Strokovno-znanstveni prispevek ■

Upravljanje z varnostjo informacij v zdravstvenih organizacijah

Drago Rudel

Izvleček. Po mnenju vzdrževalcev IS v slovenskih zdravstvenih organizacijah je stanje varovanja informacij neustrezno glede na pomembnost informacij, ki se hranijo in izmenjujejo. Z načrtovano uvedbo elektronskega zdravstvenega zapisa (elektronska zdravstvena kartoteka pacienta) in izmenjavo elektronskih podatkov med zdravstvenimi organizacijami bodo potrebe po zagotavljanju varnosti še večje. Avtor predlaga, da zdravstvene organizacije oblikujejo poenoteno celostno varnostno politiko po priporočilih standarda ISO17799 (BS7799:2002). Slovensko zdravstvo potrebuje ustrezen nadzorni organ, ki bo izdelal za zdravstvo specifična merila in preverjal skladnost organizacij z zahtevami standarda. Dolgoročno naj bi bilo zagotavljanje skladnosti pogoj za vključitev zdravstvene organizacije v načrtovani nacionalni sistem elektronske izmenjave podatkov.

Information security management in healthcare organizations in Slovenia

Abstract. According to opinion of IT managers in Slovene healthcare institutions security of medical data and information is insufficient when related to their importance. In the future an exchange of electronic healthcare records is planned what will further increase information security requirements. The author suggest that all healthcare organizations in Slovenia should adopt a unified and global security policy based on recommendation of the ISO17799 (BS7799:2002) standard. Accordingly, Slovenia would need a credible monitoring institution to prepare healthcare specific criteria and assess compliance of an institution with the standard requirements. Achieving the compliance should be an entry ticket for a planned national healthcare electronic data exchange system.

■ **Infor Med Slov**: 2005; 10(1): 1-8

Institucija avtorja: Medicinska fakulteta – Inštitut za biomedicinsko informatiko, Ljubljana; MKS Elektronski sistemi d.o.o., Ljubljana.

Kontaktna oseba: Drago Rudel, MKS d.o.o., Rožna dol. C.XVII/22b, 1000 Ljubljana. email: drago.rudel@mf.uni-lj.si.

Uvod

Zagotavljanje varnosti informacij postaja vse bolj pereč problem vseh modernih informacijskih sistemov (IS), torej tudi IS v zdravstvu. Grožnja varnosti IS v zdravstvu pomeni grožnjo poslanstvu, poslovnim ciljem in poslovnemu uspehu, delovanju zdravstvene institucije in posredno zdravju pacientov.

V zdravstvu nastaja velika količina zaupnih osebnih podatkov, ki so vezani na telesno, duševno in mentalno zdravje ljudi. Hranijo se na različnih nosilcih: na papirju, slikah, filmih, magnetnih trakovih, gibkih diskih, zgoščenkah, v glavah zaposlenih… Med uporabniki se prenašajo bodisi fizično, elektronsko in tudi kot govorjena beseda. V drugih poslovnih IS se potrebna stopnja varovanja podatkov pogosto ocenjuje z vrednostjo podatkov. Na nekaterih področjih lahko to vrednost ocenimo kot npr. izguba zaradi začasnega izpada delovanja IS podjetja, cena ponovne vzpostavitve baze podatkov po izgubi itd. V zdravstvenih organizacijah (ZO) je vrednost podatkov težko oceniti, saj imajo poleg objektivne tudi veliko subjektivno vrednost. Razumljivo je torej, da so v ZO zahteve glede varnosti pri beleženju, hranjenju in prenosu teh podatkov raznolike in velike.

Varovanje informacij v zdravstvu ni nov proces. Zdravstvene delavce veže k varovanju že etični kodeks[1], zakoni s področja zdravstvenega varstva[2] in zdravstvene dejavnosti[3], zakon o varstvu osebnih podatkov, zakon o zbirkah podatkov[4] ter različni predpisi. Za varnost elektronskih podatkov in informacij uvajajo ZO številne tehnološke rešitve kot npr. varovan dostopov do IS z gesli ter požarnimi zidovi, protivirusna zaščita, kodiranje podatkov ob prenosu...

