UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VARNOST IN TEHNOLOŠKA ZAŠČITA INFORMACIJSKEGA SISTEMA V BANKI

Ljubljana, februar 2003 MATEJ GRIL

IZJAVA

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

V Ljubljani, dne 17. 2. 2003

Podpis:

KAZALO

PRILOGA

KAZALO SLIK

KAZALO TABEL

PRILOGA

1 UVOD

Sedanji čas in našo celotno civilizacijo zaznamuje povezanost z računalniki in močna odvisnost od informacijske tehnologije. Ta se je v zadnjih tridesetih letih zelo hitro razvijala, tako hitro, da je bilo včasih kar premalo pozornosti posvečene njeni varnosti. Zlorabe te tehnologije so pokazale njeno ranljivost, zato se zlasti v zadnjem desetletju posveča veliko več pozornosti njeni varnosti in zaščiti.

Banke so organizacije, katerih poslovanje v celoti temelji na informacijski tehnologiji, saj so danes praktično vsi podatki predstavljeni v digitalni obliki. Hkrati pa so podatki, s katerimi se srečuje banka, zelo zaupne narave, pa naj gre za področje poslovanja s fizičnimi ali pravnimi osebami. Za banko bi pomenila vsaka izguba ali razkritje podatkov veliko finančno in poslovno škodo, pa tudi izgubo ugleda, ki ga uživa pri strankah.
Zaposlen sem v Novi Ljubljanski banki, pri svojem delu pa se ukvarjam z informacijsko tehnologijo, predvsem z administracijo sistemov in strežniki. Poleg tega tudi aktivno sodelujem v skupini, ki skrbi za varnost podatkov v banki in vseh organizacijah, ki so poslovno tesno povezane z njo. Zaradi vsega naštetega sem se odločil, da to delo posvetim proučevanju varnosti informacijskega sistema predvsem s tehnološkega vidika.

Narava problema je takšna, da ni mogoče javno razgrniti vseh podrobnosti informacijskega sistema, saj bi lahko te podatke potencialni napadalec s pridom uporabil pri svojem početju. Zaradi tega so nekateri podatki v nalogi namerno spremenjeni ali zamegljeni, vendar na način, ki ne spremeni bistva problema.

V nalogi se nisem preveč podrobno poglabljal v eno samo tehnološko rešitev ali v en sam del sistema, ampak sem poskušal na problem gledati s stališča tehnološke zaščite informacijskega sistema banke kot celote. Informacijski sistem, ki je predmet proučevanja, je velik in zapleten, vsaj za slovenske razmere, zato ga je posamezniku praktično nemogoče poznati vse do podrobnosti. V delu sem izpostavil nekatere bolj zanimive in aktualne probleme, ki jim danes posvečamo premalo pozornosti, obstajajo pa tudi področja, ki se jih nisem dotaknil, čeprav bi mogoče nekako sodila v sklop proučevanja, vendar bi lahko s tem delo prešlo zastavljene okvirje.

Zavedam pa se, da k varnost informacijskih sistemov sodi še veliko več, kot samo tehnologija. Za učinkovito zaščito je najprej potrebna ustrezna varnostna politika, ki uživa polno podporo vodstva organizacije, ustrezen in kakovosten nadzor izvajanja te politike, dobra organiziranost, strokovni kadri, kultura, osveščenost in motivacija zaposlenih v organizaciji ter še veliko drugih dejavnikov, ki jih ni za zanemariti.

1.1 NAMEN IN CILJI DELA

Namen in cilji dela pa so naslednji:

- proučitev tveganj, s katerimi se srečujejo banke na področju informacijske tehnologije, še posebej pa Nova Ljubljanska banka;
- proučitev tehnologij, ki se uporabljajo za izboljšanje varnosti v informacijskih sistemih ter kako so te tehnologije uporabljene v banki;
- ugotovitev stopnje varnosti informacijskega sistema, tako posameznih večjih področij kot celote, ter iskanje šibkih točk;
- predlog izboljšav, ki bi pripomogle k izboljšanju varnosti.

Komitenti banke upravičeno pričakujejo, da je denar, ki so ga zaupali banki, na varnem. Glede na to, sem na začetku izhajal iz hipoteze, da je tudi bančni informacijski sistem varen, saj se to od takšnega in tako velikega sistema pričakuje. V nalogi sem skozi proučevanje sistema večkrat preverjal to tezo in jo skušal potrditi ter ugotoviti, v koliki meri drži, oziroma jo ovreči in dokazati nasprotno. Način za sistematično proučevanje in ugotovitev stanja predstavlja metoda analize tveganja, ki se temeljito poglobi v komponente informacijskega sistema ter vrne oceno tveganj za posamezne komponente. V primeru, da bi metoda podala večje število velikih tveganj, bi lahko uvodno tezo naloge ovrgel in sklepal, da računalniški sistem ni varen.

1.2 SESTAVA NALOGE IN UPORABLJENE METODE

Naloga je sestavljena iz dveh sklopov, vsak pa vsebuje več poglavij. Prvi sklop je posvečen predvsem proučevanju sestave in zaščite bančnega informacijskega sistema ter varnostnih metod v banki, v drugem sklopu pa sem se posvetil konkretnim metodam analize in ocenjevanja tveganj. Izdelal sem oceno varnosti informacijskega sistema in predlagal ukrepe, ki bi jo izboljšali.

V prvem sklopu je predstavljen informacijski sistem banke ter poglavje, ki se ukvarja s smislom in z obsegom varnostnih ukrepov v organizaciji. Najobširnejše poglavje proučuje tehnološko zaščito informacijskega sistema, opisuje teorijo in prakso, ki velja na posameznemu področju, kakšna tveganja se pojavljajo, kako se zaščititi pred nevarnostjo ter kako je zaščita konkretno izvedena v banki. Področja, katerim je posvečena pozornost, so predvsem identifikacija in overjanje uporabnikov, kriptiranje, računalniško omrežje, operacijski sistemi in okolja, baze podatkov, programi ter zlonamerna programska oprema. Pozornost je posvečena tudi razpoložljivosti računalniškega sistema. Na koncu prvega sklopa je tudi poglavje o motnjah pri delovanju informacijskega sistema ter poglavje, ki predstavi sodobno elektronsko poslovanje banke ter zaščitno tehnologijo, ki se pri tem uporablja. Dobro poznavanje tematike prvega sklopa poglavij je nujno za nadaljnje ocenjevanje varnosti sistema.

Drugi sklop poglavij vsebuje na začetku splošen pregled razvoja teorij o modelih in vrednotenju varnosti informacijskih sistemov ter najbolj znane modele. Predstavljena je metoda, s pomočjo katere v organizaciji zmanjšamo tveganja. Ključna metoda v nalogi je analiza tveganja, katero sem izbral tudi za ocenjevanje varnosti informacijskega sistema banke. Kratek opis s primeri uporabe razloži njen potek, nato pa sledi poglavje, kjer sem se lotil ocenjevanja varnosti informacijskega sistema. V poglavju ocena varnosti informacijskega sistema je tematika obdelana pregledno, podrobnosti pa so v prilogi. Rezultat analize tveganj so ocene, ki osvetljujejo dejansko varnostno stanje. Na osnovi teh ocen sem v zadnjem poglavju podal ukrepe za kritična področja in priporočila za področja, kjer je varnost pogojno sprejemljiva.

