UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

LUKA TOMAT

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

SISTEM ZA UPRAVLJANJE VAROVANJA INFORMACIJ TER SKLADNOST POSLOVANJA V GORENJSKI BANKI S STANDARDOM BS 7799

Ljubljana, september 2007 LUKA TOMAT

IZJAVA

Študent **Luka Tomat** izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom **dr. Tomaža Turka** in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis_____

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

Varovanje informacij postaja v vsakdanjem življenju čedalje pomembnejše na vseh področjih. Porajajo se vedno večje možnosti za učinkovitejše upravljanje z različnimi informacijami, žal pa se povečujejo tudi možnosti za njihovo zlorabljanje. Za podjetja je smotrno, da nenehno povečujejo in izboljšujejo stopnjo varovanja informacij, saj lahko le tako preprečijo veliko škodo, ki bi nastala ob morebitnem izpadu komunikacijskega ali informacijskega sistema.

Organizacija lahko na najboljši možni način upravlja z varovanjem informacij, če upošteva priporočila standarda BS 7799, ki ga uporabljajo različne organizacije širom celega sveta. V grobem zajema standard varovanje podatkov in informacij pred nepooblaščenim razkritjem, varovanje točnosti in popolnosti podatkov in informacij in zagotavljanje dostopnosti do informacij v skladu s potrebami uporabnikov (Storitve s področja svetovanja in izobraževanja o varovanju podatkov, 2007).

Za organizacijo je smiselno, da vpelje sistem za upravljanje varovanja informacij, ki deluje po načelu nenehnega izboljševanja, vsebuje pa načrtovanje, uvedbo, preverjanje in ukrepanje. Sistem zajema natančne opredelitve vlog in odgovornosti zaposlenih pri izvajanju varovanja informacij.

Cilj diplomskega dela je opredeliti varovanje informacij in sistem za upravljanje varovanja informacij ter na podlagi standarda BS 7799 analizirati stanje informacijske varnosti v Gorenjski banki, d. d.

Diplomsko delo je razdeljeno na štiri tematska poglavja. Gre za opredelitev varovanja informacij, sledi poglavje o standardu BS 7799, naslednje poglavje opisuje sistem za upravljanje varovanja in formacij, zadnje poglavje pa zajema preverjanje skladnosti Gorenjske banke, d. d., s standardom BS 7799.

2 VAROVANJE INFORMACIJ

2.1 Kaj je informacija in katere so lastnosti informacije

Informacija je rezultat interpretacije podatkov. Je obratno sorazmerna verjetnosti pojava določenega dogodka oziroma podatka – čim manjša ko je verjetnost pojava, tem večja je informacija ob določenem dogodku – podatku (Vidmar, 2002, str. 25).

Informacija je rezultat procesiranja, upravljanja in organiziranja podatkov na način, ki prejemniku informacije omogoča boljše razumevanje in poznavanje določene tematike.

Prejemnik informacije nato interpretira informacijo v skladu s svojimi interesi, na podlagi te interpretacije pa tudi sprejme odločitve, ki ga vodijo k določenemu dejanju. Informacije imajo lahko različne oblike. Lahko so natisnjene ali napisane na papir, lahko so v elektronski obliki, lahko se pošiljajo po posti ali preko elektronskih kanalov, lahko pa je oblika tudi govorne narave.

Lastnosti informacije delimo na (Measures of The Value of Information, 2007):

- pravočasnost: ali je informacija prišla do prejemnika pravočasno,
- zadostnost, dovršenost: ali je informacija primerna za svoj namen,
- združitev: ali so podatki povezani v pomenske enote,
- obilje: če je informacij preveč ali premalo, se lahko pojavi problem,
- razumljivost: uporabnost, preprostost, dojemljivost,
- zanesljivost: ali je informacija preverljiva,
- primerljivost: omogoča primerjanje informacij,
- velikost: kako obsežna je informacija, kvantiteta podatkov ne pomeni boljše informacije.

2.2 Kaj pomeni varovanje informacij

Informacije v podjetjih so vse bolj pomemben dejavnik poslovanja. Za podjetje imajo veliko vrednost, zato je še toliko bolj pomembno njihovo varovanje pred različnimi nevarnostmi, ki so pojasnjene v nadaljevanju diplomske naloge. Namen varovanja informacij je zagotavljanje čim bolj učinkovitega poslovnega procesa podjetja, čim višje uspešnosti investicij podjetja v informacijsko tehnologijo, čim višje konkurenčnosti podjetja na trgu ter odpiranja novih poslovnih priložnosti podjetja (Egan, Mather, 2005, str. 7).

Varovanje informacij zagotavljamo preko treh osnovnih pojmov (Rakovec, 2005a, str. 3):

- zaupnost,
- celovitost,
- razpoložljivost.

Pri varovanju zaupnosti gre za zagotavljanje vpogleda v informacije (kakršnekoli oblike) med njeno obdelavo, prenašanjem ali shranjevanjem le pooblaščenim osebam. Varovanje celovitosti pomeni, da morajo biti informacije vedno natančne in popolne, tako med shranjevanjem in prenašanjem, kakor tudi med samim obdelovanjem. Razpoložljivost informacij pomeni, da so le-te pooblaščenim uporabnikom dostopne, ko jih potrebujejo.

Za varovanje informacij je zelo pomemben sistem upravljanja z njimi, saj temelji na primernosti in učinkovitosti varnostne politike podjetja, ki pa se stalno primerja in zaradi tega tudi izboljšuje.

Ključnega pomena je seznanjenost vseh zaposlenih v podjetju z varnostno politiko podjetja, saj ta za vsako posamezno področje natančno določa, kako ukrepati, če se poveča tveganje in zmanjša nadzor uporabe informacij.

Zaupnost, celovitost in razpoložljivost informacij v podjetju igrajo ključno vlogo pri doseganju višje konkurenčnosti, dobičkonosnosti, boljšega finančnega poslovanja ter boljše skladnosti z zakonodajo, pomembno pa vplivajo tudi na organizacijsko klimo in kulturo podjetja.

Podjetja, predvsem pa njihovi informacijski sistemi, se srečujejo z vse večjimi varnostnimi grožnjami. Gre za računalniški kriminal, industrijsko vohunstvo, sabotaže, naravne nesreče, zlonamerne kode itd. Le standardizirano in organizirano varovanje informacij lahko zmanjša tveganja podjetja na sprejemljivo raven. Podjetje mora določiti svoje posebne varnostne zahteve; le-te se oblikujejo na podlagi ocene tveganja, ki mu je podjetje izpostavljeno, na podlagi obveznosti, ki jih podjetje mora izpolnjevati glede na zakonodajo ter na podlagi posebnih pravil za obdelavo, prenašanje in shranjevanje informacij, ki jih je podjetje oblikovalo za čim boljšo podporo poslovanju. Podjetje mora v vsakem trenutku upoštevati nove grožnje, ki se pojavijo v njegovem okolju. Upravljanje in varovanje informacij mora biti ključnega pomena, predstavljati pa mora stalen proces v podjetju.

2.3 Izpostavljenost informacijskih sistemov nevarnostim

Za podjetje je zelo pomembno, da ima zelo dobro varovanje, saj drugače informacijski sistem ne bi dobro funkcioniral, dobro delovanje sistema pa je ključ do uspeha podjetja. Zlonamerni programi lahko povzročijo ogromno ekonomske škode, zato je zavedanje in poznavanje nevarnosti ključnega pomena.

2.3.1 Manipulacija

Pri manipulaciji gre za to, da nek zunanji napadalec izvaja psihološke trike na računalniških uporabnikih, da bi pridobil informacije, ki jih potrebuje za dostop do kakega informacijskega sistema. Lahko govorimo tudi o socialnem inženiringu. V večini primerov so žrtve socialnega inženiringa telefonske, finančne in državne institucije.

Najbolj razširjene metode socialnega inženiringa so (Bratuša, Verdonik, 2005, str. 118-119):

- prijateljstvo (vstopna gesla se širijo na podlagi zaupanja med zaposlenimi),
- elektronska pošta (ponarejanje naslova pošiljatelja),
- pregledovanje smeti podjetja (razkrije lahko uporabne informacije),

- pregled pisarn (napadalec vohlja po odklenjenih pisarnah in kabinetih),
- zaupanje (napadalec si pridobi zaupanje zaposlenih),
- čas (je vedno na strani napadalca).

Napadalec lahko do žrtve 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, 2003). Najbolj pogosti primeri fizičnih napadov se zgodijo na samem delovnem mestu, preko telefona, preko elektronske pošte ali pa v smeteh podjetja. Vdiralec npr. vstopi v organizacijo in se pretvarja, da je serviser ali pa svetovalec in da je prišel zaradi kritične zadeve. Od zaposlenih lahko tako zahteva le vstopna gesla, ki jih bo pozneje uporabil za vdor in raziskovanje omrežja. Lahko pa se domnevni serviser tudi preprosto razgleduje po pisarni in si ogleda nekaj gesel, ki prav gotov ležijo razmetana okoli. Še bolj preprost način je opazovanje nič hudega slutečega zaposlenega, kako vtipkava svoje geslo.

Veliko informacij pa lahko vdiralec pridobi tudi preko smeti določene organizacije. Tako je lahko v smeteh kakega podjetja npr. telefonski imenik, organizacijska shema, pisma, priročniki, datumi pomembnih dogodkov, zapiski, informacije o zaposlenih itd.

Zelo razširjen je tudi telefonski socialni inženiring. Vdiralec v tem primeru pokliče v podjetje in preko psiholoških trikov prepriča določenega zaposlenega, da mu zaupa svoje podatke. Lahko se izdaja za zunanjega serviserja ali svetovalca, nemalokrat pa se zgodi, da se vdiralec pretvarja, da je nekdo izmed zaposlenih v podjetju. Tako lahko vdiralec pridobi pomembno uporabniško ime in geslo.

Vdiralci lahko dostopajo do različnih uporabniških računov tudi preko elektronske pošte. Gre za pošiljanje nagradnega vprašanja, pri odgovoru pa je treba vpisati tudi uporabnikove podatke, tudi e-poštni naslov, preko katerega potem vdiralec pridobi uporabniško ime in geslo. Slabost uporabnikov je, da za različne račune uporabljajo enaka gesla; to pomeni, da lahko vdiralec vdre v slabo zavarovan forum in v njegovi bazi odčita uporabnikovo geslo, ki ga potem lahko uporabi na bolj zavarovanih sistemih. Lahko pa elektronska pošta vsebuje priponko, ki je nekakšne vrste virus, črv ali trojanski konj.

2.3.2 Kraje in ponaredbe

Nezakonito kopiranje ali distribuiranje programske opreme za poslovno ali osebno rabo imenujemo piratstvo. Obstaja pet vrst piratstva, in sicer ponarejanje, nalaganje na disk, mehko piratstvo, dajanje v najem in spletno piratstvo (Izogibanje nezakoniti programski opremi, 2007).

Piratstvo je zelo razširjeno v svetu in tudi v Sloveniji. Leta 1999 je stopnja piratstva v Sloveniji znašala 70%; to pomeni, da je bilo od 100 računalniških programov le 30 programov pridobljenih legalno (Računalniško piratstvo, 2007). Uporaba piratskih programov negativno vpliva na gospodarstvo, saj razvijalci programske opreme ne dobijo zadostne količine denarja, ki bi lahko vlagali v nadaljnji razvoj novejše programske opreme.

Legalno uporabo programske opreme ureja zakonodaja. Dovoljena je namestitev računalniškega programa na enem samem računalniku, če pa je potrebno, pa je dovoljeno tudi reproduciranje največ dveh varnostnih kopij. Uporaba legalne programske opreme ohranja dobro ime podjetja, daje možnost dostopa do tehnične pomoči proizvajalca ter legalnih nadgradenj, zagotavlja kakovost in operacijsko zanesljivost, priložena pa je tudi popolna dokumentacija programa.

2.3.3 Napake

2.3.3.1 Človeški dejavniki

Največkrat informacijski sistemi nepravilno delujejo zaradi napak uporabnikov. Vzrokov za nastanek teh napak je veliko, najpogosteje pa uporabniki ne upoštevajo navodil, organizacijskih predpisov ali pa so pri delu površni (Gradišar, 2003). Do napak uporabnikov lahko pride tudi zaradi nepoznavanja dela z določenim informacijskih sistemom, nepoznavanja delovanja protivirusne zaščite ali zaradi nezaupanja podjetju. Do nepravilnega delovanja informacijskega sistema pride velikokrat tudi tedaj, če gre za javni računalnik.

Napake uporabnikov lahko skušamo preprečevati. Zato je zelo pomembna usposobljenost uporabnikov (tudi z varnostnega vidika) za delo z določenim informacijskim sistemom. To je širok pojem in predpostavlja izvedbo različnih tečajev in podobnega usposabljanja, možnost dostopa do uporabniških priročnikov, ki morajo biti vedno na voljo, neposredno uvajanje pri delu in, če so težave pomoč na delovnem mestu. Za uporabnika je pomembna tudi motivacija, ki je

pomemben del organizacije poslovanja, saj zagotavlja delovanje uporabnikov v dogovorjenih in predpisanih okvirih na posameznih delovnih mestih (Vidmar, 2002, str. 504).

Nemalokrat so uporabniki kakega informacijskega sistema odgovorni tudi za napake v podatkih. Do njih pride pri vnašanju podatkov kak sistem. Take napake skušamo preprečevati z določenimi kontrolami, vendar pa v večini primerov ne odpravijo napačnega vnosa podatkov, temveč vnos le omejujejo. Največkrat gre za preverjanje dolžine vnosa, tipa spremenljivke ter črkovne in številske karakteristike podatkov.

