UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VAROVANJE INFORMACIJ SKLADNO S STANDARDOM BS 7799

Ljubljana, maj 2005 SAŠO RAKOVEC

IZJAVA

Študent Sašo Rakovec izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Mira Gradišarja, in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 2. 5. 2005

Podpis:

KAZALO

PRILOGE

KAZALO TABEL

PRILOGE

KAZALO SLIK

PRILOGE

1. UVOD

1.1. Problematika magistrskega dela

Živimo v času, ko poslovanje brez podpore informacijskih sredstev ni več mogoče. Tudi sicer nas informacijski sistemi spremljajo na vsakem koraku in brez njih si življenje težko predstavljamo. Zaradi vse večje odvisnosti od informacijskih sistemov in od pravih informacij ter vse večje globalizacije poslovanja je toliko pomembnejša njihova zaupnost, razpoložljivost in celovitost [BS ISO/IEC TR 13335 Part 5, 2001]. Vse premalo se zavedamo nevarnosti, ki so ji naši informacijski sistemi vsakodnevno podvrženi. V velikem porastu je računalniški kriminal, virusi so postali že vsakdanjost, pa tudi odpovedi strojne in programske opreme ne gre zanemariti.

Vodilni v organizaciji se teh problemov največkrat sploh ne zavedajo in tako se z informacijsko varnostjo v glavnem ukvarjajo tehniki. Varnost, ki jo lahko dosežemo s tehničnimi sredstvi, je omejena in jo je zato potrebno ustrezno upravljati. [Hajtnik, 2004]. Informacijska varnost je predvsem upravljavska funkcija. Potrebna je jasna strategija, za katero mora stati varnostna politika in ustrezne procedure [www.palsit.com]. Vedno je potrebno najprej ugotoviti, katere stvari so za uspešno delovanje organizacije pomembne. Nato skušamo ugotoviti njihove ranljivosti, oziroma nevarnosti, ki jim grozijo. Temu postopku pravimo analiza tveganja. Iz teh podatkov ugotovimo, katere informacije in informacijska sredstva je potrebno varovati. Vendar pa tudi varovanje za vsako ceno ni ekonomsko upravičeno. Vodstvo organizacije mora zato postaviti sprejemljivo stopnjo tveganja. Nato pa začnemo s postopkom upravljanja s tveganji, v katerem lahko tveganja s pomočjo ukrepov zmanjšamo, se jim izognemo, prenesemo na druge ali pa jih sprejmemo.

Najboljša osnova za upravljanje varovanja informacij je standard BS 7799, ki je leta 2000 postal tudi ISO 17799. Ta standard določa zahteve za vzpostavljanje, vpeljevanje, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje dokumentacije sistema za upravljanje varovanja informacij v okviru celotnega poslovnega tveganja organizacije.
Standard BS 7799 nudi vrsto splošnih kontrol, ki temeljijo na najboljši praksi pri varovanju informacij. Njegov namen je služiti kot enotna referenca pri določanju različnih kontrol, ki so potrebne v različnih situacijah, kjer se uporabljajo informacijski sistemi, tako v industriji, državni upravi, bančništvu in trgovini [BS ISO/IEC 17799:2000, 2000].
V postopku upravljanja s tveganji se organizacije izmed naštetih možnosti največkrat odločajo ravno za zmanjševanje tveganj. Standard BS 7799 predpisuje 127 kontrol, s pomočjo katerih tveganja zmanjšujemo na sprejemljivo raven.
V začetni fazi upravljanja z informacijsko varnostjo je smiselno izvesti tudi analizo odstopanj. Tu ugotavljamo odstopanje trenutnega stanja informacijske varnosti od standarda BS 7799. Analizo odstopanja izvedemo s pomočjo vprašalnikov, ki nam na koncu dajo končno oceno odstopanja oziroma skladnosti. S tem postopkom dokaj hitro ugotovimo, kje se organizacija nahaja oziroma, kje bo še posebej potrebno angažiranje.

Za vpeljavo, delovanje in nadzor informacijske varnosti je v organizaciji smiselno vpeljati sistem za upravljanje varovanja informacij (SUVI).
Ta sistem deluje po principu Demingovega kroga stalnega izboljševanja, ki vključuje načrtovanje, uvedbo, kontrolo in ukrepanje. Zavedati se je potrebno, da SUVI ni cilj, pač pa pot, ki se nikoli ne zaključi. Neprestano se spreminjajo okolje, ranljivost informacijskih sistemov ter grožnje. Prav tako se stalno spreminjata strojna in programska oprema, pa tudi zaposleni, ki z njo upravljajo.

V okviru sistema za upravljanje varovanja informacij morajo biti natančno določene tudi vloge in odgovornosti. Tako mora pravo težo sistemu prisoditi vodstvo organizacije, postaviti je treba osebo, ki celoten SUVI vodi, skupino pristojnih ljudi, ki odobravajo odločitve, skupino, ki upoštevanje pravil preverja. Vsi zaposleni pa morajo ta pravila upoštevati.
Vzpostaviti je potrebno tudi sistem dokumentacije, kajti vsa pravila uporabe informacij in informacijskih sredstev je potrebno formalizirati.
Ne smemo pa pozabiti na stalno izobraževanje, saj le tako lahko od zaposlenih pričakujemo upoštevanje predpisanih pravil.

1.2. Namen in cilj magistrskega dela

Zavedanje o pomembnosti varovanja informacijskih sistemov ima dokaj kratko zgodovino. V Sloveniji se s to problematiko ukvarjamo šele zadnjih nekaj let. Zato je namen magistrskega dela podrobneje predstaviti samo področje informacijske varnosti ter ozavestiti vodstveno strukturo, da je uvedba sistema za upravljanje varovanja informacij nujna.

Cilj magistrskega dela je torej v luči standarda BS 7799 analizirati stanje informacijske varnosti v organizaciji (analiza odstopanja) in navesti predloge za izboljšanje stanja.
Cilj naloge je tudi predstaviti načrt uvedbe sistema za upravljanje varovanja informacij vodstvu organizacije.

1.3. Metodološki pristop

Pri izdelavi magistrskega dela sem uporabil naslednje metode preučevanja:

1. teoretično raziskovanje, ki zajema zbiranje in urejanje obstoječe literature in znanj,
2. deskriptivno metodo,
3. študijo primera.

Iz zbrane literature in pridobljenih znanj sem najprej podrobneje predstavil področje in namen varovanja informacij ter standard BS 7799.
Nato sem se posluževal študije primera, kjer sem analiziral trenutno stanje v organizaciji in podal predloge za izboljšavo.

1.4. Omejitve magistrskega dela

Do analize stanja informacijskega sistema in predlogov za izboljšave, ki so predmet študijskega primera, ni prišlo po naročilu vodstva organizacije, pač pa v dogovoru z vodjem službe za informatiko, na pobudo avtorja. Čeprav se tako analiza kot tudi predlogi nanašajo na opazovano organizacijo, so lahko v veliko pomoč vsem srednje velikim in velikim slovenskim organizacijam.
Praktični del naloge je omejen zgolj na analizo odstopanj, kar je le del celotnega sistema za upravljanje varovanja informacij. Ostale teme so obdelane le na teoretičnem nivoju.

1.5. Struktura magistrskega dela

Magistrsko delo je razdeljeno na devet poglavij. Od tega uvod ter literatura in viri niso vsebinski del naloge. V drugem poglavju je natančneje razloženo področje informacijske varnosti in zakaj je le-to sploh potrebno. V tretjem poglavju je opisan standard BS 7799 in smernice za njegovo uporabo. Četrto poglavje opisuje celoten sistem upravljanja varovana informacij (SUVI). Peto poglavju predstavlja organizacijo, v kateri sem opravil študijo primera. V šestem poglavju je po točkah standarda BS 7799 narejena analiza odstopanja, in predlogi izboljšav omenjene organizacije. Sedmo, sklepno poglavje, povzema vsebino ter pomembnejše ugotovitve celotne naloge.

2. VAROVANJE INFORMACIJ

2.1. Kaj je varovanje informacij

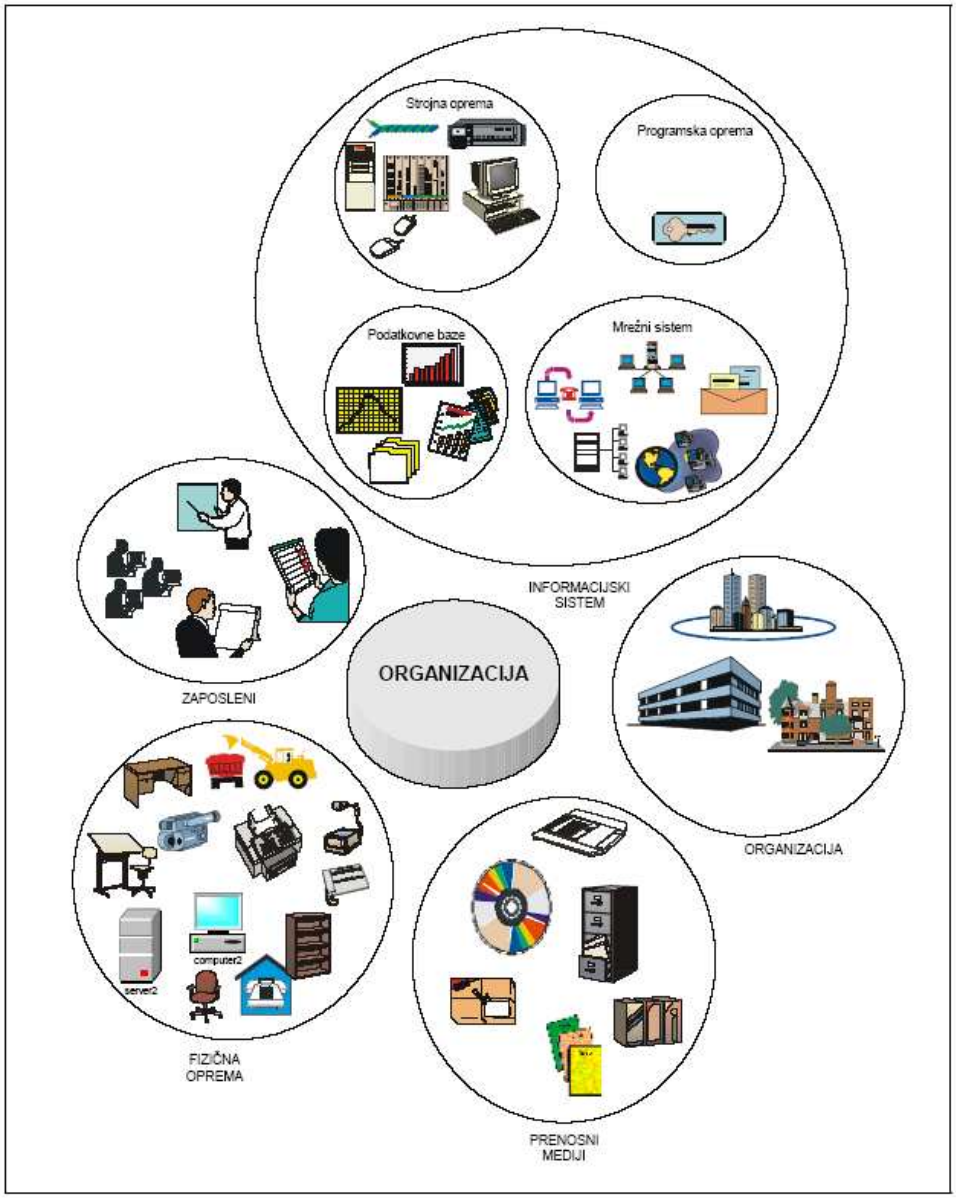
Informacije so poleg kapitala, ljudi, naravnih virov in znanja čedalje pomembnejši vir podjetja. So sredstva z določeno vrednostjo, ki jih je potrebno ustrezno zaščititi. Varovanje informacij le-te ščiti pred različnimi nevarnostmi, z namenom zagotoviti varno in neprekinjeno poslovanje ter omejiti poslovno škodo na najmanjšo možno raven.
Informacije se lahko pojavljajo v različnih oblikah. Lahko so zapisane na papir, shranjene na elektronski medij, poslane po pošti, lahko pa zgolj izgovorjene v pogovoru. Neodvisno od oblike in sredstva, po katerem so prenesene, jih je potrebno primerno varovati [emea.bsi-global.com].

Pojem varovanja informacij zajema predvsem zagotavljanje naslednjih treh osnovnih načel:

- **neoporečnost**: varovanje točnosti in popolnosti informacij ter računalniške programske opreme,
- **zaupnost**: zagotavljanje, da so informacije dostopne samo pooblaščenim osebam,
- **razpoložljivost**: zagotavljanje, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom, kadar jih potrebujejo.

Varovanje informacij ima tako nalogo varovati vse pomembne informacije in sredstva, ki so pomembna za nemoteno delovanje organizacije. Katere pa so te informacije in sredstva (slika 1) pa je potrebno ugotoviti s popisom sredstev. Nato izvedemo analizo tveganj. Na osnovi te analize lahko pripravimo ukrepe za zmanjševanje tveganj in pa nadzor njihove uporabe. Vse ukrepe (načine dela, postopke, organizacijsko strukturo in funkcije programske opreme) nato zapišemo v varnostno politiko, ki za vsako posamezno področje ali problem natančno določa, kako ukrepati. Z vsebino varnostne politike morajo biti seznanjeni vsi zaposleni.

Slika 1: Spekter virov in sredstev, primernih za varovanje



Vir: Janežič, 2004

Varovanje informacij je pot, ki se nikoli ne zaključi. Z doseženim ne smemo biti nikoli zadovoljni, pač pa moramo stalno stremeti k izboljšanju. Tudi razmere, v katerih nek informacijski sistem deluje, se stalno spreminjajo.
Zavedati se moramo, da popolne varnosti ni in da je v veliki meri odvisna od tega, kaj si organizacija lahko privošči. Vsekakor pa mora varovanje informacij izhajati iz ciljev organizacije.

2.2. Zakaj je varovanje informacij pomembno

Informacije ter podporni procesi, sistemi in omrežja so pomembna poslovna sredstva. Neoporečnost, zaupnost in razpoložljivost informacij lahko igrajo bistveno vlogo pri ohranjanju konkurenčnosti, denarnih tokov, dobičkonosnosti, usklajenosti z zakonom ter pri ohranjanju komercialne podobe [BS/IEC 17799:2000].
Neustavljiva rast računalništva in komunikacij sili podjetja v vse večjo odvisnost od informacijskih sistemov. Medtem ko so informacije vse lažje dosegljive vedno večjemu številu ljudi, se vzporedno povečujejo tudi možnosti zlorab (računalniške prevare, vohunstvo, sabotaže, zlonamerna koda …).
Tudi odpovedi sistemov in napake v programih lahko ogrozijo delovanje in celo obstoj podjetja.
Poleg tega so v zadnjem času najpogostejši vzrok uvedbe sistema za varovanje informacij ravno zahteve revizij, vladnih agencij in centralne banke. Pričakovati je, da bodo v kratkem to postale tudi zahteve poslovnih partnerjev.
Kvalitetno organizirano varovanje informacij lahko vsa ta tveganja zmanjša na sprejemljivo raven.

2.3. Kaj ogroža informacijske sisteme

2.3.1. Zlonamerna koda

Zlonamerna koda obsega viruse, črve, trojanske konje, vohune in drugo nezaželeno kodo. Namen piscev take kode je povzročanje škode, izgube, vohunjenje ali zgolj dokazovanje svojega znanja.
Škoda, ki jo taka koda povzroča, je velika, tako zaradi samih izpadov sistemov, kot tudi zaradi časa, ki ga zaposleni porabijo za njihovo odstranitev in ponovno delovanje sistemov. Kljub temu da na svetu obstaja ogromno organizacij in posameznikov, ki se ukvarjajo z odkrivanjem in preprečevanjem zlonamerne kode, teh ni dovolj. Zato je zelo pomembno, da ima organizacija vgrajene naprave in postopke, ki omogočajo zaščito teh podatkov [Damij, 1995].

2.3.1.1. Vrste zlonamerne kode

Med zlonamerno kodo uvrščamo:

- viruse
- črve
- trojanske konje
- vohune

Virusi

Definicija:

»Virus je submikroskopski, obligatni intercelularni parazit, ki se sam ni sposoben razmnoževati, temveč samo s pomočjo translacijskega sistema celice gostiteljice. Nastanek virusov tolmačimo kot izpad nukleinskih kislin iz celice. Klasifikacija virusov temelji na tipu njihove nukleinske kisline in morfologije nukleokapside« [Iwanowsky, 1892].

Podobno kot Iwanowsky leta 1892, lahko danes definiramo računalniški virus: Program, ki se prilepi v gostiteljski program in ki lahko povzroči škodo v strojni in programski opremi ter v datotekah.
Glede na nevarnost za računalniške sisteme ločimo več vrst virusov. Od takih, ki nam prikažejo spremenjen ekran, zaigrajo glasbo, upočasnjujejo delovanje sistema, do takih, ki spreminjajo podatke, ali te celo zbrišejo.
Virusi se najbolj širijo s prilogami v elektronski pošti, lahko pa tudi z brezplačnimi vsebinami, ki jih prenesemo z interneta. Z zagonom okuženega programa se aktivira tudi virus, ki sproti okuži zdrave datoteke oz. programe, s katerimi pride v stik. Da je problematika virusov dokaj resna stvar, kaže tudi podatek, da na svetu obstaja že preko sto tisoč znanih virusov, vsak dan pa se pojavi še kakšen nov. Nekje med 95 – 98 procenti se jih prenaša preko elektronske pošte, največkrat preko šaljivih sporočil, glasbe, slik, voščilnic ... Virusi se ponavadi zelo hitro širijo. V manj kot 24 urah se lahko razširijo po vsem svetu. Podjetja, ki se ukvarjajo z odkrivanjem virusov, te tudi poimenujejo. Vendar pa se pojavljajo tudi spremenjene verzije istega virusa. Zato se na koncu imena doda še črka, lahko tudi dve.

Tabela 1: Lestvica najpogostejših virusov v septembru 2004

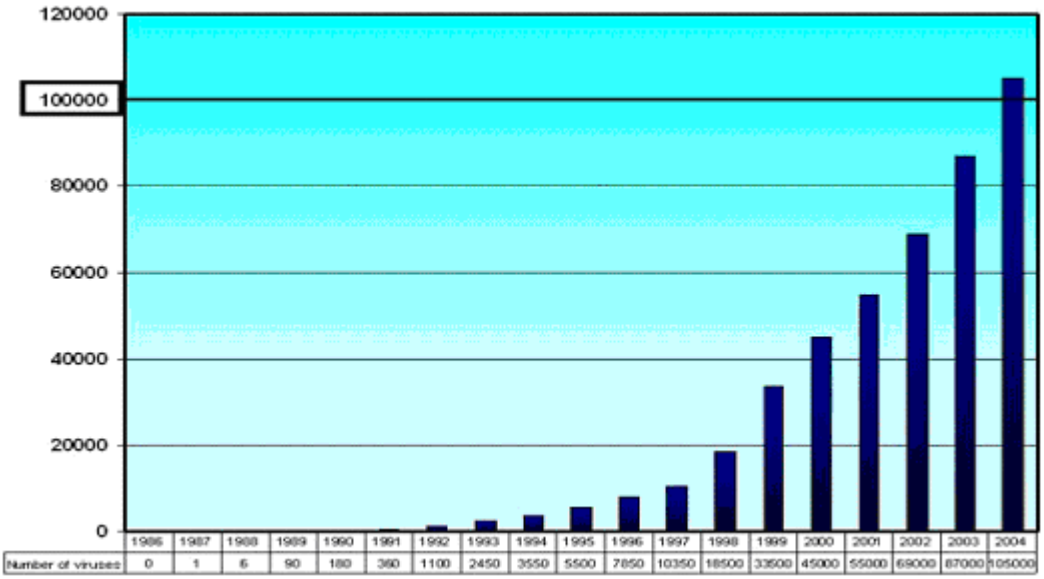
Mesto	Sprememba v razporedu	Ime	Odstotek pojavitve
1	+3	I-Worm.Netsky.q	21.67%
2	-1	I-Worm.Netsky.aa	13.79%
3	+1	I-Worm.Zafi.b	12.70%
4	-2	I-Worm.Netsky.b	9.63%
5	-	I-Worm.Mydoom.m	5.34%
6	+2	I-Worm.Bagle.z	4.86%
7	+2	I-Worm.Netsky.d	4.55%
8	nov	TrojanDownloader.JS.Gen	4.41%
9	-3	I-Worm.Netsky.t	2.51%
10	+1	I-Worm.Netsky.y	1.62%

Vir: www.kivi.si

Tabela 1 prikazuje najpogosteje odkrite viruse v septembru 2004. Vsakemu imenu je dodana tudi črka (verzija). Pri vodilnem (I-Worm.Netsky.) je to črka q, kar pomeni, da obstaja že 17. verzija tega virusa.

Tudi preteklo leto 2004 lahko štejemo med rekordno po številu virusov, saj je bila presežena meja 100.000 virusov (slika 2).

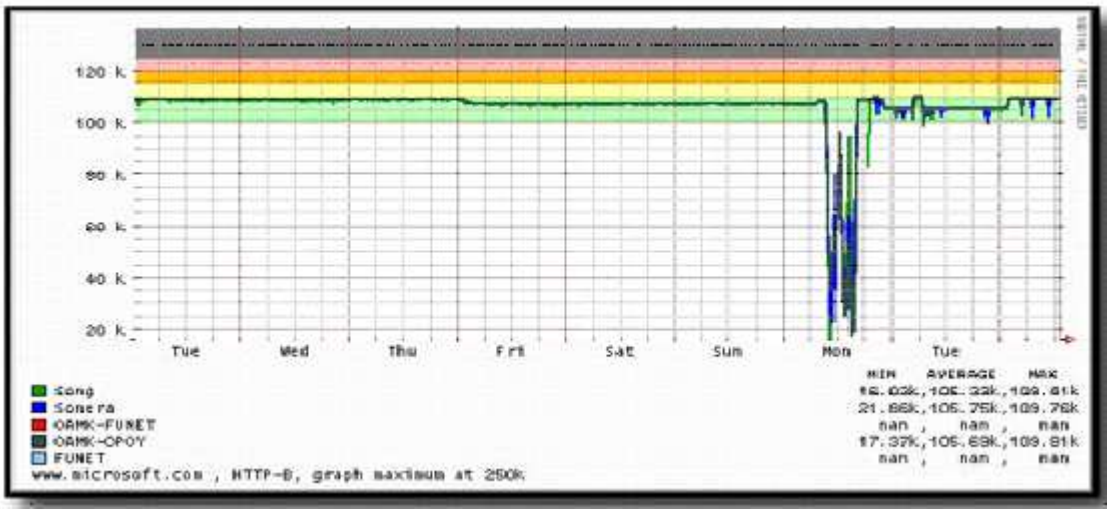
Slika 2: Rast virusov od leta 1986 do 2004



Vir: F-Secure, 2004

Slika 3 prikazuje, kako je virus Doomjuice.A v februarju leta 2004 uspel za nekaj ur popolnoma onemogočiti dostop do spletne strani www.microsoft.com.

Slika 3: Prikaz onemogočenega dostopa do strani www.microsoft.com



Vir: F-Secure, 2004

Črvi

Črv je oznaka za program, ki se samodejno širi po računalniškem omrežju. Pri tem lahko na računalniku izvaja različne operacije. Za razliko od virusov ne okužijo datotek, pač pa ostanejo aktivni v delovnem polnilniku, od koder se skušajo preko pošte ali omrežja razširiti na čim več računalnikov. Da se črv sploh lahko namesti na računalnik, je največkrat krivda napak operacijskega sistema, ki jih pisci črvov s pridom izkoriščajo. Podobno kot virus se brez vednosti uporabnika namesti na računalnik, odvisno od samega

črva pa je, kaj bo na okuženem sistemu naredil. Lahko prisluškuje tipkovnici, sodeluje pri napadu na tuj računalnik ali pa briše oz. spreminja podatke. Po navadi se širijo z elektronsko pošto, kjer črv samodejno razpošlje svojo kopijo. Za prejemnike navadno izberejo kar uporabnikovo zbirko naslovnikov. Lokalno pa se pogosto širijo tudi preko map v skupni rabi. Ironija je, da se največ črvov in virusov napiše ravno na osnovi popravkov, ki jih izdaja Microsoft. Pisci pregledajo, katere napake popravlja zadnji izdan popravek in le-te izkoristijo. Preden vsi uporabniki uspejo zadnji popravek naložiti, je škoda lahko že ogromna. Iz tega sledi, da je pametno skrbeti za politiko sprotnega nalaganja najnovejših popravkov, in sicer izključno od izdelovalca operacijskega sistema.

Trojanski konji

Trojanski konj je samostojen izvršljiv program, ki vsebuje uničevalno kodo.
Enako kakor njihov antični vzornik se prek na videz popolnoma nedolžnega programa ali dokumenta v elektronski pošti pritihotapijo v računalnik in nato skrivaj odprejo njegova vrata. Tako lahko zlonamernim posameznikom v skrajnem primeru omogočijo popoln nadzor nas sistemom (ang. Back Door) in dostop do poljubnih, tudi na videz še tako varovanih podatkov. Najbolj znana sta Back Orifice in NetBus. Ponavadi so skriti v priljubljenih datotekah (npr. Kazza, iMesh ipd.). Težko jih je odkriti, kajti so zelo majhni in skriti v kodi drugega programa. Za obrambo pred trojanskimi konji je zelo pomembno redno osveževanje protivirusnih programov in redno nalaganje zadnjih možnih popravkov operacijskega sistema. Odkrivajo jih tudi programi, ki preverjajo, ali so bile datoteke spremenjene.

Vohuni

Omrežni vohuni (ang. sniffer) omogočajo prisluškovanje prometu, ki se pretaka po omrežju.
Nepridipravi jih uporabljajo za pridobivanju tajnih podatkov in gesel, sistemski upravitelji pa legalno za prikaz stanja omrežja, iskanje morebitnih napak in porazdelitev obremenjenosti omrežja.
Znano je, da so tajne službe v ZDA, Angliji in Avstraliji ravno s prisluškovanjem nekodiranemu prometu na razpisih pridobile veliko število poslov.
Najboljša obramba je tu seveda kodiran promet, kjer je to mogoče, kajti vohunov se skoraj ne da izslediti.
Poznamo tudi vohune (ang. Spyware), ki spremljajo uporabnikove poteze na internetu (najpogosteje brez njegove vednosti) in jih posredujejo oglaševalcem in drugim zainteresiranim. Ponavadi se ti programi namestijo na skrivaj, včasih pa spremljajo katerega od brezplačnih programov. Posebna oblika vohunskih programov so internetni piškotki (ang. Cookie), ki oglaševalcem pomagajo zbirati podatke o uporabniku in njegovih navadah na določeni spletni strani.
Skrajna oblika vohunov so opazovalci tipkovnice (ang. Keylogger), ki si zapisujejo tipke, ki jih pritiskamo, in tako mimogrede pridejo celo do podatkov o uporabniških imenih in geslih.

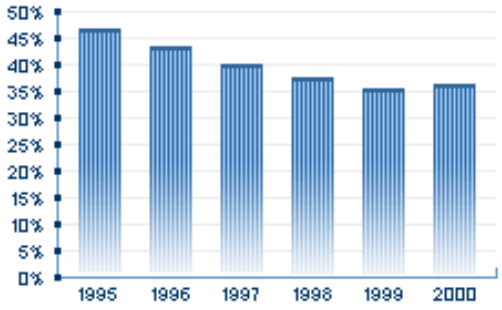
2.3.2. Socialni inženiring »manipulacija«

Najenostavnejši in najcenejši napad na informacijske sisteme je ravno socialni inženiring, ki s pridom izkorišča človeško nevednost, lahkomiselnost in zaupljivost.
Napadalec do žrtve lahko pristopi na več načinov. Lahko je avtoritativen, prijazen, lahko pa se izdaja za osebo, ki pozna nekoga v podjetju, lahko trdi, da gre za nujno zadevo, kjer je potrebna takojšnja reakcija [Berčič, 2003a]. Največkrat se napadalec izdaja za serviserja, ki odpravlja neko kritično napako, od nas pa zahteva le vstopna gesla. Svojo vlogo podkrepi še z nekaj imeni znotraj podjetja, ki so mu problem sporočila. V veliki večini uporabnik nič hudega sluteč napadalcu želene informacije tudi zaupa. Dober primer socialnega inženiringa je tudi elektronska pošta, ki prejemnike obvešča o najnovejšem virusu, ki je okužil že na milijone računalnikov po svetu. Uporabnik naj bi preveril, če ima na svojem disku datoteko z imenom JDBGMGR.EXE, ki naj bi bila znak okuženosti. Sledijo točna navodila, kako datoteko poiskati, zbrisati in za nameček izprazniti celo koš. Žal je to standardna datoteka (Java debugger manager in Microsoft Java runtime engine), ki jo za svoje delovanje potrebuje vsak osebni računalnik. Povrh vsega pa ima še nekoliko neresno ikono – medvedka. Največkrat svoje izjave potrdijo še s sindromom lažne identitete, češ da je ta virus odkrila skupina znanstvenikov neke pomembne univerze, recimo Princeton. Tudi prošnja po pošiljanju sporočila naprej je eden osnovnih pokazateljev, da gre za lažno obvestilo [Symantec, 2004].
Primer lepo pokaže, s kako malo vložka je možno podjetju narediti ogromen izpad sistema in posredno tudi finančno škodo. Tu odpovejo vsa klasična orodja varovanja. Če želimo, da nam napadalci s pomočjo socialnega inženiringa ne bodo več škodovali, moramo veliko vlagati predvsem v stalno izobraževanje in ozaveščanje zaposlenih.

2.3.3. Kraja in nezakonito razmnoževanje intelektualne lastnine

Tako podjetja kot posamezniki morajo skrbno varovati svoje informacije, saj lahko v trenutku celotno njihovo znanje, know-how, načrti in proizvodi, podatki o kupcih in cenah pridejo v roke konkurentov, obveščevalnih služb ali drugih nepridipravov [Berčič, 2004a].
Nezakonito razmnoževanje in prodajo intelektualne lastnine z namenom pridobitve večje protipravne premoženjske koristi se smatra kot kriminalno dejanje in se preganja po 159. členu Kazenskega zakonika Republike Slovenije. V Sloveniji se proti temu bori tudi organizacija BSA (Business Software Alliance).
Po podatkih BSA je leta 1999 stopnja nezakonito pridobljene programske opreme v Sloveniji znašala 70 %, kar pomeni, da je bilo od 100 računalniških programov le 30 programov pridobljenih legalno. Po zadnjih raziskavah stopnja piratstva sicer pada in naj bi v letu 2001 znašala 60%, vendar je še vedno visoka [http://www.bsa.si/piratstvo.php].

Tabela 2: Raven piratstva po svetu



Vir: Microsoft, 2005

Študija BSA, ki je bila leta 2001 izvedena na mednarodnem nivoju kaže, da se je v letu 2000 stopnja ponarejanja dvignila na 37 odstotkov (tabela 2). Po regijah je na najvišjem mestu Vietnam s 97 odstotki, v vzhodni Evropi se je stopnja piratstva povzpela na 63 odstotkov, v Združenih državah pa je padla na 25 odstotkov (tabela 3) [Microsoft, 2005].

Tabela 3: Prvih deset držav po stopnji piratstva

Država	1999	2000
Vietnam	98%	97%
Kitajska	91%	94%
Indonezija	85%	89%
Ukraina/ostale države SND	90%	89%
Rusija	89%	88%
Libanon	88%	83%
Pakistan	83%	83%
Bolivija	85%	81%
Katar	80%	81%
Bahrajn	82%	80%

Vir: Microsoft, 2005

2.3.4 Vsiljivci (ang. intruders)

Med vsiljivce štejemo vse nepooblaščene (ne-avtorizirane) vstope v informacijski sistem. Uporabniki nekaterih zlonamernih kod ali vohunov se prikradejo v sistem zaradi pridobivanja podatkov in izkoriščanja virov informacijsko-komunikacijskega sistema. Orodja, ki preprečijo vstop vsiljivcev imenujemo orodja za preprečevanje vdora v sistem (intrusion detection systems).

2.3.5. Ponaredbe in kraje

Računalniške sisteme je mogoče izkoristiti na različne načine. Večinoma gre za kriminalno dejanje, kjer storilec s svojim dejanjem oškoduje lastnika. Znan je primer iz bančništva, kjer je programer predelal program, ki je navzdol zaokroževal zneske na tekočih računih. Razliko si je nakazoval na svoj račun. Podoben primer je tudi izkoriščanje sistema mednarodne telefonije, kjer storilci kličejo na tuj račun. Seveda s tem oškodujejo telefonsko podjetje.