2 INFORMACIJSKI SISTEM

2.1 Zgodovinsko ozadje in razvoj

Začetki informacijskega sistema v Novi Ljubljanski banki segajo v leto 1968, ko je banka kupila prvi računalnik IBM 360. Informacijski sistem v banki je bil v sedemdesetih in osemdesetih let dokaj zaprt sistem. Temeljil je predvsem na velikih centralnih računalnikih, ki so bili v računalniškem centru. Od leta 1985 do 1989 je začela banka intenzivno širiti svoje omrežje z uvajanjem sistema IBM 4700 na zunanje lokacije po vsej Sloveniji. Oddaljene lokacije in centrala so bile povezane preko stalnih najetih ali klicnih povezav. Delo z računalniki je obvladovalo razmeroma malo strokovnjakov, večina ljudi pa je opravljala na terminalih rutinska opravila. Sistemi so bili zaradi tega tudi precej varni.
Ko so se leta 1984 v banki pojavili prvi osebni računalniki, so se začeli podatki seliti iz glavnih na osebne računalnike, preko disket in modemov so se prenašali na druge osebne računalnike in se tako zbirali in obdelovali na več mestih. S tem se je širil krog uporabnikov, ki so imeli razmeroma enostaven dostop do podatkov, saj operacijski sistem DOS ni nudil praktično nobene zaščite zanje. Kako ranljivi so osebni računalniki in s tem tudi podatki na njih, pa je postalo jasno s pojavom prvih programov s škodljivim delovanjem - virusov.
Kasneje so se ob masovnem uvajanju osebnih računalnikov začela pojavljati prva lokalna omrežja, ki so ponujala nove enostavne in hitre načine pretoka podatkov ter nove storitve, med katerimi je bila leta 1989 elektronska pošta. Novi načini so omogočili enostaven dostop do podatkov ter hiter prenos velike količine informacij preko omrežja. Takrat je začela rasti tudi zavest, da je treba nekaj storiti, saj je postalo jasno, da je ugled podjetja odvisen tudi od tega, kako skrbi za varnost in zaupnost podatkov. Še posebej je to veljalo za organizacije kot so banke, ki so obdelovale zelo občutljive podatke.
Pojav globalizacije je prinesel s seboj tudi svetovno omrežje internet in banke so morale, če so hotele ostati v koraku s časom, ponuditi storitve svojim komitentom tudi preko tega novega medija. Tako je banka leta 1998 začela uvajati storitve elektronskega bančništva in se s požarnim zidom zaščitila pred vdori od zunaj. Po masivnem uvajanju mobilne telefonije so se lani pojavili tudi novi načini poslovanja z banko preko mobilnih telefonov. S temi novimi storitvami pa je postal bančni sistem še bolj odprt navzven in s tem izpostavljen možnim napadom.

Nova tveganja so banko vzpodbujala, da je zaposlovala vedno nove posebne strokovnjake in celo ekipe strokovnjakov, ki so se ukvarjali z vprašanjem, kako zaščititi informacijski sistem, da bo kos vsem grožnjam. V skrbi za varnost je banka leta 2000 ustanovila tudi Svet za varovanje informacij, ki ima za cilj sistematično uskladitev vseh aktivnosti z mednarodnima standardoma ISO 17799 ter BS 7799, tako da se tudi na tem področju obetajo izboljšave.

Banka posveča tudi veliko pozornosti kakovosti in varnosti poslovanja, še posebej na področju informacijske tehnologije. Tako je leta 2001 pridobila certifikat kakovosti informacijskega sistema ISO 9001/TickIT.

2.2 Informacijski sistem banke

V slovenskem prostoru je razmeroma veliko število bank, ki pa se po velikosti med seboj precej razlikujejo. Nova Ljubljanska banka d.d., Ljubljana (v nadaljnjem besedilu banka) je univerzalna banka z licenco Banke Slovenije za opravljanje vseh bančnih poslov v Sloveniji in tujini. Banka opravlja dejavnosti poslovnega bančništva, investicijskega bančništva in varčevanja. S svojo razvejano poslovno mrežo nudi storitve doma in v tujini za individualne stranke, javne ustanove, obrtnike ter mala, srednja in velika podjetja. Prek svojih hčerinskih podjetij upravlja tudi investicijske sklade, se ukvarja z nepremičninami, opravlja leasinške storitve, posle izvoznega faktoringa in finančnega svetovanja. Nova Ljubljanska banka je tudi največja slovenska banka, saj ima največje tržne deleže na ključnih področjih poslovanja, s svojimi hčerinskimi bankami pa obvladuje okrog 44% slovenskega prostora[1].

Taka široka zasnova ima za posledico tudi zelo velik in zapleten informacijski sistem, ki se je razvijal več desetletij. Strojno opremo predstavlja več glavnih računalnikov, okrog sto strežnikov, nekaj tisoč osebnih računalnikov, več sto kontrolnih enot in terminalov, veliko število bankomatov in POS-terminalov.
Ker je banka prisotna na celotnem slovenskem prostoru, je tudi omrežje razvejano po celi Sloveniji. Na centralni lokaciji je razmeroma kompleksen požarni zid, preko katerega poteka dostop do interneta, računalniško omrežje pa povezujejo stotine usmerjevalnikov, preklopnih stikal in modemov. Bančne poslovalnice so med seboj povezane s stalnimi najetimi povezami, obstajajo pa tudi klicne povezave, ki se uporabljajo, kadar se prekinejo najete zveze.
Čeprav se v zadnjem času vlaga veliko energije v poenotenje sistemov, je oprema še vedno precej raznolika. Takšna pestrost pa ima svojo razlago po eni strani v zgodovinskem razvoju bank, ko so se dogajali procesi razdruževanja in v zadnjih letih ponovnega združevanja, po drugi strani pa je posledica burnega razvoja tehnologije v računalništvu.
Pri programski opremi je zgodba podobna, velik del uporabniških programov je bil napisan kar v banki sami za lastne potrebe, nekaj uporabniških rešitev je bilo kupljenih, sistemska programska oprema in pisarniški paketi pa so urejeni z licenčnimi pogodbami. Tudi na tem področju poteka celovita prenova informacijskega sistema imenovana Sigma, ki bi naj v bližnji prihodnosti prinesla nove enotne rešitve, določene pa so že v uporabi.

[1] Predstavitev banke na internetu, 2002

Zaradi vsega naštetega je varovanje takega sistema kar precej trd oreh. Zaščititi je potrebno veliko število informacijski naprav, od katerih vsaka skupina zahteva nekoliko drugačen pristop, na primer varnostna politika na usmerjevalnikih se precej razlikuje od varnostne politike na osebnem računalniku, čeprav so izhodišča podobna. Prav tako je zaščita spletne poslovalnice Klik popolnoma drugačna kot zaščita programske opreme v običajni poslovalnici. Toliko različnih tehnologij pa zahteva veliko specializiranih strokovnjakov za vsako področje.

2.3 Varnost informacijskega sistema

Varnost informacijskega sistema je postopek zaščite in zavarovanja računalniške in programske opreme, podatkov, fizičnih naprav, omrežij in osebja pred nesrečami, namerno škodo ali naravnimi katastrofami[2]. To je neprekinjena aktivnost, ki traja 24 ur dnevno.
Vodstvo podjetja je odgovorno za postavitev temeljne varnostne politike. Razumeti mora, kaj ščiti in zakaj ter določiti, koliko sredstev je potrebno vložiti v varnostne ukrepe. Ukrepi morajo biti postavljeni zelo na široko, saj ni možno vedno vnaprej predvideti, od kod bo prišel napad. Za zagotavljanje varnosti je potreben sklop administrativnih, proceduralnih in tehničnih ukrepov[3]. Kontrole vodstva temeljijo na treh principih:

- posameznikovi odgovornosti,
- ločevanju nalog,
- nadzoru.