2.3.3.2 Tehnološki dejavniki

Čeprav je tehnologija vedno bolj razvita, lahko strojna oprema vseeno odpove. Vzroke lahko iščemo v pregrevanju pomembnih komponent strojne opreme, vlagi v okolju, udarcih, preveliki električni napetosti in še bi lahko našteval. Navadno ponudnik strojne opreme vzdržuje tudi sistem oskrbovanja in podpore strojne opreme, kar pomeni, da bo napaka v čim krajšem času tudi odpravljena. Gre za hitro ukrepanje ob morebitnih napakah (na lokaciji ali pa s pomočjo daljinskega diagnosticiranja), odpravo napak in preventivno pregledovanje strojne opreme. Poznamo pa tudi delno odpoved strojne opreme. To pomeni, da naprava deluje, vendar pa so lahko rezultati obdelav napačni. Sodobni informacijski sistemi zaznajo delno odpoved programske opreme in se zaradi varnosti zaustavijo.

Poznamo pa tudi napake, ki povzročijo prenehanje izvajanja kakega programa – programske napake (hrošči). Lahko jih razdelimo v več vrst (Wikipedia, 2007):

- sintaktična napaka: povzroči jo nepravilna uporaba programskega jezika,
- logična napaka: napaka v zasnovi programa,
- napaka med izvajanjem: povzroči jo kombinacija podatkov, ki jo programer ni predvidel,
- napaka prekoračitve: število je preveliko, da bi ga računalnik še lahko obravnaval,
- napaka podkoračitve: število je premajhno, da bi ga računalnik še lahko obravnaval,
- napaka zaokrožitve in odreza: nastanejo pri zaokroževanju oziroma odrezu decimalnih mest; to se zgodi, kadar je število decimalnih mest, ki jih omogoča računalnikova natančnost, preseženo.

Zelo je pomembno, da imajo programi v sebi vgrajena večstopenjska samopreverjanja, saj s tem znatno zmanjšajo možnost pojava napake v programski opremi.

2.3.4 Nesreče

Nesreče so dejavnik tveganja, ki ga podjetje mora upoštevati in temu primerno tudi urejati politiko varovanja strojne in programske opreme. Na naravne nesreče, kot so poplave, potresi, strele in viharji, ne moremo vplivati, niti jih ne moremo predvideti. Pomembno je, da podjetje čim bolj ažurno izdeluje varnostne kopije in jih shranjuje v prostoru, ločenim od prostora, kjer so podatki, ki so tudi na varnostnih kopijah, nastali. Dve izmed najbolj pogostih računalniških nesreč sta požar in izliv tekočine. Obe sta v večini primerov posledica nepazljivega in neodgovornega delovanja uporabnika, v obeh primerih pa je treba čim hitrejše ukrepati, saj se s tem zmanjša možnost negativnih posledic. Še posebno nevarne so nesreče, do katerih pride takrat, ko ni v podjetju nikogar, da bi lahko ukrepal (nočni čas, sindikalni dopust, prenova poslovnega prostora...). Predvsem v nočnem času lahko pride tudi do kraje računalniške opreme.

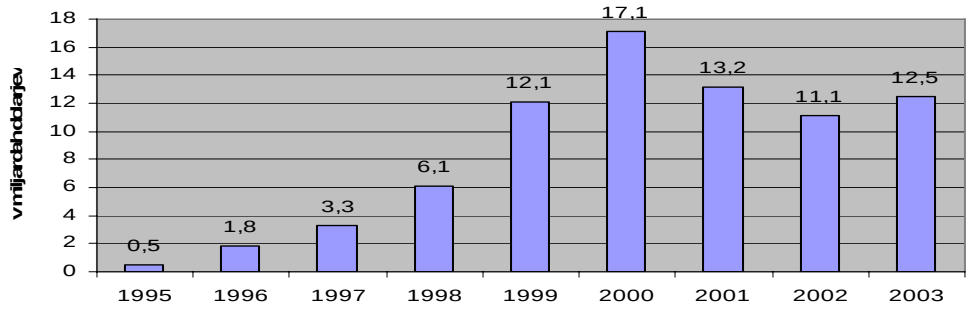
2.3.5 Zlonamerna koda

Gre za računalniško kodo, ki je v računalniškem okolju zlonamerna ali uničevalna. Vanjo lahko uvrščamo viruse, črve, vohune, trojanske konje in kakršnokoli drugačno programsko opremo, ki lahko povzroči škodo posameznemu računalniku, strežniku ali omrežju.

Z zlonamerno kodo se sistem lahko okuži na več načinov. Najpogosteje se v sistem prenesejo preko file sharing programov, kot so eMule, Kazaa, iMesh in drugi. Nekateri se naložijo preko spletnih strani, kjer se izdajajo za program, ki je potreben za ogled spletne strani. Najredkeje pa se naložijo skozi varnostne luknje v spletnem brskalniku, za kar je potreben samo obisk napačne spletne strani (Egan, Mather, 2005, str. 8).

Zlonamerne kode so v preteklosti povzročile tudi veliko ekonomske škode. Slika 1 prikazuje svetovno gospodarsko škodo napadov zlonamerne kode v zadnjih letih.

Slika 1: Gospodarska škoda zaradi zlonamerne kode (v miljardah dolarjev)



Vir: Egan, Mather, 2005, str. 9.

Ni natančno znano, kdaj so se pojavili prvi zlonamerni programi, vendar pa se večina strokovnjakov strinja, da so bili računalniki okuženi s prvimi virusi že sredi sedemdesetih let dvajsetega stoletja. Prva znana žrtev zlonamernega programa je bilo omrežje ameriške vojske ARPANET, preko katerega se je širil virus z imenom Creeper. Pridobil je nadzor nad računalnikom in se sam kopiral naprej na naslednje računalnike.

Naslednji znani virus se je imenoval Rabbit. Njegova naloga je bilo zgolj množenje samega sebe, kar je omejilo sposobnosti okuženega računalnika. V osemdesetih letih dvajsetega stoletja so se pojavili prvi trojanski konji (v primerjavi z virusi se ti niso sami množili, temveč jih je uporabnik sam naložil na računalnik).

Leta 1986 se je pojavil virus po imenu Brian. Zapisal se je v zagonski sektor in se hitro širil. Gre za prvi virus za IBM združljive računalnike. Potem pa so se pojavili virusi, ki so direktno napadali podatke na disku (IBM je takrat že razvijal protivirusne programe za splošno uporabo). Znan primer je virus z imenom Datacrime, ki je na disku okuženega računalnika sprožil nizko nivojsko formatiranje in s tem uničil vse podatke. Po letu 1990 je število virusov iz dneva v dan naraščalo, pojavili pa so se tudi virusi, ki so napadali protivirusne programe in jih onemogočali.

Najbolj zloglasen virus prejšnjega stoletja pa je zagotovo virus Michelangelo, ki je z diska izbrisal vse podatke. O njem so leta 1992 pisali vsi svetovni mediji. Michelangelo je povzročil, da so uporabniki po vsem svetu množično kupovali protivirusne programe. Michelangelo naj bi samo v ZDA okužil 25 % vseh računalnikov.

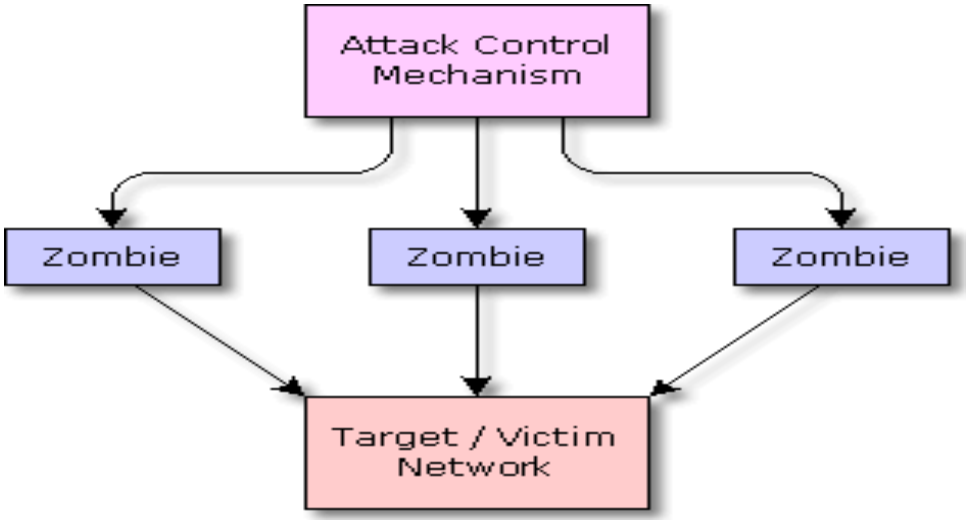
Po letu 1995 so se začeli pojavljati virusi za operacijski sistem Windows. Prvi znan primer je bil virus z imenom Win.Tentacle, ki se je sam širil preko omrežja. Napadal je datoteke s končnico

exe. Prvi virus za operacijski sistem Linux se je pojavil leta 1997, širil pa se je preko FTP protokola.

Črvi in virusi pa so se sčasoma vedno bolj širili tudi preko elektronske pošte. Priložena datoteka je vsebovala virus, ki je ob zagonu uničil datoteke najbolj priljubljenih programov (Microsoft Word, Microsoft Excel…). Po letu 2001 so se virusi širili in kopirali na računalnike tudi direktno preko spletnih strani. Zaradi varnostne luknje v najbolj priljubljenem spletnem brskalniku Microsoft Explorer je bil za zagon določenega virusa dovolj je obisk okužene spletne strani.

Eden izmed najbolj poznanih načinov škodovanja z zlonamerno kodo zadnjih let pa je proces, ki se imenuje Dos (Denial of Service). Poteka tako, da vdiralec pošlje tarči (strežnik, spletna aplikacija, portal ipd.) veliko količino podatkov preko določenih vrat. Iz Dosa se je pozneje razvil Ddos (Distributed Denial of Service), kjer pa za razliko od Dos-a vdiralec uporablja več podračunalnikov (zombiji), ki sledijo njegovim ukazom. To povzroči, da tarča pri napadu prejme veliko več podatkov kot pri napadu preko Dos-a.

Slika 2: Skica Ddos napada na tarčo



Vir: Gibson, 2002, str 7.

2.3.1.1 Virusi

Virus je računalniška koda, ki se pripne na program ali datoteko, tako da se lahko razširi iz enega računalnika v druge in jih tako okuži. Virusi lahko poškodujejo programsko opremo, strojno opremo in datoteke (Predstavitev virusov, črvov in trojanskih konjev, 2004).

Večina virusov se prenaša preko interneta. Gre za računalniški program, ki se sam razširja preko drugih računalniških programov ali dokumentov.

Čeprav je lahko določen virus tudi poguben za kak računalnik, pa so dandanes virusi predvsem zgolj nadležni in ne spreminjajo ali brišejo podatkov na disku. V večini primerov se le reproducirajo in čakajo, da bodo prek interneta lahko napadli nov računalnik. Take vrste virusi predvsem obremenijo računalniški procesor, pomnilnik ali količino prostega trdega diska. Za zaščito pred virusi se uporabljajo protivirusni programi in požarni zidovi, pomembno pa je tudi, da uporabnik pravočasno nalaga popravke programov na svoj računalnik.

2.3.1.2 Vohuni

Gre za program, ki spremlja in zapisuje aktivnost okuženega računalnika, potem pa te, na skrivaj pridobljene podatke, pošlje preko interneta lastniku programa. V večini primerov vohuni niso škodljivi, na računalnik pa se naložijo predvsem zaradi oglaševalskih namenov (What is spyware, 2006).

Vohunski programi lahko računalnik okužijo na več načinov. Eden izmed dveh najpogostejših načinov je vgrajevanje vohunskega programa podjetij v lastno programsko opremo, drugi pa je izkoriščanje varnostnih lukenj v priljubljenih spletnih brskalnikih.

Ko se vohunski program naloži na računalnik, si dodeli edinstveno šifro, preko katere lastniku vohunskega programa potem pošilja podatke o aktivnosti in načinu uporabe okuženega računalnika. Tako lahko lastnik vohunskega programa vzdržuje bazo podatkov aktivnosti uporabnikov, katerih računalnike je okužil njihov vohunski program. Ko nek uporabnik preko interneta išče ali prebira določeno besedo ali besedno zvezo, se mu na ta način odpre pojavno okno, ki oglašuje kak izdelek ali storitev, ki je povezana s to besedo ali besedno zvezo.

Posebna oblika vohunskih programov so spletni piškotki, ki se naložijo v spomin spletnega brskalnika in so namenjeni pridobivanju podatkov o uporabnikovih navadah na določeni spletni strani.

Obstajajo tudi omrežni vohuni; le-ti lahko zapisujejo in shranjujejo pogovore, ki potekajo preko elektronske pošte ali programov, namenjenih komuniciranju prek spleta (Skype, MSN messenger,…). Take vohunske programe so predvsem v preteklosti uporabljale tajne službe, saj

so ravno s prisluškovanjem komunikaciji, ki je nekodirana, pridobile veliko pomembnih informacij.