Večino takih poneverb izvedejo zaposleni, ki imajo dostop do računalniških sistemov in jih dobro poznajo. Seveda pa obstajajo tudi vdori in izkoriščanja računalniških sistemov od zunaj. Tu je potrebno precej več znanja in izkušenj. Nekateri taki vdori se zgodijo s pridobitniškimi nameni, spet drugi pa le kot dokazovanje pred »hekerskimi« kolegi. Največkrat gre za spremembo ali izbris spletne strani, s čemer storilec osramoti določeno podjetje.
Zaradi svojega ugleda podjetja vse te poneverbe le s težavo javno objavijo. S tem si lahko močno zmanjšajo ugled ali celo izgubijo stranke.

2.3.6. Napake

2.3.6.1. Napake strojne opreme

Kljub visoki zanesljivosti strojna oprema lahko vseeno odpove. Odpovedi največkrat nastopijo zaradi pregretja, tresljajev, vlage, udarcev, izpada ali pretrganja kablov … Delna odpoved strojne opreme je redka, a zelo kritična. Takrat naprava deluje, a rezultati obdelav so lahko napačni. Največkrat se z odpovedjo enega od podsistemov zaradi varnosti ustavi celoten sistem. Izjema je oprema, kjer so vsi vitalni deli podvojeni. To pomeni, da v primeru izpada enega sistema z avtomatskim ali ročnim preklopom le-tega začne nadomeščati drug sistem. Sistem, ki v primeru izpada skrbi kot nadomestni, je lahko v fazi delovanja primarnega sistema nedelujoč, lahko si s primarnim delita naloge, lahko pa opravlja popolnoma druge naloge.

2.3.6.2. Napake v programski opremi

Zaradi obsežnosti in vse krajših rokov izdaje nove programske opreme, jo je pred prihodom na tržišče v celoti nemogoče testirati. Tako se večina napak pokaže šele ob sami uporabi [Gradišar, 1996]. Napake se lahko ob uporabi pokažejo na način, da nadaljnje delo ni več mogoče ali pa ostajajo prikrite. To pomeni, da se program ustavi ter javi napako ali pa da deluje naprej, rezultati obdelave pa so napačni. Drugi način je precej bolj problematičen, kajti take napake delovanja programske opreme je izredno težko izslediti. Zato je pomembno, da imajo programi v sebi vgrajena večstopenjska preverjanja, ki močno zmanjšajo možnost tovrstnih napak.

2.3.6.3. Napake uporabnikov

Napake uporabnikov so najbolj pogost vzrok nepravilnega delovanja informacijskih sistemov. Vzrokov za nastanek teh napak je mnogo. Najpogosteje uporabniki ne upoštevajo navodil, organizacijskih predpisov ali pa so pri delu površni [Gradišar, 2003]. Večina informacijskih sistemov ima vgrajenih veliko varoval, ki napake preprečujejo, oziroma nanje opozarjajo. A še vedno lahko uporabnik po nekem naključju izvede operacijo, ki v fazi testiranja ni bila predvidena. Ne glede na kakovost informacijskih sistemov, bodo ti vedno ostali občutljivi na napake uporabnikov.

2.3.6.4. Napake v podatkih

Tako kot lahko uporabniki nepravilno rokujejo z informacijskimi sistemi, lahko vanje vnašajo tudi napačne podatke. Določene kontrole sicer obstajajo tudi pri vnosu. Vendar gre tu največkrat za preverjanje dolžine vnosa, kontroliranje, ali gre za črke ali števila, velikost črk, velikostni razred oziroma format vnosa. Ni pa možno kontrolirati vnosa podatkov, ki je znotraj omenjenih formatov.

2.3.7. Nesreče

2.3.7.1. Naravne nesreče

Naravnih nesreč, kot so poplave, potresi, strele, neurja, vnaprej ne moremo napovedati niti nanje ne moremo bistveno vplivati. Večina naštetih lahko popolnoma uniči informacijski sistem organizacije. Navkljub majhni verjetnosti nastanka jih je potrebno predvideti.

2.3.7.2. Požar

Požar je pri uporabi informacijske tehnologije ena od nesreč, za katero obstaja velika verjetnost dogodka. Zato smo ponavadi nanjo tudi najbolje pripravljeni.

2.3.7.3. Izliv vode

Za razliko od možnosti požara možnost izliva vode upoštevajo le redki. Vemo pa, da počena cev centralne kurjave ali pa počena vodovodna cev lahko dokaj hitro zalijeta dragocene informacijske vire, ki navadno niso dvignjeni od tal. Še posebej je to nevarno, če do izlitja pride v nočnem času, ko nihče ne more ukrepati. Poleg vode informacijskim sredstvom škodijo tudi ostale tekočine. Neredek primer je, ko uporabnik po tipkovnici (ali prenosniku) polije kavo ali kako drugo tekočino.

2.3.8. Napačno dimenzionirani sistemi

Napačno dimenzionirani sistemi v realnem času niso sposobni izvajati zahtevanih nalog. Zato so velikokrat vzrok manjše razpoložljivosti, lahko pa tudi izpad informacijskega sistema. Zato je dimenzioniranje zelo pomembno že pred samim nakupom opreme. Da pa znamo pravilno dimenzionirati sistem, moramo zelo dobro poznati potrebe, katerim bo sistem služil. Prav tako moramo poznati časovni prirastek podatkov, ki jih bo sistem upravljal, in pa prirastek uporabnikov, ki bodo sistem uporabljali. Prirastek oziroma obremenitev sistema moramo stalno beležiti, saj le tako lahko dovolj hitro reagiramo in sistem nadgradimo ali zamenjamo.

Ne glede na to, ali gre za sesutje celotne stavbe ali zgolj za počeno cev vodovodne napeljave, se je pomembno zavedati možnosti nastanka problema. Vsekakor so ukrepanja v obeh skrajnih točkah zelo različna, vendarle pa moramo za različne scenarije imeti

pripravljene tudi različne ukrepe. In nenazadnje morajo biti vsi ti ukrepi redno testirani, uporabniki pa z ukrepi natančno seznanjeni [Hvala, 2002].

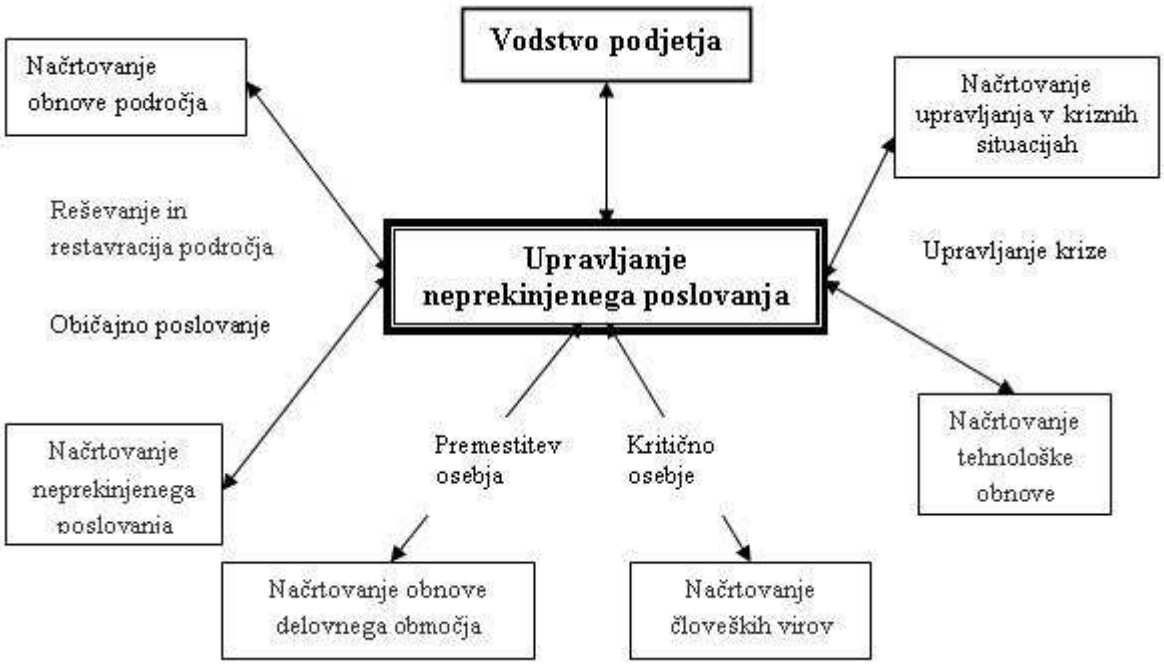
2.4. Kdo zahteva varovanje informacij

2.4.1. Zahteve organizacije po neprekinjenem poslovanju

Vsaka organizacija mora imeti za zaščito pomembnejših poslovnih procesov vpeljan proces neprekinjenega poslovanja (ang. BCM- Busines Continuity Management). Ta jo ščiti pred učinki večjih napak ali katastrof, s tem pa zmanjšuje prekinitev dela na sprejemljivo raven [BS ISO/IEC 17799:2000, 2000].
Upravljanje neprekinjenega poslovanja mora biti sestavni del upravljanja podjetja. Vodstvo naj ga načrtuje in sprejme ter mu s tem doda poslovno vrednost. Prijemi pri načrtovanju in vzpostavitvi neprekinjenega poslovanja so v tesni zvezi z vsemi poslovnimi procesi v organizaciji (slika 4) ter so neposreden in oprijemljiv rezultat upravljanja tveganj v urejeni organizaciji.

Vse prepogosto je načrtovanje teh aktivnosti prepuščeno samo tehničnemu osebju s področja informatike in ni celovit odgovor organizacije na tveganja, ki jim je izpostavljena. Varnostna ozaveščenost vodilnih delavcev je zelo pomembna, saj ravno oni določajo izbiro strategije informacijske varnosti v organizaciji [Kajić, 1999].
Tudi dejstvo, da smo zavarovani, ni dovolj. Zavarovanje v primeru nesreče poskrbi zgolj za finančno plat, ne pa tudi za preprečevanje nesreč ali za samo obnovitev in nadaljevanje prekinjenega procesa [PAS 56, 2003].
Organizacija naj objavi sprejeto politiko in smernice za upravljanje neprekinjenega poslovanja, hkrati pa poskrbi, da se ta tudi pravilno izvaja.

Slika 4: Odnosi v upravljanju neprekinjenega poslovanja



Vir: Smith, 2001

2.4.2. Zakonske zahteve

Podjetja, vladne ustanove in bančne institucije se za varovanje informacij odločajo predvsem zaradi poslovnih, pa tudi zaradi zakonskih zahtev. Elektronsko poslovanje je poslovna kategorija. A z globalizacijo trga, hitrim razvojem tehnologije ter znanj, za varno delo subjektov potrebuje tudi pravne okvire [Jerman-Blažič Borka, 2001]. Informacijska varnost je močno povezana tudi s informacijskim pravom. Tu se začnejo odpirati vprašanja s področja dostopa do programske, strojne, sistemske opreme, varstva osebnih podatkov, kriptiranja, elektronskega poslovanja in podpisovanja, intelektualne lastnine …[Berčič, 2003b]. Pravni problemi prav tako nastajajo zaradi anonimnosti sodelujočih, novih oblik komunikacije, brezmejnosti okolja, … [Makarovič, 2001].

Zakoni, ki v Sloveniji opredeljujejo varovanje informacij, so:

- Zakon o elektronskem poslovanju in elektronskem podpisu,
- Zakon o elektronskih komunikacijah,
- Zakon o varstvu osebnih podatkov,
- Zakon o avtorskih in sorodnih pravicah,
- Zakon o pogojnem dostopu do zaščitenih elektronskih storitev,
- Zakon o varstvu potrošnikov,
- Zakon o tajnih podatkih.

Banka Slovenije je leta 2004 celo izdala sklep, ki ga za opravljanje bančnih oziroma drugih finančnih storitev morajo upoštevati vse banke in hranilnice [www.danesa.com].
Sklep pa se glasi: »*...banka mora v svojem poslovanju upoštevati slovenska standarda SIST BS 7799-2:2003 in SIST ISO/IEC 17799:2003* ...« [Uradni list RS, št. 83/04].

2.4.3. Zahteve tržišča

S časom bo trg na organizacije in ustanove začel vršiti vedno večji pritisk na stopnjo varnosti svojih podatkov. Kajti prav nič nam ne pomaga, če svoje podatke v podjetju dobro varujemo, ko pa jih izmenjujemo s partnerjem, ki je varnostno šibak. Tudi povezovanje v omrežja s podjetji, ki neustrezno varujejo informacije, je tvegano, kajti nepridipravi lahko informacijski sistem napadejo tudi preko podjetja, ki je v ta sistem povezan.
S sklepom guvernerja Banke Slovenije iz decembra 2003 morajo vse banke prilagoditi svoje delovanje standardu BS 7799.
Zadnji primer je organizacija BMW, ki je od vseh svojih dobaviteljev zahtevala skladnost poslovanja s standardom BS 7799.

2.4.4. Zahteve zavarovalnic

Zavarovalnice v tujini že zavarujejo nevarnosti elektronskega poslovanja. Najprej se je potreba po tem pokazala pri bankah in podjetjih, ki poslujejo preko interneta [Svetič, 2002]. Pri teh zavarovanjih je v ospredju Amerika, kjer je bilo elektronsko poslovanje najprej razvito. Vendarle pa se je potrebno zavedati, da nam zavarovanja za vrednost podatkov na notranjih pomnilnikih ne bo sklenila nobena zavarovalnica, če prej ne dokažemo, da redno skrbimo za ažurne kopije podatkov.

3. STANDARD BS 7799

3.1. Splošno o standardu BS 7799

Zaradi kompleksnosti informacijskih sistemov se v poslovnih okoljih pojavlja potreba po sistematičnem obvladovanju varnosti na organizacijskem nivoju. Takšen celovit način upravljanja varnosti vpeljuje standard BS 7799/ISO 17799. Je mednarodno veljaven standard, namenjen vodstvenemu osebju, ter predstavlja model za učinkovit sistem upravljanja varovanja informacij (SUVI). Sestavljen je iz dveh delov. Prvi del predstavlja najboljšo prakso pri zadovoljevanju zahtev standarda in razlaga, kaj naj bi organizacija imela. Drugi del je specifikacija z napotki za uporabo in razlaga, kaj organizacija mora imeti, če želimo biti skladni s standardom in se po njem certificirati [Ključevšek, 2002b].
V kodeksu je opisana najboljša poznana praksa, katere postopki niso zavezujoči, v specifikaciji pa so postavljene zahteve po vzpostavitvi, izvedbi in dokumentiranju SUVI.

Vsebuje 10 poglavij, 36 ciljev, 127 kontrol.

Osnovna poglavja standarda so:

1. Varnostna politika
2. Organiziranost varovanja
3. Razvrstitev in nadzor sredstev
4. Varovanje v zvezi z osebjem
5. Fizična zaščita in zaščita okolja
6. Upravljanje s komunikacijami in s produkcijo
7. Nadzor dostopa
8. Razvoj in vzdrževanje sistemov
9. Upravljanje neprekinjenega poslovanja
10. Združljivost

Prvo poglavje je namenjeno krovnemu dokumentu, kjer organizacija napiše svojo varnostno politiko. Ta je ponavadi sestavljena večnivojsko, od krovne politike na najvišjem nivoju, preko politik za posamezna področja, do posameznih navodil in obrazcev na najnižjem nivoju.
Drugo poglavje govori o organiziranosti varovanja ter definira varnostni forum, ki v organizaciji skrbi za smernice varnostne politike.
Tretje poglavje je namenjeno temeljitemu popisu vsega fizičnega premoženja in sredstev. S tem dosežemo nadzor nad opremo, pa tudi določimo odgovornost za posamezne elemente informacijskega sistema.
V četrtem poglavju je govora o varnostni politiki za uporabnike informacijskega sistema, kot so izobraževanje, postopki odobritve dostopa, sprejem novih sodelavcev …
Peto poglavje je namenjeno fizični varnosti informacijskih sistemov, poudarjena je predvsem varnost vitalnih informacijskih sredstev.
Šesto poglavje obravnava varnost omrežij in računalnikov, njihovo pravilno uporabo ter postopke upravljanja. Obravnava tudi postopke za zaščito pred zlonamerno programsko opremo ter postopke izmenjave podatkov in programske opreme.
Sedmo poglavje obravnava izvajanje nadzora dostopa do sistema. Govori o politiki gesel, postopkih registracije, dostopu do omrežja, do računalnika, do seje …
Osmo poglavje je namenjeno razvoju in vzdrževanju informacijskih sistemov, posebej so obdelane varnostne zahteve sistema samega, pa tudi aplikacijskih sistemov ter ostalih datotek.

Deveto poglavje govori o neprekinjenem poslovanju, njegovem načrtovanju, testiranju in obnavljanju. Govori tudi o vlogah, zadolžitvah in pooblastilih v primeru informacijskega izpada.
Deseto poglavje pa obravnava usklajenost informacijskega sistema z zakonodajo, tako na področju pravnih zahtev, kot tudi varnostnih pregledov informacijskega sistema [Konečnik, 2002].
Upoštevanje določil standarda BS 7799 nam omogoča, da bomo v podjetje vpeljali učinkovit sistem za upravljanje informacijske varnosti, saj nam zagotavlja:

- **neoporečnost**: varovanje točnosti in popolnosti informacij in računalniške programske opreme,
- **zaupnost**: zagotavljanje, da so informacije dostopne samo pooblaščenim osebam,
- **razpoložljivost**: zagotavljanje, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom, kadar jih potrebujejo.

Uporaba standarda prinaša poslovne koristi in je potrebna, da se izognemo nepreglednemu poslovanju in ravnanju z informacijami. Šele ko upravljamo z varnostjo informacij, zares postanemo njeni dobri gospodarji [Ključevšek, 2002b].

3.2. Razvoj standarda

Standard je kot kodeks upravljanja varovanja informacij prvič izšel leta 1995 v Veliki Britaniji. Izdal ga je British Standard Institution (BSI). Leta 1998 pa je izšla še specifikacija z napotki za uporabo. Leta 2000 je prvi del postal BS ISO/IEC 17799-1:2000 (Code of practice for Information Security Management), leta 2002 pa je izšla nova različica drugega dela standarda, ki pa ni ISO in nosi naziv BS 7799-2:2002 (Specification for Information Security Management).
V Sloveniji je leta 1997 standard kot kodeks dobil tudi status slovenskega standarda.
Trenutno sta v Sloveniji v veljavi standarda:

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

3.3. Sorodnost z ostalimi ISO standardi

Pridobljen certifikat po standardu BS 7799 pomeni vodilo za vse aktivnosti zagotavljanja varnosti pri posredovanju in hrambi informacij. Je orodje stalnega izboljševanja poslovnega procesa v smislu upravljanja varnosti informacij (slika 5).

Slika 5: Uporaba modela PDCA (NSPU) v času

Vir: Berčič, 2003a

Vzpostavljen notranji sistem je potrebno namreč vzdrževati ter ga stalno izboljševati. Ravno v tem je ta standard soroden s standardi ISO 9000 (kakovost), 14000 (okolje), 18000 (zdravje zaposlenih). Omenjeni standardi se zbližujejo tudi po svoji strukturi z namenom zniževanja stroškov pri vzpostavitvi in vzdrževanju dveh ali več standardov v istem podjetju [Sorodnost med standardi, 2005].

4. SISTEM ZA UPRAVLJANJE VAROVANJA INFORMACIJ (SUVI)

Sistem za upravljanje varovanja informacij (v nadaljevanju SUVI), ali (ang. ISMS – Information security management system) je sistem, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju informacijske varnosti. Je vodstveni sistem in je osnova standarda BS 7799. Temeljiti mora na ciljih, ki jih organizacija želi doseči z varovanjem in zaščito, na izbiri ustrezne strategije, ki bo ustrezala velikosti podjetja, na načinu in obsegu poslovanja, resursih, organizacijski kulturi ter znanju. Predvsem je pomembno da organizacija v SUVI vidi poslovne priložnosti, kot so:

- zadovoljevanje potreb trga v skladu s kakovostjo in varnostjo, ki jo organizacija obljublja,
- obvladovanje lastnih poslovnih procesov in dejavnikov,
- stalno izboljševanje kakovosti in varnosti poslovanja,
- zmanjševanje poslovnih in operativnih tveganj [Berčič, 2003a].

Tako kot vsi ostali upravljavski sistemi tudi SUVI za vzpostavitev in upravljanje uporablja procesni pristop načrtuj-stori-preveri-ukrepaj (NSPU) (slika 6).

4.1. Faze uvedbe in upravljanja SUVI

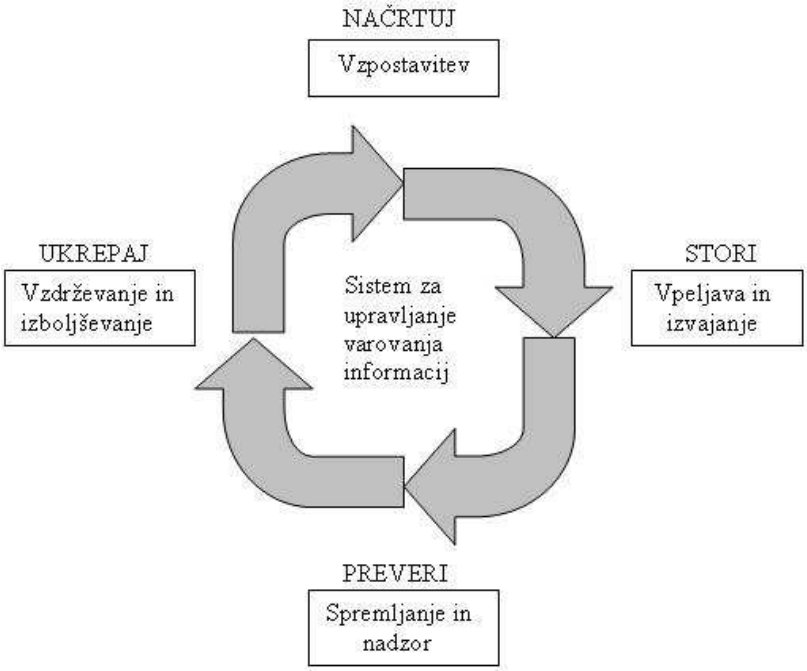
4.1.1. Načrtuj

Prvi del cikla NSPU je Načrtuj. To je faza, v kateri načrtujemo aktivnosti, ki jih bomo kasneje izvedli.
V tej fazi je potrebno:

- določiti politiko varovanja informacij,

- določiti obseg SUVI,
- izvesti analizo odstopanja,
- oceniti tveganja,
- izdelati načrte za obravnavanje tveganja,
- izdelati izjavo o primernosti.

Slika 6: Model NSPU za proces SUVI



Vir: BS 7799-2:2002, 2003

4.1.1.1. Politika varovanja informacij

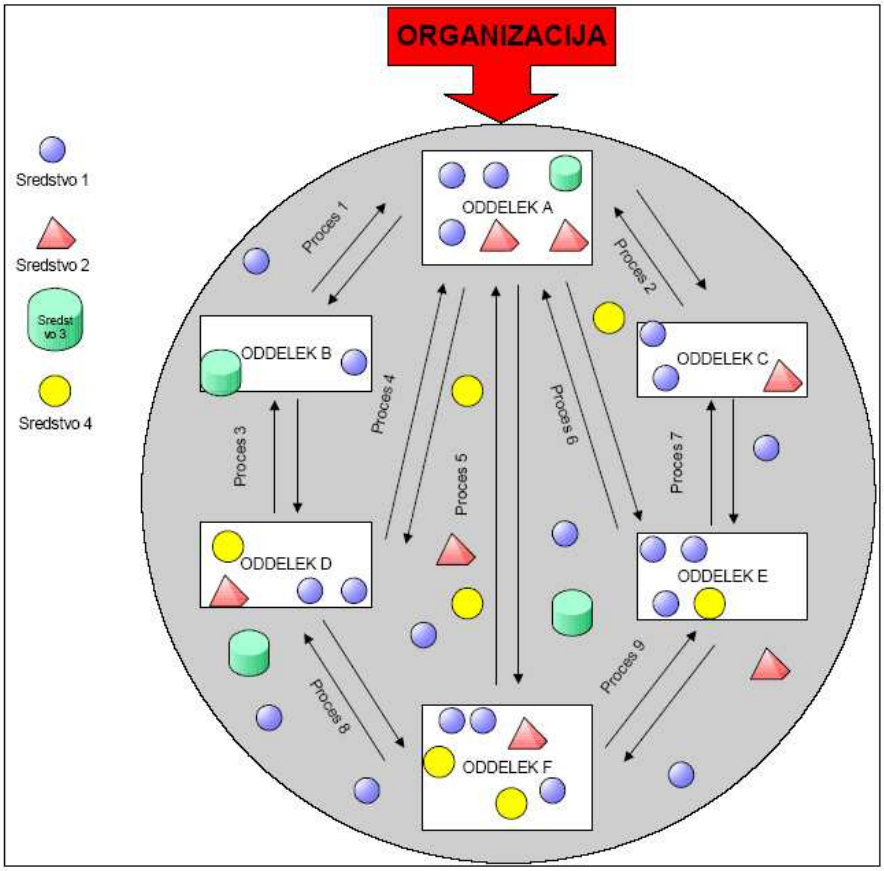
Vsaka organizacija naj bi imela izdelano politiko varovanja informacij. Ta dokument naj bi bil osnova za vse ostale dokumente, ki varnostno problematiko obravnavajo bolj podrobno in so namenjeni reševanju specifičnih problemov. Politiko mora vedno potrditi najvišje vodstvo organizacije [Rakovec, 1995]. V varnostni politiki morajo biti natančno definirani cilji varovanja, vloge in odgovornosti ter merila, načela in postopki za njeno uvedbo in nadzor. Politika varovanja informacij je interni akt organizacije, ki določa jasna navodila v zvezi z varnostjo in odgovornostmi zaposlenih za izvajanje te politike [Andolšek, 2002]. Vsebuje pravila obnašanja in delovanja znotraj organizacije, obenem pa določa, kaj je in kaj ni dopustno. Lahko je napisana kot en dokument, lahko pa je razdeljena na več nivojev, od krovnega na najvišjem, taktičnega na srednjem, in operativnega na najnižjem nivoju. Politika varovanja informacij mora biti posredovana vsem zaposlenim, študentom, praktikantom in zunanjim izvajalcem.

Več o nivojski organiziranosti politike varovanja informacij je napisanega v poglavju 4.3. Varnostna politika.

4.1.1.2. Določitev obsega SUVI

SUVI lahko vpeljemo v celo organizacijo ali pa si izberemo le del organizacije. Vsekakor je z varnostnega stališča idealno, če vključimo celotno organizacijo, vendarle pa to ponavadi zaradi kompleksnosti povezav med oddelki (slika 7) na začetku ni vedno lahko. Zato je za začetek vpeljave SUVI enostavneje določiti le del organizacije, vanj vnesti vse prvine informacijske varnosti in nenazadnje ta del organizacije tudi certificirati po standardu BS 7799. Kasneje lahko na osnovi izkušenj enega dela SUVI širimo po oddelkih ali procesih na celotno organizacijo.

Slika 7: Kompleksnost povezanosti med oddelki



Vir: Janežič, 2004

Obseg SUVI določamo s stališča:

- organizacijskih delov, ki jih zajema SUVI,
- procesov, ki jih bomo varovali,
- ljudi, ki nastopajo v procesih,
- aktivnosti, ki bodo v SUVI nastopale,
- storitev in preskrbe (komunikacijske storitve, elektrika, ogrevanje, klimatizacija),
- vhodov in izhodov sistema,
- medsebojne povezave,
- velikosti organizacije,
- geografskega položaja,
- informacijskih sredstev, ki so vključena v obseg,

- strateških in organizacijskih okoliščin,
- kriterijev, po katerih bomo ocenjevali tveganja.

Glede na kompleksnost vidikov lahko meje obsega SUVI določimo na več načinov. Vsekakor pa je obseg SUVI potrebno natančno določiti z vseh vidikov tako, da je za vsak informacijski vir jasno, ali spada v SUVI ali ne [Plate, 2002c]. SUVI je lahko tudi del celotnega upravljavskega sistema, kamor štejemo upravljanje kakovosti (ISO 9001), varstvo okolja (ISO 14000) ter varstvo in zdravje pri delu (ISO 18000).
Obseg SUVI je treba redno, najmanj pa enkrat letno, pregledovati in po potrebi spremeniti. Obvezno pa ga je potrebno spremeniti ob:

- reorganizaciji,
- fizični selitvi,
- spremembi v informacijski in omrežni komunikaciji,
- spremembi v preskrbi.

4.1.1.3. Določitev skupine za uvedbo in usklajevanje SUVI

Za uvedbo in delovanje SUVI mora organizacija natančno določiti kadre, njihova pooblastila in dolžnosti. V večjih organizacijah je smiselno ustanoviti oddelek informacijske varnosti in pa vodjo informacijske varnosti (Ang. Securuty Manager ali Chif Security Officer). Nekatere organizacije pa se odločijo za postavitev vloge pooblaščenca za informacijsko varnost. Njegova naloga je strokovno svetovanje s področja varovanja informacij, obenem pa prevzema celotno odgovornost za razvoj in vpeljavo varovanja ter določa način kontrole. Poleg tega mora vzpostavljati stike z zunanjimi strokovnjaki za varovanje, saj je le tako mogoče ostati v koraku z industrijskimi trendi, nadzorovati mora standarde, ocenjevati metode ter priskrbeti ustrezno pomoč v primeru incidentov v varnostnem sistemu. Spodbujati mora multidisciplinarni pristop k varovanju informacij, kar pomeni spodbujanje sodelovanja med vodstvom organizacije, uporabniki, skrbniki, načrtovalci aplikacij, revizorji, varnostnim osebjem ter strokovnjaki na področjih, kot sta varovanje in upravljanje tveganja.
Standard narekuje tudi uvedbo varnostnega foruma, katerega naloga je sprejemanje predlaganih dokumentov v zvezi s SUVI in pomagati pri vpeljavi le-tega v celotno organizacijo. V njem naj bo vsaj en predstavnik vodstva in po en predstavnik procesov, določenih v obsegu SUVI. Priporočilo standarda je, da bi bila v varnostnem forumu vsaj dva certificirana notranja presojevalca.
V začetni fazi uvajanja SUVI se je smiselno opreti na zunanje izvajalce s specifičnim znanjem s področja informacijske varnosti. Ti lahko s svojimi strokovnimi nasveti pripomorejo k hitrejši, kvalitetnejši in celovitejši uvedbi SUVI. Če je že v začetku namen organizacije, da se po standardu tudi certificira, je dobro že pri uvajanju vključiti tudi eno od certifikacijskih hiš.
Nenazadnje pa SUVI brez sodelovanja vseh zaposlenih in pogodbenih strank ne more uspeti.

4.1.1.4. Analiza odstopanja

Z analizo odstopanj ugotavljamo neskladje organizacije s standardom BS 7799. Po točkah standarda ugotovimo, v kakšnem stanju se na področju varovanja informacij nahajamo. Zelo hitro ugotovimo, kje smo s standardom skladni in kje odstopamo. Rezultat je dobra

osnova za ocenjevanje tveganj. Prav tako pa nam rezultati analize odstopanj pomagajo pri ugotavljanju stroškov celotne uvedbe SUVI. Ponavadi je narejena na osnovi analize vprašalnikov, ki jih v organizaciji izpolnijo odgovorne osebe. V Sloveniji obstaja orodje Poslovni ščit, ki poleg vodenja celotne dokumentacije SUVI vključuje tudi analizo odstopanj.
Analizo odstopanj s predlogi za dosego skladnosti z BS 7799 sem izvedel tudi v študiji primera, ki je predstavljena v točki 6.

4.1.1.5. Ocena tveganja

Po identifikaciji poslovnih procesov, fizičnih sredstev, programske in strojne opreme, podatkov in ljudi (glej prilogo 3 Popis sredstev) ter na osnovi analize odstopanja se lahko izvede ocena tveganj. Slika 8 prikazuje, da se s tveganji srečujemo na vseh področjih delovanja. Zato je pomembno, da jih poznamo in ocenimo. Ocena tveganj omogoča sistematičen pristop k strukturiranju in definiciji prioritet pri gradnji celovitega SUVI. Določiti je potrebno tveganje v odvisnosti od vrednosti sredstev, groženj in ranljivosti.

