UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

PRILAGODITEV INFORMACIJSKEGA SISTEMA VARNOSTNIM ZAHTEVAM NA PRIMERU DELAVSKE HRANILNCE

Ljubljana, februar 2008 RENATO ZALOŽNIK

IZJAVA

Študent Renato Založnik izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom 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 6.2.2008

Podpis:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

PRILOGA 1

SLOVAR IZRAZOV IN KRATIC

ACL (Access Control Lists) - seznam za kontrolo dostopov,
AD (Active Directory) - aktivni imenik domene,
ADSL (Asymmetric Digital Subscriber Line) - model tehnologije DSL za prenos podatkov,
AES (Advanced Encryption Standard) - novejši šifrirni algoritem,
ARP (Address Resolution Protocol) - protokol za pretvorbo omrežnega naslova v fizični naslov naprave,
BIA (Bussines Impact Analysis) - analiza vplivov na poslovanje,
BCP (Business Continuity Plan) - plan neprekinjenega poslovanja,
BGP (Border Gateway Protocol) - internetni protokol za usmerjanje,
CA (Certificate Authority) - certifikatska agencija,
CIA (Confidentiality, Integrity, Availability) - oznaka za zaupnost, neokrnjenost, razpoložljivost,
DBA (Database Administrator) - skrbnik baze podatkov,
DBMS (DataBase Management System) - sistem za upravljanje baz podatkov,
DES (Data Encryption Standard) - starejši šifrirni algoritem,
DHCP (Dynamic Host Configuration Protocol) - protokol za dinamično dodeljevanje omrežnih naslovov,
DNS (Domain Name System) - sistem za preslikavo domenskih imen in omrežnih naslovov,
DMZ (Demilitarized Zone) - vmesno področje na požarni pregradi,
DOS (Denial-of-Service) - vrsta napada z onemogočanjem storitev,
DRP (Disaster Recovery Plan) - načrt okrevanja po katastrofi,
DSL (Digital Subscriber Line) - tehnologija za prenos podatkov,
EMV (Eurocard, MasterCard, Visa) - standard za plačilne kartice s čip tehnologijo,
FR (Frame Relay) - tehnologija za posredovanje blokov,
FW (Firewall) - požarna pregrada,
ISMS (Information Security Management System) - standard za upravljanje informacijske varnosti,
ISDN (Integrated Services over Digital Network) - digitalno telefonsko omrežje,
ITSEC (Information Technology Security Evaluation Criteria) - standard za ocenjevanje varnosti informacijskih sistemov v Evropski uniji,
ITIL (Information Technology Infrastructure Library) - zbirka najboljših praks v informatiki,
LAN (Local Area Networks) - lokalno omrežje,
MPLS (MultiProtocol Label Switching) - tehnologija za posredovanje poti,
MSBA (Microsoft Security Baseline Analyzer) - orodje za ugotavljanje varnosti,
NAT (Network Address Translation) - tehnika preslikave omrežnih naslovov,
NSA (National Security Agency) - nacionalna varnostna agencija v Združenih državah Amerike,
OS (Operating System) - operacijski sistem,
OSI (Open Systems Interconnection) - referenčni model za povezovanje odprtih sistemov,
PGP (Pretty Good Privacy) - program za šifriranje podatkov,
PIN (Personal Identification Number) - osebna številka,
PKI (Public Key Infrastructure) - infrastruktura javnih ključev,
RDP (Remote Desktop Protocol) - protokol za oddaljen dostop do računalnika,

RSA (Rivers, Shamir, Adleman) - algoritem za šifriranje z javnim ključem,
SAN (Storage Area Network) - omrežje pomnilniških naprav,
SEPA (Single Euro Payments Area) - enotno področje plačil v evrih,
SIGEN-CA (Slovenian General Certification Authority) - certifikatska agencija Ministrstva za javno upravo,
SNMP (Simple Network Management Protocol) - protokol za upravljanje omrežja,
SQL (Structured Query Language) - strukturni poizvedovalni jezik za delo s podatkovnimi bazami,
SSH (Secure Shell) - program za prijavo na oddaljen sistem,
SSL (Secure Sockets Layer Protocol) - protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem,
TCSEC (Trusted Computer Security Evaluation Criteria) - standard za ocenjevanje varnosti informacijskih sistemov v Združenih državah Amerike,
VDSL (Very-high-bit-rate DSL) - model tehnologije DSL za prenos podatkov,
VLAN (Virtual Local Area Networks) - navidezno lokalno omrežje,
VPN (Virtual Privat Network) - navidezno zasebno omrežje,
WAN (Wide Area Networks) - omrežje velikega dosega,
WSUS (Windows Update Server) - sistem za nadgrajevanje Windows okolja,
3DES (Triple Data Encryption Standard) - novejši šifrirni algoritem.

1 UVOD

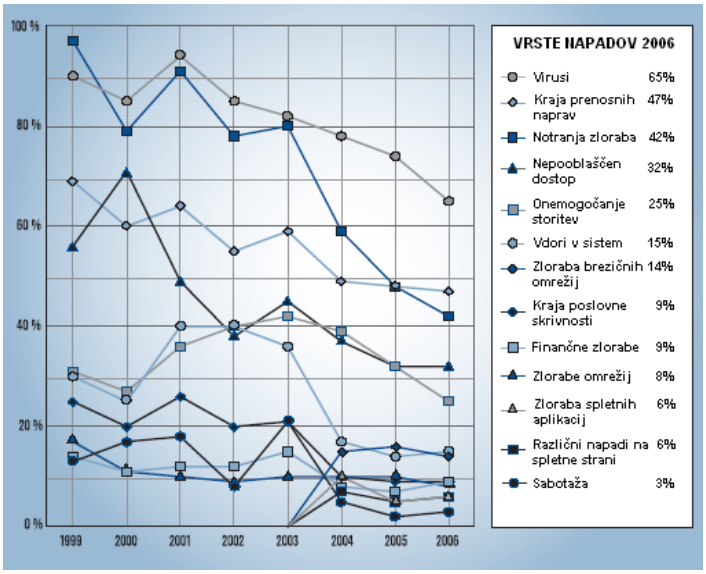
Opredelitev problema

Banke in hranilnice v Sloveniji so v procesu prilagajanja svojih informacijskih in plačilnih sistemov tako imenovani Skupni evropski platformi in vključevanja vanjo. Omenjene aktivnosti in projekti, nadzorovani s strani Banke Slovenije, zahtevajo hitre in relativno zahtevne prilagoditve informacijskih sistemov na strani bank in hranilnic.

Vzporedno z omenjenim projektom so se banke in hranilnice v skladu z zahtevo Banke Slovenije pripravile tudi na uresničevanje sklepa o izračunavanju in obvladovanju tveganj po kapitalskem sporazumu Basel II, ki je začel veljati v začetku leta 2008. Udejanjenje sprejetih sklepov bo vsekakor izboljšalo nivo merjenj in upravljanj tveganj na posameznih področjih, med katerimi tveganja informacijskih sistemov oziroma informacijska tveganja obravnavamo kot eno izmed pomembnih področij operativnih tveganj (Basel II, 2007).

Različne raziskave potrjujejo, da se banke in hranilnice še vedno premalo zavedajo tveganj na področju varnosti informacijskih sistemov. Kot prikazuje Slika 1, se različne oblike varnostnih incidentov, kot so okužbe z virusi, odtujitve mobilnih naprav, zlorabe omrežij od znotraj, nepooblaščeni dostopi, onemogočanje storitev in druge oblike vdorov v informacijske sisteme, dogajajo.

Slika 1: Raziskava o računalniškem kriminalu in varnosti za leto 2006



Vir: CSI/FBI Computer Security Institute, 2006, str. 13.

V Sloveniji se spominjamo odmevnega varnostnega incidenta v letu 2002, ko je gumarskemu tehniku Robertu Škulju s pomočjo trojanskega konja uspelo vdreti v spletno poslovalnico Klik, kar mu je omogočilo vključitev v zaupno komunikacijo med banko in komitentom. Področje varnosti elektronskega poslovanja je potrebno

obravnavati celovito ter pri tem upoštevati tudi pravne vidike elektronskega poslovanja na internetu (Jerman-Blažič, 2001, str. 102).

Prelomni primer vdora v poslovanje banke se je zgodil v letu 2005 z ropom sefov SKB banke. Zaradi tega dogodka so banke in hranilnice spoznale, da morajo varnost sistema in prostorov obravnavati bolj resno ter na višjem nivoju. Več kot polovica informacijskih napadov v letu 2005 je imelo za cilj pridobivanje zaupnih podatkov s prevaro, sledijo: zlonamerno preusmerjanje uporabnikov na lažne spletne strani, napadi z vohunsko in s škodljivo programsko opremo, odtujitev kritične opreme. Izvedba teh kršitev kaže na dobro organizacijo, najverjetneje celo organiziranih kriminalnih združb. V Sloveniji o organiziranih kriminalnih združbah sicer še ne moremo govoriti, včasih gre za primere šibko povezane hekerske skupine. Na trgu obstaja literatura, ki podrobno opisuje metode in postopke različnih vdorov v informacijski sistem (Bratuša, 2006, str. 10-45).

Tudi v letu 2006 je prišlo do zlorab in poskusov zlorab bančnih informacijskih sistemov in varnostnih mehanizmov. Tako beležimo vdor v bančni sistem in krajo številk bančnih kartic, odtujitve prenosnih računalnikov, POS opreme za plačevanje s plačilnimi karticami, zlorabe kartic na bankomatih, zlorabe poslovanja s spletnimi bankami itd. Raziskava, ki jo je opravila mednarodna organizacija JupiterResearch v letu 2005 je pokazala, da lahko banke varnost lastnega spletnega bančništva poudarjajo kot prednost pred konkurenco. Kar 37 % uporabnikov elektronskega bančništva verjame, da so nekatere banke bolj varne od drugih, 43 % jih postavlja spletno varnost med tri najpomembnejše dejavnike pri izboru banke. 34 % spletnih uporabnikov glede varnosti bolj zaupa velikim kot pa manjšim lokalnim bankam (JupiterMedia, 2005).

Problema zagotavljanja informacijske varnosti se z vso resnostjo zavedamo tudi v Delavski hranilnici, kjer sem zaposlen. Hranilnica ima v svoji poslovni mreži 14 poslovalnic, v katerih je zaposlenih 90 ljudi po vsej Sloveniji. Bančno poslovanje je podprto s centralnim informacijskim sistemom, ki je nameščen v računalniškem centru v Ljubljani. Informacijski sistem poleg podpore bančnim okencem in zalednim službam vključuje tudi podporo za domači plačilni sistem Giro kliring, mednarodni plačilni sistem Swift, spletno banko Dh-Plus za fizične in Dh-Net za pravne osebe ter lastno bankomatsko omrežje hranilnice. Za zagotavljanje varnosti informacijskega sistema v hranilnici je odgovorna uprava hranilnice in višje vodstvo, ki je zadolženo za uresničevanje in vzdrževanje že sprejete varnostne politike ter za upravljanje informacijskih in drugih operativnih tveganj v hranilnici. Pri načrtovanju informacijske varnosti hranilnica upošteva priporočila Banke Slovenije ter metodologije, pripravljene v okviru Združenja bank Slovenije. Zagotavljanje informacijske varnosti pomeni neprekinjen proces planiranja, izboljševanja ter stalnega preverjanja informacijskega sistema (Egan, 2005, str. 45-64).

Zaradi hitrega razvoja poslovne mreže in z njim povezane rasti števila zaposlenih, ki se je v zadnjih dveh letih podvojilo, ter sočasne izvedbe zahtevnih projektov, kot sta

prevzem evro valute in uvedba mednarodnih računovodskih standardov, je hranilnica v zadnjem letu verjetno premalo pozornosti posvečala varnosti informacijskega sistema. Poraja se vprašanje, ali so bili omenjeni projekti v celoti izvedeni v skladu s strategijo razvoja informacijskega sistema in organizacije kot celote? (Gradišar, 2001, str. 423)

Ocenjujem, da informacijski sistem hranilnice zaradi hitrega in nenehnega razvoja ter omejenosti s kadrovskimi in finančnimi viri na področju informacijske tehnologije trenutno ne izpolnjuje vseh varnostnih zahtev in trendov, ki jih opredeljujejo mednarodno uveljavljeni standardi varovanja informacij, kot sta: ISO/IEC 17799:2005 in ISO/IEC 27001:2006 (Haren, 2006, str. 9).

Skrb za zagotavljanje varnosti sedanjega informacijskega sistema hranilnice dodatno povečujejo zgoraj omenjene raziskave in podatki, ki nazorno prikazujejo trend naraščanja varnostnih incidentov v slovenskem bančnem okolju, kjer po pogostosti dogodkov izstopajo sistemi za elektronsko poslovanje s komitenti (spletne banke, bankomati, kartični terminali). Tudi na področju zagotavljanja neprekinjenega poslovanja hranilnica do sedaj z izjemo plačilnega sistema Swift še nima zagotovljenih drugih gradnikov informacijskega sistema na rezervni lokaciji, kar dodatno povečuje pomembnost zagotavljanja varovanja podatkov na primarni lokaciji (White, 2003, str. 405). Za hranilnico bi morebitna izguba podatkov, razkritje le-teh, nedelovanje informacijsko podprtih poslovnih procesov ali zloraba sistema pomenili veliko finančno in poslovno škodo ter težko merljivo in popravljivo izgubo ugleda, ki jo hranilnica ima pri svojih komitentih.

Omenjena dejstva opisujejo problematiko zagotavljanja varnosti informacijskega sistema hranilnice, ki trenutno ne izpolnjuje vseh zahtev in ga je potrebno podrobno analizirati s standardnim pristopom pregleda vseh delov sistema: naprav, operacijskih sistemov, programov, baz podatkov, fizičnih in logičnih kontrol ter organizacije dela (Champlain, 2003, str. 25-202).

V nadaljevanju dela bom na primeru Delavske hranilnice poiskal največja tveganja in predlagal ukrepe ter priporočila za prilagoditev njenega informacijskega sistema varnostnim zahtevam za bančno poslovanje.

Namen in cilj magistrskega dela

Namen magistrskega dela je s stališča varnosti kritično analizirati dele informacijskega sistema, ki jih hranilnica uporablja za podporo bančnemu poslovanju. Cilj dela je na podlagi analize obstoječih varnostnih mehanizmov in analize tveganj predlagati ukrepe in rešitve za izboljšanje varnosti ter prilagoditev informacijskega sistema hranilnice varnostnim zahtevam za bančno poslovanje. Priporočila bodo osnova za odločanje, ali je potrebno posamezno tveganje zmanjšati z investicijo v varnostne elemente, ali lahko to tveganje hranilnica sprejme, prenese ali obvlada.

Metode dela

V magistrski nalogi bom uporabil znanje, ki sem ga pridobil pri podiplomskem študiju na Ekonomski fakulteti, ter izkušnje pri vodenju in sodelovanju v različnih projektih na področju informacijske tehnologije in plačilnih sistemov. Pri tem bom znanje o posameznih strokovnih področjih dodatno izpopolnjeval s študijem domače in tuje literature, člankov, mednarodnih standardov, zakonov, internih virov Delavske hranilnice ter informacij, pridobljenih na svetovnem spletu.

Naloga je razdeljena na štiri dele. V prvem delu bom predstavil informacijski sistem Delavske hranilnice in strategijo upravljanja z varnostjo. V drugem delu bom z metodo kritične analize obstoječega stanja analiziral zaščito in varnostne mehanizme informacijskega sistema. V tretjem delu bom s pomočjo analize tveganj izdelal oceno varnosti informacijskega sistema hranilnice in njegovih posameznih delov. V zadnjem delu bom z ukrepi in s priporočili predlagal rešitve za prilagoditev informacijskega sistema hranilce varnostnim zahtevam za bančno poslovanje.

2 INFORMACIJSKI SISTEM

2.1 Zgodovina in razvoj

Delavska hranilnica je največja hranilnica v Sloveniji. Na slovenskem bančnem trgu je prisotna od leta 1991. Od leta 1992 ima dovoljenje Banke Slovenije za opravljanje finančnih storitev ter je vključena v jamstveno shemo bank in hranilnic za zavarovanje vlog. Kot je prikazano na Sliki 2, je v poslovni mreži hranilnice 12 podružnic, ki jih sestavlja 14 poslovalnic, ki so enakomerno razporejene po celotni Sloveniji. Hranilnica ima zaposlenih 90 ljudi, pretežno z višjo in visoko izobrazbeno stopnjo, ki so locirani na sedežu hranilnice v Ljubljani ter v poslovalnicah po Sloveniji. S svojo poslovno mrežo hranilnica opravlja storitve bančništva na drobno za fizične osebe in storitve poslovnega bančništva za pravne osebe s poudarkom na kreditno-depozitni dejavnosti.

Slika 2: Poslovno omrežje Delavske hranilnice

Vir: Interni akti Delavske hranilnice, 2007.

Uvedba informacijskega sistema hranilnice sega v leto 1991, ko je hranilnica prvič vzpostavila celovit informacijski sistem za podporo svojim poslovnim procesom na zmogljivem HP strežniku z uporabo bančne aplikacije Hibis (računalniška programska oprema za podporo bančnemu informacijskemu sistemu, ki jo razvija podjetje HRC). Glavni poudarek pri postavitvi takratnega sistema je bil na vzpostavitvi računalniške podpore poslovanju, ni pa bil tudi na zadostitvi zahtevam za varovanje podatkov in zaščito sistema.

Razvoj informacijskega sistema je vseskozi sledil potrebam in ciljem hranilnice in se je razvijal skladno z rastjo poslovanja, s širjenjem poslovne mreže in z večanjem števila zaposlenih. Potekal je na vseh področjih, in sicer od prenov in dograditev strojne in komunikacijske opreme pa vse do stalnih dograditev aplikativne programske opreme. Največji razvoj je bil narejen prav na področju razvoja programske opreme, in sicer zaradi uvedbe novih storitev in funkcionalnosti, ki jih je narekoval konkurenčni slovenski bančni trg. To so bile različne oblike varčevanj in kreditiranj, spremembe na področju domačega in tujega plačilnega prometa, uvedba elektronskega bančništva, kartičnega in bankomatskega poslovanja, itd. V zadnjih dveh letih je trend razvoja programske opreme narekovala zahteva po prilagajanju najrazličnejšim mednarodnim standardom in evropskim predpisom, ki urejajo bančno poslovanje na področju varnosti poslovanja in upravljanja s tveganji.

Od prvega sistema pa vse do danes je hranilnica izvedla tri večje prenove centralnega informacijskega sistema za podporo bančnemu poslovanju. Pri vsaki naslednji prenovi je imela in ima varnost informacijskega sistema pomembnejšo vlogo in večjo pozornost. Z razvojem internetnega omrežja so se razvijale nove oblike elektronskega poslovanja, vendar so se istočasno povečevale tudi grožnje za vdor in zlorabe informacijskega sistema, kar dokazujejo nekateri odmevnejši primeri vdorov in zlorab v slovenskem bančnem prostoru. Nova tveganja so hranilnico spodbudila, da je v zadnjih dveh letih več sredstev vlagala v varnost in razvoj zaščite informacijskega sistema. Pri tem je upoštevala priporočila mednarodnih standardov BS7799 in ISO17799. Na ta način je hranilnica izboljševala zaščito na vseh delih informacijskega sistema. Tako je investirala v zaščitno opremo, vzpostavila je varnostno politiko in centralni sistem za upravljanje z informacijsko varnostjo, pripravila je načrt za zagotovitev neprekinjenega poslovanja in okrevanje posameznih delov informacijskega sistema. Skozi celoten razvoj sistema hranilnice je varnost postopoma postala eden od najpomembnejših dejavnikov za nadaljnji razvoj informacijskega sistema hranilnice.

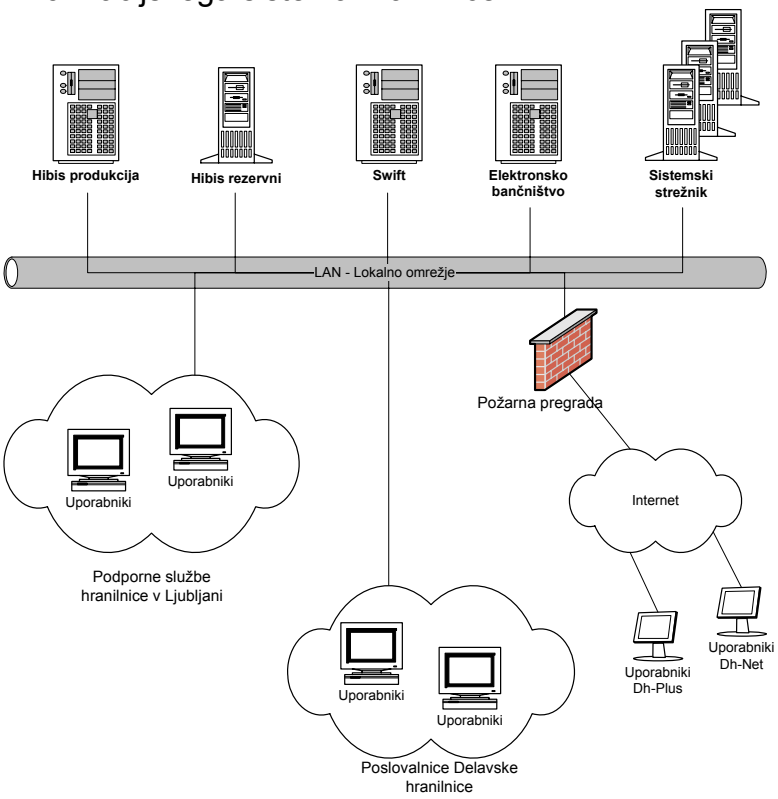
2.2 Informacijski sistem hranilnice

Informacijski sistem hranilnice se nahaja na sedežu hranilnice v Ljubljani in je z oddaljenimi poslovalnicami povezan z zasebnim omrežjem, in sicer z uporabo šifriranih komunikacijskih kanalov. Vsi komunikacijski vhodi in izhodi v hranilnico potekajo po mreži usmerjevalnikov ter po sistemu požarne pregrade in antivirusne zaščite.

Osnovne sistemske gradnike informacijskega sistema tvorijo strežniki prikazani na Sliki 3, ki so nameščeni v gruče in na katerih deluje različna namenska programska oprema. Značilnost strežnikov v hranilnici je, da so poenoteni, večinoma istega proizvajalca, enake arhitekture, uporabljajo samo dve vrsti operacijskih sistemov, kar poenostavlja nadzor in vzdrževanje sistema.

Bančni informacijski sistem tvorijo zmogljivi strežniki, ki povezani v gručo zagotavljajo visoko razpoložljivost in zanesljivost delovanja in na katere je nameščena bančna aplikacija Hibis. To je celovit informacijski sistem za bančno poslovanje v hranilnici, ki ga sestavlja množica programskih modulov za podporo posameznim področjem poslovanja. Uporaba enotnega in celovitega sistema, kot je Hibis, za hranilnico predstavlja veliko prednost, saj je vzdrževanje lažje, nadaljnji razvoj sistema pa bolj pregleden in enostaven.

Slika 3: Shema informacijskega sistema hranilnice



Vir: Interni akti Delavske hranilnice, 2007.

Za elektronsko poslovanje hranilnica svojim komitentom omogoča uporabo spletne banke Dh-Plus za fizične osebe in spletne banke Dh-Net za pravne osebe. Leta 2005 je hranilnica postavila lastno bankomatsko omrežje, ki danes vključuje 8 bankomatov, ki so nameščeni v poslovalnicah hranilnice. Sistemi za podporo omenjenim elektronskim storitvam delujejo v režimu 24/7, kar pomeni, da jih je potrebno vzdrževati predvsem v nočnem času, ko je uporaba sistemov najmanjša. Vse omenjene sisteme hranilnica vzdržuje s svojimi lastnimi kadrovskimi viri v sodelovanju z zunanjimi pogodbenimi izvajalci.

2.3 Smernice razvoja

Zaradi zahtev po prilagajanju sistema evropskim in mednarodnim predpisom in zakonom, zahtev po izboljšanju varnosti poslovanja ter zaradi razvoja novih storitev mora hranilnica informacijski sistem nenehno spreminjati in nadgrajevati. Hranilnica vzdržuje in razvija informacijski sistem skladno s sprejeto strategijo razvoja hranilnice ter strategijo razvoja informacijskega sistema.

Trendi sodobnega bančništva nadaljujejo pohod storitev elektronskega bančništva in približevanja bančnih storitev komitentom ter spodbujajo elektronsko procesiranje in izmenjevanje podatkov med poslovnimi subjekti. Ves razvoj elektronskega bančništva temelji na razvoju informacijskega sistema. Informacijska tehnologija se na področju strojne in programske opreme ter komunikacij še naprej razvija zelo hitro. Hranilnica sledi smernicam razvoja tako, da izvaja posodobitev in združevanje strojne in programske opreme z uporabo navideznih strežnikov ter posledično z zmanjševanjem števila fizičnih strežnikov. Na ta način na eni strani znižuje stroške nakupa in vzdrževanja opreme, na drugi strani pa povečuje možnosti za hitro postavitev novih strežnikov ob novi poslovni potrebi.

Na področju komunikacij je hranilnica izvedla zamenjavo najetih vodov, ki z nizkimi prenosnimi hitrostmi in visokimi stroški niso bili več konkurenčni novo razvijajočim se komunikacijskim tehnologijam po poslovnih internetnih povezavah in optičnih omrežjih. Na ta način je hranilnica povečala prenosne hitrosti omrežja poslovalnic in s tem tudi odzivnost aplikacij in izmenjave podatkov. Pri načrtovanju razvoja hranilnica upošteva varnostne zahteve in priporočila tako, da izboljšuje nadzor informacijskega sistema na vseh kritičnih mestih, dodatno uvaja sisteme notranjih kontrol ter vlaga sredstva v sisteme za zaščito informacijskega sistema in prostorov.

3 STRATEGIJA UPRAVLJANJA Z VARNOSTJO

Varnostna politika hranilnice

Hranilnica ima izdelano varnostno politiko za varovanje informacijskega sistema in podatkov hranilnice, ki jo periodično preverja in nadgrajuje. Varnostna politika se uporablja za zaščito vseh delov informacijskega sistema tako, da predpisuje pravila in postopke za zagotavljanje varnosti. Politika obravnava področje uporabe strojne in programske opreme, varovanje dostopov do opreme in prostorov, pravila za nadgrajevanje in menjavo opreme, postopke za zagotavljanje, preverjanje in hranjenje varnostnih kopij podatkov, metode za zagotavljanje varnosti prenosa podatkov, itd.

V zadnjih letih je hranilnica dograjevala varnostno politiko in prakso z novimi pravili in postopki za dnevni nadzor informacijskega sistema, za poročanje o dogodkih operativnega tveganja, za evidentiranje vseh incidentov. Poleg navedenega hranilnica izvaja redno letno izobraževanje zaposlenih, kjer jih informira in opozarja v

zvezi z uporabo informacijske tehnologije in varnostjo poslovanja. Varnostna politika in postopki za zaščito informacijskega sistema so del rednih pregledov notranje in zunanje revizije.

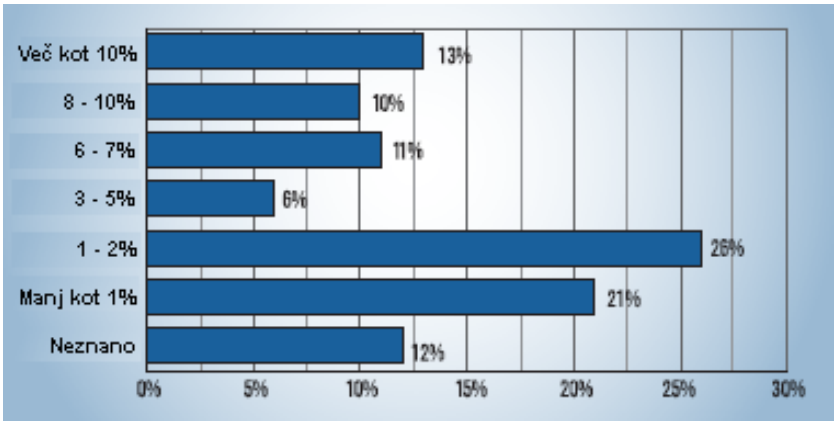
Upoštevani standardi in priporočila

Pri vzdrževanju varnostne politike in zagotavljanju zaščite informacijskega sistema hranilnica upošteva mednarodna standarda na področju varovanja informacij, in sicer ISO/IEC 17799:2005 in ISO/IEC 27001:2006 ter priporočila Banke Slovenije in Združenja bank Slovenije za posamezna področja. Poleg navedenega hranilnica upošteva tudi zbirke najboljših praks v informatiki. Hranilnica si prizadeva, da bi že vzpostavljen sistem za upravljanje z varnostjo uskladila z ISMS (Information Security Management System) sistemom za upravljanje informacijske varnosti, ki je opredeljen v standardu ISO/IEC 27001:2006.

Naložbe v varnost

Hranilnica vlaga sredstva v zaščito informacijskega sistema v skladu z zmožnostmi in s prednostnimi listami, ki si jih je postavila. V zadnjih letih je hranilnica veliko sredstev vlagala v zamenjavo komunikacijske opreme, ki varuje prenos podatkov s šifriranjem komunikacijskih povezav, v posodobitev sistema požarne pregrade in antivirusne zaščite, v uvedbo sistema za uporabo kvalificiranih digitalnih potrdil, v postavitev sistemov za kontrolo pristopa v prostorih hranilnice, itd. Zaradi omejitve s sredstvi hranilnica še ni investirala v sistem za preventivno odkrivanje vdorov in aktivno zaščito omrežja, vendar ima to v kratkoročnem načrtu.

Slika 4: Raziskava o vlaganjih sredstev informatike v informacijsko varnost



Vir: CSI/FBI Computer Security Institute, 2006, str. 5.

Kot je prikazano v raziskavi na Sliki 4, ki jo je opravil Computer Security Institute za leto 2006, se hranilnica uvršča med podjetja, ki za informacijsko varnost v zadnjih dveh letih namenjajo več kot 10 % letnega proračuna informatike.

4 ANALIZA ZAŠČITE INFORMACIJSKEGA SISTEMA

Najpogostejše grožnje za informacijski sistem so (Verdonik, Bratuša, 2005, str. 81):

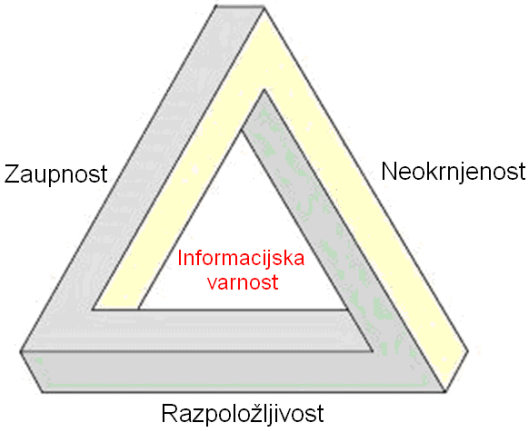
- vdori v informacijski sistem:
  to so nepooblaščeni oddaljeni dostopi (izvlečenje in razbijanje gesel, beleženje tipk, trojanski konji in različni virusi, preusmerjanje vrat, oddaljen nadzor itd), ki lahko povzročijo nepooblaščen dostop do podatkov, spremembo, ali uničenje podatkov;
- napadi na spletni strežnik:
  to so običajno napadi na spletni strežnik proizvajalca Microsoft ali Java, ki izkoriščajo ranljivost njunih sistemov (prekoračitev vmesnikov ob napakah, dostop do datotečnega sistema, povečevanje pooblastil, razkritje izvorne kode, podtaknjene povezave, ničelni bajti ali v zadnjem času zelo pogosto tako imenovani phishing itd.);
- zloraba pooblastil in razpoznavnih sredstev:
  kjer je potrebno zagotoviti, da za dostop pooblaščeni uporabniki v sistemu počno le tisto, za kar so pooblaščeni (npr. vpogled v bančni račun), s tem pa lahko preprečimo zlorabo s strani tretje osebe;
- prestrezanje in potvarjanje sporočil:
  napadalec ne vdre neposredno v sistem, temveč za dostop do podatkov uporabi prenosne poti, kjer z ustrezno strojno in programsko opremo prisluškuje ali spreminja podatke, ki potujejo po napadeni poti;
- onemogočanje storitev:
  tako imenovan DoS (Denial-of-Service), ko napadalec poskuša poslabšati kakovost storitve ali jo povsem onemogočiti (npr. z izjemno povečanim številom zahtev po določeni storitvi v sistemu, ki pod tako obremenitvijo ne deluje več zadovoljivo, ali pa z umetnim ustvarjanjem nepotrebnega omrežnega prometa zmanjša propustnost prenosne poti);
- povzročanje stroškov:
  napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen; to napadenemu povzroča nepotrebne stroške, druge škode običajno nima; ti napadi so danes zelo popularni, saj napadalec pride do informacijskih virov zastonj ali mnogo ceneje kot sicer.