2.3.1.3 Črvi

Črv je prav tako kot virus zasnovan z namenom, da bi se širil v druge računalnike, vendar to naredi samodejno, tako da prevzame nadzor nad računalniškimi funkcijami za prenos datotek in podatkov. Ko se črv naseli v vašem sistemu, lahko potuje sam. Nevaren je prav zaradi izjemne sposobnosti hitrega širjenja: svoje kopije lahko na primer pošlje na vse naslove, ki jih imate v imeniku, računalniki naslovnikov pa bi naredili isto, kar povzroči učinek domin. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, zato morate včasih do dvakrat dlje čakati za ogled posameznih spletnih strani (Predstavitev virusov, črvov in trojanskih konjev, 2004).

V zadnjem času je veliko črvov napisanih ravno na podlagi popravkov za operacijski sistem Windows, kar pomeni, da avtorji črvov pregledajo, katere napake je novi popravek odpravil in jih izkoristijo. V času, preden uporabniki na svoj računalnik naložijo Microsoftov popravek, lahko črv že povzroči veliko škode.

2.3.1.4 Trojanski konji

Trojanski konj je program, ki je na prvi pogled popolnoma neškodljiv, vendar pa vsebuje zlonamerno kodo. Škodo začne povzročati v trenutku, ko ga zaženemo. Trojanski konji se ne reproducirajo sami. Med najbolj znane trojanske konje spadajo BackOrifice (ta po namestitvi sprejema zveze na poljubnem portu, lastnik BackOrifica pa lahko prek IP številke izvaja poljubne ukaze na gostiteljevem računalniku), Netbus (zagotovi lastniku dostop do gostiteljevega računalnika, omogoča pa mu zbiranje podatkov, spreminjanje gesel, nadzor na elektronsko pošto, prisluškovanje tipkovnici, presnemavanje datotek, spreminjanje registra …), Subseven, Beast Trojan in Downloader EV (Predstavitev virusov, črvov in trojanskih konjev, 2004).

2.3.1.5 Stranska vrata

Gre za dostop do računalniškega programa, spletnih storitev ali pa do celotnega informacijskega sistema mimo varnostnih mehanizmov programa. Stranska vrata v večini primerov napiše programer, ki naredi programsko kodo za program. Veliko je škodljivih programov, ki lahko odprejo stranska vrata kakega programa ali informacijskega sistema. V večini primerov se na računalnik prenesejo preko elektronskih pošte ali zastonjskih programov, ki se prenašajo preko spletnih strani (lahko tudi brez vednosti uporabnika).

2.3.1.6 Mobilna zlonamerna koda

Mobilna zlonamerna koda je pojem, ki zajema več vrst zlonamernih programov, kot so virusi, črvi in trojanski konji. Mobilna zlonamerna koda se največkrat pojavi med brskalnikovimi ukaznimi datotekami, kontrolniki ActiveX in programčki v Javi (Frelih, 2004, str. 6).

2.4 Celovita obramba pred vdori

2.4.1 Varnostne tehnologije sistemske programske opreme

Varnostne tehnologije sistemske programske opreme temeljijo na uporabi seznama za kontrolo dostopa - ACL (angl. Access Control List). Seznam je vezan na določen objekt in določa, katere operacije se lahko na nekem objektu izvajajo in kdo lahko seznam spreminja. Sistem ima lahko vgrajeno kontrolo neomejenega dostopa, kar pomeni, da ima avtor nekega objekta popolne pravice za njegovo manipulacijo, lahko pa ima sistem vgrajeno tudi kontrolo pooblaščenega dostopa, kar pomeni, da so pravice na objektu omejene. Naslednja varnostna tehnologija, ki jo podjetja vse bolj uporabljajo se imenuje RBAC (angl. Role Based Access Control)- kontrola dostopa na podlagi funkcionalnosti, ki se od ACL tehnologije razlikuje v tem, da RBAC dodeli dovoljenje nekemu uporabniku glede na njegovo vlogo v organizaciji. ACL dovoli ali prepreči dostop do nekega objekta, RBAC pa tudi točno določi, katere operacije se na nekem objektu lahko izvajajo.

Informacijski sistemi uporabljajo tudi varnostne mehanizme, ki temeljijo na metodah tajnopisja. Tajnopisje poteka preko algoritmov za pretvorbo osnovnega besedila v tako obliko, da je originalna vsebina nedostopna brez poznavanja informacije, ki ji pravimo ključ. Osnovnemu besedilu pravimo čistopis, pretvorjenemu besedilu pa skriptopis ali tudi tajnopis (Trček, 2001, str. 83).

Tajnopisne algoritme delimo v grobem na dva dela (Trček, 2001, str. 85):

- Simetrični algoritmi: za pretvorbo čistopisa v tajnopis se uporablja isti ključ kot za pretvorbo tajnopisa v čistopis. Ti algoritmi ne potrebujejo toliko procesorske moči, vendar pa niso primerni za sisteme, ki ji uporablja veliko uporabnikov naenkrat.
- Asimetrični algoritmi: za pretvorbo čistopisa v tajnopis se uporablja drugačen ključ kot za pretvorbo tajnopisa v čistopis. Ključa sta komplementarna. Asimetrični algoritmi tudi omogočajo izvedbo digitalnega podpisa (deluje na podlagi skritega in javnega ključa).

Informacijski sistemi so sami po sebi zaščiteni tudi z uporabniškim imenom in geslom. Tako lahko skrbnik informacijskega sistema različnim uporabniškim imenom dodeljuje različne nivoje pravic. S tem postane uporabnik znotraj informacijskega sistema omejen.

2.4.2 Protivirusni programi

Vdiralska orodja, kot so virusi in trojanski konji, napadajo informacijski sistem na značilen način. V večini primerov gre za spremembe določenih datotek, vnose v register ali zaganjanje določenih procesov v okuženem računalniku. Vse te značilnosti so protivirusnimi programom dobro poznane, kar pomeni, da vdiralsko orodje najprej prepoznajo, potem pa onemogočijo njegovo delovanje. Zaradi vsakodnevnega nastajanja novih virusov, je treba zbirko vdiralskih orodij in njihovih značilnosti[1] nenehno posodabljati.

Sodobni protivirusni programi imajo vgrajene možnosti za sprotno internetno posodabljanje protivirusnih definicij, kar občutno zmanjša možnost okužbe sistema (Bratuša, Verdonik, 2005, str. 203).

Sodobni protivirusni programi preverjajo poleg skeniranja sistema, vsakodnevne posodobitve protivirusne definicije in preverjanja e-poštnega protokola SMTP tudi protokola HTTP in FTP, ki ju uporabljajo internetni brskalniki pri dostopanju do spleta. Protivirusni program v prehodu skenira več protokolov ali storitev hkrati, saj lahko vdiralci uporabijo različne načine za prenos zlonamerne programske opreme (Egan, Mather, 2005, str. 159).

[1] Takšni zbirki pravimo protivirusna definicija. Uporaba protivirusne definicije predstavlja hevristični način za zaščito sistema pred zlonamerno kodo.

2.4.3 Zaščita pred vohunskimi programi

Večina vohunskim programov se naloži v okuženi računalnik preko spletnih strani. Najbolj pogosta zaščita pred takimi programi je zato požarni zid, saj nadzira ves promet, ki pride v računalnik. Računalnik je mogoče pred vohunskimi programi zaščititi tudi kar neposredno v spletnem brskalniku, saj večina sodobnih spletnih brskalnikov omogoča nastavitev varnostnih parametrov; to pomeni, da omrežni promet prepreči že spletni brskalnik (Bratuša, Verdonik, 2005, str. 239).

Najbolj učinkovita metoda zaščite pred vohunskimi programi so posebna orodja, ki delujejo podobno kot protivirusni programi. Ravno tako skenirajo datoteke in potem na podlagi zbirke definicij vohunskih programov ugotovijo, ali je računalnik okužen ali ne. Tabela 1 prikazuje tri najbolj razširjena orodja za zaščito pred vohunskimi programi.

Tabela 1: Tri najbolj razširjena orodja za zaščito pred vohunskimi programi

Orodje	Lastnosti
Spybot Search & Destroy	Uporabniku prijazen, avtomatsko posodabljanje, uporaba real-time zaščita, skeniranje diska.
Ad-aware SE Personal	Uporabniku prijazen, dnevno posodabljanje, uporaba real-time zaščite, post-scan tehnologija, skeniranje diska.
Windows Defender	Uporabniku prijazen, avtomatsko posodabljanje, uporaba real-time zaščite, preprečuje spremembe registra.

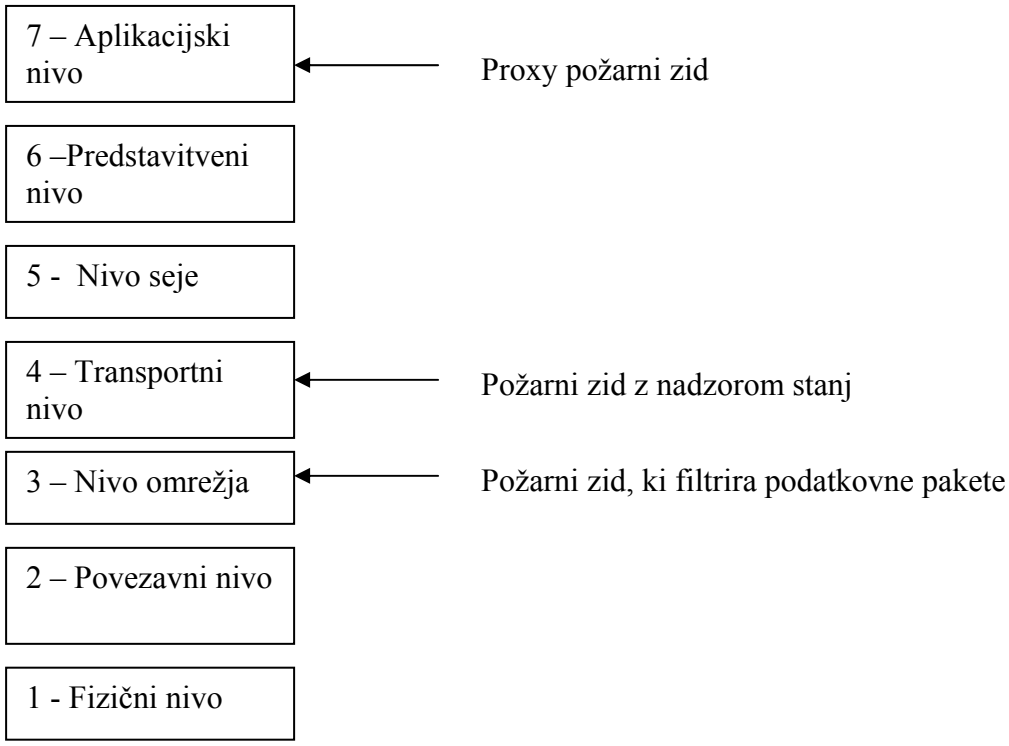
Vir: Bratuša, Verdonik, 2005, str. 241.

2.4.4 Požarni zid

Požarni zid je v današnjem času najbolj razširjeno varnostno orodje. V grobem ga lahko delimo na zunanji in notranji požarni zid. Zunanji je nameščen v prehod za zaščito DMZ (demilitarized zone). Gre za vmesno omrežje med lokalnim omrežjem (LAN) in zunanjim omrežjem. Njegova prednost je predvsem v hitrosti, saj strojne rešitve svoje delo opravljajo precej hitreje kot programske in tako omogočajo večjo prepustnost. Notranji požarni zid je programska oprema, ki deluje na podlagi seznama dovoljenj, na katerem je označeno, katerim storitvam in protokolom naj požarni zid omogoči dostop do računalnika.

Danes je na voljo več vrst požarnih zidov, ki jih najlažje opišemo z referenčnim modelom povezanih odprtih sistemov - OSI (angl. Open System Interconnection). Referenčni model OSI je svetovni standard, ki komunikacijske protokole obdeluje na sedmih ravneh. V modelu se podatki prenašajo z ene ravni na drugo. Začnejo na ravni aplikacij in nadaljujejo proti spodnji ravni, preden se po hierarhiji spet vrnejo do svojega začetka. Različne vrste požarnih zidov delujejo na različnih ravneh, ki omogočajo različne stopnje zaščite. Na sliki 3 je grafični prikaz modela OSI in kategorij požarnih zidov (Egan, Mather, 2005, str. 157).

Slika 3: Model OSI in požarni zidovi



Vir: Egan, Mather, 2005, str. 157.

Čim višje se pomikamo po modelu OSI, tem bolj neprepustni in strožji je požarni zid, zaradi tega pa se tudi upočasni njegovo delovanje. Najbolj učinkovit je posredovalni strežnik, ki poleg preverjanja glave poslanih paketov prebere in ponovno zapiše tudi vsebino paketov. Žal pa so posredovalni strežniki počasni, saj imajo veliko dela pri pregledovanju pretokov. Hitrejši so požarni zidovi, ki filtrirajo pakete in nadzorujejo stanja, primerni pa so predvsem za spletna mesta z veliko prometa in manj občutljivejšimi podatki.

Za požarne zidove, ki filtrirajo podatkovne pakete, je značilno, da delujejo na tretjem sloju (to je na omrežni ravni, znani pa so tudi kot port-based požarni zidovi). Vsak paket se primerja s

seznamom pravil (izvorni/ponorni IP, izvorna/ponorna vrata, protokol...). Taki požarni zidovi so poceni in hitri, vendar pa nekoliko manj varni, temeljijo na petindvajset let stari tehnologiji in motijo bolj zapletene aplikacije.

