtorja BS 7799



Slika 3: **Prikaz zaslonske maske orodja Poslovni ŠČIT (graf z opredelitvijo odstopanj od ISO17799)**

standarda) je druga pogosta napaka, ki jo delajo podjetja, da varnost podatkov prepuščajo oddelku za informatiko. Za varnost nikakor ne more biti odgovorna le določena tehnična funkcija ali oddelek, saj gre za sistematičen proces, ki zadeva celotno organizacijo. Vzroki za delegiranje tako pomembne naloge izvirajo iz prepričanja, da informacijska tehnologija lahko reši vse težave, zato se je treba zavedati, da je tehnologijo mogoče uporabiti le za podporo tem postopkom, ter da tehnologija sama pa še ne pomeni varnosti informacij in ni primarni vir nadzora. V praksi se pogosto srečamo tudi z ovirami, kot so nezadostna zavzetost vodstva, neformalni pristopi k organiziranju varovanja, razkorakom med dodelitvijo virov in pričakovanji ter odsotnostjo funkcije neodvisnega preverjanja delovanja in urejanja varnosti v organizacijah.

Z varnostjo informacij se je treba spoprijeti na vseh ravneh poslovanja in se ji posvetiti na dnevni ravni. Ključnega pomena so stalni pregledi sistema in njegovo izboljševanje. Le na ta način lahko zagotavljamo varnost informacijskega sistema v vsakem trenutku, ne glede na spremembe, ki se odvijajo v procesih in sredstvih.

Ključni dejavnik uspeha vpeljave SUIV so zaposleni, ki morajo varnostno politiko sprejeti, vključno z upravo in vodstvom, ki morata še posebej z zgledi in lastnim upoštevanjem napisanih pravil pokazati, da izdelana politika varovanja velja za vse.

Dostikrat se kot težava izkaže tudi preobsežna in neobvladljiva dokumentacija. Zelo hitro se lahko zgodi, da upravljamo z goro papirja, v katerem se težko znajdejo že njegovi avtorji, kaj šele ciljni zaposleni. Težave so tudi pri razdeljevanju dokumentacije med zaposlene. Rešitev omenjenih težav predstavlja uporaba referenčnega orodja pod točko 3.1.

8. IZDELAVA OCENE TVEGANJA JE ZA MNOGE NAJTEŽJI DEL PRI VZPOSTAVITVI UPRAVLJAVSKEGA SISTEMA ZA VARNOST INFORMACIJ

Standard BS7799-2 predvideva 127 nadzorstev, ki so razvrščena v deset poglavij in namenjena doseganju 36 ciljev. Očitno je, da standard ni namenjen temu, da bi ga vzeli v roke in v svoje politike neposredno prepisali vsa nadzorstva. V ta namen standard zahteva izvedbo formalne ocene tveganja, ki je temeljna osnova za izbiro ustreznih nadzorstev ter za izdelavo varnostne politike, notranjih standardov in postopkov. Mnogim je ravno ta del najtežji del uvajanja standarda.

Standard ne predpisuje metodologije in načina ocenjevanja, izbira je prepuščena izvajalcu, vendar mora biti formalizirana, kar pomeni opredeljena,