Načrtovani razvoj informatike v zdravstvu v Sloveniji kaže, da se bodo zahteve glede varovanja informacij še povečale. Načrtujemo uvedbo elektronskega zdravstvenega zapisa[5] o pacientu. Vseboval bo večino podatkov, ki so se do sedaj nahajali v papirnatih kartotekah. Hkrati načrtujemo[6] izmenjevanje teh podatkov med ZO, kar pomeni, da bomo namesto ločenih IS ZO imeli povezan IS. Tak sistem bo bolj ranljiv kot posamezni IS, varnostna tveganja pa se bodo s tem še povečala. To bo povečalo zahteve za varno zajemanje, hranjenje in posredovanje podatkov med zdravstvenimi organizacijami. Sistem ne bo smel "puščati" nikjer, niti v tisti ZO, ki bodo imele najslabše razmere za varno delo s podatki oz. prenos podatkov.

Veliko skrbnikov IS v ZO navaja, da zgolj tehnološki ukrepi za zagotavljanje varnosti informacij niso zadostni in da je potreben celosten pristop k reševanju te problematike. Vsakodnevno delo jim potrjuje spoznanje, da menedžment ZO ne kaže pravega zanimanja za reševanje težav in prelaga reševanje problemov varovanja informacij nanje. Skrb za varnost je bolj ali manj serija "gasilskih" akcij, v katerih se poskrbi zgolj za tisto, kar že "gori".

Za izboljšanje varnostnih razmer v ZO pogosto ni pravega razumevanja in volje vodstva ZO. Pripravljenost za zagotavljanje večje stopnje varovanja informacij ne odseva dejstva, da so informacije v zdravstvu sploh pomembne. Vodstveni delavci se pogosto izgovarjajo, da za to ni zadostnih finančnih sredstev, čeprav je zagotavljanje varnosti povezano predvsem z organizacijo dela in ne s tehnologijo. V ZO prednostno namenjajo investicijska sredstva neposrednemu izvajanju zdravstvenih storitev, tehnične rešitve v informatiki pa običajno čakajo na ostanek investicijskih sredstev. Kaj rado pa se zgodi, da se najdejo investicijska sredstva, za katera pa se ne ve, kje bi bila najučinkovitejše vložena za povečanje varnosti, saj ZO običajno ne izdelajo ustreznih analiz in načrtov. Brez politike varovanja informacij ostajajo skrbniki IS v ZO nemočni, da bi celostno uredili varnostne razmere.

Velika stopnja sedanje in pričakovane ogroženosti informacij v zdravstvu kliče po ustreznem sistemskem pristopu, ki bi slonel na poenoteni politiki zagotavljanja ustrezne (dogovorjene) stopnje varnosti v vsaki ZO.

Standard ISO17799 za upravljanje z varnostjo v zdravstvenih organizacijah

V zadnjem času je tudi v Sloveniji dozorelo spoznanje, da lahko z upoštevanjem splošno veljavnih (mednarodnih) standardov najučinkoviteje uredimo določeno področje dejavnosti. Spoznanje sloni na pozitivnih izkušnjah organizacij, ki so uvedle bodisi standard za upravljanje s kakovostjo (ISO 9001), za upravljanje z okoljem (ISO 14000), ali za upravljanje z zdravjem zaposlenih (ISO 18000). Skupni imenovalec teh zvenečih standardov je "upravljanje". Upravljati z varnostjo informacij pomeni zagotoviti zaupnost, celovitost in dostopnost informacij. Ali lahko torej pričakujemo, da bomo tudi na področju zagotavljanja varnosti informacij v zdravstvu najhitreje in najučinkoviteje prišli do poenotene politike varovanja informacij s pomočjo mednarodnih standardov? Bomo sprejeli evropsko rešitev, to je standard za upravljanje z varnostjo informacij ISO17799 (BS7799)?