Za požarne zidove z nadzorom stanj je značilno, da nadzirajo prehode na ravni tokokroga. Delujejo na četrtem sloju (to je na transportni ravni), prenašajo TCP povezave, ki temeljijo na portih in so poceni, a bolj zanesljivi od požarnih zidov, ki filtrirajo pakete.

Za posredovalne strežnike je značilno, da delujejo na petem nivoju in so aplikacijsko naravnani. So nekoliko dražji in počasnejši od drugih, vendar pa so neprimerno bolj varni. Omogočajo tudi zapisovanje uporabnikove dejavnosti. Zahtevajo konfiguriranje uporabnikov, omrežij in aplikacij.

Obstajajo tudi večslojni požarni zidovi s stanjem, ki filtrirajo tretji sloj, validirajo četrti sloj in preiskujejo peti sloj. So dragi in zapleteni, vendar pa so zelo varni. V zadnjem času so se pojavile tudi nekatere nove vrste požarnih zidov, ki omogočajo dodatno zaščito sistemov in omrežij. To so osebni oziroma strežniški požarni zidovi in omrežni dinamični požarni zidovi. Za osebne ali strežniške požarne zidove je značilno blokiranje gonilnikov protokolov, kar programom prepoveduje nalaganje in uporabo nestandardnih protokolnih gonilnikov. Ti požarni zidovi uporabljajo tudi blokiranje aplikacij, ki dovoljuje izvajanje omrežnih akcij in sprejemanje omrežnih povezav le nekaterim aplikacijam. Blokiranje značilnih vzorcev poskrbi za stalno spremljanje omrežnega prometa in zaustavitev vseh možnih znanih napadov (Bratuša, Verdonik, 2005, str. 233-234).

Proizvajalci požarnih zidov v večini primerov izdajo različico, ki je brezplačna in primerna za domače uporabnike, ponujajo pa tudi komercialno različico, ki ima vgrajene dodatne funkcije in omogoča večjo zaščito. Drugače pa je v podjetjih, kjer požarni zidovi ne varujejo enega samega računalnika, temveč večjo skupino medsebojno povezanih računalnikov (lokalna omrežja). Za podjetja ni na voljo brezplačnih učinkovitih požarnih zidov. Med bolj znanimi požarnimi zidovi za podjetja so Check Point FireWall-1, Symantec Enterprise Firewall, NetWolves Proplus, eTrust Firewall in Cisco IOS Firewall 5000/7000.

2.4.5 Izobraževanje uporabnikov

Pomembno je, da so v izobraževanje o varnosti informacijskega sistema v podjetju vključeni vsi zaposleni. Znanje pridobijo preko izobraževalnih seminarjev, kjer se učijo splošno o varovanju informacij, o vpeljavi in izvajanju standarda BS 7799 ter o pomembnosti varovanja informacij. Uporabnike je treba naučiti ravnanja z gesli ter jim razložiti, kakšne so pri tem njihove

odgovornosti, ravnanja z informacijskim sistemom, ravnanja z elektronsko pošto in ravnanja z omrežjem. Skrbeti morajo, da geslo ostane zaupno, izogibati se morajo zapisovanju gesel, upoštevati pa morajo varnostna priporočila, ki jih predpisuje sistem. Če nastane sum, da je geslo razkrito, je potrebno geslo takoj spremeniti.

Vlada Republike Slovenije v ta namen tudi vsako leto izdela priporočila za pripravo informacijske varnostne politike, v katerem je natančno opisano, na kakšen način naj podjetja izobrazijo svoje uporabnike ter kateremu segmentu varnostne politike naj namenijo posebno pozornost.

3 STANDARD BS 7799

3.1 Razvoj standarda BS 7799

Zametki standarda segajo v leto 1987, ko je bil v Veliki Britaniji ustanovljen komercialni računalniški varnostni center – CCSC (angl. Commercial Computer Security Centre). Njegov namen je bil vzpostaviti mednarodno priznane kriterije za vrednotenje varnosti. Tako se je rodil ITSEC (angl. Information technology security evaluation criteria), ki je bil leta 1990 v večini evropskih držav tudi splošno sprejet kot nabor kriterijev za vrednotenje računalniške varnosti. CCSC se je ukvarjal tudi z razvojem kodeksa varovanja informacij, ki je prvič izšel leta 1989, potem pa se je nadalje razvijal, dokler ni leta 1995 izšel kot kodeks upravljanja varovanja informacij, ki ga je izdal British Standard Institution (BSI). Prvi del standarda je leta 2000 postal BS ISO/IEC 17799-1:2000, drugi del pa je leta 2002 postal BS 7799-2:2002. V Sloveniji se uporabljata dva standarda, in sicer SIST BS 7799-2:2003 (sistemi za upravljanje varovanja informacij ter specifikacija z napotki za uporabo) in SIST ISO/IEC 17799:2003 (kodeks upravljanja varovanja informacij).

3.2 Povezava z drugimi standardi

Za uporabo standarda BS 7799 so nujni naslednji referenčni dokumenti. Pri datiranih referencah velja samo navedena izdaja, pri nedatiranih pa velja zadnja izdaja tega dokumenta.

Referenčni dokumenti (BS 7799-2, 2002, str. 10):

- BS EN ISO 900:2000, Sistemi za upravljanje kakovosti – Zahteve.
- BS ISO/IEC 17799:2000, Informacijska tehnologija – Kodeks varovanja informacij.
- ISO Guide 73:2002, Upravljanje tveganja – Smernice za uporabo v standardih.

3.3 Splošno o standardu BS 7799

Pri vpeljavi standarda BS 7799 je glavni namen podjetja zagotoviti ustrezen nivo varovanja programske in strojne opreme ter informacij in informacijskih sistemov. Potrebno je proučiti vse potrebne procese za preprečevanje varnostnih nesreč in zagotoviti učinkovit ter s standardom BS 7799 skladen sistem vodenja varovanja informacij.

Standard BS 7799 podjetju zagotavlja vpeljavo učinkovitega sistema za upravljanje informacijske varnosti, saj zagotavlja:

- neoporečnost: varovanje natančnosti in popolnosti informacij med shranjevanjem in prenašanjem ter varovanje računalniške programske opreme;
- zaupnost: zagotavljanje, da so informacije dostopne samo pooblaščenim osebam; zaupnost pomeni zaščito informacij v kakršnikoli obliki pred vsakršnim nepooblaščenim vpogledom med njenim shranjevanjem, obdelavo ali prenašanjem;
- razpoložljivost: zagotavljanje, da so računalniške storitve in informacije 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, 2002, str. 18-19).

Standard se deli na 10 poglavij (Konečnik, 2002, str. 22-23):

1. Varnostna politika.
   Podjetje izda krovni dokument, v katerem je zajeta vsa varnostna politika podjetja. Gre za večnivojski dokument.
2. Organiziranost varovanja.
   Podjetje definira varnostni forum, ki skrbi za smernice varnostne politike.
3. Razvrstitev in nadzor sredstev.
   Sprva gre za popis vseh sredstev in fizičnega premoženja podjetja, na podlagi katerega se potem izvaja nadzor nad opremo. Določi se tudi odgovornost za posamezne elemente informacijskega sistema.
4. Varovanje v zvezi z osebjem.
   V tem poglavju je razdelana varnostna politika podjetja v povezavi z uporabniki njihovega informacijskega sistema. Gre predvsem za izobraževanje uporabnikov, omejevanje dostopa in pravic ter dodeljevanje in upravljanje z uporabniškimi gesli.
5. Fizična zaščita in varovanje okolja.
   To je zagotavljanje fizične zaščite informacijskih sistemov in njegovih elementov.
6. Upravljanja s komunikacijami in s produkcijo.

To poglavje govori o varnosti omrežij in računalnikov, njihovi pravilni uporabi ter o postopkih upravljanja. Obravnava tudi zaščito informacijskega sistema pred zlonamerno programsko kodo.

7. Nadzor dostopa.
   Govori o tem, kdo in na kakšen način se izvaja nadzor nad dostopom do informacijskega sistema. Gre za varnostno politiko gesel ter pripadajočih pravic, ki jih uporabnik ima.
8. Razvoj in vzdrževanje sistemov.
   Gre za natančno analizo varnostnih zahtev informacijskega sistema ter njegovo nadaljnjo nadgradnjo.
9. Upravljanje neprekinjenega poslovanja.
   To poglavje poudarja neprekinjeno poslovanje, njegovo načrtovanje, testiranje in obnavljanje. Razloži tudi ukrepe za primer izpada informacijskega sistema.
10. Združljivost.
    Obravnava, kako je informacijski sistem združljiv z aktualno zakonodajo, tako na pravnem in varnostnem področju.

3.4 Vpeljava standarda BS 7799

Podjetje se na podlagi poslovnih ciljev samo odloči, ali bo standard vpeljalo ali ne. Če se odloči, da bo standard vpeljalo, mora natančno definirati aktivnosti, ki so za vpeljavo standarda potrebne. V splošnem lahko govorimo o desetih aktivnostih (Golec, 2005, str. 3):

1. priprava plana projekta ter predstavitev vodstvu;
2. uvajalne aktivnosti – odprtje mape projekta, imenovanje vodje projekta in članov projektne skupine;
3. ocena obstoječega stanja, priprava analize tveganj in priprava analize vrzeli;
4. opredelitev politike varovanja;
5. priprava poslovnika varovanja in ostalih dokumentov v sistemu varovanja;
6. izobraževanje in usposabljanje sodelavcev (vključno s preizkušenim revizorjem informacijskih sistemov);
7. notranje presoje, varnostni pregledi (testiranje načrta okrevanja);
8. začetni pregled in certifikacijska presoja;
9. vzpostavljanje sistema varovanja – implementacija ukrepov;
10. trženje svetovalnih in implementacijskih storitev.

4 SISTEM ZA UPRAVLJANJE VAROVANJA INFORMACIJ (SUVI)

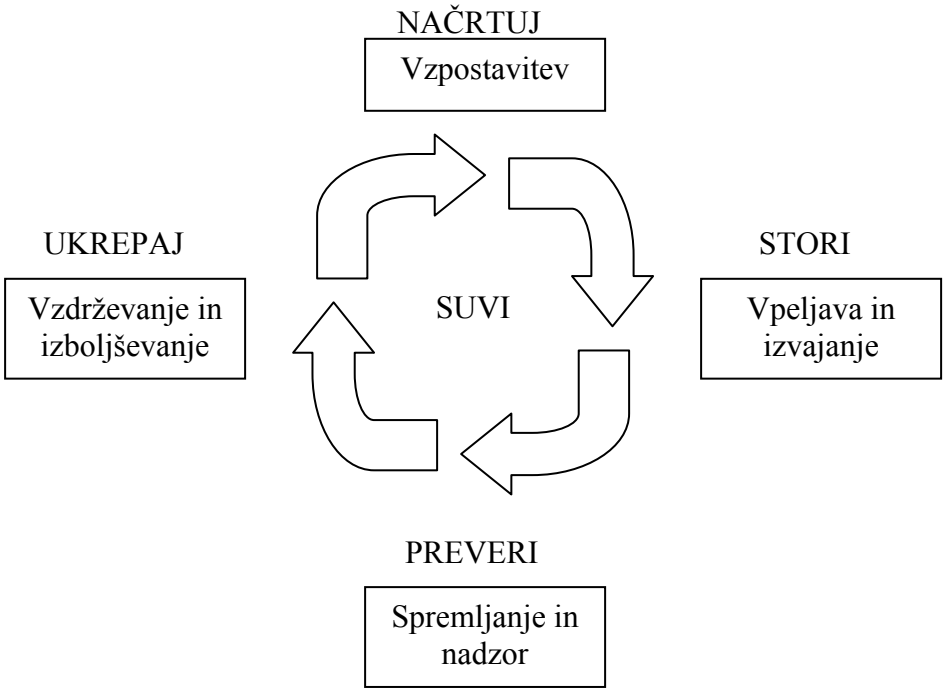
Sistem za upravljanje varovanja informacij (SUVI) v podjetju zahteva vzdrževanje in nenehno izboljševanje informacijske varnosti. Je ključni element standarda BS 7799. Osnovan je na ciljih

podjetja, na izbiri ustrezne strategije, na načinu in obsegu poslovanja, organizacijski kulturi, klimi in znanju. SUVI za podjetja predstavlja pomembne poslovno priložnosti (Berčič, 2003, str. 126):

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

Za vzpostavitev in upravljanje SUVI uporablja procesni pristop načrtuj – stori - preveri – ukrepaj (NSPU), tako kot je prikazano na Sliki 4.

Slika 4: Model NSPU za SUVI



Vir: BS 7799-2, 2002, str. 8.

4.1 Faze sistema za upravljanje varovanja informacij

4.1.1 Načrtuj

Faza načrtuj mora biti zasnovana tako, da zagotavlja pravilno določitev namena in okoliščin SUVI, Pomembno je, da so ocene varnostnih tveganj, ki ogrožajo informacije in pripravo načrta

za primerno obravnavo teh tveganj, čim bolj pravilne. Podjetje mora tudi vse stopnje faze načrtuj dokumentirati, saj so ti dokumenti pozneje podlaga za upravljanje z morebitnimi spremembami.