V informacijskem sistemu varujemo podatke in informacijske storitve, ki so običajno glavni cilj napadalcev. Za zaščito podatkov in informacijskih virov je potrebno zagotoviti varnost na različnih stopnjah (Pepelnjak, 1997, str. 158):

- na dostopu, kjer se varujejo informacijski viri in storitve pri vhodu v sistem ali pri izhodu iz njega,
- pri uporabi, kjer se zagotavlja pooblastila uporabniku ter se izvaja nadzor nad aktivnostmi vsakega uporabnika, ki mu je dodeljen dostop,
- pri transakcijah, kjer se varuje celovitost in zaupnost podatkov, ki se izmenjujejo po informacijskih virih.

Kot je prikazano na Sliki 5, je cilj informacijske varnosti zagotoviti zaupnost, neokrnjenost in razpoložljivost podatkov, kar s tujko imenujemo CIA (Confidentiality, Integrity, Availability). Z uporabo omrežij za poslovne namene je potrebno dodatno omogočiti še dokazovanje verodostojnosti pošiljatelja (Authentitaction) ter onemogočiti zanikanje prejema sporočila (Nonrepudiation) (White, 2003, str. 8).

Slika 5: Trije glavni cilji informacijske varnosti



Vir: Securology, 2007.

Zaupnost sporočila in podatkov preprečuje njihovo nepooblaščeno razkritje. Razkritje sporočila, ki potuje po omrežju lahko, povzroči negativne posledice. Edina rešitev je, da tako sporočilo potuje po omrežju v šifrirani obliki z uporabo primerne metode šifriranja.

Neokrnjenost oz. celovitost sporočila preprečuje njegovo nepooblaščeno spremembo. Sporočilo, ki potuje po omrežju, ne sme biti spremenjeno s strani tretje osebe, kar zagotovimo z digitalnim podpisovanjem sporočila.

Cilj razpoložljivosti je zagotovilo, da je sistem na voljo, ko ga uporabniki potrebujejo, kar je mogoče doseči z ustreznim načrtovanjem informacijskega sistema na način, da omogoča visoko zanesljivost delovanja ter hiter prehod na rezervne zmogljivosti.

Verodostojnost prejemniku zagotavlja, da je sporočilo poslal točno določen pošiljatelj in ne morda nekdo drug, ki bi se zanj izdajal, ter, da je sporočilo pristno oz. ni ponarejeno. Overitev pošiljatelja omogoča uporaba digitalnega podpisa, ki ga izdaja ena od pooblaščenih certifikatskih agencij. Pooblaščanje oz. avtorizacija je preverjanje pooblastil uporabnika. Sistem preverja, ali ima uporabnik pravico dostopa do informacij, ki jih zahteva. Onemogočanje zanikanja preprečuje nepriznavanje katerega izmed udeležencev v izmenjavi informacij, da je poslal oz. prejel določeno sporočilo. Onemogočanje zanikanja je izvedeno z digitalnim podpisom. Kontrola dostopa je ukrep za varovanje vsakega sistema v omrežju, ki ustavi vse tiste zahteve, ki dejansko nimajo kaj iskati v varovanem delu omrežja. V sporočilih se preverjajo naslovi pošiljateljev, naslovi prejemnikov, njihova vsebina, dostop je omogočen samo pooblaščenim uporabnikom.

4.1 Obvladovanje fizičnega dostopa

Obvladovanje fizičnega dostopa pomeni ločitev prostorov in opreme informacijske tehnologije, in sicer zaradi varovanja naprav pred nepooblaščenim dostopom in ravnanjem, ki bi lahko povzročilo onemogočenje delovanja ali celo odtujitev opreme. Potrebno je varovati vse komunikacijske naprave (usmerjevalnike, modeme, telekomunikacijske priključke), strežnike in delovne postaje, tiskalnike, sisteme za kontrolo pristopa, sisteme za videonadzor, alarmne sisteme itd. Še posebej je potrebno zaščititi delovna mesta, opremljena z informacijsko opremo, kjer ni stalne prisotnosti zaposlenih ter bi na ta način obiskovalci lahko prišli v stik z delovno postajo ali drugo opremo (npr. prostore za osebno obravnavo).

4.1.1 Kontrola dostopa

Hranilnica varuje fizični dostop do informacijske opreme s sistemov kontrole dostopa in protivlomnih vrat. Večina sistemov v hranilnici je opremljena s čitalci brezkontaktnih kartic, ki se uporabljajo kot sredstvo za dodelitev dostopa. Sistem čitalcev je povezan na strežnik za kontrolo dostopa, kjer se dostopi centralno upravljajo in beležijo. Zaposleni in morebitni obiskovalci za dostop v posamezne prostore uporabljajo čip kartice, ki jim v skladu z vnaprej določenimi pooblastili v sistemu kontrole dostopa omogočajo ali onemogočajo dostop. Prostori s pomembnejšo opremo, kot so računalniške omare in bankomati v poslovalnicah ali računalniški center na sedežu hranilnice, imajo dostop zelo omejen.

4.1.2 Videonadzor

Poleg s sistemi kontrole dostopa hranilnica nadzira dostop do kritične opreme z izvajanjem videonadzora na vseh točkah, kjer so dostopi do računalniške in komunikacijske opreme, bankomatov ali odročnih delovnih mest. Hranilnica izvaja videonadzor v vseh poslovnih prostorih. Nadzor se izvaja v skladu s pravilnikom, ki natančno opredeljuje način izvajanja videonadzora, varstvo osebnih podatkov ter postopke kontrole sistema.

4.1.3 Tehnično varovanje prostorov

Drugi nivo varovanja fizičnega dostopa do vseh prostorov z računalniško opremo se izvaja s sistemi za tehnično varovanje. Hranilnica ima v vseh poslovalnicah vzpostavljene alarmne sisteme s stalno povezavo do pogodbenega izvajalca varovanja. Tehnično varovanje, ki zajema tudi protipožarno varovanje, se izvaja v skladu z načrtom tehničnega varovanja. Hranilnica ne uporablja sistemov za aktivno protipožarno varnost.

4.1.4 Zagotavljanje ustreznih pogojev

Za zaščito računalniške opreme pred nepredvidenimi izpadi električne energije in nenadnimi sunki napetosti iz omrežja hranilnica uporablja naprave za neprekinjeno napajanje, ki zagotavljajo premostitve krajših izpadov električnega toka. Na nekaterih

lokacijah hranilnica dodatno uporablja agregat, ki omogoča premostitev daljših izpadov električnega omrežja. Računalniški center na sedežu hranilnice je opremljen s sistemom za zaznavanje izliva vode in prekoračitve temperature v prostoru, ki omogoča takojšnje alarmiranje ob odstopanjih od normalnih razmer. Dodatno je prostor opremljen s senzorji vibracij, ki zaznavajo morebiten nasilen vdor v prostor.

4.2 Obvladovanje logičnega dostopa

Hiter razvoj internetnega omrežja in širitev elektronskega poslovanja povečujeta tveganje za vdor v informacijski sistem hranilnice. Varovanje logičnih dostopov je zahtevna naloga, saj komunikacijsko omrežje in nekatere aplikacije (spletne banke, internetne strani) hranilnice delujejo v režimu 24/7 (vse ure in vse dni v tednu). Obvladovanje logičnega dostopa pomeni omejitev dostopa zaposlenih, komitentov in poslovnih partnerjev do informacijskih virov hranilnice zaradi preprečitve nepooblaščenega dostopa. Uporablja se kot dodatna zaščita k že obravnavani fizični zaščiti opreme. Hranilnica ima zelo poenoten informacijski sistem, ki omogoča dokaj enostavno upravljanje sistema in kontrolo logičnih dostopov.

4.2.1 Razpoznavanje in overjanje uporabnikov

Razpoznavanje oz. identifikacija uporabnikov je proces, ki se uporablja za razpoznavanje posameznika, ki želi dostopati v določen sistem ali omrežje. Izvaja se z razpoznavnimi sredstvi, kot so uporabniško ime, kartica, digitalno potrdilo itd.

Overjanje oz. avtentikacija uporabnikov je proces, ki se uporablja za preverjanje verodostojnosti posameznika. Z različnimi metodami, kot so uporabniško geslo, biometrični podatki, zasebni ključ itd., se preveri, ali je oseba tista, za katero se predstavlja. Kot je zapisano v standardu ISO/IEC 17799:2005 v točki kontrola A.11.5.2, mora organizacija zagotoviti enolično razpoznavo uporabnikov ter hkrati preprečiti, da so že z uporabniškega imena zaznani privilegiji posameznega uporabnika (npr.: admin, adm, root itd.). Naloga procesa overjanja uporabnika je, da overi pristnost osebe, ki se predstavlja z določenim sredstvom razpoznave (Calder, Watkins, 2006, str. 263).

Razpoznavanje in overjanje se lahko izvaja na tri načine. Ti načini so naslednji sistemi overjanja (White, 2003, str. 18):

- nekaj, kar uporabnik ve (geslo, osebna številka),
- nekaj, kar uporabnik ima (različne kartice, digitalno potrdilo),
- nekaj, kar uporabnik je (biometrični podatki posameznika).

Najpogostejša metoda overjanja uporabnikov je overjanje po sistemu »nekaj, kar uporabnik ve«. V hranilnici je to uporaba uporabniškega imena in gesla. Tovrstna metoda se uporablja za overjanje dostopov do komunikacijskih naprav, strežnikov, delovnih postaj, programov in drugih sistemov. Hranilnica v skladu s sprejeto varnostno politiko za razpoznavo uporabnikov uporablja kompleksna gesla (Politika upravljanja z gesli, 2007).

Za uresničevanje politike gesel v omrežju delovnih postaj in strežnikov se uporabljata domenska strežnika AD (Active Directory), ki sta nastavljena skladno z zgoraj omenjeno varnostno politiko. Razpoznava uporabnikov in preverjanje gesel se v bančni aplikaciji Hibis izvaja po posebnem uporabniškem profilu, ki je nastavljen v podatkovni bazi Oracle. Nadzor nad logičnimi dostopi se izvaja s preverjanjem dnevnikov dostopov in z beleženjem revizijskih sledi. Omenjen način razpoznave in overjanja je enostaven in omogoča ob upoštevanju varnostne politike dobro zaščito.

4.2.2 Razpoznavanje in overjanje oddaljenih dostopov

Pri procesu razpoznavanja in overjanja oddaljenih dostopov oz. dostopov uporabnikov v omrežje hranilnice in iz njega je tveganje nepooblaščenega dostopa zaradi vplivov iz okolice še večja. Pri tovrstnih overjanjih posameznikov hranilnica zaradi zagotavljanja višjega nivoja varnosti uporablja metodo po sistemu »nekaj, kar uporabnik ima«.

Hranilnica za dostop v omrežja poslovnih partnerjev, kot so različni plačilni in medbančni sistemi, uporablja kombinacijo različnih sredstev razpoznave in preverjanja osebnega gesla. Najpogosteje se uporabljajo kartice z magnetno stezo ali čip kartice, ki v kombinaciji z geslom oz. osebno številko omogočajo višji nivo zaščite. Podobno je pri sredstvih razpoznave, ki jih hranilnica izdaja svojim komitentom v obliki plačilnih kartic Maestro in MasterCard za dostop do sredstev na njihovem osebnem ali kartičnem računu. Hranilnica je zaradi vse pogostejših zlorab plačilnih kartic in zmanjšanja tovrstnih tveganj nadgradila vse tipe kartic s čip tehnologijo, v skladu z mednarodnim kartičnim standardom EMV (Eurocard, MasterCard, Visa). Na področju uporabe digitalnih potrdil hranilnica uporablja kvalificirana digitalna potrdila SIGEN-CA (Slovenian General Certification Authority), ki jih izdaja Ministrstvo za javno upravo, ter potrdila POŠTA®CA, ki jih izdaja Certifikatska agencija Pošte Slovenije.

Pri tretjem načinu razpoznave in overjanja po sistemu »nekaj, kar uporabnik je« se uporabljajo biometrične metode, ki izkoriščajo edinstvene fizične ali značajske lastnosti uporabnika, kot so prstni odtis, očesna mrežnica, oblika roke, podpis, glas. Hranilnica teh metod ne uporablja za zaščito logičnega dostopa.

4.3 Zaščita in varovanje komunikacijskih povezav

Področje komunikacij je v zadnjih letih doživelo izjemen razvoj zaradi uvedbe novih žičnih in brezžičnih tehnologij, ki so internetno omrežje razširile v mnoga gospodinjstva in v večino podjetij po celem svetu. Omejitve propustnosti omrežij, ki so jih narekovale tehnološko zastarele klicne oz. modemske povezave, so sedaj presežene z novimi DSL (Digital Subscriber Line) in optičnimi povezavami.

Z razvojem omrežja se na žalost povečujejo tudi možnosti za zlorabo omrežij. Statistike o računalniškem kriminalu in varnosti za leto 2006 (Computer Security

Institute, 2006, str. 13) so pokazale, da so med najpogostejšimi razlogi za finančno škodo podjetij zlorabe omrežja od znotraj (42 %), onemogočanje storitev (25 %), vdor v informacijski sistem (15 %), zloraba brezžičnih omrežij (14 %) itd. Omrežja postajajo še bolj ranljiva z razvojem storitev elektronskega poslovanja, ki povečuje uporabo različnih vstopnih točk in protokolov ob stalno vzpostavljeni povezavi do internetnega omrežja. Vse to zelo otežuje prepoznavanje zlonamernih prenosov in dostopov. Morebitni napadalci z motivom po dokazovanju, škodovanju ali celo okoriščanju preizkušajo zaščito poslovnih omrežij. Oblike možnih zlorab so različne, od vdora v sistem, onemogočanja storitev, kraje ali uničenja podatkov pa vse do kraje denarja z osebnih računov.

4.3.1 Omrežje in povezave

4.3.1.1 Poslovno omrežje hranilnice

Poslovno omrežje hranilnice oz. WAN (Wide Area Networks) omrežje sestavlja navidezno zasebno omrežje z infrastrukturo Telekoma Slovenije, ki za posredovanje poti uporablja MPLS (MultiProtocol Label Switching) protokol. Poslovno omrežje povezuje lokalna omrežja poslovalnic oz. LAN (Local Area Networks) z omrežjem računalniškega centa v Ljubljani. Priklop poslovalnic v navidezno omrežje je izveden z digitalnimi naročniškimi ali optičnimi povezavami, odvisno od potreb posamezne poslovalnice. Asimetrične povezave ADSL (Asymmetric Digital Subscriber Line) in VDSL (very-high-bit-rate DSL) dosegajo različne hitrosti prenosa podatkov v obe smeri. Te se običajno gibljejo od 1 do 10 Mbit/s za prenos k poslovalnici ter od 256 kb/s do 4 Mb/s za hitrosti prenosa od poslovalnic do računalniškega centra. Optične povezave dosegajo očitno višje hitrosti prenosov, ki so v obe strani enake, zato se hranilnica pri večjih poslovalnicah odloča za vzpostavitev le-teh.

Hranilnica ima v vsaki izmed poslovalnic nameščen usmerjevalnik proizvajalca Cisco, ki lahko povezuje različne tipe povezav v eno komunikacijsko točko. Zaradi izpostavljenosti zgoraj omenjenih povezav, ki deloma potekajo tudi po poslovnem internetnem omrežju, hranilnica za zagotovitev celovitosti in zaupnosti prenosa podatkov na vseh usmerjevalnikih uporablja šifriranje prenosa z uporabo 3DES (Triple Data Encryption Standard) algoritma. Vse oddaljene povezave poslovalnic dostopajo v omrežje računalniškega centra hranilnice po sistemu požarne pregrade in antivirusne zaščite, kjer se v skladu s sprejeto politiko upravljajo dostopi do informacijskih virov. Za vzdrževanje usmerjevalnikov in mrežnih stikal skrbi zunanji pogodbeni izvajalec, ki izvaja nadgraditve operacijskih sistemov, nastavitve parametrov in vzdrževanje naprav. Nastavitve usmerjevalnikov se periodično shranjujejo na poseben strežnik, kjer so na voljo vzdrževalcem sistema za morebitno hitro zamenjavo okvarjenega usmerjevalnika na terenu. Informatika v hranilnici z upravljanjem požarne pregrade skrbi, da je dostop zunanjih izvajalcev do usmerjevalnikov hranilnice omogočen samo ob intervencijah in planiranih posegih. Hranilnica se zaveda tveganj, ki jih prinaša zunanje izvajanje (outsourcing) na področju vzdrževanja komunikacijskih naprav in kritičnih sistemov. Hkrati z večanjem števila zaposlenih v hranilnici se povečuje tudi služba informatike, ki tako počasi prevzema vse večji obseg del iz rok zunanjih izvajalcev.

4.3.1.2 Partnerske povezave

Hranilnica ima vzpostavljene tako imenovane partnerske povezave, ki hranilnico vključujejo v omrežja plačilnih sistemov in procesnega centra. Vse omenjene povezave so priključene v informacijski sistem hranilnice s posebnim področjem na požarni pregradi. Na ta način hranilnica z nastavljenimi varnostnimi politikami upravlja in nadzira dostope v informacijski sistem in iz njega.

Hranilnica ima na področju partnerskih povezav vzpostavljeno komunikacijsko povezavo z omrežjem Banke Slovenije, omrežjem plačilnega sistema Swift ter omrežjem procesnega centra Bankart. Vse omenjene povezave so ključne za normalno delovanje sistema hranilnice, zato ima večina povezav zagotovljeno rezervno povezavo s klicno ISDN (Integrated Services over Digital Network) povezavo, ki se samodejno vzpostavi ob prekinitvi primarne povezave. Rezervne povezave za Bankart ni. Varnost na tovrstnih povezavah se zagotavlja s simetričnim šifriranjem prenosa podatkov z uporabo 3DES algoritma, z nadziranjem dostopov na požarni pregradi ter z antivirusno zaščito sistemov.

4.3.1.3 Internetne povezave

Hranilnica ima vzpostavljeno povezavo v internetno omrežje, ki zagotavlja hitro komunikacijo s svetovnim spletom. Povezava je izvedena po optičnem omrežju enega od ponudnikov, ki poteka po posebnem področju DMZ (Demilitarized Zone) na požarni pregradi. Vsa komunikacija prehaja po sistemu požarne in antivirusne zaščite v omrežje hranilnice v skladu z nastavitvami na pregradi.

Internetna povezava je zelo pomembna, saj na eni strani zagotavlja dostop komitentov, poslovnih partnerjev in obiskovalcev do spletnih bank, spletne strani in do drugih storitev, na drugi strani pa omogoča elektronsko izmenjavo in dostop zaposlenih v hranilnici do zunanjega sveta. Varnost povezave se zagotavlja z nastavitvami na usmerjevalniku, požarni pregradi ter antivirusni zaščiti. Dostopi so omejeni na način, da je onemogočen vsakršen promet, ki ni posebej odobren na požarni pregradi. Za zagotavljanje dostopa in kot mehanizem proti onemogočanju dostopa do posameznih virov in storitev se uporablja sistem nastavljenih uteži, ki določa prednostno listo dostopov (npr. dostopi do spletne banke imajo prednost pred dostopi zaposlenih v internetno omrežje). Uporaba samo enega ponudnika za povezavo v internetno omrežje predstavlja pomanjkljivost in tveganje ob morebitnem izpadu sistema ponudnika.

4.3.1.4 Navidezne zasebne povezave

Hranilnica ima z nekaterimi zunanjimi izvajalci vzpostavljene navidezne zasebne tako imenovane VPN (Virtual Privat Network) povezave, ki omogočajo oddaljen dostop za vzdrževanje kritičnih delov informacijskega sistema. Predvsem se tovrstne povezave uporabljajo za dostop razvijalcev bančne aplikacije Hibis do testnega okolja hranilnice, na katerem se izvaja testiranje popravkov in nadgradenj.

Navidezna zasebna povezava je izvedena s programsko opremo proizvajalca požarne pregrade, ki omogoča razpoznavanje in overjanje uporabnika ter vzpostavitev šifriranega komunikacijskega kanala s pomočjo digitalnega potrdila in gesla, ki ga ustvari skrbnik na požarni pregradi. Povezava se po internetnem omrežju vzpostavi med delovno postajo oddaljenega uporabnika in požarno pregrado hranilnice. Program omogoča skrbniku požarne pregrade, da določa politiko dostopa za dodatno varnost dostopa (tip dostopa, urnik dostopa, veljavnost potrdila itd.). Vzpostavitev tovrstne povezave je mogoča samo na podlagi zahteve za dostop, ki jo odobri pooblaščena oseba v hranilnici. Vse dostope upravlja in nadzira služba informatike v sistemu požarne pregrade in antivirusne zaščite. Dostopi do produkcijskega okolja hranilnice so onemogočeni in se lahko vzpostavijo po uradnem postopku odobritve samo v izrednih primerih.

4.3.1.5 Bankomatsko omrežje

Hranilnica je v letu 2005 vzpostavila lastno bankomatsko omrežje, ki danes povezuje mrežo 8 bankomatov po vsej Sloveniji. To poteka po omrežju poslovalnic do že vzpostavljene partnerske povezave s procesnim centrom Bankart. Za ta namen je hranilnica z zunanjim izvajalcem nadgradila usmerjevalnike v poslovalnicah, kjer so nameščeni bankomati, in usmerjevalnika na povezavi do procesnega centra Bankart, ki upravlja bankomatsko omrežje v Sloveniji. Bankomati komunicirajo s strežnikom v centru Bankart. Za varnost povezave se uporablja 3DES šifriranje podatkov od usmerjevalnika v poslovalnici do usmerjevalnika v centru Bankart. Nekateri kritični deli bankomatskih transakcij, kot je osebna številka oz. PIN (Personal Identification Number), se dodatno šifrirajo z naključno ustvarjenim ključem, ki ga hkrati v dveh ločenih parih vneseta pooblaščena predstavnika Bankarta in hranilnice.

4.3.1.6 Brezžična omrežja

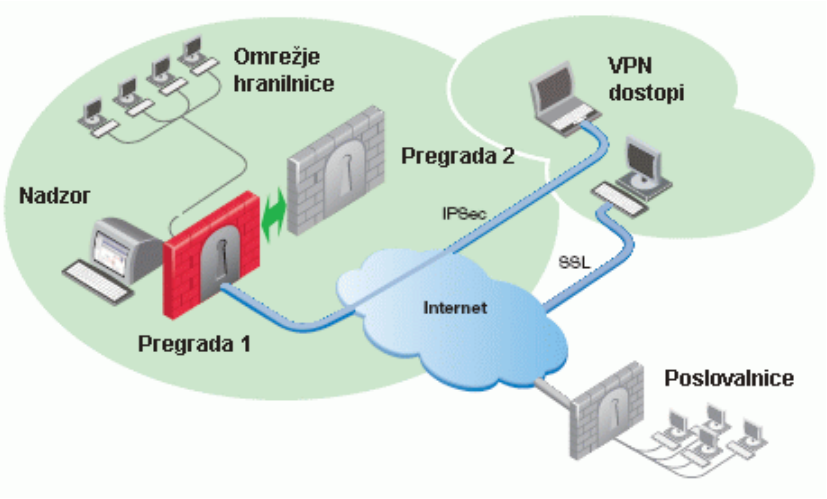
Hranilnica se je v varnostni politiki opredelila, da zaradi zagotavljanja varnosti informacijskega sistema brezžičnih omrežij zaenkrat ne bo uporabljala. Tovrstnih povezav hranilnica nima.

4.3.2 Sistem požarne pregrade

Sistem požarne pregrade v hranilnici je eden od najpomembnejših mehanizmov za zagotavljanje varnosti omrežnih povezav in dostopov. Hranilnica uporablja programsko opremo priznanega proizvajalca, ki je značilna za bančno okolje. Sistem je nameščen na strežnikih, na katerih teče poseben operacijski sistem, ki je zaradi manjše ranljivosti zelo omejen in prilagojen samo za delo požarne pregrade. Omogoča zmogljivo filtriranje paketov, preverjanje prometa tako na transportnem kot na aplikacijskem nivoju ter vzpostavljanje navideznih zasebnih povezav. Požarna pregrada v hranilnici je nastavljena v skladu z varnostno politiko po načelu, da je prepovedano vse, kar ni izrecno dovoljeno. Omenjena politika otežuje delo skrbnikom pregrade, saj zahteva vnos vsakega odobrenega dostopa oz. pravila, vendar pa na ta način zagotavlja višji nivo varnosti dostopov.

Požarna pregrada varuje hranilnico pred neželenimi dostopi v informacijski sistem ter iz njega. Različne povezave se povezujejo z različnimi področji na pregradi kot so internetni dostopi, partnerske povezave, omrežje poslovalnic in omrežje računalniškega centra. Naloga pregrade je, da preverja pooblastila omrežij, skupin in uporabnikov in jim na podlagi imen, mrežnih naslovov, storitev, vhodov in drugih tehničnih podatkov odobrava oz. zavrača dostop. Sistem požarne pregrade ima vmesno povezavo z ločenim sistemom za antivirusno zaščito, po katerem se posreduje ves promet in na ta način omogoča takojšnjo zaustavitev prometa, ki vsebuje viruse, črve, trojanske konje ali drugo morebitno nevarno vsebino.

Slika 6: Shema povezav požarne pregrade



Vir: Centech, 2005.

Za zagotavljanje neprekinjenosti poslovanja hranilnica uporablja dve požarni pregradi z vzpostavljenim sistemom prenosa nastavitev. Poleg navedenega se izvaja varovanje podatkov po določeni varnostni politiki. Hranilnica s pomočjo nadzorne postaje in vnaprej nastavljenih poizvedb izvaja stalni nadzor prometa po požarni pregradi. Shemo povezav požarne pregrade prikazuje Slika 6.

4.3.3 Šifriranje sporočil

Šifriranje sporočil ali kriptiranje je pretvorba sporočila v tako obliko, da ga nepooblaščene osebe praviloma ne morejo razumeti. Kriptografija ali skrivnopisje (grško kryptós – skrit, gráphein - pisati) je znanstvena veda o tajnosti, šifriranju, zakrivanju sporočil in o razkrivanju šifriranih podatkov. Izvaja se z uporabo zapletenih šifrirnih algoritmov, ki uporabljajo šifrirni ključ in veliko procesno moč računalnikov, da pretvorijo podatke iz nezaščitene v neprepoznavno oz. šifrirano obliko. Kadar se podatke pretvarja v obratni smeri, iz šifrirane oz. kriptirane oblike v nezaščiteno obliko, govorimo o dešifriranju oz. dekriptiranju.

Poznamo dve obliki modernega šifriranja: simetrično in asimetrično šifriranje. Pri simetričnem šifriranju obe strani uporabljata isti skrivni ključ za šifriranje in dešifriranje sporočil. Asimetrično šifriranje je varnejše, saj obe strani za šifriranje in dešifriranje uporabljata javni in zasebni ključ (Egan, Mather, 2005, str. 41).

4.3.3.1 Simetrično šifriranje

Hranilnica za zaščito celotnega poslovnega in bankomatskega omrežja ter partnerskih povezav med različnimi usmerjevalniki in požarno pregrado uporablja simetrično šifriranje z uporabo 3DES algoritma. Včasih uporabljeni algoritem DES (Data Encryption Standard) z uporabo 56-bitnega ključa danes ne zagotavlja več zadostne varnosti, ker lahko zmogljiv strežnik tak ključ ugotovi relativno hitro. Zaradi tega ga je zamenjal algoritem 3DES, kjer se podatki večkrat šifrirajo ali dešifrirajo z dvema ali s tremi različnimi ključi. Ta način šifriranja je še vedno relativno hiter in omogoča normalne hitrosti izmenjave podatkov. Njegova slabost je v tem, da ključe pri partnerski povezavi največkrat poznata oba partnerja in je tako težje zagotoviti varnost ključa (White, 2003, str. 289).

Hranilnica se zgoraj omenjenemu tveganju izogiba na način, da ena od strani zagotovi povezavo in usmerjevalnika na obeh straneh ter tako omogoči bolj varen dostop. Tak primer je tudi povezava do procesnega centra Bankart, kjer hranilnica upravlja ključe usmerjevalnika na svoji strani in usmerjevalnika, ki je nameščen v Bankartu. Vseeno se postavlja vprašanje, kako dolgo bo algoritem 3DES zadoščal za varno kriptiranje podatkov. Kot naslednik se vse pogosteje pojavlja algoritem AES (Advanced Encryption Standard), ki je zaradi šifriranja 128 bitov dolgih blokov hitrejši ter zaradi uporabe daljših ključev (128, 192, 256-bitnih) tudi bolj varen.

4.3.3.2 Asimetrično šifriranje

Pri navideznih zasebnih povezavah, ki so namenjene dostopu zunanjih izvajalcev, hranilnica uporablja asimetrično šifriranje z algoritmom RSA (Rivers, Shamir, Adleman), kar predstavlja začetnice priimkov študentov s fakultete MIT, ki so algoritem iznašli. RSA je prvi algoritem, ki uporablja infrastrukturo javnih ključev, znano kot PKI (Public Key Infrastructure). Lahko se uporablja za šifriranje ali digitalno podpisovanje. Algoritem uporablja zasebni in javni ključ, ki sta matematično povezana. Zasebnega oz. privatnega ključa ne moremo izračunati s pomočjo javnega ključa. Algoritem uporablja zmnožek dveh velikih praštevil, medtem ko je obratni postopek, to je ugotavljanje obeh števil iz zmnožka, zelo zahteven. Zasebni ključ mora biti strogo varovan, javni ključ pa je lahko objavljen in dostopen javnosti (White, 2003, str. 297). Pošiljatelj, ki želi sporočilo posredovati prejemniku, mora poznati njegov javni ključ s katerim sporočilo šifrira. Sporočilo lahko dešifrira samo prejemnik s svojim zasebnim ključem. Ker je algoritem RSA zelo zahteven, je šifriranje dolgih sporočil temu primerno počasno. Uporaba šifriranja v tem primeru zagotavlja zaupnost podatkov. Algoritem RSA najdemo tako v mnogih programskih paketih kot tudi v operacijskih sistemih ter varnostnih protokolih.

4.3.3.3 Kombinirano šifriranje

Danes se vedno pogosteje uporablja tako imenovano kombinirano šifriranje, ki združuje prednosti simetričnega in asimetričnega sistema. Pri tem postopku šifriramo dokumente po klasičnem simetričnem postopku, za varno izmenjavo simetričnega

ključa pa uporabimo asimetrično šifriranje. Naključno izbrani simetrični ključ tako asimetrično šifriramo z javnim ključem prejemnika ter ga posredujemo skupaj s šifriranim dokumentom. Prejemnik s svojim zasebnim ključem dešifrira simetrični ključ ter z njim dešifrira celoten dokument. Na ta način se izkoristi prednosti asimetričnega postopka in hitrost simetričnega šifriranja.