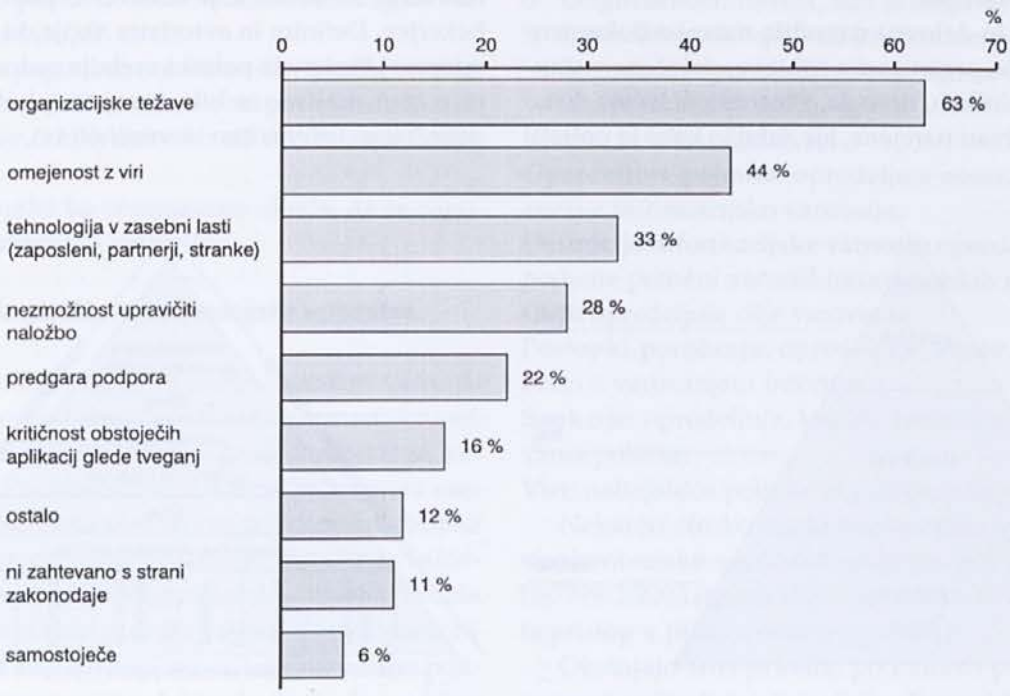
zapisana, učinkovita, ponovljiva, izvajana in pregledana.

Cilj analize tveganja so racionalna in gospodarna poraba sredstva za varovanje informacij ter uvedba mehanizmov za zmanjševanje tveganja, s katerimi zmanjšamo možnosti pojava groženj ter nadziramo velikost izgube sredstev.

V praksi se pogosto pojavlja miselnost, da lahko tudi brez predhodno izvedene analize tveganja uspešno vpeljemo sistem varovanja. Na trgu se pojavljajo celo podjetja, ki ponujajo izdelavo krovne varnostne politike in treh elementarnih politik za zelo nizko ceno. Slednje lahko povzroči napačno razumevanje problematike nepoznavalcev in tistih, ki se področja lotevajo na novo. Opisani pristop nam lahko le navidezno prinese manjše stroške, zelo vprašljiva pa je učinkovitost in sploh smiselnost vpeljave takega sistema varovanja.

Mnogi se znajdejo pred vprašanjem, kako pravzaprav vpeljati sistem varovanja, kje se lotiti. Smiselno je pristopiti sistematično in uporabiti fazni pristop. Najprej izvedemo analizo trenutnega stanja, s katero pregledamo, katera od nadzorstev, ki jih priporoča standard, imamo implementirana v našem informacijskem sistemu (to omogoča tudi referenčno orodje pod točko 6, ki z vgrajenimi posebnimi pametnimi vprašalniki omogoča izvedbo analize odstopanj). V drugem koraku se lotimo izvedbe analize tveganja, ki pove, ali je treba implementirati dodatna nadzorstva. Opisani pristop pomeni tudi smotrno ravnanje z viri, saj vemo, da varnostne rešitve lahko zahtevajo izdatna finančna sredstva. Tudi pri varovanju informacij je smiselno upoštevati princip 80/20. To pomeni, da najprej implementiramo tista nadzorstva, ki prinašajo 80 % koristi oziroma predstavljajo 20 % investicije. Začeti je treba pri preprostih in učinkovitih rešitvah. Ta nadzorstva pogosto zahtevajo izboljšanje ali spremembo postopkov, kar ne zahteva velikih finančnih sredstev, temveč predvsem čas, trud in vztrajnost. Zanimivo je, da META Group ocenjuje, da je ravno potreba po spremembi organiziranosti najpogostejši vzrok, zakaj se podjetja ne odločajo za vpeljavo informacijske varnosti (slika 4) [6].

Odstotek, ki ponazarja organizacijske težave (63 %) bi bilo smotrno podrobneje analizirati in razdeliti v podskupine, kjer bi podrobneje ugotavljali vzrok težav (zaposleni, organiziranost podjetja, poslovna vizija organizacije, plačilna politika in drugo). Načeloma tudi



Slika 4: **Razlogi za nezadostno vpeljavo infrastrukturnih rešitev informacijske varnosti** (Vir: META Group 2003)

na področju uvajanja informacijske varnosti velik zaviralni dejavnik predstavljajo ljudje, ki so predvsem v togih organizacijskih strukturah nenaklonjeni spremembam in je zato uvajanje nove discipline in organizacijskih pravil lahko težavno.