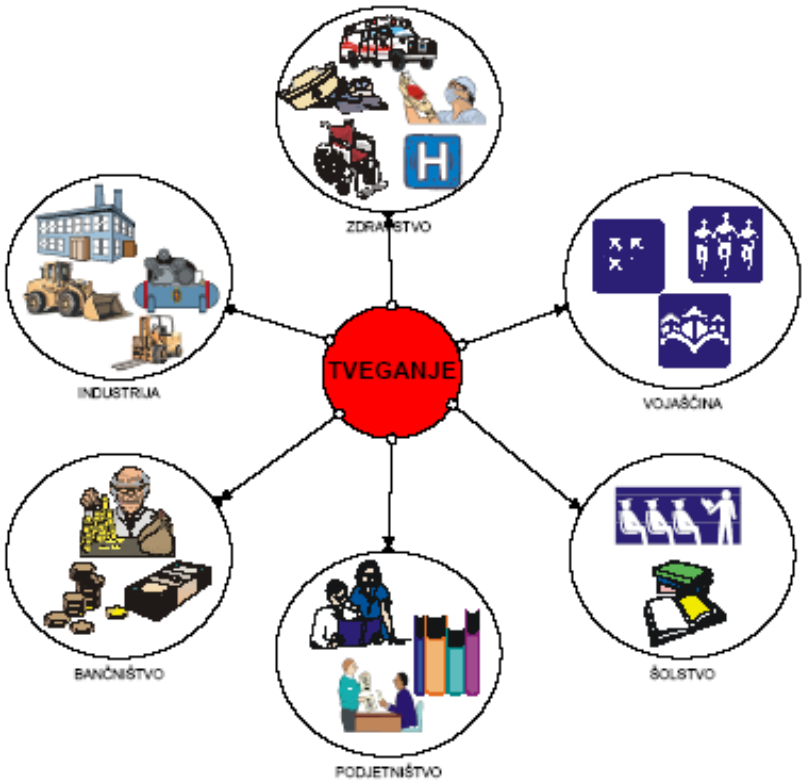
Tabela 4: Določanje ocene tveganja

	Stopnje grožnje	Nizka			Srednja			Visoka		
	Stopnje ranljivosti	N	S	V	N	S	V	N	S	V
Vrednost sredstva	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Vir: Rakovec, 2005b

Ocena tveganj poteka v dveh fazah.
V prvi fazi določimo vsa sredstva za varovanje ter jih ovrednotimo glede na pomen v organizaciji.
V drugi fazi pa ta sredstva povežemo z možnimi ranljivostmi in grožnjami oziroma tveganji, ki jih iz tega izračunamo. To lahko storimo z uporabo splošno znanih groženj in ranljivosti, ki so zbrane v prilogi 9 (Spisek ranljivosti) in 10 (Spisek groženj).
Preprost rezultat dobimo s tabelo 4, ki prikaže tveganje na osnovi vrednosti, grožnje in ranljivosti.

Slika 8: Področja tveganj



Vir: Janežič, 2004

Ocena tveganj omogoča fazni pristop pri vzpostavljanju varnostnih mehanizmov, saj se na osnovi ocenjenih tveganj določijo prioritete aktivnosti. Ocena tveganj je tako poleg klasifikacije informacij ključni element v procesu odločanja in izvedbe SUVI [http://www.hicsalta.si/storitve/storitve-s7.htm].

4.1.1.6. Načrtovanje upravljanja s tveganji

Organizacija mora oblikovati natančen načrt za obravnavanje tveganj, ki mora za vsako tveganje vsebovati:

- metodo za obravnavanje posameznega tveganja,
- uporabljene kontrole,
- časovni plan uvedbe kontrole.

Načrt za obravnavanje tveganj je dokument, ki določa ukrepe za zmanjševanje visokih tveganj na sprejemljivo stopnjo.

4.1.1.7. Izjava o primernosti (Ang. SoA – Statement of Aplicability)

Izjava o primernosti vsebuje seznam kontrol, ki jih narekuje standard. Na osnovi tveganj se na tem dokumentu opredelimo, ali bomo kontrolo vpeljali ali ne. Pomembna je predvsem

razlaga, zakaj neke kontrole ne bomo uvedli. Smiselno je tudi v navesti, na katero politiko oziroma kak drug dokument SUVI se kontrola nanaša.
Primer izjave o primernosti je priložen v prilogi 8.

4.1.2. Stori

Drugi del cikla NSPU je Stori. To je faza, v kateri načrtovane aktivnosti izvedemo.
V tej fazi je potrebno:

- upravljati s tveganji,
- implementirati kontrole,
- izobraževati in ozaveščati zaposlene,
- odkrivati varnostne incidente.

4.1.2.1. Upravljanje s tveganji

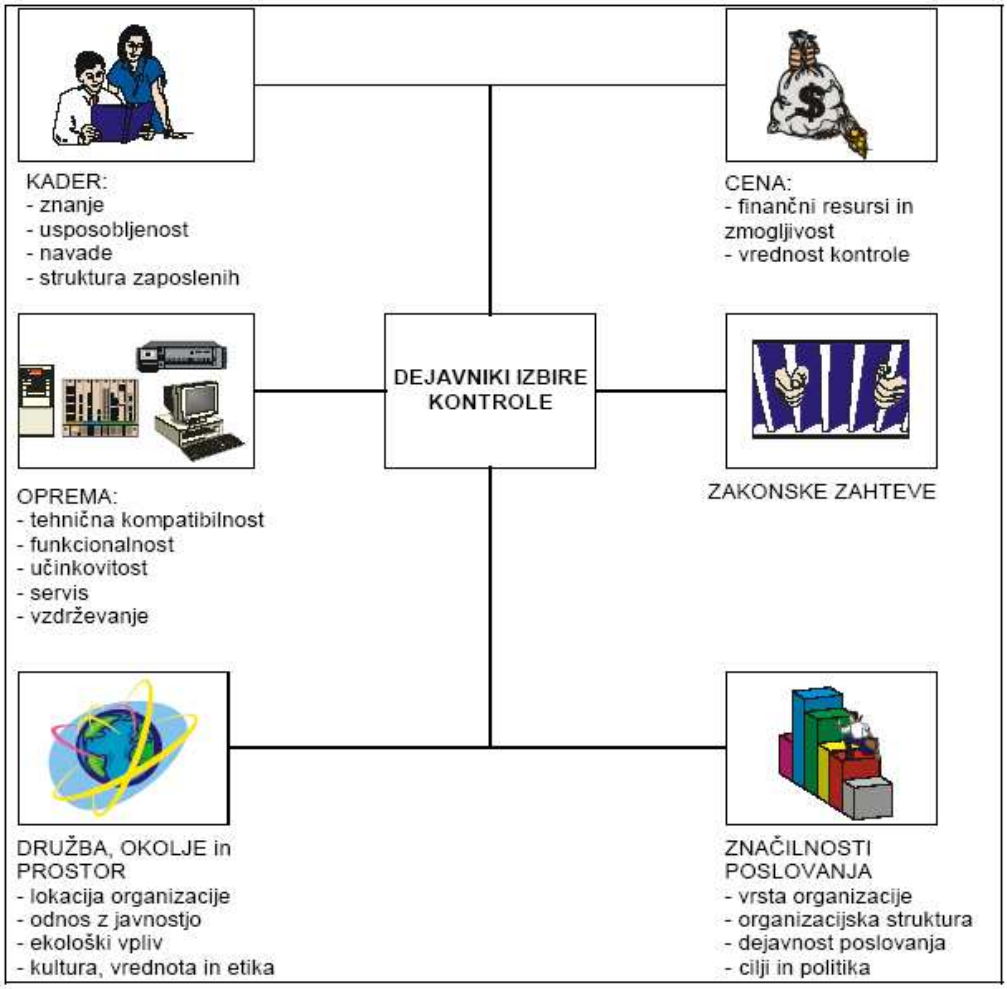
Upravljanje s tveganji je tipičen upravljavski proces, kar pove že samo ime. Kako bomo upravljali s tveganji, je odvisno od več dejavnikov (slika 9). Vsekakor so cena (slika 10), preprostost rešitve in razpoložljivost virov ter sredstev med pomembnejšimi [Ključevšek, 2002a].

Potrebna je opredelitev do ugotovljenega tveganja. Organizacija lahko ta tveganja:

- sprejme,
- zmanjša,
- prenese,
- se jim izogne [Janežič, 2004].

Če je ugotovljeno tveganje sprejemljivo, nadaljnji ukrepi niso potrebni. Vsekakor to ni stanje, ki je ugotovljeno enkrat za vselej, pač pa ga je potrebno ciklično ponavljati. Kadar se ugotavlja, da je tveganje previsoko, je potrebno uvesti ukrepe, da se le-to zmanjša. Takrat uvedemo izbrane kontrole, ki smo jih določili v fazi Načrtuj. V prilogah 11 in 12 sta zbrana spiska kontrol po področju in po standardu BS 7799. Za uspešno zmanjševanje tveganj je potreben učinkovit sistem, ki določa izbrane metode, natančno opredeljuje odgovornosti in ukrepe za njihovo izvajanje. Organizacija lahko tudi zavestno sprejme tveganje, ki je višje od sprejemljivega, vendar ga mora ustrezno obravnavati, vsekakor pa sprejetje mora odobriti vodstvo.
Tveganja lahko prenesemo tudi na tretjo osebo. Za to se odločimo, če ugotovimo, da se tveganju ni mogoče izogniti, oziroma je zmanjševanje tveganj za organizacijo prezahtevno ali pa si ga zaradi visokih stroškov ne more privoščiti. V tem primeru je zelo pomembno, da se organizacija, na katero je tveganje preneseno, zaveda tveganj in je sposobna z njimi upravljati. To urejamo s posebnimi pogodbami ali zavarovalnini sporazumi, kjer točno opredelimo svoje varnostne zahteve, kontrolne cilje. To je pomembno še posebej zato, ker kljub prenosu tveganja na tretjo osebo odgovornost za varnost informacij in neprekinjeno poslovanju ostaja še vedno naša [Plate, 2002e]. Primeri prenosa tveganj na tretjo osebo so varnostna služba, spletno gostovanje, zavarovanje …
Pri iskanju primerne tretje osebe, na katero bi prenesli tveganje, bi nam bilo v veliko pomoč, če bi ta podjetja že bila certificirana po BS 7799 ali imela vsaj dokazila o skladnem delovanju s tem standardom.

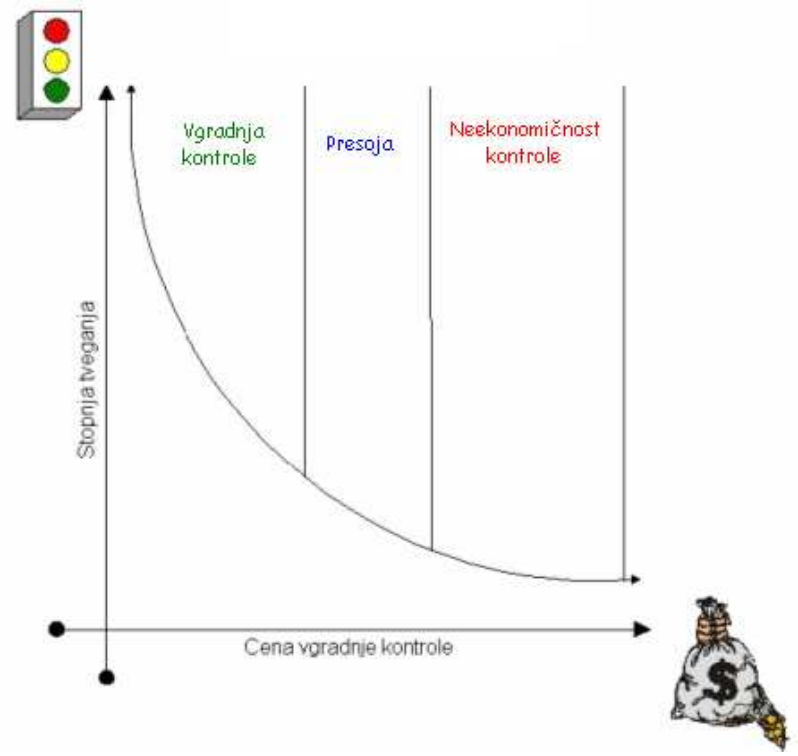
Slika 9: Dejavniki izbire kontrol



Vir: Janežič, 2004

Tveganju se je skoraj nemogoče izogniti, razen če izpostavljeno sredstvo umaknemo s področja tveganja. To pa je v praksi največkrat neizvedljivo. Ne glede na rešitev nekaj tveganja vedno ostaja, kajti informacijskega sistema nikoli ni možno popolnoma zavarovati. Za končno oceno vpeljave kontrol je potrebno rezultate stalno preverjati [Plate, 2002b].

Slika 10: Upravičenost implementacije kontrole



Vir: Janežič, 2004

4.1.2.2. Upravljanje virov in sredstev

Za dobro delovanje SUVI so potrebni tako viri kot tudi sredstva, kot so ljudje, denar in čas. Organizacija mora priskrbeti vire, ki bodo zadolženi za načrtovanje, vpeljavo, delovanje in vzdrževanje SUVI.

4.1.2.3. Izobraževanje in ozaveščanje

Izobraževanje in ozaveščanje je eno ključnih področij za dosego uspešnega SUVI. Če ne poznamo problematike informacijske varnosti, če ne vemo, čemu so namenjena vsa pravila, omejitve in kontrole, potem SUVI ne more zadostno delovati. Ključnega pomena je prenos znanja na vodstvo, delavce, pogodbene stranke in poslovne partnerje. S tem postavljamo trdne temelje za upravljanje tveganj in kulturo varnosti. Izobraževanja naj se izvajajo ciklično, kajti problematika informacijske varnosti se s časom zelo hitro spreminja. Hkrati s tem pa se ponovno osvežuje znanje. Seveda morajo biti izobraževanja različna glede na to, ali gre za vodstvo, uporabnike ali ključne uporabnike informacijskih sredstev. Vsekakor pa morajo biti trendi, nevarnosti in ukrepi za varovanje s področja informacijske varnosti stvar osnovnega izobraževanja uporabnikov še preden začnejo delati z informacijskimi sredstvi, pa tudi ves čas uporabe le-teh. Način podajanja znanja naj bo skladen z družbenimi, kulturnimi in psihološkimi vidiki. Izobraževanje se lahko izvaja preko predavanj, seminarjev, delavnic, vaj, multimedije, interneta, časopisa, plakatov …[BS ISO/IEC TR 13335 Part 2, 1999].
Uporabniki naj po koncu izobraževanja podpišejo Izjavo o varovanju informacij. S podpisom izjavljajo, da so z informacijsko varnostno politiko seznanjeni in da se z njo

strinjajo. S tem se strinjajo tudi s sankcioniranjem kršitev. Izjava o varovanju informacij se nahaja v prilogi 2.

4.1.2.4. Odkrivanje varnostnih incidentov

Varnostne incidente je potrebno čim prej odkriti in preprečiti škodo. Moramo jih tudi natančno zabeležiti in o njih voditi evidenco in dokaze. Poročilo o incidentu se nahaja v prilogi 4.
Za ta namen moramo uvesti sistem sporočanj, preko katerega lahko vsak posameznik sporoči, kakšen incident se je zgodil, kdo (če je znano) ga je povzročil in kakšna škoda je bila s tem povzročena.
Vsak incident posebej je potrebno natančno analizirati ter določiti protiukrepe (preventivi ali korektivni ukrep), ki v bodoče preprečujejo ponovitev. Določiti je potrebno nosilca in pa rok uvedbe protiukrepa, kar je potrebno tudi ustrezno kontrolirati.

4.1.3. Preveri

Tretji del cikla NSPU je Preveri. To je faza, v kateri preverjamo izvedeno z načrtovanim.
V tej fazi so potrebni:

- samoupravljavski postopki,
- notranje presoje,
- vodstveni pregledi,
- spremljanje in analiza trendov.

4.1.3.1. Samoupravljavski postopki

Samoupravljalski postopki so namenjeni takojšnjemu odkrivanju napak, do katerih prihaja med delovanjem sistema. Če je to izvedljivo, že sam postopek napako odpravi ali pa o njej obvesti odgovorno osebo. Če je dogodek za organizacijo varnostno zelo pomemben, mora biti o tem obveščeno tudi vodstvo. Smiselno je, da se vsi ti dogodke tudi beležijo, nadzorujejo in analizirajo.

4.1.3.2. Notranja presoja SUVI

Interna presoja informacijskih sistemov vsebuje enake metodološke postopke, kakor jih uporablja revizija računovodskih izkazov. Mednarodna združenja presojevalcev informacijskih sistemov določajo standarde za izvajanje notranjih presoj (ISACA) [Šušnjar, 2000]. Namen notranje presoje je pregledati delovanje SUVI in ga primerjati z načrtovanim. Izvaja naj se periodično, po vnaprej določenih intervalih, najmanj pa enkrat letno. Načrtovana mora biti tako, da se v predvidenem intervalu pregleda celotno področje SUVI. Notranja presoja mora vodstvu pokazati ali:

- se za oceno tveganj uporablja pravilna metoda,
- se uporabljajo dokumentirani postopki,
- ti postopki dosegajo želene cilje,
- so tehnične kontrole pravilno nameščene in delujejo v skladu s pričakovanjem,
- so preostanki tveganj pravilno ocenjeni in še sprejemljivi za vodstvo,

- so izvedeni korektivni ukrepi, ugotovljeni na prejšnji notranji presoji,
- je SUVI skladen s standardom BS 7799.

V notranji presoji se vzorčno pregleda tudi dokumentacija SUVI.

4.1.3.3. Vodstveni pregled

Vodstvo podjetja načrtovano periodično pregleduje SUVI ter ovrednoti, ali je še v skladu s poslovnimi zahtevami. Osnova za pregled so periodična poročila o rezultatih poslovanja, o stanju korektivnih in preventivnih ukrepov, o ukrepih iz predhodnih pregledov in morebitne spremembe v okolju, ki bi lahko vplivale na SUVI. Na osnovi pregleda se načrtujejo korekcije in izboljšave SUVI. Za načrtovanje sprememb se določijo odgovorni nosilci, roki in ocenjena sredstva. Rezultati pregledov se dokumentirajo v obliki izjave vodstva o primernosti SUVI in zahteve za morebitne ukrepe in izboljšave.

4.1.3.4. Spremljanje in analiza trendov

Področje informatike je dokaj turbulentno in edina stalnica tu so spremembe. Le redno spremljanje in analizira trendov na področju SUVI lahko pomagata organizaciji, da se na nevarnosti, ki ji pretijo, tudi primerno pripravi in odzove.

4.1.4. Ukrepaj

Četrti del cikla NSPU je Ukrepaj. To je faza, v kateri izvajamo izboljšave in odpravljamo nepravilnosti, ugotovljene v fazi Preveri.
V tej fazi je potrebno:

- analizirati neskladnosti,
- izvajati preventivne in korektivne ukrepe,
- sankcionirati kršitve.

4.1.4.1. Analiza neskladnosti

Neskladnost pomeni odstopanje od predvidenega delovanja. Za področje SUVI je potrebno ponovno preiskati glavne vzroke za neskladja (ugotovljena v fazi Preveri) in zanje poiskati ukrepe, ki jih odpravijo in preprečijo njihovo ponovitev.

4.1.4.2. Preventivni in korektivni ukrepi

Korektivni ukrepi se izvajajo z nalogo odstranitve neskladnosti in preprečevanja njihovega ponovnega nastaneka. Korektivni ukrep je zasnovan na opisu neskladnosti, analizi podatkov in ugotovitvi osnovnega vzroka ter oceni potreb po ukrepih, s katerimi se zagotovi, da se neskladnosti ne ponovijo. Določi se izvedba ukrepa, zaključi pa se s poročilom o izvedbi in s pregledom učinkovitosti izvedbe.

Preventivni ukrepi pa preprečujejo nastanek neskladnosti s tem, da predhodno odstranijo razloge za nastanek. Proces preventivnih ukrepov temelji na opisu potencialnih neskladnosti, analizi podatkov in oceni potreb za ukrepanje z namenom, da se prepreči morebitno odstopanje. Prav tako je potrebno določiti izvedbo ukrepa ter zaključiti s poročilom o izvedbi. Preveriti je potrebno tudi učinkovitost izvedbe. Tudi izobraževanje in usposabljanje vseh zaposlenih sta pomembni preventivni dejavnosti.

4.1.4.3. Sankcioniranje kršitev

Za varovanje informacij so odgovorni vsi zaposleni. Če so o informacijski varnosti tudi primerno izobraženi, vsako odstopanje od predpisanega pomeni lažjo ali težjo kršitev delovne obveznosti. Le-to ima podjetje pravico in dolžnost sankcionirati. Sankcije so odvisne od teže kršitve in se gibljejo od opomina disciplinske komisije do odpusta iz organizacije in povračila povzročene škode.

4.2. Vloge in odgovornosti

Sistem varovanja informacij v organizaciji predstavlja nabor različnih vlog (slika 11) in njihovih odgovornosti. Pomembno je poudariti, da mora biti vsaka vloga jasno opredeljena z vidika odgovornosti, pristojnosti in dolžnosti [Berčič, 2003a]. Vse naloge in pristojnosti morajo biti zabeležene tudi v dokumentaciji SUVI, seveda pa morajo biti zaradi svojih odgovornosti tudi primerno ovrednotene.

Za izvajanje SUVI so v podjetju odgovorni:

- vodstvo organizacije,
- pooblaščenec za informacijsko varnost (vodja informacijske varnosti),
- varnostni forum,
- krizni timi,
- vsi zaposleni, pogodbeni partnerji in stranke.

Poleg njih pa v SUVI ponavadi sodelujejo še:

- zunanji svetovalci in
- akreditirana certifikacijska hiša.

Slika 11: Organizacijska shema vlog v SUVI

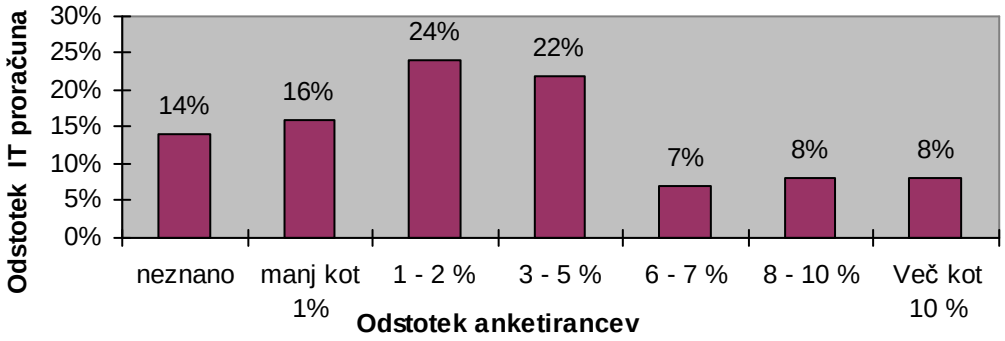
Vir: Berčič, 2003a

4.2.1. Vodstvo organizacije

Vodstvo ima nalogo skrbeti za dolgoročen obstoj in poslovanje organizacije. To pa je v veliki meri povezano tudi z ustreznim nivojem varovanja informacij. Zavedati se moramo, da se varnost ne konča pri fizični varnosti, temveč zahteva tudi aktivnosti, kot so upravljanje z znanjem, ljudmi, opremo, poslovnimi procesi in zagotavljanje nemotenega poslovanja. Vse te aktivnosti so nujno potrebne za dolgoročno poslovanje organizacije.
Zato se mora vodstvo zavezati, da:

- prepoznava varovanje informacij kot eno kritičnih poslovnih področij,
- bo podpiralo vpeljevanje SUVI,
- bo definiralo obseg in opis področij ter poslovnih procesov, ki so kritični za poslovanje organizacije in s tem prioritetni za varovanje,
- bo definiralo cilje SUVI, ki bodo povezani s poslovnimi cilji in strateškimi usmeritvami organizacije,
- bo priskrbelo vire in sredstva za uspešno uvedbo in delovanje SUVI (glej tabelo 6),
- bo določilo sprejemljiv nivo tveganja,
- bo izvajalo vodstvene preglede SUVI [Plate, 2002a].

Tabela 5: Odstotki proračuna za IT, porabljeni za informacijsko varnost



Vir: CSI/FBI, 2004

Tabela 5 kaže, da se vodstvo pomena informacijske varnost še vedno ne zaveda dovolj. V raziskavi, ki jo že deveto leto zapored izvajata CSI in FBI in v kateri sodeluje 494 največjih ameriških organizacij, rezultati kažejo, da največ organizacij za informacijsko varnost porabi med ena in pet procenti proračuna za informatiko.

4.2.2. Pooblaščenec za informacijsko varnost

Večje organizacije (multinacionalke, banke, zavarovalnice ...) večinoma ustanovijo oddelek Informacijska varnost, ki ga vodi vodja informacijske varnosti. Če je organizacija srednja ali manjša (večina slovenskih organizacij), pa je možna tudi uvedba pooblaščenca za informacijsko varnost. Ne glede na velikost in naziv je njegova naloga strokovno svetovanje s področja varovanja informacij, obenem pa prevzema celotno odgovornost za razvoj in vpeljavo varovanja ter določa način kontrole. Poleg tega mora vzpostavljati stike z zunanjimi strokovnjaki za varovanje, nadzorovati mora standarde, ocenjevati metode ter priskrbeti ustrezno pomoč v primeru incidentov v varnostnem sistemu. Spodbujati mora multidisciplinarni pristop k varovanju informacij, kar pomeni spodbujanje sodelovanja med vodstvom organizacije, uporabniki, skrbniki, načrtovalci aplikacij, revizorji, varnostnim osebjem ter strokovnjaki na področjih, kot sta varovanje in upravljanje tveganj.

4.2.3. Odbor za upravljanje varovanja (Varnostni forum)

Odbor za upravljanje varovanja ponavadi sestavljajo člani, ki so vodje posameznih delov organizacije.
Njihove naloge v SUVI so:

- pregled in potrjevanje dokumentov informacijske varnostne politike skupaj z ukrepi za izvedbo posamezne politike,
- spremljanje pomembnih sprememb na informacijskih sredstvih, ki jih povzroči izpostavljenost različnim nevarnostim,
- spremljanje in analiza incidentov pri varovanju informacij,
- odobravanje pomembnejših pobud za izboljšanje varovanja informacij [Plate, 2002d].

4.2.4. Krizni timi

Krizne time sestavljajo strokovnjaki za posamezna področja.
Njihova naloga je, da v primeru incidenta, kritičnega za delovanje organizacije, tega nemudoma analizirajo in izvedejo vse ukrepe za takojšnjo rešitev situacije in sanacijo nastale škode. Njihove naloge in tudi scenariji reševanja za različne situacije morajo biti že vnaprej znani, dokumentirani in preizkušeni. Glej prilogo 7 (Zadolžitve in postopki v primeru izpada posameznega informacijskega sredstva).

4.2.5. Vsi zaposleni, pogodbeni partnerji, stranke

Vsekakor pa SUVI brez sodelovanja vseh zaposlenih, pogodbenih partnerjev in strank ne more uspeti. Vse to pa lahko dosežemo poleg uzakonjanja politik, navodil in standardov le s stalnim ozaveščanjem in izobraževanjem. Standard prav tako predpisuje podpis izjave o varovanju informacij s strani vseh zaposlenih in pogodbenih partnerjev, pa tudi sankcije za posamezne kršitve. Vsekakor je za vse smiselno uvesti podpis izjave o varovanju informacij. S to izjavo se zavezujejo k varovanju informacij, hkrati pa se zavedajo, da se vsaka kršitev primerno sankcionira. Glej prilogo 2 (Izjava o varovanju informacij).

4.2.6. Zunanji svetovalci

Zunanji svetovalci s področja informacijske varnosti nam pri delovanju SUVI, predvsem pa pri njegovi uvedbi, veliko pomagajo. S svojimi izkušnjami so nam lahko v pomoč v različnih fazah uvedbe in delovanja SUVI, lahko pa projekt prevzamejo v celoti. Največkrat je smiselno, da z njimi sodelujemo na začetku projekta uvedbe, kjer animiramo vodstvo, analiziramo stanje, določamo obseg SUVI in izvajamo analizo tveganj. Seveda pa je strokovno mnenje zunanjih svetovalcev neobhodno tudi pri izbiri in implementaciji posameznih tehničnih rešitev, kot so požarna pregrada in protivirusna zaščita.

4.2.7. Akreditirana certifikacijska hiša

Ko enkrat SUVI uspešno uvedemo in ta že nekaj časa zadovoljivo deluje, je smiselno, da uspeh okronamo še z uradnim potrdilom o uspešnosti, to je s certifikatom. Trenutno v Sloveniji še ni hiše, ki bi smela samostojno podeljevati certifikat BS 7799. Lahko pa pod okriljem tujih certifikacijkih hiš ta standard pri nas podelijo BSI, BVQI, TUV, SIQ.

4.3. Varnostna politika

Slika 12: Večnivojska ureditev varnostne politike

Vir: Rakovec, 2005b

Dokumentacija SUVI je lahko kar zajetna, zato jo je smiselno hierarhično strukturirati. Priporočljivo je, da varnostno politiko ločimo na tri nivoje, in sicer:

- krovna varnostna politika na najvišjem nivoju,
- varnostne politike za posamezna področja (podpolitike) na srednjem nivoju in
- delovna navodila, procedure in obrazci na najnižjem nivoju [Rakovec, 2005a].

Z nivoji dosežemo prehod od strateških usmeritev in ciljev prek mehanizmov do konkretnih postopkov in tehnologij, ki se bodo uporabili za izpolnitev zastavljenih ciljev. Cilji so dolgoročni in niso vezani samo na trenutno obdobje, tehnologija, ki je na voljo za varovanje informacijskih virov, pa se s časom spreminja. Z ločitvijo v nivoje dosežemo tudi boljšo preglednost dokumentacije in tudi možnost, da do različnega nivoja dokumentov dostopajo različni uporabniki.

4.3.1. Krovna varnostna politika

Na najvišjem nivoju naj bo krovna varnostna politika, ki predstavlja temeljni dokument za varovanje informacij v podjetju. Osnovni cilj dokumenta je pridobivanje podpore in priprava organizacije na izgradnjo celovitega sistema varovanja. Zato naj krovna varnostna politika vsebuje:

- potrditev varnostne politike s strani vodstva,
- namen in cilje varnostne politike,
- vloge in odgovornosti,
- temeljna načela delovanja,
- organizacijo dokumentacije,
- usklajenost,
- notranji in zunanji nadzor,

- pregled varnostnih politik za posamezna področja,
- postopek prijave varnostnih incidentov,
- sankcije kršitev,
- veljavnost varnostne politike.

4.3.2. Varnostne politike za posamezna področja

Varnostne politike za posamezna področja so dokumenti srednjega nivoja, ki natančneje opisujejo posamezna področja in sklope, a še vedno ne omenjajo imen konkretnih oseb niti konkretne računalniške opreme.
Nekaj primerov varnostnih politik za posamezna področja:

- politika v zvezi z varovanjem osebja,
- politika elektronske pošte (glej prilogo 5 Primer politike elektronske pošte),
- politika fizičnega varovanja,
- politika varovanja pred zlonamerno programsko kodo,
- politika naročanja storitev pri zunanjih izvajalcih,
- politika izdelovanja, preverjanja in hranjenja varnostnih kopij,
- politika uporabe prenosne računalniške opreme in dela na daljavo,
- politika dodeljevanja in nadzora dostopov,
- politika razvoja in vzdrževanja aplikacijskih sistemov,
- politika upravljanja neprekinjenega poslovanja …

4.3.3. Operativna navodila, interni standardi in postopki za delo

Na najnižjem nivoju dokumentacije pa se nahajajo operativna navodila, interni standardi in postopki za delo, ki pa zelo natančno določajo postopke za posamezna področja.
Nekaj primerov:

- navodilo in postopek prevzema opreme v času zaposlitve in oddaje opreme ob prenehanju zaposlitve,
- deponiranje ključnih gesel,
- prižiganje, ugašanje in delovanje strežnikov,
- pravila dostopov do strežnikov,
- pravila evidentiranja in arhiviranja licenc,
- navodilo za postavitev delovnih postaj,
- navodilo za standardno namestitev operacijskega sistema na delovni postaji,
- navodilo za shranjevanje dokumentov,
- zahtevek za dodelitev/ukinitev uporabniških pravic (glej prilogo 6).

4.3.4. Porazdelitev kontrol v politikah

Za vse tri nivoje dokumentacije je smiselno izdelati spisek kontrol, ki so vključene znotraj posameznih politik .
Primer Krovne varnostne politike (prvi nivo) in Politike fizičnega varovanja (drugi nivo).