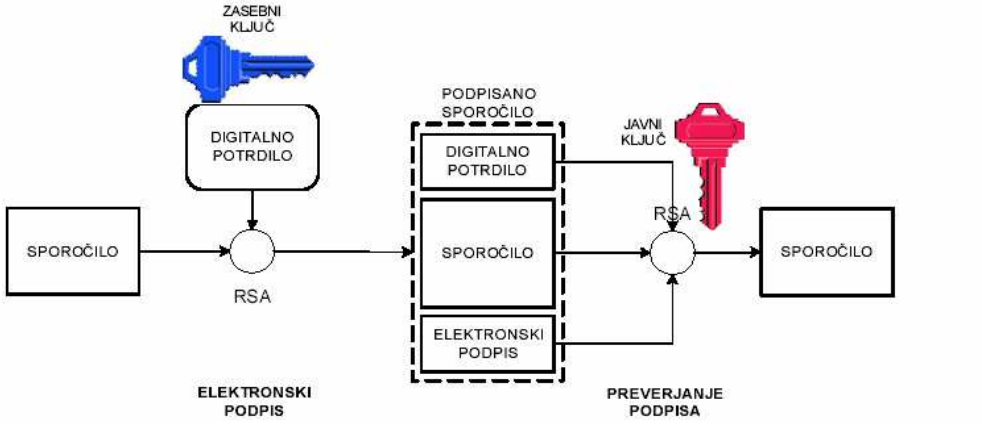
4.3.4 Uporaba elektronskega podpisa in digitalnega potrdila

Samo šifriranje varuje zaupnost sporočila, vendar ne zagotavlja onemogočanja zanikanja, ugotavljanja neokrnjenosti sporočila in overitve pošiljatelja. Uporaba elektronskega podpisa, ki nadomešča lastnoročni podpis, zagotavlja tako pristnost sporočila oz. podatkov kot tudi overitev podpisnika. Obstaja več oblik elektronskega podpisovanja, od enostavnih metod z uporabo simetričnih algoritmov, ki ne zagotavljajo visoke stopnje varnosti, pa vse do uporabe asimetričnih algoritmov. Elektronski podpis, ki je dobljen z elektronsko tehnologijo, za razliko od digitalnega podpisa, ki ga dobimo z asimetričnim šifrirnim postopkom, ne omogoča neokrnjenosti podpisanega dokumenta in overitve podpisnika (Toplišek, 1998, str. 30).

Državni zbor Republike Slovenije je 22. 8. 2000 sprejel Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP - Uradni list RS, št. 57/2000) in Uredbo za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 ter št. 2/2001). Zakon ureja elektronsko poslovanje in uporabo podatkov v elektronski obliki ter uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje. S sprejetjem tega zakona je bilo vzpostavljeno varno okolje za preverjanje pristnosti elektronsko oblikovanih, shranjenih, poslanih, sprejetih ali kako drugače obdelanih podatkov.

Hranilnica uporablja elektronsko podpisovanje sporočil pri poslovanju z Banko Slovenije s programsko opremo PGP (Pretty Good Privacy). Podpisovanje sporočila poteka z uporabo asimetričnega algoritma RSA, kot prikazuje Slika 7.

Slika 7: Poenostavljen prikaz izvedbe elektronskega podpisa



Vir: Crea, 2003.

V prvi fazi se s pomočjo zgoščevalne funkcije celotno sporočilo preslika v blok podatkov konstantne dolžine, imenovan tudi prstni odtis. Vsakršna sprememba sporočila povzroči spremembo bloka. Blok se v drugi fazi šifrira z zasebnim ključem. Tako dobimo digitalni oz. elektronski podpis. Prejemnik sporočila z javnim ključem pošiljatelja dešifrira podpis in dobi povzetek. Ponovno izračuna povzetek sporočila, ki je bilo poslano v nešifrirani obliki, z isto zgoščevalno funkcijo kot pošiljatelj. Enakost obeh dokazuje neokrnjenost in verodostojnost sporočila oz. podpisa (Jerman Blažič, 2001, str. 108).

Digitalno potrdilo je elektronski dokument, lahko bi rekli tudi nekakšna elektronska osebna izkaznica, ki potrjuje povezavo med javnim ključem in fizično osebo (lahko tudi pravno osebo ali celo strežnikom). Z njim lahko preverimo, komu pripada javni ključ, oz. imetnik lahko z njim, dokaže lastništvo ključa in s tem tudi svojo identiteto. Potrdilo vsebuje javni ključ imetnika in informacijo o imetniku, ki ju izda zaupanja vredna ustanova.

Overjanje javnih ključev je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetrični kriptografiji. Za overjanje skrbijo tako imenovani overitelji oz. certifikatske agencije - CA (Certificate Authority). Digitalna potrdila, izdana s strani CA, imenujemo kvalificirana potrdila in se razlikujejo od drugih potrdil, ki jih izdajajo za to nepooblaščene organizacije in nepooblaščena podjetja. Delavska hranilnica omogoča uporabnikom, da za poslovanje s spletnima bankama uporabljajo kvalificirana digitalna potrdila POŠTA®CA ali SIGEN-CA.

4.3.5 Nadzor omrežja

Hranilnica nadzoruje dogajanje v omrežju za ugotavljanje razpoložljivosti kritičnih omrežnih naprav in za zgodnje odkrivanje izpadov sistema, predvsem pa za preverjanje vstopov in izstopov v informacijski sistem. Za zaščito dostopov hranilnica uporablja programsko opremo, ki dopolnjuje program požarne pregrade in omogoča nadzor, poizvedbe ter alarmiranje vnaprej nastavljenih dogodkov. Hranilnica po sprejeti varnostni politiki izvaja formalni dnevni nadzor vseh dnevnikov dostopov.

4.3.6 Aktivno odkrivanje in preprečevanje vdorov

Hranilnica je v zadnjih dveh letih vlagala sredstva v prenovo in posodobitev komunikacijskih omrežij ter programske in strojne opreme za zagotavljanje varnosti. Za odkrivanje vdorov hranilnica uporablja dodatne programske module na požarni pregradi, vendar je ta zaščita pasivna, saj ne omogoča samodejnega preprečevanja sumljivih in kritičnih dogodkov. Za zaščito omrežnih virov hranilnica nima vzpostavljenega sistema aktivne opreme, kar predstavlja pomanjkljivost pri zaščiti omrežja. Hranilnica bi morala vzpostaviti sistem za aktivno zaščito - IPS (Intrusion Prevention System), ki bo sposoben na podlagi zbranih podatkov samostojno zaustaviti tovrstne dostope.

4.4 Zaščita strojne opreme

Pravilna izbira in uporaba posameznih delov informacijskega sistema lahko ne le izboljša njegovo odzivnost delovanja, ampak lahko tudi poveča njegovo varnost. Infrastrukturno opremo sestavlja aktivna in pasivna komunikacijska oprema, strojna oprema strežnikov in delovnih postaj. Pogosto se dogaja, da se pri načrtovanju sistemov zelo upošteva doseganje razpoložljivosti sistema, manj pa varnosti sistema. Tako obnašanje lahko ob neželenih dogodkih, kot so vdori v sistem, onemogočanje storitev, zlorabe pooblastil itd., povratno vpliva na zmanjšanje visoke razpoložljivosti. Primarni cilj zaščite infrastrukturne opreme je, da dovoljuje vso pooblaščeno uporabo ter hkrati preprečuje vso nepooblaščeno uporabo (White, 2003, str. 155).

4.4.1 Računalniška oprema

Računalniške naprave v hranilnici sestavljajo delovne postaje, prenosni računalniki, strežniki, mrežni tiskalniki in druga oprema. Vsaka od naprav je postavljena s točno določenim namenom, da izpolnjuje zahteve uporabnika ali skupine uporabnikov. Naprave v hranilnici so prilagojene in omejene glede na zahteve delovnega mesta uporabnika. Uporabnikom je omogočeno, da delajo samo tisto, za kar so pooblaščeni. Uporabo računalniških naprav v hranilnici opredeljuje Pravilnik o zaščiti informacijskega sistema in podatkov.

4.4.1.1 Delovne postaje

Hranilnica opremlja delovna mesta zaposlenih z delovnimi postajami proizvajalca Fujitsu-Siemens z modeli višjega kakovostnega razreda, ki so mednarodno uveljavljeni in ustrezajo evropskim standardom (Esprimo, 2006, str. 2). Hranilnica trenutno upravlja 120 delovnih postaj, ki so večinoma pripravljene za blagajniško poslovanje ali za poslovanje posameznih podpornih služb v hranilnici. Vsako delovno postajo se namešča za vnaprej določen tip delovnega mesta po navodilu, ki natanko opredeljuje postopek nameščanja dovoljene programske opreme. Za posamezen tip delovnega mesta se lahko uporabi tudi že vnaprej pripravljena tipska namestitev postaje.

Pred predajo v produkcijsko okolje se vsako delovno postajo in programsko opremo na njej testira in ustrezno preveri. Če se zamenja že delujočo postajo, se pripravi načrt preklopa na novo. Po zamenjavi stare se vse podatke in programe na stari postaji izbriše z orodjem, ki podatke uniči na način, da morebiten kasnejši povratek ni možen.

Za zaščito delovnih postaj hranilnica v skladu z varnostno politiko:

- onemogoča zagon s pomočjo diskete ali diska,
- omejuje dostop do podatkov, dovoljuje samo uporabnikom,
- uporabi samodejno zaklepanje ekrana po 5 minutah z geslom,
- uporablja beleženje dogodkov na postaji in izvaja centralno preverjanje dnevnika dogodkov,

- uporablja sistem antivirusne zaščite ter samodejnega tedenska preverjanja vseh datotek na računalniku,
- glede na potrebe delovnega mesta nastavlja dostope do postaje in iz nje po požarni pregradi,
- določa varnostne zahteve in pravila (gesla, dostopi itd.) delovnih postaj z vnaprej določenimi pravili v domeni.

Na delovnih postajah, ki so izjemnega pomena (kot je na primer delovna postaja v plačilnem prometu), hranilnica dodatno zagotovi:

- varnost hrambe podatkov (šifriranje, varovanje podatkov, arhiviranje),
- nadomestno opremo in načrt za okrevanje,
- priklop na sistem za neprekinjeno napajanje.

Gledano z varnostnega vidika je postavitev, nastavitev in uporaba delovnih postaj eden od zelo pomembnih elementov za zaščito informacijskega sistema. V poslovalnicah se na nekaterih izpostavljenih področjih, kot so prostori za posebne obravnave strank, lahko obiskovalci kljub fizični zaščiti približajo delovni postaji, kar povečuje tveganje za zlorabo. Prav tako predstavlja tveganje uporaba prenosnih medijev, kot so diskete, diski in v zadnjem času zelo priljubljene USB naprave. Za ozaveščanje zaposlenih o pretečih nevarnostih uporabe informacijske opreme hranilnica vsako leto izvaja izobraževanje uporabnikov.

4.4.1.2 Prenosni računalniki

Prenosni računalniki spadajo v posebni razred delovnih postaj, ki zaradi svoje prenosljivosti še povečujejo tveganje za zlorabo informacijskega sistema in podatkov. Tudi v Sloveniji se dogaja, da nepridipravi ukradejo prenosni računalnik katerega od zaposlenih iz vodstva podjetja in na ta način pridejo do pogodb in drugih pomembnih podatkov podjetja. Zavedajoč se višje stopnje izpostavljenosti prenosnih naprav, hranilnica omejuje uporabo prenosnih računalnikov na majhen krog zaposlenih, ki prenosnik dejansko potrebujejo zaradi narave svojega dela (sestanki, predstavitve, potrebe informatike itd.).

Za zaščito prenosnih računalnikov hranilnica uporablja poseben profil nastavitev uporabnikov v domeni, ki določa obnašanje naprav takrat, ko le-te niso priključene v domače omrežje (npr. osveževanje antivirusne zaščite se ne izvaja več centralno, ampak po internetnem omrežju, ob izklopu se samodejno vklopi požarna pregrada operacijskega sistema itd.). Najtežja naloga zaščite prenosnikov je varovanje podatkov na njih. Hranilnica za ta namen uporablja različne šifrirne metode, ki zagotavljajo višjo raven hrambe podatkov, ne morejo pa preprečiti dostopa do podatkov takrat, ko ima nepridiprav na voljo veliko procesorsko moč, znanje iz kriptografije ter čas. Za izognitev tovrstnim tveganjem hranilnica kritične aplikacije namešča na običajne delovne postaje, podatke na prenosnikih pa praviloma shranjuje na diskovno polje SAN (Storage Area Network) in ne lokalno na prenosnik.

4.4.1.3 Dlančniki in mobilni telefoni

Hranilnica v skladu z varnostno politiko ne uporablja dlančnikov in mobilnih telefonov za dostop do informacijskega sistema.

4.4.1.4 Strežniki

Strežniki so računalniške naprave v omrežju, ki so namenjene izvajanju aplikacij in shranjevanju podatkov. Hranilnica uporablja zelo poenoteno arhitekturo strežnikov, in sicer proizvajalca HP (Hewlett Packard), ki z dolgoletnimi izkušnjami zagotavlja kakovostno strojno opremo in zanesljivo delovanje (podvojena vsa kritična oprema, zanesljiva in hitro dostopna diskovna polja, kakovostni pomnilniki, dober nadzor in diagnostika naprav, zagotovljena podpora v režimu 24/7 itd.). Hranilnica kupuje strežnike namensko v skladu s planom investicij za točno določeno potrebo oz. projekt. Zaradi preglednosti in lažjega vzdrževanja hranilnica omejuje izbor operacijskih sistemov za strežnike na sisteme Linux in Windows. Za doseganje visoke razpoložljivosti sistemov s kritičnimi procesi se hranilnica odloča za nameščanje strežnikov v gruče. Za manj kritične, vitalne procese uporablja sistem navideznih oz. virtualnih strežnikov (tehnologija Vmware), da bo tako postopno zmanjšala število fizičnih strežnikov in povečala prilagodljivost ter zanesljivost sistema. Vse namestitve so načrtovane in predhodno testirane, kar omogoča varen in kontroliran preklop strežnikov v produkcijsko okolje.

Za zaščito strežnikov hranilnica v skladu z varnostno politiko:

- nadzira fizičen dostop do strežnikov,
- nadzira delovanje in odzivnost strežnikov,
- skrbi za zaščito posameznih elementov (področja, datoteke, objekti),
- uporablja beleženje dogodkov in dostopov,
- uporablja sisteme antivirusne zaščite,
- določa varnostne zahteve in pravila v skladu s sprejeto varnostno politiko,
- skrbi za varnost hrambe podatkov (šifriranje, varovanje in arhiviranje podatkov, hranjenje varnostnih kopij na varni lokaciji),
- upravlja dostope do strežnika in iz njega po požarni pregradi,
- opravlja periodične preventivne preglede za zgodnje odkrivanje napak,
- skrbi za pogodbeno vzdrževanje opreme in njeno hitro zamenjavo ob okvari,
- načrtuje okrevanje ob katastrofi.

Gledano z varnostnega vidika je najtežji del zagotavljanja varnosti na strežnikih pooblaščanje in nadziranje dostopov iz omrežja.

4.4.1.5 Mrežni tiskalniki

Hranilnica uporablja mrežne tiskalnike v zaokroženih skupinah uporabnikov. Dostop do omrežnih naprav je omejen s pooblastili uporabnika v domeni. Gledano s stališča varnosti in tako imenovane »politike čiste mize« so mrežni tiskalniki nevarni, kadar se dokumenti z občutljivo vsebino znajdejo na območju, ki je dostopen tudi

nepooblaščenim uporabnikom. Hranilnica v skladu z varnostno politiko določa in nadzoruje, da se mrežni tiskalniki uporabljajo samo na območjih, ki so fizično ločena od nepooblaščenih uporabnikov.

4.4.2 Komunikacijska oprema

Mrežne naprave v hranilnici sestavlja pasivna oprema (fizično ožičenje, parapetski kanali, razdelilni paneli) in aktivna mrežna oprema (mrežna stikala, usmerjevalniki, požarne pregrade).

4.4.2.1 Fizično omrežje

Za zagotavljanje varnosti fizičnih omrežij hranilnica namešča računalniška ožičenja v montažne in parapetske kanale, vso ostalo pasivno opremo pa v komunikacijske omare, ki so zaklenjene. Na ta način preprečuje nepooblaščene posege na ožičenju in stikalni opremi. Pri priklapljanju uporabniških naprav na parapetske priključke v poslovnih prostorih hranilnica sproti in samo po potrebi vključuje posamezne mrežne priključke ter tako onemogoča dostop do mreže na še neuporabljenih priključkih.

4.4.2.2 Mrežna stikala

Hranilnica na kritičnih delih omrežja uporablja zmogljiva mrežna stikala, ki so sposobna delovati na omrežnem (tretjem) nivoju OSI (Open Systems Interconnection) modela. Na ta način hranilnica na nekaterih mrežnih stikalih s kontrolo paketov preverja listo dovoljenih dostopov ACL (Access Control Lists) in posledično odobrava ali zavrača posamezne komunikacijske pakete. Dodaten element zagotavljanja varnosti na mrežnih stikalih je oblikovanje navideznih lokalnih omrežij VLAN (Virtual Local Area Networks), ki omogočajo razmejitev omrežnega prometa v več navideznih med seboj ločenih omrežij oz. področij. Hranilnica za zagotavljanje varnosti še neuporabljene mrežne priključke povezuje v neaktivno navidezno omrežje, ki tako nimajo dostopa do drugih omrežij.

Največjo skrb glede varnosti mrežnih stikal predstavlja dejstvo, da so to aktivne in pametne naprave, ki so kot take zelo pogoste tarče poskusa vdora s strani nepridipravov. Z morebitnim vdorom v napravo lahko nepooblaščene osebe spremenijo nastavitve, onemogočijo dostope uporabnikov ali prisluškujejo omrežnemu prometu. Mrežna stikala za upravljanje uporabljajo SNMP (Simple Network Management Protocol) protokol, ki ima resno varnostno pomanjkljivost, saj se geslo po omrežju prenaša v nezaščiteni obliki. Podoben problem predstavlja dobava novih stikal, ki omogočajo prvi dostop s splošno znanim geslom proizvajalca (Bratuša, 2006, str. 26).

Hranilnica varuje mrežna stikala tako, da skrbi za varnost gesel, onemogoča vse protokole, ki jih ne potrebuje, ter za dostop uporablja varnejši komunikacijski protokol SSH (Secure Shell), ki šifrira promet med napravo in odjemalcem.

4.4.2.3 Usmerjevalniki

Usmerjevalniki so naprave, ki usmerjajo promet med različnimi omrežji in tako povezujejo različna omrežja skupaj. Delujejo na omrežnem nivoju OSI modela. Preverjajo vsak paket in naslov prejemnika ter z uporabo usmerjevalnih tabel in algoritmov določajo pot za posredovanje paketa. Usmerjanje se izvaja na podlagi mrežnih naslovov.

Hranilnica na vseh delih svojega omrežja uporablja zanesljive usmerjevalnike proizvajalca Cisco. Za usmerjanje prometa uporablja BGP (Border Gateway Protocol) protokol. Na kritičnih usmerjevalnikih za zagotavljanje višjega nivoja varnosti preverja listo dovoljenih dostopov. Podobno kot pri mrežnih stikalih hranilnica zagotavlja, da je vsa aktivna mrežna oprema nameščena v varovanih komunikacijskih omarah, ki varujejo naprave pred nepooblaščenimi posegi iz okolice. Za zagotavljanje varnosti oddaljenih dostopov do usmerjevalnikov hranilnica onemogoča prijave z uporabniškimi imeni in gesli, ki jih je nastavil proizvajalec. Dodatno hranilnica zahteva kompleksnost gesel, onemogoča prenos gesel v nezaščiteni obliki ter posodablja operacijske sisteme usmerjevalnikov s preizkušenimi varnostnimi popravki. Z varovanje nastavitev vseh usmerjevalnikov hranilnica uporablja centralni sistem za shranjevanje nastavitev.

4.4.2.4 Požarne pregrade

Požarna pregrada je namenska naprava, ki s strojno in programsko opremo uveljavlja varnostno politiko na omrežnih povezavah. Varnostna politika je skupek pravil, ki odobravajo ali preprečujejo posamezne natančno določene dostope. V hranilnici se uporablja načelo, da so vsi dostopi, ki niso posebej odobreni s pravilom v varnostni politiki, zavrnjeni. Podrobneje sem sistem požarne pregrade v hranilnici opisal že v točki 4.3.2.

Hranilnica na požarni pregradi uporablja različne mehanizme za zagotavljanje varnosti dostopov, kot so:

- napredno filtriranje paketov,
- preslikava omrežnih naslovov (NAT - Network Address Translation),
- kontrola seznamov dovoljenih dostopov (ACL),
- kontrola paketov na programskem nivoju OSI modela.

Zavedajoč se nevarnosti, ki jim je izpostavljena požarna pregrada in posledično celotno omrežje, hranilnica stalno nadzoruje pretok prometa po pregradi. Hranilnica tako dnevno izvaja kontrolo dnevnikov na požarni pregradi po različno nastavljenih merilih, istočasno pa uporablja sistem samodejnega alarmiranja po vnaprej postavljenih pogojih (npr. oddaljena prijava na namizje drugega računalnika). Na ta način skrbniki pregrade sledijo dogajanju na pregradi in preverjajo morebitne nepričakovane in sumljive prenose.

4.4.3 Prenosni mediji

Prenosni mediji predstavljajo eno od najbolj tveganih skupin opreme, ki pa se ji žal ne moremo izogniti. Poznamo magnetne (diski, diskete, trakovi), optične (CD, DVD) in elektronske medije (različne pametne kartice). Prvo in največjo nevarnost predstavlja zagotavljanje varnosti podatkov na prenosnih medijih. Le-ti so običajno shranjeni v nezaščiteni obliki ter omogočajo branje podatkov s strani nepooblaščenih oseb. Drugo nevarnost predstavlja vnos prenosnih medijev na računalniško opremo v hranilnici in uporaba le-teh. Če je prenosni medij okužen z virusom, s črvom ali trojanskim konjem, lahko predstavlja resno nevarnost informacijskemu sistemu. Hranilnica se v skladu s sprejeto varnostno politiko izogiba uporabi prenosnih medijev, saj se varovanje podatkov izvaja v centralnem sistemu. Kadar je potrebno podatke posredovati izven hranilnice, se jih predhodno zaščiti z uporabo šifriranja. Za zaščito pred morebitnimi okužbami s prenosnih medijev ima hranilnica na vseh računalnikih nameščeno antivirusno zaščito, ki pregleduje vse prenosne medije in pri odkriti okužbi samodejno blokira prenos ter o tem obvesti skrbnika sistema.

4.4.3.1 Diskete in zgoščenke

Delovne postaje v hranilnici imajo nameščen disketni in CD/DVD pogon, ki omogočata vnos in iznos podatkov na teh medijih. V skladu z varnostno politiko hranilnice uporabniki ne smejo iznašati in vnašati podatkov brez predhodne najave pri svojem nadrejenem. Vseeno oprema zaposlenim omogoča iznos in vnos podatkov, kar predstavlja nevarnost za vnos zlonamerne kode ali za nekontroliran iznos pomembnih dokumentov.

4.4.3.3 Prenosne USB naprave

V zadnjem času smo bili priča zelo hitremu razcvetu prenosnih naprav, kot so diski, ključi, razni čitalci, ki s pomočjo USB priklopa omogočajo hiter priklop na vsako napravo, ki ima tovrsten priključek. Te naprave se lahko uporabljajo za varovanje podatkov, prenos uporabniških ali zelo razširjenih multimedijskih datotek ali za kakšen drug namen. S stališča varnosti so to zelo nevarne naprave. V skladu z varnostno politiko hranilnice uporabniki ne smejo uporabljati USB prenosnih naprav brez predhodne odobritve službe informatike.

4.4.3.2 Trakovi

Poseben del zagotavljanja varnosti prenosnih medijev predstavljajo trakovi, ki jih hranilnica uporablja za zagotavljanje varnostnih kopij v centralnem sistemu za varovanje podatkov. S trakovi upravljajo samo pooblaščene osebe, ki ravnajo s trakovi po posebej izdelanem protokolu. Trakovi se hranijo v varovanih ognjevarnih omarah, ki so nameščene na varni lokaciji, ki je oddaljena od računalniškega centra. Največjo nevarnost predstavlja prenos trakov iz računalniškega centra na varno lokacijo. Ta se izvaja s pomočjo posebne torbe za prenos trakov. Zelo pomembno je, da hranilnica kritične podatke na trakove zapisuje v zaščiteni obliki, ki bi bili ob morebitni odtujitvi težko dosegljivi.

4.5 Varnost operacijskih sistemov

Operacijski sistem je osnovna programska oprema, ki omogoča, da različna strojna oprema navzven deluje kot enovit sistem. Varnost celotnega informacijskega sistema je zelo odvisna tudi od operacijskih sistemov, ki ga sestavljajo. Zaradi množice proizvajalcev strojne in programske opreme bi bilo zelo težko prilagoditi operacijski sistem posameznim ciljnim skupinam, zato se v praksi na nove računalnike nameša operacijski sistem določenega proizvajalca, ki vsebuje osnovni sistem in nekatere skupne gonilnike. Ker takšen sistem omogoča množico različnih namestitev in povezav, proizvajalci običajno ne naredijo veliko za varnost sistema ter to odgovornost prenesejo na končnega uporabnika oz. skrbnika sistema. V splošnem je potrebno po namestitvi sistema odstraniti vso nepotrebno programsko opremo, onemogočiti vse nepotrebne storitve sistema, nastaviti ustrezne pravice dostopov do datotek ter nadgraditi operacijski sistem z najnovejšimi popravki. Proces, ko sistemu izboljšamo varnost in odpornost proti morebitnim vdorom, se v angleščini imenuje hardening. Za vsak operacijski sistem je v splošnem ideja enaka, koraki pri postopku pa so različni (White, 2004, str. 226).

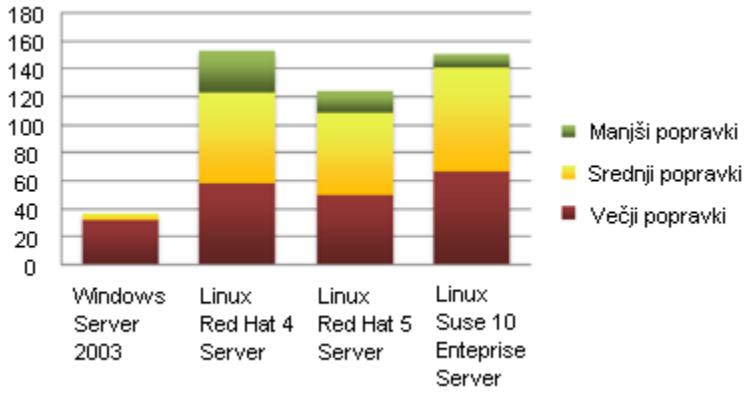
Na področju varnosti operacijskih sistemov obstajajo varnostni certifikati in standardi. Trenutna standarda TCSEC (Trusted Computer Security Evaluation Criteria) in ITSEC (Information Technology Security Evaluation Criteria) sta v osnovi vojaška standarda, ki se uporabljata tudi v poslovnem svetu (Boran, 8. 5. 2002). Po standardu TCSEC, ki je poznan tudi kot Orange Book, se sistemi razvrščajo v štiri hierarhične razrede: A, B (B1, B2, B3), C (C1, C2), D. Sistemi v skupini A so najbolj varni, sistemi v skupini D pa najmanj. Osnovna ideja standarda TCSEC je uporaba zaupnega računalniškega jedra, ki zagotavlja ločevanje naslovnega prostora, zaupne poti, načelo najmanj enakih pravic in neokrnjenost operacij. Ocenjevanje po tem standardu opravlja ameriška vladna organizacija NSA (National Security Agency), ki tudi podeli ustrezen certifikat. Najpogostejši certifikat v poslovnem okolju je C2, za katerega je značilno, da lastnik sam določi, kdo lahko dostopa do njegovega objekta. Sistemi razreda B so redkejši, razviti pa so predvsem za vojaške namene.

ITSEC je evropska različica varnostnega standarda, ki ga je Evropska unija sprejela in velja za vse članice od aprila 1995. ITSEC v osnovi temelji na standardu TCSEC, vendar je od njega širši in vključuje tudi vrednotenje funkcionalnosti in stopnje zavarovanja. Poleg varnosti operacijskih sistemov določa tudi standarde za druga področja.

4.5.1 Operacijski sistemi v hranilnici

Hranilnica se zaveda nevarnosti vdorov v operacijske sisteme, zato se odloča za čim večje poenotenje operacijskih sistemov ter se izogiba sistemom, ki so redki in imajo slabo podporo razvijalcev. Kot v večini drugih organizacij hranilnica na vseh delovnih postajah uporablja operacijski sistem Windows XP ali 2000. Na področju strežnikov ima hranilnica zaradi različnih zahtev proizvajalcev programske opreme nameščene operacijske sisteme Windows Server 2003 in Linux.

Slika 8: Prikaz števila popravkov za odkrite ranljivosti pogostih operacijskih sistemov za strežnike za prvo polletje 2007



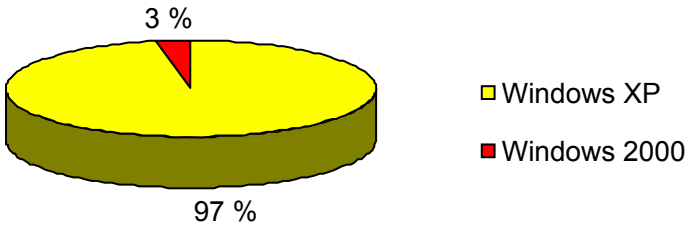
Vir: Jones, 2007.

Diagram na Sliki 8 prikazuje število popravkov za sisteme Windows Server 2003, Linux Red Hat Server 4, Linux Red Hat Server 5 ter Linux Suse Enterprise Server 10. Iz diagrama je razvidno, da se je s širitvijo sistemov najbolj uporabljenih Linux operacijskih sistemov Red Hat in Suse povečalo tudi število ranljivosti obeh sistemov. Za uporabnike tovrstnih sistemov je zelo pomembno redno testiranje in posodabljanje popravkov.

4.5.1.1 Microsoft Windows 2000 / XP

Hranilnica upravlja 120 delovnih postaj, ki imajo življenjsko dobo od 3 do 5 let. Kot je razvidno s Slike 9, je kar 97 % delovnih postaj opremljenih z operacijskim sistemom Windows XP, le 3 % pa s sistemom Windows 2000 (pa še te so v fazi zamenjave).

Slika 9: Prikaz operacijskih sistemov delovnih postaj



Vir: Interni podatki Delavske hranilnice, 2007.

Za omenjena Windows operacijska sistema je značilno, da sta bistveno bolj varna od svojih predhodnikov, vendar sta kljub temu zaradi splošne razširjenosti sistemov zelo pogosta tarča napadalcev. Večina napadalcev začne delo z zbiranjem informacij o sistemu, nadaljuje s prestrezanjem identitete, z razbijanjem gesel, s ponarejanjem ARP (Address Resolution Protocol) tabel, z nameščanjem skrivnega vhoda, onemogočanjem delovanja, razširjanjem pooblastil, s prisluškovanjem komunikacijam in na koncu s prikrivanjem sledi (Bratuša, 2006, str. 68).

Veliko ranljivosti izhaja iz naslova osnovne namestitve operacijskega sistema, ki je s stališča varnosti zelo ranljiv. Vse nove delovne postaje ali postaje, kjer se izvajajo spremembe, se nameščajo v službi informatike. Ta je zadolžena, da v skladu z navodili namesti odobreni operacijski sistem ter ga nastavi po vnaprej določenih varnostnih pravilih.

Pri nameščanju nove postaje hranilnica sledi pravilom za zagotavljanje varnosti:

- namesti uveljavljen in preverjen operacijski sistem (Windows XP SP2),
- odstrani vse protokole, ki niso potrebni (netbios, telnet itd.),
- onemogoči vsa mesta za skupno rabo (network shares), ki niso potrebna,
- odstrani ali onemogoči vse račune, ki niso potrebni,
- zahteva kompleksnost gesel, zaklepanje računov in beleženje,
- dovoljuje oddaljeni dostop samo skrbniku sistema,
- uporabniku omogoči samo uporabniške privilegije,
- namesti delovno postajo v centralni sistem antivirusne zaščite,
- namesti samo potrebno programsko opremo, ki je licenčna,
- nadgradi popravke za programsko opremo in operacijski sistem.

Druga nevarnost, ki preti operacijskim sistemom, so naknadno odkrite ranljivosti oz. tako imenovane varnostne luknje sistema. Hranilnica za centralno vzdrževanje in posodobitev operacijskih sistemov delovnih postaj in strežnikov Windows uporablja program WSUS (Windows Update Server). Program je nameščen na posebnem Windows strežniku in omogoča upravljanje z varnostnimi in drugimi popravki za vse Microsoftove proizvode. S sistemom upravlja informatika v hranilnici, ki preizkuša popravke v testnem okolju ter jih posledično odobri ali zavrne. Posebna pozornost je namenjena varnostnim popravkom, ki odpravljajo naknadno odkrite ranljivosti operacijskega sistema. Vsi odobreni popravki in dodatki se v skladu z nastavljenim časovnim načrtom prenašajo in nameščajo na delovne postaje. Na ta način hranilnica zagotavlja poenotenje in skladnost operacijskih sistemov Windows z vsemi varnostnimi popravki proizvajalca. Hranilnica je zelo previdna pri uvajanju novega operacijskega sistema za delovne postaje, saj ne želi sistema, ki še ni v celoti preizkušen in zaščiten.