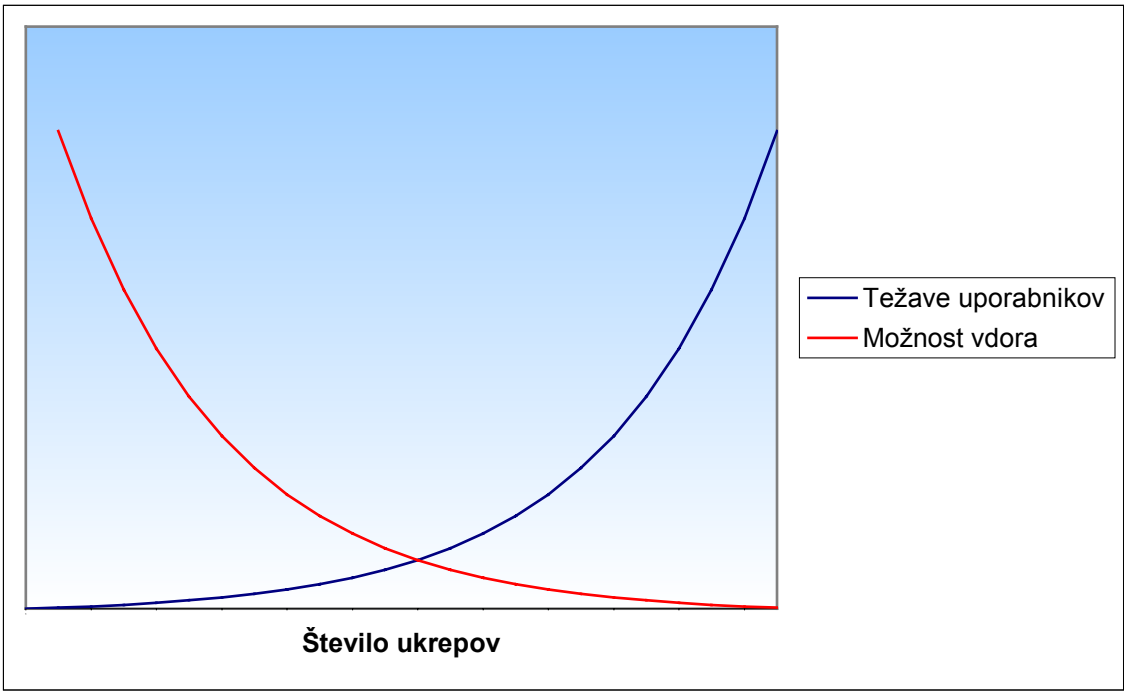
2.3.1 Obseg varnostnih ukrepov

Kljub temu da lahko rečemo, da sistem ni nikoli popolnoma varen, se postavlja pomembno vprašanje, koliko varnostnih ukrepov izvesti. Vsak varnostni ukrep v IS pomeni tudi neko oviro pri delu uporabnikov (npr. vnos gesla). Če je teh ukrepov preveč, je lahko to že moteče za redno delo. Poleg tega pa z naraščanjem števila varnostnih ukrepov narašča stopnja težavnosti za uporabnike eksponentno in ne linearno. Po drugi strani pa je sistem brez varnostnih ukrepov zelo ranljiv na vdore. Z večanjem števila ukrepov pa hitro upada verjetnost vdora oziroma zlorabe, vendar nikoli ne pade na 0. To stanje prikazuje Slika 1. Obliko obeh krivulj na grafu določijo upravljavci in administratorji IS s svojimi ukrepi. Točka, kjer se krivulji sekata, imenovana tudi izenačitvena točka, predstavlja stanje, kjer dela organizacija najbolj učinkovito. Če je količina ukrepov levo od izenačitvene točke, pomeni, da je preveč ogrožena varnost sistema na račun udobnosti dela. Količina ukrepov desno od izenačitvene točke po pomeni, da je število varnostnih ukrepov tolikšno, da že ovira

[2] Gupta, 2000, str. 327
[3] Caelli, 1994, str. 7

učinkovitost dela organizacije. Zaradi tega je pomembno, da se upravljavci IS zavedajo pomena krivulj.
Količina varnostnih ukrepov pa je odvisna tudi od politike vodstva. Varnostna politika je vedno kompromis med stroški in tveganji. Na grobo rečeno je sistem varen takrat, ko so stroški, ki jih imajo napadalci na sistem, večji kot koristi, ki jo pridobijo z uspešnim vdorom v sistem.

Slika 1: Razmerje med varnostnimi ukrepi, težavami uporabnikov in možnostjo vdora



Vir: Eckel, 1996, str. 424

Pravilna pot pri zagotavljanju varnosti v organizaciji je naslednja:

- Najpomembnejše je, da vodstvo spozna in razume pomen varnosti ter se zavestno odločiti vzpostaviti varnost v organizaciji.
- Drugi korak je, da se poiščejo tveganja, ki obstajajo v organizaciji. Ponavadi si pri tem pomagamo s sistematično metodo.
- Nato je potrebno oceniti ta tveganja in opredeliti, kakšno nevarnost v resnici predstavljajo za poslovanje ali celo preživetje organizacije. Tudi na tem koraku je dobrodošel pripomoček sistematična metoda, ki oceni tveganja.
- Na osnovi teh ocen je potrebno izdelati ukrepe, ki bodo zmanjšali tveganja. Ponavadi taki ukrepi niso ravno poceni, zato se je potrebno odločiti, katera tveganja so takšna, da se ne splača uvajati dodatnih kontrol. S tem pridemo do sprejemljivega tveganja za organizacijo.

2.3.2 Naložba v varnost

Kljub možni škodi nekatera manjša podjetja menijo, da je vlaganje v informacijsko varnost razmetavanje denarja. Pri večjih podjetjih je slika drugačna. Študija ameriškega inštituta za računalniško varnost iz leta 2000 ugotavlja[4], da namerava 60% podjetij povečati sredstva, ki jih namenja za informacijsko varnost. Raziskave tudi kažejo, da se za te potrebe namenja 1% do 3% denarja za informacijske sisteme.

Ignoriranje varnostnega področja lahko prinese podjetju neslutene izgube. Znan je primer glavne banke v New Yorku, ki je zaradi računalniškega vdora utrpela 34 milijonov dolarjev neposrednih izgub, poleg tega pa še veliko več posrednih.

Naložbo v varnost lahko smatramo tudi kot prihranek pri stroških, ki bi jih imelo podjetje pri morebitnem vdoru v informacijski sistem. V komercialnem svetu se stroški, ki jih povzročijo vdori, delijo na vidne in nevidne. Vidni stroški vdorov so lahko naslednji:

- izguba posla zaradi nerazpoložljivih informacijskih virov;
- izguba posla zaradi strank, ki so zaradi vdora prestopile h konkurenci;
- padec produktivnosti ali celo popolna prekinitev dela pri zaposlenih izven IT;
- stroški dela zaposlenih v IT zaradi ugotavljanja in popravljanja posledic vdora;
- stroški zbiranja dokazov in sodni stroški ob morebitnih sodnih postopkih;
- stroški povezani s pojasnjevanjem vdora v javnosti.

Nevidne stroške je težje opredeliti in meriti, nedvomno pa so opazni pri slabših poslovnih rezultatih. Povežemo jih lahko z izgubo konkurenčne prednosti podjetja zaradi vdora, kar ima za posledico zmanjšanje zaupanja strank, težave pri pridobivanje novih strank, zmanjšanje ugleda zaradi negativne publicitete in podobno. Afera, ki se je pojavila v zvezi z NLB in Klikom, ni povzročila neposrednih vidnih stroškov, je pa nedvomno povzročila kar nekaj nevidnih.[5]

[4] Gupta, 2000, str. 328
[5] Kuščer, 2002, str. 8

3 TEHNOLOŠKA ZAŠČITA INFORMACIJSKEGA SISTEMA

3.1 Zaščita pred vdori

3.1.1 Uvod

Eksplozivna rast interneta prinaša s sabo poleg obilice dobrot tudi veliko nevarnosti in pasti. Paleta je široka: od najstniških potegavščin do vdorov v računalniške sisteme, zlorabe elektronskega poslovanja, otroške pornografije, zlonamerne programske opreme in podobnega. Preko povezave v internet je napadenih vsako leto več podjetij, ki pa največkrat ne prijavljajo takih dejanj. Po ocenah skupine Gartner[6] se bo škoda zaradi računalniškega kriminala od leta 2001 do 2004 povečala od 10 do 100-krat. Problem pa je tudi nedorečena zakonodaja, ki v nekaterih državah sploh ne obravnava področij računalniškega kriminala.

Informacijski sistem predstavlja v sedanjem času srce podjetja, zato je pogosta tarča napadalcev. Zaradi tega ga je pomembno dobro zaščititi tako fizično kot logično.

Fizična zaščita pomeni ločitev prostorov in naprav informacijske tehnologije, zato da se zavarujejo pred prekinitvami in nepooblaščenim dostopom. Onemogoča krajo informacijskih sredstev, preprečuje dostop do občutljivih konzol in kriptografskih modulov ter zagotavlja zaščito pred nepooblaščenimi spremembami v opremi informacijske tehnologije. Največkrat se za fizično zaščito uporabijo posebni dobro zaščiteni prostori, ki so zaklenjeni, opremljeni z video nadzorom ter so varni pred požari in poplavami. V NLB so prostori v banki fizično zaščiteni v štirih conah z različnimi varnostnimi ukrepi. Bolj kot je cona bližje računalniškemu centru, bolj restriktivni so varnostni ukrepi in zaščite ter manj zaposlenih ima dostop vanjo.