Krovna varnostna politika:

Spisek kontrol po standardu BS 7799:
3.1. Politika varovanja informacij
    3.1.1. Dokument o politiki varovanja informacij
    3.1.2. Pregled in ocena
4.1.3. Dodeljevanje odgovornosti za varovanje informacij
12.2.1. Združljivost z varnostno politiko
12.2.2. Preverjanje tehnične združljivosti

Politika fizičnega varovanja:

Spisek kontrol po standardu BS 7799:
7.1. Varovana območja
    7.1.1. Fizični varnostni pas
    7.1.2. Kontrole fizičnega dostopa
    7.1.3. Varovanje pisarn, sob in naprav
    7.1.4. Delo v varovanih območjih
    7.1.5. Ločeno območje za dostavo in odpošiljanje
7.2. Varovanje opreme
    7.2.1. Namestitev in zaščita opreme
    7.2.2. Oskrba z energijo
    7.2.3. Varovanje kabelskih vodov
    7.2.4. Vzdrževanje opreme
    7.2.5. Varovanje opreme izven prostorov organizacije
    7.2.6. Varno uničenje ali ponovna uporaba opreme
7.3. Splošne kontrole
    7.3.1. Politika čiste mize in praznega ekrana
    7.3.2. Odstranitev lastnine
8.6. Varno upravljanje z nosilci podatkov
    8.6.1. Ravnanje z zamenljivimi računalniškimi nosilci podatkov
    8.6.2. Odstranitev nosilcev podatkov
    8.6.3. Postopki ravnanja z informacijami
    8.6.4. Varovanje sistemske dokumentacije
8.7.2. Varovanje nosilcev podatkov med prenosom
12.1.5. Preprečevanje zlorabe opreme za obdelavo informacij

4.4 Ključni dejavniki uspeha

Za uspešno uvedbo SUVI v organizacijo moramo upoštevati kar nekaj dejavnikov, posebej pa moramo biti pozorni na:

- dobro varnostno politiko, ki odraža poslovne cilje organizacije,
- podporo in vključenost vodstva organizacije,
- dobro analizo trenutnega stanja in oceno tveganj,
- izkušeno, dobro motivirano projektno skupino,
- jasno določene odgovornosti in pristojnosti za varovanje informacij,
- dobro pripravljeno in periodično izpeljano izobraževanje uporabnikov,
- posredovanje splošnih smernic varovanja informacij vsem zaposlenim in pogodbenim partnerjem,

- računalniško podprt sistem kreiranja, dokumentiranja, pregledovanja, odobravanja, distribucije in spreminjanja dokumentov,
- v delovne procese integriran nadzorni sistem nad izvajanjem varnostne politike,
- učinkovite ukrepe ob odstopanju od politike varovanja informacij.

Uvajanje SUVI v organizacijo, tako kot vse inovacije, pri ljudeh povzroča nek strah, negotovost in odpor do novega. Stare utečene navade zamenjuje nekaj novega, sodobnega. Zato je nujno, da tako vodstvo kot vse ostale zaposlene o nujnosti in pozitivnem namenu sprememb predhodno dobro ozavestimo. Kajti če zaposleni ne bodo vedeli, kaj je smisel informacijske varnosti, kaj s tem pridobimo, kako ogroženi smo,… potem tega ne bodo vzeli resno, projekt pa bo neuspešen.

4.5. Stroškovna upravičenost vlaganja v informacijsko varnost

Stroškovni vidik varovanja informacij je zelo pomemben, kajti brez analize donosa investicije v varovanje se hitro lahko zgodi, da stroški varovanja presežejo vrednost informacij ali sredstev, ki jih varujemo. Zato moramo kot prvo določiti vrednost posameznih informacij in sredstev. Vrednost določimo na podlagi vpliva, ki ga imajo informacije ali sredstva na poslovanje, in glede na škodo za poslovanje, ki jo lahko povzroči izguba karakterističnih lastnosti informacij ali sredstev:

- zaupnosti,
- celovitosti,
- razpoložljivosti.

Poslovne posledice se lahko odražajo na različnih področjih poslovanja. Izbranim informacijam ali sredstvom določimo vrednost glede na posledico, ki poslovanje najbolj prizadene, torej na podlagi najhujšega možnega scenarija. Posledice se lahko kažejo na področjih:

- poslovnih interesov,
- finančnih izgub,
- zakonskih kršitev,
- ugleda podjetja,
- varnosti osebja ter
- družbe, okolja in prostora.

Ko določimo vrednost, moramo določiti ukrepe (kontrole), ki te informacije in sredstva varujejo. Seveda moramo tudi te ukrepe ovrednotiti. S tem ugotovimo, koliko nas varovanje določenih informacij in sredstev. Na koncu moramo vedno analizirati, ali bomo z novimi ukrepi za preprečevanje nastajanja škode in njihovimi stroški v boljšem položaju, kot smo sedaj. Ugotovimo lahko, da:

- Ukrepi ne povečajo varnosti.
- Ukrepi povečajo varnost, vendar so stroški varovanja višji od vrednosti informacij ali sredstev, oziroma stroškov njihove izgube.
- Ukrepi povečajo varnost, stroški varovanja pa so nižji od vrednosti informacij ali sredstev, oziroma stroškov njihove izgube [Jaušovec, 2003].

Za uvedbo je sprejemljiva le zadnja možnost.

Vodstva organizacij velikokrat vidijo varnost kot velik strošek. Vendar ni vedno tako. Veliko varnostnih ukrepov oziroma kontrol je organizacijske narave in ne predstavlja večjih stroškov. Predvsem imam v mislih pisanje varnostnih politik, predpisov ter navodil za delo, njihovo spoštovanje, izobraževanje, interne revizije, evidentiranje sprememb, popravkov, razvrstitev vlog in odgovornosti ... Vse to lahko izvedejo zaposleni znotraj organizacije brez večjih stroškov. Za vsa ostala vlaganja v varovanje, kot so fizična varovanja, video nadzor, požarna pregrada, sistem javnih in privatnih ključev, uporaba biometrije, zavarovanje, pa je predhodno vedno potrebno izdelati analizo upravičenosti vlaganja (ROI). Organizacije velikokrat ločeno uvajajo različne sisteme vodenja (ISO 9000, ISO 14000, BS 7799 …). Ko govorimo o upravičenosti stroškov uvajanja in delovanja teh sistemov, je njihova integracija nujna, predvsem z enotnim sistemom vodenja in enotnim dokumentnim sistemom [Tič, 2004]. Organizacija naj za varovanje informacij uvede sistem (SUVI). Kajti tu ne gre za »ad hoc« akcije, kjer se rešuje vsak primer po svoje, pač pa se informacijska varnost obravnava sistematično. Poleg ostalih pozitivnih plati sistematične obravnave ne smemo zanemariti tudi finančne. Ni nujno, da takoj odpravimo vsa tveganja, ki grozijo našim informacijam in virom. V odpravo tveganj oziroma nevarnosti vložimo toliko, kolikor si lahko privoščimo. Ni nujno, da se sploh odločimo za odpravo vseh tveganj. To je lahko za organizacijo prevelik strošek. Lahko se odločimo, da v neki fazi del tveganj odpravimo, del pa zaradi previsokih stroškov sprejmemo. Tega dela tveganja se moramo zavedati in nanj biti še posebej pozorni. Tudi ostala merila informacijske varnosti, ki jih postavlja standard BS 7799, morajo biti finančno upravičena, kajti sama skladnost s standardom brez donosa ne more biti nikoli opravičljiva. SUVI naj se uvaja postopoma. Nesmiselno je začeti delo na več področjih hkrati, ker se lahko zgodi, da bo zaradi obilice dela projekt presegel razumne meje. Uporabniki, pa tudi vodstvo ne bo videlo pozitivnih učinkov, s tem pa projekt počasi zamre, z njim pa tudi vsi vloženi stroški. Zato se je projekta SUVI potrebno lotevati po korakih, in sicer s tempom, ki mu je organizacija sposobna slediti. Upravičenost vlaganja v informacijsko varnost je podobna zavarovanju stavb, avtomobilov ter življenjskim zavarovanjem. Želimo si, da zavarovanja nikoli ne bi potrebovali, ne smemo pa si privoščiti, da ga ne bi imeli.

Analiza upravičenosti vlaganja v informacijsko varnost je vsekakor nujna, vendar bi natančnejša obravnava te teme presegla okvir naloge, v kateri sem se prioritetno lotil primerjave trenutnega stanja s standardom BS 7799.

5. PODJETJE ISKRAEMECO, D. D.

5.1. Predstavitev podjetja

V podjetju Iskraemeco uspešno združujemo izkušnje z inovacijami in novimi tehnologijami pri zadovoljevanju različnih potreb na področju merjenja in obračuna porabe električne energije. Po prodaji števcev se uvrščamo med največje na svetu, izdelke z našo blagovno znamko poznajo danes že v skoraj sto državah na vseh petih kontinentih. Iskraemeco je danes na trgu sistemski ponudnik opreme, svojo ponudbo pa razširjamo tudi na storitve s področja merjenja in obračuna energije. Odpiranje trga električne energije ponuja vrsto možnosti za nove izdelke in rešitve, ki so velik izziv za naše strokovnjake. Začetek družbe Iskraemeco, d. d. sega v leto 1945, proizvodnja enofaznih elektromehanskih števcev teče v Kranju že od leta 1946. Mehansko tehnologijo smo nadgradili z elektronsko, leta 1975 smo začeli proizvajati elektronske precizijske števce. Do današnjega dne smo kupcem dobavili več kot 40 milijonov izdelkov, od tega skoraj 2

milijona v elektronski izvedbi. Leta 1986 smo postavili prvi sistem za merjenje in obračun električne energije. Ponosni smo na dejstvo, da so vsi izdelki iz našega programa plod lastnega znanja, zasnovani na številnih lastnih patentih [Predstavitev podjetja, 2003].

Že po prvem desetletju delovanja smo svoje izdelke začeli prodajati na tuje, najprej le v nekaj držav, z leti pa po vsem svetu. Poleg izvoza končnih izdelkov smo se uspešno uveljavili tudi s prenosi tehnologije in s prodajo licence za proizvodnjo števcev na tujih trgih. Zadnjih deset let sledimo težnji po globalizaciji tako, da se uporabnikom na različnih trgih približujemo z ustanavljanjem lastnih podjetij in podjetij v mešani lasti. Danes ima skupina Iskraemeco poleg matične družbe v Kranju še 8 proizvodnih podjetij z različnim lastninskim deležem, 4 lastna trgovska podjetja in licenčno proizvodnjo pri treh partnerjih.

Osnova razvojne politike Iskraemeca je lasten koncept števcev, naprav in sistemov za merjenje in obračun v energetiki. Naši izdelki zadovoljujejo potrebe kupcev in rešujejo njihove probleme na odprtih trgih z električno energijo. Izpolnjujejo zahteve veljavnih mednarodnih standardov in zakonodaje. Hitre spremembe na trgu z energijo vsako leto prinašajo nove izzive, vstopanje na nove trge zahteva stalne tehnične spremembe in prilagoditve. Pripravljeni smo prisluhniti potrebam kupcev, saj nam to omogoča fleksibilna zgradba naših izdelkov. V organizaciji razvijamo, proizvajamo in tržimo naprave ter sisteme za merjenje in obračun porabe električne energije tako v gospodinjstvih, industriji kakor tudi v elektroenergetskih prenosnih sistemih. Poleg izdelkov ponujamo tudi svetovanje, izdelavo projektov in inženiring.

5.2. Izzivi, vizija in poslanstvo

Odpiranje trga električne energije, globalizacija in tehnološki napredek so naši izzivi za prihodnost. Naše delovanje bo tudi naprej usklajeno z našim poslanstvom – s svojimi izdelki, sistemi in storitvami omogočamo učinkovito rabo energije. Trgu bomo ponujali celovite rešitve pri merjenju in obračunu energije za vse nivoje odjemalcev. Še naprej bomo upoštevali zahteve kupcev in širili ponudbo industrijskih števcev ter sistemov za merjenje in upravljanje električne energije. Vse svoje sile bomo usmerili tudi v razvijanje sistemov za vodenje in obračun energije za pokrivanje potreb odprtih trgov. Delovali bomo še bolj globalno in si tako okrepili svoje mesto med vodilnimi ponudniki tovrstne opreme. Uporabnikom po vsem svetu se bomo približevali z načrtovanim prenosom proizvodnje, prodajne in inženiring dejavnosti v njihovo domače okolje [Prodajni program, 2004]. Z odpiranjem trga energije se spreminja položaj naših kupcev – elektrogospodarskih družb, ki jim naš proizvodni program omogoča boljše poslovanje. Le-te izgubljajo monopolni položaj in prehajajo na tržne odnose. Za Iskraemeco to na eni strani prinaša zaostritev razmer poslovanja, na drugi strani pa se odpirajo možnosti za prodajo novih izdelkov in celotnih sistemov.V organizaciji razvijamo nove generacije elektronskih števcev. Števec energije se vse bolj spreminja v kompleksno napravo, ki poleg osnovnega merjenja opravlja vrsto dodatnih funkcij. Naša pozornost je tako vse bolj uprta v razvoj komunikacij, dodatnih funkcij in v programsko opremo kot podporo pri povezovanju števcev v sisteme. Delo naših razvojnih strokovnjakov je v koraku s svetovnimi trendi na tem področju. Z razvojno raziskovalno dejavnostjo si podjetje zagotavlja samostojno in uspešno rast, trgu pa ponuja kakovostne in konkurenčne izdelke, ki so plod lastnega inovativnega dela in znanja.

5.3. Celovit sistem vodenja stalnih izboljšav

Zavedamo se, da je med najpomembnejšimi dejavniki uspeha podjetja uskladitev želja kupcev in lastnikov z zadovoljstvom zaposlenih ob upoštevanju zakonodaje in varovanja okolja v celotnem procesu poslovanja. Zato smo v letu 2001 sistema kakovosti in varstva okolja preoblikovali v integrirani sistem vodenja poslovanja, ki združuje sisteme od vodenja kakovosti, ravnanja z okoljem, kakovosti laboratorijev do finančnega vodenja, prava, varnosti in zdravja pri delu ter varnosti premoženja in podatkov. Celoviti sistem vodenja poslovanja temelji na procesnem modelu stalnih izboljšav, ki je določen v standardih ISO9000:2000. Celovito vodenje izboljšav (Total Improvement Management) z vključevanjem ustvarjalnosti vseh zaposlenih smo vnesli v politiko vodenja poslovanja, da se lažje in bolje prilagajamo spremembam v okolju, ki pritiskajo na izboljšanje kakovosti poslovanja. Timsko delo na vseh nivojih družbe je temelj, na katerem izboljšujemo konkurenčnost, kakovost izdelkov, procesov in storitev ter s tem povečujemo učinkovitost in zadovoljstvo kupcev, zaposlenih in lastnikov [Inegrirani poslovnik vodenja, 2002]. Sistem kakovosti poslovanja formalno periodično preverjamo z notranjimi in zunanjimi presojami že od leta 1992, ko smo usvojili standard ISO 9001. Merilni laboratoriji so akreditirani po standardu SIST EN ISO/IEC 17025, s katerim je usklajena tudi končna kontrola. Po lastnih standardih nas nenehno preverjajo tudi kupci. Glede na zakonodajo v posameznih državah smo že pridobili certifikate za prvo overjanje števcev v nekaterih evropskih državah.
Po pridobitvi certifikata za sistem ravnanja z okoljem po standardu ISO14001 v letu 1999 le-tega stalno dopolnjujemo in izboljšujemo tudi zaradi večje konkurenčnosti na svetovnem trgu in zaradi zadovoljevanja zahtev naših kupcev, hkrati pa s tem izboljšujemo tudi svoj odnos do okolja z vseh okoljskih vidikov. Pozitiven odnos do okolja izkazujemo tudi z letnimi poročili, iz katerih so razvidni stalni trendi upadanja in zmanjševanja negativnih vplivov na okolje: manjša poraba pitne vode, energije in nevarnih snovi, manjše količine odpadnih voda z nižjimi koncentracijami nevarnih snovi, manjše količine odpadkov in emisije v zrak. To dosegamo z letnimi programi za ravnanje z okoljem ter s stalnim usposabljanjem zaposlenih v dejavnostih in storitvah, ki imajo pomemben vpliv na okolje. Pri načrtovanju in razvoju novih izdelkov upoštevamo okoljske zahteve in naredimo okoljske ocenitve izdelkov tudi v smislu ravnanja z njimi po preteku življenjske dobe.

5.4. Organizacijska struktura

Organizacijsko je podjetje Iskraemeco sestavljeno iz petčlanske Uprave (predsednik Uprave ter štirje člani), dveh poslovnih enot (Indukcijski števci in Elektronski števci) in dvanajstih poslovnih funkcij. Poslovni enoti Indukcijski števci in Elektronski števci še naprej združujeta poslovne funkcije, ki so deljive po tehnologiji izdelka, in sicer: planiranje proizvodnje, nabavo, tehnologijo, proizvodnjo in kontrolo proizvodnje. Funkcije in službe, ki so neposredno podrejene Upravi in se ne delijo po tehnologiji izdelka, so organizirane v enovite poslovne funkcije. Poslovne enote in poslovne funkcije so organizacijsko razdeljene na oddelke, službe, odseke, obrate in temeljne enote dela. Zaradi lažjega koordiniranja posameznih poslovnih enot in poslovnih funkcij je koordinacija le-teh razdeljena med posamezne člane uprave [Organizacijska shema, 2004].

5.5. Informacijski sistem

Razdelitev informacijskega sistema v organizaciji je prikazana v tabeli 6.

Tabela 6: Informacijski sistem v organizaciji

skupina	podskupina	naloge
sistemi	strežniki in omrežja	OS strežnikov (IBM AIX, Microsoft Windows NT, 2003 Server)
		podatkovne baze Informix, DB2, Microsoft SQL, Oracle
		glavno in pomožna omrežna vozlišča (usmerjevalniki in stikala)
		požarni zid
		poštni strežnik (SMTP in POP3 oz. IMAP)
		spletni strežnik (Lotus Domino)
		Lotus Notes strežnik
		Baan (sistemski del)
		datotečni in tiskalniški strežniki
	delovne postaje	strojna oprema (OE Razvoj, merilne delovne postaje, ostale delovne postaje)
		OS delovnih postaj (Windows 95, NT, 98, ME, 2000, XP in SGI, linux?)
		standardne aplikacije (pisarniški paket – urejevalnik, preglednica, predstavitve, WinZip, Acrobat reader, LN odjemalec, Citrix odjemalci, protivirus, Baan odjemalci – Reflection, grafični pregledovalci – RFANView, odjemalci za DIS – Metacube Explorer, ShowBusiness, MicroStrategy …)
		posebne aplikacije (AutoCAD, CorelDraw, Photoshop …)
		osrednje upravljanje uporabnikov (aktivni direktorij in NT domene)
aplikacije	Lotus Notes	upravljanje z e-pošto in vse ostale lastne aplikacije v okviru LN
	Baan	standardni deli, posebni deli, vmesniki do Baan-a (Cordys)
	direktorski informacijski sistem (DIS) in podatkovno skladišče (DW)	zajem podatkov iz različnih virov, obdelava in predstavitev za končne uporabnike (ETL)
	ostale lastne aplikacije	ACIS, spletna predstavitev, kontrola/proizvodnja v Elektroniki PIS – Proizvodni Informacijski Sistem …

Vir: Interno gradivo organizacije

6. ANALIZA ODSTOPANJA IN PREDLOGI ZA DOSEGO SKLADNOSTI Z BS 7799

6.1. Namen

V nalogi sem analizo odstopanj izdelal z namenom seznaniti najvišje vodstvo s trenutnim stanjem informacijske varnosti v proučevani organizaciji. Vodstvo se namreč le redko zaveda širine področja informacijske varnosti, prav tako pa so največkrat premalo seznanjeni z realnim stanjem tega področja. Analiza odstopanja natančno opredeli in analizira celotno področje informacijske varnosti, ki je po standardu BS 7799 razdeljeno na 10 področij, 36 ciljev in 127 kontrol.

Analiza odstopanja je prav tako dobra osnova za oceno tveganj, ki bo naslednji logičen korak v proučevani organizaciji. Daje nam tudi grobo oceno stroškov, potrebnih za dosego skladnosti s standardom, in informacijo o nivoju varnosti v organizaciji. Analizi odstopanj

sem pri vsaki od 127 točk dodal še predlog za dosego skladnosti s standardom BS 7799, s čimer sem organizaciji poleg problemov nakazal tudi rešitev.

6.2. Metoda dela

Analizo odstopanja sem izvedel na dva načina.
Prvi del analize sledi točkam standarda BS 7799, kjer je za vsako od 127 točk analizirano trenutno stanje v organizaciji. Z odgovornimi v organizaciji sem od točke do točke pregledal celotno področje informacijske varnosti, zraven pa sem dodal tudi predloge izboljšav.
Analiza odstopanja po točkah standarda se nahaja od poglavja 6.3 do poglavja 6.12.3.2.

Drugi del analize odstopanj pa je izveden s pomočjo orodja Poslovni ščit.
Poslovni ščit je orodje za vpeljavo in upravljanje informacijskega varnostnega sistema, ki ustreza standardu BS 7799.
Tu je analiza odstopanja zasnovana na osnovi »pametnih« vprašalnikov, ki so jih v organizaciji izpolnile za posamezna področja odgovorne osebe. Rezultati ocenjevanja kažejo trenutno odstopanje organizacije od priporočil standarda BS 7799.
Analiza odstopanja, izvedena s pomočjo orodja Poslovni ščit, se nahaja v poglavju 6.13.

6.3. Varnostna politika

6.3.1. Politika varovanj informacij

Cilj: Zagotoviti, da vodstvo organizacije usmerja in podpira varovanje informacij.

6.3.1.1. Dokument o politiki varovanja informacij

Stanje:
Organizacija nima politike varovanja informacij.

Predlog:
Organizacija naj izdela, vodstvo pa naj potrdi politiko varovanja informacij.
Dokumenti varnostne politike naj se razdelijo v več nivojev. Na najvišjem nivoju naj bo krovna varnostna politika, na srednjem politike za posamezna področja in na najnižjem nivoju navodila, organizacijski predpisi in postopki za delo. Organizacija naj z varnostno politiko seznani vse zaposlene, to naj bo tudi tema uvajalnega seminarja ob vstopu v delovno razmerje. Ob zaključku seminarja naj vsak podpiše izjavo o zaupnosti, s katero potrjuje, da je z varnostno politiko seznanjen, da se zaveda pomena varovanja informacij, ter odgovornosti, ki jih sprejema. S tem sprejme tudi posledice kršenja varnostne politike.

6.3.1.2. Pregled in ocena

Stanje:
Organizacija nima politike varovanja informacij.

Predlog:
Organizacija naj izdela varnostno politiko in določi lastnika, ki je odgovoren za njeno vzdrževanje in redno pregledovanje. Razvije naj postopek, ki opozarja na pregled politike in njene spremembe (incidenti, nove ranljivosti, grožnje, sprememba tehnologije). Časovna razporeditev pregleda politike naj ustreza celotnemu tveganju. O spremembah naj bodo zaposleni redno obveščeni.

6.4. Organiziranost varovanja

6.4.1. Infrastruktura varovanja informacij

Cilj: Upravljanje varovanja informacij v organizaciji.

6.4.1.1. Odbor za upravljanje varovanja informacij

Stanje:
Organizacija nima odbora (foruma) za varovanje informacij.

Predlog:
Ustanovi naj se odbor za varovanje informacij, katerega člani morajo imeti vplivno funkcijo v podjetju. Ponavadi so to kar vodje posameznih delov organizacije.
Člani odbora naj:

- pregledujejo in potrjujejo dokumente informacijske varnostne politike, skupaj z ukrepi za izvedbo posamezne politike,
- spremljajo pomembne spremembe na informacijskih sredstvih, ki jih povzroči izpostavljenost različnim nevarnostim,
- spremljajo in analizirajo incidente pri varovanju informacij,
- odobravajo pomembnejše pobude za izboljšanje varovanja informacij,
- ozaveščanjo in usklajujejo varovanje informacij v svojih oddelkih.

6.4.1.2. Usklajevanje varovanja informacij

Stanje:
Organizacija nima organa za usklajevanje varovanja informacij.

Predlog:

Organizacija je relativno velika, zato predlagam, da bi uvedli tudi usklajevalni odbor, katerega naloge bi bile:

- odobravati vloge in odgovornosti pri varovanju informacij v organizaciji,
- odobravati metodologije in procese za varovanje informacij,
- klasificirati varnost,
- odobravati in podpirati pobude za varovanje informacij v celotni organizaciji, npr. program seznanjanja z varovanjem informacij,
- zagotavljati, da je varnost vključena v procese informacijskega planiranja,
- ocenjevati primernost in usklajevati vpeljavo posebnih kontrol za varovanje informacij v novih sistemih in storitvah,
- pregledovati incidente pri varovanju informacij,
- spodbujati razumevanje poslovnega pomena varovanja informacij v organizaciji.

6.4.1.3. Dodeljevanje odgovornosti za varovanje informacij

Stanje:
V organizaciji obstaja šibka odgovornost za varovanje informacij. Dodeljena in dokumentirana je izključno odgovornost za osnovna sredstva, kot so mize, stoli, osebni računalniki ...

Predlog:
Organizacija naj določi vodjo oziroma pooblaščenca za informacijsko varnost, ki prevzema celotno odgovornost za razvoj in vpeljavo varovanja informacij.
Za vsako posamezno informacijsko sredstvo naj se določi lastnika, ki skrbi za njegovo varovanje. Raven pooblastil in odgovornosti naj se jasno opredeli in dokumentira.

6.4.1.4. Postopek za odobritev zmogljivosti za obdelavo informacij

Stanje:
Organizacija izvaja postopek za odobritev zmogljivosti. Pokriva ga organizacijski predpis OP.M.06.01 Priročnik za naročanje osnovnih sredstev. Ločimo poslovno in tehnično odobritev zmogljivosti. Vsi zahtevki morajo biti zabeleženi, primerno obrazloženi in formalno predloženi. Pri poslovni odobritvi vsak zahtevek po novi zmogljivosti oziroma razširitvi stare najprej pregleda in odobri odgovorni vodja, nato pa zahtevek potrditi še predsednik uprave. Podobno je tudi pri tehnični odobritvi, le da tu poleg vodje vsako zahtevo pregledata še pooblaščenec za okolje, ki preveri, če je predlagano skladno s standardom za varovanje okolja, in pa tehnični skrbnik, ki preveri, če je predlagano združljivo z obstoječim sistemom.

Predlog:
Oprema naj se izbira pazljivo, saj se le tako lahko zagotovi primeren nivo varnosti. Nakupi novih zmogljivosti naj bodo skladni s poslovnimi potrebami organizacije. Vsak nov nakup naj predhodno potrdi pooblaščenec za informacijsko varnost ter s tem potrdi, da oprema ustreza varnostnim zahtevam.

6.4.1.5. Strokovno svetovanje pri varovanju informacij

Stanje:
Organizacija nima vodje oziroma pooblaščenca za informacijsko varnost. Poslužuje se izključno zunanjih svetovalcev, pa še to dokaj neorganizirano, kajti z njimi komunicirajo posamezniki, ki problem zaznajo.

Predlog:
Organizacija naj postavi vodjo oziroma pooblaščenca za informacijsko varnost. Ni nujno, da je strokovnjak za vsa področja informacijske varnosti, nujo pa je, da se vsi varnostni problemi rešujejo preko njega. Pomaga lahko s svojim strokovnim znanjem ali pa za pomoč zaprosi zunanje svetovalce. Pooblaščenec za informacijsko varnost mora v organizaciji imeti visoka pooblastila in neposreden dostop do vodij oddelkov. Pomembno je, da se takoj, ko se incident zazna, le-tega sporoči pooblaščencu za informacijsko varnost.

6.4.1.6. Sodelovanje med organizacijami

Stanje:
Organizacija ima po potrebi stike s ponudniki informacijskih storitev in telekomunikacijskimi operaterji, predvsem v primeru izpadov in nekajkrat v primeru incidentov. Sodelovanje je zgledno, saj so v vseh primerih ustrezno reagirali oziroma strokovno svetovali.

Predlog:
Gospodarska zbornica ali Ministrstvo za informacijsko družbo naj bi organiziralo forum za informacijsko varnost, v katerem bi sodelovali predstavniki slovenskih organizacij. Forum naj bi se sestajal enkrat mesečno, v primeru večjih groženj lahko tudi pogosteje. Organizirali naj bi predavanja na temo informacijske varnosti, organizacije pa naj bi med seboj izmenjavale izkušnje in znanje. Organizacija naj obiskuje tudi konference in seminarje s področja informacijske varnosti. V veliko pomoč pa so lahko tudi informacije na internetu.

6.4.1.7. Neodvisen pregled varovanja informacij

Stanje:
Pregled varovanja informacij se v organizaciji ne izvaja.

Predlog:
Organizacija naj po vpeljavi SUVI redno izvaja neodvisne preglede varovanja informacij. Te lahko izvajajo notranja revizijska služba, vodstvo ali pa za to pooblaščena zunanja organizacija.

6.4.2. Varovanje dostopa tretje stranke

Cilj: Vzdrževati varnost zmogljivosti za obdelavo informacij v organizaciji in informacijskih virov, do katerih imajo dostop tretje stranke.

6.4.2.1. Prepoznavanje tveganja pri dostopu tretje stranke

Stanje:
Organizacija beleži veliko število dostopov tretjih strank, tako fizičnih, kot logičnih, vendar tveganja ne prepoznava. Fizično dostopajo predvsem poslovni partnerji, vzdrževalci strojev in opreme, čistili servis, oskrbovalna služba, varnostna služba, študentje, pogodbeno zaposleni …Logično pa dostopajo poslovni partnerji, dislocirane enote, dobavitelji, kupci …

Predlog:
Organizacija naj oceni tveganje, s čimer se ugotovijo varnostne zahteve, na katere se lahko reagira z ustreznimi varnostnimi kontrolami.
Prepoznavanje tveganja pri dostopu tretje stranke naj se izvaja ciklično, oziroma vsaj takrat, ko pride do sprememb v razmerju s tretjo stranko.

6.4.2.2. Varnostne zahteve v pogodbah s tretjo stranko

Stanje:
Organizacija v pogodbe s tretjimi strankami ne vključuje varnostnih zahtev.

Predlog:
Organizacija naj pregleda vse pogodbe s tretjimi strankami in vanje vključi varnostne zahteve. Podpisniki pogodb obeh strank naj bodo primerno pooblaščeni. Kopije vseh pogodb naj bodo ustrezno vključene v dokumentacijo informacijske varnosti, vsako izjemo ali odmik od teh zahtev pa naj se opraviči in dokumentira.

6.4.3. Zunanji viri

Cilj: Vzdrževati varnost informacij tudi kadar se odgovornost za obdelavo informacij zaupa drugim organizacijam.

6.4.3.1. Varnostne zahteve pri pogodbah z zunanjimi viri

Stanje:
Organizacija ne prenaša odgovornosti za obdelavo informacij na zunanje vire.

Predlog:

Če bi organizacija prenesla odgovornosti za obdelavo informacij na zunanje vire, je predhodno potrebno posvetiti pozornost ugotavljanju tveganja in zagotavljanju varnostnih kontrol. Organizacija naj natančno opredeli varnostne zahteve, kontrole in odgovornosti obeh strank.

6.5. Razvrstitev in nadzor sredstev

6.5.1. Odgovornost za sredstva

Cilj: Vzdrževati ustrezno zaščito sredstev organizacije.

6.5.1.1. Popis sredstev

Stanje:
Organizacija ima primerno urejen popis fizičnih sredstev.
Popis sredstev vključuje:

- opis,
- model,
- vrsto,
- datum izdelave,
- serijsko številko,
- identifikacijsko številko,
- lastnika,
- trenutno nahajališče.

Organizacija prav tako vodi odpis sredstev, ki poleg zgornjih atributov vsebuje še datum, vzrok in osebo odpisa.

Predlog:
Poleg fizičnih sredstev naj organizacija popiše še:

- vsa informacijska sredstva (podatkovne baze, sistemsko dokumentacijo, uporabniške priročnike, načrt neprekinjenega poslovanja),
- programska sredstva (aplikacijska in sistemska programska oprema, razvojna orodja, pripomočki),
- storitve (računalniške in komunikacijske storitve, ogrevanje, elektrika, klimatske naprave).

Pri fizičnih sredstvih naj podjetje vodi tudi vrednost in varnostno klasifikacijo.

6.5.2. Klasifikacija informacij

Cilj: Zagotoviti ustrezen nivo zaščite informacijskih sredstev.

6.5.2.1. Smernice za klasifikacijo

Stanje:
Organizacija nima klasifikacijskega načrta in ne vodi klasifikacije informacij.