4.1.1.1 Politika varovanja informacij

Pri politiki varovanja informacij gre za skupino dokumentov, v katerih so opisani postopki v procesu varovanja informacij, in varnostna pravila, ki so odvisna od poslovnih ciljev podjetja. Ti postopki in pravila so obvezujoči za vse zaposlene v podjetju. Pomembno je, da ti dokumenti zagotavljajo zaupnost, neoporečnost in razpoložljivost informacij, saj je to ključno za doseganje konkurenčne prednosti in dobrega imena podjetja. Čim boljša je varnostna politika podjetja, tem manj je podjetje dovzetno za napade iz okolja, poslovna škoda v primeru takega napada pa je tako reducirana na najmanjšo možno mero.

Z varnostno politiko podjetje pridobi (Varnostna politika, 2007):

- preverjanje trenutnega stanja varnosti informacijskih sistemov,
- definiranje postopkov za komunikacijo z zunanjimi partnerji,
- dokaz o ustreznosti zaščite informacij,
- skladnost z zakonodajo,
- pogoj za pridobitev certifikata po standardu ISO/IEC 27001:2005.

Varnostno politiko lahko razdelimo na več nivojev:

- krovna varnostna politika,
- politike za posamezna področja,
- delovna navodila, postopki in obrazci na najnižjem nivoju.

Z razdelitvijo varnostne politike na več nivojev dosežemo boljšo preglednost dokumentacije ter zagotovimo enostaven prehod od strateških ciljev prek mehanizmov do konkretnih postopkov, ki se bodo uporabili za dosego zastavljenih ciljev (Rakovec, 2005, str. 6-7).

4.1.1.1.1 Krovna varnostna politika

Predstavlja temeljni dokument za varovanje informacij v podjetju. Cilj te politike je pridobivanje podpore in priprava organizacije na oblikovanje celovitega sistema varovanja. Krovna varnostna politika vsebuje (Rakovec, 2005a, str. 33):

- namen in cilj 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.

Varnostno politiko potrdi vodstvo.

4.1.1.1.2 Varnostne politike za posamezna področja

Gre za opis posameznih področij, vendar pa ti dokumenti še ne govorijo o posameznih ljudeh ali računalniški opremi. Najbolj ključna področja so varovanje osebja in elektronske pošte, zaščita pred zlonamerno programsko kodo, politika dodeljevanja in nadzora dostopov…

4.1.1.1.3 Delovna navodila, postopki in obrazci na najnižjem nivoju

To so dokumenti, ki vsebujejo operativna navodila, interne standarde ter postopke za delo. Tu so zajeta pravila dostopov do strežnikov, prevzema in oddajanja opreme, navodila za shranjevanje dokumentov…

4.1.1.2 Določitev velikosti SUVI

Sistem za upravljanje varovanja informacij lahko vgradimo v celotno podjetje, lahko pa ga vpeljemo le v posamezni oddelek podjetja. Odločitev o tem je odvisna predvsem od postopkov, ki jih podjetje namerava varovati, ter seveda od velikosti samega podjetja.

4.1.1.3 Določitev ekipe za upravljanje SUVI

Podjetje mora v fazi načrtovanja SUVI določiti tudi ljudi, ki bodo skrbeli za uspešno uvedbo, pozneje pa tudi izvajanje SUVI. Potrebno je določiti njihove naloge in aktivnosti ter jim dodeliti pooblastila in naloge. Ekipa mora biti vedno v stiku s časom, to pomeni, da mora sodelovati z zunanjimi strokovnjaki.

Standard BS 7799 določa, da se ustanovi tudi poseben varnostni forum, ki skrbi za odobritve posameznih dokumentov in nadzira vpeljavo le-teh v celotno podjetje.

4.1.1.4 Analiza odstopanja

V analizi odstopanj podjetje ugotovi, ali je v posameznih določilih skladno s standardom BS 7799 ali ne. Analiza odstopanja podjetju pomaga tudi pri ocenjevanju, kakšni bodo končni stroški vpeljave in uvedbe SUVI.

4.1.1.5 Ocena tveganja

Pri oceni tveganja izhaja podjetje iz naslednjih osnovnih vprašanj (Shrestha, 2004, str. 10):

- Kaj gre lahko narobe?
- Kako se to lahko zgodi?
- Zakaj se to zgodi?
- Kakšne so možne posledice te napake?

Podjetje mora najprej popisati vsa svoja sredstva (fizična sredstva, programska, strojna oprema, podatki, ljudje), nato pa jih mora glede na pomen za podjetje tudi ovrednotiti. Podjetje mora pripraviti tudi spisek ranljivosti in spisek groženj, ki ju potem poveže s popisanimi sredstvi in predvidi možna tveganja.

Podjetje mora imeti tudi načrt, kako bo s temi tveganji upravljalo, predvsem pa, kako bo tveganja z visoko stopnjo preusmerilo na tveganja z nizko stopnjo.

4.1.1.6 Izjava o uporabnosti

Gre za dokument, v katerem so opisani kontrolni cilji in kontrole, primerne in uporabne v SUVI organizacije, izbrane na temelju rezultatov in zaključkov procesov cene in obravnave tveganja (BS 7799-2, 2002, str. 14).

4.1.2 Stori

V tej fazi gre za vpeljavo izbranih kontrol ter izvedbo načrtovanih aktivnosti, ki so bile sprejete v prvi fazi.

4.1.2.1 Upravljanje s tveganji

S tveganji, ki jih je organizacija izračunala, se mora tudi ukvarjati; predvsem gre za to, da organizacija ta tveganja (Janežič, 2004):

- sprejme,
- zmanjša,
- prenese,
- se jim izogne.

Ko organizacija ugotovi, da je tveganje previsoko, mora imeti učinkovit sistem metod in ukrepov za zmanjševanje tveganja, lahko pa to tveganje tudi prenese na neko tretjo osebo. Za prenos tveganja se podjetje odloči, če ugotovi, da bi bilo zmanjševanje tveganja znotraj podjetja prezahtevno ali predrago.

Dejstvo je, da informacijski sistem ne more nikoli biti popolnoma zavarovan. To pomeni, da se podjetje nikoli ne more popolnoma izogniti tveganju. Izjema je možna le, če podjetje določeno sredstvo umakne iz območja tveganja oziroma se mu popolnoma odpove.

4.1.2.2 Upravljanje z viri in sredstvi podjetja

Za dobro delovanje SUVI so potrebni tako viri kot tudi sredstva, kot so ljudje, denar in čas. Organizacija mora priskrbeti vire, ki bodo odgovorni za načrtovanje, vpeljavo, delovanje in vzdrževanje SUVI (Rakovec, 2005b, str. 25).

4.1.2.3 Izobraževanje in usposabljanje

Izobraževanje in usposabljanje vseh v podjetju za varovanje informacij je zelo pomembno, je pa tudi prvi pogoj za uspešno izvedbo SUVI. Pomembno je, da v sklopu izobraževanja sodelujejo vsi zaposleni v podjetju in tudi poslovni partnerji podjetja. Seveda se izobraževanja razlikujejo glede na to, komu so namenjena. Lahko gre za usposabljanje vodstva, delavcev ali pa tudi ključnih uporabnikov informacijskih sredstev. Ker se stvari, povezane z informacijsko varnostjo nenehno spreminjajo, je tudi ključnega pomena, da se izobraževanja redno ponavljajo in dopolnjujejo. V praksi taka izobraževanja potekajo v obliki seminarjev ali delavnic, vsakodnevno pa zaposleni tudi preko pošte, interneta, televizije in drugih sredstev javnega obveščanja, pridobivanja pomembna nova znanja o varnosti informacijskih sredstev.

4.1.2.4 Varnostni incidenti

Pomembno, je da organizacija čim hitreje odkrije varnostne incidente in kar najbolj zmanjša škodo in okvare, ki so zaradi incidenta nastale, ter da te incidente spremlja in se iz njih uči. Podjetje mora tudi določiti odgovornosti in postopke za ravnanje ob incidentih, in sicer tako, da

zagotovi hiter, učinkovit in urejen odziv na incidente, in da zbira podatke, ki so povezani z incidentom, kot so npr. revizijske sledi in dnevniki.

BS 7799 določa kontrole, ki skrbijo za čim bolj učinkovito soočanje z varnostnimi incidenti (BS 7799-2, 2002, str. 38):

- Prijava incidentov pri varovanju informacij: varnostne incidente je treba čimprej prijaviti po ustreznih postopkih.
- Prijava pomanjkljivosti pri varovanju informacij: od uporabnikov informacijskih storitev se zahteva, da čimprej opazijo in prijavijo vsako pomanjkljivost pri varovanju ali vsak sum pojava pomanjkljivosti pri varovanju, kot tudi vsako grožnjo, ki ogroža sisteme ali storitve.
- Prijava nepravilnega delovanja programske opreme: določiti je treba postopke za prijavo okvar v delovanju programske opreme.
- Česa se lahko naučimo iz incidentov: potrebno je namestiti mehanizme, ki omogočajo merjenje in spremljanje vrst, obsegov in stroškov incidentov in okvar.
- Disciplinski postopki: kršitve varnostnih politik in postopkov organizacije, ki jih zagrešijo uslužbenci, se bodo obravnavale po uradnih disciplinskih postopkih.

4.1.3 Preveri

V tej fazi podjetje zagotovi uspešno delovanje kontrol SUVI, lahko pa na podlagi analize SUVI tudi preoblikuje, vendar le tedaj, če so nastale spremembe v predpostavkah ali obsegu ocene tveganj. Vsi podatki, ki so zbrani v okviru faze preveri, se porabijo za merjenje uspešnosti SUVI pri doseganju poslovnih ciljev podjetja.

4.1.3.1 Rutinsko preverjanje

Podjetje mora redno izvajati rutinska preverjanja za odkrivanje napak v rezultatih obdelave. Takšna preverjanja so npr. inventura, reševanje pritožb strank in preverjanje podatkov, prikazanih na spletni strani podjetja.

4.1.3.2 Samoupravljalni postopki

Gre za kontrolo, ki je zasnovana tako, da lahko takoj zazna kakršnokoli napako ali okvaro, ki nastane med izvajanjem. Primer tega je naprava, ki spremlja omrežje (npr. napake ali okvare opreme) in sproži alarm. Alarm o nastali težavi obvesti odgovorne osebe. Njihova naloga je, da odkrijejo vzrok in ga odpravijo. Če se težava v določenem času ne odpravi, se sprožijo dodatni alarmi, ki obvestijo višje vodstvo organizacije, tako se težava stopnjuje (BS 7799-2, 2002, str. 74).

Smotrno za podjetje je, da vse te dogodke, ki so povezani z odkrivanjem napak, zapisuje in tudi analizira, saj te podatke lahko pozneje izkoristi za še bolj učinkovit postopek samoupravljanja.

4.1.3.3 Učenje od drugih

Podjetje se lahko uči doseganja optimalnih učinkov tudi od drugih podjetij, in sicer preko konferenc, strokovnih združenj, sredstev javnega obveščanja in interesnih skupin.

4.1.3.4 Notranja revizija SUVI

Splošen namen podjetja je, da pregleduje, ali so vsi vidiki SUVI skladni z načrti. Revizije morajo potekati čim bolj redno, med njimi pa ne sme biti več kot eno leto premora. Načrtovati je treba ustrezno število revizij, tako da je revizijske naloge moč enakomerno porazdeliti v celotnem izbranem obdobju revizije.
Notranja revizija mora vodstvu zagotoviti, da (BS 7799-2, 2002, str. 74):

- politika varovanja informacij še vedno močno kaže poslovne zahteve
- se uporablja ustrezna metoda za oceno tveganja,
- se uporabljajo dokumentirani postopki (v okviru namena SUVI) in, da dosegajo želene cilje,
- so tehnične kontrole (npr. požarni zid, fizične kontrole dostopa) nameščene, da so pravilno nastavljene in da delujejo v skladu s pričakovanji,
- je pravilno ocenilo preostanke tveganj in da so še vedno sprejemljiva za vodstvo organizacije,
- so izvedeni ukrepi, ki so bili sprejeti na podlagi prejšnjih revizij in pregledov,
- je SUVI v skladu s standardom BS 7799.

4.1.3.5 Vodstveni pregled

Vodstvo podjetja mora nenehno pregledovati potek SUVI in ugotavljati, če je še vedno učinkovit in v skladu s poslovnimi zahtevami. Tudi če ugotovi, da je trenutno stanje SUVI zadovoljivo, mora vseeno biti pozorno, saj se tehnologijo venomer spreminja, v okolju pa se lahko pojavljajo nove grožnje. Vodstvo mora tudi predvideti, kakšne so ranljivosti SUVI in zagotoviti, da bo še naprej učinkovit. V kolikor vodstvo ugotovi, da SUVI ni več učinkovit, se mora odločiti za spremembe. Določiti mora tudi odgovorne nosilce sprememb.

4.1.3.6 Analiza trendov

Na področju varovanja informacij in informatike se hitro pojavljajo spremembe, zato je za podjetje zelo pomembno, da redno analizira trende in s tem pripomore k večjemu prepoznavanju morebitnih nevarnosti in potreb po izboljševanju. Le tako se lahko na te nevarnosti in spremembe temeljito pripravi in ustrezno odzove.

4.1.4 Ukrepaj

V fazi ukrepaj podjetje izhaja iz faze preveri. Gre za sprejetje in implementacijo raznih popravnih ukrepov, o teh spremembah pa je treba obvestiti vse zaposlene.

4.1.4.1 Neskladnost

Tu gre za odstopanje od predvidenega delovanja ene ali več zahtev SUVI. Za področje, kjer je prišlo do neskladnosti, je potrebno ugotoviti, zakaj je do nje prišlo in določiti ukrepe, s katerimi se bo ta neskladnost zmanjšala.

