Novosti, ki jih prinašajo spremembe standarda BS 7799

Lucija Zupan[1], Alenka Brezavšček[2]

[1]HERMES SoftLab d.d., Litijska 51, 1000 Ljubljana, lucija.zupan@hermes.si
[2]Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva cesta 55a, 4000 Kranj, alenka.brezavscek@fov.uni-mb.si

Članek opisuje lastnosti standarda za informacijsko varnost BS 7799 in navaja koristi njegove uvedbe v organizacijo. Podana je kratka zgodovina standarda. Podrobno so opredeljene spremembe, ki jih prinašata najnovejši izdaji standarda, in sicer BS ISO/IEC 17799:2005 in BS ISO/IEC 27001:2005. Avtorici obravnavata možne vplive teh sprememb na organizacije, ki so svoje sisteme za upravljanje informacijske varnosti (SUIV) oblikovale na osnovi prejšnjih verzij standarda BS 7799. Opisano je tudi, katere standarde s področja zagotavljanja informacijske varnosti lahko organizacije pričakujejo v naslednjih letih.

Ključne besede: informacijska varnost, standard BS 7799, nova izdaja, spremembe, vpliv na organizacije, prihodnost standarda

1 Uvod

V današnjem tekmovalnem poslovnem okolju so informacije, ki so ključne dobrine vsakega poslovnega sistema, stalno podvržene številnim grožnjam iz različnih virov. Z uporabo sodobnih tehnologij pa ogroženost informacij še narašča. Vsaka organizacija razpolaga s številnimi informacijami različnih tipov. Informacije so lahko napisane ali natisnjene na papir, shranjene na različnih medijih, posredovane elektronsko ali preko običajne pošte, lahko so različne predstavitve ali video gradiva, podatkovne zbirke ali govorne informacije. Skrbi za informacijsko varnost so začele organizacije po celem svetu posvečati pozornost v poznih devetdesetih letih. Nekaj katastrofalnih dogodkov je bilo potrebnih, da so organizacije na lastni koži občutile resnost posledic zaradi izgube zaupnosti, celovitosti ali razpoložljivosti informacij oziroma drugih dobrin informacijskega sistema.

Upravljanje informacijske varnosti v organizaciji zahteva dobro poznavanje lastnih dobrin, njihove vrednosti za organizacijo kakor tudi njihovih ranljivosti. Prevzemanje odgovornosti za zagotavljanje varnosti informacijskih dobrin pomeni zmanjševanje tveganj za uresničitev različnih groženj, ki tem dobrinam pretijo. V ta namen je potrebno v organizaciji vzpostaviti ustrezen sistem za upravljanje informacijske varnosti (v nadaljevanju SUIV), ki nudi organizaciji ogrodje za učinkovitejše obvladovanje varnostnih tveganj.

Pri vzpostavitvi SUIV v organizaciji se je smotrno opreti na ustrezne standarde. Strokovnjaki so si enotni, da je na področju informacijske varnosti najbolj celovit standard BS 7799. Standard BS 7799 se je pojavil leta 1995, njegovemu velikemu razmahu pri uporabi pa smo priča šele po letu 2001. Standard podaja preizkušene smernice, kako naj se organizacije spoprimejo s problemi zagotavljanja informacijske varnosti na celovit in učinkovit način. Z uvedbo standardov, kot je BS 7799, želijo organizacije zmanjšati pogostost uresničenih groženj varnosti in tako znižati stroške, ki pri tem lahko nastanejo. Poleg tega omogoča uvedba standardov boljšo organiziranost poslovnih procesov, kar zagotovo poveča učinkovitost poslovanja. Organizacije želijo nastopati v očeh svojih poslovnih partnerjev kot ugleden in zanesljiv partner, saj le na ta način lahko ohranijo konkurenčnost in obdržijo svoj prostor na tržišču. V reviji ISMS (2004) lahko zasledimo, da je poslovanje organizacij, katerih varnostna politika je skladna s standardom BS 7799, bolj urejeno, bolj pregledno in ga je laže nadzirati. Take organizacije so bolje pripravljene na zahteve neprekinjenega poslovanja, v 85% primerov bolje obvladujejo uresničene grožnje varnosti (z nižjimi stroški in boljšo odzivnostjo), 53% pa jih celo dosega višjo donosnost investicij. V splošnem lahko rečemo, da zavest organizacij o pomembnosti standardov, kot je BS 7799, tudi v Sloveniji raste. Slovenske organizacije so začele prepoznavati številne koristi, ki jih vpeljava standarda lahko prinese. Pričakovati je, da bo uporaba standardov s področja informacijske varnosti v slovenskem prostoru v prihodnosti še narasla.

V članku bomo na kratko predstavili zgodovino standarda BS 7799 in opisali dosedanjo verzijo standarda. Podrobno bomo predstavili spremembe v obeh delih nove izdaje standarda, ki sta izšla v drugi polovici leta 2005. Skušali bomo povzeti bistvene spremembe ter jih podati na strukturiran in razumljiv način. Proučili bomo, kako te spremembe vplivajo na organizacije, ki so svoje sisteme

varovanja informacij zasnovale na prejšnjih verzijah standarda. Navedli bomo tudi, katere standarde s področja informacijske varnosti lahko organizacije pričakujejo v naslednjih letih.

2 Zgodovina standarda BS 7799

BS (British Standard) 7799 je mednarodno uveljavljen standard za varovanje informacij. Prvič se je pojavil v Veliki Britaniji leta 1995 kot BS 7799:1995 Kodeks varovanja informacij (*angl. Code of practice for information security management*). V Sloveniji je bil s strani Slovenskega inštituta za standardizacijo (SIST) leta 1997 sprejet kot predlog slovenskega standarda PSIST BS 7799:1997. V takratni obliki je standard vseboval zgolj priporočila za zagotavljanje varnosti informacij, ni pa omogočal certificiranja organizacij.