Predlog:
Organizacija naj izdela klasifikacijski načrt, s katerim postavi klasifikacijo, s tem pa poenostavi odločanje, kako ravnati z informacijami in kako jih zaščititi. Klasifikacijski načrt naj bo v pisni obliki in na voljo vsem, ki so pooblaščeni za njegovo uporabo. Informacije je potrebno klasificirati glede na njihovo vrednost in občutljivost za organizacijo. Določi naj se tudi trajanje klasifikacije, kajti informacija čez čas zgubi vrednost in občutljivost, pa tudi stroški počasi postanejo neopravičljivi. Predlagam preprosto klasifikacijo z največ tremi stopnjami:

- javno,
- zaupno,
- poslovna skrivnost.

Vsaka stopnja naj bo jasno in nedvoumno opredeljena, da odgovorni pri izbiri klasifikacije ne bi imeli težav.
Za klasifikacijo informaciji naj bodo odgovorni lastniki informacij.

6.5.2.2. Označevanje ter ravnanje z informacijami

Stanje:
Organizacija nima postopkov za označevanje in ravnanje z informacijami

Predlog:
Organizacija naj izdela postopke za označevanje in ravnanje z informacijami, ki naj bodo v skladu s klasifikacijskim načrtom. Iz oznak naj bo razvidna klasifikacija informacij.
Najprimernejša oblika označevanja so fizične oznake. Kadar to ni mogoče (elektronska oblika), naj se uporabi elektronsko označevanje.

6.6. Varovanje v zvezi z osebjem

6.6.1. Varnost pri opredelitvi dela in pri pridobivanju novih sodelavcev

Cilj: Zmanjšati tveganje zaradi človeških napak, kraje, poneverbe ali zlorabe zmogljivosti.

6.6.1.1. Vključitev varovanja med službene odgovornosti

Stanje:
Zaposleni v organizaciji med službenimi odgovornostmi nimajo določene odgovornosti za varovanje informacij.

Predlog:
Organizacija naj določi vlogo in odgovornost za varovanje informacij vsem zaposlenim, ki so kakor koli odgovorni za varovanje informacij. To naj bo zapisano kar v opisu del in nalog ali v delovni pogodbi. Obvezno mora biti dokument podpisan s strani uprave in zaposlenega. S tem vsak zaposleni potrdi sprejem in razumevanje odgovornosti.

6.6.1.2. Politika preverjanja uslužbencev

Stanje:
Organizacija ob sprejemanju prijav za novo delovno mesto ne preverja verodostojnosti predloženih dokumentov. Ne preverja niti dokazil o akademskih in profesionalnih kvalifikacijah. Preverjanja kazenske kartoteke kandidata pa slovenska zakonodaja ne dovoljuje.

Predlog:
Organizacija naj za informacijsko odgovorna delovna mesta obvezno preveri verodostojnost kandidatov.
Preveri naj se:

- značajske lastnosti (poslovne in osebne),
- življenjepis,
- akademske in profesionalne kvalifikacije,
- identiteta kandidata.

Ob predhodnem pisnem soglasju je možna tudi poizvedba o kandidatu pri predhodnem delodajalcu. Kandidatu lahko zastavimo tudi vprašanje o njegovi kazenski preteklosti, z opozorilom, da na vprašanje ni dolžan odgovoriti.
Tudi kasneje med delom naj vodje preverjajo kredibilnost svojih podrejenih. Pozorni naj bodo predvsem na depresivne osebe, osebe z denarnimi težavami, osebe, ki veliko izostajajo z dela … Vsi ti kazalci lahko pripeljejo do prevar, kraj, napak in drugih dogodkov, ki vplivajo na varnost.

6.6.1.3. Sporazumi o zaupnosti

Stanje:
Organizacija ne uporablja sporazuma o zaupnosti.

Predlog:

Organizacija naj vsem zaposlenim, študentom in pogodbenim strankam v podpis predloži sporazum o zaupnosti. S podpisom se zavežejo k zaupnosti in nerazkritju informacij, s katerimi delajo.
Sporazum o zaupnosti se prvič podpiše ob nastopu delovnega mesta, se med delom ciklično podpisuje, zadnjič pa se ta sporazum preveri in podpiše ob prenehanju delovnega razmerja.
Organizacija bi lahko dokument vključila kot točko kolektivne in individualne pogodbe, ki jo zaposleni podpišejo enkrat letno.

6.6.1.4. Pogoji zaposlovanja

Stanje:
Organizacija v pogojih zaposlovanja posebej ne poudarja odgovornosti uslužbenca pri varovanju informacij.

Predlog:
Organizacija naj v pogojih zaposlovanja poudari odgovornost, ki jo bo uslužbenec imel do varovanja informacij. Ta odgovornost traja v organizaciji, izven organizacije in v nekaterih primerih tudi za določen čas, ko oseba prekine delovno razmerje. Vključene naj bodo tudi pravice in dolžnosti zaposlenih, ki jih predpisuje Zakon o varstvu osebnih podatkov in Zakon o avtorskih in sorodnih pravicah. Organizacija naj navede tudi ukrepe za primer kršitev navedenih varnostnih zahtev.

6.6.2. Usposabljanje uporabnikov

Cilj: Zagotoviti, da se uporabniki zavedajo pomembnosti in groženj, ki ogrožajo varnost informacij, in da so opremljeni tako, da lahko med delom podpirajo varnostno politiko organizacije.

6.6.2.1. Izobraževanje in usposabljanje za varovanje informacij

Stanje:
Organizacija razen samoiniciativnih posameznikov ne izobražuje in usposablja za varovanje informacij.

Predlog:
Organizacija naj za vse zaposlene organizira usposabljanje za osnovno varnostno ozaveščanje. Tu naj bodo vsi udeleženci seznanjeni z varnostno politiko, cilji in okviri, v katerih naj bi delali. Redno morajo biti seznanjeni tudi z njenimi spremembami in dopolnitvami. Poleg splošnega usposabljanja s področja informacijske varnosti naj se za vsakega posameznika izdela načrt usposabljanja, ki je v skladu z njegovim znanjem in delovnim mestom. Smiselno bi bilo uvesti izobraževanje in preverjanje znanja na daljavo (preko intraneta). Zapise o opravljenih tečajih in usposobljenosti naj hrani kadrovska služba.

6.6.3. Kako ravnati v primeru incidentov in okvar

Cilj: Kar najbolj zmanjšati škodo, ki jo povzročijo varnostni incidenti in okvare, ter spremljati incidente in se iz njih učiti.

6.6.3.1. Prijava incidentov pri varovanju informacij

Stanje:
Organizacija nima uradnega postopka prijave incidentov s področja varovanja informacij. Če se incident že prijavi, je to v ustni obliki. Zapisi o incidentih ne obstajajo.

Predlog:
Organizacija naj določi uradni postopek prijave incidentov, zraven pa naj določi tudi postopek, ki določa, kako ob prijavi incidenta ukrepati. Postopek prijave incidenta naj bo zapisan in poznan vsem zaposlenim. Dolžnost vseh zaposlenih pa naj bo vsak incident prijaviti, takoj ko je to mogoče. Obvezno mora biti o vseh incidentih obveščen pooblaščenec za informacijsko varnost. Obravnava naj vsak prijavljen incident in po reševanju o njem poda tudi poročilo.

6.6.3.2. Prijava pomanjkljivosti pri varovanju informacij

Stanje:
Organizacija nima uradnega postopka prijave pomanjkljivosti pri varovanju informacij. Večinoma se te ne prijavljajo niti na kak drug način.

Predlog:
Organizacija naj določi uraden postopek prijave pomanjkljivosti pri varovanju informacij. Zaposlene naj se spodbuja, da prijavijo vse pomanjkljivosti oziroma samo sume nanje. S tem se omogoči, da se le-te pregleda in odpravi. Nikakor pa zaposleni varnostnih pomanjkljivosti ne smejo izkoriščati. Obvezno mora biti o vseh pomanjkljivostih obveščen pooblaščenec za informacijsko varnost.

6.6.3.3. Prijava nepravilnega delovanja programske opreme

Stanje:
Organizacija nima v celoti pokritega področja prijavljanja nepravilnega delovanja programske opreme. Uraden postopek prijave je izveden le za orodje za podporo skupinskemu delu. Za ostala področja uradnega postopka prijave ni, prijave pa se vršijo telefonsko.

Predlog:
Organizacija naj določi enoten uradni postopek prijave nepravilnosti delovanja programske opreme za vsa področja. Dolžnost zaposlenih naj bo, da čim prej prijavijo nepravilnost delovanja programske opreme, kajti zgodnja prijava računalniškega virusa lahko prepreči

neizmerno škodo. Programsko opremo oziroma računalnik, na katerem ta programska oprema teče, naj se čim prej osami ali vsaj do rešitve nepravilnosti ne uporablja. Zaposleni nepravilnega delovanja programske opreme ne smejo izkoriščati. Nepravilnosti delovanja programske opreme in vse spremembe oziroma nadgradnje le-te naj se primerno vodi. Obvezno mora biti o vseh nepravilnostih obveščen pooblaščenec za informacijsko varnost in lastnik sredstva oziroma procesa .

6.6.3.4. Česa se lahko naučimo iz incidentov

Stanje:
Organizacija za izpade strežnikov vodi preprosto evidenco, iz katere so razvidni predvsem vrsta, obseg in pa vzrok izpada.

Predlog:
Organizacija naj uvede mehanizme, s katerimi lahko izmeri in spremlja vrsto, obseg in stroške incidentov ali okvar. S tem naj se ugotovi ponavljajoče incidente in pa tiste, ki organizacijo stanejo največ. S pomočjo evidence in analize naj se omeji pogostost in škoda incidentov, informacije pa nam služijo tudi pri oceni tveganj in izdelavi varnostne politike.

6.6.3.5. Disciplinski postopki

Stanje:
Organizacija izvaja uraden disciplinski postopek za vse zaposlene, ki kršijo politiko ali postopke organizacije.
Ker pa organizacija nima varnostne politike, tudi disciplinski postopki zoper varnostne kršitve niso možni.

Predlog:
Organizacija naj po uvedbi varnostne politike tudi za to področje izvaja disciplinske postopke ter se s tem primerno odzove na kršitve varovanja. Postopki naj bodo dokumentirani, tako da bodo vsi zaposleni seznanjeni s podrobnostmi. Disciplinski postopek naj bo po eni strani svarilo vsem, ki kršijo varnostno politiko, po drugi strani pa zagotovilo pravilne in poštene obravnave hujših kršiteljev varnostne politike.

6.7. Fizična zaščita in zaščita okolja

6.7.1. Varovana območja

Cilj: Preprečiti nepooblaščen fizičen dostop, škodo in motnje v poslovnih prostorih in informacijah.

6.7.1.1. Fizičnen varnostni pas

Stanje:
Organizacija ima znotraj informacijskega centra fizičen varnostni pas, v katerem se nahajajo pomembnejša informacijska sredstva. Varnostni pas od okolja ločujejo do stropa pozidane stene in ognjevarna vrata, ki se odpirajo le z magnetno kartico. Prostor nima oken in je klimatiziran. Varnostni pas je razdeljen v dne coni. V prvi se nahajajo vsi strežniki, v drugi pa diskovni del in tračna knjižnica. Celoten varnostni pas pa je protipožarno varovan s protipožarno opremo. Ostali prostori znotraj službe informatika so nezavarovani in dostopni vsem.

Predlog:
Organizacija naj razširi varnostni pas na celotno službo informatike. Na vrata naj namesti elektronsko ključavnico, ki se odpira le z magnetno kartico. Dostop pa naj se dovoli le pooblaščenim.

6.7.1.2. Kontrole fizičnega dostopa

Stanje:
Organizacija varovana območja varuje z vhodnimi kontrolami. Za vhodno kontrolo služijo magnetne kartice. Nihče pa ne pregleduje spiskov dostopa.

Predlog:
Organizacija naj glede na oceno tveganj določi varovana območja in jih primerno zaščiti. Poleg tega naj se:

- nadzoruje in pregleduje vse dostope,
- beleži točnen čas vhoda in izhoda,
- dostop omogoči le pooblaščenim osebam,
- na vidnem mestu nosi razvidno identifikacijo organizacije,
- prepove vstop brez identifikacije organizacije (tretje stranke, partnerji …),
- redno pregleduje spisek pravic dostopa.

6.7.1.3. Varovanje pisarn, sob in naprav

Stanje:
Organizacija varuje glavni sistemski prostor znotraj službe informatike. Ostali prostori, kot so pisarne in druge sobe, se ne varujejo. Večinoma se niti ne zaklepajo, oziroma je to prepuščeno izbiri lastnika. Znotraj službe informatika se nahaja glavni tiskalnik, kamor po natisnjene dokumente hodijo ljudje s celotne organizacije.

Predlog:
Organizacija naj poskrbi, da se celotna služba informatike organizira kot varovano območje, v katerega imajo dostop le zaposleni. Prostor naj bo opremljen z alarmom in protipožarnimi napravami. Kadar so prostori prazni, naj bodo okna in vrata zaklenjena in

alarmna naprava aktivirana. Gorljivi predmeti naj bodo ločeni od varovanih območij, prav tako naj bodo od varovanih prostorov ločena tudi rezervna oprema in varnostne kopije.

6.7.1.4. Delo na varovanih območjih

Stanje:
Na varovanem področju se dela le izjemoma, in sicer, kadar gre za vzdrževalna dela ali popravila. Vsa ta dela pa niso vedno zabeležena in nadzorovana.

Predlog:
Organizacija naj bo dosledna pri najavi del v varovanem območju in naj to delo tudi nadzira.

6.7.1.5. Ločeno območje za dostavo in odpošiljanje

Stanje:
Organizacija ima ločen prostor za dostavo in odpošiljanje. Oba prostora sta tudi povsem ločena od varovanega območja.

Predlog:
Organizacija naj poskrbi, da bo gibanje dostavnih in prevzemnih služb omejeno in primerno nadzorovano. Zabeleži naj se tudi ime voznikov ter registrska številka dostavnih in prevzemnih vozil.

6.7.2. Varovanje opreme

Cilj: Preprečiti izgubo, škodo ali kompromitiranje sredstev in prekinitev poslovnih dejavnosti.

6.7.2.1. Namestitev in zaščita opreme

Stanje:
Organizacija ima znotraj varovanega območja dobro nameščeno in zaščiteno opremo, česar pa ne bi mogli reči za opremo izven varovanega območja.

Predlog:
Organizacija naj pri zaščiti opreme izhaja iz ocene tveganj. Oprema naj bo nameščena tako, da bo tveganje pred naravnimi in drugimi nesrečami ter nepooblaščenim dostopom čim manjše. Uvedejo naj se kontrole, ki najbolj zmanjšujejo nevarnost pred:

- krajo,
- ognjem,
- eksplozijo,
- dimom,
- prahom,

- tresljaji,
- električnimi motnjami,
- kemičnimi učinki.

Organizacija naj postavi tudi pravila glede hranjenja in kajenja v bližini informacijske opreme. Upošteva pa naj se tudi možnost vpliva nesreč na sosednjih stavbah.

6.7.2.2. Oskrba z energijo

Stanje:
Organizacija se oskrbuje z električno energijo iz dveh neodvisnih virov napajanja. Poleg tega je celotno varovano območje opremljeno z napravami za neprekinjeno napajanje (UPS). Znotraj varovanega območja je v primeru električnega izpada poskrbljeno tudi za zasilno razsvetljavo. Organizacija nima generatorja za električno energijo.

Predlog:
Organizacija naj preveri, če nazivna moč naprave za neprekinjeno napajanje še ustreza porabnikom v primeru izpada toka. Organizacija naj redno, najmanj pa enkrat letno, preveri delovanje naprave za neprekinjeno napajanje ter izmeri čas delovanja, ko so nanjo priključene vse naprav znotraj varovanega območja. Preveri naj se, ali je časa dovolj za pravilen izklop vseh naprav, oziroma če je skladen s časom, ki naj bo naveden v načrtu za neprekinjeno poslovanje. Zagotovi naj se tudi, da bo oskrba z elektriko enakomerna, brez vzponov in padcev napetosti. Nujna pa je tudi zaščita pred udarom strele.

6.7.2.3. Varovanje kabelskih vodov

Stanje:
Organizacija ima glavne električne in telekomunikacijske vode speljane pod zemljo. Vodi znotraj organizacije pa so nameščeni po zato namenjenih kanalih.

Predlog:
Organizacija naj poskrbi, da bodo električni in telekomunikacijski vodi, ki prenašajo podatke ali podpirajo informacijske storitve, primerno zaščiteni pred prestrezanjem ali poškodbami. Zaradi možnosti prestrezanja naj se prostori nadzornih in končnih točk vedno zaklepajo, prav tako pa naj se uvede tudi šifriranje podatkov. Telekomunikacijski in električni kabli naj se zaradi motenj med seboj ločijo.

6.7.2.4. Vzdrževanje opreme

Stanje:
Organizacija ima za vitalno informacijsko opremo z dobavitelji sklenjene vzdrževalne pogodbe. Ti v rednih vzdrževalnih terminih pregledujejo in po potrebi zamenjajo posamezne dele opreme.

Predlog:
Organizacija naj opremo vzdržuje v skladu z navodili proizvajalca. Vzdrževanje in servisiranje naj dovoli le pooblaščenim serviserjem. Beležijo naj se vsi sumi, dejanske okvare, popravila in preventivna vzdrževalna dela. Če se vzdrževalna dela izvajajo izven organizacije, naj se poskrbi za varnost informacij, ki se nahajajo na opremi.

6.7.2.5. Varovanje opreme izven prostorov organizacije

Stanje:
Organizacija nima politike za varovanje opreme izven svojih prostorov. Zabeleženih je že kar precej kraj računalniške opreme, predvsem prenosnih računalnikov. Tudi varovanje prenosne opreme doma je na zelo nizkem nivoju (nalaganje računalniških igric, glasbe, virusi …).

Predlog:
Organizacija naj v skladu z oceno tveganj pripravi politiko za varovanje opreme, ki se nahaja izven njenih prostorov. Nivo varnosti, kot ga ima oprema znotraj organizacije, mora biti zagotovljen tudi izven nje. Uporabnik naj bo izven organizacije stalno poleg opreme, če pa to ni mogoče, naj poskrbi tudi za primerno fizično varnost. Organizacija naj za opremo, ki se nahaja izven njenih prostorov, sklene ustrezno zavarovalno polico.

6.7.2.6. Varno uničenje ali ponovna uporaba opreme

Stanje:
Organizacija nima politike za zagotavljanje varnega uničenja opreme. Večinoma se podatki pred ponovno uporabo ali odpisom z medijev zgolj izbrišejo.

Predlog:
Organizacija naj pripravi politiko varnega uničenja in ponovne uporabe opreme. Ker zgolj brisanje podatkov z medijev za popolno zaščito ne zadošča, naj organizacija razmisli o popolnem uničenju medijev (razmagnetenje, razkosanje). Če bo medij šel v ponovno uporabo, je potrebno predhodno z njega pobrisati vse informacije.

6.7.3. Splošne kontrole

Cilj: Preprečiti kompromitiranost ali krajo informacij in zmogljivosti za obdelavo informacij .

6.7.3.1. Politika čiste mize in čistega zaslona

Stanje:
Organizacija nima politike čiste mize in čistega zaslona. Med delovnim časom je tudi v odsotnosti uporabnikov vključena večina osebnih računalnikov, v glavnem brez ohranjevalnikov zaslona. Tudi dokumenti v papirni obliki niso deležni primerne zaščite.

Predlog:
Organizacija naj tako za varnost informacij na papirju in tudi na informacijskih medijih uvede politiko čiste mize in čistega zaslona. Kadar dokumenti niso v uporabi, naj bodo hranjeni v ustrezno zaklenjenih omarah, bolj občutljivi pa celo v ognjevarnih sefih. To je še posebej pomembno, če je pisarna prazna. Osebni računalniki naj ne bodo vključeni brez nadzora, sploh če na njih ni nameščen z geslom zavarovan ohranjevalnik zaslona. Pri tiskanju občutljivih dokumentov naj se le-ti takoj odstranijo s tiskalnika.

6.7.3.2. Odstranitev lastnine

Stanje:
Organizacija za iznos opreme na uporablja pooblastil. Večinoma se iznašajo prenosni računalniki, CD-ji, diskete in tiskani mediji. V organizaciji obstaja tudi delo od doma.

Predlog:
Organizacija naj za iznos opreme in občutljivih dokumentov uvede uradna pooblastila. Vsi deli opreme, ki se iznaša, naj bodo označeni kot last organizacije. Organizacija naj ve, kje vse se njena oprema nahaja. To je pomembno tudi, ko uslužbenci prekinejo delovno razmerje in morajo vrniti vso lastnino organizaciji. Prav tako naj ima organizacija spisek vse opreme, ki se uporablja za delo od doma. Obiskovalci, ki prinašajo v organizacijo svojo lastnino, naj le-to ob vstopu prijavijo, da jo lahko ob odhodu tudi brez težav odnesejo. Organizacija naj se opredeli tudi do odstranitev informacij preko interneta, saj tu za iznos iz organizacije niso potrebna fizična sredstva.

6.8. Upravljanje s komunikacijami in s produkcijo

6.8.1. Postopki in odgovornosti produkcije

Cilj: Zagotoviti pravilno in varno delovanje zmogljivosti za obdelavo informacij.

6.8.1.1. Dokumentirani delovni postopki

Stanje:
Organizacija nima dokumentiranih delovnih postopkov.

Predlog:
Organizacija naj po izdelavi varnostne politike vse v njej naštete postopke dokumentira in vzdržuje. Za vsak postopek naj se podrobno navede navodila za delo:

- ravnanje z informacijami,
- lastništvo,
- časovna razporeditev dela,
- ravnanje v primeru napak in incidentov,
- postopki zaustavljanja in ponovni zagon sistema.

Postopkov naj brez ustreznega pooblastila ne bi bilo mogoče spremeniti ali zaobiti.

6.8.1.2. Kontrole sprememb v produkciji

Stanje:
Organizacija nima dokumentiranih postopkov za nadzorovanje sprememb v produkciji. Redno pa spremembe pred prenosom v produkcijo pregleda in preizkusi.

Predlog:
Organizacija naj izdela postopke za nadzor in spremembe v produkciji. Vse spremembe naj se spremljajo, o njih pa naj se hrani natančne zapise. Nobena sprememba naj se ne izvede brez pisnega soglasja odgovorne osebe. Pred spremembami naj se izvede predhodna ocena možne škode, do katere bi lahko privedla sprememba. Prav tako naj bo ob neuspeli spremembi vedno zagotovljena možnost povratka na predhodno stanje. O spremembah naj bodo obveščeni vsi udeleženci v procesu.

6.8.1.3. Kako ravnati v primeru incidenta

Stanje:
Organizacija nima dokumentiranih postopkov za ravnanje v primeru incidenta.

Predlog:
Organizacija naj določi odgovornosti in postopke za ravnanje v primeru incidenta.
Incidente naj se loči na:

- izbruhe zlonamerne kode,
- napake na strojni opremi,
- napake v programski opremi,
- zavrnitev storitve,
- izpad napajanja,
- nepravilne podatke,
- poneverbe ali kraje
- naravne katastrofe,

Vsak incident naj se prijavi, izdela naj se analiza in ugotovi vzrok. Na osnovi tega naj se vpeljejo ukrepi za preprečevanje ponovnega pojava incidenta. Zberejo in urejajo naj se vse revizijske sledi, ki kažejo nastanek, potek in reševanje incidenta.

6.8.1.4. Ločevanje nalog

Stanje:
Organizacija nima uvedenega ločevanja nalog na vseh področjih. Predvsem je to šibko na področju informatike. Večinoma ena oseba spremembo načrtuje in jo tudi izvede.

Predlog:

Organizacija naj uvede postopek ločevanja nalog, s katerim ločimo upravljanje in izvajanje nalog. Kjer je to mogoče, naj se naloge razdelijo na dve ali več oseb, s čimer na točki predaje druga oseba vidi, ali je prva izvedla vse potrebno. S tem se močno zmanjša možnost nepooblaščenega spreminjanja in zlorab informacij.

6.8.1.5. Ločevanje razvojnih in produkcijskih zmogljivosti

Stanje:
Organizacija ima ločeno razvojno, testno in produkcijsko okolje. Ločene so tudi dostopne pravice do različnih okolij. Kjer je to mogoče, so razvojno, testno in produkcijsko okolje ločeni tudi fizično, kar pomeni, da tečejo na različnih strežnikih.
Predlog:
Organizacija naj uvede postopke, kjer bodo faze razvoja, testa in produkcije natančno opredeljene:

- kdaj je možen prenos iz enega v drugo okolje,
- na osnovi katerih podatkov se potrjuje prenos,
- kdo ga lahko izvede,
- revizijska sled prenosa,
- menjava gesel po testiranju.

Informacijska oprema naj bo vsaj za testno in produkcijsko okolje enako zmogljiva, kajti le tako resnično lahko zagotovimo enake pogoje med testiranjem in kasnejšo produkcijo.

6.8.1.6. Upravljanje z zunanjimi zmogljivostmi

Stanje:
Organizacija izven svojih meja nima zmogljivosti.

Predlog:
Če se organizacija odloči prenesti upravljanje svojih zmogljivosti na zunanjega pogodbenika, naj se najprej preveri tveganje. V pogodbo naj se vključijo varnostne zaščite in delovne kontrole.

6.8.2. Načrtovanje in sprejem sistema

Cilj: Zmanjšati tveganje izpada sistema.

6.8.2.1. Načrtovanje zmogljivosti

Stanje:
Organizacija v glavnem vnaprej ne načrtuje zmogljivosti. Večinoma se začne razmišljati o povečanju zmogljivosti, ko so meje obstoječega sistema že presežene.

Predlog:

Organizacija naj v izogib ozkim grlom sproti nadzoruje zahteve po zmogljivosti in na osnovi teh izdela osnutek zmogljivosti, ki bodo v prihodnje potrebne. Upoštevati je potrebno časovni zamik pri dobavi novih zmogljivosti. Pri načrtovanju novih zmogljivosti ne smemo pozabiti tudi na kadrovsko zasedbo, ki je s povečanjem del ob neustrezni zasedbi lahko kritična.

6.8.2.2. Prevzem sistema

Stanje:
Organizacija nima uradnih postopkov za prevzem novih niti za nadgradnjo starih sistemov. Novi sistemi se sicer pred vključitvijo v produkcijo preverjajo, vendar se to nikjer ne dokumentira.

Predlog:
Organizacija naj postavi kriterije za prevzem novega ali nadgradnjo starega sistema. Uvede naj se nadzor nad negativnimi posledicami, ki jih nov sistem ali nadgradnja starega lahko prinese obstoječemu sistemu. Pred prevzemom novega ali nadgrajenega sistema v produkcijo naj se vedno izvaja faza testiranja. V tej fazi naj se upoštevajo vsi kriteriji za prevzem novega ali nadgradnjo starega sistema. Paziti je treba, da se v fazi testiranja testni sistem ne poveže s produkcijskim. Na koncu testiranja naj se potrdi ustreznost in izda dovoljenje za prevzem v produkcijo. Vsi koraki naj bodo primerno dokumentirani.

6.8.3. Zaščita pred zlonamerno kodo

Cilj: Zaščititi programsko opremo in informacije pred škodo, ki jo povzroči zlonamerna koda.

6.8.3.1. Kontrole proti zlonamerni kodi

Stanje:
Organizacija uporablja kontrole za zlonamerno kodo, vendar ne na vseh področjih.
Avtomatsko odkrivanje in čiščenje ali odstranjevanje zlonamerne kode je dobro podprto na področjih:

- elektronske pošte (notranje in zunanje),
- internetnega prehoda,
- delovnih postaj.

Strežniki se proti zlonamerni kodi ne ščitijo. O področju zlonamerne kode govori tudi organizacijsko navodilo. Zaposlene se o pojavu pomembnejših virusov in nadaljnem ravnanju obvešča po elektronski pošti. Na delovnih postajah nekateri zaposleni zaradi povečanja računalniških zmogljivosti protivirusni program izklopijo. Ker so orodja za odkrivanje in čiščenje zlonamerne kode po področjih različna, je potrebno osveževati vsak vzorec posebej. Pojavljajo se tudi nasedanja na potegavščine, kjer uporabniki brišejo pomembne ali nameščajo nepotrebne dele sistema.

Predlog:

Organizacija naj več naredi na področju ozaveščanja uporabnikov, saj je to najboljša pot do preventive. Uvedejo naj se postopki in odgovornosti za izvajanje zaščite proti zlonamerni kodi. Uvedejo naj se avtomatske kontrole, ki bodo z odkrivanjem in čiščenjem pokrivale vsa področja. Še posebej naj se varuje prenosno opremo, ki se dnevno iznaša in ponovno vključuje v omrežje organizacije. Za vsa področja naj se poenoti orodje za odkrivanje in čiščenje zlonamerne kode. S tem se poenoti uporabniški vmesnik, skrbeti pa je potrebno za osveževanje le enega vzorca zlonamerne kode. Uvedejo naj se kontrole, ki bodo onemogočale odstranitev orodja za odkrivanje in čiščenje zlonamerne kode brez odobritve administratorja sistema. Zagotoviti je potrebno, da uporabniki ne nasedajo potegavščinam o prihodu in zaščiti proti zlonamerni kodi, pač pa da upoštevajo le navodila administratorja sistema. Postopki za odpravo posledic zlonamerne kode naj se vključijo v načrt za neprekinjeno poslovanje.

6.8.4. Skrbništvo

Cilj: Vzdrževati celovitost in razpoložljivost obdelave informacij in komunikacijskih storitev.

6.8.4.1. Varnostna kopija informacij

Stanje:
Organizacija ustrezno izdeluje in hrani varnostne kopije informacij. Pogostost kopiranja je skladna z odvisnostjo od pomembnosti informacij. Varnostni nosilci se hranijo v ognjevarnem sefu, ločeno od sistema, ki se varuje. Ni pa dokumentiranih procedur za izdelavo varnostnih kopij, ne dela se spiska varnostnih kopij, prav tako se ne izvaja redno testiranje medijev in postopkov vračanja podatkov nazaj na sistem.

Predlog:
Organizacija naj dokumentira procedure kopiranja informacij. Redno naj se izdelujejo spiski obstoječih kopij. Kopije naj bodo podvržene istemu nivoju varnosti, kakor ga ima njene izvirnik. Redno naj se testira varnostne nosilce, pa tudi postopek vračanja in pravilnost povrnjenih podatkov. Izmeri naj se tudi čas, ki je potreben za vračilo določenih podatkov. Določi naj se, kako dolgo naj se posamezne informacije hranijo. Dolžina hranjena nekaterih informacij je celo zakonsko določena.

6.8.4.2. Dnevnik operaterja

Stanje:
V organizaciji se dnevnik operaterja ne vodi.

Predlog:
Organizacija naj uvede dnevnik operaterja, kjer naj se redno beleži:

- uro zagona in zaustavitve sistema,
- napake sistema in opravljeno delo,
- ime operaterja.

Operaterjev dnevnik naj nadrejeni redno pregledujejo.

6.8.4.3. Beleženje okvar

Stanje:
Organizacija ne beleži okvar.

Predlog:
Organizacija naj redno beleži vse okvare in tudi postopke reševanja. Beleži naj se tudi vzroke okvar in nastalo škodo. Beleženje okvar je smiselno tudi zaradi ugotavljanja zanesljivosti opreme.

6.8.5. Upravljanje omrežja

Cilj: Zagotoviti varovanje informacij in omrežij ter zaščititi podporno infrastrukturo.

6.8.5.1. Kontrole omrežja

Stanje:
Organizacija solidno kontrolira omrežje. Poleg lastne kontrole nam mesečno kontrolo omrežja vrši zunanji izvajalec. Kontrole omrežja se ne dokumentirajo.

Predlog:
Organizacija naj dodeli odgovornost za delovanje in kontrolo omrežja in tudi za delo z oddaljeno opremo (VPN). Uvesti je potrebno kontrole, ki zaznajo in preprečijo prestrezanje, kopiranje in spreminjanje podatkov v omrežju. Kontrolira naj se tudi dostop do omrežja (omejitev na naslov v omrežju ali z gesli). Kjer se po omrežju pretakajo občutljivi podatki, naj se promet ustrezno šifrira.

6.8.6. Ravnanje z nosilci podatkov in njihovo varovanje

Cilj: Preprečiti škodo na sredstvih in prekinitve v poslovanju.

6.8.6.1. Ravnanje z zamenljivimi računalniškimi nosilci podatkov

Stanje:
Organizacija primerno ravna z zamenljivimi računalniškimi nosilci podatkov. Primerno označene hrani v za to namenjenem sefu. Postopki in ravni pooblastil niso dokumentirane.

Predlog:
Organizacija naj dokumentira vse postopke in pooblastila v zvezi z zamenljivimi računalniškimi nosilci podatkov (trakovi, diski, CD-ji, diskete, natisnjeni dokumenti).

Dokumentirajo naj se tudi postopki brisanja nosilcev, ko ti za organizacijo niso več potrebni.