4.1.4.2 Popravni in preventivni ukrepi

Popravni ukrepi so namenjeni odstranjevanju vzroka za neskladnost ali drugih nezaželenih položajev in preprečevanju njihove ponovitve, preventivni ukrepi pa so namenjeni odstranitvi razlogov ali možnih neskladij in drugih nezaželenih položajev.

Posameznih neskladnosti ni nikoli mogoče povsem odstraniti. Po drugi strani pa je lahko dogodek, ki se na prvi pogled zdi osamljen, posledica ranljivosti, ki lahko vpliva na celotno organizacijo, če se ne odkrije. Pri določanju in izvajanju popravnih ukrepov je treba posamezne dogodke obravnavati s tega vidika. Poleg določitve takojšnjih popravnih ukrepov je treba upoštevati tudi srednjedolgi in dolgotrajni vidik popravnih ukrepov, saj tako zagotovimo, da popravna dela ne le odpravijo ugotovljeno napako, temveč tudi preprečijo ali zmanjšajo verjetnost, da se podoben dogodek ponovi (BS 7799-2, 2002, str. 78).
Popravni ukrepi temeljijo na analizi osnovnega vzroka za nastalo neskladnost ter oceni potreb po ukrepih za zmanjšanje verjetnosti za ponovitev neskladnosti. Podjetje mora določiti, kako se bo ukrep izvedel, potem pa mora o tem izvedenem ukrepu pripraviti tudi poročilo o učinkovitosti izvedbe ukrepa. Tudi za preventivni ukrep mora podjetje določiti, na kakšen način se bo izvedel, potem pa mora o tem izvedenem ukrepu pripraviti poročilo o učinkovitosti izvedbe ukrepa.

4.2 Izvajanje SUVI v organizaciji

Pri izvajanju SUVI morajo biti vloge izvajanja jasno opredeljene, predvsem z vidika odgovornosti.

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 v SUVI navadno sodelujejo tudi zunanji svetovalci in akreditirana certifikacijska hiša (Rakovec, 2005b, str. 28).

Vodstvo organizacije skrbi za njen uspešen in učinkovit dolgoročen razvoj, ki temelji tudi na sistemu upravljanja varovanja informacij. Vodstvo mora budno spremljati vpeljavo in razvoj SUVI, določiti, kateri poslovni procesi so kritični v procesu varovanja informacij ter jih obsežno dokumentirati, spremljati skladnost SUVI s poslovnimi in strateškimi cilji podjetja ter skrbeti za dosledno izvajanje SUVI. Pomembno je tudi, da vodstvo varovanju informacij namenu tudi čim večji delež proračuna, saj se mora zavedati, da je področje varovanja informacij eno izmed ključnih dejavnikov pridobivanja konkurenčne prednosti. Vodstvo mora tudi nenehno spremljati dogajanje na področju informacijske varnosti, upoštevati pa mora tudi državno zakonodajo in predpise, direktive, uredbe, standarde in tehnološka orodja.

Vodstvo mora tudi določiti sprejemljiv nivo tveganja, nato pa ga mora tudi učinkovito upravljati, saj lahko na tak način (Kako varovati informacije v javni upravi, 2007):

- zmanjša možnost motenj poslovanja,
- minimizira stroške,
- prepreči škodo na lastnini in opremi,
- izboljša moralo in zadovoljstvo zaposlenih,
- izboljša procese,
- zmanjša število operativnih napak,
- izogne tožbam,
- ohranja dobro ime podjetja.

Vodstvo mora nenehno komunicirati s pooblaščencem za informacijsko varnost, saj je ta v podjetju odgovoren za strokovno svetovanje s področja varovanja informacij, obenem pa je odgovoren za vpeljavo in nadzor SUVI in določanje kontrol SUVI. Skrbi, da je komunikacija o

varovanju informacij med vodstvom podjetja, uporabniki informacijskega sistema, skrbniki informacijskega sistema, načrtovalci aplikacij in vsemi zaposlenimi čim večja.

Odbor za upravljanje varovanja ponavadi sestavljajo člani, ki so vodje posameznih delov organizacije. Njihove naloge v SUVI so (Rakovec, 2005b, str. 30):

- 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.

Krizni tim je v podjetju sestavljen iz članov, ki so strokovnjaki za posamezna področja. Člani tima morajo biti potrjeni s strani vodstva podjetja, ki določi tudi vodjo tima. Seveda mora biti podjetje na krizo že vnaprej pripravljeno. V ta namen mora preventivno izdelati različne možne načine ukrepanja za različne scenarije. Pomembno je, da se krizni tim čim hitreje odzove na krizo, ko se le-ta pojavi, preuči in analizira nastali problem, ter ga čim hitreje odpravi. Ves proces reševanja problema mora biti dokumentiran, saj predstavlja izhodišče za nadaljnje učenje in usposabljanje članov kriznega tima, kako ravnati v takšni situaciji.
Za uspeh SUVI je ključnega pomena, da v njem sodelujejo vsi zaposleni, pogodbeni partnerji in stranke. Podjetje mora zato nenehno izobraževati in obveščati predvsem zaposlene o pomembnosti in novostih na področju informacijske varnosti.

5 PREVERJANJE SKLADNOSTI PODJETJA GORENJSKA BANKA, D. D., S STANDARDOM BS 7799

5.1 Gorenjska banka, d. d.

Predhodnica Gorenjske banke je bila Kmetska posojilnica, šlo pa je za prvo denarno ustanovo na Gorenjskem. Kmetska posojilnica je bila ustanovljena v Podbrezjah leta 1885. Pozneje se Kmetska posojilnica razširila, in sicer so leta 1891 ustanovili posojilnico v Radovljici, leta 1893 mestno hranilnico v Kranju, leta 1900 okrajno hranilnico v Škofji Loki ter leta 1901 hranilnico in posojilnico v Tržiču (Razvojne prelomnice, 2007).

Formalno je Gorenjska banka nastala leta 1955, ko je bila ustanovljena prva komunalna banka v Kranju, nato pa so banke ustanovile tudi v Škofji Loki, Radovljici, Tržiču in na Bledu. Sprva je šlo le za poslovanje z občani, pozneje pa so banke začele opravljati tudi druge posle. Sčasoma so se banke na Gorenjskem trudile povezati v skupno celoto, leta 1972 pa so se kot skupina bank Gorenjske vključile v sistem Ljubljanske banke, sprva kot podružnica, 17. 12. 1989 pa tudi kot sestrska družba Ljubljanske banke in kot delniška družba. Leta 1994 se je tako poslovno kot

organizacijsko ločila od sistema Ljubljanske banke in od 24. 5. 1994 poslovala pod imenom Gorenjska banka, d. d., Kranj. Leta 1994 je tudi od Banke Slovenije pridobila koncesijo za opravljanje kreditno-garancijskih poslov s tujino, postala članica organizacije mednarodnega plačilnega prometa S.W.I.F.T. ter pridobila dovoljenje Banke Slovenije za opravljanje vseh poslov z vrednostnimi papirji. Februarja 2003 je v svoje poslovanje uvedla tudi sistem elektronske banke LINK, ki omogoča poslovanje občanov in podjetnikov na domačem trgu in tudi s tujino.

5.1.1 Poslovna politika in vizija

Poslovna politika Gorenjske banke izhaja iz poslovne strategije banke. V aktivnostih za njeno uresničevanje so upoštevana pričakovana makroekonomska gibanja v domačem in mednarodnem okolju, smernice razvoja bančništva, vse večja konkurenca in evropski trendi zaradi integracijskih procesov, v katere se Slovenija vključuje.

Banka bo v letu 2007 poslovala glede na možnosti povečevanja konkurenčnosti slovenskega gospodarstva in približevanja prevzemu evra. Še naprej bo poslovala kot univerzalna banka. Glavni poudarek bo še naprej v krepitvi varnosti in v izboljševanju kakovosti poslovanja.

Najpomembnejši cilji poslovne politike Gorenjske banke, d. d., Kranj v letu 2007, ki temeljijo na strategiji razvoja banke, so:

- povečevanje obsega poslovanja,
- zagotavljanje konkurenčnosti poslovanja,
- celovito obvladovanje bančnih tveganj,
- racionalizacija poslovanja z ohranjanjem učinkovitosti poslovanja,
- razvoj integralnega informacijskega sistema in izboljšanje tehnološke podpore poslovanja,
- razvoj kadrovske in organizacijske strukture,
- prilagajanje poslovanja zakonodaji in novim predpisom,
- vključevanje v procese reorganizacije bančnega sistema v Sloveniji.

Vizija Gorenjske banke je utrditi ime stabilne, zanesljive in zaupanje vredne finančne institucije, ki bo svojim strankam ponujala najkakovostnejše storitve po konkurenčnih cenah in dolgoročno zagotavljala dobiček delničarjem.

Temeljne vrednote, ki jih bo banka zasledovala pri svojem poslovanju, so (Strategija razvoja, 2007):

- kakovost storitev,

- stabilnost poslovanja,
- poslovna korektnost.

5.1.2. Organizacijska shema

Slika 5: Organizacijska shema Gorenjske banke, d. d., Kranj

Vir: Interno gradivo Gorenjske banke, d. d., Kranj, 2007.

Organizacijska shema Gorenjske banke d. d., Kranj, je sestavljena iz sedmih sektorjev: trženje, zakladništvo, plačilni promet in devizno poslovanje, posli z občani, podpora poslovanju in upravljanje s tveganji, splošni posli in sektor informacijskih sistemov.

5.2 . Analiza skladnosti podjetja Gorenjska banka, d. d., s standardom BS 7799

Analiza skladnosti podjetja Gorenjska banka, d.d., s standardom BS 7799 zajema celotno območje informacijske varnosti, deli pa se na 10 temeljnih področij. Gre za področje varnostne politike, organiziranosti varovanja, razvrstitve in nadzora sredstev, varovanja v zvezi z osebjem, fizične zaščite in varovanje okolja, upravljanja s komunikacijami in produkcijo, nadzora dostopa, razvoja in vzdrževanja sistemov, upravljanja neprekinjenega poslovanja ter področje združljivosti.

Analizo skladnosti sem izvedel s pomočjo zaposlenih v sektorju informacijskih sistemov v Gorenjski banki, d. d., kjer smo od področja do področja pregledali in ocenili stanje na določenem področju.

5.2.1 Varnostna politika

Podjetje Gorenjska banka, d. d., ima izdelano politiko varovanja informacij[2]. Izdelano ima tudi krovno varnostno politiko, ki zajema navodila ter predpise in postopke za delo že na najnižjem nivoju v podjetju; to pomeni, da so odgovornosti za varovanje informacij v podjetju jasno opredeljene. V podjetju seznanjajo svoje zaposlene tudi na seminarjih z vsemi novostmi področja varovanja informacij. Vodstvo podjetja podpira in usmerja varovanje informacij, določilo pa je tudi zaposlenega, ki je odgovoren za izvajanje, vzdrževanje in redno pregledovanje varnostne politike.

5.2.2 Organiziranost varovanja

Gorenjska banka ima posebno ekipo, ki skrbi za varovanje informacij. Člani ekipe se sestajajo enkrat mesečno, na sestanku pa pregledujejo in potrjujejo sprejemanje novih informacijskih varnostnih politik, spremljajo dogajanje na informacijskih sredstvih – in če so potrebne spremembe - le-te tudi predstavijo vodstvu podjetja, vodijo natančno analizi incidentov pri varovanju informacij ter pripravljajo seminarje o varovanju informacij, kjer vse zaposlene tudi seznanijo z novostmi na tem področju. Ekipo vodi pooblaščenec za informacijsko varnost, ki je strokovnjak na svojem področju.

Gorenjska banka sodeluje na področju varovanja informacij tudi z zunanjimi organizacijami, predvsem na področju protivirusne opreme in razvoja specifičnih aplikacij. Največ v Gorenjski banki sodelujejo s podjetjem HERMES Softlab, včlanjeni pa so tudi v Združenje slovenskih bank, enkrat mesečno pa se tudi sestajajo s predstavniki različnih bank, da preko izmenjave informacij še bolj izboljšajo varovanje informacij. V podjetju imajo tudi posebne varnostne ukrepe, ki veljajo tedaj, če podjetje sodeluje z zunanjo organizacijo.

V podjetju izvajajo tudi neodvisen pregled varovanja informacij, in sicer s strani za to pooblaščenih zunanjih organizacij.

V času izvajanja analize skladnosti Gorenjske banke s standardom BS 7799 v podjetju še niso imeli izdelane politike za varovanje dostopa tretje stranke, vendar pa so zatrdili, da je le-ta v izdelavi.

[2] O varovanju in ravnanju z informacijo imajo v podjetju poseben pravilnik, po katerem se morajo ravnati vsi zaposleni.

Predlagam, da v Gorenjski banki ocenijo tveganje pri dostopu tretje stranke in s tem ugotovijo, katere varnostne zahteve bodo potrebne, da bodo varnostne kontrole uspešno delovale. Varnostne zahteve naj vključijo v vse pogodbe, ki bodo sklenjene med organizacijo in tretjo stranko. Kopije teh pogodb naj primerno shranijo.

5.2.3 Razvrstitev in nadzor sredstev

V Gorenjski banki, d. d., imajo popisana vsa fizična sredstva, ki so v njihovi lasti, popisane pa imajo tudi vse podatkovne baze in aplikacije, ki jih uporabljajo v podjetju. Odgovornosti za posamezna sredstva so jasno opredeljene v posebnem pravilniku.