Logična zaščita dostopa do informacijskih sistemov je težji oreh. Ukvarja se z omejevanjem dostopa tam, kjer ni fizičnih zaščit ali kot dopolnilo. Večkrat imata ti dve zaščiti skupne lastnosti. Pri logični zaščiti pride v poštev več tehnik in prijemov:

- identifikacija in overjanje uporabnikov
- kriptiranje, elektronski podpisi, digitalni certifikati

3.1.2 Identifikacija in overjanje uporabnikov

Identifikacija in overjanje uporabnikov se izvaja na treh dejstvih[7]:

- nekaj, kar uporabnik ve;
- nekaj, kar uporabnik ima;
- nekaj, kar uporabnik je.

[6] Cvjetović, 2001, str. 12
[7] Caelli, 1994, str. 456

Nekaj, kar uporabnik ve

Identifikacija na osnovi nečesa, kar uporabnik ve, je najbolj preprost in pogost način razpoznavanja uporabnikov. Pri tem se največkrat uporablja geslo ali PIN (Personal Identification Number). Skupna značilnost obeh načinov identifikacije je, da zagotavljata razmeroma visoko stopnjo zaščite pri minimalnih stroških, ne rabita dodatne opreme, upravljanje pa je lahko. Največja slabost pa je naslednja:

- če so gesla oziroma PIN-i kratki, si jih je moč hitro zapomniti, vendar jih je možno tudi hitro uganiti;
- če pa so dolga, si jih uporabniki ne zapomnijo, ampak si jih zapisujejo, zato jih lahko napadalci zlorabijo.

Pomembno je, da se gesla redno menjavajo, da so varno shranjena in da je vzpostavljen nadzor nad uporabo gesel.

Banka uporablja gesla pri dostopu do računalnikov, operacijskih sistemov in aplikacij, PIN-e pa pri bankomatih in POS-terminalih v kombinaciji z magnetno kartico. Na področju gesel zagovarja banka naslednjo varnostno politiko[8]:

- geslo mora vsebovati najmanj 6 znakov, na področju NT omrežja pa najmanj 8 znakov;
- geslo ne sme biti povezano z uporabnikovimi osebnimi podatki, datumom in podjetjem, ne sme vsebovati samo črkovnih ali samo številskih nizov;
- zamenjati ga je potrebno najmanj vsakih 30 dni;
- ne sme bit shranjeno na računalniku v nekriptirani obliki;
- zadnjih 12 gesel se ne sme ponavljati;
- po določenem številu napačnih prijav (3-5) se mora uporabnika avtomatsko blokirati;
- gesla ne smejo biti shranjena v računalniški aplikaciji skupaj s podatki. Shranjena morajo biti z uporabo enosmernega šifrirnega algoritma.

Nekaj, kar uporabnik ima

Identifikacija na osnovi nečesa, kar uporabnik ima, zahteva od uporabnika nek žeton, s katerim se identificira. Prednosti te metode je v tem, da mora napadalec imeti žeton, preden lahko napade. Navadno je žeton zaščiten še s PIN-om zaradi zaščite pred krajo. Pomanjkljivost tega načina pa je nekoliko višja cena, kot pri načinu z geslom/PIN-om ter potreba po napravi, ki bere žeton. Magnetne kartice so tipičen in najpogostejši primer za identifikacijo na osnovi nečesa, kar uporabnik ima. V zadnjem času pa jih izpodrivajo tako imenovane pametne kartice, ki imajo možnost varnega shranjevanja in/ali procesiranja podatkov. V Hong Kongu, na primer, jih nameravajo uporabljati kot osebne izkaznice za vse prebivalce že leta 2003[9].

[8] Obvladovanje dostopa do sistema, 2001
[9] Winggins, 2002

Obstajajo pa tudi super pametne kartice, ki premorejo poleg vsega, kar ima pametna kartica, še tipkovnico, zaslon in baterijo in vse to skupaj na ploščici velikosti kreditne kartice. Uporaba pametnih kartic je široka, saj se lahko uporabljajo za:

- elektronsko denarnico,
- za zavarovanje bančnih transakcij,
- kontrolo dostopa,
- hranjenje osebnih podatkov,
- osebno kriptirno napravo,
- zamenjavo večih magnetnih kartic.

Poznamo tudi žetone za generiranje gesel. To so naprave, ki so podobne kalkulatorju in temeljijo na sinhroniziranih urah v žetonu in v sistemu, na katerega se uporabnik prijavlja. Žeton na osnovi ure in uporabnikovega PIN-a generira geslo, ki je veljavno samo toliko časa, da se uporabnik lahko normalno prijavi v sistem.

Banka uporablja magnetne plačilne kartice Maestro in kreditne kartice Karanta. Uporaba teh kartic je pri poslovanju z bankomati in novejšimi POS-terminali kombinirana še z osebno identifikacijsko številko (PIN). Pri elektronskem poslovanju pa se pametne kartice uporabljajo za shranjevanje digitalnega certifikata pri poslovanju preko Klika, Proklika in Proklika Plus ter sistemov SMPV (sistem plačil malih vrednosti) in S.W.I.F.T.. Generatorje gesel banka uporablja pri prijavljanjih v določene bolj občutljive sisteme.

Nekaj, kar uporabnik je

Metode identifikacije na osnovi nečesa, kar uporabnik je, so poznane tudi pod imenom biometrične metode. Izkoriščajo neko edinstveno fizično ali značajsko lastnost uporabnika. Te lastnosti so lahko prstni odtis, očesna mrežnica, oblika roke, podpis, glas, razporeditev ven itd. Dobre lastnosti tega načina so, da ni treba uporabniku imeti ničesar pri sebi, pa tudi vedeti mu ni treba ničesar. Napadalec težko prevara ali najde pomanjkljivost pri tem načinu identificiranja. Slaba stran tega načina pa je, da so lahko naprave za zajemanje vzorcev sorazmerno drage, zato se uporabljajo v glavnem za zaščito pomembnejših sistemov. Lahko so tudi neprijetne (npr. skeniranje očesne mrežnice), ali pa neprimerne za vse uporabnike (npr. prstni odtis pri invalidih). Je pa tudi res, da so občutljive na številne zunanje vplive in da niso popolnoma zanesljive. Tipično je zanesljivost nekje od 99% do 99,9%, odvisno od posameznega sistema, zato se ta način večkrat uporablja v kombinaciji z drugimi metodami.

V banki se biometrične naprave uporabljajo v kombinaciji z magnetnimi karticami za kontrolo pri fizičnem dostopu v glavni računalniški center.

3.1.3 Kriptiranje

Splošno

Kriptografija je ena glavnih metod za logično zaščito dostopa. Prvenstveno je namenjena za zagotavljanje tajnosti informacij, vedno bolj pa se uveljavlja za zagotavljanje neoporečnosti, celovitosti sporočil. Omogoča ugotavljanje nedovoljenih sprememb informacij, omogoča dokazovanje legitimnosti sporočil, izkazovanje identitete uporabnikov in onemogoča zanikanje.
Šifriranje je kompleksen postopek skrivanja sporočil, ki zahteva precejšnjo računsko moč. Pri postopku se uporabljata šifrirni ključ in kriptografski algoritem, s pomočjo katerega se besedilo pretvori v nerazpoznavno obliko. Dešifriranje je obraten proces, ki iz šifriranega besedila dobi navadno besedilo.

V splošnem ločimo dve vrsti kriptografskih sistemov:

- Simetrični - šifrirni in dešifrirni ključ sta lahko enaka ali pa se da eden enostavno izračunati iz drugega.
- Asimetrični - ključa sta različna in se ne da eden enostavno izračunati iz drugega.

Simetrični algoritmi imajo prednost v hitrosti šifriranja, so pa problematični pri razdeljevanju ključev, saj mora ključ ostati vedno skrit pred napadalcem. Tipičen predstavnik simetrične kriptografije je DES (Data Encryption Standard).
Asimetrični algoritmi pa za razliko od prvih nimajo problemov z razdeljevanjem ključev, saj obstajata dva različna ključa, so pa neprimerno počasnejši od simetričnih. Primer teh algoritmov je RSA. Problem pri asimetrični kriptografiji je tudi veliko število ključev pri velikem številu subjektov, ki si izmenjavajo sporočila. Zato se večkrat v praksi uporablja kombinacija obeh algoritmov, da se izkoristijo dobre strani obeh sistemov, asimetrične za šifriranje ključev, simetrične pa za šifriranje podatkov.