Leta 1999 je bil v Veliki Britaniji objavljen posodobljen prvi del standarda, BS 7799-1:1999 Upravljanje informacijske varnosti – 1. del: Kodeks varovanja informacij (*angl. Information security management – Part 1: Code of practice for information security management*) in povsem nov drugi del standarda, BS 7799-2:1999 Upravljanje informacijske varnosti – 2. del: Specifikacija za sisteme za upravljanje informacijske varnosti (*angl. Information security management – Part 2: Specification for information security management systems*). Drugi del standarda iz leta 1999 je prvič vpeljal pojem sistema za upravljanje informacijske varnosti SUIV (*angl. ISMS – Information security management system*). Z opredelitvijo preverljivih minimalnih zahtev za zagotavljanje varnosti informacij je postavil osnovo za možnost certificiranja organizacij po BS 7799-2 (Hermes SoftLab, 2002-2005).

Prvi del standarda s priporočili je posodobljen izšel leta 2000 kot BS 7799-1:2000 Informacijska tehnologija – Kodeks za upravljanje varovanja informacij (*angl. Information technology – Code of practice for information security management*) in je bil v identični obliki sprejet tudi kot mednarodni standard ISO/IEC 17799:2000 (glej BSI, 2000). Leta 2002 je izšla posodobljena izdaja drugega dela standarda s specifikacijami kot BS 7799-2:2002 Sistemi za upravljanje informacijske varnosti – Specifikacija s smernicami za uporabo (*angl. Information security management systems - Specification with guidance for use*; glej BSI, 2002). SIST je leta 2003 sprejel zadnji izdaji obeh delov standarda kot slovenska standarda z oznakama SIST ISO/IEC 17799:2003 in SIST BS 7799-2:2003. Slednja standarda nista prevedena v slovenščino.

Junija 2005, natančneje 15.6.2005, je izšla prenovljena izdaja prvega dela standarda BS 7799 pod imenom BS ISO/IEC 17799:2005 Informacijska tehnologija – Tehnike za zagotavljanje varnosti – Kodeks za upravljanje informacijske varnosti (*angl. Information technology – Security techniques – Code of practice for information security management;* glej BSI, 2005). Jeseni 2005, natančneje 18.10.2005, pa je izšla tudi posodobljena različica drugega dela standarda z novim imenom BS ISO/IEC 27001:2005 Informacijska tehnologija – Tehnike za zagotavljanje varnosti – Sistemi za upravljanje informacijske varnosti – Zahteve (*angl. Information technology - Security techniques - Information security management systems – Requirements;* glej BSI, 2005a).

3 Kratka predstavitev dosedanje verzije standarda BS 7799

Dosedanjo verzijo standarda BS 7799 sestavljata dva dela: BS ISO/IEC 17799:2000 in BS 7799-2:2002. Prvi del standarda obsega priporočila in obsežen nabor nadzorstev[1], ki predstavljajo najboljšo prakso na področju zagotavljanja informacijske varnosti. Ta del standarda lahko služi kot enotna referenčna točka za izbiro nadzorstev pri vzpostavitvi SUIV in oblikovanju krovne varnostne politike v organizaciji. Osnovni cilji nadzorstev, ki jih BS ISO/IEC 17799:2000 predlaga, so zagotavljanje:

- zaupnosti – občutljive informacije so dostopne samo pooblaščenim uporabnikom,
- celovitosti – informacije oziroma druge dobrine informacijskega sistema[2] niso bile nepooblaščeno spremenjene; informacije kakor tudi postopki za njihovo obdelavo so točni in popolni;
- razpoložljivosti – informacije oziroma druge dobrine informacijskega sistema so dostopne pooblaščenim uporabnikom kjerkoli in kadarkoli jih le-ti potrebujejo.

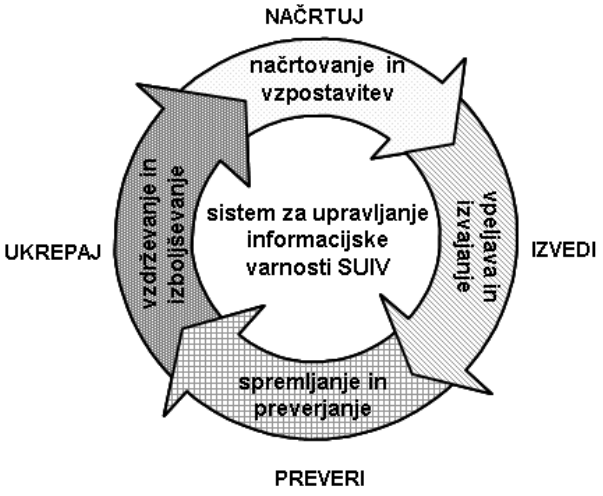
BS ISO/IEC 17799:2000 je odprt standard in je uporaben v vseh industrijskih panogah. Prenosljiv je v različna okolja in primeren za različne velikosti organizacij (tudi za zelo majhne organizacije, ki imajo do pet zaposlenih).

Drugi del standarda, BS 7799-2:2002, predstavlja zbirko lastnosti, katerim mora SUIV v organizaciji ustrezati, da je s tem standardom skladen. Organizacije, ki dosegajo določila, navedena v drugem delu standarda, lahko pridobijo certifikat skladnosti s standardom. Osnovni cilj vpeljave BS 7799 v organizacijo naj ne bi bil pridobitev samega certifikata skladnosti s standardom, temveč oblikovanje učinkovitega SUIV, ki se bo sposoben hitro in učinkovito prilagajati nenehnim spremembam poslovnega, informacijskega in zakonodajnega okolja.

Drugi del standarda BS 7799 temelji na ti. principu PDCA (**P**lan- Načrtuj, **D**o - Izvedi, **C**heck - Preveri, **A**ct – Ukrepaj), ki ga prikazuje slika 1.

[1] V slovenskih prevodih standarda BS 7799 se v pomenu angleškega izraza »control« uporablja izraz »nadzorstvo«. V ta namen bi se lahko uporabil tudi izraz »kontrola«.

[2] Izraz »dobrina informacijskega sistema« je slovenski prevod angleškega izraza »information security asset«, ki se uporablja v standardu BS 7799. V slovenskih prevodih standarda se v tem pomenu uporablja tudi termin »sredstvo informacijskega sistema«.



Slika 1: Princip PDCA, ki je osnova za vzpostavitev sistema za upravljanje informacijske varnosti SUIV v organizaciji (Zupan, 2005)

Princip PDCA pokriva vse faze delovanja SUIV, od njegove vzpostavitve do zrele faze delovanja. Podrobnejši opis posameznih faz delovanja SUIV najdemo v članku Zupan (2005a).