Predlagam, da v Gorenjski banki popišejo tudi vso sistemsko dokumentacijo, razvojna orodja in pripomočke.

Klasifikacija informacij v Gorenjski banki na javne in tajne je jasno opredeljena, vendar pa ni natančno jasno, kakšni so postopki za označevanje informacij, zato predlagam, da izdelajo pravilnik za označevanje informacij, ki bo jasno opredeljeval, katere informacije so lahko javnega in katere tajnega značaja.

5.2.4 Varovanje v zvezi z osebjem

V Gorenjski banki imajo poseben dokument (dokument poslovne tajnosti), v katerem so opredeljene odgovornosti vsakega posameznika, zaposlenega za varovanje informacij. Smotrno je, da ima podjetje tak dokument, podpisati pa ga mora zaposleni in vodstvo podjetja. Le na tak način se vsak zaposleni strinja in prevzema odgovornost na področju varovanja informacij.

Pri sprejemanju novih zaposlenih v podjetje morajo odgovorni za zaposlovanje v Gorenjski banki upoštevati posebno navodilo vodstva, da od bodočega zaposlenega pridobijo dokazilo, da ni bil nikoli sodno kaznovan, drugih verodostojnosti kandidata pa jim ni treba preverjati.

Predlagam, da podjetje preveri tudi identiteto kandidata ter njegove značajske lastnosti, saj bi se tako lahko izognili morebitnim težavam v zvezi z varnostjo, ki jih pozneje povzročajo kot zaposleni. Poudarijo naj tudi odgovornosti, ki jih bo uslužbenec imel do varovanja informacij.

Novo zaposleni mora tudi podpisati t. i. sporazum o zaupnosti, kjer se zaveže k tajnosti informacij, s katerimi dela. Odgovornost uslužbenca v zvezi z varovanjem informacij je urejena tudi v pogojih zaposlovanja, ki vključujejo tudi zakon o varovanju osebnih podatkov.

Vsi zaposleni v Gorenjski banki so usposobljeni za osnovno varovanje informacij, pooblaščenec za informacijsko varnost pa po potrebi izvede tudi poseben tečaj za tisti zaposlene, ki zaradi

specifičnega delovnega mesta in delovnih nalog potrebujejo dodatna znanja s področja varovanja informacij. Vsi zaposleni v sektorju informacijskih sistemov imajo enkrat mesečno tudi interno izobraževanje o novostih na področju varovanja informacij.

V primeru incidentov imajo v Gorenjski banki pripravljen načrt, ki natančno opredeljuje mesta, kjer lahko pride do izpadov ali okvar. V načrtu so natančno določeni tudi postopki ukrepanja ob incidentu na določenem mestu. Zaposleni so dolžni, da takoj prijavijo vsak incident, saj je to ključno za uspešno odpravo problema. V podjetju vsak incident skrbno opišejo, nato pa ga strokovnjaki preučijo in po potrebi izboljšajo postopek ukrepanja ob morebitni ponovitvi incidenta.

Za kršitelje varovanja informacij imajo v Gorenjski banki natančno določene disciplinske postopke, s katerimi so seznanjeni vsi zaposleni. S tem skušajo preprečiti hujše kršitve varnostne politike.

Predlagam, da naj v Gorenjski banki uvedejo tudi postopek za prijavo pomanjkljivosti pri varovanju informacij, saj za zdaj takega postopka ne poznajo. Organizacija naj zaposlene spodbuja k prijavi kakršnihkoli pomanjkljivosti, ki bi se pojavile pri varovanju informacij.

5.2.5 Fizična zaščita in varovanje okolja

Pred naravnimi nesrečami, kot so poplave in potresi, so najpomembnejša informacijska sredstva v Gorenjski banki zavarovana z debelimi nepropustnimi zidovi, vsi podatki pa se že v času zapisovanja beležijo na dveh različnih, med seboj ločenih lokacijah.

Delovni prostori v podjetju so dobro zavarovani pred nepooblaščenimi osebami. Vsi zaposleni morajo imeti pri sebi magnetne kartice, ki jim omogočajo vstope in izstope iz vnaprej določenih delovnih prostorov. Sistem pristopne kontrole z magnetnimi karticami tudi omogoča vodstvu podjetja, da lahko natančno nadzoruje prehode zaposlenih preko posameznih delovnih prostorov, zapisuje pa tudi natančen čas vhoda in izhoda. Pomembnejši delovni prostori pa so tudi dodatno zavarovani preko elektronskih kombinacijskih ključavnic, ki omogočajo odpiranje vrat z vnosom številčne kode, ki jo pozna le odgovorna oseba.

Ker spiskov s pravicami dostopa po vnosu pravic nihče več ne pregleduje, predlagam, da v organizaciji uvedejo postopek, s katerim bi lahko pooblaščenec za informacijsko varnost redno pregledoval spisek pravic dostopa.

Delovni prostori so opremljeni tudi s požarnim alarmom in protipožarno zaščito. Če pride do požara, se avtomatsko zaprejo vsa vrata okoli prostora, kjer je izbruhnil požar, zaposleni pa potem po posebnem predvidenem postopku zapustijo prostor. Kadar so prostori prazni, so vrata

avtomatsko zaklenjena, alarmne naprave pa so aktivirane. Zunaj delovnega časa izvaja nad poslovnimi prostori tudi fizični nadzor pooblaščena zunanja organizacija.

Delo na varovanih območjih s strani zunanje organizacije se izvaja pod budnim očesom pooblaščenca za informacijsko varnost ter pooblaščenca za splošno varnost. Vsa dela, ki jih v varovanih prostorih izvaja zunanji izvajalec, so natančno opisana v posebnem dokumentu.

V Gorenjski banki imajo tudi poseben prostor, ki se nepredušno zapre, ko se opravlja sprejem ali oddaja večje količine denarja, prevzemno ali dostavno službo pa preverijo le preko delovnih nalogov.

Predlagam, da naj v organizaciji beležijo tudi natančen čas sprejema ali oddaje, ime in priimek osebe, ki je sprejem ali oddajo izvedlo ter registrske številke sprejemnih ali dostavnih vozil.

Gorenjska banka se z energijo oskrbuje preko zunanje organizacije; če pa izpade električna energija, imajo v organizaciji tudi svoj agregat, ki ga enkrat mesečno preveri tudi zunanji strokovnjak.

Za vzdrževanje informacijske opreme v Gorenjski banki skrbijo zaposleni na oddelku za sistemsko podporo in produkcijo; če pa je projektov več, pa za podporo poskrbi zunanji izvajalec. V organizaciji izvajajo tudi politiko varnega uničenja opreme, ki jo določa pravilnik o arhiviranju in uničevanju nosilcev podatkov (gre za komisijsko uničevanje).

Glavni telekomunikacijski vodi so speljani pod zemljo, znotraj organizacije pa potekajo po zato nameščenih kanalih.
Predlagam, da v organizaciji uvedejo pravilnik, ki bo določal, na kakšen način morajo biti vodi, ki prenašajo podatke in podpirajo informacijske storitve, zaščiteni pred prestrezanjem ali poškodbami.

V Gorenjski banki nimajo nobenega posebnega dokumenta, ki bi določal varovanje prenosne opreme doma pri zaposlenih. Predlagam, da uvedejo enako stopnjo varnosti, kot velja znotraj organizacije, za prenosno opremo pa naj sklene tudi ustrezno zavarovalno polico.

Organizacija vzdržuje tudi t. i. hišni red, v katerem je natančno opredeljeno, v kakšnem stanju mora biti delovna miza med delovnim procesom, kako morajo biti nastavljeni ohranjevalniki zaslona, papirnati dokumenti pa morajo biti v predalih in nikakor ne smejo ležati na mizi. Hišni red obravnava tudi varovanje gesel, ki jih poleg odgovornih zaposlenih ne sme vedeti nihče razen njih samih, prepovedano pa jih je tudi kamorkoli zapisovati. V primeru odsotnosti odgovorne osebe z delovnega mesta, lahko vodja posameznega sektorja odobri sektorju za varovanje informacijskih sistem namestiti novo geslo.

5.2.6 Upravljanje s komunikacijami in produkcijo

Delovni postopki v Gorenjski banki so jasno opredeljeni, saj obstaja za vsak delovni postopek poseben dokument, ki zajema odgovornosti za ravnanje z informacijami, časovno razporeditev dela ter navodila za ravnanje, če nastane okvara se delovni proces zaustavi. Ravno tako imajo za delovanje informacijskega sistema poseben načrt, ki opredeljuje, kako naj odgovorni zaposleni ravnajo v primeru kakršnegakoli incidenta (izbruh zlonamerne kode, napake v strojni ali programski opremi, izpad elektrike…).

V Gorenjski banki nimajo najbolje urejeno ločevanje nalog, saj v večini primerov ena oseba neko novost načrtuje in jo tudi izvede. Predlagam, da v organizaciji ločijo načrtovanje in izvajanje nalog, saj bi tako lahko neka oseba preverila, ali je prejšnja oseba izvedla vse potrebno za prehod na spremembo.

V Gorenjski banki redno (dvakrat dnevno) preverjajo zaščito pred zlonamerno kodo na področju elektronske pošte, lokalnih delovnih postaj in medmrežja. Vse podatke o preverjanju zaščite tudi shranjujejo za morebitne poznejše odpravljanje težav. Vsi podatki, ki se zapisujejo na nosilce podatkov v glavni zgradbi Gorenjske banke, se istočasno zapisujejo tudi na nosilce podatkov na drugi lokaciji. Za izdelavo teh varnostnih kopij imajo poseben pravilnik, ki natančno opredeljuje, koliko časa naj se podatki hranijo ter na kakšen način naj se shranjujejo. Tudi za odstranitev nosilcev podatkov imajo poseben dokument, ki opredeljuje natančne postopke uničenja.

Predlagam, da uvedejo dokumentiranje postopka dvojnega zapisovanja podatkov. Redno naj testirajo varnostne nosilce ter pravilnost podatkov. Za informacije, pri katerih ni zakonsko določen čas hranjenja, predlagam, da uvedejo pravilnik, ki bo določal čas hranjenja teh informacij.

V Gorenjski banki imajo za varovanje informacij uraden postopek. Informacije so razporejene v skupine, za vsako skupino informacij pa so določene kontrole za varno ravnanje z vsemi oblikami informacij znotraj te skupine. Za izmenjavo informacij z drugimi organizacijami nimajo nobenih posebnih dokumentov, vendar pa morajo vsi zaposleni upoštevati krovno varnostno politiko, kjer je jasno opredeljeno, katere informacije so tajne narave.

Predlagam, da v Gorenjski banki uvedejo tudi varovanje sistemske dokumentacije, do katere naj imajo dostop le pooblaščene osebe.

5.2.7 Nadzor dostopa

Gorenjska banka ima izdelano politiko nadzora dostopa, kjer so natančno opredeljene vse pravice za posamezna delovna mesta. Gre za pravila o registraciji uporabnika, ki zajemajo navodila, kako ravnati s podatki o uporabniku ter kakšen nivo dostopa naj ima uporabnik, pravila o upravljanju s pravicami, kjer je opredeljeno, kakšne pravice ima lahko nek uporabnik na določenem delovnem mestu, ter pravila o uporabniških geslih, kjer so tudi zapisane odgovornosti uporabnika do ravnanja z geslom (na koliko časa ga je treba spremeniti, dolžina in struktura gesla…). Zunanje uporabnike v organizaciji preverjajo preko uporabniškega imena in gesla ter certifikata, ki je izdelan na podlagi javnega in zasebnega ključa. Tudi dostop do določenih aplikacij je omejen, saj organizacija skrbi, da imajo uporabniki dostop do informacij v skladu s poslovnimi zahtevami. Za vsakega uporabnika je tudi določeno, ali lahko informacije le bere ali pa jih lahko tudi spreminja in briše. Vsi dostopi do določenih delov informacijskega sistema se zapisujejo. Tako je mogoče natančno ugotoviti identifikacijo uporabnika, datum in natančno uro prijave in odjave od sistema ter njegov omrežni naslov.

V organizaciji nimajo postopkov za redno pregledovanje pravic dostopa, zato predlagam, da uvedejo pravilnik, ki bo to dovoljeval. Pomembno je, da bodo uporabnike s posebnimi pravicami preverjali bolj redno, kot ostale uporabnike. Preverjanje uporabnikov naj se beleži, izvaja pa naj ga pooblaščenec za informacijsko varnost.

V organizaciji nimajo nobenih pravil, kako naj zaposleni ravnajo ob odsotnosti z delovnega mesta, zato predlagam, da takoj, ko prenehajo z delom, prekinejo sejo s strežnikom, računalnik pa zaklenejo.

Predlagam tudi, da v organizaciji izdelajo poseben pravilnik za varovanje omrežja, kjer bo natančno določeno, kakšen dostop je posameznemu uporabniku dovoljen, dostopanje pa naj se tudi beleži. Smotrno bi bilo, da bi imela organizacija odprto minimalno možno število omrežnih povezav.

Ponudnik interneta za Gorenjsko banko je zunanja organizacija, zato predlagam, da pridobi seznam uporabljenih varnostnih značilnosti, na njegovi osnovi pa izdela pogodbo o varovanju.