Standard ima dva dela: ISO/IEC 17799:2003 in BS7799-2:2003. Prvi del ISO/IEC17797 imenujemo tudi "kodeks varovanja informacij" in podaja primer dobre prakse. Temelji na spoznanju, da je potrebno varnost upravljati tako kot kakovost izdelkov in storitev. Določa enoten pristop k razvijanju, uporabi in nadzoru varnostnih meril, načel in postopkov. Osnovna poglavja prvega dela standarda so:

1. Politika varovanja informacij
2. Organiziranost delovanja
3. Razvrstitev in nadzor sredstev
4. Varovanje v zvezi z osebjem
5. Fizično in okoljsko varovanje
6. Upravljanje s komunikacijami in obratovanjem
7. Obvladovanje dostopa
8. Razvijanje in vzdrževanje sistema
9. Zagotavljanje neprekinjenega poslovanja
10. Usklajenost z veljavno zakonodajo

Drugi del standarda BS7799-2:20038 je specifikacija z napotki za uporabo ter zbirka lastnosti, ki jim IS organizacije mora zadostiti, če se organizacija želi certificirati po standardu. V nadaljevanju bomo, kjer ločitev ni potrebna, za oba dela uporabljali oznako "ISO17799".

Zanimanje za certificiranje po standardu BS7799-2 po svetu hitro raste. Sredi leta 2005 je bilo certificiranih okoli 1.800 podjetij oz. ustanov, od tega več kot polovico na Japonskem (967), v Evropi okoli 20% (360), največ v Veliki Britaniji (210) in le eno slovensko podjetje.[9]

V nasprotju z obstoječo prakso ZO v Sloveniji standard ISO17799 poudarja, da so za varnost informacij v vsaki organizaciji odgovorni vsi zaposleni in ne le skrbniki IS. Prav tako poudarja osebno zavezanost vodstva organizacije za izdelavo in uresničevanje vseh faz varnostne politike.

Standard nadalje zahteva, da je varnostna politika usklajena s poslovnimi cilji ZO. Zagotavljanje varnosti po standardu zato ni zgolj strošek, temveč pripomoček za doseganje ciljev ZO. Skozi to prizmo pomeni ogrožanje varnosti informacij tudi grožnjo doseganju poslovnih ciljev. Kot kažejo primeri iz drugih poslovnih sistemov (npr. izgubljeni potni listi pri pošiljanju prek DHL kurirske službe pomladi l.2003 v Sloveniji), lahko izguba, odtujitev ali zloraba podatkov/informacij hitro zmanjša ugled organizacije, ki upravlja s podatki.

Zagotavljanje varnosti po standardu ISO17799 pomeni tudi, da je varnost potrebno vrednotiti tudi s stališča zagotavljanja neprekinjenega delovnega procesa. Varnostni incidenti lahko upočasnijo, ali pa v celoti prekinejo delovni proces. Vrednost informacij je zato po standardu

ISO 17799 potrebno oceniti tudi v luči škode, ki bi jo povzročila uresničitev katere od groženj IS.

Varnost je torej potrebno upravljati kot druge poslovne procese. Zagotavljanje varnosti skladno s standardom ISO17799 je tako v organizacijah postalo upravljavski in ne zgolj tehnološki proces.

Z vsemi opisanimi lastnostmi bi bil standard ustrezna osnova tudi za zagotavljanje dogovorjene politike varovanja informacij v ZO v Sloveniji.

Standard varovanja informacij v Sloveniji

V Sloveniji smo standard za varovanje informacij že nekoliko okusili. Leta 1998 je takratni Urad za standardizacijo pri Ministrstvu za znanost in tehnologijo RS izdal osnutek standarda PSIST BS7799:1995,[10] ki pa ni dosegel statusa SIST standarda (PSIST = slovenski standard v pripravi, SIST = Slovenski standard). To je bil prevod britanskega standarda BS7799-1995, ki pa so ga Britanci medtem že preklicali. Standard pa je bil leta 2003 proglašen tudi za slovenski standard v dveh delih:

- **SIST ISO/IEC 17799:2003** - Informacijska tehnologija – Kodeks upravljanja varovanja informacij
- **SIST BS 7799-2:2003** – Sistemi za upravljanje varovanja informacij – Specifikacija z napotki za uporabo