Uvedba standarda BS 7799 v organizacijo lahko prinese sami organizaciji mnoge koristi, kot npr. (glej tudi Zupan, 2005a):

- celovito pokrivanje področja zagotavljanja informacijske varnosti,
- neprestano izboljševanje nivoja informacijske varnosti na podlagi nepristranskega merjenja,
- zmanjševanje verjetnosti za uresničitev groženj varnosti in/ali ublažitev posledic, ki jih le-te lahko povzročijo,
- povečanje ugleda organizacije, zaupanja poslovnih partnerjev in strank,
- povečanje konkurenčnosti,
- pripravljenost na bodoče zahteve zakonodajalca ali poslovnih partnerjev.

Standard BS 7799 je združljiv z drugimi upravljalskimi standardi, kot so ISO 9001:2000 in ISO 14001:1996. BS 7799 pravzaprav predstavlja nadgradnjo teh standardov in predpostavlja enake postopke vpeljave standarda v organizacijo. V praksi je zato veliko enostavneje vpeljati BS 7799 v organizacije, ki že imajo vzpostavljenega katerega od navedenih standardov.

Podrobnejši opis standarda BS 7799 lahko najdemo v člankih Ključevšek (2002) in Zupan (2005a).

4 Nova izdaja standarda BS 7799

V drugi polovici leta 2005 je standard BS 7799 doživel prenovo. Prilagodil se je spremembam v poslovnih in drugih okoljih v zadnjih letih. Struktura standarda je preglednejša in razumljivejša, izrazoslovje pa je usklajeno z drugimi standardi in vodniki, ki obravnavajo informacijsko varnost: BS ISO/IEC 13335-1:2004[3], PD ISO/IEC TR 18044:2004[4] in PD ISO/IEC Guide 73:2002[5].

4.1 Spremembe v prvem delu standarda

Glavna področja sprememb v prvem delu standarda so naslednja:

- spremembe v strukturi standarda,
- dodana nova nadzorstva,
- nova struktura in format zapisa posameznega nadzorstva,
- dodatna pozornost, posvečena analizi tveganja,
- poseben poudarek na opredelitvi odgovornosti, povezanih z zagotavljanjem informacijske varnosti.

V nadaljevanju si bomo spremembe na posameznem področju boj podrobno ogledali.

Spremembe v strukturi standarda

Standarda BS ISO/IEC 17799:2000 in njegova prenovljena verzija se razlikujeta v številu poglavij, njihovemu oštevilčenju in poimenovanju kakor tudi v strukturi nekaterih podpoglavij. Na novo so dodana tri poglavja, od tega sta dve poglavji uvodni. Nekatera poglavja so preimenovana. Naslove poglavij (v angleškem in slovenskem jeziku) in njihovo oštevilčenje za obe izdaji standarda prikazuje tabela 1.

Preimenovala so se tudi nekatera podpoglavja in sama nadzorstva. Mnoga preimenovanja ne vplivajo bistveno na samo strukturo standarda, saj je vsebina v številnih primerih ostala popolnoma nespremenjena. Nekatera podpoglavja oziroma nadzorstva pa so v novi verziji standarda samo prerazporejena v druga poglavja oziroma podpoglavja.

Dodana nova nadzorstva

Precejšnje število nadzorstev iz ISO/IEC 17799:2000 ni v novi verziji doživelo nobenih sprememb. Devet obstoječih nadzorstev je izpuščenih, medtem ko je v prenovljeni verziji standarda 17 nadzorstev oblikovanih na novo. Skupno število nadzorstev je naraslo iz 127 na 135.

[3] BS ISO/IEC 13335-1:2004 Information technology. Security techniques. Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management
[4] PD ISO/IEC TR 18044:2004 Information technology. Security techniques. Information Security incident management
[5] PD ISO/IEC Guide 73:2002 Risk management. Vocabulary. Guidelines for use in standards

Tabela 1: Poglavja standardov BS ISO/IEC 17799:2000 in BS ISO/IEC 17799:2005

	Št.	Naslov poglavja	Naslov poglavja	Št.	
BS ISO/IEC 17799:2000	0.	Uvod Introduction	Uvod Introduction	0.	BS ISO/IEC 17799:2005
	1.	Namen standarda Scope	Namen standarda Scope	1.	
	2.	Pojmi in definicije Terms and definitions	Pojmi in definicije Terms and definitions	2.	
			Struktura standarda Structure of this standard	3.	
			Ocenjevanje in obravnavanje tveganj Risk assessment and treatment	4.	
	3.	Varnostna politika Security policy	Varnostna politika Security policy	5.	
	4.	Organizacijska varnost Organisational security	Organiziranje informacijske varnosti Organising information security	6.	
	5.	Razvrstitev in kontrola dobrin Asset classification and control	Ravnanje z dobrinami Asset management	7.	
	6.	Varovanje v zvezi z osebjem Personnel security	Varovanje v zvezi s človeškimi viri Human resources security	8.	
	7.	Fizično in okolno varovanje Physical and environmental security	Fizično in okolno varovanje Physical and environmental security	9.	
	8.	Upravljanje komunikacij in obratovanja Communications and operations management	Upravljanje komunikacij in obratovanja Communications and operations management	10.	
	9.	Obvladovanje dostopa Access control	Obvladovanje dostopa Access control	11.	
	10.	Razvoj in vzdrževanje sistema System development and maintenance	Nabava, razvoj in vzdrževanje informacijskega sistema Information systems acquisition, development and maintenance	12.	
			Ravnanje ob uresničitvi grožnje varnosti Information security incident management	13.	
	11.	Upravljanje neprekinjenega poslovanja Business continuity management	Upravljanje neprekinjenega poslovanja Business continuity management	14.	
	12.	Usklajenost Compliance	Usklajenost Compliance	15.	