9 VPELJAVA INFORMACIJSKE VARNOSTNE POLITIKE

Da bi razumeli poslanstvo varnostne politike, moramo najprej razumeti razliko med varnostno politiko, internimi varnostnimi standardi in varnostnimi postopki ter delovnimi navodili.

Varnostna politika daje odgovor na temeljno vprašanje »Zakaj naša organizacija sploh varuje svoje podatke?« Običajno imamo samo eno visokonivojsko varnostno politiko, kjer so zajeti cilji in strategija informacijske varnosti. Poleg krovne politike obstajajo še področne varnostne politike, ki se lahko nanašajo na različna poslovna področja, različne vire ali kritične procese. Varnostna politika navaja, kaj mora biti narejeno, kdo mora to narediti in zakaj.

Standardi organizacije dokumentirajo, kaj organizacija namerava narediti, da bi se varnost informacijskih sistemov implementirala in vzdrževala. Standardi določajo, kaj mora biti narejeno in kakšna varnostna nadzorstva so zahtevana, da se zaščiti informacijska varnost.

Postopki in delovna navodila natanko dokumentirajo, kako bo organizacija zahteve, določene v standardih in politikah, dosegla. Postopki določajo, kako morajo biti stvari narejene, kje, kdaj in kako je potrebno politiko vpeljati v prakso. Postopki so hkrati tudi osnova za napisane nadzorne sezname (angl. *Checklists*).

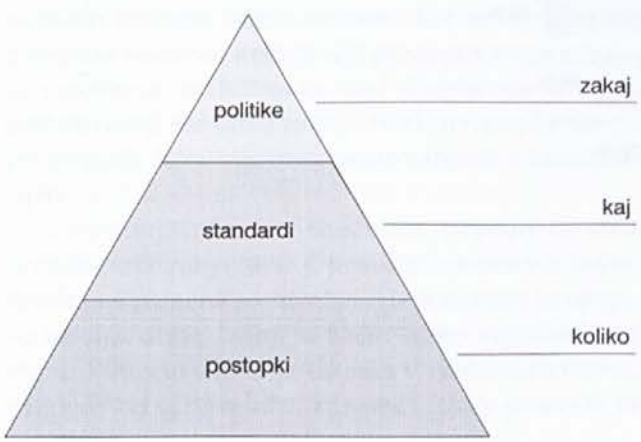
Slika 5 prikazuje razmerje med politikami, standardi in postopki.

9.1 Lastnosti in zgradba informacijske varnostne politike

Informacijska varnostna politika je nabor izbranih ukrepov za zaščito informacije. Uvedeni ukrepi morajo biti rezultat ocene tveganja, ki je določena na podlagi ranljivosti virov. Varnostna politika obsega strateške usmeritve varovanja in zaščite informacij, ne opisuje pa podrobnosti o izvajanju nadzorstev. V okviru vzpostavitve SUIV se predvideva pristop od zgoraj navzdol. Najprej izdelamo visokonivojsko varnostno politiko, kjer določimo obseg varovanja, na podlagi ocene tveganja pripravimo izjavo o primernosti nadzorstev, varnostne politike in šele nato definiramo ustrezna delovna navodila, standarde in postopke.

Shematsko zgradbo SUIV prikazuje slika 6.

Varnostna politika ščiti ljudi in informacije. Postavlja pravila za pričakovano obnašanje ljudi, sistemskih administratorjev, vodstva in varnostnega osebja. Varnostno osebje pooblašča za nadzor, raziskovanje, preiskovanje na način, ki je lahko zelo podoben početju hekerjev. Definira in avtorizira akcije, ki so posledica vdorov. Učinkovita politika vsebuje zadostno definicijo o tem, kaj mora biti narejeno, kako jo lahko definiramo ter merimo in vrednotimo.