5.2.8 Razvoj in vzdrževanje sistemov

Za kakršnokoli nadgradnjo informacijskega sistema ali za razvoj nove programske opreme, imajo v organizaciji dokument, ki jasno opredeljuje, kako naj se izvede analiza tveganja ter kako naj se na podlagi izvedene analize tveganja opredeli varnostne zahteve. Določeno je tudi, kako naj se preverja vhodne podatke, kako naj se nadzira notranja obdelava podatkov ter kako naj se preverja izhodne podatke. Uporabljajo tudi kriptografske kontrole, s katerimi skrbijo za zaščito zaupnosti, verodostojnosti in celovitosti informacij. Kriptografske kontrole uporabljajo na področju

elektronske pošte in elektronskega bančništva (na tem področju se uporablja tudi šifriranje in digitalni podpis).

Na področju varovanja informacijskega sistema in aplikacij sodeluje Gorenjska banka z zunanjimi organizacijami, ki so na tem področju že dolgo časa prisotne in preizkušene, vseeno pa na ključnih mestih, kjer obstaja nevarnost trojanskega konja ali skritega prehoda, vgradijo tudi svoje kontrole.

5.2.9 Upravljanje neprekinjenega poslovanja

Za upravljanje neprekinjenega poslovanja imajo v Gorenjski banki poseben načrt (sestavljen je na podlagi analize dogodkov, ki lahko ogrozijo neprekinjeno poslovanje), ki vsebuje navodila, kako ravnati, če nastanejo prekinitve, motnje ali okvare. Natančno je tudi opredeljeno, kdo je odgovoren za izvajanje takšnih ukrepov. Znotraj načrta so izdelani različni scenariji, ki jih po potrebi tudi testirajo. Če testi rezultirajo nepričakovano, je treba načrt neprekinjenega poslovanja ustrezno dopolniti. Učinkovitosti načrta za neprekinjeno poslovanje ne preverjajo.

Predlagam, da naj v Gorenjski banki redno preverjajo učinkovitost načrta za neprekinjeno poslovanje,. Določijo naj se časovni razmiki med posameznimi testiranji, rezultati preverjanja pa naj se ustrezno shranijo. Smotrno bi bilo, da se izvajajo tudi nenapovedani testi, da se lahko oceni usposobljenost zaposlenih.

5.2.10 Združljivost

V Gorenjski banki so s strani slovenske zakonodaje in Banke Slovenije zavezani spoštovati zakonske zahteve na področju varovanja informacij, veljavno zakonodajo pa redno preverjajo preko Uradnega lista. Vse pravne, zakonske in pogodbene obveznosti so dokumentirane, dokumentirana pa je tudi zakonodaja držav, s katerimi Gorenjska banka posluje. Tudi organizacijski zapisi se shranjujejo v skladu s slovensko zakonodajo in predpisi. Na področju varovanja osebnih podatkov imajo v Gorenjski banki kataloge zbirk osebnih podatkov, pravilnik o varstvu podatkov, za zunanjo obdelavo podatkov pa imajo pogodbe in pooblastila.

Vsi uporabniki, ki upravljajo z opremo za obdelavo informacij, so s podpisom izjave o varovanju informacij zavezani k spoštovanju varovanja informacij. Gorenjska banka tudi zagotavlja izvajanje vseh varnostnih postopkov, njihovo redno pregledovanje ter združljivost z varnostno politiko organizacije. Izvaja se tudi presoja informacijskega sistema, ki je ključna za zmanjšanje nevarnosti prekinitve poslovnega procesa.
Nadzor uporabe programske opreme je dokaj slab, saj v organizaciji nimajo dokumentirano, katera licenčna programska oprema se nahaja na posameznem računalniku. Predlagam, da programsko opremo za vsak posamezen sistem dokumentirajo in shranijo na varno mesto. Uvede

naj se tudi pravilnik o uporabi programske opreme, ki uporabniku lahko služi le v službene namene.

6 SKLEP

Za informacijsko varnost v podjetjih ni odgovorna le služba za informatiko, temveč postaja informacijska varnost problem celotnega podjetja. Vodstvo podjetja mora zagotoviti ustrezno politiko varovanja informacij, ki mora biti skladna s poslovnimi cilji podjetja. Tudi vsi zaposleni, pogodbeni delavci in navsezadnje stranke se morajo nenehno izobraževati na tem področju. Varovanje informacij je sistematični model, ki mora biti zajet na vseh nivojih organizacije.

V diplomski nalogi je najprej razloženo področje varovanja informacij, sistem za upravljanje varovanja informacij in standard BS 7799, drugi del pa preverja skladnost podjetja Gorenjska banka, d. d., s tem standardom. Preverjanje je izvedeno na podlagi poglavij, ki jih standard zajema. Gre za preverjanje varnostne politike, organiziranosti varovanja, razvrstitve in nadzora sredstev, varovanja v zvezi z osebjem, fizične zaščite in varovanja okolja, upravljanja s komunikacijami in produkcijo, nadzora dostopa, razvoja in vzdrževanja sistemov, upravljanja neprekinjenega poslovanja in preverjanje združljivosti.

Preverjanje skladnosti podjetja s standardom BS 7799 sem izvedel s pomočjo pogovora s pooblaščencem za informacijsko varnost, vpogled pa sem dobil tudi v vse interne akte, ki na kakršenkoli način zajemajo področje varovanja informacij. Ugotovil sem, da se v Gorenjski banki, d. d., ne ravnajo popolnoma po priporočilih, ki jih postavlja standard BS 7799, saj določenih pravilnikov sploh nimajo, nekateri pa slabo opredeljujejo svoje področje. V pogovoru so mi zatrdili, da se trenutno stanje nenehno izboljšuje, vendar pa sem mnenja, da bi dodatno pomoč pri uvajanju skladnosti organizacije s standardom lahko poiskali tudi pri kakšnem strokovno usposobljenem podjetju.

Poseben varnostni forum skrbi za informacijsko varnost in za čim bolj dosledno upoštevanje standarda, zaposleni pa se morajo na tem področju nenehno izobraževati. V podjetju je vpeljan tudi sistem za upravljanje varovanja informacij, v njem pa sodelujejo vsi zaposleni, pogodbeni delavci in tudi stranke.

LITERATURA

1. Berčič Boštjan et al.: Ukrepi v primeru informacijskih nesreč. Nova Gorica : Inštitut za informacijsko varnost, 2003. 148 str.
2. Bratuša Tomaž, Verdonik Ivan: Hekerski vdori in zaščita. Ljubljana : Pasadena, 2005. 280 str.
3. British standard BS 7799-2: 2002: Sistemi za upravljanje varovanja informacij – specifikacija s smernicami za uporabo. Nova Gorica : Inštitut za informacijsko varnost, 2003. 93 str.
4. Divjak Saša: Operacijski sistemi. Ljubljana : Fakulteta za računalništvo in informatiko, 2001. 175 str.
5. Egan Mark, Mather Tim: Varovanje informacij – grožnje, izzivi in rešitve. Ljubljana: Pasadena, 2005. 300 str.

6. Frelih Gregor: Zlonamerni programi in zaščita informacijskih sistemov podjetja. Diplomsko delo. Ljubljana : Ekonomska fakulteta, 2004. 46 str.
7. Gibson Steve: Description and analysis of a potent, increasingly prevalen, and worrisome internet attack. Gibson Research Corporation. [URL: http://www.grc.com/dos/drdos.htm], 22. 2. 2002.
8. Golec Darko: Vpeljava standarda BS 7799-2:2002. Seminarska naloga. Ljubljana : Fakulteta za računalništvo in informatiko, 2005. 18 str.
9. Gradišar Miro: Informatika v poslovnem okolju. Ljubljana : Ekonomska fakulteta, 2001. 508 str.
10. Gradišar Miro: Uvod v informatiko. Ljubljana : Ekonomska fakulteta, 2003. 516 str.
11. Janežič Damjan et al.: Grožnje elektronskega poslovanja – upravljanje z informacijskimi tveganji. Zbornik. Nova Gorica : IZZIV, 2004. str 34.
12. Kjaer Torben: Začnimo z internetom: naj ostane preprosto!. Šempeter pri Gorici : Flamingo, 2000. 58 str.
13. Ključevšek Rado: Standard za varnost. Sistem (Priloga revije Monitor), Ljubljana, 2002, 9, str. 18-19.
14. Konečnik Tadeja: Novi standardi za varnost podatkov. Gospodarski vestnik, Ljubljana, 2002, št. str. 22-23.
15. Može Marko: Zagotavljanje varnosti v lokalnem informacijskem sistemu. Diplomska naloga. Ljubljana : Fakulteta za elektrotehniko, 2003. 47 str.
16. Rakovec Sašo: Iskraemeco vzpostavlja celovit sistem obvladovanja informacijske varnosti. Varnostni forum, februar 2005, str. 6-7.
17. Rakovec Sašo: Varovanje informacij skladno s standardom BS 7799. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 2005a. 92 str.
18. Razvojne prelomnice. [URL: http://www.gbkr.si/html/banka/prelomnice_nastanek.html], 1. 8. 2007.
19. Shrestha Amarottam: Information Security Management System (7799) for an Internet Gateway. Maryland: SANS Institute, 2004. 30 str.
20. Trček Denis: Informatika: od tehnologije do poslovanja. Koper : Visoka šola za management, 2001. 177 str.
21. Vidmar Tone: Informacijsko komunikacijski sistem. Ljubljana : Pasadena, 2002. 864 str.
22. Zupan Blaž: Standardizacija in kakovost informacijskih sistemov. Ljubljana : Fakulteta za računalništvo in informatiko, 2003. 112 str.

VIRI

1. Hajtnik Tatjana: Kako varovati informacije v javni upravi?. Ministrstvo za javno upravo. [URL: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/sodobnajavnauprava/ppt/smaragdna_B/HAJTNIK_T..ppt#439], 20. 7. 2007.

2. Izogibanje nezakoniti programski opremi. [URL: http://www.microsoft.com/slovenija/piratstvo/default.mspx], 15. 7. 2007.
3. Krovna varnostna politika. Interno gradivo. Kranj : Gorenjska banka, 2005.
4. Measures of the Value of Information. [URL: http://www.umsl.edu/~sauter/analysis/info/info.htm], 19. 7. 2007.
5. Navodila za omejitev prejemanja elektronske pošte in sproščanje zaustavljene pošte. Interno gradivo. Kranj : Gorenjska banka, 2003.
6. Pravilnik o hišnem redu. Interno gradivo. Kranj : Gorenjska banka, 2007.
7. Pravilnik o naročanju in izdaji digitalnih certifikatov. Interno gradivo. Kranj : Gorenjska banka, 2003.
8. Pravilnik o varstvu osebnih podatkov. Interno gradivo. Kranj : Gorenjska banka, 2004.
9. Pravilnik o vzdrževanju predstavitvenih strani Gorenjske banke, d. d. Kranj na internetu. Interno gradivo. Kranj : Gorenjska banka, 2004.
10. Predstavitev virusov, črvov in trojanskih konjev. [URL: http://www.microsoft.com/slovenija/doma/varnost/virusi/predstavitev_virusov.mspx], 9. 3. 2004.
11. Računalniško piratstvo. [URL: http://www.bsa.si/piratstvo.php], 25. 6. 2007.
12. Singh Simon: Knijga šifer. Tržič : Učila International, 2006. 430 str.
13. Slovar informatike. [URL: http://www.islovar.org/slovar_oslovarju.asp], 4. 9. 2007.
14. Storitve s področja varovanja in izobraževanja o varovanju podatkov. [URL: http://www.microprocess.si/vp.htm], 23. 7. 2007.
15. Strategija razvoja. [URL: http://www.gbkr.si/html/banka/strategija_politika.html], 15. 8. 2007.
16. Tulloch Mitch: Zvijače za Windows server: 100 najboljšnih nasvetov in orodij. Ljubljana : Pasadena, 2005. 403 str.
17. Varnostna politika. [URL: http://www.astec.si/slo/index.php?option=com_content&task=view&id=27&Itemid=62]. 3. 8. 2007.
18. What is spyware. [URL: http://www.microsoft.com/protect/computer/basics/spyware.mspx], 23. 10. 2006.
19. Wikipedia. [URL: http://sl.wikipedia.org/wiki/Napaka], 1. 7. 2007.

SLOVAR SLOVENSKIH PREVODOV TUJIH IZRAZOV

- Backdoor: stranska vrata
- Bug: hrošč
- Datagram: paket
- E-mail:elektronska pošta
- File sharing programs: programi za deljenje datotek
- Firewall: požarni zid
- Hardware: strojna oprema
- Hecker: vdiralec
- Malicious code: zlonamerna koda
- Malicious mobile code: mobilna zlonamerna koda
- Piracy: piratstvo
- Port: vhodno – izhodna vrata
- Proxy: namestniški strežnik
- Social engineering: socialni inženiring
- Software: programska oprema
- Spyware: vohuni
- Trojan horse: trojanski konj
- Virus: virus
- Worm: črv

SLOVAR KRATIC

- ACL: Access Control List
- BS: British Standard
- BSI: British Standard Institution
- CCSC: Commercial Computer Security Centre
- CFIS: Common Internet File System
- Ddos: Distributed Denial of Service
- DMZ: Demilitarized zone
- Dos: Denial of Service
- FTP: File Transfer Protocol
- HTTP: Hypertext Transfer Protocol
- ITSEC: Information technology security evaluation criteria
- LAN: Local Area Network
- OSI: Open System Information
- RBAC: Role Based Access Control
- S.W.I.F.T.: Society for Worldwide Interbank Financial Telecommunication
- SMB: Server Message block
- SMTP: Simple Mail Transfer Protocol
- SUVI: Sistem za upravljanje varovanja informacij