Glavne vsebinske spremembe je zaslediti predvsem na naslednjih področjih:

Varnost storitev tretje stranke

Organizacije se vse pogosteje poslužujejo zunanjega izvajanja informacijskih storitev, zato je v prenovljeni verziji prvega dela standarda področju zagotavljanja varnosti storitev tretje stranke posvečeno več pozornosti. S to problematiko se ukvarjata podpoglavji 6.2 Zunanje stranke (*angl. External parties*) in 10.2 Upravljanje storitev tretje stranke (*angl. Third party service delivery management*). Podpoglavje 6.2 predstavlja razširitev obstoječega podpoglavja 4.3 Zunanje izvajanje (*angl. Outsourcing*) in zajema:

- opredelitev možnih tveganj pri poslovanju s tretjo stranko,
- opredelitev varnostnih zahtev pri sodelovanju s strankami,
- opredelitev varnostnih zahtev v pogodbah s tretjo stranko.

Varovanje v zvezi s človeškimi viri

Poleg tega, da se je poglavje, ki obravnava varovanje v zvezi s človeškimi viri, preimenovalo, je doživelo tudi precejšnjo mero sprememb. Razporeditev podpoglavij znotraj sedanjega poglavja 8. Varovanje v zvezi s človeškimi viri (*angl. Human resources security*) je popolnoma drugačna kakor razporeditev podpoglavij znotraj prejšnjega poglavja 6. Varovanje v zvezi z osebjem (*angl. Personnel Security*) v prejšnji izdaji prvega dela standarda.

V prenovljeni izdaji prvega dela standarda je cikel zaposlitve razdeljen na tri faze:

- zaposlitev še ni sklenjena,
- trajanje zaposlitve,
- prekinitev zaposlitve.

Navedena so različna nadzorstva, ki jih je v posamezni fazi cikla zaposlitve smiselno upoštevati.

Podpoglavje, ki obravnava aktivnosti pred sklenitvijo zaposlitve, zajema naslednja nadzorstva:

- opredelitev vlog in odgovornosti za doseganje informacijske varnosti,
- preverjanje ustreznosti kandidatov,
- uskladitev pogojev zaposlitve.

Podpoglavje, ki obravnava aktivnosti tekom trajanja zaposlitve, vključuje sledeča nadzorstva:

- upravljanje odgovornosti za doseganje informacijske varnosti,
- ozaveščanje, izobraževanje in usposabljanje zaposlenih na področju informacijske varnosti,
- disciplinski postopki v primeru kršenja določil.

Novost predstavljajo predvsem nadzorstva, ki jih je potrebno upoštevati ob prekinitvi zaposlitve:

- prekinitev obstoječih odgovornosti,
- vrnitev dobrin, ki so last organizacije in jih je posameznik tekom zaposlitve posedoval,
- preklic dostopnih pravic, ki so bile posamezniku tekom zaposlitve dodeljene.

Slednjim aktivnostim so organizacije do sedaj posvečale premalo pozornosti.

Odgovornost za dogajanje ob uresničitvi določene grožnje varnosti

Dodano je novo poglavje 13. Ravnanje ob uresničitvi grožnje varnosti (*angl. Information security incident management*[6]). Nekatera podpoglavja v poglavju 13 so prenesena iz stare verzije standarda, kjer je bilo področje ravnanja ob uresničitvi groženj varnosti obravnavano v podpoglavju 6.3 Odzivanje v primeru uresničitve grožnje varnosti ali motenj v delovanju sistema (*angl. Responding to security incidents and malfunctions*). Dodane so nove zahteve in priporočila glede spremljanja uresničitev posameznih groženj varnosti, poročanja o teh dogodkih in vpeljave mehanizmov za vodenje evidence o teh dogodkih. Poglavitno spremembo predstavlja zahteva po opredelitvi oseb, ki so odgovorne za ravnanje ob uresničitvi določene grožnje varnosti.

Ravnanje s tehnično ranljivostjo

Dodano je novo podpoglavje 12.6 Ravnanje s tehnično ranljivostjo (*angl. Technical vulnerability management*). V tem podpoglavju je poudarjena opredelitev odgovornosti za odkrivanje tehničnih ranljivosti informacijskega sistema, ocenjevanja tveganja zaradi obstoječih ranljivosti, uvedbe ustreznih popravkov v predvidenem časovnem roku, ipd.

Upravljanje komunikacij in obratovanja

Zaradi porasta uporabe elektronskega poslovanja je dodano novo podpoglavje 10.9 Storitve elektronskega poslovanja (*angl. Electronic commerce services*), ki zajema naslednja nadzorstva:

- elektronsko poslovanje,
- transakcije v realnem času,
- javno dostopne informacije.

Nadzorstva znotraj podpoglavja 10.9 omogočajo avtorizacijo udeležencev v komunikaciji, zagotavljanje zaupnosti prenosnih poti, zagotavljanje zasebnosti pri izvajanju storitev elektronskega poslovanja, ipd. Na novo je oblikovano tudi podpoglavje 10.10 Spremljanje (*angl. Monitoring*). To podpoglavje vključuje različna nadzorstva, ki omogočajo beleženje uporabe sistema z namenom odkritja nepooblaščenih aktivnosti v sistemu.

Fizična varnost

Znotraj področja fizične varnosti je zaslediti številna preimenovanja, prerazporejanja in prestrukturiranja podpoglavij. Dodano je podpoglavje 9.1.4 Zaščita zoper zunanje in okolne grožnje (*angl. Protecting against external and environmental threats*).

Nova struktura in format zapisa posameznega nadzorstva

Znatno spremembo predstavlja nova struktura in format zapisa nadzorstev. Zelo jasno so določene zahteve v okviru posameznega nadzorstva. Podani so tudi podrobni napotki za njegovo vpeljavo v organizacijo. Prenovljeno strukturo in format zapisa nadzorstev prikazuje slika 2.

Nadzorstvo
Definirana so natančna določila za doseganje cilja nadzorstva.
Napotki za vpeljavo nadzorstva
Podane so bolj podrobne informacije, ki služijo kot pomoč pri vpeljavi nadzorstva in doseganju cilja nadzorstva.
Dodatne informacije
Podane so dodatne informacije, ki jih je pri vpeljavi nadzorstva smiselno upoštevati (npr. zakonska določila, sklicevanje na druge standarde).