Slika 5: **Relacije med varnostnimi politikami, varnostnimi standardi in varnostnimi postopki** (Vir: Broderick S., 2003)

Slika 6: **Organiziranost SUIV** (Vir: Thorp, 2004)

Varnostna politika mora iskati ravnotežje med nivojem dostopnosti do sistema in varnostjo. Nivo dostopnosti vključuje zmogljivost in enostavnost uporabe, varnost pa vključuje celovitost, razpoložljivost in zaupnost. Ti koncepti se ne nanašajo samo na računalnike in omrežje, temveč na celotno organiziranost.

V kolikor politika ni direktno povezana z realnimi potrebami in zahtevami organizacije, bo organizacija še nadalje izpostavljena tveganjem, kot da politike sploh ne bi bilo. Varnostna politika mora po obsegu biti sorazmerna z dejansko izmerjenimi tveganji. Politika predstavlja smernice, ki nakazujejo zavestno odločitev v zvezi s sprejetimi cilji. Politika mora biti učinkovita in realna glede želenih ciljev. Učinkovita in realna varnostna politika je ključ do učinkovite in dosegljive varnosti. Na praktično vsakem z varnostjo povezanem seminarju je dobra varnostna politika omenjena kot nujna osnova za ukrepe in procedure. Moramo razumeti, kaj pomeni politika, ker se v zvezi s tem pojavlja veliko nasprotujočih si definicij.

Varnostna politika bi morala vsebovati prepričanje vodstva o tem, kakšen vpliv imajo informacije na poslovanje podjetja. Politika bi morala tudi jasno povedati:

- Zakaj je informacija strateškega pomena za organizacijo?
- Kakšne so poslovne zahteve za informacijsko varnost organizacije?
- Kakšne so pogodbene obveznosti v zvezi z varnostjo informacij, ki se nanaša na poslovne procese, informacije, ki jih zbiramo od svojih zaposlenih, kupcev?
- Katere korake bo organizacija ubrala, da se zagotovi informacijska varnost?

9.2 Vsebina in struktura informacijske varnostne politike

Menja o tem, kako najbolj pravilno napisati varnostno politiko, se med strokovnjaki za informacijsko varnost precej razlikujejo. Razlike gredo vse od tega, koliko strani naj politika obsega, katere točke mora vsebovati, do tega, kako obsežna in celo kako podrobna naj bo. BSI je na temo strukture in obsega informacijske varnostne politike podal skromne okvire. Na zadnjem sestanku presojevalcev in izvedencev BS7799 je bila tematika informacijske varnostne politike resno obravnavana. Izkazalo se je, da različna podjetja različno prakticirajo število in dolžino politik (koliko strani obsega). Številke so se gibale od 1–20.

Iz navedenih razlogov je bistvenega pomena, da se strokovna javnost zedini in posvetuje glede odprtih vprašanj na tem področju in osnuje najboljšo prakso. Slovenija ima zaradi svoje majhnosti še posebno veliko specifik in se teže opira na prakso razvitih držav, kjer majhno podjetje šteje 100–200 zaposlenih.

Pri pisanju varnostne politike se je koristno in smotrno opreti na najboljšo prakso. Zato navajam priporočila SANS Institute, ki so hkrati tudi priporočila mnogih drugih institucij, po katerih naj varnostna politika vključuje naslednje tipične elemente [7]:

1. **Namen:** pojasnjuje razloge, zaradi katerih je bila politika ustvarjena.
2. **Povezani dokumenti:** našteva vse dokumente (ali druge politike), ki vplivajo na vsebino te politike.
3. **Preklic:** identificira katerokoli obstoječo politiko, ki je bila preklicana z nastankom te politike.
4. **Ozadje:** zagotavlja obsežno informacijo o tem, zakaj je politika potrebna, poudari pomen informacijske varnosti.
5. **Obseg:** pojasnjuje, katera področja politika pokriva (celotna organizacija ali njeni deli).
6. **Izjava:** določa dejanske principe oziroma kaj mora biti narejeno, da se zagotovi želeni nivo varnosti.
7. **Akcije:** navaja, katere akcije so potrebne in kdaj morajo biti izvršene.
8. **Odgovornost:** navaja, kdo je odgovoren za kaj.
9. **Lastništvo:** navaja, kdo je sponzor politike in od koga dobiva pooblastila, prav tako navaja, kdo lahko spreminja politiko.