4.5.1.2 Microsoft Windows Server 2003

Operacijski sistemi Windows so zaradi svoje zgodovine in razširjene uporabe zelo priljubljena tarča napadalcev. Napadi se običajno pričnejo s pregledovanjem oz. s tako imenovanim skeniranjem vseh vhodov strežnika. Na ta način napadalec pridobi osnovne informacije o sistemu, ki ga napada. Ker so omenjeni sistemi velikokrat gostitelji domenskega strežnika, je ta zelo pogosta tarča napadalcev, ki lahko tako prevzamejo nadzor in onemogočijo delovanje vseh računalnikov v domeni (Bratuša, 2006, str. 69).

Hranilnica za informacijsko podporo sistemskim procesom (AD - Active Directory, DNS - Domain Name System, DHCP - Dynamic Host Configuration Protocol, WSUS

- Windows Update Server) in nekaterim poslovnim procesom uporablja strežnike z nameščenim operacijskim sistemom Windows 2003 Server. Strežniki imajo glede na svojo namembnost nameščene različne storitve.

Pri nameščanju strežnikov hranilnica sledi pravilom za zagotavljanje varnosti:

- namesti uveljavljen in preverjen operacijski sistem z zadnjimi popravki (Windows Server 2003 SP1),
- poskrbi za redno nameščanje popravkov, ki so objavljeni pri proizvajalcu,
- nadgradi kritične popravke za programsko opremo in operacijski sistem,
- odstrani vse protokole in storitve, ki niso potrebni (Telnet, FTP, SSH itd.),
- onemogoči vsa mesta za skupno rabo (network shares), ki niso potrebna,
- odstrani ali onemogoči vse račune, ki niso potrebni,
- vklopi kompleksnost gesel, zaklepanje računov in beleženje,
- varuje datoteke in datotečna področja,
- neznanim uporabnikom onemogoči dostop do registra,
- nastavi pozdravno sporočilo z opozorilom pred nepooblaščeno uporabo,
- pred uporabo preveri sistem s programom proizvajalca MSBA (Microsoft Security Baseline Analyzer),
- namesti samo licenčno programsko opremo.

Proces zagotavljanja varnosti zahteva stalen nadzor dogajanja v sistemih. Hranilnica dnevno nadzira različne dnevnike dogajanj na Windows strežnikih ter skrbi, da se kritični popravki proizvajalca sproti testirajo in redno nameščajo na strežnike. Na ta način hranilnica zmanjšuje varnostno tveganje v operacijskih sistemih strežnikov.

4.5.1.3 Linux operacijski sistemi

Na področju operacijskih sistemov za strežnike vse pogosteje srečujemo operacijske sisteme Linux, ki so osnovani na sistemih Unix in so zelo zmogljivi. V različnih distribucijskih paketih jih na trgu ponujajo mnogi proizvajalci (Suse, Red Hat, Debian itd.). V zadnjih letih so dokazali, da se na področju operacijskih sistemov za strežnike lahko kosajo s sistemi, ki jih pomembnejši proizvajalci razvijajo že desetletja (HP Unix, IBM Aix, SUN Solaris itd.). Še več, spodrivajo in zamenjujejo jih iz najbolj zahtevnih informacijskih okolij na vseh poslovnih področjih. Razlogi za to dogajanje so predvsem v odprti kodi, cenovni ugodnosti (kupec plača samo vzdrževanje oz. podporo) ter neodvisnosti Linux sistemov, ki omogočajo delovanje na strojni opremi različnih proizvajalcev.

Hranilnica za informacijsko podporo poslovnim in nekaterim sistemskim procesom uporablja strežnike z nameščenim 64-bitnim operacijskim sistemom Linux Suse Enterprise Server. Pred kratkim je hranilnica izvedla prenovo poslovnega sistema in na ta način prešla še iz zadnjega operacijskega sistema HP Unix na Linux Suse. Vsi strežniki so nameščeni in prilagojeni glede na namembnost, ki jo opravljajo. Linux SuSe je certificiran po standardu TCSEC za razred C2, zato hranilnica skrbi za ustrezne nastavitve in nadzor sistema za zagotavljanje C2 nivoja varnosti v praksi.

Pri nameščanju in vzdrževanju Linux operacijskih sistemov hranilnica sledi pravilom za zagotavljanje varnosti:

- namesti Linux operacijski sistem, ki ima zagotovljen razvoj popravkov in tehnično podporo ter je skladen z arhitekturo strežnika,
- operacijski sistem nadgradi z vsemi potrebnimi popravki, ki jih predhodno preveri v testnem okolju,
- odstrani vse storitve in programe, ki se ne uporabljajo,
- omeji dostop do datotek in področij v skladu s potrebami ter onemogoči vsa mesta za skupno rabo, ki niso potrebna,
- odstrani ali onemogoči vse račune, ki niso potrebni,
- preveri vse skupine uporabnikov,
- vklopi kompleksnost gesel, zaklepanje računov in beleženje,
- nadzoruje delovanje in kontrolira dnevnike sistema.

Za zagotavljanje varnosti operacijskih sistemov Linux hranilnica sledi priporočilom UNIX and Linux Security Checklist Notes (AusCert, 2007).

4.5.2 Upravljanje popravkov in nadgradenj

Hranilnica upravlja popravke in nadgradnje (change management) na dva načina. Vsi popravki in vse nadgradnje za Windows operacijske sisteme se upravljajo s strežnikom WSUS, kjer se vodi sledljivost in celotna zgodovina vseh nadgradenj sistemov, istočasno pa se osvežuje zbirka popravkov, ki jih priporoča proizvajalec Microsoft. Vsi popravki se pred namestitvijo testirajo in potrdijo v testnem okolju. Popravki in nadgradnje se prenašajo v produkcijo po posebej nastavljenem časovnem razporedu, ki ga določa skrbnik sistema. Drugi način se uporablja za Suse Linux strežnike. Pri tem načinu skrbnik sistema preverja predlagane popravke proizvajalca v testnem okolju ter jih ročno namešča po posameznih strežnikih. O vseh posegih vodi dokumentacijo za vsak posamezni strežnik s celotno zgodovino popravkov in nadgradenj.

4.6 Zaščita baz podatkov

Baze podatkov so za podjetje in posameznika najpomembnejši del informacijskega sistema, kamor se shranjujejo najrazličnejši podatki, ki jih podjetje ali posameznik uporablja pri svojem delu. To so lahko poslovni podatki, podatki o zaposlenih, podatki o strankah, osebni podatki itd. Vsak delček našega življenja je shranjen v različnih bazah podatkov, ki hranijo naše matične, finančne, zdravstvene, telefonske in druge podatke. Ne glede na to, ali so to poslovni ali osebni podatki, je potrebno zaščititi dostop do njih ter zagotoviti varnost baz podatkov.

Ena od značilnosti večine baz podatkov je, da so sestavljene iz množice objektov, ki so v medsebojni povezavi ter v katere se podatki zapisujejo po zapletenih logičnih povezavah oz. relacijah. Podatki so shranjeni tako, da so neodvisni od programov, ki jih uporabljajo (Grad, 1985, str. 1).

Tudi baze podatkov imajo varnostne pomanjkljivosti, kar potrjuje podatek, da je Oracle, kot največji ponudnik na trgu baz podatkov, v zadnjem času izdal kar 69 varnostnih popravkov, v katerih je zakrpal od 50 do 100 varnostnih pomanjkljivosti. Njegov največji konkurent Microsoft je v istem času izdal 36 popravkov za MS SQL Server (Bratuša, 2006, str. 196). Tako kot na drugih delih sistema je tudi pri varovanju baz podatkov potrebno zagotoviti zaupnost, neokrnjenost, razpoložljivost in celovitost podatkov. Potrebno je poskrbeti, da bodo posamezni podatki v bazi na razpolago le pooblaščenim osebam, kar je naloga sistema za upravljanje baze podatkov. Zelo pomemben element pri zagotavljanju varnosti je skrbnik baze podatkov, tako imenovan DBA (Database Administrator), ki sistem nadzira in upravlja.

Najpogostejše vrste varnostnih pomanjkljivosti pri bazah podatkov so (Bratuša, 2006, str. 197):

- zlorabe v omrežnih protokolih (črv Slammer),
- pomanjkljivosti v avtentikacijskih protokolih (nezaščiten prenos gesel),
- dostop do funkcionalnosti brez avtentikacije (Oracle TNS listener),
- izvršitev arbitrarne kode v elementih SQL (slabe internet aplikacije),
- razširjanje pooblastil (izvrševanje procedur z višjimi privilegiji).

4.6.1 Baze podatkov v hranilnici

Hranilnica za shranjevanje in obdelavo podatkov v informacijski podpori poslovnim procesom uporablja več baz podatkov Oracle različice 10g. Zanje je značilno, da so zelo priljubljene med razvijalci sistemov in imajo največji tržni delež. Proizvajalec baz podatkov, podjetje Oracle sicer poudarja, da je njihov sistem baz podatkov nezlomljiv, kar pa zanika veliko število odkritih varnostnih pomanjkljivosti, ki jih podjetje Oracle vseskozi odpravlja s popravki in z novimi različicami. Šele v različici 9i je baza podatkov Oracle zagotovila varnost najmanjše enote, ki zagotavlja možnost revidiranja tabele na osnovi uporabnika ali posameznega polja (Finnigan, 2004, str. 2). Prednost baz podatkov Oracle proti nekaterim drugim bazam je, da imajo le-te vgrajene varnostne funkcionalnosti, ki ob pravilnih nastavitvah zagotavljajo visok nivo varnosti in neodvisnosti od programskih rešitev. Na ta način so tovrstne baze podatkov primerne za delo z različnimi operacijskimi sistemi (An Oracle White Paper, 2006, str. 4).

Pri nameščanju in vzdrževanju baz podatkov Oracle hranilnica sledi pravilom za zagotavljanje varnosti:

- uporablja baze podatkov, ki so preizkušene in primerne za produkcijsko uporabo ter so skladne z operacijskim sistemom,
- skrbi za redno nameščanje varnostnih popravkov po priporočilih razvijalca,
- skrbi za upravljanje dostopov uporabnikov in kompleksnost gesel za nastavljeni profil uporabnikov,
- preverja dnevnike in delovanje sistema,
- skrbi za varovanje podatkov na medijih, ki so shranjeni na varni lokaciji,
- skrbi za periodične preglede sistema baz podatkov.

4.6.1.1 Upravljanje baz podatkov

Sistem baz podatkov je sestavljen iz same baze podatkov ter sistema za upravljanje baz podatkov - DBMS (DataBase Management System), ki skrbi za branje, pisanje, spreminjanje, brisanje, iskanje ter nadzor nad izvajanjem. Standardiziran programski jezik četrte generacije, ki uporabnikom omogoča, da sami izvajajo operacije nad podatki, se imenuje strukturiran poizvedovalni jezik ali SQL (Structured Query Language).

Pri upravljanju različnih baz podatkov Oracle hranilnica zagotavlja zaupnost, neoporečnost ter razpoložljivost podatkov z naslednjimi varnostnimi mehanizmi v sistemu upravljanja:

- razpoznavanje in overjanje uporabnikov,
- pooblaščanje,
- šifriranje podatkov,
- omogočanje revizijske sledi,
- nadzor delovanja.

4.6.1.2 Razpoznavanje in overjanje uporabnikov

Razpoznavanje in overjanje uporabnikov pri bazah podatkov Oracle v hranilnici poteka ob prijavi v informacijski sistem Hibis. Izvaja se na nivoju baze s preverjanjem uporabniškega imena in gesla, ki je v šifrirani obliki shranjeno v sami podatkovni bazi. Hranilnica v skladu s sprejeto varnostno politiko za overjanje uporabnikov uporablja poseben profil uporabnikov, nastavljen v bazi podatkov, ki zagotavlja osnovne zahteve za kompleksnost gesel (Politika upravljanja z gesli, 2007):

- geslo mora vsebovati vsaj tri od štirih tipov znakov,
- geslo uporabnika mora biti dolgo vsaj x znakov in mora biti shranjeno v šifrirani obliki (gesla uporabnikov s skrbniškimi pooblastili morajo biti daljša),
- geslo je potrebno menjati vsakih 30 dni,
- po tretji napačni prijavi se uporabniški račun zaklene in ostane zaklenjen.

4.6.1.3 Pooblaščanje

Po uspešni overitvi uporabnika se dodatno izvaja tudi preverjanje pooblastil uporabnika za dostop do posameznih objektov v bazi podatkov. Oracle tako omogoča omejen dostop do podatkov glede na dodeljena pooblastila posameznega uporabnika, ki lahko dovoljujejo branje, spreminjanje, brisanje ali samo pregledovanje podatkov v bazi. Hranilnica kontrolo dostopa do posameznih objektov v bazi zagotavlja z nastavitvami v bazi podatkov in v bančni aplikaciji Hibis (npr. vnos kreditov, obdelava kreditov, vpogled v kreditno kartico itd).

4.6.1.4 Omogočanje revizijske sledi

Za zagotavljanje varnosti podatkov v bazah je zelo pomembno, da sistem baze podatkov omogoča revizijske sledi. Hranilnica ima na vseh bazah podatkov Oracle

vključen mehanizem za beleženje sledi, ki omogoča kasnejše revidiranje glede na objekt, dogodke, pravice ali uporabnika, kjer se beležijo uspešne in neuspešne prijave v podatkovno bazo. Oracle hrani zapise na nivoju baze, do njih pa je mogoče dostopiti z uporabo že vnaprej pripravljenih kompleksnih poročil in poizvedb. Prav zahtevnost za dostop do teh podatkov predstavlja eno od dveh slabosti beleženja dogodkov v bazah Oracle, saj je za preverjanje sledi običajno potrebno veliko znanja. Drugo slabost predstavlja razmeroma velika obremenitev sistema, ki je potrebna za beleženje sledi in tako posledično zmanjšuje odzivnost baze podatkov za delo z uporabniki (An Oracle White Paper, 2002, str. 20).

4.6.1.5 Uporaba šifriranja podatkov

Tako kot na drugih področjih je potrebno tudi v bazi podatkov zagotoviti zaščito podatkov. Na nek način že razdrobljenost podatkov v bazi, ki so shranjeni s pomočjo povezav in ključev v različnih tabelah, do neke mere ščiti le-te pred enostavnim pregledom. Vseeno pa je za podatke, ki so zelo pomembni (npr. gesla), potrebno zagotoviti visoko zaupnost s pomočjo šifriranja podatkov. Hranilnica za šifriranje tovrstnih podatkov v bazah podatkov Oracle uporablja že prej omenjeni 3DES algoritem, ki zagotavlja visoko stopnjo zaščite podatkov.

4.6.1.6 Nadzor delovanja

Hranilnica podobno kot na drugih delih informacijskega sistema izvaja redni nadzor delovanja baz podatkov Oracle z dnevnimi kontrolami sistemskih dnevnikov, kjer se beležijo vsi dogodki baze. Hkrati se dnevno izdeluje poročilo o posebnih dogodkih (npr. zaklenjeni uporabniški računi, istočasne prijave uporabnika z različnih mrežnih naslovov, poizvedbe z večjimi obremenitvami, zaklenjeni dostopi do tabel itd). Poročilo se pregleduje dnevno, ob ugotovljenih odstopanjih pa se izvajajo ustrezni ukrepi. Podrobnejši pregledi objektov in zmogljivosti baze podatkov so del rednih periodičnih pregledov.

4.7 Programska oprema in informacijski sistemi

Hranilnica za računalniško podporo poslovnim procesom, ki jih izvajajo zaposleni ali komitenti, omogoča uporabo različne programske opreme in različnih informacijskih sistemov. To so lahko enostavni uporabniški programi, ki se izvajajo na lokalni delovni postaji ali pa zapleteni informacijski sistemi, ki tečejo na kritičnih strežnikih. Ključna elementa zagotavljanja varnosti pri programski opremi sta zagotavljanje kontrole dostopa v skladu s sprejeto politiko varovanja ter nadzor nad spremembami v programski opremi in sistemih.

4.7.1 Uporabniški programi

Zaposleni v hranilnici pri svojem delu uporabljajo različna osnovna programska orodja in pakete, ki jim omogočajo upravljanje dokumentov ter komuniciranje z okolico.

Tabela 1: Pregled uporabniških programov v hranilnici

Program	Namen
Microsoft Office (Word, Excel, Power Point, Outlook, Access)	Pisarniški program
NOD32	Program za antivirusno zaščito
Internet Explorer	Brskalnik
Adobe Acrobat Reader	Pregledovalnik
ZBS EOM	Program za izračun efektivne obrestne mere
IBON	Bonitetni program
PGP	Program za šifriranje datotek
Microsoft Visio	Program za načrtovanje

Vir: Interni podatki Delavske hranilnice, 2007.

S stališča zagotavljanja varnosti je za uporabniške programe navedene v Tabeli 1, pomembno, da hranilnica zagotavlja kontroliran in omejen dostop do uporabniških podatkov, ter, da zagotavlja varnostne kopije dokumentov na varni lokaciji. Dokumenti se dnevno shranjujejo v centralni tračni knjižnici.

4.7.2 Bančni informacijski sistem Hibis

Hranilnica za podporo poslovanju s fizičnimi in pravnimi osebami uporablja programsko opremo Hibis, proizvajalca HRC, ki je v vlogi razvijalca in pogodbenega vzdrževalca za vse programske pakete in module, ki so navedeni v Tabeli 2.

Tabela 2: Pregled programskih modulov v informacijskem sistemu Hibis v hranilnici

Štev.	Modul
1	Blagajniško poslovanje
2	Transakcijski računi
3	Hranilne vloge
4	Kreditno in depozitno poslovanje
5	Rentno varčevanje
6	Menjalnica
7	Posli zaledja
8	Novi plačilni instrumenti
9	Domači in tuji plačilni promet
10	Glavna knjiga
11	Saldakonti dobaviteljev
12	Poročanje
13	Pranje denarja
14	Osnovna sredstva

Vir: Interni podatki Delavske hranilnice, 2007.

Bančni informacijski sistem Hibis je zasnovan in izdelan s pomočjo programskih orodij četrte generacije (sql forms, reports, menu) na relacijski bazi podatkov Oracle. Skrbniku sistema omogoča, da s sistemom za upravljanje baze podatkov upravlja, vodi in nadzoruje dostope do posameznih programskim paketov, modulov in podatkov, in sicer v skladu z dodeljenimi pravicami uporabnikov. Sistem omogoča revizijske sledi za posamezne dogodke uporabnikov. Informacijski sistem Hibis je predmet periodičnih notranjih in zunanjih revizijskih pregledov.

Hranilnica se zaveda nevarnosti za vdor v informacijski sistem Hibis, zato skrbi za:

- politiko dostopov do aplikacije in produkcijske baze Hibis,
- pooblaščanje in kontrolo dostopov do posameznih modulov in podatkov,
- razmejevanje pooblastil po načelu štirih oči (operater, kontrolor),
- uporabo logičnih kontrol pri vnosu in obdelavi podatkov,
- varovanje osebnih podatkov in poslovnih skrivnosti,
- redni nadzor poročil in dnevnikov dogodkov,
- zagotavljanje varnostnih kopij na varni lokaciji.

Posebno skrb hranilnica namenja nadzoru sprememb v programski opremi. Za ta namen ima hranilnica za vsak programski paket ali modul določenega vsebinskega skrbnika, ki je zadolžen za naročanje in testiranje popravkov in nadgradenj ter za odobritev prenosa sprememb v produkcijsko okolje.

4.7.3 Spletni banki Dh-Plus in Dh-Net

Hranilnica svojim komitentom omogoča uporabo dveh spletnih bank. V ponudbi sta spletna banka za fizične osebe Dh-Plus ter spletna banka za pravne osebe Dh-Net. Dh-Net je bila uvedena v letu 2002 z namenom, da se pravnim osebam, ki imajo v hranilnici odprt transakcijski račun, omogoči pregled nad sredstvi na računu ter enostaven plačilni promet z računom. Spletna banka Dh-Plus za fizične osebe je bila uvedena v letu 2005 z namenom, da se obstoječim in novim strankam hranilnice omogoči spletno poslovanje z osebnim računom. Obe spletni banki sta bili razviti v sodelovanju s pogodbenim razvijalcem HRC, ki za hranilnico razvija in vzdržuje že zgoraj opisani bančni informacijski sistem. Zaradi zahteve po varnosti poslovanja se je hranilnica odločila za uporabo sistema digitalnih potrdil in zasebnih ključev, ki zagotavljajo zaupnost in celovitost prenosa podatkov ter omogočajo elektronsko podpisovanje v skladu z Zakonom o elektronskem podpisu in elektronskem poslovanju. Varno poslovanje s spletnima bankama je zagotovljeno s šifriranjem in z elektronskim podpisovanjem sporočil med uporabnikom in hranilnico, kjer se uporablja algoritem RSA z dolžino ključa 1024 bitov.

Uporabniki za vstop v spletno banko Dh-Plus ali Dh-Net uporabljajo kvalificirana digitalna potrdila enega od dveh izdajateljev, ki jih podpira informacijski sistem hranilnice, in sicer:

- POŠTA®CA, ki jih izdaja Pošta Slovenije,
- SIGEN-CA, ki jih izdaja Ministrstvo za javno upravo.

Pri poslovanju s spletno banko obstaja nevarnost za zlorabo zaradi vdora:

- v informacijski sistem hranilnice,
- v povezavo med uporabnikom in hranilnico,
- v računalnik na strani uporabnika.

Hranilnica varnost informacijskega sistema zagotavlja s sistemom požarne pregrade in antivirusne zaščite, z notranjo kontrolo, s pooblaščanjem in z nadzorom dostopa do spletne banke. Vsi dostopi se redno pregledujejo s strani skrbnika sistema. Sistem beleži vse podatke o dostopih uporabnikov, vključno z nekaterimi sistemskimi podatki, ki ob morebitni zlorabi omogočajo sledi.

Za ustrezno stopnjo varnosti in zaupnosti pri prenosu podatkov med uporabnikom in spletno banko se uporablja protokol SSL (Secure Sockets Layer Protocol) in 128-bitni ključ. SSL protokol s pomočjo digitalnega potrdila spletnega strežnika in uporabnika poskrbi za medsebojno prepoznavo ter omogoči oblikovanje ključa oziroma žetona za simetrično šifriranje povezave med uporabnikovim brskalnikom in spletnim strežnikom. Pogoj za varno povezavo je, da je digitalno potrdilo strežnika kvalificirano oz. overjeno s strani priznane certifikatske agencije (Jerman Blažič, 2001, str. 120). Hranilnica uporablja 128-bitno zaščito, ki je bistveno boljša od stare 40-bitne ter zaenkrat še zadošča za varno poslovanje. Uporabnik mora imeti nameščen brskalnik, ki podpira 128-bitno zaščito (Internet Explorer 5.5 SP2, Mozilla 1.4 ali novejši).

Hranilnica uporabnikom svetuje, da shranijo digitalno potrdilo na pametno kartico, ki omogoča hranjenje v šifrirani obliki. Ena od največjih nevarnosti, ki preži na uporabnike spletne banke, je shranjevanje digitalnih potrdil oz. prevzem le-teh neposredno na disk lokalnega računalnika. Zaradi velike povezanosti računalnikov v svetovni splet obstaja nevarnost odsvojitve potrdila in zasebnega ključa ali drugih elementov razpoznavanja in overjanja.

4.7.4 Plačilni sistem Swift

Hranilnica za bruto poravnavo v realnem času uporablja mednarodni plačilni sistem SWIFT (Society for Worldwide Interbank Financial Telecommunications). To je kompleksen sistem, v katerega so vključene banke po vsem svetu. S sistemom SWIFT je hranilnica vključena v zaprt evropski plačilni sistem Target II, ki je namenjen plačilom velikih vrednosti.

Sistem SWIFT v hranilnici tvorijo strežniki, ki so nameščeni z namensko programsko opremo za varno izmenjavo plačilnih transakcij. Te se z več ločenimi povezavami povezujejo z regionalnimi vstopnimi točkami SWIFT ter tako komunicirajo z drugimi strežniki bank v omrežju. V skladu z zelo dodelano strategijo SWIFT skrbi za zagotavljanje varnosti poslanih sporočil z različnimi metodami in elementi:

- uporaba Swift certifikata o istovetnosti javnega ključa banke ali hranilnice,
- dvostranska izmenjava ključev z drugimi bankami v sistemu (vsaka banka izmenja ključe z vsako banko v sistemu),

- uporaba čitalcev kartic in pametnih kartic (za delo operaterja, za skrbnika sistema, za izmenjavo ključev),
- uporaba lastnega algoritma za overjanje,
- logična kontrola sporočil, ki zagotavljajo celovitost, preprečujejo izgubo ter onemogočajo podvajanje (Caelli, 1994, str. 698),
- varnostni mehanizmi, ki preprečujejo nepooblaščeno prisluškovanje in potvarjanja sporočil s sistemom uporabe enkratnih gesel iz množice gesel,
- uporaba več sistemov za zagotovitev neprekinjenega poslovanja (trije strežniki).

Tveganje varnosti plačilnih sistemov spada med največja operativna tveganja hranilnice. Varnost pri uporabi sistema SWIFT se zagotavlja z rednim vzdrževanjem in nadgrajevanjem sistema v skladu s priporočili sistema, z izobraževanjem zaposlenih v plačilnim prometu, z doslednim razmejevanjem pristojnosti (operater, kontrolor, skrbnik). Hranilnica zagotavlja fizično in logično varovanje dostopov.

4.7.5 Plačilni sistem Giro kliring

Vzporedno s sistemom za plačila velikih vrednosti je hranilnica vključena tudi v sistem plačil malih vrednosti ali v tako imenovani Giro kliring po omrežju Banke Slovenije. V to omrežje so vključene vse slovenske banke in hranilnice ter ostale finančne ustanove in podjetja, ki se neposredno vključujejo v sistem za izmenjavo plačilnih nalogov.

Sistem tvorijo strežniki, ki se nahajajo v računalniškem centru Banke Slovenije. Do teh strežnikov hranilnica dostopa po najetem vodu. Overjanje uporabnikov se izvaja neposredno na strežnikih Banke Slovenije, kjer se odobravajo dostopi delovnih postaj hranilnice do strežnikov za varno izmenjavo podatkov. Varnost poslovanja je zagotovljena z različnimi metodami in elementi:

- uporaba najetega voda in rezervne povezave, na katerih se izvaja zmogljivo šifriranje podatkov,
- upravljanje aktivne opreme za povezavo neposredno s strani Banke Slovenije,
- omejitev dostopov s požarno pregrado hranilnice, kjer se povezava nahaja v svojem ločenem okolju (partnerske povezave),
- razpoznavanje in pooblaščanje uporabnikov delovnih postaj hranilnice se izvaja na strani Banke Slovenije,
- uporaba kartic, na katerih so shranjeni certifikati, potrebni za overjanje ter namensko razvite programske opreme za šifriranje plačilnih nalogov,
- napredna struktura plačilnih nalogov,
- podvojenost opreme na strani Banke Slovenije in hranilnice.

Tveganje varnosti plačilnega sistema je predmet rednih notranjih in zunanjih revizijskih pregledov. Hranilnica zagotavlja varnost z zagotavljanjem varnosti fizičnega in logičnega dostopa do sistema, z razmejevanjem pristojnosti (operater, kontrolor, skrbnik), z dnevnim shranjevanjem podatkov na varno lokacijo ter z dnevnim nadzorom sistema.

4.7.6 Komunikacijski program Connect Direct

Hranilnica ima vzpostavljeno komunikacijsko povezavo s procesnim centrom Bankart za podporo kartičnemu in bankomatskemu poslovanju ter za transakcije zbirnega centra, ki poteka v okviru standarda Novih plačilnih instrumentov. Program Connect Direct skrbi za avtomatizirano izmenjavo podatkov ter proženje procesov na strani strežnikov Bankarta.

Varnost poslovanja je zagotovljena z različnimi elementi:

- uporaba najetega voda in šifriranje podatkov,
- upravljanje aktivne opreme za povezavo je v celoti pod kontrolo hranilnice,
- strežnik, na katerem je nameščena aplikacija Connect Direct, je priključen na posebno področje partnerskih povezav, ki ščiti dostope s požarno pregrado,
- overjanje dostopov na strani centra in hranilnice,
- zagotovljeno je varovanje podatkov in zagotovljen je okrevalni načrt,
- hranilnica zagotavlja fizične in logične kontrole dostopa do strežnika,
- aplikacija zagotavlja avtomatizacijo procesov in sledljivost vseh prenosov,
- aplikacija ima vzpostavljen sistem obveščanja po elektronski pošti.

Zaščita in neprekinjenost izmenjave podatkov je zelo pomembna za poslovanje hranilnice, saj se z njo prenašajo občutljive finančne informacije. Hranilnica načrtuje vzpostavitev rezervne povezave s centrom Bankart, ki ta trenutek še ni vzpostavljena, kar bi ob prekinitvi lahko povzročilo operativne težave hranilnice.

4.7.7 Spletni portal in elektronska pošta

Za informiranje komitentov, poslovnih partnerjev in ostale javnosti hranilnica objavlja vse zanimive informacije in podatke na svojem spletnem portalu. Ta je opremljen z osnovnimi informacijami in različnimi spletnimi izračuni, ki obiskovalcem omogočajo enostaven izračun kreditnih in varčevalnih ponudb v hranilnici.

Sistem je vzpostavljen na strežniku, na katerem je nameščen tudi program za elektronsko pošto. Strežnik je nameščen na vmesno področje hranilnice, ki je s požarno pregrado ločeno od internetnega in lokalnega omrežja hranilnice. Varnost poslovanja je zagotovljena z naslednjimi mehanizmi:

- omejitev dostopov s požarno pregrado in sistemom antivirusne zaščite,
- zagotovljene so fizične in logične kontrole dostopa,
- sistemsko okolje je zaradi velike izpostavljenosti redno nadgrajeno z najnovejšimi varnostnimi popravki,
- vse neuporabljene storitve so onemogočene,
- vklopljena je sledljivost,
- izvaja se dnevni nadzor dostopov do strežnika,
- vklopljeno je alarmiranje kritičnih dogodkov na požarni pregradi,
- zagotovljeno je dnevno varovanje podatkov in okolja,
- pripravljen je okrevalni načrt.

V zadnjem času so vse pogostejši najrazličnejši napadi na strežnike za elektronsko pošto in spletne strani. Zavedajoč se nevarnosti, hranilnica vlaga sredstva v posodobitev sistema požarne pregrade, antivirusne in antispam zaščite, ki so sposobne učinkovito zaščititi sistem in uporabnike. Pri tem veliko vlogo opravlja sistem nastavljenih uteži na požarni pregradi, ki določa prednostno listo dostopov in na ta način do neke mere varuje spletni strežnik pred napadi tipa DoS, vendar verjetno ni učinkovit pri ponavljajočih in spreminjajočih se napadih.

4.8 Zaščita pred zlonamernimi programi

Vedno pogostejši so napadi na informacijske vire z različnimi virusi, črvi, trojanskimi konji, z neželeno pošto (spam), vohunskimi programi (spyware). Omenjene nevarnosti se vnašajo v sistem z elektronsko pošto, z uporabo brskalnikov, z vnosom prenosnih naprav, itd. Računalniški strokovnjaki so pred časom leto 2003 preimenovali kar v leto črvov. Takrat se je začel širiti črv, imenovan Slammer, ki je v desetih minutah okužil 75.000 občutljivih strežnikov, pri čemer je onemogočil sisteme bankomatov in povzročil zamude na letališčih. Črv Slammer je izkoriščal ranljivost Microsoft SQL strežnikov z napadom tipa Buffer Overflow. Kasneje se je pojavil črv Blaster, ki je za razširjanje uporabljal ranljivost sistemov Windows. V avgustu 2003 se je pojavil črv, imenovan Sobig.F, ki je za razširjanje uporabljal elektronsko pošto in se je zelo razširil. Okuženo naj bi bilo vsako 17. sporočilo. Po nekaterih ocenah naj bi njegovo odstranjevanje in izguba produktivnosti podjetjem povzročilo škodo v vrednosti 82 milijard dolarjev. Ob zaključku leta 2003 je svet preplavil črv Mydoom, ki je okužil vsako 5. elektronsko sporočilo! Prišlo je do aretacij in sodnih postopkov. Od takrat so se napadalci prilagodili tudi na način, da sedaj sami samo pripravijo zlonamerno kodo in navodilo za razširjanje ter ga objavijo na svetovnem spletu, samo izvajanje kode pa prepustijo drugim (Bratuša, 2006, str. 352).