Za uveljavljanje BS7799 standarda v Sloveniji je zelo pomembno dejstvo, da je Banka Slovenije sprejela PSIST BS-7799-1995 kot merilo zagotavljanja varnosti informacij v slovenskem bančništvu. Tako komercialni banki ne izda dovoljenja za delo, če njena politika varovanja podatkov ni usklajena standardom v pripravi PSIST BS7799.[11]

Aktivnosti na področju varovanja informacij v skladu s standardom ISO17799 tečejo še na drugih področjih. Tudi v državni upravi RS dobiva standard ISO17799 svoje mesto.[12] Nekdanji Center vlade za informatiko (CVI) je pripravil priporočila za pripravo informacijske varnostne politike,[13] ki so zasnovana na standardu ISO17799. Vlada RS je kot lastnik, upravljavec in uporabnik informacijskih sistemov v letu 2002 zadolžila vsa ministrstva in njihove organe ter upravne enote, da pripravijo svoje politike varovanja informacij ter pričnejo izvajati vse ukrepe v zvezi z varovanjem na podlagi priporočil CVI izdala vsem državnim organom navodilo, da do uvajajo upravljavski sistem za varovanje informacij, ki ga definira standard BS7799.

Kot je bilo že omenjeno, imamo zaenkrat v Sloveniji le eno certificirano podjetje po standardu BS7799.[9] Prav gotovo lahko v prihodnje pričakujemo povečano zanimanje za standard, saj bodo slovenska podjetja, ki sodelujejo s tujimi poslovnimi partnerji, prisiljena zagotoviti skladnosti s standardom, če bodo želela (še naprej) trgovati s tujimi poslovnimi partnerji.[14]

Povečane aktivnosti je mogoče zaslediti tudi pri institucijah oz. podjetjih, ki so povezane s certificiranjem. Slovenski inštitut za kakovost in meroslovje SIQ se pripravlja, da bo prevzel certificiranje organizacij za standard ISO17799, tako da bo njihov certifikat tudi mednarodno priznan. Slovenska svetovalna podjetja kot npr. Palsit,[15] Danesa,[16] Housing,[17] Kivi se pripravljajo na pomoč ustanovam v Sloveniji pri zagotavljanju varnosti po priporočilih standarda oz. certificiranju po tem standardu, zato je že mogoče rekrutirati neodvisne svetovalce za področje informacijske varnosti.

Tudi pri zagotavljanju varnosti informacij v zdravstvu ob pomoči standarda ISO17799 v Sloveniji ne bomo orali ledine, niti ne bomo med zadnjimi v Evropi, ki bodo pristopili k sistemskemu reševanju problema s pomočjo omenjenega standarda.

Standard varovanja informacij v zdravstvu v tujini

Naštejmo le nekaj primerov prizadevanj za uvedbo tega standarda v zdravstvu:

Svet Evropske unije je skupaj z Evropsko komisijo izdelal strategijo na področju informacijske varnosti, ki med drugim vključuje ISO 17799 v upravljanje varnosti informacij v privatnih in javnih organizacijah.[12]

Pri Evropskem komiteju za standardizacijo CEN delujeta v okviru tehničnega komiteja CEN/TC251 "Zdravstvena informatika" dve delovni skupini (WG3 in WG4), ki se med drugim ukvarjata tudi z aktivnostmi, da se ISO17799 priporoči za uporabo v zdravstveni informatiki.[18] Pri tem so aktivni tako Velika Britanija, Nizozemska, Avstrija, Nemčija in Švedska kot tudi Kanada, Japonska. Dejstvo je, da v posameznih državah ni posebnih certifikacijskih organov za področje zdravstva.

Delovna skupina pri "IMIA – International Medical Informatics Society" "WG4/Health - Informatics/Security" je leta 2001 pripravila predlog standarda za sistem javnih ključev v zdravstvu (ISO/DTS 17090). V predlogu so predpostavili, da bodo vsi uporabniki tega sistema v zdravstvu predhodno poskrbeli za varnost IS po standardu ISO17799.