6.8.6.2. Odstranitev nosilcev podatkov

Stanje:
Organizacija nima uradnih postopkov glede odstranitve nosilcev podatkov.

Predlog:
Organizacija naj pripravi postopke za odstranitve nosilcev podatkov. Nosilce podatkov naj se primerno uniči (sežiganje, raztrganje), če pa gredo ti v nadaljnjo uporabo, pa naj se podatke predhodno izbriše. O uničenih in izbrisanih nosilcih podatkov naj se vodi evidenca.

6.8.6.3. Postopki ravnanja z informacijami

Stanje:
Organizacija nima uradnih postopkov glede ravnanja z informacijami.

Predlog:
Organizacija naj uvede postopke glede ravnanja z informacijami. Informacije naj se razvrsti v smiselne skupine. Če je mogoče, naj se za posamezne tipe določi kontrole, ki skupaj z ustreznim vodenjem in zapisi skrbijo za varno ravnanje z vsemi oblikami informacij. Vedno naj bo določeno, kdo je v danem trenutku za neko informacijo odgovoren.

6.8.6.4. Varovanje sistemske dokumentacije

Stanje:
Organizacija nima urejenega varovanja sistemske dokumentacije.

Predlog:
Organizacija naj uredi varovanje sistemske dokumentacije (priročnike za delo s sistemom, informacije o konfiguraciji sistema, varnostne postopke …). Sistemska dokumentacija naj bo varno shranjena. Dostop do nje naj imajo le pooblaščene osebe. Če se sistemska dokumentacija shranjuje na omrežju, naj bo ustrezno zaščitena.

6.8.7. Izmenjava informacij in programske opreme

Cilj: Preprečiti izgubo, spremembo ali zlorabo informacij, ki si jih izmenjujejo organizacije.

6.8.7.1. Sporazumi o izmenjavi informacij in programske opreme

Stanje:
Organizacija nima uradnih sporazumov o izmenjavi informacij in programske opreme.

Predlog:
Organizacija naj ugotovi, s katerimi organizacijami izmenjuje občutljive informacije. Nato naj z njimi sklene pogodbe, ki naj vključujejo potrebne varnostne kontrole. Preveri naj, kako te organizacije varujejo informacije, ki smo jim jih zaupali. To še posebej velja za organizacije, ki so nam razvile programsko opremo in zaradi vzdrževanja ali testiranja dostopajo do naših podatkov. Zagotoviti je potrebno tudi primerna pogodbena razmerja in kontrole z zunanjimi serviserji naših informacijskih sredstev. Pred vsakim iznosom opreme naj se pridobi soglasje lastnika.

6.8.7.2. Varovanje nosilcev podatkov med prenosom

Stanje:
Organizacija nima uradnega postopka za varovanje nosilcev podatkov med prenosom. Organizaciji (prodajnim referentom) je bilo na službenih potovanjih odvzeto že veliko prenosnih računalnikov. S tem podjetje ni utrpelo le izgube računalnika, pač pa tudi možnost razkritja in uporabo informacij, ki so se na njem nahajale. Organizacija fizično prenaša informacije še v papirni obliki, na disketah, CD-jih, kjer pa za varnost prav tako ni poskrbljeno.

Predlog:
Organizacija naj na osnovi ocene tveganj za posamezen tip in vrsto prenosa informacij uvede postopke za varovanje med prenosom. Če gre za pošiljanje po pošti, naj bo vsebina ustrezno zaščitena pred poškodbami, pošiljka pa naj bo poslana v priporočeni ovojnici. Kadar pa se izven organizacije prenašajo mediji z občutljivo vsebino, naj bo vsebina na mediju primerno šifrirana. Prenosni računalniki in mediji z informacijami naj se prenašajo ločeno.

6.8.7.3. Varovanje elektronskega poslovanja

Stanje:
Organizacija nima politike o elektronskem poslovanju. Dejavnost elektronskega poslovanja opravljajo za to pooblaščene osebe, ne obstaja pa o tem noben pisni dokument.

Predlog:
Organizacija naj izdela politiko elektronskega poslovanja, ki jo ščiti pred prevarami, pogodbenimi nesoglasji in razkritjem ali spremembo informacij.
Vsebuje naj:

- seznam pooblastil za elektronsko poslovanje,
- proces za izdajo teh pooblastil,
- način ločevanja nalog za preprečitev prevar,

- ustrezne kriptografske kontrole,
- kontrole za spremljanje in zaščito poslovanja.

Uporabljajo naj se mrežne varnostne kontrole, ki ščitijo omrežje organizacije pred posledicami prepletanja z drugimi omrežji. Organizacije, ki med seboj elektronsko poslujejo, naj se pisno zavežejo k uresničevanju sklenjenih dogovorov.

6.8.7.4. Varovanje elektronske pošte

Stanje:
Organizacija ima politiko za področje elektronske pošte, nima pa izdelane analize tveganj, ki so za to področje dokaj visoka, kajti dogodilo se je precej napadov, groženj izsiljevanja in ostalih incidentov. V večini se raziščejo, niso pa nikjer zabeleženi. Organizacija ščiti elektronsko pošto s primernimi kontrolami.

Predlog:
Organizacija naj za področje elektronske pošte izdela analizo tveganj, stalno pa naj preverja, če je politika elektronske pošte ažurna in če se primerno izvaja. Prav tako naj preverja, če so uporabljene kontrole primerne in jih po potrebi odvzame oziroma doda.

6.8.7.5. Varovanje elektronskih pisarniških sistemov

Stanje:
Organizacija nima politike varovanja elektronskih pisarniški sistemov niti za to področje nima izdelane analize tveganj. Večina režijskih delavcev ima dostop do elektronskih pisarniških sistemov, a se tveganj, katerim s svojim delom izpostavljajo informacije, v večini ne zavedajo.

Predlog:
Organizacija naj pripravi politiko varovanja elektronskih pisarniških sistemov, ki naj poleg pravil obnašanja vsebuje tudi smernice za nadzor poslovnih in varnostnih tveganj. Preveri naj se način hrambe informacij. Opredeli naj se tudi način, pogostost in dolžina hrambe informacij, ki se ustvarjajo, prenašajo in spreminjajo v toku elektronskih pisarniških sistemov. Posebna pozornost pa naj se posveti sistemom, ki so dostopni preko javnih omrežij, kot je internet.

6.8.7.6. Javno dostopni sistemi

Stanje:
Organizacija ima javno dostopen sistem, ki je primerno nadzorovan in zaščiten. Za objavo na spletu obstaja postopek, ki se začne s predlogom objave, gre preko odgovornega za objavljeno področje do odgovornega za objavo na spletu. Če tema presega poznavanje odgovornega za objavo, o tem odloča uredniški odbor. V nobenem primeru pa na spletno stran organizacije ne morejo priti ali se tam spremeniti informacije brez odobritve pooblaščenih oseb. Vodi se tudi celoten postopek objav s potrditvami odgovornih.

Organizacija poleg javnih vsebin na svoji spletni strani objavlja tudi vsebine, ki so varovane z gesli. Ta gesla se izdajajo po potrebi in bolj ali manj ostajajo stalna.

Predlog:
Organizacija naj izdela postopek pridobivanja uporabniškega imena in dostopa do zaupnih vsebin. Definira naj se, za kakšne namene se uporabnik kreira, kaj lahko pregleduje in koliko časa naj bo uporabniško ime in geslo veljavno. Uporabniška imena in gesla naj se uporabnikom po svetu varno preda in njihovo uporabo tudi stalno nadzira.

6.8.7.7. Druge oblike izmenjave informacij

Stanje:
Organizacija nima politike, ki ščiti informacije, prenesene preko glasu, telefonov, telefaksov …

Predlog:
Organizacija naj izdela politiko, ki bo obravnavala to področje. Hkrati pa naj stalno izobražuje zaposlene o nevarnostih, kot so:

- prisluškovanje osebnemu pogovoru,
- prisluškovanje telefonskemu pogovoru,
- napačno poslano faksirano sporočilo,
- nepooblaščeno poslušanje sporočil na telefonskem odzivniku,
- nepooblaščen dostop do odložišč za faksirana sporočila.

6.9. Nadzor dostopa

6.9.1. Poslovne zahteve pri nadzoru dostopa

Cilj: Nadzorovati dostop do informacij.

6.9.1.1. Politika nadzora dostopa

Stanje:
Organizacija nima politike nadzora dostopa, mehanizmi za nadzor dostopa pa se uporabljajo. Je pa nadzor dostopa večkrat postavljen više, kot to narekujejo poslovne zahteve.

Predlog:
Organizacija naj izdela politiko nadzora dostopa, ki naj bo skladna s poslovnimi potrebami. Dostop do občutljivih informacij naj temelji na principu »kdo mora vedeti«. Osebje, ki ima dostop do občutljivih informacij, naj bo za delo z njimi ustrezno usposobljeno. Vsako dovoljenje za dostop naj bo pretehtano v skladu s poslovnimi zahtevami in tudi primerno dokumentirano. Za poenostavitev dodeljevanja in boljši nadzor naj se uvede standardne profile dostopa uporabnikov.

6.9.2. Upravljanje dostopa uporabnikov

Cilj: Zagotoviti, da se pravice do dostopa do informacijskih sistemov izdajajo z ustreznim dovoljenjem, da se ta pravica ustrezno dodeljuje in vzdržuje.

6.9.2.1. Registracija uporabnika

Stanje:
Organizacija vse uporabnike informacijskih sistemov uradno registrira. Vendar registracije niso vedno skladne s poslovnimi potrebami. Organizacija uporablja obrazec za registracijo uporabnika, ki ga lastniku posreduje vodja enote. Lastnik sistema pa zahtevo posreduje administratorju sistema. V njem je opredeljeno področje dela in pa zahteve za registracijo. Na tej osnovi administrator dodeli pravice in varno obvesti uporabnika o njegovi identifikaciji.

Predlog:
Organizacija naj preverja, ali so zapisi o registriranih uporabnikih točni. Uporabnike naj se umakne iz seznama takoj, ko so premeščeni na drugo delavno mesto ali ko zapustijo organizacijo.

6.9.2.2. Upravljanje s pravicami

Stanje:
Organizacija primerno upravlja s pravicami. Kritično pa je področje posebnih pravic, kot so pravice sistemskih administratorjev, sistemskih inženirjev, dobaviteljev strojne in programske opreme. Tu se pravice težko nadzorujejo, kajti gre za »super uporabnike«, ki imajo najvišje pravice. Zanje standardne kontrole ne veljajo. Uporabniki s posebnimi pravicami svoja gesla kuvertirana hranijo v sefu, kjer so v primeru odsotnosti na voljo njegovim namestnikom.

Predlog:
Uporabnikov s posebnimi pravicami naj bo čim manj. Na osnovi dejanskih potreb naj jih odobrava najvišje vodstvo (lahko tudi ob pomoči neodvisnega strokovnjaka). Organizacija naj definira postopke pridobivanja in odvzemanja posebnih pravic serviserjem v primerih okvar. Vzpostavi naj se tudi postopek pridobivanja posebnih pravic, ko ena od oseb s posebnimi pravicami ni razpoložljiva. Po opravljeni storitvi se mora geslo vedno odvzeti, originalno pa spremeniti.

6.9.2.3. Uporabniška gesla

Stanje:
Organizacija uporablja gesla kot glavni mehanizem, ki pooblaščenim uporabnikom omogoča dostop do informacijskih sredstev. Uporabniki ob registraciji prejmejo začasna gesla, ki jih ob prvi prijavi zamenjajo. Niso pa definirane poti, kako začasna gesla

uporabnikom sporočiti. Uporabniki ob prevzemu gesla ne podpišejo ničesar in se tudi večkrat ne zavedajo prejete odgovornosti.

Predlog:
Organizacija naj definira postopek sporočanja začasnih gesel uporabnikom, ob upoštevanju možnosti razkritja in izkoriščanja. Geslo naj se vedno izda za eno osebo, kajti pri souporabi je odgovornost težko določiti. Uporabniki naj ob prevzemu gesla podpišejo izjavo, s katero se zavezujejo k zaupnosti gesla, hkrati pa sprejmejo odgovornosti za delo s sistemom. Gesla naj se zaščitena hranijo na centralnem mestu.

6.9.2.4. Pregled uporabniških pravic do dostopa

Stanje:
Organizacija nima postopkov za redno pregledovanje uporabniških pravic do dostopa.

Predlog:
Organizacija naj definira postopek za redno pregledovanje uporabniških pravic do dostopa. Posebej je to pomembno za uporabnike s posebnimi pravicami, ki naj se jih kontrolira vsake tri mesece. Ostale uporabnike naj se kontrolira vsakih šest mesecev. Pooblaščene osebe naj ob vsakem pregledu potrdijo, da so našteti uporabniki še vedno upravičeni do dostopa. Vsi postopki pregledovanja naj se primerno zabeležijo.

6.9.3. Odgovornosti uporabnikov

Cilj: Preprečiti dostop nepooblaščenim uporabnikom.

6.9.3.1. Uporaba gesel

Stanje:
Organizacija nima politike o hranjenju, spreminjanju, dolžini in strukturi gesla. Veliko uporabnikov še vedno uporablja začasna gesla. Redko jih spreminjajo in so slabo sestavljena. Pogosto je opaziti gesla, nalepljena na ekran oziroma skrita pod tipkovnico.

Predlog:
Organizacija naj izdela politiko za ravnanje z gesli, kjer naj bo natančno opisano, na koliko časa naj se gesla menjavajo, kako naj bodo sestavljena, kakšna naj bo dolžina. Politika naj se opredeli tudi do hranjenja gesel in samodejnih prijav v sistem. Prepove naj se souporaba gesel. Če se uporabniki prijavljajo v več različnih sistemov, se priporoča uporaba enega kakovostnega gesla.

6.9.3.2. Oprema v odsotnosti uporabnika

Stanje:
Uporabniki opremo ob odsotnosti slabo varujejo. Večinoma jo puščajo vključeno, brez prekinitve sej in nezavarovano. Redko se uporablja ohranjevalnik zaslona z geslom. Večkrat so brez nadzora v polni funkcionalnosti tudi glavne strežniške konzole.

Predlog:
Uporabniki naj svojo opremo ob odsotnosti primerno zaščitijo. Takoj ko prenehajo z delom, naj sejo s strežnikom prekinejo, računalnik pa zavarujejo z mehanizmom za zaklepanje. Če to ni izvedljivo, naj uporabijo ohranjevalnik zaslona, ki naj bo zavarovan z dovolj dobrim geslom.

6.9.4. Nadzor dostopa do omrežja

Cilj: Zaščita omrežnih storitev.

6.9.4.1. Uporaba omrežnih virov

Stanje:
Organizacija primerno nadzira uporabo omrežnih virov. Uporabniki imajo v omrežnih sistemih dostop le do virov, ki jih potrebujejo za opravljanje svojega dela. Nadzor in dostopne pravice niso primerno dokumentirane.

Predlog:
Organizacija naj izdela načrt za varovanje omrežnih virov. Natančno naj se opredeli, kakšen dostop je posameznim uporabnikom dovoljen, to pa naj se primerno evidentira. Opredeli naj se tudi, kdo lahko dostopa do operacijskega sistema glavnih strežnikov.

6.9.4.2. Uveljavljena pot

Stanje:
Organizacija ima primerno uvedene in nadzorovane uveljavljene poti, s katerimi vodi uporabnike od terminalov do računalniških storitev, za katere imajo dovoljenje.

Predlog:
Organizacija naj za lažje načrtovanje in nadzor izdela natančen načrt omrežne topologije in nanj nariše vse kontrole, ki jih ima uvedene.

6.9.4.3. Overjanje identitete zunanjih uporabnikov

Stanje:
Organizacija ima precej zunanjih uporabnikov. To so:

- Zaposleni, ki lahko izven organizacije berejo svojo elektronsko pošto. Tu je varovanje izvedeno na aplikacijskem nivoju z gesli, v kombinaciji z varnostnimi ključi in šifriranjem prometa.
- Zaposleni v zunanji izpostavi organizacije in sistemska skupina, ki sistem vzdržuje v popoldanskem času. Ti se priključujejo preko VPN (virtual privat network) povezave, kjer pa je varovanje izvedeno na omrežnem sistemu.
- Poslovni partnerji, ki pomagajo pri vzdrževanju sistema. Tu pa je varovanje izvedeno zgolj na aplikacijskem nivoju.

Predlog:
Organizacija naj natančno preveri vse možne točke zunanjega dostopa do omrežnih naprav in jih analizira na osnovi ocene tveganj. Za vsako posebej je potrebno ugotoviti, ali zagotavlja zadovoljiv nivo varnosti. Če je mogoče, naj se poleg aplikacijskih kontrol uvedejo še mrežne.

6.9.4.4. Overjanje vozlišča

Stanje:
Organizacija uporablja overjanje vozlišča z oddaljenim računalnikom, ki je izven organizacije.

Predlog:
Organizacija naj spremlja dogodke na vozlišču in na vsak sum poskus vdora primerno reagira.

6.9.4.5. Zaščita oddaljenih diagnostičnih vrat

Stanje:
Organizacija uporablja računalniške sisteme, ki imajo vgrajena diagnostična vrata. Ta skrbijo za komunikacijo med sistemom in serviserjem (vzdrževalcem sistema). Dostop do teh vrat je logično in tudi fizično primerno urejen.

Predlog:
Vsako uporabo diagnostičnih vrat naj se predhodno odobri in zabeleži. Organizacija naj na določeno obdobje preveri varno in uspešno delovanje diagnostičnih vrat.

6.9.4.6. Ločevanje v omrežjih

Stanje:
Organizacija ima segmentirano omrežje, ki se v grobem deli na notranjo in zunanjo domeno. V notranji domeni se nahaja celotno omrežje organizacije, v zunanji pa domača stran organizacije in elektronska pošta. Domeni sta med seboj ločeni s požarnim zidom, ki skrbi za nadzorovanje dostopa in pretoka informacij med domenama.

Predlog:
Organizacija naj domene in njihove medsebojne odnose natančno dokumentira. V načrtu za varovanje omrežja naj se opredeli, kaj natančno posamezna domena zajema.

6.9.4.7. Kontrola omrežnih povezav

Stanje:
Organizacija omrežne povezave varuje s pomočjo kontrol na požarnega zidu in usmerjevalnikih. Te kontrole določajo pravila za elektronsko pošto, dostop do interneta in ftp (ang. file transfer protokol).

Predlog:
Organizacija naj ima odprto minimalno možno število omrežnih povezav. Vse povezave in kontrole naj bodo dokumentirane in v skladu z načrtom varovanja omrežja.

6.9.4.8. Kontrola omrežnega usmerjanja

Stanje:
Organizacija uporablja kontrole omrežnega usmerjanja, ki temeljijo na mehanizmih preverjanja izvornega in ciljnega naslova. Prav tako uporablja tudi prevod omrežnega naslova (NAT – ang. Network alocation translation).

Predlog:
Organizacija naj pri ponudniku interneta preveri, kako zagotavlja celovitost, razpoložljivost in neprekinjeno uporabo poti. Preveri naj tudi alternativne poti v primeru izpada primarnega voda.

6.9.4.9. Varovanje omrežnih storitev

Stanje:
Organizacija je pri določenih omrežnih storitvah, kot je internet, odvisna od zunanjega ponudnika.

Predlog:
Organizacija naj od zunanjega ponudnika pridobi natančen opis uporabljenih varnostnih značilnosti, obenem pa naj izdela oceno tveganja. Na osnovi tega naj z zunanjim partnerjem izdela medsebojni dogovor o varovanju.

6.9.5. Nadzor dostopa do operacijskega sistema

Cilj: Preprečiti nepooblaščen dostop do računalnika.

6.9.5.1. Samodejno prepoznavanje terminala

Stanje:
Organizacija za dostop do občutljivih aplikacij uporablja samodejno prepoznavanje terminalov.

Predlog:
Organizacija naj preveri, kaj se zgodi, če se tak terminal pokvari in ga je potrebno zamenjati. Poleg te oblike overjanja naj se uporabi vsaj še ena. Tovrstni terminali naj se nahajajo na varovanem območju.

6.9.5.2. Postopki prijavljanja na terminal

Stanje:
Organizacija uporablja primerne prijavne postopke, ki razkrivajo kar najmanj informacij o sistemu. Prav tako je število neuspelih poskusov prijave omejeno. Med neuspelimi prijavami pa sistem izsiljuje vedno daljše časovne zamude.

Predlog:
Organizacija naj beleži in analizira vse neuspele prijave. Ob najmanjšem sumu poskusa vdora naj primerno reagira.

6.9.5.3. Prepoznavanje in overjanje uporabnika

Stanje:
Skoraj vsi uporabniki v organizaciji uporabljajo enolično identifikacijo, ki omogoča izsleditev posameznika. V proizvodnih oddelkih pa obstaja nekaj skupin, ki uporabljajo skupinsko identifikacijo. Odgovornost pa je vezana na vodjo skupine. Prepoznavanje in overjanje v večini temelji na uporabniškem imenu in geslu. V komunikaciji z banko pa se za prepoznavanje in overjanje uporablja pametne kartice.

Predlog:
Pri uporabi skupinske identifikacije naj bodo za dejanja odgovorni vsi uporabniki v skupini. Posebej naj se pazi na uporabo identifikacije sistemskih administratorjev in skrbnikov baz. Organizacija naj preveri, če prihaja do souporabe osebne identifikacije in to odpravi.

6.9.5.4. Postopek za upravljanje gesel

Stanje:
Organizacija nima politike upravljanja z gesli. Večina orodij v organizaciji omogoča samodejno kontrolo kakovosti in pogostosti menjave gesel. Vendar pa ta kontrola ni povsod aktivirana. Tako nekateri uporabniki še vedno uporabljajo začasno geslo ali pa uporabljajo slabo grajena gesla.

Predlog:
Organizacija naj izdela politiko upravljanja z gesli, ki naj določa:

- pogostost spreminjanja,
- kako naj bodo sestavljena,
- kakšna naj bo dolžina,
- spreminjanje začasnih gesel,
- souporabo gesel.

Politika naj navede tudi pravila dodeljevanja gesel.

6.9.5.5. Uporaba sistemskih pripomočkov

Stanje:
Organizacija uporablja sistemske pripomočke, ki omogočajo, da zaobidemo varnostne kontrole. Uporabljajo se predvsem ob težavah na kontrolah, zaradi možnosti lažjega in hitrejšega dostopa pa prihaja tudi do izkoriščanj.

Predlog:
Organizacija naj prepozna, izvede analizo tveganj in strogo nadzoruje vse sistemske pripomočke. Za uporabo sistemskih pripomočkov naj se izdelajo pooblastila, uporaba pa naj se nadzoruje.

6.9.5.6. Alarm za varovanje uporabnikov

Stanje:
V organizaciji noben uporabnik ni toliko ogrožen, da bi moral biti opremljen z alarmom.

Predlog:
Kontrola je za organizacijo nepotrebna.

6.9.5.7. Samodejno izključevanje terminala

Stanje:
V organizaciji se večina terminalov po določenem času nedelovanja samodejno izklopi. S tem se zaključijo tudi seje in delo z aplikacijami. Nekateri sicer omejeno možnost izključitve uporabljajo tudi na osebnih računalnikih (ohranjevalnik zaslona, zaščiten z geslom).

Predlog:
Organizacija naj z oceno tveganja določi časovni zamik, po katerem se terminal avtomatsko izključi. Predvsem je to pomembno za delovna mesta, kjer je mogoč javen dostop. Preveri naj se tudi, ali uporabniki gesla za izključitev ohranjevalnika uporabljajo v skladu s politiko.

6.9.5.8. Časovne omejitve povezave

Stanje:
Organizacija ne uporablja časovno omejenih povezav.

Predlog:
Organizacija naj na osnovi analize tveganj poišče najbolj ogrožene aplikacije in zanje preveri smiselnost uvedbe te kontrole.

6.9.6. Nadzor dostopa do aplikacij

Cilj: Preprečiti nepooblaščen dostop do informacij v informacijskem sistemu.

6.9.6.1. Omejitev dostopa do informacij

Stanje:
Organizacija skrbi, da imajo uporabniki dostop do informacij v skladu s poslovnimi zahtevami. Prav tako skrbi za nadzor dostopa do informacij.

Predlog:
Organizacija naj nekoliko zniža nivo dostopa in za posameznika določi, ali lahko informacije:

- bere,
- piše,
- spreminja,
- briše,
- tiska.

Organizacija naj zagotovi, da se informacije ščitijo v skladu s klasifikacijsko shemo.

6.9.6.2. Osamitev občutljivih sistemov

Stanje:
Organizacija nima tako občutljivih sistemov, da bi jih bilo potrebno osamiti.

Predlog:
Organizacija naj na osnovi analize tveganj poišče najbolj občutljive sisteme in zanje preveri smiselnost uvedbe te kontrole.

6.9.7. Spremljanje dostopa in uporabe sistemov

Cilj: Odkriti nepooblaščene dejavnosti.

6.9.7.1. Beleženje dogodkov

Stanje:
Organizacija nima politike beleženja. V nekaterih sistemih in aplikacijah se dogodki beležijo bolje, v drugih slabše. Vse pa imajo možnost nastavljanja različnih stopenj beleženja.

Predlog:
Organizacija naj izvede analizo zahtev glede spremljanja in beleženja dogodkov ter sprejme politiko beleženja. V njej naj definira, kaj naj revizijska sled vsebuje. Predlagam, da se beleži:

- identifikacija uporabnika,
- datum in ura prijave in odjave,
- omrežni naslov,
- uspešne in zavrnjene dostope v sistem.

Zagotoviti je potrebno primerno hranjenje revizijskih zapisov (čas, oblika in zaščita) in onemogočiti uporabnikom dostop in spreminjanje.

6.9.7.2. Spremljanje uporabe sistema

Stanje:
Organizacija nima določenih postopkov spremljanja uporabe sistema. Uporaba sistema se spremlja šele, ko pride do incidenta ali večje nepravilnosti, nato pa zopet počasi usahne. Organizacija beleži neprečiščene revizijske sledi, ki so za spremljanje dokaj nepregledne.

Predlog:
Organizacija naj na osnovi analize tveganj določi postopke spremljanja uporabe sistema, ki naj bodo skladni s sprejeto politiko beleženja. Na osnovi tveganja naj se izdela tudi stopnja, vrsta in pogostost spremljanja sistema. Predlagam, da se za prečiščevanje revizijskih sledi, ki je večkrat zelo nepregledno, uporabi posebno orodje za prepoznavanje pomembnih dejavnosti in incidentov.

6.9.7.3. Časovna uskladitev

Stanje:
Organizacija ne usklajuje računalniškega časa. V izogib spreminjanju časovnih nastavitev na lokalnih postajah se v vseh zapisih beleži strežniški čas. Še vedno pa se pojavlja problem pri sestavljanju revizijske sledi, ko se analizira dogodek med več strežniki.

Predlog:
Organizacija naj postavi strežnik (ang. time server), katerega naloga bo pridobivanje univerzalnega točnega časa. Ostali strežniki in delovne postaje pa naj se nastavijo tako, da točen čas pridobivajo s tega strežnika.

6.9.8. Prenosna računalniška oprema in delo na daljavo

Cilj: Zagotoviti varovanje informacij pri uporabi prenosnih računalnikov in naprav za delo na daljavo.

6.9.8.1. Prenosna računalniška oprema

Stanje:
Organizacija nima politike o prenosni računalniški opremi. Zabeleženih pa je nekaj kraj prenosnikov in tudi njihova neprimerna uporaba (naložene računalniške igre, glasbene datoteke, virusi …).

Predlog:
Organizacija naj sprejme politiko o prenosni računalniški opremi, ki naj vsebuje:

- fizično zaščito,
- nadzorovanje dostopa,
- varnostne kopije,
- šifrirne tehnike,
- protivirusno zaščito.

Zaposlene, ki uporabljajo prenosno računalniško opremo, je potrebno o nevarnostih in pravilnem ravnanju predhodno zadostno ozavestiti in izobraziti.

6.9.8.2. Delo na daljavo

Stanje:
Organizacija nima politike niti postopkov za delo na daljavo. Prav tako vodstvo za delo na daljavo ne izdaja pooblastil, uporabniki pa o nevarnostih in pravilnem ravnanju niso dovolj poučeni.

Predlog:
Organizacija naj sprejme politiko za delo na daljavo, ki naj vključuje:

- fizično varnost,
- varno komunikacijo,
- sistem pooblaščanja,
- način vzdrževanja strojne in programske opreme,
- varnostne kopije,
- neprekinjeno poslovanje.

Vodstvo organizacije naj po opravljenem izobraževanju uporabnikom izda pooblastilo za delo na daljavo, kjer naj bo natančno navedeno, do katerih informacij lahko dostopajo. Informacij, do katerih se lahko dostopa na daljavo, naj bo čim manj, zagotovi pa naj se, da bodo primerno zaščitene.

6.10. Razvoj in vzdrževanje sistemov

6.10.1. Varnostne zahteve sistemov

Cilj: Zagotoviti vgradnjo varnosti v informacijske sisteme.

6.10.1.1. Analiza in opredelitev varnostnih zahtev

Stanje:
Organizacija daje pri razvoju novih aplikacij in sistemov (enako tudi pri že obstoječih) premalo poudarka na prepoznavanje in opredelitev varnostnih zahtev.

Predlog:
Organizacija naj tako pri nadgradnji obstoječih kot pri razvoju novih aplikacij in sistemov poleg opredelitve funkcionalnosti na osnovi analize tveganj prepozna in opredeli varnostne zahteve.
Varnostne zahteve naj odražajo poslovno vrednost aplikacije ali sistema. Prej ko jih uvedemo, cenejša je vpeljava (najbolje že na stopnji oblikovanja sistema).

6.10.2. Varovanje aplikacijskih sistemov

Cilj: Preprečiti izgubo, spremembo ali zlorabo uporabniških podatkov v aplikacijskih sistemih.

6.10.2.1. Preverjanje vhodnih podatkov

Stanje:
Organizacija ima v pomembnejših aplikacijskih sistemih vgrajena preverjanja, ki odkrivajo napačen vnos podatkov.

Predlog:
Organizacija naj na osnovi analize tveganj določi strateške aplikacijske sisteme ter nanje namesti kontrole za preverjanje podatkov. Zagotovi naj se ustrezna stopnja celovitosti vnosa podatkov.

6.10.2.2. Nadzor notranje obdelave podatkov

Stanje:
Organizacija ima v pomembnejših aplikacijskih sistemih vgrajena preverjanja, ki odkrivajo napačno obdelavo podatkov.

Predlog:
Organizacija naj na osnovi analize tveganj določi strateške aplikacijske sisteme ter nanje namesti kontrole za preverjanje podatkov. Zagotovi naj ustrezno stopnjo celovitosti obdelave podatkov.

6.10.2.3. Overjanje sporočil

Stanje:
Organizacija, razen pri bančnih transakcijah, ne uporablja overjanja sporočil.

Predlog:
Organizacija naj na osnovi analize tveganj ugotovi smiselnost uporabe overjanja sporočil. Uvedba je smiselna predvsem tam, kjer se zahteva, da je sporočilo res poslala oseba, ki to trdi, in da sporočila med prenosom ni nihče spreminjal.

6.10.2.4. Preverjanje izhodnih podatkov

Stanje:
Organizacija ne preverja izhodnih podatkov. Napake se največkrat ugotovijo šele pri vnosu v naslednji sistem.

Predlog:
Organizacija naj kljub kontroli vnosa in obdelave uvede tudi postopke za preverjanje izhodnih podatkov.
Preverja naj se njihova:

- smiselnost,
- pravilnost,
- celovitost.

Postopki naj bodo nastavljeni tako, da jih ne bo mogoče zaobiti.

6.10.3. Kriptografske kontrole

Cilj: Zaščititi zaupnost, verodostojnost ali celovitost informacij.

6.10.3.1. Uporaba kriptografskih kontrol

Stanje:
Organizacija ima nekaj izkušenj z uporabo kriptografskih kontrol. Uporabljajo se na področju elektronske pošte in bančnega poslovanja. Politike kriptografskih kontrol pa organizacija nima. To se kaže v slabem poznavanju in obvladovanju elementov, nujnih za varno poslovanje s pomočjo kriptografskih kontrol.

Predlog:
Organizacija naj razvije politiko uporabe kriptografskih kontrol za zaščito svojih informacij.

6.10.3.2. Šifriranje

Stanje:
Organizacija uporablja šifriranje elektronske pošte za uporabnike, ki se nahajajo izven LAN omrežja.

Predlog:
Organizacija naj na osnovi analize tveganj določi področja, kjer bi še bila primerna uporaba šifriranja.

6.10.3.3. Digitalni podpis

Stanje:
Organizacija uporablja digitalni podpis pri plačevanju preko elektronskih bančnih storitev.