K temu bi lahko dodali še:

Opredelitev pojmov: opredeljuje osnovne pojme v zvezi z informacijsko varnostjo.

Definicija informacijske varnosti: opredeljuje, kaj za podjetje pomeni varnost informacijskih sistemov.

Cilji: opredeljuje cilje varovanja.

Postopki poročanja: opredeljuje, komu se poroča v zvezi z varovanjem informacij.

Sankcije: opredeljuje, kakšne so sankcije neupoštevanja politike.

Viri: nahajališče politike in zadnje verzije.

Nekateri strokovnjaki zagovarjajo tudi izdelavo visokonivojske varnostne politike, kot ga predlaga BS7799-2:2002 standard v točki: 4.2.1 a in b. Vendar se ta pristop v praksi redkeje uporablja.

Obstajajo štiri pravila, po katerih preverite ustreznost vaše obstoječe politike. Preveriti morate [7]:

- Ali je konsistentna in usklajena z visokonivojsko varnostno politiko in smernicami?

- Ali je dolgoročno perspektivna in s tem neobčutljiva na spremembe?
- Ali ima določen terminski načrt za pregled in je trenutno veljavna?
- Ali je hitro in brez težav dostopna vsem, ki jim je namenjena?

Pri preverjanju ustreznosti obstoječe politike ali snovanju nove politike se lahko poslužujete sledečih devetih korakov.

Korak 1: Preverite, da varnostne politike vsebujejo najbolj splošne elemente. Preglejte zgoraj predlagane elemente in preverite, kaj manjka v vaši politiki. Različne organizacije imajo različno vsebino politik in uporabljajo različno terminologijo za opis specifičnih področij. V praksi ni smiselno vključiti vseh postavk, temveč predvsem tiste, ki so za organizacijo relevantne in omogočajo organizaciji učinkovite smernice. Npr. vsi v organizaciji morajo vedeti, katero politiko morajo upoštevati.

Korak 2: Preglejte, če je varnostna politika jasno in zgoščeno napisana. Najlažji način, da preverimo jasnost politike je, da intervjuvamo odgovorno osebje o tem, ali razume in se strinja z vlogami, opredeljenimi v politiki.

Korak 3: Preglejte, če je zgoščena in jedrnata. Področna varnostna politika ne bi smela preseči dveh strani. Mnogo organizacij jo omeji na eno stran. Zalo pogosto bo politika vključno z izjavo obsegala en stavek. Ne smemo pozabiti, da je to politika, ne delovno navodilo. Mora biti opisano, kaj je zaželeno o neki določeni stvari, ne pa kako naj bo to izvedeno.

Korak 4: Preglejte, če je realistična. Politika od ljudi ne bi smela zahtevati, da izvršijo nekaj, kar ni možno ali se ne sme izvršiti. To se zlahka zgodi, kadar politika presega svoje okvire in se spušča globlje od smernic in napotkov ter začenja razlagati izvedbene podrobnosti.

Korak 5: Preglejte, če zagotavlja zadostna navodila o tem, katere procedure se morajo na podlagi politike definirati. Preverite, če politike omogočajo zadostno osnovo za razvoj specifičnih postopkov. Če imate politiko povezave do medmrežja, morate biti na podlagi te sposobni razviti postopke, ki vam omogočajo napotke za nastavitve požarnega zidu. Postopki so tudi osnova za nadzorne liste. Pisanje politik in nadzornih list predstavlja dodatno delo, zato je včasih to za mnoge tudi nadležna naloga. Mnogo organizacij ima enega ali dva zaposlena, ki sta sposobna konfigurirati sisteme, požarne zidove in usmerjevalnike. Ampak kaj se zgodi, ko to osebje ni dostopno ali ko je minilo že več mesecev, odkar so nastavili določen sistem? Če je pomembno, da stvari izvedemo prav, je pomembno tudi, da za to obstaja in se upošteva določen nadzorni seznam.