V Veliki Britaniji je krovna zdravstvena organizacija NHS-National Health Service na zahtevo vlade opustila svoj prvotni sistem zagotavljanja varnosti informacij in vsem zdravstvenim organizacijam naložila, da za varnost informacij poskrbijo v skladu s standardom ISO/IEC17799:2000. Cilj NHS je, da se v nekaj letih vse zdravstvene organizacije v sistemu NHS (tudi splošni zdravniki), ki želijo imeti dostop do podatkov o pacientih v elektronski obliki (elektronski zdravstveni zapis) certificirajo po standardu BS7799-2. Trenutno izvajajo dvofazne pilotne projekte uvajanja ISO/IEC17799:2000v več pokrajinah Velike Britanije.[19] NHS organizira in sponzorira izvajanje seminarjev po UK za top NHS menedžment, da zagotovi podporo uvedbi standarda. Vzporedno izvajajo informacijsko-edukacijsko dejavnost ter aktivnosti za pridobitev mnenja ZO, na državnem nivoju pa ustanavljajo tudi nadzorno institucijo. Vsaka organizacija mora imeti tudi nadzorni organ za varovanje informacij o pacientu t.i. "Caldicott Guardian", ki ga običajno predstavlja starejši zdravstveni delavec. Prehod bo skupen za vse NHS organizacije zato, da bo pristop do varovanja informacij cenejši in učinkovitejši.

Certificiranje ali zagotavljanje skladnosti z ISO17799 v zdravstvene organizacije v Sloveniji?

Zagotavljanje skladnosti s standardom ISO17799 v ZO je potrebno gledati v luči urejanja razmer na področju upravljanja zdravstvenih IS v Sloveniji. Perspektivo je nakazal vladni projekt "*Projekt razvoja upravljanja sistema zdravstvenega varstva - PRUSZV*",[6] ki je predvidel ustanovitev Centra za informatiko v zdravstvu, ki bi med drugim tudi pripravljal ustrezne politike in standarde za zdravstveno informatiko.

Prvo vprašanje glede zagotavljanja varnosti informacij v povezanem slovenskem zdravstvenem IS je, ali je potrebno, da bi se ZO certificirale po standardu oz. ali bi bilo dovolj, da bi zagotovile skladnost in morda kako drugače, brez certificiranja, potrdile zagotavljanje varnosti informacij skladno s standardom? Certificiranje ZO v Sloveniji ob podpori domačih strokovnjakov bi teoretično bilo mogoče, vendar je vprašljiv njegov smisel. Postopek je zahteven, dolgotrajen ter drag. Visoki so tako stroški pridobitve certifikata kot tudi stroški vzdrževanja njegove veljavnosti.

Verjetno bo za slovenske ZO bolj smotrno, če bi uporabile standard ISO17799 zgolj kot referenčno nivo, ki ga morajo v bližnji prihodnosti doseči vse

ZO. Izpolnjevanje priporočil standarda in uporaba ustreznih mehanizmov, ki jih predvideva standard, bi pomenila zagotavljanje zadostne mere varnosti informacij v ZO. Vsi stroški, ki bi pri tem nastajali, bi bili vezani neposredno na urejanje razmer v ZO in ustvarjanje takšnih pogojev dela v ustanovi, ki bi zagotavljali želeno (in za ZO priporočeno) stopnjo varnosti informacij. Zgolj zagotavljanje skladnosti s standardom ne zahteva plačevanje pristojbin certifikatskim institucijam.

Zaradi verodostojnosti "lastno ugotovljene skladnosti" pa bi bilo potrebno, da bi neodvisni organ s področja informatike v zdravstvu potrdil izpolnjevanje priporočil standarda v ZO. Takšen organ, ki ga sedaj nimamo, se bo moral formirati tudi zaradi drugih potreb v informatike v zdravstvu, bi lahko bil del načrtovanega Centra za informatiko v zdravstvu. Zaradi specifičnosti zdravstvenega področja bi moral ta organ pripraviti merila ocenjevanja, vrednotenja, nadzora itd. za varnost informacij. Standard ISO17799 sam namreč ne daje konkretnih meril za vrednotenje v zdravstvu, zato bo potrebno merila doreči na nacionalnem nivoju. Prav tako bo potrebno določiti ustrezne ponderje, s pomočjo katerih bo mogoče kvantitativno vrednotiti stanje ogroženosti informacij v zdravstveni ustanovi. Za področje zdravstva bo potrebno določiti tudi, kaj so sprejemljivi sistemski ukrepi za konkretne probleme s področja varnosti informacij. Takšno institucijo potrebujemo torej še preden bo lahko prva ZO vstopila v postopek potrjevanja skladnosti s standardom.