Predlog:
Organizacija naj pridobi potrebne certifikate za poslovanje in komuniciranje z organi javne uprave. Tudi vsa ostala zaupna dokumentacija naj se pred pošiljanjem digitalno podpiše.

6.10.3.4. Neovrgljive storitve

Stanje:
Organizacija zaenkrat še ni imela primera, v katerem bi bilo potrebno reševati spore v zvezi z digitalno overovljenim poslom.

Predlog:
Organizacija naj preveri, če imajo aplikacije, ki te posle izvajajo, same po sebi vključeno možnost beleženja in dokazovanja izvedbe in podpisa posla.

6.10.3.5. Upravljanje s ključi

Stanje:
Organizacija nima izdelane politike upravljanja s kriptografskimi ključi. Delovne postaje, kjer se ti ključi nahajajo, so fizično nezavarovane. Neprimerno so shranjene tudi varnostne kopije ključev.

Predlog:
Organizacija naj izdela politiko upravljanja s kriptografskimi ključi. Na delovnih postajah, kjer se ti ključi nahajajo, naj se izvaja poostrena fizična varnost. Kopije vseh ključev naj bodo varno shranjene v trezorju. Iz politike naj bo razvidno tudi, kako naj se ključi generirajo oziroma pridobijo, kako naj se razdelijo med uporabnike in kako naj jih uporabniki uporabljajo. Natančno naj bo navedeno, kako ukrepati v primeru menjave in v primeru kompromitiranja ključev. Izdela naj se tudi seznam vseh ključev, kjer naj bo za vsakega posebej zabeležen čas aktiviranja in deaktiviranja, trenutna lokacija, pooblaščen uporabnik in vse aktivnosti, povezane z njihovim upravljanjem.

6.10.4. Varovanje sistemskih datotek

Cilj: Zagotoviti, da se projekti, ki so povezani z informacijsko tehnologijo in podporne dejavnosti, izvajajo na varen način. Potrebno je nadzorovati dostop do sistemskih datotek.

6.10.4.1. Nadzor produkcijske programske opreme

Stanje:
Organizacija nima primernega nadzora nad produkcijsko programsko opremo.

Predlog:
Organizacija naj vse spremembe na produkcijski programski opremi kontrolira, zraven pa naj za vsako spremembo ali dopolnilo pridobi potrebna pisna soglasja in pooblastila. Pred spremembo naj se vse stare konfiguracije shranijo, zagotoviti pa je potrebno, da se ob neuspeli spremembi le-te povrnejo v produkcijo. Za vsak sistem naj se beleži, katere spremembe in kdaj so bile izvedene ter kateri popravki oziroma knjižnice so trenutno naložene. Organizacija naj poskrbi, da bodo vse spremembe ali dopolnitve vključevale tudi licenčno pokritost. Dobaviteljem naj se omogoči fizičen in logičen dostop le v vzdrževalne namene. Za vsak poseg morajo pridobiti dovoljenje, njihovo delo pa naj bo nadzirano.

6.10.4.2. Zaščita testnih sistemskih podatkov

Stanje:
Organizacija nima načrtov za testiranje. V testne namene največkrat uporablja produkcijske podatke, ki pa se tudi ščitijo na nivoju produkcijskih. Organizacija za testiranje ne izdaja pooblastil, prav tako testnih rezultatov ne shranjuje.

Predlog:
Organizacija naj izdela načrte za testiranje, ki naj vključujejo:

- zaščito testnih podatkov,
- pridobitev pooblastil za testiranje,
- zagotavljanje revizijske sledi pri kopiranju produkcijskih podatkov v testne,
- beleženje dostopa do testnih podatkov,
- brisanje osebnih podatkov pri uporabi produkcijskih podatkov v tesne namene.

Produkcijski podatki naj se po testu zbrišejo, testni podatki pa naj se primerno shranijo.

6.10.4.3. Nadzor dostopa do knjižnice programov v izvorni kodi

Stanje:
Organizacija nima primerno urejenega dostopa do programskih knjižnic v izvorni kodi. Dostop je dovoljen prevelikemu številu, pravice pa so previsoke. Dostop do knjižnic se ne nadzoruje.

Predlog:
Organizacija naj strogo zaščiti dostop do knjižnic izvornih kod, dostope pa naj beleži in redno spremlja. Dostop do knjižnic izvornih kod naj imajo le skrbniki knjižnic. Vsako spremembo je potrebno predhodno potrditi.

6.10.5. Varnost v razvojnih in vzdrževalnih procesih

Cilj: Varovati informacije in programsko opremo sistemov.

6.10.5.1. Postopki za nadzorovanje sprememb

Stanje:
Organizacija nima uradnih postopkov za nadzorovanje sprememb. Zahteve po spremembah so le redko dokumentirane. Spremembe se pred prehodom v produkcijo redno testirajo, testni rezultati pa se ne dokumentirajo.

Predlog:
Organizacija naj izdela uradne postopke za nadzorovanje sprememb. Vsaka sprememba naj se strogo nadzoruje. Zanjo naj se predloži dokumentirana zahteva, potrjena s strani skrbnika sistema. Sprememba naj bo smiselna in naj doprinaša k stabilnosti sistema. Skrbnik sistema naj nadzoruje tudi testiranje in potrditev testnih rezultatov s strani. Določi naj se tudi nadzor vpeljave v produkcijo ter dokumentiranje prevzemnih in predajnih zapisnikov in sprememba pripadajoče dokumentacije in navodil.

6.10.5.2. Tehnični pregled sprememb v operacijskih sistemih

Stanje:
Organizacija nima postopkov za pregledovanje sprememb v operacijskih sistemih. Nadgradnje operacijskih sistemov se ne izvajajo redno, največkrat takrat, kadar to zahteva nova programska oprema.

Predlog:
Organizacija naj izdela postopke za pregledovanje sprememb v operacijskih sistemih. Pred spremembo naj se izdela ocena vpliva spremembe na varnost sistema. Če je mogoče, naj se postavi testna namestitev. Pred prehodom naj se izdela plan prehoda, ki naj vsebuje podatke o izdaji in ugotovljene potrebne spremembe, ki naj se izdelajo na aplikacijah. Na osnovi tega naj se planira namestitev novih različic operacijskega sistema. Različica novega operacijskega sistema naj se opredeli v dokumentaciji kunfiguracije. Če organizacija ne sledi predpisanim rednim nadgradnjam operacijskega sistema, naj preveri, ali jim je še vedno na voljo potrebna stopnja podpore in to opredeli tudi v oceni tveganj.

6.10.5.3. Omejitve pri spremembah programskih paketov

Stanje:
Organizacija kar precej spreminja programske pakete, spremembe pa so le redko upravičene in dokumentirane. Problemi z nedokumentiranimi in največkrat že pozabljenimi spremembami se pojavljajo tudi pri nalaganju nove izdaje programskih paketov, kjer se vse izdelane spremembe uničijo.

Predlog:
Organizacija naj programske pakete spreminja le, če za to obstaja poslovna zahteva. Za vsako spremembo je potrebno pridobiti primerno pooblastilo, soglasje lastnika programa v organizaciji in soglasje dobavitelja oziroma prodajalca. Pred vsako spremembo naj se izvede analiza tveganja, s katero naj se ugotovi vpliv spremembe na ranljivost programa. Če sprememba vpliva na ranljivost, naj se uvedejo nadomestne kontrole. Vse spremembe naj bodo ustrezno dokumentirane. Če je sprememba zares smiselna in upravičena, naj se predlaga dobavitelju oziroma izdelovalcu programske opreme, naj želeno spremembo vključi v programski paket. Sicer pa je potrebno paziti na spremembe tudi pri nalaganju nove verzije programskih paketov.

6.10.5.4. Skriti prehodi in trojanski konji

Stanje:
Organizacija uporablja programe iz preizkušenih in uglednih virov. Na pomembnejši programski opremi skriti prehodi in trojanski konji niso bili opaženi.

Predlog:
Organizacija naj kupuje izključno programsko opremo poznanih proizvajalcev. Uporablja naj se le preverjena programska oprema. Pred uporabo naj se vse izdelke primerno testira. Kjer obstaja nevarnost trojanskega konja ali skritega prehoda, naj se postavijo primerne kontrole.

6.10.5.5. Zunanji razvoj programske opreme

Stanje:
V veliki meri se uporablja programska oprema, razvita izven organizacije. Kritični so predvsem kvaliteta programske opreme, roki izvedbe in pa napake v delovanju. Organizacija vso zunaj razvito programsko opremo pred namestitvijo testira.

Predlog:
Organizacija naj izdela analizo tveganj, ki izhajajo iz zunanjega razvoja programske opreme. Pogodbeno naj se opredelijo roki izvedbe, kvaliteta in pa intelektualna lastnina programske opreme. Organizacija naj za zagotovitev kvalitete pridobi pravico izvajanja presoje pri zunanjem razvijalcu programske opreme. Vsa programska oprema naj se pred namestitvijo primerno testira.

6.11. Upravljanje neprekinjenega poslovanja

6.11.1. Pregledi upravljanja neprekinjenega poslovanja

Cilj: Zagotoviti neprekinjeno poslovanje in zaščititi kritične poslovne procese pred večjimi okvarami ali nesrečami.

6.11.1.1. Upravljalni postopek neprekinjenega poslovanja

Stanje:
Organizacija nima načrta za neprekinjeno poslovanje.

Predlog:
Organizacija naj analizira tveganja in posledice ter na osnovi tega izdela načrt neprekinjenega poslovanja. Obseg načrta naj bo skladen z varnostnimi in poslovnimi zahtevami.

6.11.1.2. Analiza neprekinjenega poslovanja in njegovega vpliva

Stanje:
Organizacija nima načrta za neprekinjeno poslovanje.

Predlog:
Organizacija naj skupaj z lastniki virov analizira dogodke, ki lahko povzročijo prekinitev poslovanja, ter posledice, ki jih imajo tovrstne prekinitve za organizacijo. Analiza naj upošteva stroške obnove in nadomeščanja pa tudi stroške, ki izhajajo iz dejstva, da organizacija nekaj časa ne more opravljati nekaterih dejavnosti (oportunitetni stroški).

6.11.1.3. Izdelava in vpeljava načrtov za neprekinjeno poslovanje

Stanje:
Organizacija nima načrta za neprekinjeno poslovanje.

Predlog:
Organizacija naj izdela načrte za vzdrževanje in pravočasno obnovo poslovnih procesov po prekinitvi, motnji, okvari ali katastrofi. Ti načrti naj vsebujejo natančna navodila, ki jih je potrebno izvesti v primeru prekinitve poslovanja. Točno naj se tudi določi, kdo je odgovoren za izvajanje teh ukrepov. Zagotovi naj se, da bodo vsi zaposleni primerno ozaveščeni in usposobljeni. Po vpeljavi načrta naj se zagotovi, da se ta redno testira in dopolnjuje v skladu z varnostnimi in poslovnimi zahtevami.

6.11.1.4. Okvir za načrtovanje neprekinjenega poslovanja

Stanje:
Organizacija nima načrta za neprekinjeno poslovanje.

Predlog:
Organizacija naj z načrtovanjem neprekinjenega poslovanja pokrije celotno podjetje. S tem dobi veliko število načrtov, ki pa naj bodo med seboj usklajeni.To pomeni, da naj se izdela enoten okvir za določanje prednostih nalog, načrtovanje, testiranje in vzdrževanje vseh načrtov neprekinjenega poslovanja. Organizacija naj prav tako poskrbi za zadostno in primerno osebje in nadomeščanja v primeru odsotnosti. Izdelajo naj se tipični scenariji (okvare, virusi, požar …), ki pa naj se jih z odločbo redno testira.

6.11.1.5. Preverjanje, vzdrževanje in ponovno ocenjevanje načrtov za neprekinjeno poslovanje

Stanje:
Organizacija nima načrta za neprekinjeno poslovanje.

Predlog:
Organizacija naj z rednim preverjanjem zagotavlja učinkovitost načrtov za neprekinjeno poslovanje. Izdela naj se razpored testiranj, dokazi o testiranjih pa naj se shranijo. Organizacija naj poleg razporejenih (napovedanih) testov izvaja tudi nenapovedane teste, s katerimi ocenjuje stabilnost načrtov, obenem pa se pokaže tudi usposobljenost osebja. Določi naj se osebo, ki je odgovorna za redno pregledovanje načrtov neprekinjenega poslovanja. Če ta v poslovanju zazna spremembo, ki v načrtu neprekinjenega poslovanja ni zajeta, naj jo ustrezno dopolni.

6.12. Združljivost

6.12.1. Združljivost z zakonskimi zahtevami

Cilj: Preprečiti kršitve kazenskega in civilnega prava ter kršitve statutov, zakonskih ali pogodbenih obveznosti in vsakršnih varnostnih zahtev.

6.12.1.1. Preverjanje veljavne zakonodaje

Stanje:
Organizacija se premalo zaveda obveznosti, ki jih nalaga veljavna zakonodaja.

Predlog:
Organizacija naj prepozna in dokumentira vse pravne, zakonske in pogodbene obveznosti. Preuči naj tudi zakonodajo držav, s katerimi posluje. Organizacija naj določi odgovorne osebe in kontrole za nadzorovanje združljivosti z veljavno zakonodajo.

6.12.1.2. Zaščita intelektualne lastnine (ZIL)

Stanje:
Organizacija sicer uporablja licenčno programsko opremo, vendar nima točne evidence, kaj se na posameznem računalniku nahaja.

Predlog:
Organizacija naj strogo nadzira uporabo programske opreme. Uvede naj postopke, s katerimi ščiti intelektualno lastnino. Vzdržujejo naj se dokumenti o vsem programskem inventarju posameznega sistema. Odgovorne osebe naj se zavedajo, da so lahko za zlorabo intelektualne lastnine kazensko odgovorne.

6.12.1.3. Varovanje organizacijskih zapisov

Stanje:
Organizacija varuje pomembne zapise pred uničenjem in poneverbo v skladu z zakonodajo in predpisi. Ne vodi seznama ključnih informacij niti redno ne preverja berljivosti nosilcev.

Predlog:
Organizacija naj izdela seznam ključnih informacij, kjer naj bo navedeno, za kakšen tip informacij gre (finančne, davčne, pravne …) in na kakšen časovni interval se izdelujejo. Navede naj se tudi čas hranjenja informacij, ki je za različne tipe informacij različen. Zagotovi naj se, da bodo informacije zapisane v formatu in na mediju, ki je univerzalen in bo berljiv tudi v bodoče. Redno naj se preverja tudi berljivost medijev. Če bo organizacija

hranila tudi informacije povezanih podjetij izven države, naj se te zahteve preverijo v posamezni državi.

6.12.1.4. Zaščita podatkov in varovanje osebnih podatkov

Stanje:
Organizacija je ravno v fazi, ko se prilagaja novemu zakonu o varstvu osebnih podatkov (ZVOP). Sicer pa osebne podatke varuje skladno z zakonsko regulativo.

Predlog:
Organizacija naj dobro prouči novo zakonodajo, ki je precej natančnejša od prejšnje.
Pripravi naj se:

- katalog zbirk osebnih podatkov,
- pravilnik o varstvu osebnih podatkov,
- za podatke, ki se obdelujejo izven organizacije, tudi pogodba in pooblastilo za procesiranje osebnih podatkov.

Za vsako zbirko osebnih podatkov naj se opredeli namen obdelave, uporabnike, ki bodo zbirko uporabljali, ter način varovanja.
Pri prenosu osebnih podatkov preko telekomunikacijskih omrežij naj se uporabljajo kriptografske metode. Odgovorne osebe naj se zavedajo, da so za neupoštevanje ZVOP-a kazensko odgovorne.

6.12.1.5. Preprečevanje zlorabe opreme za obdelavo informacij

Stanje:
Organizacija različno nadzira zlorabo informacijske opreme. Področje elektronske pošte in interneta je zelo dobro nadzorovano. Vsak teden se avtomatsko izdelujejo pregledi uporabe elektronske pošte. Prav tako je uvedena politika preprečevanja pošiljanja in prejemanja datotek avdio video formata in izvršilnih datotek. Nadzira se tudi internetni promet. Ti pregledi se pošiljajo vodjem, ki na posamezne kršitve primerno reagirajo. O pravilih dela z elektronsko pošto in internetom ter o nadzoru so uporabniki obveščeni preko organizacijskega predpisa za to področje. Ostala področja se ne nadzirajo, je pa znano, da se zlorabljajo.

Predlog:
Organizacija naj za vsa področja izdela pravila uporabe informacijske opreme. Napiše naj se izjava o varovanju informacij. S podpisom izjave se uporabniki zavežejo zgolj k uporabi v službene namene. Zlorabe naj se obravnavajo z disciplinskimi ukrepi.

6.12.1.6. Ureditev kriptografskih kontrol

Stanje:
Organizacija uporablja kriptografske kontrole le za branje elektronske pošte izven podjetja. (SHTTP ang. Secure Hiper Text Transfer Protokol). Drugje se kriptografske kontrole ne uporabljajo.

Predlog:
Organizacija naj preveri pravne in zakonske zahteve glede kriptografskih kontrol. Nato naj na osnovi analize tveganj poišče kritična področja, kjer bi bila uvedba smiselna. Posebej je treba paziti pri uporabi kriptografskih kontrol v poslovanju s tujino, ker ni nujno, da sta zakonodaji kompatibilni.

6.12.1.7. Zbiranje dokazov

Stanje:
Organizacija nima postopkov za zbiranje in hranjenje dokazov.

Predlog:
Organizacija naj izdela postopke za zbiranje dokazov, ki zagotavljajo njihovo ustrezno kakovost. Izdelajo naj se tudi postopki za varno hranjenje dokazov, ki zagotavljajo, da jih brez ustreznih pooblastil nihče ne more spremeniti ali uničiti. Dokazi naj se začnejo zbirati takoj ob odkritju incidenta, saj nikoli ne vemo, kdaj se bo razvil v postopek pred sodiščem.

6.12.2. Pregledi varnostne politike in tehnične združljivosti

Cilj: Zagotoviti združljivost sistemov z varnostno politiko in standardi organizacije.

6.12.2.1. Združljivost z varnostno politiko

Stanje:
Organizacija nima varnostne politike.

Predlog:
Po uvedbi varnostne politike naj organizacija zagotovi izvajanje vseh varnostnih postopkov, njihovo redno pregledovanje in zagotavljanje skladnosti. Vodstvo naj redno zagotavlja izvajanje notranje presoje združljivosti, s katerimi se določa stopnja usklajenosti organizacije z varnostnimi politikami in postopki. Te presoje naj izvaja usposobljeno osebje v vnaprej določenih intervalih. V celoti naj bodo dokumentirane in sporočene vodstvu organizacije. Tako presoje kot tudi ukrepi za rešitev neskladnosti naj bodo primerno shranjeni.

6.12.2.2. Preverjanje tehnične združljivosti

Stanje:
Organizacija nima načrta za preverjanje tehnične združljivosti. S strani neodvisne svetovalne hiše je bil narejen penetracijski test internetnega prehoda, ki je pokazal nekaj pomanjkljivosti, ki so bile odpravljene. Na ostalih področjih se tehnična združljivost ni preverjala.

Predlog:
Organizacija naj izdela načrt za preverjanje tehnične združljivosti, ki zajema področja, pogostost in uporabljene metode. Pogostost izvajanja celovitih tehničnih pregledov naj se določi na osnovi analize tveganj. Pregledi naj bodo dokumentirani skupaj z rezultati, neskladnostmi in nadaljnimi ukrepi.

6.12.3. Presojanje sistema

Cilj: Povečati uspešnost procesa revizije in zmanjšati motnje zaradi procesa revizije.

6.12.3.1. Kontrole presojanja

Stanje:
Organizacija ne izvaja presoje informacijskih sistemov.

Predlog:
Organizacija naj natančno in sporazumno izvaja presoje informacijskih sistemov in s tem zmanjša nevarnost prekinitve poslovnih procesov. Načrti za presojo naj bodo dokumentirani in potrjeni s strani vodstva. Orodja, uporabljena pri presoji, morajo biti uradno potrjena. Presoje naj bodo dokumentirane skupaj z rezultati, neskladnostmi in nadaljnjimi ukrepi.

6.12.3.2. Zaščita orodij za presojanje sistema

Stanje:
Organizacija ne izvaja presoje informacijskih sistemov.

Predlog:
Organizacija naj pred uporabo orodij za namene presoje, zanje predhodno pridobi odobritev. Med uporabo naj se jih povsem zaščiti pred možnostmi zlorabe in natančno nadzoruje. Ko orodja niso v uporabi, naj bodo strogo ločena od produkcijskega sistema in primerno varovana.

6.13. Analiza odstopanja s pomočjo orodja Poslovni ščit

V Poslovnem ščitu ima analiza odstopanja vgrajenih 10 vprašalnikov, ki pokrivajo vsa področja standarda BS 7799.
Znotraj vprašalnikov analize odstopanj obstajata dva tipa vprašanj:

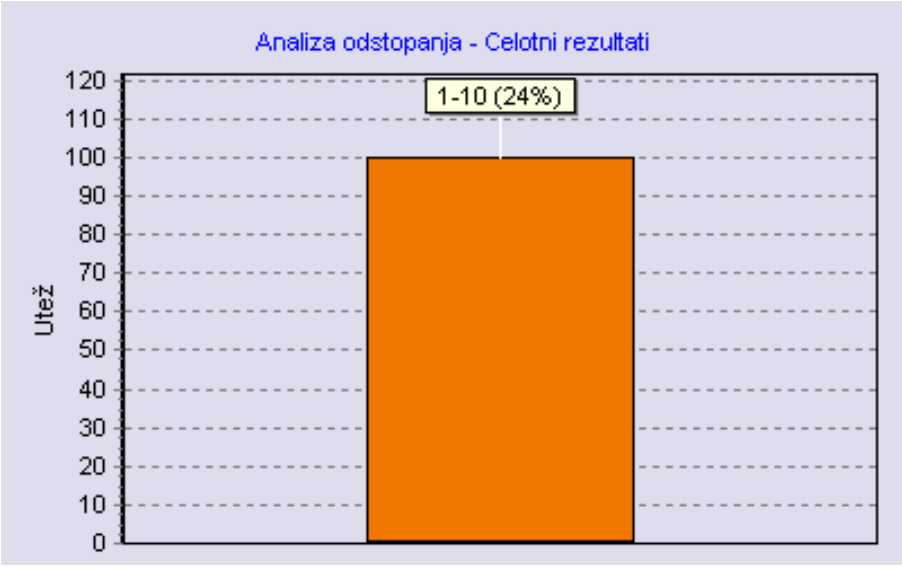
- vprašanja, pri katerih se odgovori med seboj izključujejo (en možen odgovor),
- vprašanja, pri katerih lahko izberete več odgovorov (naštevanje).

Vsi vprašalniki so sestavljeni hierarhično. Če na hierarhično višje postavljeno vprašanje odgovorimo z "*NE*" oziroma "*Ni izvedljivo*", se možnost odgovarjanja na podrejena vprašanja avtomatično izključi in potrditvena polja se obarvajo sivo.
Vsi odgovori na vprašanja Analize odstopanj so uteženi, kar določa njihovo pomembnost. Odgovor "*Ni izvedljivo*" je vrednoten podobno kot odgovor "*DA*", kar pomeni, da tak odgovor ne povečuje odstopanja od standarda. Pri vprašanjih, kjer je možnih več odgovorov, so glede na težo posameznega odgovora, le-ti različno uteženi.
Vprašalniki z odgovori, na osnovi katerih je izdelana analiza odstopanja, se nahajajo v prilogi.
Rezultati so predstavljeni v grafu s stolpčnimi diagrami (histogrami). Odstopanje od priporočil standarda je v grafu predstavljeno na dva načina:

- *barvno* – vsak stolpec je glede na stopnjo odstopanja drugačne barve:
  zelena barva pomeni, da stanje na področju varovanja informacij ne odstopa od priporočil standarda,
  rdeča barva je indikator največjega odklona od standarda,
  vmesne stopnje so označene z različnimi odtenki oranžne barve,
- *s procenti* – nad stolpcem je v kvadratku izpisana številka vprašanja ter procent skladnosti. 100 odstotkov pomeni, da ni odstopanj od priporočil standarda.

Velikost vsakega stolpca v grafu je v razmerju s faktorjem uteži vprašanja, ki ga stolpec predstavlja. Utež pa predstavlja pomembnost posameznega področja (vprašanja) za dosego skladnosti s standardom. Suma vseh desetih področij (slika 13) je 100 odstotkov. [Poslovni ščit, Hermes SoftLab, 2002-2005]

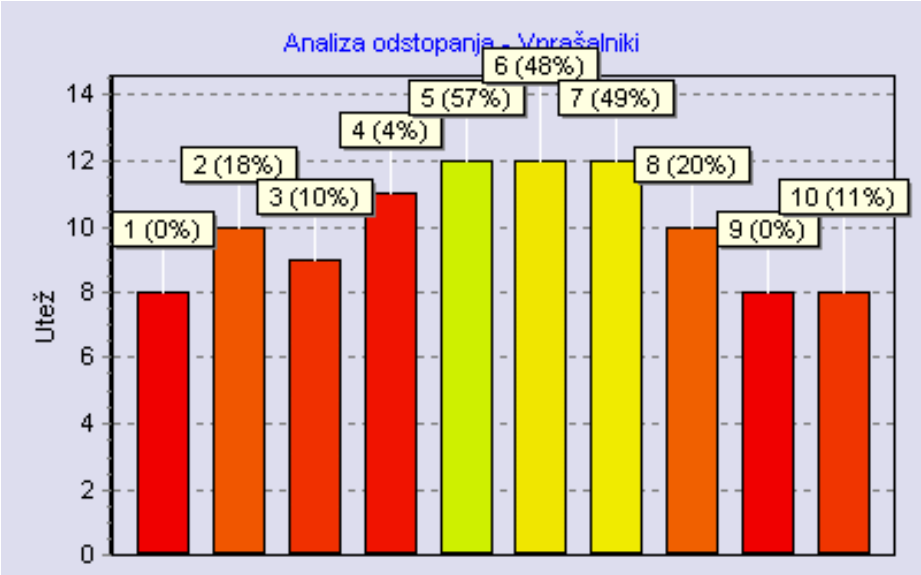
Slika 13: Skupni rezultat analize odstopanja



Vir: Poslovni ščit, Hermes SoftLab, 2002-2005

Skupni rezultat analize odstopanj (slika 13) kaže, da je proučevana organizacija v 24 odstotkih skladna s standardom BS 7799, ali povedano drugače, kar v 76 odstotkih od standarda odstopa.

Slika 14: Analiza odstopanja po posameznih področjih



Vir: Poslovni ščit, Hermes SoftLab, 2002-2005

Slika 14 prikazuje odstopanja po posameznih področjih, kjer so s številkami označena naslednja področja:

1. Politika informacijske varnosti
2. Organiziranost varovanja
3. Razvrstitev in nadzor sredstev
4. Varovanje v zvezi z osebjem
5. Fizična zaščita in zaščita okolja
6. Upravljanje s komunikacijami in s produkcijo
7. Nadzor dostopa
8. Razvoj in vzdrževanje sistema
9. Upravljanje neprekinjenega poslovanja
10. Združljivost

Iz slike 14 je razvidno, da sta v organizaciji kritični predvsem dve področji, in sicer področje 1 Politika informacijske varnosti in področje 9 Upravljanje neprekinjenega poslovanja. Na teh področjih je bila dosežena 0 odstotna skladnost s standardom BS 7799, saj organizacija nima ne politike informacijske varnosti ne politike upravljanja neprekinjenega poslovanja. Področji sta sicer obteženi z najnižjo vrednostjo 8 %, a sta za organizacijo vseeno nujni. Najbolj je organizacija s standardom skladna na področju 5 Fizična zaščita in zaščita okolja, kjer je analiza pokazala 57 % skladnost. Področje je pomembno, saj je uteženo z 12 odstotki. Ostala področja so dosegla od 4 do 49 odstotno skladnost.
Primer izpolnjenega vprašalnika s pripadajočim grafom skladnosti je priložen v prilogi 1.

7. SKLEPNE UGOTOVITVE

Informacije različnih oblik postajajo kri organizacij in brez njih si uspešnega poslovanja ne moremo več predstavljati. Biti morajo neoporečne in v vsakem trenutku razpoložljive, a le pooblaščenim osebam.
Zavest o potrebi po varovanju informacij tudi v slovenskem prostoru pridobiva vse večji pomen. Vsekakor k temu veliko pripomorejo vsakdanje izkušnje z virusi, črvi in druge zlorabe informacijskih sistemov, ki pa žal še vedno kažejo trend povečevanja. Vendar pri varovanju informacij poleg zlorab ne smemo pozabiti tudi na napake in odpovedi strojne ter programske opreme.
Problem informacijske varnosti počasi pridobiva zanimanje v najvišjih vodstvenih krogih organizacij, kar opušča staro miselnost, da je to le naloga službe za informatiko. To zavedanje je še posebej pomembno, kajti varovanje informacij je vodstvena aktivnost, ki mora poleg finančnih sredstev zagotoviti tudi upravljanje znanja, kadrovsko zasedbo in primerno politiko upravljanja. Ta mora biti skladna s poslovnimi interesi organizacije. Sicer pa varovanje informacij brez sodelovanja vseh zaposlenih, pogodbenih delavcev in strank ne more uspeti. Zato je poleg uvedbe varnostnih politik, navodil in standardov, stalno izobraževanje za uspešno varovanje informacij ključnega pomena. Zaradi kompleksnosti področja se je varovanja informacij smiselno lotiti sistematično, in sicer na nivoju celotne organizacije. Celovit način upravljanja varovanja informacij obravnava standard BS 7799. Je mednarodno veljaven standard, namenjen vodstvenemu osebju, ter predstavlja model za učinkovit sistem upravljanja varovanja informacij (SUVI). Standard ISO 17799 je soroden s standardi ISO 9000, ISO 14000 ter ISO 18000, kar organizacijam, ki te standarde že imajo, poenostavi in poceni uvedbo.

Organizacije z resno željo po obvladovanju informacij naj uvedejo sistem za upravljanje varovanja informacij (SUVI). To je vodstveni sistem, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju informacijske varnosti. Organizacija mora v tem videti svoje poslovne priložnosti. Tako kot vsi ostali upravljavski sistemi tudi SUVI za vzpostavitev in upravljanje uporablja procesni pristop načrtuj-stori-preveri-ukrepaj (NSPU). To sistemu omogoča stalno izboljševanje. Za uspešno delovanje SUVI je nujna ustrezna razporeditev vlog in odgovornosti od vodstva organizacije na najvišjem nivoju, do vseh zaposlenih na najnižjem nivoju. Pomembna pa je tudi odgovornost pooblaščenca za informacijsko varnost in varnostnega foruma.
Z uvedbo SUVI lahko pridobimo kar zajeten kup dokumentacije. Smiselno jo je razdeliti v več nivojev, saj s tem dosežemo prehod od strateških usmeritev in ciljev na najvišjem nivoju, prek mehanizmov do konkretnih postopkov in tehnologij na najnižjem nivoju. S tem obenem pridobimo na preglednosti in možnosti omejevanja dostopa do dokumentov posameznega nivoja.

V prvem, teoretičnem delu, naloga prispeva k boljšemu razumevanju samega področja informacijske varnosti. Uporabna vrednost naloge se poleg natančne razlage samega področja kaže tudi v podrobno opredeljenem postopku vpeljave in vzdrževanja SUVI, kar je bil tudi eden izmed ciljev naloge.
Drugi, praktični del naloge, na dva različna načina prikazuje analizo odstopanj od priporočil standarda BS 7799. Analiza odstopanja, narejena po točkah standarda BS 7799, prikazuje realno stanje za vseh 127 kontrol. Za vsako odstopanje so podani tudi predlogi izboljšav za dosego skladnosti s standardom BS 7799. Analiza, narejena z orodjem Poslovni ščit, odstopanje od priporočil standarda BS 7799 ugotavlja preko »pametnih« vprašalnikov. Ta metoda je še posebej zanimiva za predstavitev vodilnim strukturam, saj

so rezultati prikazani grafično. S tem je omogočena vizualna projekcija pomembnosti področja in stopnja odstopanja od standarda.
Obe analizi kažeta podobno sliko – prva je dokaj podrobna, nekoliko tehnična, s kvalitativnimi rezultati, druga pa poljudna, kvantitativna in vizualno nazorna.
Oba modela analize pa tudi rezultati odstopanj s predlogi izboljšav so uporabni za vse slovenske organizacije, dosežen pa je tudi eden izmed ciljev magistrske naloge.

Da sta bila oba zastavljena cilja naloge uspešno dosežena, kaže tudi dejstvo, da je najvišje vodstvo proučevane organizacije na predstavitvi teoretičnega in praktičnega dela (analiza odstopanja) naloge privolilo v začetek projekta uvedbe SUVI. Avtorju dela pa je predsednik uprave podelil vlogo pooblaščenca za informacijsko varnost.