Šifrirne algoritme lahko delimo tudi glede na način šifriranja, poznamo bločne in pretočne algoritme. Pri bločnem šifriranju se šifrira blok podatkov za blokom, pri pretočnem pa se šifrira besedilo bit po bitu. Primer pretočnega šifrirnega algoritma je RC4-algoritem z variabilno dolžino ključa do 2048 bitov, primer bločnega pa AES. DES je zanimiv tudi po tem, da obstajajo različice pretočnih in bločnih algoritmov[10].

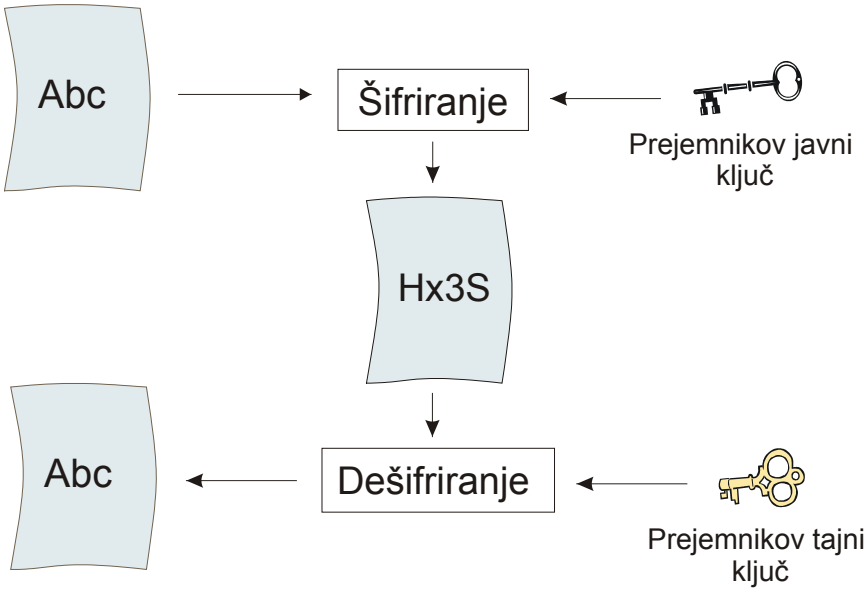
Banka uporablja oba načina kriptiranja. Storitev Proklik^{+}, na primer uporablja asimetrični algoritem RSA za avtentikacijo in izmenjavo ključev, pri čemer je ključ 1024-bitni, in simetrični algoritem RC4 za kodiranju podatkov, ta pa uporablja 128-bitni ključ.

[10] Vidmar, 1997, str. 177

Šifriranje z javnim ključem, elektronski podpis in certifikati

Šifriranje z javnim ključem je asimetrično šifriranje z algoritmom RSA, ki uporablja dva različna ključa; tajnega in javnega. Javni ključ je lahko objavljen, ne rabi varnega kanala za prenos, tajni pa mora biti skrbno varovan.
Če hoče oseba A poslati osebi B zaupno besedilo, mora dobiti javni ključ osebe B. S tem ključem šifrira besedilo ter ga pošlje prejemniku. Samo prejemnik, ki pozna svoj tajni ključ, pa ga lahko dešifrira s svojim tajnim ključem (Slika 2).
Operacija šifriranja po algoritmu RSA je računsko precej zahtevna, zato utegne trajati šifriranje dolgega sporočila kar precej časa. V veliko primerih poslovne uporabe pa ne rabimo šifriranja zaradi tajnost besedila, ampak samo zagotovilo, da se besedilo med prenosom ni po nesreči pokvarilo ali namerno spremenilo in zagotovilo, da je res od določenega uporabnika. To pomeni, da je treba zagotoviti celovitost in avtentičnost besedila.

Slika 2: Asimetrično kriptiranje



Tudi v tem primeru si lahko pomagamo z RSA-algoritmom. Uporabi se zgoščevalna funkcija, ki preslika celotno pošiljateljevo besedilo v blok podatkov. Vsaka, tudi najmanjša, sprememba besedila ima za posledico drugačen blok. Ta blok se podpiše s tajnim ključem pošiljatelja in tako dobimo elektronski podpis, ki se doda k originalnemu besedilu ter se pošlje prejemniku. Prejemnik pa nato s pomočjo pošiljateljevega javnega ključa dešifrira podpis in sam še enkrat izvede isto zgoščevalno funkcijo nad besedilom pošiljatelja in dobi prav tako blok podatkov. Če se bloka ujemata, potem je lahko zelo prepričan, da je podpis pravi[11].

Da pa lahko prejemnik verjame, da je javni ključ, ki mu ga ponuja pošiljatelj, res njegov, mu mora le-ta ponuditi potrdilo neke ustanove, ki jamči za resničnost

[11] Jerman Blažič, 2001, str. 108

podatkov. Ta ustanova, overitelj, izda lastniku javnega ključa digitalno podpisano potrdilo, ki se imenuje tudi certifikat. Certifikat vsebuje poleg lastnikovega javnega ključa tudi druge podatke, kot je ime lastnika, ime overitelja, obdobje veljavnosti, različico formata certifikata, ime algoritma in drugo.

Uporaba v banki

Elektronski podpis je v Sloveniji postal pravno veljaven s sprejetjem zakona o elektronskem poslovanju in elektronskem podpisu leta 2000[12]. Banka uporablja ta način podpisovanja pri poslovanju z Banko Slovenije s pomočjo varnostnega paketa PGP Personal Privacy[13]. Paket uporablja hibriden kriptografski sistem, ki podatke najprej stisne in zaščiti z enkratnim ključem seje, nato pa uporabi še kriptografijo z javnim ključem. Omogoča elektronsko podpisovanje, šifriranje sporočil, šifriranje podatkov na disku, varno brisanje in podobno.
Pri poslovanju banka uporablja tudi programski paket Entrust/Intelligence, ki uporablja za osnovo Entrust/PKI infrastrukturo z javnim ključem. Paket omogoča naslednje varnostne storitve:

- šifriranje in podpisovanje datotek in sporočil;
- enkratno prijavljanje v Entrust Ready aplikacije;
- časovno overjanje datotek;
- varno brisanje datotek.

Oba programska paketa ponujata precej podobne storitve, razlika je le v tem, da prvega uporablja pri svojem poslovanju Banka Slovenije, drugega pa NLB.

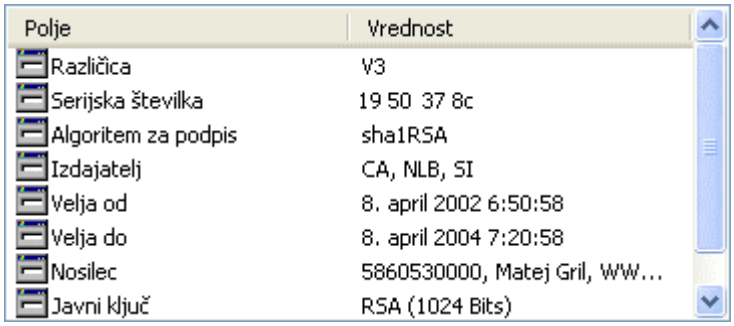
Banka uporablja digitalne certifikate za zaščito elektronskega poslovanja pri aplikacijah Klik, Proklik, Proklik$^+$. Certifikat preverja brskalnik, ki med drugim podpira 128-bitni ključ in šifriranje RC4 ter trojni DES, vendar pa pri tem obstajajo omejitve, ki imajo zgodovinsko ozadje. Ameriški zakon[14] uvršča šifrirno opremo med orožje, zato veljajo za tako opremo omejitve. Najprej je veljala splošna omejitev izvoza take opreme na 40-bitne ključe, leta 1998 pa so dovolili uporabo 56-bitnih ključev in dodatno izjemo, imenovano "Server Gated Cryptography (SGC)", ki je vezana na strežnikov certifikat. Ob vzpostavitvi povezave brskalnik preveri strežnikov certifikat. Če ima ta vključen dodatek SGC za rabo ključa, brskalnik ve, da sme uporabljati neomejene ključe (npr. 128 bitov za RC4). Vendar pa take certifikate lahko podeljujeta samo Verisign in od konca leta 1999 tudi Thawte. Lahko jih dobijo le bančne, finančne in zdravstvene organizacije ter trgovci za poslovanje izven ZDA, iz držav, ki niso prepovedane. Slovenija je med dovoljenimi državami, zato imajo strežniki Ljubljanske banke, SKB ter Eona take Verisignove certifikate. Američani so 14. januarja 2000 objavili nov predpis, ki je dovoljeval objaviti izvorno kodo programov in algoritmov za šifriranje podatkov in izvoz algoritmov, ki se jih je tako ali

[12] ZEPEP, 2000
[13] An introduction to cryptography, 2000
[14] Lah, Zaščita podatkov na internetu s šifriranjem

tako že prej dalo dobiti iz strežnikov po svetu, ter zvišal zgornjo mejo za ključe simetričnih algoritmov na 64 bitov. Vendar pa veljajo še vedno nekatere omejitve.