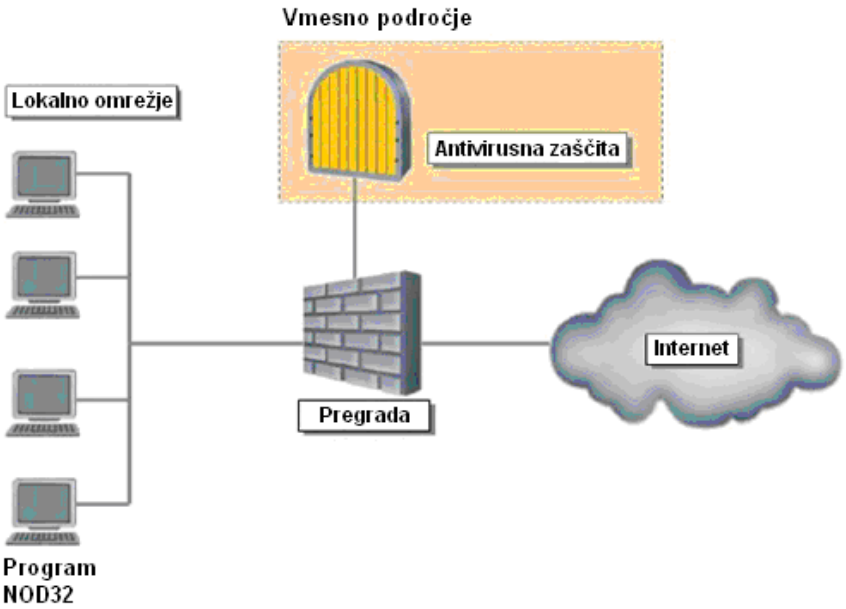
Na srečo braniteljev sistemov imajo vse omenjene nevarnosti prepoznavne načine za spreminjanje napadenega sistema, ki so nekakšni prstni odtisi, dobro znani antivirusnim programom, ki jih na ta način zaznajo in preprečijo škodljivo delovanje. Glavni problem pri zaščiti pred virusi in črvi je njihovo hitro spreminjanje ter razvijanje novih, zato je potrebno zbirko odtisov nenehno posodabljati in prenašati v sistem zaščite.

4.8.1 Antivirusna zaščita

Delavska hranilnica zaradi varnosti pred virusi, trojanskimi konji in podobnimi zlonamernimi kodami, ki prežijo v okolici, izvaja dvostopenjsko zaščito svojih računalnikov in omrežja, kot je prikazano na Sliki 10 (na str. 41).

Na prvi stopnji antivirusna zaščita zagotavlja varnost omrežja pri komuniciranju z zunanjim svetom (internetne in partnerske povezave) tako, da se ves promet, ki vstopa v hranilnico po sistemu požarne pregrade, pred vstopom v lokalno omrežje usmerja na antivirusni strežnik.

Slika 10: Shema sistema antivirusne zaščite in požarne pregrade



Vir: Aladdin, 2007.

Osnovne smernice nastavitve antivirusne zaščite so:

- preverja se ves promet po požarni pregradi,
- blokira se prenos vseh sporočil in priponk, ki so prepoznana kot virusi, črvi, trojanski konji ali neželena sporočila,
- blokirana sporočila se preusmerijo v karanteno,
- antivirusna zaščitna oprema se samodejno posodablja.

Na drugi stopnji hranilnica izvaja dodatno zaščito strežnikov in delovnih postaj z antivirusnim programom NOD32 ANTIVIRUS, ki je mednarodno priznan, in sicer kot eden od boljših zaščitnih programov. Centralni sistem NOD32 Enterprise Edition je nameščen na namenskem strežniku, odjemalski programi pa so nameščeni na delovnih postajah in strežnikih. Osnovni muduli NOD32 programa so:

- monitor datotek in programov v izvajanju,
- monitor dokumentov Microsoft Office,
- monitor programa za elektronsko pošto (Microsoft Outlook),
- monitor internetnega prometa,
- preverjanje področji na zahtevo uporabnika,
- program za samodejno nadgrajevanje in posodabljanje zaščite.

Sistem antivirusne zaščite je nastavljen tako, da v dejanskem času preverja vse dokumente, ki se nalagajo v sistem, elektronsko pošto ter internetne povezave. Dodatno se enkrat tedensko izvaja podroben pregled vseh delovnih postaj. Skrbnik ima pregled nad celotnim dogajanjem ter je z elektronskimi sporočili redno obveščen o najdenih virusih ali o drugih škodljivih programih. Že samo uporaba požarne pregrade ob izvajanju stroge politike vnašanja prenosnih naprav zagotavlja visoko stopnjo varnosti pred virusi, kar se v praksi potrjuje z izredno redkimi primeri odkritja virusov na delovnih postajah.

4.8.2 Zaščita pred neželeno pošto

Zaradi povečanega obsega neželene pošte (spam) je hranilnica nadgradila sistem antivirusne zaščite z dodatnim modulom za izločanje neželene pošte. V praksi hranilnica beleži od 1000 do 2000 takšnih sporočil na dan, ki jih modul samodejno zazna in že na vhodu v sistem odstrani z več kot 99-odstotno pravilnostjo delovanja. Tovrstna sporočila ne prispejo do uporabnikov. Le redko se zgodi, da kakšno pravo sporočilo zaide v karanteno, kamor se preusmeri vsa neželena pošta. Naloga skrbnika sistema je, da dnevno preverja in prazni karanteno ter ob odkritih pravih sporočil le-te posreduje naslovniku.

4.8.3 Zaščita pred vohunskimi programi

Poleg virusov, črvov in trojanskih konjev informacijskim sistemom vse pogosteje grozijo tudi vohunski programi (spyware), ki izkoriščajo naivnost uporabnikov. Najpreprostejša obramba je ozaveščenost uporabnikov, da na delovne postaje ne nameščajo nepoznanih priponk in programov (Bratuša, 2006, str. 328). Uporabniki v hranilnici nimajo pooblastil za nameščanje programov, tako je možnost za okužbo majhna. Večja nevarnost izhaja iz uporabe brskalnika in odpiranja priponk v elektronski pošti. Hranilnica redno pregleduje sumljive delovne postaje.

4.9 Varovanje podatkov

Varovanje podatkov je zelo pomembno za zagotavljanje neprekinjenosti poslovanja Delavske hranilnice. Lahko si predstavljate, kaj bi se zgodilo s hranilnico, če bi zaradi kakršnegakoli vzroka izgubila del ali vse podatke o poslovanju svojih komitentov (stanje na transakcijskih računih, vezave sredstev, kreditni posli itd). Zaradi navedenega hranilnica načrtovanju, izvajanju ter preverjanju varovanja podatkov posveča veliko pozornosti in energije.

Hranilnica izvaja varovanje podatkov po vnaprej pripravljeni politiki in navodilih za izvajanje varovanja na nivoju delovnih postaj, strežnikov in baz podatkov. Pregled dnevnikov varovanja je del uradnega dnevnega nadzora. Po vnaprej določeni periodi hranilnica v skladu z navodili izvaja testne restavracije podatkov z varnostnih kopij, da bi ugotovila, ali so podatki na medijih berljivi in omogočajo obnovitev podatkov in sistemov. Za varovanje podatkov hranilnica uporablja programsko opremo HP Data Protector Management, ki omogoča varovanje delovnih postaj, strežnikov in podatkovnih baz. Varovanje se lahko izvaja na skupnem diskovnem polju SAN (Storage Area Network) ali na trakovih, ki so nameščeni v tračni knjižnici. Po sprejeti politiki varovanja hranilnica dnevno izvaja shranjevanje podatkov na trakovih, ki jih potem iznaša iz sistema po rotacijski shemi. Te trakove hranilnica varuje na varni lokaciji izven sedeža hranilnice ter na ta način omogoča okrevanje ob katastrofi (požar, potres, poplava itd.) na lokaciji računalniškega centra. Posamezne varnostne kopije se hranijo do naslednjega cikla, ki je določen v rotacijski shemi, takrat se nanje prepišejo novi podatki. Prenos in varovanje varnostnih kopij se izvaja skladno z varnostnimi priporočili.

4.9.1 Delovne postaje

Hranilnica v poslovnih enotah in službah obdeluje in shranjuje vse ključne poslovne podatke z aplikacijo Hibis. Dnevno ali tedensko varuje podatke in sisteme na tistih delovnih postajah, ki so ključne za poslovanje in katerih uporabniki obdelujejo pomembne dokumente, ki niso del aplikacije Hibis. To so običajno predstavniki višjega vodstva in zaposleni v službah, ki pri svojem delu uporabljajo pogodbe, načrte, politike, navodila, dopise, preglednice itd. Podatke se shranjuje na trakove v skladu z nastavitvami v aplikaciji Data Protector Management.

4.9.2 Strežniki

Varovanje strežnikov se izvaja vsak delovni dan po točno določenem postopku varovanja. Na strežnikih hranilnica varuje dele sistemskega okolja, aplikacije in podatke. V varovanje so vključeni vsi strežniki Windows in Linux v hranilnici. Na ta način je z aplikacijo Data Protector Management zagotovljeno centralno shranjevanje na trakovih ter je zagotovljen iznos le-teh na varno lokacijo. Iznos in vnos trakov se izvaja z upoštevanjem varnostnih priporočil. Uspešnost varovanja hranilnica preverja dnevno z nadzorom dnevnikov varovanja in samodejnih elektronskih sporočil sistema. Poleg navedenega hranilnica izvaja preverjanje postopkov varovanja s periodičnim testnim restavriranjem varnostnih kopij z vseh strežnikov, kar se tudi formalno zabeleži v kontrolni seznam. Varovanje sistemskih okolij se izvaja po vsaki večji spremembi v sistemu.

4.9.3 Baze podatkov

Vsi poslovni podatki, ki se vnašajo in obdelujejo v informacijskem sistemu Hibis in spletnih bankah Dh-Plus in Dh-Net, se shranjujejo neposredno v dve različni bazi podatkov Oracle. Zaradi pomembnosti podatkov se varovanje izvaja z več metodami, pri tem pa se v skladu z nastavitvami v Data Protector Management programu tvorijo dnevni ter arhivski trakovi (mesečni, polletni, letni). Za zagotovitev okrevalnih načrtov hranilnica preizkuša varnostne kopije periodično, ko izvede restavracijo produkcijskih podatkov v enega od testnih okolij ter tako preveri ustreznost in popolnost procedur.

4.10 Organizacijska varnost

Eden od najpomembnejših dejavnikov za zagotavljanje varnosti in obvladovanje operativnih tveganj v hranilnici je ustrezna organiziranost kadrov, postopkov, procesov in sistemov. Organiziranost v hranilnici je predpisana s politikami in pravilniki, ki dopolnjeni z navodili urejajo delovanje na posameznih področjih.

4.10.1 Varnostna politika in navodila za izvajanje

Hranilnica ima izdelano Politiko varovanja informacij in informacijskega sistema, ki predstavlja standard, ki ureja način varovanja in zaščite informacij ter informacijskega sistema v hranilnici. V poglavjih so v skrčeni in jedrnati obliki dokumentirani postopki

varovanja. Podrobnejši opisi in navodila se nahajajo v Navodilu za izvajanje varnostne politike. Politika varovanja je izdelana na podlagi zahtev standardov ISO 17799:2005, BS 7799-2:2002, ISO/IEC 27001:2006, to je kodeksa najboljše prakse in specifikacij upravljavskega sistema za varovanje informacij. Pri tem je hranilnica upoštevala priporočila Banke Slovenije in Združenja bank Slovenije ter strategijo nadaljnjega razvoja hranilnice (Politika varovanja, 2006, str. 2).

Poleg omenjenih dveh dokumentov, ki sta zaupne narave in namenjena ozkemu krogu zaposlenih, ki načrtujejo in izvajajo politiko varovanja, pa je hranilnica pripravila še Pravilnik o varovanju in zaščiti informacijskega sistema in podatkov, ki ga morajo poznati in upoštevati vsi zaposleni v hranilnici. Namen pravilnika je določitev predmetov, postopkov in organizacije za zaščito in varovanje informacijskega sistema in podatkov v hranilnici. Pravilnik je interni akt za zaposlene in dopolnjuje zaupni dokument - Politika varovanja, ki je krovni dokument za varovanje informacijskega sistema in podatkov v hranilnici. Cilj seznanitve zaposlenih s postopki je preprečitev neodgovornega, nepooblaščenega in zlonamernega ravnanja s programsko, strojno in komunikacijsko opremo.

4.10.2 Organiziranost in delovanje službe informatike

Informatika v hranilnici je organizirana v okviru službe informatike, ki jo upravlja svetovalec uprave za informatiko in vanjo sodijo informatiki - sistemski administratorji. Poglavitna naloga svetovalca uprave je načrtovanje strategije razvoja informatike ter izvajanje le-te, naloga sistemskih administratorjev pa je podpora sistemom, procesom in uporabnikom v skladu s sprejetimi politikami in z navodili v hranilnici.

V dinamičnem razvojnem okolju je pomembno, da informatika v hranilnici ne pozabi na varovanje informacijskega sistema. Informatika v hranilnici zato poleg tekočih aktivnosti opravlja dnevni formalni nadzor vseh ključnih informacijskih virov. Redni pregledi sicer vzamejo veliko časa, vendar hranilnici zagotavljajo zgodnje odkrivanje morebitnih napak, napadov ali vdorov v sistem ter omogočajo hitro zaščito in kasnejše okrevanje sistema. Vsa dokumentacija službe informatike se nahaja na skupnem portalu, ki je dostopen samo zaposlenim v informatiki. Na ta način se hranilnica približuje zahtevam standarda ISO/IEC 27001:2006 z željo po vzpostavitvi ISMS sistema, ki zagotavlja učinkovito prepletanje treh ključnih virov: procesov, tehnologije in obnašanja kadra (Haren, 2006, str. 11).

4.10.3 Dograditev, zamenjava in odpis opreme

V skladu s politiko varovanja in pravilnikom o zaščiti in varovanju informacijskega sistema vse posege na strojni opremi izvajajo izključno informatiki v hranilnici oz. pooblaščeni zunanji izvajalci ob nadzoru informatikov. Odpis opreme se izvaja po ustaljenem postopku, ki zahteva predhoden in nepovraten izbris vseh podatkov in programske opreme, ustrezno uničenje opreme ter izdelavo zapisnika komisije za odpis.

4.10.4 Razvoj, testiranje in uvedba programske opreme

Zelo pogost vzrok za nedelovanje informacijskih sistemov so neprimerni postopki in neprimerne prakse pri nadgraditvi in popravkih programske opreme. Hranilnica beleži zelo hiter, praktično neprekinjen razvoj bančnega informacijskega sistema Hibis, ki se razvija zaradi sistemskih in komercialnih zahtev. Ustrezna politika nadgraditev in popravkov, tako imenovani »change management«, je obvezen del teh procesov. Za ta namen ima hranilnica organizacijsko določene vsebinske skrbnike, ki so odgovorni za razvoj in testiranje sprememb v testnem okolju. Informatika v hranilnici zagotavlja testno okolje, kjer se vse spremembe predhodno preverjajo s strani vsebinskih skrbnikov. Prenos v produkcijsko okolje hranilnice je mogoč samo na podlagi zapisnika o testiranju posameznih popravkov ali nadgraditev ter zahtevka za prenos v produkcijo, ki ga podpiše pooblaščen vsebinski skrbnik. Spremembe brez testiranja in potrditve skrbnika niso mogoče.

4.10.5 Izobraževanje in ozaveščanje uporabnikov

Neozaveščeni in neusposobljeni uporabniki so najšibkejši člen v varovanju informacijskega sistema in podatkov. Kljub vsem internim aktom, ki predpisujejo pravila za zagotavljanje varnosti, je zelo pomembno, da se uporabniki nevarnosti zavedajo in interne akte tudi v resnici dosledno upoštevajo. S tem namenom hranilnica izvaja redna letna izobraževanja uporabnikov s področja uporabe informacijske tehnologije in zagotavljanja varnosti. Informatika v hranilnici beleži vse klice in vsako pomoč uporabnikom ter na podlagi evidenc ugotavlja potrebe po izobraževanju in izpopolnjevanju določenih uporabnikov. Iz evidenc je razvidno, da se napake pogosto pojavljajo samo pri nekaterih uporabnikih, zato je potrebno tem posvetiti več časa za izobraževanje.

4.10.6 Upravljanje s projekti

Z rastjo hranilnice in večjimi projekti, kot je bil prehod na evro, se je povečala tudi potreba po boljšem upravljanju projektov. Hranilnica je s tem namenom uvedla Politiko za vodenje projektov, ki opredeljuje postopke in dokumentacijo, ki je potrebna za upravljanje projektov v hranilnici.

4.10.7 Upravljanje z informacijskimi tveganji

Hranilnica ima vzpostavljen sistem upravljanja informacijskih tveganj. Tveganje nadzoruje z rednim preverjanjem informacijskega sistema, s samoocenjevanjem ter s poročanjem o vseh operativnih dogodkih na področju informatike Službi za upravljanje tveganj v hranilnici.

Hranilnica obvladuje informacijska tveganja:

- s sprejemom tveganja, kadar je pričakovana škoda informacijskega tveganja manjša od ocenjenih stroškov za obvladovanje tveganja, zato vzpostavi nadzor in preventivo;

- z zmanjševanjem tveganja, kadar obstajajo možnosti znatnega zmanjšanja velikosti informacijskega tveganja z investicijami v opremo in znanje;
- s prenosom tveganja, kadar so predvideni stroški prenosa tveganja manjši od predvidene škode, ki bi lahko nastala ob uresničitvi tveganja; hranilnica tako prenese izvajanje nekaterih poslovnih procesov (ki niso ključni) s pripadajočimi tveganji in s pokrivanjem morebitne škode na drugega izvajalca;
- z izognitvijo tveganju, kadar je pričakovana škoda večja od koristi aktivnosti; hranilnica zato kritični sistem ali dejavnost ukine.

Hranilnica zmanjšuje in prenaša tveganje na področju informatike z:
- razvojem in investiranjem v informacijsko tehnologijo,
- izboljšavo procesov in dograditvijo dokumentacije,
- ustrezno kadrovsko politiko,
- upoštevanjem standardov in priporočil,
- uporabo in nadzorom zunanjih izvajalcev,
- varovanjem osebnih podatkov in poslovnih skrivnosti,
- načrtovanjem neprekinjenosti poslovanja,
- uporabo zavarovanj.

4.11 Načrtovanje neprekinjenega poslovanja

Različni tipi katastrof, ki so lahko posledica naravnih in drugih nesreč ali so povzročeni s strani napak zaposlenih oz. vdorov napadalcev, lahko ohromijo ali v celoti zaustavijo poslovanje hranilnice, kar lahko v najslabšem primeru vodi tudi v propad in zaprtje hranilnice. Najpogostejši vzroki za večje prekinitve so lahko: poplava, požar, potres, električni sunki in strele, eksplozije plina, teroristična dejanja, politični nemiri, izpadi sistema zaradi človeške napake, okvare naprav, izguba podatkov, vdor v informacijski sistem, itd.

Banke in hranilnice, ki imajo poslovanje podprto z informacijsko tehnologijo morajo zagotavljati neprekinjenost poslovanja. To lahko dosežejo s (Javornik, 2005, str. 4):
- podvojenostjo zmogljivosti na različnih lokacijah,
- podvojenim procesiranjem,
- podvojenimi komunikacijami,
- podvojenim hranjenjem podatkov.

Hranilnica mora preživeti tudi, če se pojavijo naravne ali druge nesreče, ki povzročijo izpad dela ali celotnega informacijskega sistema. Hranilnica danes še nima vzpostavljenega rezervnega centra, ima pa izdelan Plan neprekinjenega poslovanja, ki je omejen na zagotovitev postopkov ob izpadih delov sistema, in Načrt okrevanja po katastrofi, ki predvideva okrevanje informacijskega sistema na primarni lokaciji. Hranilnica že izvaja projekt neprekinjenega poslovanja, ki vključuje vzpostavitev rezervne lokacije s podvojenimi zmogljivostmi. Pri izvedbi projekta hranilnica upošteva Metodologijo načrtovanja neprekinjenega poslovanja in vzpostavitev rezervnih zmogljivosti (Banka Slovenije, 2005).

4.11.1 Plan neprekinjenega poslovanja

Hranilnica ima izdelan Plan neprekinjenega poslovanja (BCP - Business Continuity Plan), ki natančno opredeljuje postopke, ki jih morajo zaposleni in posamezniki upoštevati ob nedelovanju informacijskega sistema. Namen plana je, da se poskuša v najkrajšem času vzpostaviti ključne funkcije, potrebne za poslovanje hranilnice v kritičnih razmerah. Hranilnica se zaveda, da je trenutni plan zelo omejen, zato v projektu vzpostavitve rezervnega centra načrtuje njegovo nadgradnjo z dograditvijo načrta za del, ki se nanaša na okrevanju na rezervni lokaciji. V planu bodo opredeljeni kritični in vitalni poslovni procesi, ki morajo biti zaščiteni pred večjimi nesrečami in katastrofami. Kritičnost poslovnih funkcij je hranilnica določila na podlagi Analize vplivov na poslovanje (BIA - Bussines Impact Analysis), kjer je skupina strokovnjakov hranilnice ovrednotila vpliv na poslovne procese glede na najdaljše dopustne čase prekinitve. Z omenjeno analizo, ki jo je potrdila uprava, je hranilnica prepoznala poslovne procese, ki so nujno potrebni za zagotavljanje neprekinjenosti poslovanja hranilnice ob katastrofi na primarni lokaciji v Ljubljani ter so potrebni za preživetje hranilnice. Pri prenovi plana bo hranilnica upoštevala ISO/IEC 17799:2005 kontrole, ki so navedene v poglavju A.14. - Business Continuity Management (Calder, Watkins, 2006, str. 315).

4.11.2 Načrt okrevanja po katastrofi

Hranilnica ima izdelan Načrt okrevanja po katastrofi (DRP - Disaster Recovery Plan), ki predvideva postopke za okrevanje posameznih delov informacijskega sistema, ne vključuje pa jasno določene vloge posameznikov. Če je Plan za neprekinjeno poslovanje usmerjen v čimprejšnjo nadaljevanje poslovnih procesov, pa je Načrt za okrevanje po katastrofi usmerjen v reševanje življenj (evakuacijo ljudi) in sistemov (zaustavitev sistemov) ter vključuje postopke, ki to natančno opredeljujejo. Običajna praksa je, da se, če pride do katastrofe, najprej izvede načrt in šele nato plan. Če je časa za obnovo malo, se lahko izvajata oba vzporedno (White, 2006, str. 408). Hranilnica bo v omenjenem projektu morala posodobiti Načrt za okrevanje po katastrofi na način, ki bo obravnaval zaščito ljudi in sistemov ter njihovo okrevanje na rezervni lokaciji.

4.11.3 Rezervna lokacija

Hranilnica je v fazi načrtovanja rezervne lokacije, na kateri bo vzpostavljen rezervni računalniški center s podvojeno opremo in s podvojenimi komunikacijami. Po projektni dokumentaciji se predvideva, da bo rezervni center vzpostavljen do poletja 2008, v celoti pa bo operativen in podprt z vsemi načrti do konca leta 2008. Hranilnica ima izbrano lokacijo, kjer so v fazi izgradnje novi poslovni prostori, ki bodo omogočali postavitev rezervne lokacije za kritične podporne službe in rezervni računalniški center. Pri izgradnji in opremljenosti prostorov bo hranilnica upoštevala že prej omenjene mednarodne standarde in priporočila Združenja Bank Slovenije. V omenjenem projektu hranilnica trenutno načrtuje rešitev za zagotovitev podvojenosti kritičnih delov informacijskega sistema in komunikacij na rezervni lokaciji.

5 ANALIZA TVEGANJ INFORMACIJSKEGA SISTEMA

Osnovni pojmi

Vir je stvar oz. predmet, ki ga obravnavamo pri analizi tveganj. Med informacijske vire štejemo komunikacijske povezave, strojno opremo, programsko opremo ali posamezne informacijske podsisteme, baze podatkov, kadre oz. človeške vire in dokumentacijo.

Grožnja je dogodek ali okoliščina, ki bi lahko šla v sistemu narobe (požar, poplava, vdor napadalca, okvara opreme itd.) in bi posledično povzročila izpad informacijskih virov ter škodo pri poslovanju. Grožnje so prisotne v vsakem informacijskem sistemu (Calder, Watkins, 2006, str. 79).

Ranljivost je slabost posameznega informacijskega vira, ki jo izkorišča grožnja (odprti nepotrebni vhodi na požarni pregradi, uporaba slabih gesel, nezavarovani podatki, slabo poučeni uporabniki itd.). Sistem je bolj ranljiv, kadar obstaja večja verjetnost, da se določena grožnja resnično izvede. Tveganje je verjetnost, da se zaradi ranljivosti posameznega informacijskega vira določena grožnja tudi uresniči. Tveganja moramo upravljati in zmanjševati, vendar se jim ne moremo v celoti izogniti. Ukrep je dejanje, varovalni ali zaščitni mehanizem, s katerim poskušamo z zmanjšanjem ranljivosti posledično zmanjšati tudi posamezno tveganje.

Namen analize

Analiza tveganj je osnovni postopek za sistematično preverjanje in ocenjevanje varnosti informacijskega sistema glede na grožnje in ranljivosti, ki so za vsako podjetje ali organizacijo različne. Ocena analize tveganj je ključnega pomena za odločitve poslovodstva o uvedbi zaščitnih ukrepov oz. za sprejem, prenos ali izognitev tveganjem na področju varnosti informacijskih sistemov. Zelo pomembno je, da so zaščitni ukrepi in njihovi stroški prilagojeni posameznim tveganjem, ki jim je podjetje izpostavljeno (Calder, Watkins, 2006, str. 74).

Z analizo tveganj sistematično opredelimo informacijske vire in grožnje, ki jim pretijo, ter na ta način podrobno spoznamo naravo in strukturo tveganj. Izvedba analize tveganj in poznavanje metodologije ocenjevanja prispevata k razumevanju izpostavljenosti in bistveno pripomoreta h kakovostnim odločitvam poslovodstva glede načina in obsega obvladovanja tveganj. Ocenjevanje in analiza tveganj je eden od osnovnih in prvih korakov, ko ugotavljamo skladnost varovanja podatkov in informacij s skupino standardov ISO 27000. Že ISO/IEC 27001 v poglavju o postavitvi in upravljanju ISMS sistema govori o zahtevi po določitvi metode ocenjevanja in analiziranja tveganj. Ocenjevanje in analiziranje tveganj je rdeča nit cele družine standardov ISO 27000, zato je ključnega pomena, da izberemo in uvedeno metodo, ki je jasna, učinkovita in ekonomična. Redkokdaj analiziramo vsa tveganja. Največkrat se odločimo podrobneje analizirati le zelo velika in velika tveganja, manjša pa sprejmemo (Potočnik, 2006, str. 1).

Periodično izvajanje analize tveganj v hranilnici zvišuje nivo varnosti in prinaša dodatne prednosti, kot so:

- hranilnica ima izdelano oceno izpostavljenosti sistema,
- hranilnica porablja sredstva in človeške vire za najbolj tvegana področja,
- hranilnica na podlagi izdelane analize tveganj osvežuje in prilagaja varnostno politiko in druge interne akte ter izboljšuje zaščitne mehanizme,
- hranilnica izvaja ustrezno izobraževanje zaposlenih,
- hranilnica zagotavlja skladnost z zgoraj omenjenimi standardi.

Opis postopka analize

Uporaba kvalitativnega načina

Pri izdelavi analize tveganj obstaja več različnih načinov, ki se v osnovi delijo glede na obseg izgube in glede na kakovost varovanja. Pri prvi metodi (kvantitativen pristop) se uporabita dva osnovna elementa. To sta: verjetnost nekega dogodka, da se bo zgodil, in predvidena škoda, ki bi nastala, če bi se dogodek res zgodil. Ta pristop analize tveganj uporablja oceno stroškov, ki jo dobimo z zmnožkom predvidene izgube in verjetnosti. Težava pri tej metodi analize je v nezanesljivosti predvidenih podatkov. Druga metoda (kvalitativen pristop) je v praksi največkrat uporabljena za analizo tveganj. Pri tej metodi podatki o verjetnosti niso potrebni, ampak ocenimo samo predvideno škodo (Calder, Watkins, 2006, str. 78).

Analizo tveganj na primeru Delavske hranilnice sem izdelal s kvalitativno metodo v treh korakih. V prvem koraku sem popisal vse informacijske vire v okolju hranilnice ter ocenil zahtevano stopnjo varnosti za vsak posamezen vir. Vire sem ocenjeval glede na tri temeljne zahteve informacijske varnosti:

- zaupnost (označena s črko Z),
- neokrnjenost (označena s črko N),
- razpoložljivost (označena s črko R).

Pri tem sem upošteval predvsem vpliv virov na:

- finančni rezultat poslovanja,
- ogrožanje zaposlenih in komitentov hranilnice,
- izgubo poslovnih priložnosti,
- zmanjšanje operativne učinkovitosti in uspešnosti,
- možnost zastoja poslovanja,
- kršitev zakonskih in pogodbenih obveznosti,
- izgubo ugleda hranilnice in zaupanja komitentov.

V drugem koraku sem z oceno groženj in ranljivosti za vse tri temeljne zahteve izračunal oceno ogroženosti posameznega vira. V zadnjem koraku sem določil prevajalno tabelo, ki daje oceno tveganja za posamezni vir glede na zahtevano stopnjo varnosti ter oceno ogroženosti. Tabela je narejena tako, da se ocena tveganj giblje med 1 in 10. Podrobnosti o izvedbi sem zapisal v nadaljevanju.

Proces ocenjevanja zahtevane stopnje varnosti virov

Za posamezne vire, zapisane v strukturi, kot jo prikazuje Tabela 3, sem določil zahtevano stopnjo varnosti, ki naj bi jo imeli glede na tri temeljne zahteve varnosti: zaupnost, neokrnjenost in razpoložljivost. Ocena, vpisana v zadnji stolpec, izraža pomembnost posameznega vira za poslovanje hranilnice.

Zahtevano stopnjo varnosti virov sem ocenjeval z naslednjimi ocenami (1-4):

- 1 - malo pomembna,
- 2 - srednje pomembna,
- 3 - zelo pomembna,
- 4 - izredno pomembna (kritična).

Tabela 3: Primer ocenjevanja zahtevane varnosti informacijskega vira

Vir	Opis vira	Ocena zahtevane varnosti
Prenosne delovne postaje	Prenosni računalniki	Z:4
		N:4
		R:2

Vir: Lasten.

Proces ocenjevanja ogroženosti virov

V nadaljevanju ocenjevanja sem za vse informacijske vire izdelal oceno ogroženosti na način, da sem najprej prepoznal vse pomembnejše grožnje za vsak posamezen vir, nato pa sem ocenil velikost grožnje ter ranljivost vira glede na tri temeljne zahteve varnosti: zaupnost, neokrnjenost in razpoložljivost.

Pri vrednotenju groženj sem upošteval predvsem:

- težavnost udejanjenja grožnje,
- pogostost grožnje,
- vpliv grožnje na poslovanje,
- obstoječe zaščitne ukrepe.

Grožnje sem ocenil z ocenami (0-4):

- 0 - zanemarljiva,
- 1 - majhna,
- 2 - srednja,
- 3 - zelo velika,
- 4 - izredno velika.

Pri vrednotenju ranljivosti vira sem upošteval:

- kako težko je izkoristiti ranljivost,
- ali ranljivost traja ves čas,

- ali lahko izkoriščanje ranljivosti vpliva na poslovanje hranilnice,
- obstoječo zaščito in varovanje vira,
- samo tiste ranljivosti, ki se tudi v resnici pojavljajo,
- dejstvo, da so različni viri izpostavljeni različnim grožnjam.

Ranljivosti virov sem ocenil z naslednjimi ocenami (0-4):

- 0 - zanemarljivo ranljiv,
- 1 - malo ranljiv,
- 2 - srednje ranljiv,
- 3 - zelo ranljiv,
- 4 - izredno ranljiv.

Tabela 4: Primer ocenjevanja ogroženosti informacijskega vira

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg	3	Prenos opreme izven varovanih področij	Z:3	Z:6
				N:3	N:6
				R:1	R:4

Vir: Lasten.