Korak 6: Preglejte, ali je konsistentna in usklajena z visokonivojsko varnostno politiko in smernicami? Če ugotovite neskladje med področno politiko in visokonivojsko varnostno politiko, si to zabeležite, ko boste morali spremeniti tako, da bo politika imela pomen. Politika mora biti usklajena tudi z veljavno zakonodajo. Vse ugotovljena odstopanja se morajo nemudoma popraviti.

Korak 7: Preglejte, ali je pripravljena na dolgi rok in je neobčutljiva na spremembe. Vse politike, vključno z varnostno, morajo biti relativno stabilne, tako da so njene spremembe potrebne le izjemoma. Posledica tega je, da so usmerjene v prihodnost. Varnostna politika ne bi smela biti vezana na tehnologijo ali ljudi, celo ne na trenutno organiziranost in poslovne procese. Npr. odgovornosti politike morajo biti vezane na vloge in ne na posameznike. Ne sme biti specifična za programsko, strojno in drugo tehnološko opremo.

Korak 8: Preglejte, ali se politika redno pregleduje, da se zagotovi ažurnost. Politika bi morala biti redno pregledovana. Pregledi in uvajanje morajo odsevati izkušnje, ki so bile pridobljene v okviru realiziranih incidentov in novih groženj, ki pretijo informacijski varnosti. Postopki, izvedeni iz politike, so posebno odporni na spremembe, medtem ko se tehnologija in področje varnosti hitro spreminjata.

Korak 9: Preglejte, ali je hitro in brez težav dostopna vsem, ki jim je namenjena? Varnostna politika mora biti vgrajena v priročnike zaposlenih in objavljena za referenco. Morala bi biti zahtevana kot obvezno branje za novo zaposlene. Da bi bili skladni s politiko, morajo biti tisti, ki jo morajo poznati, z njo seznanjeni, jo razumeti in biti seznanjeni tudi s tem, kako ukrepati v primeru nejasnosti in biti zavezani k njenemu izvajanju. Če ne morete meriti skladnosti, je politika neizvedljiva.

9.3 Informacijska varnost zahteva dobro trženje znotraj podjetja

O potrebi po konsistentnem izvajanju zaščitnih ukrepov, postopkov in standardov je potrebno stalno osveščati vse ravni podjetja. Če varnostne politike ne

bodo sprejeli zaposleni, ne bo nikoli zaživela v praksi. Zato je interni marketing informacijske varnosti pri uspešni vpeljavi SUIV ključnega pomena. Vpeljava varnostne politike zahteva spremembo organizacijske kulture, kar je še posebej zahtevna naloga. Učinkovite organizacije se pri uvajanju informacijske varnosti poslužujejo tudi marketinga - hodnike organizacije in oglasne deske polepijo s posterji in brošurami ter organizirajo kratke tečaje tipa "how to" npr. kako izbrati dobro geslo, ter "why" – zakaj je dobro geslo pomembno. Marketing se lahko izvaja tudi z drugimi mehanizmi, ki so npr. vzpostavitev varnostnega foruma, novic na intranetu, e-izobraževanje in uporaba elektronske pošte za obveščanje. Informacijska varnost mora postati stalna točka dnevnega reda na kolegijih in zborovanjih uprave. Poleg tega je v podjetju priporočljivo vzpostaviti tudi varnostni forum, ki redno obravnava tekoče probleme v zvezi z varnostno tematiko. Strokovnjaki priporočajo, da se izobraževanje o informacijski varnosti in varnostni forum vzpostavita v čimbolj zgodnji fazi življenjskega cikla projekta. Ko je SUIV vzpostavljen, postaneta marketing in ozaveščenost zaposlenih kritična za sodelovanje zaposlenih. Zaposleni bodo veliko bolje sprejeli sistem, če bodo vanj vpleteni že od začetka, saj bodo nanj lahko vplivali, podali predloge in morebitno nestrinjanje, kar bo povzročilo večji občutek povezanosti z novim sistemom.