Slika 2: Prenovljena struktura in format zapisa nadzorstev v BS ISO/IEC 17799:2005

Dodatna pozornost, posvečena analizi tveganja

V novi verziji prvega dela standarda je dodano uvodno poglavje 4. Ocenjevanje in obravnavanje tveganj (*angl. Risk assessment and treatment*). V tem poglavju je poudarjena pomembnost postopkov opredelitve varnostnih tveganj, ki so za organizacijo relevantna, in odločitve organizacije glede obravnavanja ugotovljenih tveganj. Sklicevanja na to poglavje srečamo skozi ves standard, še posebej v okviru napotkov za vpeljavo posameznih nadzorstev (glej sliko 2). Same metodologije za izvedbo analize tve-

[6] V slovenskih prevodih standarda BS 7799 se v pomenu izraza »information security incident« uporablja izraz »varnostni incident«. Avtorici menita, da boljši prevod predstavlja izraz »uresničena grožnja varnosti«, ki ga v članku tudi uporabljata. Pod pojmom »grožnja varnosti« lahko razumemo kakršenkoli dogodek, ki lahko negativno vpliva na zaupnost, celovitost ali razpoložljivost informacij oziroma drugih dobrin informacijskega sistema.

ganja standard ne narekuje, temveč se sklicuje na standard ISO/IEC TR 13335-3[7].

Poseben poudarek na opredelitvi odgovornosti, povezanih z zagotavljanjem informacijske varnosti

Glavne zahteve za pravilno definiranje odgovornosti za zagotavljanje informacijske varnosti so opredeljene v podpoglavju 6.1.3 Dodeljevanje odgovornosti za informacijsko varnost (*angl. Allocation of information security responsibilities*). Poleg tega je za vsako izmed 39 področij, ki jih prvi del nove izdaje standarda obravnava, naveden način pravilnega definiranja odgovornosti za doseganje informacijske varnosti na posameznem področju.

4.2 Spremembe v drugem delu standarda

Drugi del prenovljenega standarda BS 7799 ima novo oznako ISO/IEC, ki ponazarja, da gre za mednarodni standard. Standard je zaradi večje prepoznavnosti dvojno poimenovan, BS7799-2:2005 in ISO/IEC 27001.

Namen sprememb v drugem delu standarda BS 7799 je naslednji:

- uvedba manjkajočih definicij in uskladitev izrazoslovja z obstoječimi dokumenti, ki obravnavajo informacijsko varnost,
- razjasnitev in dopolnitev obstoječih zahtev, ki se nanašajo na posamezne faze uvedbe SUIV v organizacijo (glej sliko 1),
- razširitev obstoječih zahtev glede oblikovanja potrebne dokumentacije in ravnanja s to dokumentacijo,
- zagotovitev rednega izvajanja interne presoje obstoječega SUIV,
- razumevanje in vpeljava postopkov za merjenje učinkovitosti obstoječega SUIV.
- razumevanje procesa ocenjevanja in obravnavanja relevantnih tveganj in pravilne uporabe metodologije za ocenjevanje tveganj.

V nadaljevanju bomo spremembe drugega dela standarda podrobno opisali.

Podpoglavje 1.2 Uporaba (*angl. Application*) je prestrukturirano. V prvem odstavku tega podpoglavja je poudarjeno, da pri vzpostavitvi SUIV ni sprejemljivo izključevanje poglavij, ki so označena z zaporednimi številkami od 4 do 8. Nekatera druga nadzorstva je mogoče izključiti pri določenih pogojih, ki so posebej navedeni v drugem odstavku podpoglavja 1.2.

Izvedene so spremembe poglavja 3. Pojmi in definicije (*angl. Terms and definitions*). V tem poglavju so dodane nove definicije iz vodnikov BS ISO/IEC 13335-1:2004, PD ISO/IEC TR 18044:2004 in PD ISO/IEC Guide 73:2002. Nekatere obstoječe definicije so spremenjene z namenom uskladitve z BS ISO/IEC 13335-1:2004. Spremenjeni sta definiciji 'Obravnavanje tveganj' (*angl. Risk Treatment*) in 'Izjava o uporabnosti' (*angl. Statement of applicability*). Z uvedbo sprememb so postale definicije bolj jasne.

Spremenjenih je več točk podpoglavja 4.2.1 Vzpostavitev SUIV (*angl. Establish the ISMS*).

- Spremenjena je točka a) 'Definirajte namen in obseg SUIV'. Dodana je zahteva, da morajo biti meje obsega SUIV jasno določene. Slednje omogoča opredelitev vseh izjem, ki so izven definiranega obsega in jih SUIV ne vključuje.
- Odstranjena je točka c) 'Definirajte sistematični pristop k analizi tveganja'. Dodana je nova točka, ki določa, da mora izbrana metoda analize tveganja omogočati večkratno ponovitev izvedbe. Rezultati posamezne izvedbe morajo biti med seboj primerljivi.
- Razširjena je točka g) 'Izberite nadzorstva za obravnavanje tveganj'. Razširitev je izvedena z namenom jasnejše obrazložitve obstoječih zahtev. Izbor relevantnih nadzorstev mora po novem upoštevati tako kriterije, ki določajo sprejemljiva tveganja[8], kakor tudi zakonodajne, pravne in pogodbene zahteve.

V podpoglavju 4.2.2 Vpeljava in izvedba SUIV (*angl. Implement and operate the ISMS*) je dodana točka d) 'Definirajte način merjenja učinkovitosti'. Vpeljana je dodatna zahteva glede vzpostavitve SUIV, ki določa, da morajo biti jasno definirana merila za ocenjevanje učinkovitosti nadzorstev ali skupin nadzorstev. Jasno mora biti tudi opredeljeno, kako naj se ta merila uporabijo.

Spremenjenih je več točk podpoglavja 4.2.3 Spremljanje in preverjanje SUIV (*angl. Monitor and review the ISMS*).