Oceno ogroženosti posameznega vira sem zapisal v strukturi, kot je prikazana na primeru prenosne delovne postaje v Tabeli 4. Dobil sem jo tako, da sem seštel oceno grožnje in oceno ranljivosti vira ter podatek vpisal v zadnji stolpec v tabeli.

Proces ocenjevanja tveganj virov

Za določitev ocene tveganj sem izdelal prevajalno matriko, ki je prikazana v Tabeli 5, kjer je določena ocena tveganja za posamezni vir glede na zahtevano stopnjo varnosti, in oceno ogroženosti vira. Tabela je narejena tako, da se tveganja vrednotijo z utežmi (0-2) glede na zahtevano stopnjo tveganja. Ocene tveganj se gibljejo od najmanjših (1) do največjih (10).

Tabela 5: Primerjalna tabela za določitev ocene tveganj

Ocena zahtevane varnosti	Ocena ogroženosti							
	1	2	3	4	5	6	7	8
1	1	1	2	2	3	4	5	6
2	1	2	2	3	5	6	7	8
3	2	3	4	5	6	7	8	9
4	3	4	5	6	7	8	9	10

Vir: Lasten.

Oceno tveganja, kot jo prikazuje Tabela 6, sem dobil na podlagi ocen zahtevane stopnje varnosti in ocen ogroženosti informacijskega vira.

Tabela 6: Primer ocene tveganja za informacijski vir

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg	Z:4	Z:6	Z:8
		N:4	N:6	N:8
		R:2	R:4	R:3

Vir: Lasten.

Na podlagi ocene tveganj sem določil velikost tveganja:

- 1 - 2 tveganje je zanemarljivo majhno,
- 3 - 4 tveganje je majhno, priporočen je periodičen nadzor,
- 5 - 6 tveganje je srednje, priporočen je reden nadzor vira,
- 7 tveganje je srednje veliko, potrebno je izboljšati zaščito ali nadzor vira,
- 8 tveganje je veliko - ni sprejemljivo, potrebno je izboljšati zaščito vira,
- 9 - 10 tveganje je izredno - kritično, zahteva se takojšnje ukrepanje.

Rezultati analize v nadaljevanju prikazujejo ocene tveganj posameznih virov. Tveganja od 1 do 2 so zelo majhna. Tveganja, ocenjena od 3 do 4, so sicer majhna, vendar je vseeno priporočljiv periodičen nadzor. Tveganja, razvrščena od 5 do 6, se smatrajo kot srednja tveganja, vendar lahko zelo hitro prerastejo v velika tveganja, zato zahtevajo reden nadzor. Tveganja, ovrednotena z oceno 7, so mejna in zahtevajo izboljšanje zaščite ali nadzora. Posebno pozornost je potrebno nameniti tveganjem, ocenjenih od 8 do 10, ki zahtevajo ukrepe.

Analiza tveganja na primeru Delavske hranilnice

Obseg analize

Analiza tveganja informacijskega sistema obsega pregled varnosti vseh ključnih informacijskih virov hranilnice, kot so:

- komunikacijske povezave in oprema,
- strojna oprema,
- operacijski sistemi,
- baze podatkov,
- programska oprema,
- kadri,
- dokumentacija.

Popis virov prikazuje Tabela 7 (na str. 53). Analiza ne obsega pregleda varnosti prostorov in opreme, ki jo hranilnica zagotavlja z vzpostavljenimi sistemi fizičnega in tehničnega varovanja. Smatra se, da hranilnica prostore in opremo varuje ustrezno.

Popis informacijskih virov

Tabela 7: Popis informacijskih virov

Tip vira	Vir
Komunikacijske povezave in oprema	Poslovno omrežje hranilnice
	Partnerske povezave
	Internet povezave
	Navidezne zasebne povezave
	Požarna pregrada
	Usmerjevalniki in stikala
	Kritični usmerjevalniki in kritična stikala
	Fizično ožičenje
Strojna oprema	Delovne postaje
	Kritične delovne postaje
	Prenosne delovne postaje
	Strežniki za bančno poslovanje
	Sistemski strežniki
Operacijski sistemi	Microsoft Windows XP / 2000
	Microsoft Windows Server 2003
	Suse Linux 10 Enterprise Edition
Baze podatkov	Oracle
Programska oprema	Microsoft Office
	NOD32 Antivirus
	Microsoft Internet Explorer
	Adobe Acrobat Reader
	ZBS program za izračun EOM
	IBON program za boniteto
	Microsoft Visio
	PGP program za šifriranje
	Bančni informacijski sistem Hibis
	Spletni banki Dh-Net in Dh-Plus
	Swift Alliance Entry
	Giro kliring
	Connect Direct
	Spletni portal
	Elektronska pošta
Kadri	Ključni kadri
	Ostali zaposleni
Dokumentacija	Politike in strategije
	Ostali interni akti
	Uporabniški dokumenti

Vir: Lasten.

Ocena glede zahtevane stopnje varnosti virov

Za navedene informacijske vire sem določil zahtevano stopnjo varnosti s stališča zaupnosti, neokrnjenosti in razpoložljivosti. V Tabeli 8 sem navedel zbirni pregled zahtevane stopnje varnosti virov, podrobna ocena za vsak vir se nahaja v Prilogi 1.

Tabela 8: Zbirni pregled zahtevane stopnje varnosti virov

Vir	Opis vira	Ocena zahtevane varnosti
Komunikacije	Poslovno omrežje hranilnice, partnerske povezave, internetne povezave, navidezne zasebne povezave	Z:4
		N:2-4
		R:2-4
Komunikacijska oprema	Požarna pregrada, usmerjevalniki in stikala, kritični usmerjevalniki in kritična stikala, fizično ožičenje	Z:2-4
		N:2-4
		R:3-4
Delovne postaje	Delovne postaje, kritične delovne postaje, prenosne delovne postaje	Z:2-4
		N:3-4
		R:2-4
Strežniki	Strežniki za bančno poslovanje, sistemski strežniki	Z:4
		N:4
		R:3-4
Operacijski sistemi	Windows XP / 2000, Windows Server 2003, Suse Linux 10	Z:4
		N:4
		R:3-4
Baze podatkov	Oracle	Z:4
		N:4
		R:4
Uporabniški programi	Microsoft Office, NOD32 Antivirus, Internet Explorer, Acrobat Reader, ZBS EOM, IBON, Microsoft Visio, PGP	Z:1-4
		N:2-4
		R:1-3
Bančni sistemi	Bančni informacijski sistem Hibis, spletni banki Dh-Net in Dh-Plus	Z:4
		N:4
		R:4
Plačilni sistemi	Programska oprema za Swift, plačilni sistem Giro kliring, Connect Direct za Bankart	Z:4
		N:4
		R:4
Elektronski sistemi	Spletni portal, elektronska pošta	Z:3-4
		N:4
		R:3
Kadri	Ključni kadri, ostali zaposleni	Z:3-4
		N:2-4
		R:2-3
Dokumentacija	Politike in strategije, ostali interni akti, uporabniški dokumenti	Z:2-4
		N:2-4
		R:2-4

Vir: Lasten.

Ocena ogroženosti virov

V drugem koraku analize sem ocenil ogroženost posameznih virov. Tabela 9 prikazuje zbirno oceno ogroženosti za vse pomembnejše skupine informacijskih virov ter njihove glavne grožnje. Največjo grožnjo razpoložljivosti vsem ključnim virom v hranilnici predstavljajo naravne in druge nesreče (katastrofe), ki izhajajo iz ranljivosti, da hranilnica še nima vzpostavljenega rezervnega informacijskega sistema na rezervni lokaciji. Kot taka hranilnica kljub izdelanemu načrtu za okrevanje ni v stanju v zelo kratkem času vzpostaviti rezervni informacijski sistem na drugi lokaciji. Podrobna ocena ogroženosti vseh virov se nahaja v Prilogi 1, točka 2.

Tabela 9: Zbirni pregled ogroženosti informacijskih virov

Vir	Glavne grožnje	Ocena ogroženosti
Komunikacijske povezave	Prekinitev povezave, naravne nesreče, prisluškovanje prenosu, prestrezanje in spreminjanje sporočil, nepooblaščen dostop	Z:2-4
		N:2-4
		R:2-6
Požarna pregrada	Naravne in druge nesreče, onemogočanje dostopov zaradi napadov, vdor v omrežje po pregradi	Z:2-5
		N:2-5
		R:3-6
Usmerjevalniki in stikala	Naravne in druge nesreče, prevzem nadzora nad opremo, odpoved strojne opreme	Z:2-4
		N:2-4
		R:3-6
Fizično ožičenje	Namestitev naprave za prisluškovanje, namerna onesposobitev omrežja	Z:1-4
		N:1-4
		R:2-3
Delovne postaje	Neprimerno ravnanje uporabnikov, odtujitev opreme ali nepooblaščen poseg, okvara opreme, izpad električnega napajanja	Z:2-3
		N:3-5
		R:3
Kritične delovne postaje	Okvara opreme, naravne in druge nesreče, odtujitev opreme ali nepooblaščen poseg	Z:2-3
		N:2-4
		R:3-5
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg, okvara opreme	Z:2-6
		N:2-6
		R:3-4
Strežniki za bančno poslovanje	Naravne in druge nesreče, odzivnost pogodbenih vzdrževalcev, okvara opreme	Z:2-3
		N:2-3
		R:3-6
Sistemski strežniki	Naravne in druge nesreče, okvara opreme	Z:1-2
		N:2-3
		R:3-6
Operacijski sistemi delovnih postaj	Nepooblaščen dostop, napad zlonamerne programske opreme	Z:4-5
		N:4-5
		R:4
Operacijski sistemi strežnikov	Nestrokovno delo in napake skrbnikov, nepooblaščen dostop, sabotaža	Z:3-5
		N:3-5
		R:3-5

Tabela 9 - nadaljevanje		
Baze podatkov	Nepooblaščen dostop, nedelovanje baze, izguba podatkov, nestrokovno delo in napake skrbnikov,	Z:1-5 N:2-5 R:3-4
Uporabniški programi	Napake v programski opremi, napad zlonamerne programske opreme, neučinkovitost antivirusne zaščite	Z:1-5 N:1-5 R:2-4
PGP program za šifriranje	Napadi na šifrirne metode in ključe, napake v nastavitvah in programski opremi	Z:3-4 N:3-4 R:2-3
Bančni informacijski sistem Hibis	Napake v programskih modulih, naravne in druge nesreče, nepooblaščen dostop do modula	Z:2-5 N:2-5 R:3-6
Spletni banki Dh-Net in Dh-Plus	Napad zlonamerne programske opreme, nepooblaščen dostop ali vdor, naravne in druge nesreče	Z:2-4 N:2-4 R:2-6
Plačilni sistemi	Nepooblaščen dostop ali vdor, naravne in druge nesreče, nestrokovno delo in napake skrbnikov	Z:2-5 N:2-5 R:3-6
Spletni portal, elektronska pošta	Napad zlonamerne programske opreme, nepooblaščen dostop ali vdor	Z:1-5 N:2-5 R:2-5
Ključni kadri	Izdaja poslovne skrivnosti ali osebnih podatkov	Z:2-5 N:3-5 R:3
Ostali zaposleni	Nestrokovno delo, napake pri delu	Z:3-5 N:3-5 R:2-5
Politike in strategije	Neskladnost s cilji in z zakonskimi smernicami	Z:3-5 N:3-4 R:2-5
Ostali interni akti	Pomanjkanje ali slaba kakovost aktov	Z:2-4 N:3-4 R:2-5
Uporabniški dokumenti	Izguba dokumentov	Z:3-4 N:3-4 R:2-4

Vir: Lasten.

Ostale grožnje se razlikujejo glede na posamezen vir. Komunikacijskim napravam in povezavam poleg naravnih nesreč pretijo še prekinitve primarnih povezav tam, kjer niso vzpostavljene rezervne, ter grožnja zaupnosti in neokrnjenosti sporočil zaradi prisluškovanja, prestrezanja ali celo spreminjanja le-teh na povezavah, ki so šifrirane s ključem, ki je poznan tudi pogodbenim izvajalcem. Požarni pregradi zaradi nevarnosti iz svetovnega spleta še prav posebej grozijo napadi, ki lahko onemogočijo dostop do storitev hranilnice, in različni vdori v omrežje hranilnice.

Delovne postaje so izpostavljene neprimerni uporabi s strani uporabnikov, morebitnim okvaram in izpadu električne energije, ker hranilnica zagotavlja neprekinjeno napajanje večinoma samo za kritično opremo. Kritičnim in prenosnim delovnim postajam največkrat grozijo okvare na opremi, odtujitev ali nepooblaščen dostop. Enako velja tudi za večino strežnikov v hranilnici, kjer zaradi zahtevane visoke razpoložljivosti sistemov dodatno grožnjo predstavlja tudi morebitni slab pogodbeni vzdrževalec ali dolg odzivni čas ob okvari.

Operacijski sistemi na delovnih postajah so kljub strogim pravilom, ki jih zagotavlja prijava v domeno, izpostavljeni nevarnosti nepooblaščenega dostopa in napadom z zlonamerno programsko opremo, ker se uporabniki običajno še premalo zavedajo pomembnosti varovanja uporabniških gesel in nevarnosti datotek, ki jih vnašajo s prenosnimi mediji in napravami. Operacijski sistemi na strežnikih so zaradi zahtevnosti sistemov najbolj izpostavljeni morebitnemu nestrokovnemu delu in napakam skrbnikov sistema, ki neposredno ogrožajo razpoložljivost, zaupnost in neokrnjenost sistemov. Podobno velja za baze podatkov in sisteme za upravljanje baz, ki jim dodatno preti grožnja za morebitno nedelovanje baze.

Na področju programske opreme in posameznih informacijskih sistemov poglavitno ogroženost predstavljajo napake v programski opremi ter nepooblaščeni dostopi do aplikacij in podatkov. Uporabniški programi so dodatno izpostavljeni zlonamerni programski opremi, ki ogroža zaupnost in neokrnjenost aplikacij in s tem tudi podatkov. Pri ključnih sistemih, kot je bančni informacijski sistem Hibis, glavno grožnjo predstavljajo naravne in druge nesreče, ki lahko resno ohromijo poslovanje hranilnice, saj ta še nima vzpostavljenega rezervnega sistema. Plačilni sistemi so zelo ranljivi zaradi morebitnega nestrokovnega dela skrbnikov in uporabnikov sistema, ki lahko ob slabem delu ogrozijo zaupnost in neokrnjenost finančnih podatkov ali zmanjšajo razpoložljivost sistema. Ogroženost spletnih bank in spletnega portala v hranilnici je največja zaradi morebitnih napadov zlonamerne programske opreme in nepooblaščenih vdorov v programe, kar se je v Sloveniji že dogajalo.

Najpomembnejši člen vsakega sistema in procesa so človeški viri oz. kadri. Ključni kadri, kot so vodstveni delavci in delavci na pomembnejših delovnih mestih (informatiki, referenti v plačilnem prometu, računovodje itd.), ki imajo dostop do ključnih dokumentov in podatkov v hranilnici, zaradi nezadovoljstva s svojim položajem predstavljajo neposredno grožnjo varovanju poslovne skrivnosti in osebnih podatkov. Pri ostalih zaposlenih, ki opravljajo manj ali srednje zahtevna dela, obstaja grožnja nestrokovnega dela in napak pri dnevnih opravilih, ki imajo lahko velike negativne finančne učinke za hranilnico in so posledica pomanjkanja znanja, strokovnosti ali motiviranosti zaposlenih.

Poglavitne grožnje dokumentaciji, kamor spadajo politike in strategije, interni akti ter uporabniški dokumenti, so neskladnost politik in strategij z zakoni in s predpisi na posameznem področju, pomanjkanje ali slaba kakovost internih aktov ter grožnja izgube uporabniških dokumentov.

Ocena tveganja informacijskega sistema

Oceno tveganj informacijskega sistema sem izvedel v tretjem koraku, ko sem za vsak posamezen informacijski vir ocenil tveganje glede na zahtevano stopnjo varnosti in dejansko ogroženost vira. Zbirno oceno tveganj za skupine virov prikazuje Tabela 10, podrobna ocena vseh virov pa se nahaja v Prilogi 1, točka 3.

Tabela 10: Zbirna ocena tveganj informacijskih virov

Vir	Glavne grožnje	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Komunikacijske povezave	Prekinitev povezave, naravne nesreče, prisluškovanje prenosu, prestrezanje in spreminjanje sporočil, nepooblaščen dostop	Z:2-4	Z:2-4	Z:2-6
		N:2-4	N:2-4	N:2-6
		R:2-4	R:2-6	R:2-8
Požarna pregrada	Naravne in druge nesreče, onemogočanje dostopov zaradi napadov, vdor v omrežje po pregradi	Z:4	Z:2-5	Z:4-7
		N:4	N:2-5	N:4-7
		R:4	R:3-6	R:5-8
Usmerjevalniki in stikala	Naravne in druge nesreče, prevzem nadzora nad opremo, odpoved strojne opreme	Z:4	Z:2-4	Z:4-6
		N:4	N:2-4	N:4-6
		R:3-4	R:3-6	R:4-8
Fizično ožičenje	Namestitev naprave za prisluškovanje, namerna onesposobitev omrežja	Z:2	Z:1-4	Z:1-3
		N:2	N:1-4	N:1-3
		R:3	R:2-3	R:3-4
Delovne postaje	Neprimerno ravnanje uporabnikov, odtujitev opreme ali nepooblaščen poseg, okvara opreme, izpad električnega napajanja	Z:2	Z:2-3	Z:2-3
		N:3	N:3-5	N:3-5
		R:2	R:3	R:3
Kritične delovne postaje	Okvara opreme, naravne in druge nesreče, odtujitev opreme ali nepooblaščen poseg	Z:4	Z:2-3	Z:4-5
		N:4	N:2-4	N:4-6
		R:4	R:3-5	R:5-7
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg, okvara opreme	Z:4	Z:2-6	Z:4-8
		N:4	N:2-6	N:4-8
		R:2	R:3-4	R:2-3
Strežniki za bančno poslovanje	Naravne in druge nesreče, odzivnost pogodbenih vzdrževalcev, okvara opreme	Z:4	Z:2-3	Z:3-5
		N:4	N:2-3	N:3-5
		R:4	R:3-6	R:5-8
Sistemski strežniki	Naravne in druge nesreče, okvara opreme	Z:4	Z:1-2	Z:3-4
		N:4	N:2-3	N:4-5
		R:3	R:3-6	R:4-7
Operacijski sistemi delovnih postaj	Nepooblaščen dostop, napad zlonamerne programske opreme	Z:4	Z:4-5	Z:6-7
		N:4	N:4-5	N:6-7
		R:3	R:4	R:5-6
Operacijski sistemi strežnikov	Nestrokovno delo in napake skrbnikov, nepooblaščen dostop, sabotaža	Z:4	Z:3-5	Z:5-7
		N:4	N:3-5	N:5-7
		R:3-4	R:3-5	R:4-7
Baze podatkov	Nepooblaščen dostop, nedelovanje baze, izguba podatkov, nestrokovno delo in napake skrbnikov	Z:4	Z:1-5	Z:3-7
		N:4	N:2-5	N:4-7
		R:4	R:3-4	R:5-6

Tabela 10 - nadaljevanje

Uporabniški programi	Napake v programski opremi, napad zlonamerne programske opreme, neučinkovitost antivirusne zaščite	Z:1-4	Z:1-5	Z:1-7
		N:2-4	N:1-5	N:1-7
		R:1-3	R:2-4	R:2-5
PGP program za šifriranje	Napadi na šifrirne metode in ključe, napake v nastavitvah in programski opremi	Z:4	Z:3-4	Z:5-6
		N:4	N:3-4	N:6-6
		R:3	R:2-3	R:3-4
Bančni informacijski sistem Hibis	Napake v programskih modulih, naravne in druge nesreče, nepooblaščen dostop do modula	Z:4	Z:2-5	Z:4-7
		N:4	N:2-5	N:4-7
		R:4	R:3-6	R:5-8
Spletni banki Dh-Net in Dh-Plus	Napad zlonamerne programske opreme, nepooblaščen dostop ali vdor, naravne in druge nesreče	Z:4	Z:2-4	Z:4-6
		N:4	N:2-4	N:4-6
		R:4	R:2-6	R:4-8
Plačilni sistemi	Nepooblaščen dostop ali vdor, naravne in druge nesreče, nestrokovno delo in napake skrbnikov	Z:4	Z:2-5	Z:4-7
		N:4	N:2-5	N:4-7
		R:4	R:3-6	R:5-7
Spletni portal, elektronska pošta	Napad zlonamerne programske opreme, nepooblaščen dostop ali vdor	Z:3-4	Z:1-5	Z:2-7
		N:4	N:2-5	N:4-7
		R:3	R:2-5	R:3-6
Ključni kadri	Izdaja poslovne skrivnosti ali osebnih podatkov	Z:4	Z:2-5	Z:4-7
		N:4	N:2-5	N:4-7
		R:3	R:3	R:3-5
Ostali zaposleni	Nestrokovno delo, napake pri delu	Z:3	Z:3-5	Z:4-6
		N:3	N:3-5	N:2-5
		R:2	R:2-5	R:2-5
Politike in strategije	Neskladnost s cilji in z zakonskimi smernicami	Z:4	Z:3-4	Z:5-7
		N:4	N:3-4	N:5-6
		R:4	R:2-5	R:4-7
Ostali interni akti	Pomanjkanje ali slaba kakovost aktov	Z:2	Z:2-4	Z:2
		N:4	N:3-4	N:5
		R:4	R:2-5	R:4-7
Uporabniški dokumenti	Izguba dokumentov	Z:3	Z:3-4	Z:4-5
		N:3	N:3-4	N:4-5
		R:3	R:2-4	R:3-5

Vir: Lasten

Pri analizi tveganj sem ugotovil, da so tveganja informacijskega sistema Delavske hranilnice pri nekaterih virih tudi srednja in velika, izrednih oz. kritičnih tveganj, ocenjenih z oceno 9 in 10, pa v analizi nisem našel.

Tveganja ocenjena z vrednostjo od 1 do 2, so zelo majhna in zanemarljiva. Tveganja, z oceno od 3 do 4, so majhna, vendar je priporočljiv periodičen nadzor. Tveganja ocenjena z vrednostjo od 5 do 6, se smatrajo kot srednja tveganja, ki lahko hitro prerastejo v velika tveganja, zato zahtevajo reden nadzor. Ker hranilnica izvaja reden dnevni nadzor vseh ključnih informacijskih virov, bom v nadaljevanju izpostavil samo srednje velika in velika tveganja, ki so ocenjena z oceno 7 in več.

Tveganja, ki so prikazana v Tabeli 11, zahtevajo podrobnejšo obravnavo hranilnice.

Tabela 11: Tveganja v hranilnici, ki zahtevajo obravnavo in upravljanje

Ocena tveganja	Vir	Tveganje
Komunikacijske povezave		
8	Partnerske povezave	Veliko tveganje glede razpoložljivosti pri prekinitvi osnovne povezave do procesnega centra (ni rezervne povezave Bankart)
8	Internetne povezave	Veliko tveganje glede razpoložljivosti ob prekinitvi osnovne internetne povezave ali ob naravnih in drugih nesrečah (ni vzporedne povezave z drugim ponudnikom, ni rezervnega sistema)
7	Poslovno omrežje hranilnice	Srednje veliko tveganje glede razpoložljivosti ob prekinitvi osnovnih povezav ali ob naravnih in drugih nesrečah (ni rezervnih povezav do poslovalnic, ni rezervnega sistema)
Komunikacijska oprema		
8	Požarna pregrada, kritični usmerjevalniki in stikala	Veliko tveganje glede razpoložljivosti ob naravnih in drugih nesrečah (ni rezervnega sistema)
8	Požarna pregrada	Veliko tveganje glede razpoložljivosti ob napadih na pregrado, ki onemogočijo druge dostope v omrežje
7	Požarna pregrada	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob vdoru v omrežje po pregradi
Strojna oprema		
8	Strežniki za bančno poslovanje, sistemski strežniki	Veliko tveganje glede razpoložljivosti ob naravnih in drugih nesrečah (rezervni strežniki so na primarni lokaciji, ni rezervnega centra)
8	Prenosne delovne postaje	Veliko tveganje glede zaupnosti in neokrnjenosti ob odtujitvi prenosne postaje ali ob nepooblaščenem posegu (varovanje zaupnosti podatkov hranilnice)
7	Strežniki za bančno poslovanje	Srednje veliko tveganje glede razpoložljivosti ob slabi odzivnosti ali usposobljenosti pogodbenih vzdrževalcev (uporaba zunanjih izvajalcev)
7	Kritične delovne postaje	Srednje veliko tveganje glede razpoložljivosti ob okvari opreme (ni podvojenosti delov)

Tabela 11 - nadaljevanje		
Operacijski sistemi		
7	Operacijski sistemi delovnih postaj	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu (varovanje zaupnosti gesel)
7	Operacijski sistemi strežnikov	Srednje veliko tveganje glede zaupnosti, neokrnjenosti in razpoložljivosti ob nestrokovnem delu in napakah skrbnikov (velika pooblastila, strokovnost)
Baze podatkov		
7	Oracle	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu (varovanje zaupnosti gesel)
Programska oprema		
8	Bančni informacijski sistem Hibis in spletni banki	Veliko tveganje glede razpoložljivosti ob naravnih in drugih nesrečah (rezervni sistemi so na primarni lokaciji, ni rezervnega centra)
7	Microsoft Internet Explorer, elektronska pošta	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob napadu z zlonamerno programsko opremo (varnostni popravki, ozaveščenost uporabnikov)
7	Bančni informacijski sistem Hibis	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu do modula (dodelitev pooblastil za posamezne module)
7	Bančni informacijski sistem Hibis	Srednje veliko tveganje glede zaupnosti, neokrnjenosti in razpoložljivosti ob napakah v programskih modulih (kakovost testiranja)
7	Plačilni sistem Swift	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu do aplikacije plačilnega sistema (dodelitev pooblastil, zunanji izvajalci)
7	Connect Direct	Srednje veliko tveganje glede razpoložljivosti ob naravnih in drugih nesrečah (rezervnega sistema ni)
Kadri		
7	Ključni kadri	Srednje veliko tveganje glede zaupnosti in neokrnjenosti ob izdaji poslovne skrivnosti ali osebnih podatkov (dostop do ključnih podatkov)
Dokumentacija		
7	Politike in strategije	Srednje veliko tveganje glede zaupnosti in razpoložljivosti ob neskladnosti z zakoni in s predpisi (preobremenjenost kadrov, hitre spremembe predpisov)
7	Ostali interni akti	Srednje veliko tveganje glede razpoložljivosti ob pomanjkanju ali slabi kakovosti internih aktov (slabo organiziranje področij)

Vir: Lasten.

6 UKREPI IN PRIPOROČILA ZA IZBOLJŠANJE VARNOSTI

Ukrepi in priporočila za komunikacijske povezave in opremo

Analiza je ugotovila veliko tveganje komunikacijske povezave do procesnega centra Bankart glede razpoložljivosti ob prekinitvi osnovne povezave do procesnega centra. Hranilnica trenutno nima vzpostavljene rezervne povezave, zato bi bilo ob izpadu moteno delovanje bankomatov ter podpore za kartično poslovanje.

Ukrep 1: Hranilnici predlagam, da vzpostavi rezervno povezavo z ISDN priključkom, ki zadošča za potrebe izmenjave podatkov s procesnim centrom, na drugi strani pa omogoča delovanje tudi v izjemnih razmerah, ko druge povezave odpovedo. Istočasno predlagam, da hranilnica ob postavitvi rezervne lokacije vzpostavi najeto povezavo in rezervno ISDN povezavo tudi do rezervnega centra Bankart.

Drugo veliko tveganje je tveganje povezave v internetno omrežje glede razpoložljivosti ob prekinitvi osnovne povezave ali ob naravnih in drugih nesrečah. Hranilnica nima vzpostavljene vzporedne povezave z drugim ponudnikom in je tako v celoti odvisna od enega samega ponudnika, njegovih povezav ter naslovnega prostora.

Ukrep 2: Hranilnici predlagam, da vzpostavi rezervno povezavo v internetno omrežje po optičnem omrežju drugega ponudnika in pri tem zagotovi neodvisni naslovni prostor za dostop do strežnikov hranilnice. Ob vzpostavitvi rezervne lokacije naj hranilnica eno od internetnih povezav preseli na novo lokacijo.

Dodatno je analiza pokazala srednje veliko tveganje poslovnega omrežja hranilnice glede razpoložljivosti ob prekinitvi osnovnih povezav ali ob naravnih in drugih nesrečah. Hranilnica v poslovalnicah, ki se nahajajo po celotni Sloveniji in so povezane z navideznimi povezavami, nima vzpostavljenih rezervnih povezav. Prekinitev posamezne navidezne povezave tako v celoti odreže poslovalnico od informacijskega sistema hranilnice, kar onemogoča delo v bančni aplikaciji Hibis.

Priporočilo 1: Hranilnici predlagam, da preveri druge možnosti za vzpostavitev rezervnih povezav iz poslovalnic do računalniškega centra hranilnice v Ljubljani.

Ocena kritične komunikacijske opreme je izpostavila veliko tveganje kritičnih usmerjevalnikov in stikal ter požarne pregrade glede razpoložljivosti ob naravnih in drugih nesrečah. Hranilnica nima vzpostavljenega rezervnega centra.

Ukrep 3: Hranilnici predlagam, da ob vzpostavitvi rezervne lokacije tudi tam namesti vso kritično komunikacijsko opremo, vključno s požarno pregrado, ki bo povezana v gručo s pregrado v računalniškem centru v Ljubljani.

Ocena požarne pregrade prikazuje veliko tveganje glede razpoložljivosti ob napadih, ki onemogočajo drugim uporabnikom dostop v omrežje hranilnice, s tem pa tudi normalno poslovanje. Napadi so običajno posledica premišljenih dejanj napadalcev, ki z zlonamernimi programi izkoriščajo ranljivost preobremenitve pregrade in povezave. Hranilnica ima vzpostavljen sistem uteži dostopov, ki omejuje posamezne dostope, vendar ni odporen proti napadalcem, ki hitro spreminjajo način napada.

Ukrep 4: Hranilnici predlagam, da nadgradi obstoječi sistem z opremo, ki nudi aktivno zaščito pred napadi že pred požarno pregrado in se je sposobna učiti ter prilagajati glede na zgodovino dostopov. Hranilnica naj izbere in uvede opremo tipa IPS (Intrusion Prevention System), ki bo izboljšala zaščito pred tovrstnimi napadi.

Ocena pregrade dodatno prikazuje srednje veliko tveganje požarne pregrade glede zaupnosti in neokrnjenosti ob vdoru v omrežje po pregrade. Vdori so običajno posledica napadalcev, ki izkoriščajo ranljivost slabo nastavljene politike na požarni pregradi ali pa slabo vzdrževane programske opreme pregrade. Hranilnica vzdrževanje programske opreme pregrade izvaja s pogodbenim izvajalcem, politiko dostopov pa določa sama po sistemu, da je zaprto vse in se omogočajo samo potrebni dostopi. Zaradi različnosti dostopov je dnevni nadzor na pregradi otežen.

Priporočilo 2: Hranilnici predlagam, da periodično pregleduje in preverja vse nastavitve varnostne politike na požarni pregradi ter odstrani vse dostope in morebitne uporabnike, ki se ne uporabljajo več.

Ukrepi in priporočila za strojno opremo

Ocena strežnikov prikazuje veliko tveganje strežnikov za bančno poslovanje in sistemskih strežnikov glede razpoložljivosti ob naravnih in drugih nesrečah. Hranilnica ima zagotovljeno podvojenost vseh ključnih strežnikov, vendar se le-ti nahajajo v računalniškem centru v Ljubljani. Hranilnica nima vzpostavljenega centra na rezervni lokaciji.

Ukrep 5: Hranilnici predlagam, da čimprej vzpostavi center na rezervni lokaciji, kamor premesti vse strežnike, ki jih ima sedaj na osnovni lokaciji. Pri tem mora posodobiti načrt za okrevanje po katastrofi ter izdelati nov načrt za neprekinjeno poslovanje.

Analiza strojne opreme je ugotovila tudi veliko tveganje prenosnih delovnih postaj oz. prenosnikov glede zaupnosti in neokrnjenosti ob odtujitvi prenosne postaje ali ob nepooblaščenem posegu. V hranilnici prenosne računalnike uporablja samo omejeno število uporabnikov, ki prenosnost naprave potrebujejo pri svojem delu. Zavedati se je potrebno, da so to večinoma ključni kadri, ki na prenosne naprave shranjujejo pomembne dokumente in izmenjujejo zaupna sporočila. Varovanje zaupnosti dokumentov na prenosniku je zagotovljeno s šifriranjem podatkov, varovanje razpoložljivosti pa s hranjenjem podatkov na strežniku v hranilnici.