Certifikat, ki ga uporablja banka, ustreza priporočilu ITU-T X.509 (1997), vključuje X.509 različico 3 in njihove pripone. Formati digitalnih certifikatov podpirajo tudi X.509 verzijo 1 po internetnem standardu RFC 1422. Življenjska doba certifikata je 2 leti. V večini primerov pri poslovanju se certifikat nahaja na pametni kartici, ki jo ima uporabnik. Dostop do kartice je še dodatno zaščiten z geslom, poleg tega pa se kartica tudi samodejno uniči po treh zaporedno napačno vnesenih geslih.
Primer takega certifikata je na spodnji sliki (Slika 3):

Slika 3: Certifikat



Agencija za certificiranje Nove Ljubljanske banke[15] overja komitente banke ter jim izdaja digitalne certifikate. Delovanje agencije je usklajeno z zakonom o varstvu osebnih podatkov in zakonom o elektronskem poslovanju in elektronskem podpisu. Osnovna varnostna izhodišča overitelja, agencije za certificiranje NLB, so skladna s standardom PSIST BS7799, delovanje pa ustreza predpisom za področje kriptiranja FIPS PUB 140-1, nivo 2. Standardi zajemajo tako varnost na področju informacijske tehnologije, kakor tudi na področju upravljanja z elektronskimi potrdili - digitalnimi certifikati. Njihova uporaba je možna, če je zagotovljena pristnosti, avtorizacija, zaupnost, celovitost, preprečevanje zavračanja (tajenja), nadzor pretoka in hierarhični princip. Da so posredovani podatki in digitalni certifikati vredni zaupanja, jamči overitelj s svojim kvalificiranim privatnim šifrirnim in podpisnim elektronskim ključem.

Tveganja povezana s šifrirnimi sistemi in varnost

Napadalci na kriptirne sisteme, kriptoanalitiki, skušajo razbiti kriptirano besedilo, da pridejo do njegove vsebine, ali pa ga neopaženo spremeniti. Napadejo lahko algoritem ali pa slabosti v šifrirnem sistemu. Če uporabljamo splošne, javno poznane kriptirne algoritme, za katere ni znano, da bi bili razbiti, lahko napadalec poskuša ugotoviti besedilo tako, da preskuša vse možne kombinacije. To pa utegne tudi z zelo dobro opremo trajati predolgo, pri pogoju da uporabljamo dovolj dolge ključe. Kaj je dovolj dolg ključ, je precej relativno, odvisno je od algoritma. Še nedavno je pri

[15] Javna varnostna politika overitelja, NLB, 2001

simetričnih algoritmih zadostoval 64-bitni ključ, danes pa je boljše, če je 128-bitni. Veliko boljša možnost za napadalca je, da si pridobi šifrirni ključ zaradi slabe varnostne politike v organizaciji. S tem oborožen napadalec lahko pošilja tudi lažna finančna sporočila, kar je še posebej nevarno v organizacijah, kot so banke.
Poseben primer napada je tudi napad s ponavljanjem, kjer napadalec prisluškuje na kanalu, ugotovi, kje je kodirano sporočilo, ki je zanj zanimivo (npr. bančna transakcija), in to sporočilo še enkrat pošlje.

Navaden algoritem DES danes ne velja več za varnega, saj je potreben čas za razbijanje 56-bitnega ključa z računalnikom vrednim 1.000.000$ le nekaj minut. Predstavlja pa standard, zato se v praksi uporablja trojni DES. Pri tem načinu se podatki šifrirajo trikrat z različnim ključem, kar pa pomeni tudi, da je ta način trikrat bolj počasen. Uveljavlja pa se že njegov naslednik AES (Advanced Encryption Standard)[16], ki je hitrejši, šifrira 128 bitov dolge bloke in uporablja 128, 192 ali 256 bitov dolge ključe.
Raziskava Arjana Lenstre in Erica Verheula: Selecting Cryptographic Key Sizes[17] iz konca leta 1999 priporoča za simetrične algoritme (RC2, RC4, IDEA, DES, 3DES …) vsaj 86-bitne ključe. Za asimetrične algoritme (RSA, Diffie-Hellman …), pa priporoča za leto 2000 vsaj 952 bitov, za 2001 vsaj 990 bitov, za 2002 pa 1028 bitov.
Zanimiva je tudi ena zadnjih raziskav s področja razbijanja ključev algoritma RC5-64[18] (64-bitni ključ). Uporabljen je bil način surove moči za odkrivanje skritega sporočila, in sicer preko projekta Distributed.net. Vključenih je bilo 331 252 uporabnikov, ki so dobili pakete podatkov s kodiranim sporočilom ter načine, na katerega so ga poskušali dešifrirati. 25. septembra 2002 so sporočilo po 1757 dneh (ali nekaj manj kot petih letih) končno uspeli razkriti, pri tem pa so preizkusili kar $1{,}57 \cdot 10^{19}$ ključev. S tem so potrdili tezo, da podatki ne bodo varni 7 let.

3.2 Računalniško omrežje in zaščita

3.2.1 Uvod

Današnji računalniški sistemi temeljijo na telekomunikacijskih omrežjih, ki povezujejo različne oddaljene lokacije. Problem zaščite omrežja nastopi zaradi zelo velikega števila vstopnih točk in različnih možnosti dostopa. Tipično omrežje srednje velikega podjetja sestavlja več sto računalnikov različnih vrst, v njem je v uporabi vsaj nekaj protokolov in ima vzpostavljeno stalno povezavo do interneta ter poleg tega vsebuje še klicne povezave.
Iz leta v leto narašča računalniški kriminal, vdiralci poskušajo pridobiti možnost dostopa do računalniških sistemov, pri tem pa izkoriščajo pomanjkljivosti v

[16] Vidmar, 2002, str. 571
[17] Lah, 2002
[18] Distributed.net, 2002

programski opremi ali pa izkoriščajo slabosti pri administraciji. Napadalci so različni: hekerji, zaposleni v podjetju, industrijski vohuni in drugi. Motivov za vdiralce je več, od želje po samodokazovanju, ustvarjanju določenega slovesa med somišljeniki, do kraje ali spreminjanja podatkov v koristoljubne namene ali pa je to celo kraja, uničevanje ali spreminjanje podatkov z namenom onemogočanja konkurence. Cilj napadov na računalniške sisteme pa je lahko:

- kraja denarja (najbolj priljubljen cilj),
- kraja podatkov,
- kraja storitev,
- kraja programov,
- sprememba podatkov,
- uničevanje podatkov,
- onemogočanje storitev za legitimne uporabnike (z ustvarjanjem prometa, ki preseže sposobnost strežbe),
- sabotaža,
- vandalizem.

S tem ko postajajo računalniški sistemi in omrežja vse bolj odprta in lažje dostopna za uporabnike, narašča tudi možnost zlorab in število točk, ki jih je treba zaščititi. Arhitektura odjemalec/strežnik, ki je danes v splošni rabi, je precej odprta in s tem občutljiva na zlorabe. S povezavo poslovnega omrežja podjetja s svetovnim spletom se odprejo nova dodatna vrata v svet, ki jih lahko izkoristijo napadalci, zato je potrebno ta segment še posebej dobro zaščititi. Po raziskavah ameriškega inštituta za računalniško varnost[19] in FBI[20] je zaslediti strmo rast računalniškega kriminala. Tabela (Tabela 1) prikazuje odstotke podjetij, ki so zasledila razne vrste zlorab in kriminala v letu 2000 in 2001.