Poleg tega podjetja v svetu ugotavljajo, da učinkovit marketing prispeva k večjim investicijam vodstva v informacijsko varnost, kar je predvsem pomembno v primeru zamenjave vodstva [11]. Pri vpeljavi kateregakoli ukrepa ali rešitve za informacijsko varnost se soočimo s potrebo po strinjanju vodstva (finančna in moralna podpora), kar pa se dostikrat izkaže kot izjemno zahtevna naloga. Vodstvo govori poslovni jezik in na področje informatike gleda predvsem s poslovnega vidika. Enako velja za področje varnosti in zaščito informacij. Iz tega izhaja potreba po vpeljavi učinkovitih pristopov k trženju informacijske varnosti znotraj podjetja. Od vodje informacijske varnosti (ali od pristojnega osebja, ki je zadolžen za projekt vpeljave varnosti informacij) se zahtevajo dobre komunikacijske veščine in sposobnosti opredelitve koristi in ne nazadnje tudi opredelitve ROI (angl. *Return On Investment*). Bistveno se je usmeriti na poslovni učinek ter se izogniti pretirano kompliciranim in tehnično obarvanim razlagam. Področje informacijske varnosti je področje, kjer se najteže izkazuje donosnost investicij ali celo povečanje dobička [18]. Le ob pravilnih metrikah lahko ocenimo bistvene prednosti, ki jih prinaša, urejen, zanesljiv in varen informacijski sistem.

Veliko vodij informacijske varnosti v okviru internih marketinških pristopov skuša kot mehanizem za prepričevanje vodstva uporabiti številke o vdorih v organizacijah iste dejavnosti [11]. Vendar pa bi se morali pri prepričevanju vodstva in predstavitvi upravičenosti v naložbo usmerjati predvsem na analizo tveganja lastnega poslovnega sistema in analizo lastnih stroškovnih koristi ter svojo bazo preteklih incidentov. V praksi se izkaže, da mnogo podjetij ne zbira podatkov o svojih incidentih in tako tudi nima ustrezne osnove za postavitev metrik. Tako zelo težko izračunamo ROI. Naj to prikažemo na primeru. Ena izmed od možnih formul za izračun ROI informacijske varnosti je sestavljena iz dveh delov pri kateri najprej izračunamo letno pričakovano izgubo [5]:

$$ALE = (R-E) + T$$

T - vrednost nakupa sistema za preprečevanje vdorov - IPS (angl. *Intrusion Prevention System*)

E - vrednost, ki jo prihranimo s preprečitvijo vdorov na podlagi implementiranega IPS

R - stroški, ki jih imamo na leto v primeru realiziranega vdora oziroma stroški okrevanja

ALE - (angl. Annual Lost Expectancy) - Pričakovana letna izguba

Iz tega nadalje izračunamo donosnost investicij sistema za preprečevanje vdorov – (ali kako drugo implementirano kontrolo).

$$R - ALE = ROSI$$

Če v podjetju ne zbiramo podatkov o tem, koliko vdorov je v enem letu nastopilo in koliko smo jih uspeli preprečiti, je jasno, da po tej formuli vrednosti ROSI ne bomo uspeli izračunati. Zato se mnogi poslužujejo zunanjih raziskav o vdorih, vendar tudi to ne kaže, da bi bila prava pot. Na splošno je uporaba raziskav zunanjih institucij kot osnove pri določanju vrednosti investicij v varnost IS lahko le dopolnilo notranjim kazalcem. Potrebno se je zavedati, da so statistike dostikrat lahko zelo zavajajoče, saj običajno nimamo podatka o tem, katere organizacije so bile vanje zajete (velikost organizacij, struktura anketiranih, položaj anketiranih v podjetju) [4]. Potrebno je

upoštevati tudi dejstvo, da večina organizacij, ki zbira podatke o vdorih in stanju varnosti le-te tudi skrbno skriva in so zato statistike lahko izkrivljene.