Ukrep 6: Hranilnici predlagam, da zaradi velike izpostavljenosti prenosnikov preveri ustreznost obstoječega zagotavljanja zaupnosti in neokrnjenosti morebitnih podatkov na prenosnih postajah ter preveri možne nove rešitve za izboljšanje zaščite na tem področju.

Ocena tveganja strežnikov za bančno poslovanje je pokazala srednje veliko tveganje glede razpoložljivosti ob slabi odzivnosti ali usposobljenosti pogodbenih vzdrževalcev. Hranilnica za vzdrževanje strojne opreme strežnikov, ki so ključni za delovanje hranilnice, uporablja pogodbenega izvajalca. V pogodbi ima opredeljene roke, ki zagotavljajo najdaljši dopustni čas popravila. Ker se okvare dogajajo dokaj poredko, hranilnica ni prepričana, ali je izvajalec še vedno pripravljen tako, kot je bilo dogovorjeno in kot se od njega pričakuje.

Priporočilo 3: Hranilnici predlagam, da periodično preverja pripravljenost in strokovnost pogodbenega izvajalca, da tako lahko ugotovi, ali je pripravljen za hiter in kakovosten poseg ob okvari kritične strojne opreme. Če hranilnica ugotovi odstopanja od pričakovanj, lahko to preveri tudi pri drugih naročnikih izvajalca ter se odloči za njegovo zamenjavo.

Analiza kritičnih delovnih postaj je ugotovila srednje veliko tveganje glede razpoložljivosti pri okvari strojne opreme postaje. To so običajne postaje, ki se uporabljajo v zalednih službah hranilnice, imajo povezavo do določenih sistemov in aplikacij ter so pomembne za poslovanje hranilnice (plačilni promet, zakladništvo, računovodstvo itd.). Ker tovrstne delovne postaje praviloma nimajo podvojenih delov, tako kot strežniki, je možnost za okvare večja.

Priporočilo 4: Hranilnici predlagam, da za vse kritične delovne postaje preveri, ali so zagotovljene rezervne postaje in ali so zagotovljeni scenariji za prehod nanje. Če niso, naj hranilnica to čimprej zagotovi. Dodatno predlagam, da hranilnica preveri postopke varovanja podatkov in aplikacij na trakovih.

Ukrepi in priporočila za operacijske sisteme

Analiza operacijskih sistemov delovnih postaj je pokazala srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu. Klub dejstvu, da ima hranilnica urejeno politiko in kompleksnost gesel, ki je določena na domenskem strežniku, je vseeno prisotno tveganje nepooblaščenega dostopa, ker se uporabniki v poslovalnicah prijavljajo na različne računalnike ter je prisotno tveganje slabega varovanja gesel.

Priporočilo 5: Hranilnici predlagam, da na letnem izobraževanju zaposlenih posebno pozornost nameni predstavitvi nevarnosti ter dobrih praks na področju varovanja informacijskega sistema.

Ocena tveganj operacijskih sistemov strežnikov prikazuje srednje veliko tveganje glede zaupnosti, neokrnjenosti in razpoložljivosti pri nestrokovnem delu in napakah skrbnikov sistemov. Hranilnica vzdržuje operacijske sisteme strežnikov sama ali s pomočjo pogodbenih izvajalcev. Zaradi velikih pooblastil, ki jih imajo skrbniški računi na strežniku, obstaja tveganje, da skrbnik z nepremišljenim ukazom ali z neprimerno nastavitvijo sistem ogrozi. Hranilnica izvaja reden nadzor pomembnejših dnevnikov operacijskih sistemov.

Priporočilo 6: Hranilnici predlagam, da tako vse morebitne spremembe operacijskega sistema in nastavitev uporabnikov kot tudi namestitve popravkov predhodno dosledno preverja na testnem strežniku ter da vsako spremembo v produkcijskem sistemu predhodno odobri pooblaščena oseba.

Ukrepi in priporočila za baze podatkov

Analiza tveganj baz podatkov je ugotovila srednje veliko tveganje glede zaupnosti in neokrnjenosti pri nepooblaščenem dostopu. Uporabniki se prijavljajo v bančno aplikacijo Hibis z neposredno prijavo v bazo podatkov Oracle. V sistemu za upravljanje baz podatkov je vzpostavljen poseben profil uporabnikov, ki zahteva kompleksnost gesel. Uporabniki so pri svojem delu podrejeni in nadrejeni drugim uporabnikom za zagotavljanje pravila štirih oči, ki ga hranilnica mora zagotavljati.

Priporočilo 7: Hranilnici predlagam, da izboljša sistem nadzora nad prijavami v bazo podatkov na način, da uvede podroben nadzor vseh prijav ter ugotavlja, ali se nekateri uporabniki prijavljajo v sistem z različnih delovnih postaj in druge okoliščine, ki lahko nakazujejo morebitno nenavadno obnašanje uporabnikov.

Ukrepi in priporočila za programsko opremo

Ocena tveganj programske opreme je potrdila veliko tveganje glede razpoložljivosti bančnega informacijskega sistema Hibis in spletnih bank Dh-Plus ter Dh-Net ob naravnih in drugih nesrečah. Rezervni sistem Hibis je vzpostavljen, vendar se nahaja na primarni lokaciji, rezervnega sistema za spletni banki pa hranilnica ta trenutek nima.

Ukrep 7: Hranilnici predlagam, da čimprej vzpostavi rezervno lokacijo, na katero preseli obstoječi rezervni sistem Hibis, in da istočasno vzpostavi rezervni sistem za spletni banki.

Ocena tveganj brskalnika Internet Explorer in programov za elektronsko pošto je opozorila na srednje veliko tveganje glede zaupnosti in neokrnjenosti ob napadu z zlonamerno programsko opremo. Hranilnica ima vzpostavljen ustrezen sistem za antivirusno zaščito in nadgrajevanje varnostnih popravkov. Tveganje večinoma izhaja zaradi neustreznega ravnanja uporabnikov. **Glej priporočilo 5.**

Analiza tveganj bančnega informacijskega sistema Hibis je pokazala srednje veliko tveganje glede zaupnosti in neokrnjenosti ob nepooblaščenem dostopu do programskih modulov. Pooblaščena oseba v hranilnici odobrava pooblastila za dostop uporabnikov do posameznih programskih modulov sistema Hibis, vendar je zaradi hitre rasti števila zaposlenih in razvoja novih modulov zelo težko spremljati in beležiti pooblastila, ki jih imajo uporabniki v sistemu.

Priporočilo 8: Hranilnici predlagam, da v sistemu Hibis preveri pooblastila za vse uporabnike ter spremeni obstoječi obrazec. Nov obrazec mora omogočati večjo sledljivost pri spremembah pooblastil.

Analiza tveganj bančnega informacijskega sistema Hibis je dodatno pokazala srednje veliko tveganje glede zaupnosti, neokrnjenosti in razpoložljivosti ob napakah v programskih modulih. Hranilnica ima določene vsebinske skrbnike in vzpostavljeno testno Hibis okolje, kjer preizkuša vse popravke in nadgradnje preden jih prenese v produkcijsko okolje. Vseeno se zaradi hitrega razvoja programov občasno dogaja, da se na posameznem programskem modulu pojavi napaka.

Priporočilo 9: Hranilnici predlagam, da preveri kakovost testiranja vsebinskih skrbnikov ter jih opozori na omenjeno problematiko. Izboljšanje kakovosti testiranja mora biti razvidno iz zapisnikov testiranja, ki jih na koncu podpišejo skrbniki.

Analiza tveganj programske opreme plačilnega sistema Swift je opozorila na srednje veliko tveganje glede zaupnosti in neokrnjenosti pri nepooblaščenem dostopu do aplikacije. Hranilnica omejuje dostop do aplikacije samo na zaposlene v plačilnem prometu ter na pogodbenega vzdrževalca, ki ima omogočen občasen dostop.

Priporočilo 10: Hranilnici predlagam, da periodično preverja pooblastila vseh uporabnikov in skrbnikov za dostop do aplikacije Swift ter po potrebi omejuje dostop glede na zadolžitve. Pooblastilo za skrbniški dostop morata imeti samo vodja plačilnega prometa in njegov namestnik.

Analiza tveganj programske opreme Connect Direct za prenos podatkov do procesnega centra Bankart je ugotovila srednje veliko tveganje glede razpoložljivosti ob naravnih in drugih nesrečah. Hranilnica ima zagotovljeno varovanje aplikacije, nastavitev in podatkov, vendar nima rezervnega sistema.

Ukrep 8: Hranilnici predlagam, da ob vzpostavitvi rezervne lokacije čimprej zagotovi rezervni sistem Connect Direct, ki bo sposoben v izrednih razmerah izmenjavati podatke z rezervne lokacije hranilnice do centra Bankart.

Ukrepi in priporočila za kadre

Analiza tveganj ključih kadrov je pokazala srednje veliko tveganje glede zaupnosti in neokrnjenosti ob izdaji poslovne skrivnosti. Hranilnica, kot manjša bančna ustanova,

mora voditi poslovne procese z majhnim krogom ljudi, ki so strokovno usposobljeni in imajo dostop do vseh ključnih dokumentov. Zaradi omenjenega je hranilnica izpostavljena tveganju, da bi kdo izmed ključnih kadrov zaradi nezadovoljstva lahko odtujil poslovne dokumente in podatke, ki so mu na voljo.

Priporočilo 11: Hranilnici predlagam, da vse dokumente objavi na informacijskem portalu, kjer zagotovi omejen dostop posameznika glede na njegova pooblastila ter sledljivost dostopa.

Ukrepi in priporočila za dokumentacijo

Ocena tveganj prikazuje srednje veliko tveganje glede zaupnosti in razpoložljivosti politik in strategij pri neskladnosti z zakoni in s predpisi. Zaradi nenehnih in hitrih sprememb zakonodaje in predpisov hranilnica težko sledi vsem tem spremembam.

Priporočilo 12: Hranilnici predlagam, da zadolženi za posamezno področje preverijo, ali je le-to skladno z zahtevami zakonodaje in predpisov ter o tem skupaj s predlogi za spremembe pisno obvestijo vodstvo.

Analiza tveganj je dodatno ugotovila srednje veliko tveganje glede razpoložljivosti internih aktov ob pomanjkanju ali slabi kakovosti internih aktov.

Priporočilo 13: Hranilnici predlagam, da vodje služb preverijo operativna navodila in druge interne akte, ki jih zaposleni potrebujejo pri svojem delu. Vse akte, ki so spoznani za nekakovostne, je potrebno dograditi, morebitne manjkajoče pa pripraviti.

7 SKLEP

V magistrskem delu sem obravnaval varnost informacijskega sistema na primeru Delavske hranilnice. Kot sem opisal že v uvodnem delu, je hranilnica v obdobju hitrega razvoja in prilagajanja sistema evropskim in mednarodnim standardom. Živimo v času, ko so računalniške komunikacije in informacijski sistemi vedno bolj pomembni, kar velja tudi za hranilnico. Ne morem si predstavljati, kako bi danes potekalo poslovanje hranilnice brez ustrezne informacijske podpore. Za normalno poslovanje hranilnice je nujno potrebno z izvajanjem periodičnih pregledov in prilagoditev sistema zagotavljati varnost informacijskega sistema.

Namen magistrskega dela je bil analizirati dele informacijskega sistema ter predlagati ukrepe in priporočila za izboljšanje varnosti ter prilagoditev sistema hranilnice varnostnim zahtevam za bančno poslovanje. V prvem delu sem predstavil informacijski sistem hranilnice, v drugem pa sem kritično opisal zaščito in varovanje posameznih delov sistema. V nadaljevanju sem izvedel analizo informacijske varnosti za celoten sistem hranilnice.

Analiza sistema ni ugotovila kritičnih tveganj, je pa opozorila na sedem velikih tveganj, ki zahtevajo ukrepe, in na petnajst srednje velikih tveganj, ki zahtevajo izboljšanje zaščitnih mehanizmov. Kar pet od sedmih velikih tveganj v celoti ali delno izhaja iz ranljivosti, da hranilnica ta trenutek še nima rezervnega sistema na rezervni lokaciji (projekt vzpostavitve rezervne lokacije sicer teče). Ostala velika tveganja pa opozarjajo na ranljivost požarne pregrade pred morebitnimi napadi, pomanjkanje nekaterih rezervnih povezav ter na nevarnost, ki bi se dogodila ob odtujitvi prenosne delovne postaje. Za srednje velika tveganja velja, da se nanašajo na najpogostejše grožnje kot so vdor v omrežje, nepooblaščen dostop, okvara opreme, nestrokovno delo in napake skrbnikov, napad zlonamerne programske kode, slaba odzivnost pogodbenih vzdrževalcev, izguba podatkov, izdaja poslovne skrivnosti, neskladnost politik z zakoni in s predpisi, pomanjkanje ali slaba kakovost internih aktov.

Skladno z opravljeno analizo sem v zadnjem delu naloge predlagal ukrepe in priporočila za prilagoditev sistema varnostnim zahtevam za bančno poslovanje na primeru hranilnice. Predlagal sem osem ukrepov, ki bi jih hranilnica morala izpolniti za obvladanje velikih tveganj, ter trinajst priporočil, ki bi jih hranilnica morala izvesti za zmanjšanje ugotovljenih srednje velikih tveganj.

Med ukrepi sem predlagal:

- čimprejšnjo vzpostavitev rezervnega sistema na rezervni lokaciji, in sicer s podvojenimi komunikacijskimi povezavami,
- uvedbo rezervne povezave do procesnega centra Bankart,
- uvedbo dodatne zaščite pred požarno pregrado,
- nadgraditev sistema za varovanje podatkov na prenosnikih.

V nadaljevanju sem hranilnici priporočil:

- izvajanje preventivnih pregledov varnostne politike in nastavitev na opremi,
- nadzor varovanja podatkov na kritičnih delovnih postajah in strežnikih,
- preverjanje pripravljenosti in usposobljenosti pogodbenih vzdrževalcev,
- izobraževanje in opozarjanje zaposlenih glede informacijskih tveganj in uporabe informacijskih sistemov,
- dosledno testiranje in uvajanje sprememb v programski opremi in operacijskih sistemih,
- redno preverjanje dnevnikov prijav v informacijske sisteme,
- izboljšanje sistema dodelitve pooblastil za bančno aplikacijo Hibis,
- izboljšanje kakovosti testiranja programskih modulov sistema Hibis,
- periodično preverjanje skladnosti internih aktov z zakoni in s predpisi,
- dosledno omejevanje dostopa uporabnikov do dokumentov, ki jih pri svojem delu ne potrebujejo,
- osveževanje internih aktov.

Ukrepi in priporočila bodo služili vodstvu hranilnice kot osnova za odločanje, ali je potrebno posamezno tveganje zmanjšati z investicijo v zaščitno opremo ali ga obvladati kako drugače.

LITERATURA

1. Anderson L. David: Management Information Systems. New Jersey : Prentice Hall, 2000. 440 str.
2. Bergadano Francesco: Cryptology and network security. Ljubljana : Slovensko društvo informatika, 2002. 345 str.
3. Bratuša Tomaž: Hekerski vdori in zaščita. Druga razširjena izdaja. Ljubljana : Založba Pasedena, 2006. 409 str.
4. Caelli William, Longley Dennis, Shain Michael: Information Security Handbook. London : MacMillan, 1994. 833 str.
5. Champlain J. Jack: Auditing information systems 2nd ed. Hoboken, 2003. 120 str.
6. Cheswick William, Steven M. Bellovin: Firewalls and Internet Security. New York : Adison-Wesley publishing company, 1994. 51 str.
7. Damij Talib: An Object-Oriented Methodology for Information Systems Development and Business Process Reengineering. 2000. str. 23-34.
8. Egan Mark, Mather Tim: Varnost informacij. Grožnje, izzivi in rešitve. Ljubljana : Založba Pasadena, 2005. 269 str.
9. Pete Finnigan: Oracle Security Step-by-Step (Version 2.0). 2004. 249 str.
10. Gallagher Michael: Business Continuity Management; How to protect your company from danger. Edinbourgh : Prenctice Hall, 2003. 172 str.
11. Gordon A. Lawrence et al. : CSI / FBI Computer crime and security survey. Elevent edition. Computer security institute, 2006. 27 str.
12. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju. Ljubljana : Ekonomska fakulteta, 2001. 508 str.
13. Gradišar Miro, Resinovič Gortan: Osnove informatike. Ljubljana : Ekonomska fakulteta, 1993. 334 str.
14. Gril Matej: Varnost in tehnološka zaščita informacijskega sistema v banki. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2003. 90 str.
15. Haren Van: Implementing Information Security Based on ISO 27001 and ISO 17799. A Management Guide, 2006. 71 str.
16. Javornik Boža: Revidiranje v okolju AOP in revidiranje kontrol delovanja informacijskega sistema. Gradivo za izobraževanje za pridobitev strokovnega naziva revizor. Ljubljana : Slovenski inštitut za revizijo, 2005. str. 43-80.
17. Jerman-Blažič Borka et al.: Elektronsko poslovanje na internetu. 1.natis. Ljubljana : Gospodarski vestnik, 2001. 206 str.
18. Jerman-Blažič Borka: Sodobne telekomunikacijske storitve. Literatura predavanj. Ljubljana : Ekonomska fakulteta, 2006.
19. Kajić Milan: Varnostna politika in načrtovanje ukrepov za izredne razmere pri varovanju IS. Organizacija, Kranj, 32(1999), 7, str. 397-402.
20. Kerzner H.: Project Management: A System Approach to Planning, Scheduling, and Controlling. 6th ed. New York : Wiley, 1998. 1180 str.
21. Knox David: Effective Oracle Database 10g Security by Design. Electronic book. California : Oracle Press, 2004. str. 512.
22. Ključevšek Rado: Zanimivosti : kako tvegano je elektronsko bančništvo. Gospodarski Vestnik : Ljubljana, (2002), 48, str. 80.

23. Kovačič Andrej: Prenova in informatizacija delovnih procesov. Ljubljana : Visoka upravna šola, 2002. 124 str.
24. Laudon C. Kenneth, Laudon P. Jane: Management Information Systems. Sixth Edition. London : Prentice Hall International, 2000. 588 str.
25. Lipovec Filip: Razvita teorija organizacije. Maribor : Založba Obzorja, 1987. 365 str.
26. Novaković Sašo: Obvladovanje tveganja na področju IT projektov. Dnevi slovenske informatike. [URL: http://www.ipmit.si], 1999.
27. Ošlak Darinka: Varnost elektronskega poslovanja v slovenskem bančništvu. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2005. 84 str.
28. Panko R. Raymond: Corporate computer and network security. New Jersey : Prentice Hall, 2003. 544 str.
29. Pepelnjak Ivan, Bradeško Marjan: Varnost računalniških sistemov in elektronskih transakcij. Banke in tveganja, Zbornik. Portorož : Zveza ekonomistov Slovenije, 1997, str. 155-165.
30. Perenič Gorazd: Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Ljubljana : Perenič svetovanje, 2001.
31. Pintarič Gašper: Varnost je v zraku. Sistem. priloga Monitorja. Ljubljana, 2007, 1, str. 20-21.
32. Potočnik Marko: Analiza tveganja za odločanje o ravni varovanja informacij. Varnostni forum. Ljubljana, 2006. str. 12.
33. Rajiv Sinha: A Security Checklist for Oracle9i: An Oracle white paper. Redwood Shores, 2001. 10 str.
34. Saje Andrej: ITSM : izkušnje iz prve roke. Sistem. priloga Monitorja. Ljubljana, 2006, 7, str. 18-19.
35. Satzinger John, Jackson Robert, Burd Stephen: System Analysis & Design in a Changing World. Forth Edition. Boston : Thomson Course, 2007. 672 str.
36. Savanovič Damir: Pet nalog informacijske varnosti. Sistem. priloga Monitorja Ljubljana, 2007, 3, str. 10-11.
37. Smith E. Richard: Internet Cryptography. Massachusetts : Addison Wesley Longman Inc., 1997. 356 str.
38. Stewart M. James, Tittel Ed, Chaplle Mike. Cissp. Certified Information Systems Security Professional Study Guide. Third edition. Alameda : Sybex, 2004. 795 str.
39. Toplišek Janez: Elektronsko poslovanje. Ljubljana : Založba Atlantis, 1998. 336 str.
40. Vidmar Tone: Informacijsko-komunikacijski sistemi. priloga Monitorja. Ljubljana, 2002, 823 str.
41. White Gregory. All-in-one Security+ Certification Exam Guide. Emeryville : McGraw-Hill/Osborne, 2003, 558 str.
42. Žnidar Borut: Organizirajte napad. Sistem. Priloga Monitorja. Ljubljana, 2006, 5, str. 18-19.

VIRI

1. Analiza in upravljanje informacijskih tveganj. Gradivo za udeležence. Ljubljana : Združenje bank Slovenije. Izobraževalni center, 2007.
2. AusCert. UNIX and Linux Security Checklist Notes.

[URL: https://www.auscert.org.au], 2007.
3. Basel II (CRD). Banka Slovenije.
   [URL: http://www.bsi.si/poslovanje-bank-in-podjetij], 24.05.2007.
4. Banke vse pogosteje na udaru spletnih napadalcev. E-bančništvo. RIS.
   [URL: http://www.ris.org/novice], 04.09.2006.
5. CIA triad. Are security Model's BanKrupt. Microsoft's Stride Chart. Securology.
   [URL: http://securology.blogspot.com], 2007.
6. Internet Gateway Security to Protect Your Network. eSafe Gateway.
   [URL: http://www.aladdin.com/esafe/gateway-content-security], 2007.
7. Kiber kriminal tudi pri nas, banke brezskrbne. E-bančništvo. RIS.
   [URL: http://www.ris.org/novice], 24.11.2005.
8. Operating System Vulnerability Scorecard. Jeff Jones.
   [URL: http://blogs.technet.com/security/archive], 2007.
9. Personal computer Esprimo. Fujitsu-Siemens.
   [URL: http://www.fujitsusiemens.com/products/deskbound], 2007.
10. Creating, Implementing and Managing the Information Security Lifecycle. TruSecure Corporation Security Solutions, Internet Security Systems.
    [URL: http://www.iss.net/customer_care/resource_center/whitepapers/], 2002.
11. An Introduction to Cryptography. NA - Network Associates: Santa Clara : Network Associates Inc. 1999. 80 str.
12. Okrevalni načrt. Ljubljana : Delavska hranilnica, 2006.
13. Operating system overview. Boran.
    [URL: http://www.boran.com/security/ref erences.html], 2003.
14. Plan neprekinjenega poslovanja. Ljubljana : Delavska hranilnica, 2006.
15. Politika varovanja informacijskega sistema in informacij. Ljubljana : Delavska hranilnica, 2006.
16. Pravilnik o varovanju in zaščiti informacijskega sistema in podatkov. Ljubljana : Delavska hranilnica, 2006.
17. Certifikatska agencija Pošte Slovenije. POŠTA®CA.
    [URL: http://postarca.posta. si/], 4.6.2007.
18. Certifikatska agencija Ministrstva za javno upravo. SIGEN-CA.
    [URL: http://www. sigen-ca.si/], 23.5.2007.
19. SIST ISO/IEC 27001:2006 Information technology. Security techniques. Information security management systems. Requirements Ljubljana : Urad RS za standardizacijo in meroslovje, 2006. 40 str.
20. SIST ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management. Ljubljana : Urad RS za standardizacijo in meroslovje, 2005. 115 str.
21. SIST ISO 17799. Information technology - Code of practice for information security management. Ljubljana : Urad RS za standardizacijo in meroslovje, 2003. 71 str.
22. Smart management. Firewall VPN1.
    [URL: http://www www.centech.com.cn], 2005.
23. Uporabniki bolj zaupajo velikim bankam. E-bančništvo. RIS.
    [URL: http://www.ris.org/novice], 14.04.2005.

24. Varen elektronski podpis kot temelj elektronskega poslovanja. Crea. [URL: http:// www.ltfe.org/pdf/Varen_el_podpis.pdf], 2003.
25. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000, 98/2004).
26. Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 25/2004).

PRILOGA

ANALIZA TVEGANJ INFORMACIJSKEGA SISTEMA NA PRIMERU DELAVSKE HRANILNICE

KAZALO

1 OCENA ZAHTEVANE STOPNJE VARNOSTI INFORMACIJSKIH VIROV

Komunikacijske povezave in oprema

Tabela 1: Ocena zahtevane varnosti komunikacijskih povezav in opreme

Vir	Opis vira	Ocena zahtevane varnosti
Poslovno omrežje hranilnice	Komunikacijske povezave posameznih poslovalnic do računalniškega centra	Z:4
		N:4
		R:3
Partnerske povezave	Povezave za plačilne sisteme in bankomate	Z:4
		N:4
		R:4
Internetne povezave	Povezava do internetnega omrežja	Z:2
		N:2
		R:4
Navidezne zasebne povezave	Povezava za dostop zunanjih izvajalcev	Z:4
		N:4
		R:2
Požarna pregrada	Strojna in programska oprema za požarno pregrado	Z:4
		N:4
		R:4
Usmerjevalniki in stikala	Usmerjevalniki in mrežna stikala v poslovalnicah	Z:4
		N:4
		R:3
Kritični usmerjevalniki in kritična stikala	Usmerjevalniki in mrežna stikala za partnerske povezave in internetno omrežje	Z:4
		N:4
		R:4
Fizično ožičenje	Lokalno ožičenje v poslovalnicah	Z:2
		N:2
		R:3

Vir: Lasten.

Strojna oprema

Tabela 2: Ocena zahtevane varnosti strojne opreme

Vir	Opis vira	Ocena zahtevane varnosti
Delovne postaje	Običajne uporabniške delovne postaje v poslovalnicah	Z:2 N:3 R:2
Kritične delovne postaje	Pomembnejše delovne postaje v zalednih službah	Z:4 N:4 R:4
Prenosne delovne postaje	Prenosni računalniki	Z:4 N:4 R:2
Strežniki za bančno poslovanje	Strežniki za poslovne aplikacije (Linux)	Z:4 N:4 R:4
Sistemski strežniki	Strežniki za domeno, antivirusno zaščito, datotečni strežniki (Windows)	Z:4 N:4 R:3

Vir: Lasten.

Operacijski sistemi

Tabela 3: Ocena zahtevane varnosti operacijskih sistemov

Vir	Opis vira	Ocena zahtevane varnosti
Microsoft Windows XP / 2000	Operacijski sistem na delovnih postajah	Z:4 N:4 R:3
Microsoft Windows Server 2003	Operacijski sistem na sistemskih strežnikih	Z:4 N:4 R:3
Suse Linux 10 Enterprise Edition	Operacijski sistem za strežnike s poslovnimi aplikacijami	Z:4 N:4 R:4

Vir: Lasten.

Baze podatkov

Tabela 4: Ocena zahtevane varnosti baz podatkov

Vir	Opis vira	Ocena zahtevane varnosti
Oracle	Baze podatkov za poslovne aplikacije	Z:4
		N:4
		R:4

Vir: Lasten.

Programska oprema

Tabela 5: Ocena zahtevane varnosti programske opreme

Vir	Opis vira	Ocena zahtevane varnosti
Microsoft Office	Pisarniški programi: Word, Excel, Power Point, Outlook	Z:2
		N:2
		R:2
NOD32 Antivirus	Program za antivirusno zaščito	Z:4
		N:4
		R:3
Microsoft Internet Explorer	Brskalnik za internet	Z:4
		N:4
		R:2
Adobe Acrobat Reader	Pregledovalnik	Z:2
		N:2
		R:1
ZBS program za izračun EOM	Program za izračun efektivne obrestne mere	Z:1
		N:3
		R:2
IBON program za boniteto	Program za preverjanje bonitete pravnih oseb	Z:1
		N:2
		R:2
Microsoft Visio	Program za načrtovanje	Z:2
		N:2
		R:2
PGP program za šifriranje	Program za šifriranje datotek pri prenosih	Z:4
		N:4
		R:3
Bančni informacijski sistem Hibis	Bančna poslovna aplikacija (vsebuje vse programske module za poslovanje hranilnice)	Z:4
		N:4
		R:4
Spletni banki Dh-Net in Dh-Plus	Dh-Net za pravne osebe, Dh-Plus za fizične	Z:4
		N:4
		R:4

Tabela 5 - nadaljevanje		
Swift Alliance Entry	Programska oprema za Swift	Z:4 N:4 R:4
Giro kliring	Plačilni sistem Banke Slovenije	Z:4 N:4 R:4
Connect Direct	Komunikacijski program za izmenjavo podatkov s procesnim centrom	Z:4 N:4 R:4
Spletni portal	Spletna stran in portal za hitre kredite po sistemu Bankredit	Z:3 N:4 R:3
Elektronska pošta	Program za elektronsko pošto	Z:4 N:4 R:3

Vir: Lasten.

Kadri

Tabela 6: Ocena zahtevane varnosti kadrov

Vir	Opis vira	Ocena zahtevane varnosti
Ključni kadri	Zaposleni na pomembnejših delovnih mestih (uprava, vodje služb, vodje poslovnih enot, referenti v plačilnem prometu, informatiki itd.)	Z:4 N:4 R:3
Ostali zaposleni	Zaposleni v poslovalnicah in službah	Z:3 N:3 R:2

Vir: Lasten.

Dokumentacija

Tabela 7: Ocena zahtevane varnosti dokumentov

Vir	Opis vira	Ocena zahtevane varnosti
Politike in strategije	Dokumenti najvišjega nivoja, ki urejajo organizacijo, politiko in strategijo poslovanja ter procesov na posameznih področjih	Z:4 N:4 R:4
Ostali interni akti	Dokumenti, ki jih potrebujejo zaposleni za kakovostno opravljanje delovnih nalog	Z:2 N:4 R:4
Uporabniški dokumenti	Dokumenti, ki jih izdelajo uporabniki in niso shranjeni v bazah podatkov	Z:3 N:3 R:3

Vir: Lasten.

2 OCENA OGROŽENOSTI INFORMACIJSKIH VIROV

Komunikacijske povezave in oprema

Tabela 8: Ocena ogroženosti komunikacijskih povezav in opreme

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Poslovno omrežje hranilnice	Prekinitev povezave, naravne nesreče	2	Ni rezervnih povezav	Z:0	Z:2
				N:0	N:2
				R:3	R:5
Poslovno omrežje hranilnice	Prisluškovanje prenosu	3	Šifrirni ključ	Z:1	Z:4
				N:0	N:3
				R:0	R:3
Poslovno omrežje hranilnice	Prestrezanje in spreminjanje sporočil	3	Šifrirni ključ	Z:1	Z:4
				N:1	N:4
				R:0	R:2
Partnerske povezave	Prekinitev povezave, naravne nesreče	2	Bankart: ni rezervne povezave	Z:0	Z:2
				N:0	N:2
				R:1-4	R:2-6
Partnerske povezave	Prisluškovanje prenosu	3	Upravljanje s šifrirnimi ključi	Z:1	Z:4
				N:0	N:3
				R:0	R:3
Partnerske povezave	Prestrezanje in spreminjanje sporočil	2	Upravljanje s šifrirnimi ključi	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Internetne povezave	Prekinitev povezave, naravne nesreče	3	Povezava z enim ponudnikom	Z:0	Z:3
				N:0	N:3
				R:3	R:6
Navidezne zasebne povezave	Prekinitev povezave, naravne nesreče	2	Poteka po internetnem omrežju	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Navidezne zasebne povezave	Nepooblaščen dostop	2	Hramba certifikata	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Navidezne zasebne povezave	Prestrezanje in spreminjanje sporočil	2	Hramba certifikata	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Požarna pregrada	Vdor v omrežje po pregrade	3	Upravljanje in nadgrajevanje sistema pregrade	Z:2	Z:5
				N:2	N:5
				R:1	R:4
Požarna pregrada	Onemogočanje dostopov zaradi napadov	3	Upravljanje uteži povezav	Z:0	Z:3
				N:0	N:3
				R:3	R:6
Požarna pregrada	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila	Z:1	Z:3
				N:1	N:3
				R:1	R:3

Tabela 8 - nadaljevanje					
Požarna pregrada	Odpoved strojne opreme	2	Obremenjenost sistema	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Požarna pregrada	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Požarna pregrada	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Usmerjevalniki in stikala	Prevzem nadzora nad opremo	2	Upravljanje z gesli, dostopi, oper. sistemom	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Usmerjevalniki in stikala	Sabotaža	1	Zaposleni v poslovalnici	Z:1	Z:2
				N:1	N:2
				R:2	R:3
Usmerjevalniki in stikala	Odpoved strojne opreme	2	Ni podvojenosti delov	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Kritični usmerjevalniki in kritična stikala	Prevzem nadzora nad opremo	3	Upravljanje z gesli, dostopi, oper. sistemom	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Kritični usmerjevalniki in kritična stikala	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, obremenjenost	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Kritični usmerjevalniki in kritična stikala	Odpoved strojne opreme	2	Ni podvojenosti delov, pogodba	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Kritični usmerjevalniki in kritična stikala	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Kritični usmerjevalniki in kritična stikala	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Fizično ožičenje	Namestitev naprave za prisluškovanje	2	Nadzor oddaljenih poslovalnic	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Fizično ožičenje	Namerna onesposobitev omrežja	1	Nadzor v oddaljenih poslovalnicah	Z:0	Z:1
				N:0	N:1
				R:2	R:3

Vir: Lasten.