S stališča odgovornosti ob morebitni zlorabi, poškodovanju ali nedostopnosti podatkov ostaja za to odgovorna sama ZO. Organizacija, ki bi bodisi certificirala ZO oz. preverila njeno skladnost, pri tem ne nosi nobene odgovornosti, saj izdata le dokument, ki potrjuje, da se v preverjeni organizaciji prizadevajo za ohranitev zaupnosti, celovitosti in razpoložljivosti informacij.

Poslovni razlogi za zagotavljanje skladnosti

Varovanje informacij je pomembna aktivnost vsake sodobne organizacije. Razumljivo je, da si tudi vodstvo ZO prizadeva, da informacijski tokovi delujejo in da pri tem niso ogroženi poslovni interesi. Po izkušnjah podjetij/organizacij, ki so uvedle enega od standardov kakovosti (npr. ISO 9001, ISO 14000 ali ISO 18000), je proces uvajanja in zagotavljanja skladnosti z določili standarda pomenil bistveno spremembo v delovnih procesih. Podoben korak pomeni tudi zagotavljanje sprejemljive informacijske varnosti z uporabo preverjenega modela, ki ga daje mednarodni standard ISO17799. Upravljanje z varnostjo informacij v podjetju oz. ustanovi postane dokumentiran vodstven proces, kar pomeni, da je varnost informacij mogoče poslej upravljati.

Za menedžment ZO bodo pomembni pozitivni učinki take strateške spremembe. V nadaljevanju je navedenih nekaj možnih neposrednih in posrednih koristi za ZO, ki opravičujejo naložbo v sistem upravljanje z varnostjo informacij:

1. izboljšano varovanje pacientovih in lastnih informacij kot lastnine
2. poenostavljeno poslovanje z notranjimi (pacienti, dobavitelji, lekarne…) in tujimi poslovnimi partnerji (tuji pacienti, naši pacienti na tujem)
3. povečan ugled in zaupanje pri pacientih, poslovnih partnerjih in v javnosti
4. obvladovanje poslovnih tveganj, ki jih prinašajo varnostni incidenti
5. zmanjševanje učinkov varnostnih incidentov ter enostavnejše zagotavljanje neprekinjenega delovnega procesa
6. finančne koristi zaradi zmanjšane posredne škode ob varnostnem incidentu

7. učinkovitejše investiranje v opremo in postopke za zagotavljanje večje informacijske varnosti

8. izpolnjevanje zakonsko naloženih obveznosti in zahtev EU glede varovanja podatkov/informacij

Eden izmed razlogov je gotovo tudi zagotavljanje ustrezne elektronske komunikacije med ZO in organizacijami, ki bi bile uradno certificirane npr. farmacevtske organizacije, drugi dobavitelji, državna uprava. Pričakovati je, da bodo ZO v bodoče morale zagotavljati ustrezno stopnjo varovanja informacij zaradi povezovanja z zunanjimi organizacijami. Medsebojno zaupanje je pogoj za vzpostavitev komuniciranja med IS organizacij. To zaupanje najlaže vzpostavimo, če so organizacije med seboj primerljive glede varnostne politike, pogoj za to pa je podrejanje istim varnostnim standardom.