- Spremenjena je točka a) 'Izvedite postopke spremljanja in preverjanja z namenom izsledite neželenih dogodkov'. Dodano je pojasnilo k obstoječim zahtevam, ki naj bi olajšalo odkrivanje neželenih dogodkov in prepoznavanje njihovih indikatorjev.
- Dodana je točka c) 'Merite učinkovitost nadzorstev'. Točka predstavlja dodatek k obstoječim zahtevam, ki priporoča, naj se učinkovitost vpeljanih nadzorstev ustrezno ovrednoti. Na podlagi izmerjene učinkovitosti nadzorstev lahko ocenimo, ali so postavljene varnostne zahteve izpolnjene.
- Dodana je točka d) 'Ob upoštevanju spremembe učinkovitosti vpeljanih nadzorstev redno, v planiranih intervalih, preverjate dobljene ocene tveganj ter nivoje sprejemljivega in preostalega tveganja[9]'. Točka je dodana z namenom upoštevanja učinkovitosti že vpeljanih nadzorstev.

[7] ISO/IEC TR 13335-3 Guidelines for the Management of IT Security: Techniques for the management of IT Security

[8] Sprejemljivo tveganje je tveganje, ki ga v organizaciji zavestno sprejmejo brez vpeljave dodatnih nadzorstev. Nivo sprejemljivega tveganja določijo odgovorne osebe.

[9] Preostalo tveganje je tveganje, ki po vpeljavi ustreznega nadzorstva v organizaciji še vedno obstaja. Nivo preostalega tveganja naj ne bi presegel toleranc, ki jih določijo odgovorne osebe.

- Dodana je točka g) 'Osvežite varnostne načrte'. Točka je dodana z namenom upoštevanja ugotovitev, ki so rezultat spremljanja in preverjanja SUIV.
  Spremenjenih je več točk podpoglavja 4.3.1 Splošno (*angl. General*)
- V prvem odstavku sta dodana pojasnilo in dodatek k obstoječim zahtevam glede dokumentiranja. Dokumentacija naj vključuje zapise o odločitvah vodstva, ki zagotavljajo izsledljivost kritičnih aktivnosti in možnost ponovnega rekonstruiranja zabeleženih rezultatov.
- Dodan je nov odstavek, ki navaja, da mora biti organizacija sposobna prikazati povezave med izbranimi nadzorstvi, rezultati analize tveganja in postopki obravnavanja tveganj kakor tudi s cilji svojega SUIV.
- Dodana je točka d) 'Opis metodologije za oceno tveganja'. Dodano je pojasnilo k obstoječim zahtevam glede dokumentacije, ki narekuje, da mora biti metodologija za izvedbo ocene tveganja v dokumentaciji ustrezno opisana.

V podpoglavju 4.3.2 Nadzor nad dokumenti (*angl. Control of documents*) je dodana točka f) 'Zagotovite, da bo dokumentacija dostopna'. Točka predstavlja dodatno pojasnilo k obstoječim zahtevam za nadzor dokumentacije. Dokumentacija mora biti na voljo vsem, ki jo potrebujejo in so jim za dostop do dokumentacije dodeljene ustrezne dostopne pravice.

V podpoglavju 5.1 Zavezanost vodstva (*angl. Management comitment*) je dodana točka g) 'Zagotovite, da se interne revizije SUIV redno izvajajo'. Točka predstavlja dodatno pojasnilo k obstoječim zahtevam z namenom zagotovitve rednega izvajanja interne presoje SUIV.

V podpoglavju 7.2 Vhodni podatki za preverjanje (*angl. Review input*) je dodana točka f) 'Rezultati merjenja učinkovitosti'. Točka predstavlja dodatno pojasnilo k obstoječim zahtevam z namenom vključitve rezultatov merjenja učinkovitosti nadzorstev. Podpoglavje 'Vhodni podatki za preverjanje' je bilo v prejšnji verziji standarda uvrščeno pod zaporedno številko 6.2.

K podpoglavju 7.3 Rezultati preverjanja (*angl. Review output*) je dodanih več točk:

- Dodana je točka b) 'Osvežite načrt ocenjevanja in obravnavanja tveganj', ki predstavlja pojasnilo k obstoječim zahtevam glede pregledovanja rezultatov analize tveganja z namenom osvežitve načrta ocenjevanja in obravnavanja tveganj.
- Točka c) je dopolnjena. Ta točka se nanaša na spremembo postopkov, povezanih z zagotavljanjem informacijske varnosti, ki se odzivajo na notranje ali zunanje neželene dogodke, ki vplivajo na SUIV. Dopolnitev točke c) predstavlja dodatek k obstoječim zahtevam, saj po novem vključuje tudi pogodbene zahteve.
- Dodana je točka e) 'Izboljšave načina merjenja učinkovitosti nadzorstev'. Ta točka predstavlja dodatno pojasnilo k obstoječim zahtevam in vključuje izboljšanje načina merjenja učinkovitosti nadzorstev, ki so že vpeljana.

Podpoglavje 'Rezultati preverjanja' je bilo v prejšnji verziji drugega dela standarda uvrščeno pod zaporedno številko 6.3.

Spremenjen je dodatek A, ki je usklajen s spremembami standarda ISO/IEC 17799:2005. Obnovljena sta tudi dodatka B in C, dodatek D pa je v novi izdaji drugega dela standarda izpuščen.

5 Vpliv novosti na organizacije

Sedanje spremembe standarda BS 7799 še zdaleč niso tako obsežne kot so bile pri zadnjem prehodu standarda iz BS7799:1995 na BS 7799-1:2000 in BS7799-2:2002. Kljub temu pa so spremembe dovolj velike, da bodo morale organizacije kritično oceniti svoj SUIV in obstoječe varnostne politike ter jih uskladiti z novim standardom tako v vsebinskem kot v oblikovnem smislu (npr. uskladiti oštevilčenje in imenovanje poglavij). Strokovnjaki ocenjujejo vrednost investicije zaradi potrebnih sprememb obstoječega SUIV na 10 - 20% vrednosti celotne investicije za vzpostavitev SUIV, kar načeloma ne presega stroškov zaradi rednih vzdrževalnih aktivnosti, ki so sestavni del življenjskega cikla SUIV.

Organizacije, ki želijo v bližnji prihodnosti pridobiti certifikat skladnosti z novim standardom, morajo izvesti podrobno primerjavo med varovalnimi ukrepi, ki so v organizaciji že vpeljani, in nadzorstvi, ki jih predlaga nova izdaja standarda. V primeru odstopanj je potrebno izvesti ustrezno analizo tveganja. Na podlagi rezultatov analize tveganja se v organizaciji odločijo, katera od dodatnih nadzorstev je potrebno vpeljati.