Tabela 1: Porast računalniškega kriminala

Vrsta zlorabe	2000	2001
Vdor v omrežje	57%	85%
Internet je najpogostejša točka, od koder izvira napad	59%	70%
Zloraba interneta s strani zaposlenih	79%	91%
Napadi zlonamerne programske opreme	85%	94%
Napadi s ciljem onemogočanja storitev	60%	78%
Kraja informacij	8%	13%

Vir: Organizations under attack, Sonicwall, 2002

Lani je kar 64% podjetij v ZDA priznalo finančne izgube zaradi računalniških vdorov. Do napadov znotraj sistema je prišlo pri 31% podjetij, tako da je do sedaj veljavno pravilo, da prihaja največ napadov znotraj sistema, do 80%, s tem postalo zastarelo.

[19] Gupta, 2000, str. 331
[20] Organization under attack, Sonicwall, 2002

3.2.2 Omrežje banke

Bančno omrežje velikega dosega (WAN) se razteza preko celotne države, banka ima poslovalnice skoraj v vsakem večjem kraju. Slika (Slika 4) prikazuje večje enote po Sloveniji. Večje poslovalnice so povezane z zakupljenimi digitalnimi povezavami kapacitete od 128 kbit do 512 kbit, odvisno od velikosti poslovalnice. Poteka pa že nadgradnja kapacitet povezav na najmanj 2 Mbit.

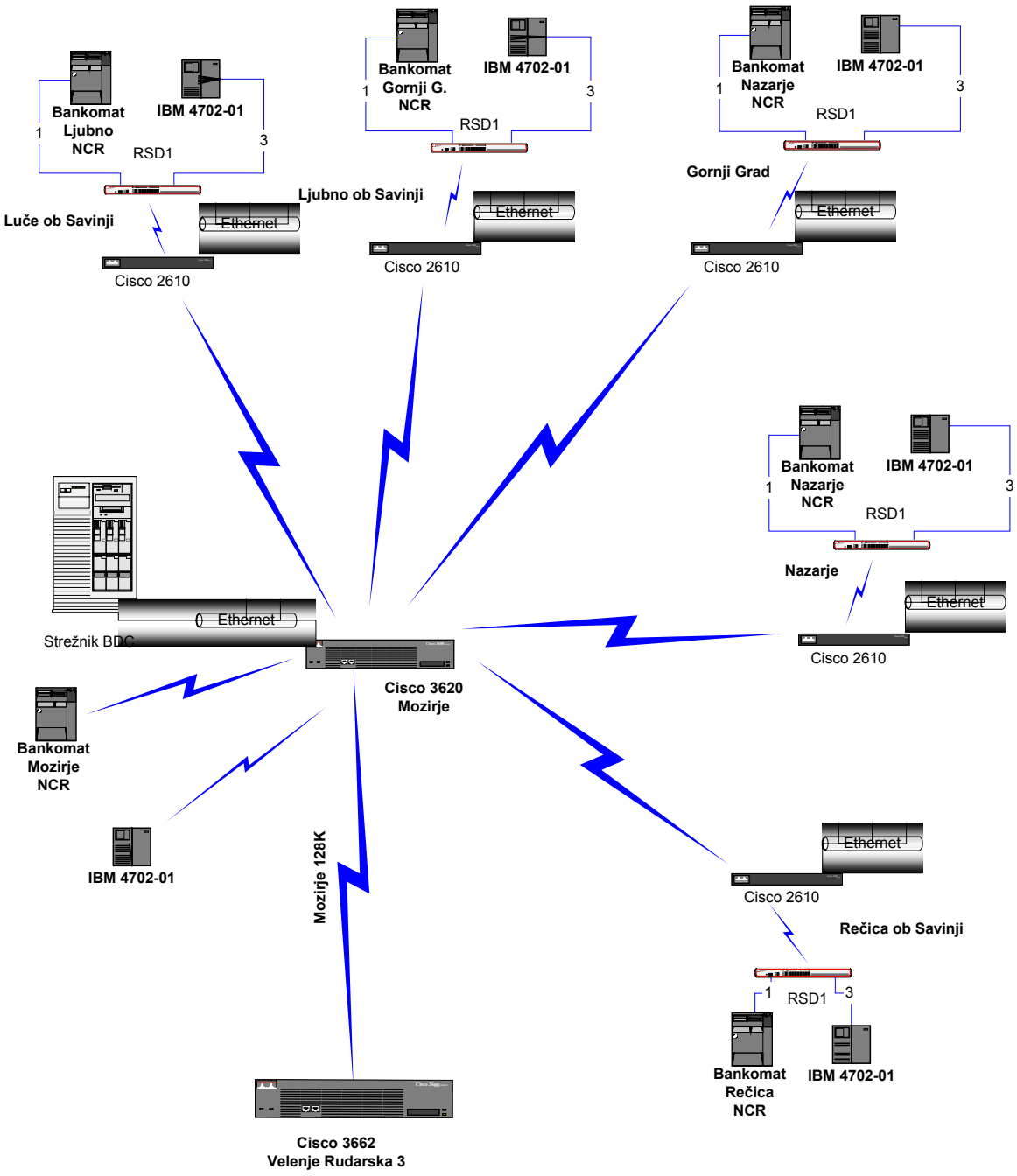
Slika 4: Večje poslovalnice banke po Sloveniji

Večje poslovalnice so naprej povezane z manjšimi, tu pa so povezave od 64 kbit do 128 kbit, prav tako poteka faza širitve kapacitete povezav na najmanj 512 kbit. Slika (Slika 5) prikazuje področje, ki ga pokriva regionalna divizija Velenje. Poleg stalnih najetih povezav pa so povsod še klicne ISDN povezave, ki se avtomatsko vzpostavijo ob prekinitvi najetih povezav. Pot, po kateri se vzpostavlja klicna ISDN povezava, poteka, kolikor je to mogoče, po drugi relaciji kot pot glavne povezave, da se s tem zmanjšajo tveganja prekinitve obeh povezav ob morebitnih prekinitvah glavnih povezav Telekoma.

Slika 5: Področje divizije Velenje

Na večjih poslovalnicah so postavljeni sekundarni domenski strežniki, ki služijo poleg drugega tudi za lokalno razdeljevanje programov ter za varnostno kopiranje podatkov. Manjše bančne enote so povezane na večje poslovalnice, na vsaki je usmerjevalnik, na katerega je povezano digitalno vozlišče z bankomati, kontrolnimi enotami IBM in lokalno omrežje z osebnimi računalniki. Slika (Slika 6) prikazuje poslovalnico Mozirje z nekaj manjšimi enotami.
Za nadzor usmerjevalnikov se uporablja nadzorni protokol EIGRP. Konfiguracije vseh usmerjevalnikov se redno shranjujejo na poseben strežnik za nadzor, kjer so dostopne v primeru zamenjave usmerjevalnika.