Strojna oprema

Tabela 9: Ocena ogroženosti strojne opreme

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Delovne postaje	Okvara opreme	2	Ni podvojenosti delov	Z:0	Z:2
				N:1	N:3
				R:2	R:4
Delovne postaje	Odtujitev opreme ali nepooblaščen poseg	2	Slab nadzor nad prostori za osebno obravnavo	Z:2	Z:4
				N:2	N:4
				R:2	R:4
Delovne postaje	Izpad električnega napajanja	2	Vse naprave niso priključene na UPS	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Delovne postaje	Neprimerno ravnanje uporabnikov	2	Otežen nadzor	Z:0	Z:2
				N:2	N:4
				R:2	R:4
Kritične delovne postaje	Okvara opreme	3	Ni podvojenosti delov	Z:0	Z:3
				N:1	N:4
				R:0-2	R:3-5
Kritične delovne postaje	Odtujitev opreme ali nepooblaščen poseg	2	Kontrola pristopa	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Kritične delovne postaje	Izpad električnega napajanja	2	Pravilnost priklopa na UPS, preobremenitev	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Kritične delovne postaje	Neprimerno ravnanje uporabnikov	1	Otežen nadzor	Z:0	Z:2
				N:2	N:3
				R:3	R:4
Kritične delovne postaje	Neprimerna zmogljivost opreme	2	Zahtevnost in kritičnost aplikacij	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Kritične delovne postaje	Naravne in druge nesreče	2	Ustreznost načrta za okrevanje	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Kritične delovne postaje	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:2	R:4
Prenosne delovne postaje	Okvara opreme	3	Prenos opreme in vremenski vplivi	Z:0	Z:3
				N:1	N:4
				R:1	R:4
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg	3	Prenos opreme izven varovanih področij	Z:3	Z:6
				N:3	N:6
				R:1	R:4

Tabela 9 - nadaljevanje					
Prenosne delovne postaje	Izpad električnega napajanja	2	Pripravljenost baterije	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Prenosne delovne postaje	Neprimerno ravnanje uporabnikov	2	Krhkost opreme	Z:0	Z:2
				N:1	N:3
				R:2	R:4
Strežniki za bančno poslovanje	Okvara opreme	2	Neprimerne klimatske razmere, drugo	Z:1	Z:3
				N:1	N:3
				R:2	R:4
Strežniki za bančno poslovanje	Nepooblaščen poseg	1	Kontrola dostopa	Z:1	Z:2
				N:1	N:2
				R:2	R:3
Strežniki za bančno poslovanje	Izpad električnega napajanja	2	Obremenjenost UPS naprave	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Strežniki za bančno poslovanje	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, zunanji izvajalci	Z:1	Z:3
				N:1	N:3
				R:2	R:4
Strežniki za bančno poslovanje	Sabotaža	1	Nezadovoljstvo zaposlenih ali zunanjih izvajalcev	Z:1	Z:2
				N:1	N:2
				R:2	R:3
Strežniki za bančno poslovanje	Neprimerna zmogljivost opreme	1	Zahtevnost in kritičnost aplikacij	Z:1	Z:2
				N:1	N:2
				R:3	R:4
Strežniki za bančno poslovanje	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Strežniki za bančno poslovanje	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:3
				N:0	N:3
				R:3	R:5
Sistemski strežniki	Okvara opreme	2	Neprimerne klimatske razmere, drugo	Z:0	Z:2
				N:1	N:3
				R:1	R:3
Sistemski strežniki	Nepooblaščen poseg	2	Kontrola dostopa	Z:0	Z:1
				N:1	N:2
				R:1	R:3
Sistemski strežniki	Izpad električnega napajanja	2	Obremenjenost UPS naprave	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Sistemski strežniki	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Sistemski strežniki	Sabotaža	1	Nezadovoljstvo zaposlenih ali zunanjih izvajalcev	Z:1	Z:2
				N:1	N:2
				R:2	R:3

Tabela 9 - nadaljevanje					
Sistemski strežniki	Neprimerna zmogljivost opreme	1	Zahtevnost in kritičnost aplikacij	Z:0	Z:1
				N:1	N:2
				R:2	R:3
Sistemski strežniki	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Sistemski strežniki	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3

Vir: Lasten.

Operacijski sistemi

Tabela 10: Ocena ogroženosti operacijskih sistemov

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Microsoft Windows XP / 2000	Nepooblaščen dostop	3	Socialni inženiring	Z:2	Z:5
				N:2	N:5
				R:1	R:4
Microsoft Windows XP /2000	Napad zlonamerne programske opreme	3	Varnostni popravki in antivirusna zaščita	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Microsoft Windows Server 2003	Nepooblaščen dostop	2	Nastavitve, politika gesel in dostopov	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Microsoft Windows Server 2003	Napad zlonamerne programske opreme	2	Varnostni popravki in antivirusna zaščita	Z:1	Z:3
				N:1	N:3
				R:2	R:4
Microsoft Windows Server 2003	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila	Z:3	Z:5
				N:3	N:5
				R:3	R:5
Microsoft Windows Server 2003	Sabotaža	2	Nezadovoljstvo zaposlenih ali zunanjih izvajalcev	Z:1	Z:3
				N:1	N:3
				R:2	R:4
Suse Linux 10 Enterprise Edition	Nepooblaščen dostop	3	Nastavitve, politika gesel in dostopov	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Suse Linux 10 Enterprise Edition	Napad zlonamerne programske opreme	2	Varnostni popravki in antivirusna zaščita	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Suse Linux 10 Enterprise Edition	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, zunanji izvajalci	Z:3	Z:5
				N:3	N:5
				R:3	R:5

Tabela 10 - nadaljevanje					
Suse Linux 10 Enterprise Edition	Sabotaža	2	Nezadovoljstvo zaposlenih ali zunanjih izvajalcev	Z:1 N:1 R:2	Z:3 N:3 R:4

Vir: Lasten.

Baze podatkov

Tabela 11: Ocena ogroženosti baz podatkov

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Oracle	Nepooblaščen dostop	3	Nastavitve, politika gesel in dostopov	Z:2 N:2 R:2	Z:5 N:5 R:5
Oracle	Napad zlonamerne programske opreme	2	Zagotavljanje varnostnih popravkov	Z:1 N:1 R:1	Z:3 N:3 R:3
Oracle	Nedelovanje baze, izguba podatkov	2	Sistemske napake, postopki varovanja podatkov	Z:1 N:0 R:2	Z:3 N:2 R:4
Oracle	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, obremenjenost	Z:3 N:1 R:1	Z:3 N:3 R:3
Oracle	Neprimerna zmogljivost opreme	1	Zahtevnost in kritičnost aplikacij	Z:0 N:1 R:2	Z:1 N:2 R:3

Vir: Lasten.

Programska oprema

Tabela 12: Ocena ogroženosti programske opreme

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Microsoft Office	Napake v programski opremi	2	Obseg kode programa	Z:1 N:2 R:2	Z:3 N:4 R:4
Microsoft Office	Napad zlonamerne programske opreme	2	Zagotavljanje varnostnih popravkov	Z:1 N:1 R:1	Z:3 N:3 R:3
NOD32 antivirusna zaščita	Napake v programski opremi	2	Zagotavljanje popravkov programa	Z:0 N:0 R:1	Z:2 N:2 R:3

Tabela 12 - nadaljevanje					
NOD32 antivirusna zaščita	Neučinkovitost antivirusne zaščite	3	Hitro zagotavljanje novih vzorcev	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Microsoft Internet Explorer	Napake v programski opremi	3	Veliko število nadgradenj	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Microsoft Internet Explorer	Napad zlonamerne programske opreme	3	Zagotavljanje varnostnih popravkov	Z:2	Z:5
				N:2	N:5
				R:1	R:4
Adobe Acrobat Reader	Napake v programski opremi	2	Veliko število nadgradenj	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Adobe Acrobat Reader	Napad zlonamerne programske opreme	3	Zagotavljanje varnostnih popravkov	Z:1	Z:4
				N:1	N:4
				R:1	R:4
ZBS program za izračun EOM	Napake v programski opremi	1	Obseg kode programa	Z:1	Z:2
				N:2	N:3
				R:1	R:2
ZBS program za izračun EOM	Napad zlonamerne programske opreme	3	Zagotavljanje varnostnih popravkov Office	Z:1	Z:4
				N:1	N:4
				R:1	R:4
IBON program za boniteto	Napake v programski opremi	2	Obseg podatkov	Z:0	Z:2
				N:1	N:3
				R:1	R:3
Microsoft Visio	Napake v programski opremi	1	Podpora različnim proizvajalcem	Z:0	Z:1
				N:0	N:1
				R:2	R:3
PGP program za šifriranje	Napake v nastavitvah in programski opremi	1	Ustreznost namestitve	Z:2	Z:3
				N:2	N:3
				R:2	R:3
PGP program za šifriranje	Napadi na šifrirne metode in ključe	2	Hranjenje šifrirnih ključev	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Bančni informacijski sistem Hibis	Nepooblaščen dostop do modula	3	Dodelitev in nadzor pooblastil, zunanji izvajalci	Z:3	Z:5
				N:3	N:5
				R:1	R:4
Bančni informacijski sistem Hibis	Napake v programskih modulih	3	Hitro uvajanje sprememb	Z:2	Z:5
				N:2	N:5
				R:2	R:5
Bančni informacijski sistem Hibis	Nedelovanje programskih modulov	2	Vzdrževanje in nadgrajevanje sistema	Z:0	Z:2
				N:1	N:3
				R:1	R:3
Bančni informacijski sistem Hibis	Nedelovanje celotnega sistema	Pogojeno z nedelovanjem baze podatkov Oracle obravnavano v točki 2.4			

Tabela 12 - nadaljevanje					
Bančni informacijski sistem Hibis	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, obremenjenost	Z:2	Z:4
				N:2	N:4
				R:1	R:3
Bančni informacijski sistem Hibis	Nezmožnost ugotavljanja revizijskih sledi	2	Izklop sistema beleženja	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Bančni informacijski sistem Hibis	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Bančni informacijski sistem Hibis	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Spletni banki Dh-Net in Dh-Plus	Nepooblaščen dostop, vdor	3	Zloraba sredstev overjanja	Z:1	Z:4
				N:1	N:4
				R:0	R:3
Spletni banki Dh-Net in Dh-Plus	Nešifrirana povezava uporabnika	2	Napaka pri vzpostavitvi šifrirane povezave	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Spletni banki Dh-Net in Dh-Plus	Onemogočanje dostopov zaradi napadov	2	Pogojeno s slabim upravljanjem požarne pregrade obravnavano v točki 2.1		
Spletni banki Dh-Net in Dh-Plus	Napake v programski opremi	2	Postopek testiranja in uvajanja sprememb	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Spletni banki Dh-Net in Dh-Plus	Nedelovanje spletne banke	2	Vzdrževanje in nadgrajevanje sistema	Z:0	Z:2
				N:1	N:3
				R:1	R:3
Spletni banki Dh-Net in Dh-Plus	Napad zlonamerne programske opreme	3	Zagotavljanje varnostnih popravkov	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Spletni banki Dh-Net in Dh-Plus	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, obremenjenost	Z:2	Z:4
				N:2	N:4
				R:1	R:3
Spletni banki Dh-Net in Dh-Plus	Nezmožnost ugotavljanja revizijskih sledi	2	Izklop sistema beleženja	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Spletni banki Dh-Net in Dh-Plus	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:6
Spletni banki Dh-Net in Dh-Plus	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Swift Alliance Entry	Nepooblaščen dostop, vdor	3	Dodelitev in nadzor pooblastil, zunanji izvajalci	Z:2	Z:5
				N:2	N:5
				R:1	R:4

Tabela 12 - nadaljevanje					
Swift Alliance Entry	Napake v programski opremi	2	Podpora zunanjih izvajalcev	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Swift Alliance Entry	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, zunanji izvajalci	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Swift Alliance Entry	Naravne in druge nesreče	2	Prenos podatkov na varno lokacijo	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Swift Alliance Entry	Odzivnost pogodbenih vzdrževalcev	2	Zunanje izvajanje vzdrževanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Giro kliring	Nepooblaščen dostop, vdor	2	Dodelitev in nadzor pooblastil pri BS	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Giro kliring	Napake v programski opremi	2	Zunanji izvajalec	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Giro kliring	Naravne in druge nesreče	2	Povezava z rezervne lokacije	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Connect Direct	Nepooblaščen dostop, vdor	2	Dodelitev in nadzor pooblastil, zunanji izvajalci	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Connect Direct	Napake v programski opremi	2	Nadgrajevanje sistema	Z:1	Z:3
				N:0	N:2
				R:1	R:3
Connect Direct	Nedelovanje programske opreme	2	Vzdrževanje sistema	Z:0	Z:2
				N:1	N:3
				R:1	R:3
Connect Direct	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila, zunanji izvajalci	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Connect Direct	Naravne in druge nesreče	2	Ni sistema na rezervni lokaciji	Z:0	Z:2
				N:0	N:2
				R:4	R:5
Spletni portal	Nepooblaščen dostop ali vdor	2	Dodelitev in nadzor pooblastil, zunanji izvajalci	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Spletni portal	Napake v programski opremi	2	Pogoste spremembe	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Spletni portal	Nedelovanje programske opreme	1	Vzdrževanje sistema	Z:0	Z:1
				N:1	N:2
				R:2	R:3

Tabela 12 - nadaljevanje					
Spletni portal	Napad zlonamerne programske opreme	3	Zagotavljanje varnostnih popravkov	Z:1	Z:4
				N:1	N:4
				R:1	R:4
Elektronska pošta	Nepooblaščen dostop ali vdor	2	Dodelitev in nadzor pooblastil	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Elektronska pošta	Napake v programski opremi	2	Zunanji izvajalci	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Elektronska pošta	Nedelovanje programske opreme	2	Vzdrževanje sistema	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Elektronska pošta	Nestrokovno delo in napake skrbnikov	2	Velika pooblastila	Z:1	Z:3
				N:1	N:3
				R:1	R:3
Elektronska pošta	Napad zlonamerne programske opreme	3	Zagotavljanje popravkov in zaščite	Z:2	Z:5
				N:2	N:5
				R:2	R:5

Vir: Lasten.

Kadri

Tabela 13: Ocena ogroženosti kadrov

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Ključni kadri	Izguba razpoložljivosti za delovne naloge	2	Pomanjkanje upravljanja	Z:0	Z:2
				N:0	N:2
				R:1	R:3
Ključni kadri	Izdaja poslovne skrivnosti ali osebnih podatkov	3	Dostop do vseh dokumentov, motivacija za delo	Z:2	Z:5
				N:2	N:5
				R:0	R:3
Ključni kadri	Nestrokovno delo, napake pri delu	2	Pomanjkanje znanja, strokovnega izobraževanja	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Ključni kadri	Namerno povzročanje škode, sabotaža	1	Nezadovoljstvo	Z:1	Z:2
				N:1	N:2
				R:2	R:3
Ostali zaposleni	Izdaja poslovne skrivnosti ali osebnih podatkov	2	Dostop do osebnih podatkov strank in dokumentov	Z:1	Z:3
				N:1	N:3
				R:0	R:2
Ostali zaposleni	Nestrokovno delo, napake pri delu	3	Nove poslovalnice, pomanjkanje znanja	Z:2	Z:5
				N:2	N:5
				R:2	R:5

Vir: Lasten.

Dokumentacija

Tabela 14: Ocena ogroženosti dokumentov

Vir	Grožnja	Ocena grožnje	Ranljivost	Ocena ranljivosti	Ocena ogroženosti
Politike in strategije	Nepooblaščen dostop	2	Dostop zaposlenih	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Politike in strategije	Neskladnost s cilji in zakonskimi smernicami	3	Obremenitev odgovornih, hitro prilagajanje	Z:2	Z:5
				N:0	N:3
				R:2	R:5
Ostali interni akti	Neskladnost s politikami in prakso	2	Slabo sledenje na posameznem področju	Z:0	Z:2
				N:1	N:3
				R:2	R:4
Ostali interni akti	Pomanjkanje ali slaba kakovost internih aktov	3	Slaba organiziranost področij	Z:0	Z:3
				N:0	N:3
				R:0-2	R:3-5
Uporabniški dokumenti	Nepooblaščen dostop, politika čiste mize	2	Zaščita dostopa	Z:2	Z:4
				N:2	N:4
				R:0	R:2
Uporabniški dokumenti	Izguba dokumentov	3	Izvajanje rednega varovanja	Z:0	Z:3
				N:0	N:3
				R:1	R:4

Vir: Lasten.

3 OCENA TVEGANJ INFORMACIJSKIH VIROV

Komunikacijske povezave in oprema

Tabela 15: Ocena tveganj komunikacijskih povezav in opreme

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Poslovno omrežje hranilnice	Prekinitev povezave, naravne nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:5	R:7
Poslovno omrežje hranilnice	Prisluškovanje prenosu	Z:4	Z:4	Z:6
		N:4	N:3	N:5
		R:3	R:3	R:3
Poslovno omrežje hranilnice	Prestrezanje in spreminjanje sporočil	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:2	R:3

Tabela 15 - nadaljevanje				
Partnerske povezave	Prekinitev povezave, naravne nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:2-6	R:4-8
Partnerske povezave	Prisluškovanje prenosu	Z:4	Z:4	Z:6
		N:4	N:3	N:5
		R:4	R:3	R:5
Partnerske povezave	Prestrezanje in spreminjanje sporočil	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:4
Internetne povezave	Prekinitev povezave, naravne nesreče	Z:2	Z:3	Z:2
		N:2	N:3	N:2
		R:4	R:6	R:8
Navidezne zasebne povezave	Prekinitev povezave, naravne nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:2	R:4	R:3
Navidezne zasebne povezave	Nepooblaščen dostop	Z:4	Z:4	Z:6
		N:4	N:2	N:6
		R:2	R:2	R:2
Navidezne zasebne povezave	Prestrezanje in spreminjanje sporočil	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:2	R:2	R:2
Požarna pregrada	Vdor v omrežje po pregradi	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:4	R:6
Požarna pregrada	Onemogočanje dostopov zaradi napada	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:6	R:8
Požarna pregrada	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Požarna pregrada	Odpoved strojne opreme	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Požarna pregrada	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Požarna pregrada	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:6	R:8
Usmerjevalniki in stikala	Prevzem nadzora nad opremo	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
Usmerjevalniki in stikala	Sabotaža	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4

Tabela 15 - nadaljevanje				
Usmerjevalniki in stikala	Odpoved strojne opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
Kritični usmerjevalniki in kritična stikala	Prevzem nadzora nad opremo	Z:4	Z:5	Z:6
		N:4	N:5	N:6
		R:4	R:4	R:6
Kritični usmerjevalniki in kritična stikala	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Kritični usmerjevalniki in kritična stikala	Odpoved strojne opreme	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:4	R:6
Kritični usmerjevalniki in kritična stikala	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:6	R:8
Kritični usmerjevalniki in kritična stikala	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Fizično ožičenje	Namestitev naprave za prisluškovanje	Z:2	Z:4	Z:3
		N:2	N:4	N:3
		R:3	R:2	R:3
Fizično ožičenje	Namerna onesposobitev omrežja	Z:2	Z:1	Z:1
		N:2	N:1	N:1
		R:3	R:3	R:4

Vir: Lasten.

Strojna oprema

Tabela 16: Ocena tveganj strojne opreme

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Delovne postaje	Okvara opreme	Z:2	Z:2	Z:2
		N:3	N:3	N:4
		R:2	R:4	R:3
Delovne postaje	Odtujitev opreme ali nepooblaščen poseg	Z:2	Z:4	Z:3
		N:3	N:4	N:5
		R:2	R:4	R:3
Delovne postaje	Izpad električnega napajanja	Z:2	Z:2	Z:2
		N:3	N:2	N:3
		R:2	R:4	R:3
Delovne postaje	Neprimerno ravnanje uporabnikov	Z:2	Z:2	Z:2
		N:3	N:4	N:5
		R:2	R:4	R:3

Tabela 16 - nadaljevanje				
Kritične delovne postaje	Okvara opreme	Z:4	Z:3	Z:5
		N:4	N:4	N:6
		R:4	R:3-5	R:5-7
Kritične delovne postaje	Odtujitev opreme ali nepooblaščen poseg	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Kritične delovne postaje	Izpad električnega napajanja	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Kritične delovne postaje	Neprimerno ravnanje uporabnikov	Z:4	Z:2	Z:4
		N:4	N:3	N:5
		R:4	R:4	R:6
Kritične delovne postaje	Neprimerna zmogljivost opreme	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:4	R:6
Kritične delovne postaje	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:4	R:6
Kritične delovne postaje	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:4	R:6
Prenosne delovne postaje	Okvara opreme	Z:4	Z:3	Z:5
		N:4	N:4	N:6
		R:2	R:4	R:3
Prenosne delovne postaje	Odtujitev opreme ali nepooblaščen poseg	Z:4	Z:6	Z:8
		N:4	N:6	N:8
		R:2	R:4	R:3
Prenosne delovne postaje	Izpad električnega napajanja	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:2	R:3	R:2
Prenosne delovne postaje	Neprimerno ravnanje uporabnikov	Z:4	Z:2	Z:4
		N:4	N:3	N:4
		R:2	R:4	R:3
Strežniki za bančno poslovanje	Okvara opreme	Z:4	Z:3	Z:4
		N:4	N:3	N:5
		R:4	R:4	R:6
Strežniki za bančno poslovanje	Nepooblaščen poseg	Z:4	Z:2	Z:3
		N:4	N:2	N:3
		R:4	R:3	R:5
Strežniki za bančno poslovanje	Izpad električnega napajanja	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Strežniki za bančno poslovanje	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:4	R:6

Tabela 16 - nadaljevanje				
Strežniki za bančno poslovanje	Sabotaža	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Strežniki za bančno poslovanje	Neprimerna zmogljivost opreme	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:4	R:6
Strežniki za bančno poslovanje	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:6	R:8
Strežniki za bančno poslovanje	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:5	R:7
Sistemski strežniki	Okvara opreme	Z:4	Z:2	Z:4
		N:4	N:3	N:5
		R:3	R:3	R:4
Sistemski strežniki	Nepooblaščen poseg	Z:4	Z:1	Z:3
		N:4	N:2	N:4
		R:3	R:3	R:4
Sistemski strežniki	Izpad električnega napajanja	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4
Sistemski strežniki	Nestrokovno delo in napake skrbnikov	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4
Sistemski strežniki	Sabotaža	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4
Sistemski strežniki	Neprimerna zmogljivost opreme	Z:4	Z:1	Z:3
		N:4	N:2	N:4
		R:3	R:3	R:4
Sistemski strežniki	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:6	R:7
Sistemski strežniki	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4

Vir: Lasten.

Operacijski sistemi

Tabela 17: Ocena tveganj operacijskih sistemov

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Microsoft Windows XP / 2000	Nepooblaščen dostop	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:3	R:4	R:6
Microsoft Windows XP /2000	Napad zlonamerne programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
Microsoft Windows Server 2003	Nepooblaščen dostop	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
Microsoft Windows Server 2003	Napad zlonamerne programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:4	R:5
Microsoft Windows Server 2003	Nestrokovno delo in napake skrbnikov	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:3	R:5	R:7
Microsoft Windows Server 2003	Sabotaža	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:4	R:5
Suse Linux 10 Enterprise Edition	Nepooblaščen dostop	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Suse Linux 10 Enterprise Edition	Napad zlonamerne programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Suse Linux 10 Enterprise Edition	Nestrokovno delo in napake skrbnikov	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:5	R:7
Suse Linux 10 Enterprise Edition	Sabotaža	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:4	R:5

Vir: Lasten.

Baze podatkov

Tabela 18: Ocena tveganj baz podatkov

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Oracle	Nepooblaščen dostop	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:5	R:7
Oracle	Napad zlonamerne programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Oracle	Nedelovanje baze, izguba podatkov	Z:4	Z:3	Z:5
		N:4	N:2	N:4
		R:4	R:4	R:6
Oracle	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Oracle	Neprimerna zmogljivost opreme	Z:4	Z:1	Z:3
		N:4	N:2	N:4
		R:4	R:3	R:5

Vir: Lasten.

Programska oprema

Tabela 19: Ocena tveganj programske opreme

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Microsoft Office	Napake v programski opremi	Z:2	Z:3	Z:2
		N:2	N:4	N:3
		R:2	R:4	R:3
Microsoft Office	Napad zlonamerne programske opreme	Z:2	Z:3	Z:2
		N:2	N:3	N:2
		R:2	R:3	R:2
NOD32 antivirusna zaščita	Napake v programski opremi	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4
NOD32 antivirusna zaščita	Neučinkovitost zaščite	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
Microsoft Internet Explorer	Napake v programski opremi	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:2	R:4	R:3

Tabela 19 - nadaljevanje				
Microsoft Internet Explorer	Napad zlonamerne programske opreme	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:2	R:4	R:3
Adobe Acrobat Reader	Napake v programski opremi	Z:2	Z:3	Z:2
		N:2	N:3	N:2
		R:1	R:3	R:2
Adobe Acrobat Reader	Napad zlonamerne programske opreme	Z:2	Z:4	Z:3
		N:2	N:4	N:3
		R:1	R:4	R:2
ZBS program za izračun EOM	Napake v programski opremi	Z:1	Z:2	Z:1
		N:3	N:3	N:4
		R:2	R:2	R:2
ZBS program za izračun EOM	Napad zlonamerne programske opreme	Z:1	Z:4	Z:2
		N:3	N:4	N:5
		R:2	R:4	R:3
IBON program za boniteto	Napake v programski opremi	Z:1	Z:2	Z:1
		N:2	N:3	N:2
		R:2	R:3	R:2
Microsoft Visio	Napake v programski opremi	Z:2	Z:1	Z:1
		N:2	N:1	N:1
		R:2	R:3	R:2
PGP program za šifriranje	Napake v nastavitvah in programski opremi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
PGP program za šifriranje	Napadi na šifrirne metode in ključe	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:2	R:3
Bančni informacijski sistem Hibis	Nepooblaščen dostop do modula	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:4	R:6
Bančni informacijski sistem Hibis	Napake v programskih modulih	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:5	R:7
Bančni informacijski sistem Hibis	Nedelovanje programskih modulov	Z:4	Z:2	Z:4
		N:4	N:3	N:5
		R:4	R:3	R:5
Bančni informacijski sistem Hibis	Nestrokovno delo in napake skrbnikov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:3	R:5
Bančni informacijski sistem Hibis	Nezmožnost ugotavljanja revizijskih sledi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:5
Bančni informacijski sistem Hibis	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:6	R:8

Tabela 19 - nadaljevanje				
Bančni informacijski sistem Hibis	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Spletni banki Dh-Net in Dh-Plus	Nepooblaščen dostop, vdor	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:3	R:5
Spletni banki Dh-Net in Dh-Plus	Nešifrirana povezava uporabnika	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:4
Spletni banki Dh-Net in Dh-Plus	Napake v programski opremi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Spletni banki Dh-Net in Dh-Plus	Nedelovanje spletne banke	Z:4	Z:2	Z:4
		N:4	N:3	N:5
		R:4	R:3	R:5
Spletni banki Dh-Net in Dh-Plus	Napad zlonamerne programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Spletni banki Dh-Net in Dh-Plus	Nestrokovno delo in napake skrbnikov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:3	R:5
Spletni banki Dh-Net in Dh-Plus	Nezmožnost ugotavljanja revizijskih sledi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:4
Spletni banki Dh-Net in Dh-Plus	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:6	R:8
Spletni banki Dh-Net in Dh-Plus	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Swift Alliance Entry	Nepooblaščen dostop, vdor	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:4	R:4	R:6
Swift Alliance Entry	Napake v programski opremi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Swift Alliance Entry	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Swift Alliance Entry	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Swift Alliance Entry	Odzivnost pogodbenih vzdrževalcev	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5

Tabela 19 - nadaljevanje				
Giro kliring	Nepooblaščen dostop, vdor	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Giro kliring	Napake v programski opremi	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R5
Giro kliring	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:3	R:5
Connect Direct	Nepooblaščen dostop, vdor	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Connect Direct	Napake v programski opremi	Z:4	Z:3	Z:5
		N:4	N:2	N:4
		R:4	R:3	R:5
Connect Direct	Nedelovanje programske opreme	Z:4	Z:2	Z:4
		N:4	N:3	N:5
		R:4	R:3	R:5
Connect Direct	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Connect Direct	Naravne in druge nesreče	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:4	R:5	R:7
Spletni portal	Nepooblaščen dostop ali vdor	Z:3	Z:4	Z:5
		N:4	N:4	N:6
		R:3	R:2	R:3
Spletni portal	Napake v programski opremi	Z:3	Z:3	Z:4
		N:4	N:3	N:5
		R:3	R:3	R:4
Spletni portal	Nedelovanje programske opreme	Z:3	Z:1	Z:2
		N:4	N:2	N:4
		R:3	R:3	R:4
Spletni portal	Napad zlonamerne programske opreme	Z:3	Z:4	Z:5
		N:4	N:4	N:6
		R:3	R:4	R:5
Elektronska pošta	Nepooblaščen dostop ali vdor	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:2	R:3
Elektronska pošta	Napake v programski opremi	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
Elektronska pošta	Nedelovanje programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4

Elektronska pošta	Nestrokovno delo in napake skrbnikov	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:3	R:4
Elektronska pošta	Napad zlonamerne programske opreme	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:3	R:5	R:6

Vir: Lasten.

Kadri

Tabela 20: Ocena tveganj kadrov

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Ključni kadri	Izguba razpoložljivosti za delovne naloge	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:5
Ključni kadri	Izdaja poslovne skrivnosti ali osebnih podatkov	Z:4	Z:5	Z:7
		N:4	N:5	N:7
		R:3	R:3	R:4
Ključni kadri	Nestrokovno delo, napake pri delu	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:3	R:2	R:3
Ključni kadri	Namerno povzročanje škode, sabotaža	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:3	R:3	R:4
Ostali zaposleni	Izdaja poslovne skrivnosti ali osebnih podatkov	Z:3	Z:3	Z:4
		N:3	N:3	N:3
		R:2	R:2	R:2
Ostali zaposleni	Nestrokovno delo, napake pri delu	Z:3	Z:5	Z:6
		N:3	N:5	N:6
		R:2	R:5	R:5

Vir: Lasten.

Dokumentacija

Tabela 21: Ocena tveganj dokumentacije

Vir	Grožnja	Ocena zahtevane varnosti	Ocena ogroženosti	Ocena tveganja
Politike in strategije	Nepooblaščen dostop	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:2	R:4
Politike in strategije	Neskladnost s cilji, z zakoni in s predpisi	Z:4	Z:5	Z:7
		N:4	N:3	N:5
		R:4	R:5	R:7
Ostali interni akti	Neskladnost s politikami in prakso	Z:2	Z:2	Z:2
		N:4	N:3	N:5
		R:4	R:4	R:6
Ostali interni akti	Pomanjkanje ali slaba kakovost aktov	Z:2	Z:3	Z:2
		N:4	N:3	N:5
		R:4	R:3-5	R:4-7
Uporabniški dokumenti	Nepooblaščen dostop, politika čiste mize	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:2	R:3
Uporabniški dokumenti	Izguba dokumentov	Z:3	Z:3	Z:4
		N:3	N:3	N:4
		R:3	R:4	R:5

Vir: Lasten.