Organizacije, ki bodo želele svoje poslovanje zasnovati na novi izdaji standarda BS 7799, bodo morale imeti jasno definirane vloge in odgovornosti, povezane z zagotavljanjem informacijske varnosti (npr. odgovornosti pri izvajanju delovnih nalog posameznika, odgovornosti glede nepooblaščenega razkritja občutljivih informacij, ipd.) kakor tudi sankcije v primeru neizvajanja le-teh. Rezultati raziskave RIV 2004 (glej Židanik idr., 2004), ki je bila izvedena v Sloveniji v letu 2004, kažejo, da z napisano varnostno politiko razpolaga približno tri četrtine organizacij, vendar imajo le redke med njimi formalno opredeljene tudi vloge in odgovornosti zaposlenih pri doseganju zastavljenih varnostnih ciljev.

V prihodnje bodo morale organizacije posvetiti večjo pozornost nadzorstvom, ki se nanašajo na zagotavljanje varnosti v procesu kadrovanja. Potrebno je vzpostaviti ustrezna nadzorstva za preverjanje osebja pred sklenitvijo zaposlitve, kakor tudi nadzorstva za zagotavljanje varnosti med samim trajanjem zaposlitve. Kar nekaj napora pa bo potrebno usmeriti tudi v obvladovanje postopkov ob zaključku zaposlitve. Bivši zaposleni so ljudje, ki vedo veliko o organizaciji. Mnogokrat pa predstavljajo ti ljudje tudi potencialno grožnjo za organizacijo, saj lahko s svojim znanjem in poznavanjem šibkih točk v poslovnem procesu povzročijo organizaciji znatno škodo. Nova izdaja standarda namenja zagotavljanju varnosti na področju človeških virov precejšnjo pozornost.

Organizacije, ki so že pridobile certifikat skladnosti z BS 7799-2:2002, bodo morale izvesti prehod na nov standard, saj je ob izdaji standarda BS ISO/IEC 27001 veljavnost standarda BS 7799-2:2002 potekla. Določeno naj bi bilo prehodno obdobje za izvedbo tega postopka, ki pa zaenkrat še ni natančno znano (glej tudi FAQ, 2005).

6 Kaj lahko pričakujemo v naslednjih letih?

V novi izdaji standarda so nekatera področja obravnavana bolj podrobno kot do sedaj, poleg tega pa so posamezna nadzorstva natančneje obrazložena. Z uvedbo teh sprememb je dosežena boljša preglednost in razumljivost standarda. Zaradi slednjega lahko pričakujemo, da bo uporaba standarda BS 7799 kot referenčnega priročnika za oblikovanje ustreznega programa za zagotavljanje informacijske varnosti v organizacijah še narasla.

Pričakovati je, da obstoječi standard v prihodnosti ne bo pokrival vseh potreb zaradi sprememb, ki so posledica na eni strani tehnološkega napredka, na drugi strani pa strožjih zahtev v poslovnem svetu. Praktiki že sedaj ugotavljajo določene pomanjkljivosti nove izdaje standarda in nekoherentnosti med posameznimi nadzorstvi znotraj standarda. Zaradi tega je v prihodnjih letih naravno pričakovati ponovne spremembe in dopolnitve standarda in s tem tudi potrebe po spremembi in dopolnjevanju že vzpostavljenih sistemov varovanja.

ISO/IEC 17799:2005 predvidoma predstavlja zadnjo objavljeno verzijo v seriji ISO/IEC 17799. Leta 2007 naj bi izšla različica pod novo serijo ISO/IEC 27002. V prihodnjih letih pa se pričakuje tudi izid naslednjih standardov oziroma priporočil[10]:

- ISO 27000 Temeljni principi in pojmovnik (*angl. Principles and vocabulary*),
- ISO 27003 Napotki za vzpostavitev sistema za upravljanje informacijske varnosti (*angl. Information security management system implementation gudelines*),
- ISO 27004 Merila sistema za upravljanje informacijske varnosti (*angl. Information security management system metrics and measurement*),
- ISO 27005 Obravnavanje tveganj, povezanih s sistemom za upravljanje informacijske varnosti (*angl. Information security management system risk management*).

Zaslediti je tudi napovedovanja, da bo v prihodnosti oblikovan tudi standard ISO 27006, ki naj bi pokrival področje neprekinjenega poslovanja[11].

7 Zaključek

Pri vzpostavitvi sistema varovanja in zaščite informacij se je smiselno in koristno opreti na uveljavljene standarde na področju informacijske varnosti. Eden najpomembnejših in najbolj razširjenih standardov na tem področju je BS 7799, ki predstavlja specifikacije za vzpostavitev, delovanje in vzdrževanje učinkovitega sistema za upravljanje informacijske varnosti SUIV v organizaciji.

V članku je podana kratka zgodovina standarda BS 7799 in opis dosedanje verzije standarda. Jedro članka predstavlja četrto poglavje, v katerem so strukturirano opisane glavne spremembe v novi izdaji obeh delov standarda, in sicer BS ISO/IEC 17799:2005 in BS ISO/IEC 27001:2005.

V prvem delu standarda, BS ISO/IEC 17799:2005, je glavne vsebinske spremembe zaslediti na naslednjih področjih: varnost storitev tretje stranke, ravnanje s tehnično ranljivostjo, upravljanje komunikacij in obratovanja, fizična varnost, varovanje v zvezi z človeškimi viri ter odgovornost za dogajanje ob uresničitvi groženj varnosti. Zadnji dve področji sta bili v prejšnji izdaji standarda precej pomanjkljivo obdelani, čeprav sta s stališča zagotavljanja ustreznega nivoja varnosti v organizaciji zelo pomembni. Novost predstavlja tudi nova struktura in format zapisa nadzorstev, ki jih standard predlaga. Ta sprememba je bistveno pripomogla k boljši preglednosti in razumljivosti standarda, zaradi česar je pričakovati, da bo priljubljenost standarda med slovenskimi organizacijami sedaj še narasla.