Koraki do zagotovljene skladnosti s standardom ISO17799

Koraki do želene varnosti informacij v slovenskem zdravstvu z zagotavljanjem skladnosti s standardom ISO17799 v ZO bi bili naslednji:

1. zagotoviti podporo Ministrstva za zdravje celotnemu procesu upravljanja z varnostjo

2. pridobiti podporo projektu s strani strokovnih institucij s področja zdravstvene informatike

3. v posameznih ZO bi morala vodstva sprejeti odločitev, da želijo zagotoviti varnost informacij v skladu s tem standardom

4. doseči bi morali konsenz mnenj in interesov ZO v strokovnih združenjih, v katera so vključene ZO

5. ZO morajo zagotoviti finančna sredstva za projekt

6. zagon projekta

7. močna podpora vodstva ZO notranjim izvajalcem projekta

8. sodelovanje z zunanjimi strokovnjaki

Za spremembo stanja na področju varnosti informacij v ZO bo pomembna tudi ustrezna kadrovska politika. Ker bo zagotavljanje skladnosti trajen multidisciplinarni projekt, ki bo vključeval vsa področja delovanja ZO, bodo ključno vlogo nosili izkušeni notranji strokovnjaki v sodelovanju z zunanjimi sodelavci. Zato bo morala ZO zagotoviti lastne usposobljene kadre, ki bodo s pomočjo zunanjih sodelavcev pripravili politiko varovanja informacij ter jo nato sami implementirali in izboljševali.

Seveda lahko pričakujemo, da bomo pri izvajanju postopkov zagotavljanja skladnosti s standardom naleteli na odpor znotraj ZO. Kot kažejo izkušnje pri uvajanju drugih standardov na področju gospodarstva, so ovire organizacijske, finančne in človeške, ne glede na to, kateri standard se uvaja. Vsak prinaša spremembe za zaposlene, ki lahko pomenijo večje zahteve do posameznika, s tem pa "poslabšanje ugodja" na delovnem mestu.

Zaključek

Za slovensko zdravstvo je korak k zagotavljanju večje varnosti informacij nujen. Najučinkovitejša pot bo z zagotavljanjem skladnosti po merilih standarda kot je ISO17799.

V strokovnih krogih informatikov v zdravstvu skoraj nihče več ne dvomi o ustreznosti tega standarda za upravljanje z varnostjo v ZO, le o tem, kako se tega lotiti, so mnenja še deljena.

Upravljanje z varnostjo informacij bo za vsako ZO trajen proces, ki se podobno kot procesi

zagotavljanja kakovosti izdelkov v gospodarstvu, nikoli ne konča.

Literatura

1. Zdravniška zbornica Slovenije: Kodeks medicinske deontologije. http://www.zzs-mcs.si/kodeks, 1997.
2. Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju. UL RS 9/92 in spremembe.
3. Zakon o zdravstveni dejavnosti. UL RS 9/92 in spremembe.
4. Zakon o zbirkah podatkov s področja zdravstvenega varstva. UL RS 5/00.
5. Widenet: Prorec.si. http://www.drustvo-sdmi.si, 2005.
6. Vlada RS: Projekt razvoja upravljanja sistema zdravstvenega varstva. http://www2.gov.si/mz/hsmp/hsmp.nsf.
7. British Standard Institute: Information technology - Code of practice for information security management. BS ISO/IEC 17799:2000 (BS7799-1:2000).
8. British Standard Institute: Information Security Management System - Specifications with guidance for use. BS7799-2:2002.
9. Andrejaš B: Uvajanje sistema vodenja varovanja informacij v skladu s standardom BS 7799-2:2002 in certificiranje. Infosec, Nova Gorica, 2003.
10. SIST Standard. PSIST BS7799. SIST 1998.
11. UL RS 52/00, 6982.
12. Hajtnik T: Zahteve Evropske unije in državne uprave za uvajanje ISO 17799 standarda. Palsit BS 7799 konferenca, Postojna, september 2004.
13. Hajtnik T: Priporočila za pripravo informacijske varnostne politike. CVI, junij 2002.
14. Ključevšek R: Varnost informacij po novem. Monitor. 2003; 13: 1. Supl. SISTEMI 2003, 14.
15. Palsit d.o.o. http://www.palsit.com/, 2005.
16. Danesa d.o.o. BS7799. http://www.bs-7799.org, 2005.
17. Housing d.o.o. http://www.housing.si, 2005.
18. CEN/TC Health Informatics. http://www.centc251.org/TCMeet/doclist/TCdoc04/N04-044WGIII-Report-Berlin-2004.pdf, 2004.
19. Sunderland NHS Health Portal. http://www.sunderland.nhs.uk/security/top, 2005.