Uporabna vrednost naloge se kaže tudi v nekaterih priloženih predlogah, ki so lahko v pomoč pri izdelavi dokumentacije SUVI.

8. LITERATURA

1. Andolšek Irena, Sedej Branka: Sestavine varnostne politike. Revizor, Ljubljana, št. 7-8, 2002, str. 39-56.
2. Berčič Boštjan et al.: Ukrepi v primeru informacijskih nesreč. Nova Gorica: Inštitut za informacijsko varnost, 2003a.
3. British standard BS 7799-2:2002: Slovenski prevod standarda, Information security management systems. Specification with guidance for use. [Part 2], Palsit. Nova Gorica, 2003.
4. British standard BS ISO/IEC 17799:2000: Slovenski prevod standarda, Information technology. Code of practice for information security management, Palsit. Nova Gorica, 2002.
5. British standard BS ISO/IEC TR 13335 Part 2: Managing and planing IT security, British Standards Institutions. London, 1999.
6. British standard BS ISO/IEC TR 13335 Part 5: Management guidance on network security, British Standards Institutions. London, 2001.
7. British standard PAS 56: Guide To Busines Continuity Management, British Standards Institutions. London, 2003.
8. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju. Ljubljana: Ekonomska fakulteta, 1996.
9. Gradišar Miro: Uvod v informatiko. Ljubljana: Ekonomska fakulteta, 2003.
10. Hvala Davor: Priprava na katastrofo. Sistem-Priloga revije Monitor, Ljubljana, Infomediji, št.11, november 2002, str. 24-26.
11. Iwanowsky Dmitri: Definicija virusa, 1892.
12. Janežič Damjan et al.: Grožnje elektronskega poslovanja – upravljanje z informacijskimi tveganji. Nova Gorica, IZIV, 2004.
13. Jauševec Matjaž et al.: Analiza varnostne ogroženosti. Ljubljana: Uporabna informatika, št 2, letnik XI, 2003, str. 61-67.
14. Jerman-Blažič Borka et al.: Elektronsko poslovanje na internetu. Ljubljana: GV Založba, 2001.
15. Kajić Milan et al.: Mehanizmi varovanja podatkov pri elektronskem poslovanju Statističnega urada RS, Elektronsko poslovanje in statistika, Statistični dnevi 99, Radenci, 1999.
16. Ključevšek Rado: Standard za varnost. Sistem-Priloga revije Monitor, Ljubljana, Infomediji, št.9, september 2002a, str. 18-19.
17. Konečnik Tadeja: Novi standard za varnost podatkov. Gospodarski vestnik, priloga I&T, Ljubljanam 2002, str. 22-23.
18. Makarovič Boštjan et al.: Internet in pravo, Izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu. Ljubljana: Pasadena, 2001.
19. Plate Angelika, Ted Hamphreys: PD 3001, Preparing for BS 7799-2 certification. British Standards Institutions, London, 2002a.
20. Plate Angelika, Ted Hamphreys: PD 3002, Preparing for BS 7799-2 certification. British Standards Institutions, London, 2002b.
21. Plate Angelika, Ted Hamphreys: PD 3003, Are you ready for a BS 7799-2 audit? British Standards Institutions, London, 2002c.
22. Plate Angelika, Ted Hamphreys: PD 3004, Guide to the implementation and auditing of BS 7799 controls. British Standards Institutions, London, 2002d.
23. Plate Angelika, Ted Hamphreys: PD 3005, Guide on the selection of BS 7799-2 controls. British Standards Institutions, London, 2002e.
24. Rakovec Sašo et al.: Varovanje podatkov v računalniško podprtem informacijskem sistemu. Seminarsko delo, Kranj, 1995.

25. Rakovec Sašo: Iskraemeco vzpostavlja celovit sistem obvladovanja informacijske varnosti, Varnostni forum, Palsit, februar 2005a, str. 6-7.
26. Smith, D.J.: A recipe for chaos, Risk management bulletion, 6 (1), 9-14, 2001.
27. Svetič Barbara: Vam kradejo informacije?, Gospodarski vestnik, Ljubljana, 27.5.2002.
28. Šušnjar Goran: Revizija upravljanja informacijske tehnologije. Magistrsko delo. Ljubljana, 2000.
29. Talib Damij, Mojca Indihar Štemberger: Uvod v poslovno informatiko in računalništvo. Ljubljana: Ekonomska fakulteta, 1995.
30. Tič Danilo, Strašek Vilijem: Integracija sistema vodenja organizacije. samozaložba, 2004.

9. VIRI

1. Berčič Boštjan: Skladnost varnostnih politik z zakonodajo, Bilten konference INFOSEC 2003, Inštitut za informacijsko varnost, Nova Gorica, 2003.
2. CSI/FBI Computer crime and Security Survey 2004, Computer Security Institut, 2004.
3. Hajtnik Tatjana: Izdelava varnostne politike. Interno gradivo. Nova Gorica: Palsit, d.o.o, 2004.
4. Inegrirani poslovnik vodenja. Interno gradivo. Kranj: Iskraemeco, 2002.
5. Ključevšek Rado, Vodopivec Tadej: Obvladovanje informacij po BS 7799 in ocena tveganj, gradivo za delavnico, Ljubljana, 2002b.
6. Mednarodno piratstvo. [URL:http://www.microsoft.com/Slovenija/piratstvo/basics/ww/], Microsoft, 10.2.2005
7. Najpogostejši virusi. [URL:http://www.kivi.si/Content.asp?NewsID=74], Kivi, 20.1.2005.
8. Oblike informacij. [URL:http://emea.bsiglobal.com/InformationSecurity/Overview/index.xalter], BSI, 23, 10, 2004.
9. Ocena tveganj. [URL:http://www.hicsalta.si/storitve/storitve-s7.htm], Hicsalta, 3.12. 2004.
10. Organizacijska shema. Interno gradivo. Kranj: Iskraemeco, 2004.
11. Poročilo podjetja F-Secure o informacijski varnosti za leto 2004, 2004.
12. Poslovni ščit. Hermes SoftLab, 2002-2005.
13. Predstavitev podjetja. Interno gradivo. Kranj: Iskraemeco, 2003.
14. Prodajni program. Interno gradivo. Kranj: Iskraemeco, 2003.
15. Računalniško piratstvo. [URL:http://www.bsa.si/piratstvo.php], BSA, 14.4.2005.
16. Rakovec Sašo: Predstavitev Sistema za upravljanje varovanja informacij upravi, Interno gradivo, Kranj: Iskraemeco, 2005b.
17. Sklep banke Slovenije. Ljubljana: Uradni list Republike Slovenije, št. 83, 2004.
18. Slovenija in standard BS7799. [URL:http://www.danesa.com/default.asp?action=article&ID=31], Danesa, 22.3.2005.
19. Sorodnost med standardi. [URL:http://www.bs-7799.org/vprasanja.asp], Danesa, 12.2.2005.
20. Strategija informacijske varnosti. [URL:http://www.palsit.com/index.php?particle=21], Palsit, 12.1.2005.
21. Tarnanje o prevarah, Symantec bilten, CHO, številka 1, Ljubljana, 2004.

Priloga 1: Analiza odstopanja

1.1. Organiziranost varovanja

1. Ali vodstvo organizacije razume vprašanje varovanja informacij kot eno od poslovnih aktivnosti in odgovornosti (kar se odraža na primer v ustreznih organih, lastništvu virov, angažiranju svetovalcev, nabavi virov in pogodbah)?
   ☐ Da ■ Ne

1.1 Ali v organizaciji obstaja strateški organ (ali član poslovodnega odbora), ki daje vodstvu organizacije smernice in podporo na področju varovanja informacij?

☐ Da ■ Ne

1.1.1 Ali je strateški organ član (del) uprave ali poslovodnega odbora organizacije?
☐ Da ■ Ne

1.1.2 Kaj od spodaj naštetega sodi med zadolžitve strateškega organa? Ustrezno označite:

- ☐ Ocenjevanje in potrjevanje politike varovanja informacij na nivoju organizacije.
- ☐ Spremljanje ključne spremembe pri izpostavljenosti grožnjam informacijskemu premoženju.
- ☐ Spremljanje in ocenjevanje varnostnih incidentov.
- ☐ Potrjevanje pobud in predlog za povečanje varnosti informacij.

1.2 Ali obstaja medoddelčni odbor, ki bi koordiniral mere in ukrepe varovanja informacij?

- ☐ Da.
- ■ Ne.
- ☐ Ni izvedljivo zaradi majhnosti organizacije.

1.2.1 Ali so v tem odboru vodje oddelkov oz. njihovi predstavniki vseh vpletenih delov organizacije?
☐ Da ■ Ne

1.2.2 Kaj od spodaj naštetega sodi med zadolžitve odbora? Ustrezno označite:

- ☐ Potrjevanje posebnih vlog in odgovornosti na področju varovanja informacij.
- ☐ Potrjevanje posebnih metodologij in postopkov za varovanje informacij.
- ☐ Sprejemanje in podpiranje pobud za varovanje informacij na ravni organizacije.
- ☐ Zagotavljanje vključevanja področja varnosti v procese informacijskega načrtovanja.
- ☐ Usklajevanje uvajanja posebnih ukrepov za varovanje informacij novih sistemov in storitev.
- ☐ Pospeševanje vidnosti poslovne podpore na področju varovanja informacij.
- ☐ Spremljanje in ocenjevanje varnostnih incidentov.

1.3 Ali je lastništvo nad informacijskimi sistemi znotraj organizacije jasno določeno in je varnost razumljena kot odgovornost lastnika?
☐ Da ■ Ne

1.4 Ali je nedvoumno definirana odgovornost za zaščito posameznega kosa premoženja in za izvajanje posebnih varnostnih postopkov?
☐ Da ■ Ne

1.5 Kaj od spodaj naštetega s področja odgovornosti in pooblastil je v organizaciji vpeljano? Ustrezno označite:

- ☐ Ugotovitev in jasna opredelitev sredstev ter varnostnih postopkov v posameznih sistemih.
- ☐ Uradna potrditev in dokumentiranje odgovornosti za sredstvo ali postopek.
- ☐ Jasna opredelitev in dokumentiranje ravni pooblastil.

1.6 Ali je vzpostavljen postopek odobritve nabave in namestitve vseh novih naprav informacijske tehnologije?
■ Da ☐ Ne

1.6.1 Ali je postopek odobritve za nabavo in namestitev vseh novih naprav informacijske tehnologije potrjen s strani vodstva organizacije?
■ Da ☐ Ne

1.6.2 Katera od naslednjih pooblastil se upoštevajo pri nabavi in namestitvi novih naprav informacijske tehnologije? Ustrezno označite:

- ☐ Odobritev vodstva uporabniku.
- ☐ Tehnična odobritev s potrdilom o skladnosti z ostalimi varnostnimi politikami in zahtevami.
- ☐ Tehnična odobritev s potrdilom o skladnosti z ostalimi sistemskim komponentami.
- ☐ Odobritev uporabe lastnih naprav informacijske tehnologije.

1.7 Ali se za zagotavljanje varnostnih odločitev angažirajo svetovalci za področje varovanja informacij?
■ Da ☐ Ne

1.7.1 Ali se angažirajo notranji svetovalci za področje varovanja informacij?

- ☐ Da.
- ☐ Ne.
- ■ Ni izvedljivo.

1.7.2 Ali se angažirajo zunanji svetovalci za področje varovanja informacij?

- ■ Da.
- ☐ Ne.
- ☐ Ni izvedljivo.

1.7.3 Ali je svetovalcem za varovanje informacij omogočen neposreden dostop do vodstvenih delavcev po vsej organizaciji?
☐ Da ■ Ne

1.8 Ali obstaja sodelovanje med zunanjimi varnostnimi strokovnjaki (organi, ki izvajajo zakone, ponudniki storitev informacijske tehnologije in operaterji telekomunikacij) in notranjimi svetovalci za varnost v smislu doslednega zagotavljanja varnostne prakse?
■ Da ☐ Ne

1.9 Ali se omejuje izmenjavanje varnostnih informacij iz organizacije navzven?
☐ Da ■ Ne

1.10 Ali se izvaja neodvisen pregled učinkovitosti in izvedbe politike varovanja informacij?
☐ Da ■ Ne

1.11 Ali so tveganja, ki zadevajo dostop (tako fizični kot logični) tretjih strank do naprav informacijske tehnologije, ocenjena in so uvedena ustrezna varnostna nadzorstva?
☐ Da ■ Ne

1.12 Ali obstajajo pogodbe s tretjimi strankami in drugimi organizacijami, ki imajo dostop do naprav informacijske tehnologije?

■ Da.
☐ Ne.
☐ Ni izvedljivo.

1.12.1 Ali obstajajo pogodbe s tretjimi strankami, ki imajo dostop do naprav informacijske tehnologije v organizaciji, in te pogodbe določajo varnostne pogoje (način dostopa, pooblaščenost uporabnikov, zakonske obveznosti ...)? Ustrezno označite:

☐ Da, oboje.
■ Da, vendar brez varnostnih pogojev.
☐ Ni formalnih pogodb.

1.12.2 Ali so natančne varnostne zahteve vključene v formalne pogodbe med strankami, če sta upravljanje in nadzorovanje celotnih ali delnih informacijskih sistemov, omrežij ali namiznih okolij oddana drugim organizacijam?

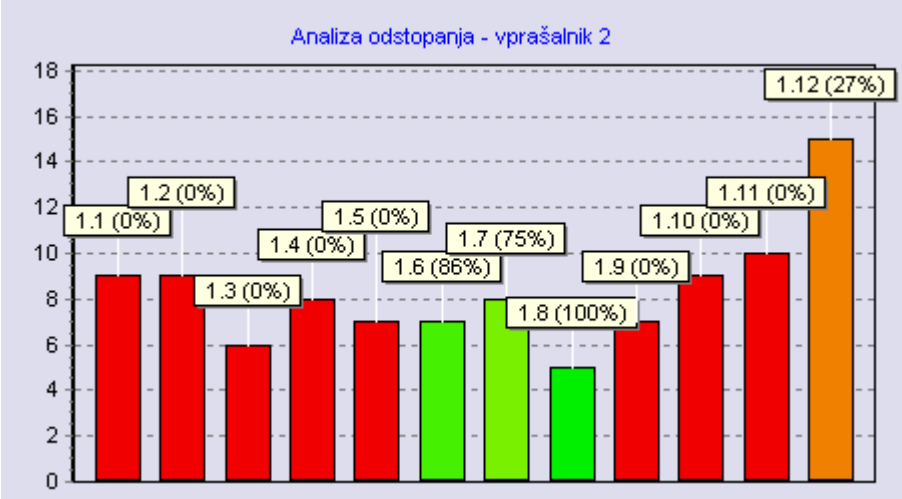
☐ Da.
■ Ne.
☐ Ni izvedljivo.

1.12.3 Kaj od spodaj naštetega je vključeno v pogodbe oddajanja opravil drugim organizacijam? Ustrezno označite:

☐ Usklajenost z zakonskimi zahtevami.
■ Sporazum o zavedanju varnostnih odgovornosti vseh vpletenih strani.
☐ Način preizkušanja in zagotavljanja celovitosti in tajnosti poslovnih virov organizacije.
■ Fizična in logična nadzorstva za omejitev dostopa do občutljivih informacij.

- ☐ Razpoložljivost storitev v primeru katastrofe.
- ☐ Stopnja fizičnega varovanja opreme ostalih organizacij.
- ☐ Pravice revizije.

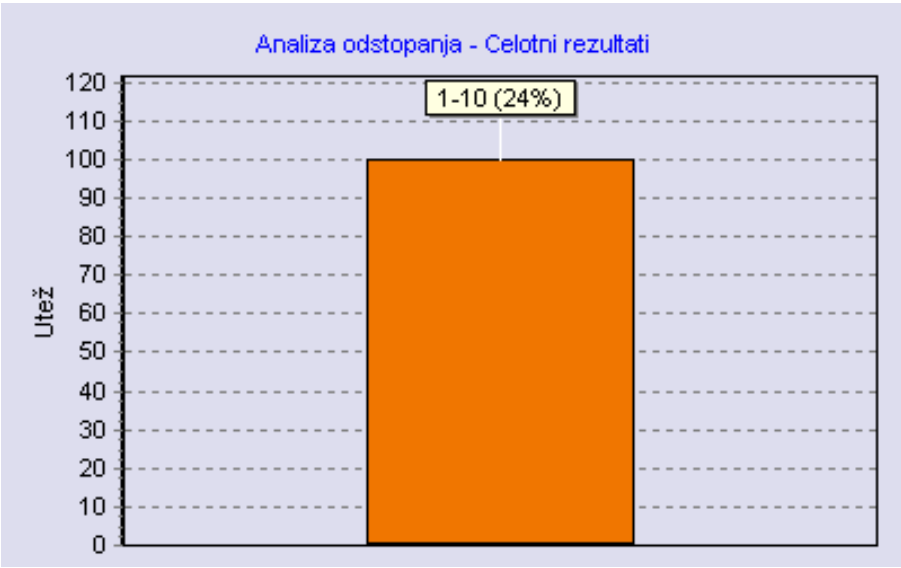
Slika 15: Analiza odstopanja za področje politike organiziranosti varovanja



Vir: Poslovni ščit, Hermes Softlab

Slika 15 prikazuje, da je organizacija pri vprašanjih 1.1, 1.2 1.3, 1.4, 1.5, 1.9, 1.10, 1.11 s področja organiziranosti varovanja popolnoma neskladna s standardom, delno skladna pri vprašanju 1.12, dokaj skladna pri vprašanjih 1.6 in 1.7 ter popolnoma skladna pri vprašanju 1.8.

Slika 16: Skupni rezultat analize odstopanja



Vir: Poslovni ščit, Hermes Softlab

Slika 16 prikazuje skupni rezultat analize odstopanja. Organizacija je na vseh desetih področjih skupaj skladna v 24 odstotkih oziroma v 76 odstotnih neskladna s standardom.

Na podlagi določb o varovanju poslovne skrivnosti, vsebina analize odstopanja ostalih področij ni na voljo.

Priloga 2: Izjava o varovanju informacij

IZJAVA O VAROVANJU INFORMACIJ

Spodaj podpisani _____ izjavljam, da sem seznanjen z Informacijsko varnostno politiko organizacije, se z njo strinjam in bom njena določila dosledno upošteval.

V primeru kršitve te politike se lahko sprožijo ukrepi, kot jih predvideva veljaven disciplinski postopek. Glede na interes organizacije se lahko uporabijo tudi drugi, nedisciplinski ukrepi.

Ta izjava je napisana v dveh izvodih, od katerih prejme en izvod podpisnik, drugega pa pooblaščenec za informacijsko varnost.

Kranj, dne_____ Podpisnik:_____

Priloga 3: Popis sredstev

Tabela 7: Popis sredstev

Popis sredstev

Področje / Organizacijska enota:

Odgovornost:

Datum:

Tip sredstva:

npr. **Fizična sredstva**

Številka sredstva	**Naziv sredstva**	**Lastnik**	**Skrbnik**	**Lokacija**	**Vrednost** Zelo velika (ZV), Velik (V), Srednja (S), Nizka (N)	**Opombe**

Vir: Interno gradivo Iskraemeco

Priloga 4: Poročilo o incidentu

Poročilo o incidentu

Oznaka:
Naslov:
Datum vnosa:
Datum incidenta:
Trajanje izpada:

Podrobnosti o incidentu
Podrobnosti reševanja
Podrobnosti o nastali škodi
Podrobnosti odkritja

Kraj odkritja:

Datum in ura odkritja:

Odkril:

Podrobnosti o storilcu

Storilec identificiran:

Storilec:

Način identifikacije:

Podrobnosti o izboljšavi

Poročilo sestavil:

Priloga 5: Primer politike elektronske pošte

Politika elektronske pošte

CILJ

Preprečiti izgubo, spremembo ali zlorabo informacij in nepooblaščen dostop do njih, spremembo ali zavrnitev storitev ter zmanjšati možnost napačnega odpošiljanja elektronske pošte.
Zagotoviti splošno zanesljivost in dostopnost storitve, učinek hitrejšega odpošiljanja, možnost morebitnega dokazovanja izvora odpošiljanja, dostave in prejema elektronske pošte. Vse uporabnike seznaniti z njihovimi pravicami in odgovornostmi v povezavi z elektronsko pošto.

.

SPLOŠNA PRAVILA

Uporaba sistema elektronske pošte

Sistem elektronske pošte se uporablja samo v službene namene.
Uporabniki morajo sistem elektronske pošte uporabljati v skladu z veljavnimi predpisi, učinkovito, etično in odgovorno. Nedopustna je uporaba, ki je v nasprotju z veljavnimi predpisi, neetična ali kakor koli škoduje ugledu organizacije.

Pravice nad podatki

Vse pravice nad sistemom elektronske pošte in vsemi sporočili pripadajo organizaciji.

Uporaba elektronske pošte s tretjimi strankami

Če uporabnik pošlje sporočilo, ki navaja njegovo osebno mnenje in ne mnenja organizacije, mora to jasno izraziti (npr. »To je osebno mnenje« ali »Izraženi pogledi so v popolnosti avtorjevi in se pod nikakršnimi pogoji ne smejo šteti kot uradno stališče organizacije«).

ELEKTRONSKI POŠTNI PREDAL

Odpiranje in zapiranje predala

Organizacija ima enoten elektronski poštni predal info@podjetje.si in elektronska sporočila, ki prispejo v ta predal, odpirajo samo pooblaščene osebe (npr. marketing).
Za potrebe, kot so npr. projekt ali neka skupina, se lahko po potrebi odprejo namenski predali. Elektronska sporočila, ki prispejo v te poštne predale, odpirajo za to odgovorne osebe.
Ob sklenitvi delovnega razmerja, na zahtevo vodja PE/PF (Zahtevek za dodelitev/ukinitev uporabniških pravic) in ob potrditvi vodje Informatike, upravitelj sistema elektronske pošte uporabniku odpre njegov osebni predal.
V primeru prenehanja uporabe poštnega predala (Zahtevek za dodelitev/ukinitev uporabniških pravic) je potrebno navesti, kaj storiti z vsebino predala, oziroma kdaj se predal dokončno zapre.

Uporaba predala
Uporabnik ne sme uporabljati predala, ki je bil dodeljen drugemu uporabniku, oziroma lahko to stori na njegovo izrecno odobritev (pooblastilo).
Prav tako ne sme uporabljati predala za pridobitne dejavnosti, razpošiljanje komercialnih informacij in nezakonite namene.
Uporabnik ne sme uporabljati elektronske pošte za zasipanje z elektronskimi sporočili (spam, junk e-mail: nenaročena reklamna gradiva, napadalna sporočila, verižna sporočila, oz. ostalih sporočil, ki ne služijo službenim namenom). Pošiljanje elektronske pošte večjim skupinam oz. celotni organizaciji je dovoljeno le z odobritvijo upravitelja.

Privzete nastavitve predala
Uporabnik ne sme spreminjati nastavitev svojega predala, razen v primeru nujnih in predpisanih vzdrževalnih del. Za uporabo katerihkoli dodatnih pripomočkov mora uporabnik pridobiti odobritev upravitelja.

ELEKTRONSKA SPOROČILA

Velikost elektronskih sporočil
Največja velikost pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena. Če je omejitev presežena, se sporočilo avtomatično zavrne, pošiljatelj pa o zavrnitvi dobi obvestilo.
Organizacija nima omejitve glede velikosti poslanih oz. prejetih elektronskih sporočil.

Načelo racionalnosti in varnosti
Pri pošiljanju elektronskih sporočil morajo uporabniki upoštevati načelo racionalnosti in varnosti. Če je mogoče, naj se večji pripeti dokumenti pred pošiljanjem pretvorijo v manj potratne podatkovne formate. Pošiljanje multimedijskih datotek ni dovoljeno. Dokumente, ki vsebujejo makre in drugo izvršno kodo, je potrebno pretvoriti v obliko, ki ob odpiranju ne omogoča samodejnega proženja izvršilne kode. Vse priponke morajo biti evidentirane v tekstovnem delu sporočila, tako da bo naslovnik lahko zanesljivo prepoznal njihov namen že iz spremljajočega opisa.
Uporabniku se ni dovoljeno prijavljati na elektronske poštne sezname, če ti niso vsebinsko povezani z delom, ki ga opravlja v okviru organizacije.

Odpiranje elektronskega sporočila
Prepovedane so vse oblike, posredovanje, prestrezanje ali snemanje elektronskih sporočil, ki potekajo na način, ki izključuje uporabo uporabniškega imena in gesla v okviru predala.
Če uporabnik po pomoti prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega sporočila ne sme shraniti ali uporabiti v katerikoli namen. O pomoti je dolžan obvestiti pošiljatelja, sporočilo pa mora nemudoma zbrisati. Če je iz sporočila nedvoumno razvidna identiteta pravega naslovnika, lahko pred izbrisom to sporočilo tej osebi tudi pošlje.

Zagotavljanje zaupnosti
Organizacija v okviru tehnoloških možnosti in pravil stroke zagotavlja zaupnost in tajnost elektronskih sporočil.
Kljub zagotavljanju varnosti in zaupnosti s strani upravitelja, se mora vsak zaposleni zavedati, da se elektronsko pošto lahko posreduje naprej, se ji prisluškuje, prestreza, tiska in shranjuje s strani drugih.

Preusmeritve elektronskih sporočil
Preusmeritve elektronskih sporočil so dovoljene samo znotraj sistema oziroma samo preko sistemov in v sisteme z najmanj tako stopnjo varnosti, kot jo ima sistem, iz katerega se sporočilo preusmerja.
Če se pojavi potreba po dostopnosti službenega poštnega predala izven delovnega mesta, so zato zagotovljeni drugi načini (VPN, dostop preko brskalnika).

Posredovanje in prejemanje elektronskih sporočil
Pri izmenjavi dokumentov oziroma elektronskih datotek veljajo varnostna pravila, ki veljajo za klasično pošto. Izvršljivih programov (.exe, .com …), ki so lahko pripeti k elektronskemu sporočilu, ni dovoljeno naložiti, inštalirati in poganjati brez odobritve odgovorne osebe. To velja tudi za programe tipa »shareware« in »freeware«.
Uporabniki morajo spoštovati avtorske pravice in pravila intelektualne lastnine, in sicer to še posebej tako, da ne uporabljajo sistema elektronske pošte za razpošiljanje avtorsko zaščitenih informacij ali računalniških programov.
Zaupnih in tajnih podatkov po elektronski pošti ni dovoljeno pošiljati.

Brisanje elektronskih sporočil
Kvota poštnega predala je omejena na 50 MB. Zato mora uporabnik elektronska sporočila, ki za organizacijo nimajo več vrednosti, periodično brisati.

Arhiviranje elektronskih sporočil
Elektronska pošta se po določenem času avtomatsko arhivira. Kadar arhivirana sporočila ponovno potrebujemo, jih je mogoče iz arhiva ponovno povrniti.

Računalniški virusi
Uporabniki elektronske pošte:

- ne smejo namerno nameščati računalniških virusov na računalnik, ali jih namerno pošiljati po elektronski pošti, razen v primeru, ko gre za pošiljanje vzorcev v preverjanje zato pooblaščeni osebi,
- ne smejo zaganjati priponk in dokumentov v elektronski pošti, če ne vedo, čemu takšni programi ali dokumenti služijo ali če ne poznajo njihovega izvora,
- naj sumljiva sporočila zbrišejo,
- ne smejo razpošiljati obvestil o morebitnih novih virusih tudi takrat, ko so prepričani, da ne gre za lažna obvestila.

UPRAVITELJI

Posebna pooblastila
Za varno in nemoteno delovanje sistema elektronske pošte skrbijo upravitelji elektronskih poštnih strežnikov.
Upravitelji ne smejo sebi ali komu drugemu pridobiti informacije o vsebini, dejstvih ali okoliščinah prenesenih sporočil, ki presegajo najmanjšo potrebno mero za upravljanje in zagotavljanje delovanja sistema.

Vzdrževalna dela

V primeru planiranih vzdrževalnih del na programski ali komunikacijski opremi so upravitelji dolžni predhodno obvestiti uporabnike o morebitnih motnjah, niso pa odgovorni za motnje, ki nastanejo izven njihovih pristojnosti.

Če je potrebno ugotoviti vzroke za težave oziroma napake v delovanju sistema elektronske pošte, lahko upravitelji (ob upoštevanju Zakona o varstvu osebnih podatkov) pregledujejo tudi vsebino elektronske pošte.

Pregledovanje iz radovednosti ali po nalogu nepooblaščenih posameznikov ni dovoljeno.

Upravitelj mora vse pridobljene podatke varovati kot zaupne in jih uporabljati izključno v zgoraj navedene namene.

NADZOR

Registracija posegov

Upravitelj mora za potrebe zakonitega in neodvisnega nadzora zagotoviti neizbrisno registracijo posegov nadzora sistema elektronske pošte.

Sledenje

Upravitelji lahko v primeru zlonamernih ali škodljivih sporočil vzpostavijo sledenje takim sporočilom in ugotavljajo identiteto pošiljatelja.

Zbiranje statističnih podatkov

Upravitelji lahko zbirajo statistične podatke, povezane z uporabo sistema elektronske pošte.

Uporaba teh podatkov je namenjena izključno za spremljanje in zagotavljanje razpoložljivosti in zanesljivosti ter načrtovanje zmogljivosti elektronske pošte.

Na osnovi pisne zahteve vodstva organizacije je dovoljeno tudi zbiranje podatkov o uporabi elektronske pošte posameznega uporabnika. Tu gre predvsem za ugotavljanje prekomerne uporabe oziroma zlorabe sistema elektronske pošte v neslužbene namene.

KRŠITVE POLITIKE ELEKTRONSKE POŠTE

V primeru kršitve te politike se lahko sprožijo ukrepi, ki jih predvideva veljaven disciplinski postopek. Glede na interes organizacije se lahko uporabijo tudi drugi, nedisciplinski ukrepi.

Tako imajo upravitelji pravico do takojšnje blokade in morebitne naknadne ukinitve poštnega predala, kadar ugotovijo kršitev določil te politike.

Priloga 6: Zahtevek za dodelitev/ukinitev uporabniških pravic

*(*Izpolni Informatika)*

Številka

(Izpolni predlagatelj)

Predlagatelj(PE/PF, oddelek, del.št.)	*Telefonska št.*	*Datum*

Vzrok(ustrezno obkroži): *DODELITEV* *UKINITEV* Delo v aplikacijah: Lotus Notes, Baan, Podatkovno skladišče, Internet *Želeni rok:*
Opis del: *Priloge:*

Predlagal	*Datum*	*Odobril*	*Datum*	*Prevzel*	*Datum*

*(*Izpolni Informatika)*

Izvršene spremembe ali dopolnitve: *Podatki o spremembi ali dopolnitvi:*

Izvršil	*Datum*	*Odobril*	*Datum*	*Prevzel*	*Datum*

Priloga 7: Zadolžitve in postopki v primeru izpada posameznega informacijskega sredstva

Zadolžitve in postopki v primeru izpada posameznega IS

INFORMACIJSKI SISTEM

Informacijski sistem/rešitev:

Lastnik/nosilec področja:

Kontaktna oseba:

Ključni dobavitelji:

ZADOLŽITVE

Odgovoren za izvedbo:

Izvajalec:

Zadolžen za obveščanje:

Obvestiti:

PREDVIDEN ČAS OBNOVE SISTEMA

Predviden čas celotne obnove sistema (glede na vzrok izpada):

Predviden čas obnove prioritetnih delov sistema (glede na vzrok izpada):

REŠEVANJE

Postopek reševanja (glede na vzrok izpada):

POMEMBNO

Ne pozabi:

Priloga 8: Izjava o primernosti

Tabela 8: Izjava o primernosti

Izjava o primernosti

BS 7799-2: 2002 Kontrolni cilji in kontrole

Št.	**Kontrolni cilj**	**Kontrola**	**Primerna (D/N)**	**Sklic na dokument**
6.	**Varovanje v zvezi z osebjem**			
6.1.	Varovanje pri opredelitvi dela in pridobivanju novih sodelavcev	6.1.1. Vključevanje varovanja med službene odgovornosti		
		6.1.2.Politika in preverjanje uslužbencev		
		6.1.3. Sporazum o zaupnosti		
		6.1.4. Pogoji zaposlovanja		
6.2.	Usposabljanje uporabnikov	6.2.1.Izobraževanje in usposabljanje za varovanje inf.		
7.	**Fizična zaščita in zaščita okolja**			
	7.1. Varovana območja	7.1.1. Fizični varnostni pas		
		7.1.2. Kontrola fizičnega dostopa		

Vir: Interno gradivo Iskraemeco