10 SKLEPNA MISEL

Informacijska varnost je pomembna, saj je od nje lahko odvisna prihodnost našega poslovanja. Pri vzpostavitvi sistema varovanja in zaščite informacij se je smiselno in koristno opreti na veljavne standarde kot je BS7799. Standard med drugim vpeljuje uporabo konsistentnih principov, ki omogočajo sistematičen in celovit pristop k vpeljavi sistema varovanja v podjetje. Pri vpeljavi sistema varovanja v organizacijo so lahko v veliko pomoč računalniško podprti sistemi za vzpostavitev in upravljanje SUIV. Ključni dejavnik uspeha pri vzpostavitvi SUIV so zaposleni, ki so še vedno največji kritični dejavnik vsakega informacijskega sistema. Zato je posebej pomembno, da uspemo razviti tehnike in pristope za zagotavljanje osveščenosti vseh zaposlenih. Bistvo vzpostavitve sistema varovanja ni certificiranje, temveč njegovo delovanje, redno vzdrževanje, spremljanje in izboljševanje. Opisani pristop je edino zagotovilo, da bo sistem dolgoročno zagotavljal učinkovito in uspešno obrambo pred številnimi grožnjami ter ustrezno prilagodljivost v svetu nenehnih sprememb poslovnega, informacijskega in zakonodajnega okolja.

LITERATURA IN VIRI

[1] Broderick S., PhD Symantec Security Services, Information Security Policies, Standards and Procedures – Part 1, 2003.

[2] BS 7799-2:2002: Information Security Management Systems - Specifications with guidance for use.

[3] BS ISO/IEC 17799:2000: Information technology – Code of practice for information security managementBroderick S., Information Security Policies, Standards and Procedures – Part 1., PhD Symantec Security Services, 2004.

[4] Carsten C., Damage Statistics: More damage than statistics?, Security and Risk strategies, Delta 2982, META Group, julij 2004.

[5] CISM REwiev Manual, 2003, ISACA.

[6] Enterprise Security Desk Reference, METAGroup, 2003.

[7] Establishing a 7799 Information Security Management System , SANS Institute, 2004.

[8] Humphreys T., Zmanjšati tveganje, SRC info, 2002.

[9] Humpreys T., Angelika P., Information Security Management Systems; Information Security Risk Management Workshop, Bled 2003.

[10] Interno gradivo Hermes SoftLab d.d., © 2002–2004.

[11] Kosanovich M., Best Practices in Enterprise Security: Staffing, Marketing, and Justification, Global Networking Strategies, Delta 707, METAGroup 1999.

[12] Predstavitev orodja za vzpostavitev SUIV v podjetju po BS7799:2002:2, http://www.business-shield.com., [2. 2. 2005].

[13] Prihodnost BS7799, http://www.gammassl.co.uk/bs7799/future.html, [1. 2. 2005].

[14] Računalniško podprt upravljavski sistem za varovanje informacij, Rado Ključevšek, Marko Zebec Koren, INDO 2001.

[15] Rudel D., Varovanje informacij v slovenskem zdravstvu, Varnostni Forum, l.1, julij/avgust 2004.

[16] Šalej A., Kako vzpostaviti sistem za uspešno in učinkovito varovanje in zaščito informacij?, INFO SRC.SI, Letnik 35, 2003.

[17] Thorp, C., Implementing ISO17799: Pleasure or Pain?, Control Journal, Volume 4, ISACA; 2004.

[18] Zupan L., Informacijska varnost – prestiž ali nujnost? SISTEM, 2004.

[19] Zupan L., Slovenija skozi prizmo informacijske varnosti, Zbornik DSI 2004.

Lucija Zupan je zaposlena v Hermes SoftLab, d. d. kot svetovalka za informacijsko varnost. Na Fakulteti za organizacijske vede Univerze v Mariboru je leta 2000 diplomirala na smeri organizacijska informatika s področja informacijske varnosti, leta 2004 pa je magistrirala s področja analize in načrtovanja informacijskih sistemov leta 2004. Ključne delovne naloge in projekti, katerim se je v preteklem obdobju posvečala, so varovanje podatkov in informacijskih sistemov, analiza in načrtovanje informacijskih rešitev, strateško načrtovanje informatike v profitnih in neprofitnih organizacijah, e-izobraževanje s področja informacijske varnosti. Opravljen ima izpit za vodilnega presojevalca po BS7799 in je članica skupine presojevalcev in izvedencev s področja BS7799, ki deluje v Sloveniji pod okriljem SIQ. Obenem je članica mednarodnega združenja revizorjev informacijskih sistemov (ISACA – Information Systems Audit and Control Association) in redno spremlja dogajanje na področju informacijske varnosti.