V novi izdaji drugega dela standarda, BS ISO/IEC 27001:2005, je zaslediti nekaj sprememb na področju izrazoslovja. Dodane so nekatere definicije, obstoječe definicije pa so usklajene z drugimi dokumenti, ki obravnavajo informacijsko varnost. Slednje spremembe pripomorejo k oblikovanju enotne terminologije na področju informacijske varnosti in k boljšemu razumevanju samih standardov med uporabniki. Razjasnjene in dopolnjene so obstoječe zahteve, ki se nanašajo na posamezno fazo uvedbe sistema za upravljanje informacijske varnosti SUIV. Prav tako je posvečeno več pozornosti zagotavljanju dokazov o delovanju takega sistema ter doslednemu merjenju njegove učinkovitosti. Postopki izvedbe posamezne faze pri oblikovanju sistema SUIV v organizaciji so tako bolj jasni in s tem tudi laže izvedljivi.

Skozi oba dela nove izdaje standarda je obilo pozornosti posvečeno tako analizi tveganja in postopku obravnavanja tveganj kakor tudi dodeljevanju vlog in odgovornosti za doseganje ustreznega nivoja informacijske varnosti. Učinkovito upravljanje s tveganji, ki so za organizacijo relevantna, predstavlja preliminarno aktivnost pri vzpostavitvi ustreznega sistema za upravljanje informacijske varnosti v vsaki organizaciji. Predpogoj za doseganje želenega nivoja varnosti pa so tudi jasno definirane odgovornosti ter sankcije v primeru neupoštevanja veljavnih določil. Menimo, da so organizacije v Sloveniji slednjima področjema posvečale premalo pozornosti. Pričakujemo, da se bo z uvedbo nove izdaje standarda zavest o pomembnosti teh področij v organizacijah dvignila in se bo stanje izboljšalo.

[10] Glej npr.: http://17799-news.the-hamster.com/interviews/interview9-audit.htm
[11] Glej npr.: http://www.iso27001security.com/html/iso27000.html

Naj zaključimo z ugotovitvijo, da enega perečih problemov v slovenskem prostoru zagotovo predstavlja neusklajenost izrazoslovja na področju informacijske varnosti. Izkazalo se je, da izrazoslovje, uporabljeno v slovenskih prevodih standarda BS 7799, variira glede na institucijo, ki je prevajanje izvedla. Slednje povzroča zmedo pri uporabnikih standardov, pri presojevalcih, ki certificirajo skladnost sistemov za upravljanje informacijske varnosti z ustreznimi standardi, kakor tudi v drugi strokovni javnosti. Oblikovanje ustreznega izrazoslovja je nedvomno področje, kjer bo v prihodnosti potrebno stremeti k priložnostim za izboljšavo in nujno zahteva pozornost s strani strokovne javnosti. Le na takšen način lahko dosežemo enotno poimenovanje v strokovni literaturi ter razumevanje med uporabniki te literature.

Literatura

BSI (2000). BS ISO/IEC 17799:2000 *Information technology – Code of practice for information security management.* British Standard Institution.

BSI (2002). BS 7799-2:2002 *Information security management systems-Specifications with guidance for use.* British Standard Institution.

BSI (2005). BS ISO/IEC 17799:2005 *Information technology – Security techniques – Code of practice for information security management*, British Standard Institution.

BSI (2005a). BS ISO/IEC 27001:2005 *Information technology - Security techniques - Information security management systems – Requirements*, British Standard Institution.

FAQ (2005). Frequently Asked Questions for BS ISO/IEC 27001:2005, http://www.bsi-global.com/ICT/Security/27001faq.xalter; November 2005.

Hermes Softlab (2002-2005). *Interno gradivo*, Hermes SoftLab d.d.

ISMS (2004). *ISMS J*ournal, **12** (5): 2 – 4.

Ključevšek, R. (2002). Na poti k vzorni varnosti informacij, *E-uprava za boljšo upravo, Zbornik referatov*, *INDO 2002*. Portorož 16-18 dec. 2002. Ljubljana: Vlada Republike Slovenije.

Zupan, L. (2005). Uporaba orodij pri vzpostavitvi sistema za upravljanje varovanja informacij (ISMS) v skladu s standardom BS7799:2-2002, *Informatika kot temelj povezovanja, Zbornik posvetovanja Dnevi slovenske informatike 2005.* Uredil: Novaković A. idr. Portorož 13-15 apr. 2005. Ljubljana: Slovensko društvo informatika.

Zupan, L. (2005a). Zahteve za uspešno vpeljavo standarda BS7799-2 za področje informacijske varnosti, *Uporabna informatika*, **13** (1): 37-50.

Židanik, M. idr. (2004). Raziskava o informacijski varnosti – RIV 2004, Inštitut za informacijsko varnost IZIV, Šempeter pri Gorici.

Lucija Zupan je leta 2000 diplomirala na Fakulteti za organizacijske vede Univerze v Mariboru s področja informacijske varnosti. Leta 2004 je na isti fakulteti magistrirala s področja analize in načrtovanja informacijskih sistemov. Zaposlena je v Hermes SoftLab d.d. kot svetovalka za informacijsko varnost in snovalka rešitev na področju upravljanja identitete in dostopov. Opravljen ima izpit za vodilnega presojevalca po standardu za informacijsko varnost ISO/IEC 17799/BS 7799-2:2002 in mednarodno priznan certifikat za vodjo informacijske varnosti - CISM (Certified Information Security Manager) ter ITIL (Foundation Certificate in IT Service Management). Je članica presojevalske ter izvedenske skupine s področja BS 7799 in aktivna članica urednikov spletnega slovarja, kjer vsebinsko pokriva področje informacijske varnosti. Redno spremlja trende na področju informacijske varnosti, sodeluje na domačih ter mednarodnih konferencah in objavlja prispevke v strokovnih publikacijah.

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 treh različnih predmetov na univerzitetnem programu in enega predmeta na visokošolskem strokovnem programu. Njeno raziskovalno delo obsega predvsem študij stohastičnih modelov zanesljivosti in razpoložljivosti kompleksnih sistemov ter zagotavljanja varnosti informacijskih sistemov. Je avtorica oziroma soavtorica več izvirnih znanstvenih člankov in referatov, objavljenih v domači in tuji strokovni literaturi.