Slika 6: Detajl omrežja banke



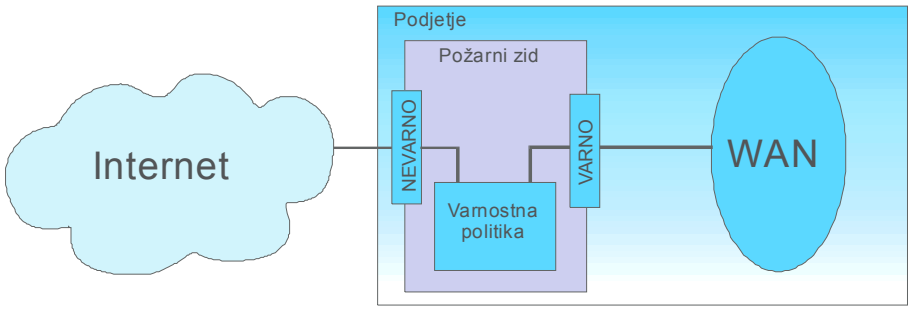
3.2.3 Požarni zid

Zavedati se je potrebno, da je varnost omrežja enaka varnosti njenega najšibkejšega člena. Povezava v internet je danes zagotovo najšibkejši člen, zato zahteva posebne varnostne ukrepe. Računalniki so v svetovni splet povezani po stalni povezavi in imajo največkrat stalne naslove[21]. S tem postane nujna uporaba nekih naprav, ki preprečujejo zunanje zlorabe informacijskih sistemov ter notranjim uporabnikom preprečujejo dostop do nedovoljenih zunanjih virov. Poznamo več vrst takšnih naprav[22]:

- Paketni filter – filtrira paketke glede na postavljena pravila. Preprost filter je usmerjevalnik. Deluje na mrežnem nivoju OSI-modela.
- Proxy – je program, ki dovoljuje ali ne dovoljuje dostop do določenih aplikacij med različnimi omrežji. Deluje na aplikacijskem nivoju OSI-modela.
- Požarni zid – je sistem ali omrežje sistemov, posebej opremljenih za nadzor prometa med omrežji. Obseg področja požarnih zidov je širok, zajema lahko vse od paketnih filtrov, stikal, računalnikov za prijavljanje do proyx-a.
- Prehod (gateway) ali obrambni gostitelj (bastion host) – je varen računalniški sistem, ki zagotavlja dostop do določene aplikacije.

Požarni zid je postavljen med LAN oziroma WAN-omrežjem in zunanjim omrežjem, kot je internet (Slika 7).

Slika 7: Požarni zid



Opravlja vlogo vratarja tako, da preverja pooblastila uporabnikov, preden jim dovoli dostop do omrežja ali pa jih zavrne. Preverja lahko imena, IP-naslove, aplikacije in podobno ter to informacijo primerja s pravili dostopa, ki jih določi administrator omrežja. V bistvu vsili varnostno politiko pri prehodu iz omrežja podjetja v zunanje omrežje in obratno. Varnostna politika pa se lahko drži enega od dveh osnovnih načel[23]:

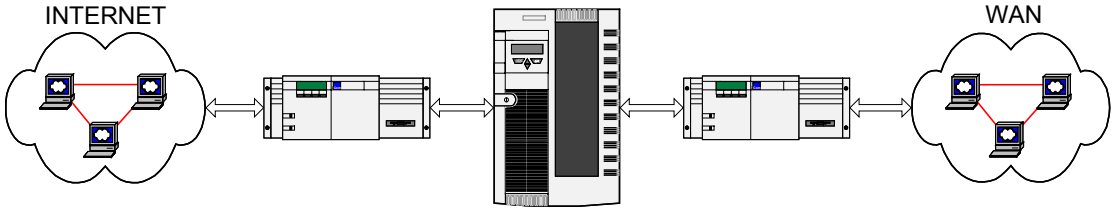
- kar ni izrecno dovoljeno, je prepovedano;
- kar ni izrecno prepovedano, je dovoljeno.

[21] Kenneth, 2001, str. 434
[22] Firewalls: a technical overview, 2002
[23] Ranum, str. 2

Prva možnost je bolj varna in prihrani administratorju veliko problemov, druga pa manj omejuje uporabnike pri delu.
Podjetje postavi požarni zid glede na zahtevo po varnosti, vrednost svojih podatkov in glede na ogroženost. Primer solidne izvedbe požarnega zidu je požarni zid (Slika 8), ki ga sestavljajo:

- dva filtra - usmerjevalnika, ki sta namenjena nadzoru paketov;
- aplikacijski pretvornik – filtrira na aplikacijskem nivoju, kjer lahko blokira posamezne storitve, kot so pošta, dostop do interneta …

Slika 8: Shema Izvedba požarnega zidu



Vir: Vidmar, 2002, str. 664

Požarni zid banke ščiti banko pred neželenimi zunanjimi vplivi na omrežje. Vsebuje večkratno filtriranje paketov in preverjanje prometa tako na transportnem nivoju kot tudi na aplikacijskem nivoju. Aplikacijski pretvornik predstavljajo različni računalniki z različnimi operacijskimi sistemi, da se izognemo možnosti vdora zaradi varnostne luknje v enem operacijskem sistemu. Požarni zid omejuje dostop do nekaterih strani in vsebin, ki niso povezane s poslovanjem banke, poleg ostalega pa je uvedeno tudi preverjanje prometa glede morebitne zlonamerne programske opreme.

3.2.4 Varnostni protokoli

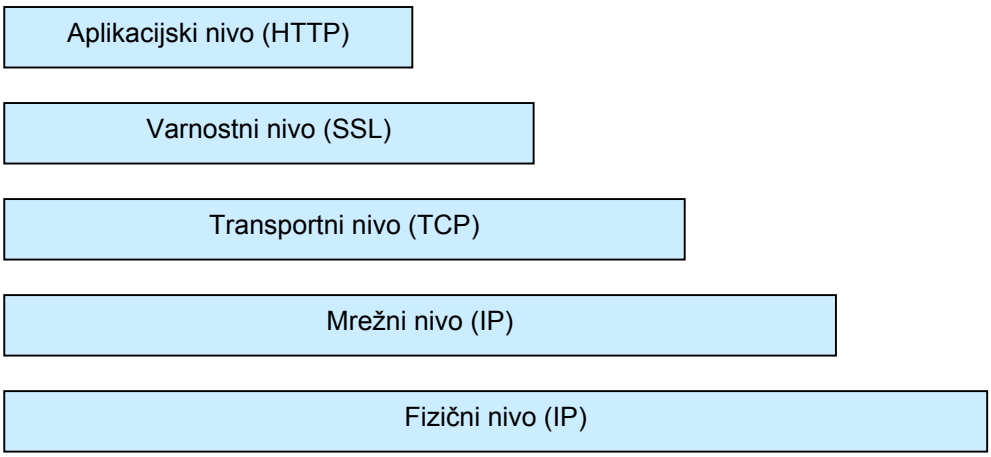
Protokol SSL

SSL (Secure Socket Layer) je varnostni protokol, ki ga je iznašel Netscape in prvič objavil različico v2.0 leta 1995, nato pa še istega leta v3.0. Dandanes predstavlja de facto standard. Odlikujejo ga odprtost, neopaznost za uporabnike, možnost dograjevanja z novimi kriptografskimi algoritmi ter učinkovitost. Omogoča vzpostavitev varne šifrirane povezave med dvema točkama, strežnikom in odjemalcem. S pridom ga izkoriščajo razne internetne aplikacije, saj na TCP/IP-povezavi zagotavlja:

- šifriranje podatkov,
- avtentikacijo strežnika in odjemalca,
- zaupnost sporočil,
- neoporečnost sporočil.

Vrinjen je med transportni in aplikacijski nivo. Temelji na TCP-protokolu in je neodvisen od aplikacij na višjih nivojih (Slika 9).

Slika 9: Položaj SSL protokola



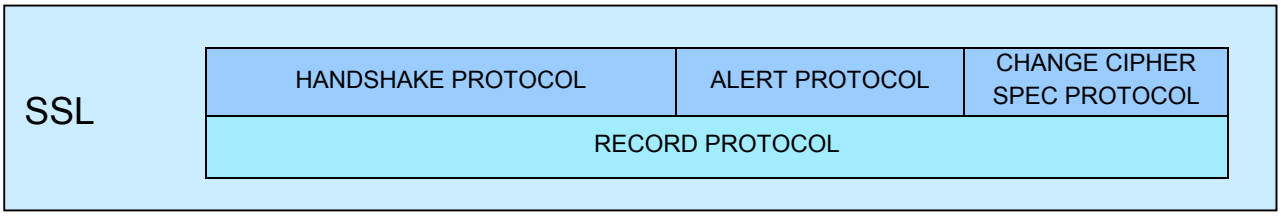
Vir: Cavin, 2000

Protokol SSL je sestavljen iz dveh slojev (Slika 10), na zgornjem sloju so protokoli:

- Handshake Protocol: skrbi za overjanje in dogovarjanje za algoritme in ključe za šifriranje;
- Alert Protocol: skrbi za obveščanje o napakah;
- Change Cipher Spec Protocol: namenjen zamenjavi šifriranja.

Na spodnjem nivoju pa leži Record Protocol.

Slika 10: Protokol SSL



Vir: Lah, 2000

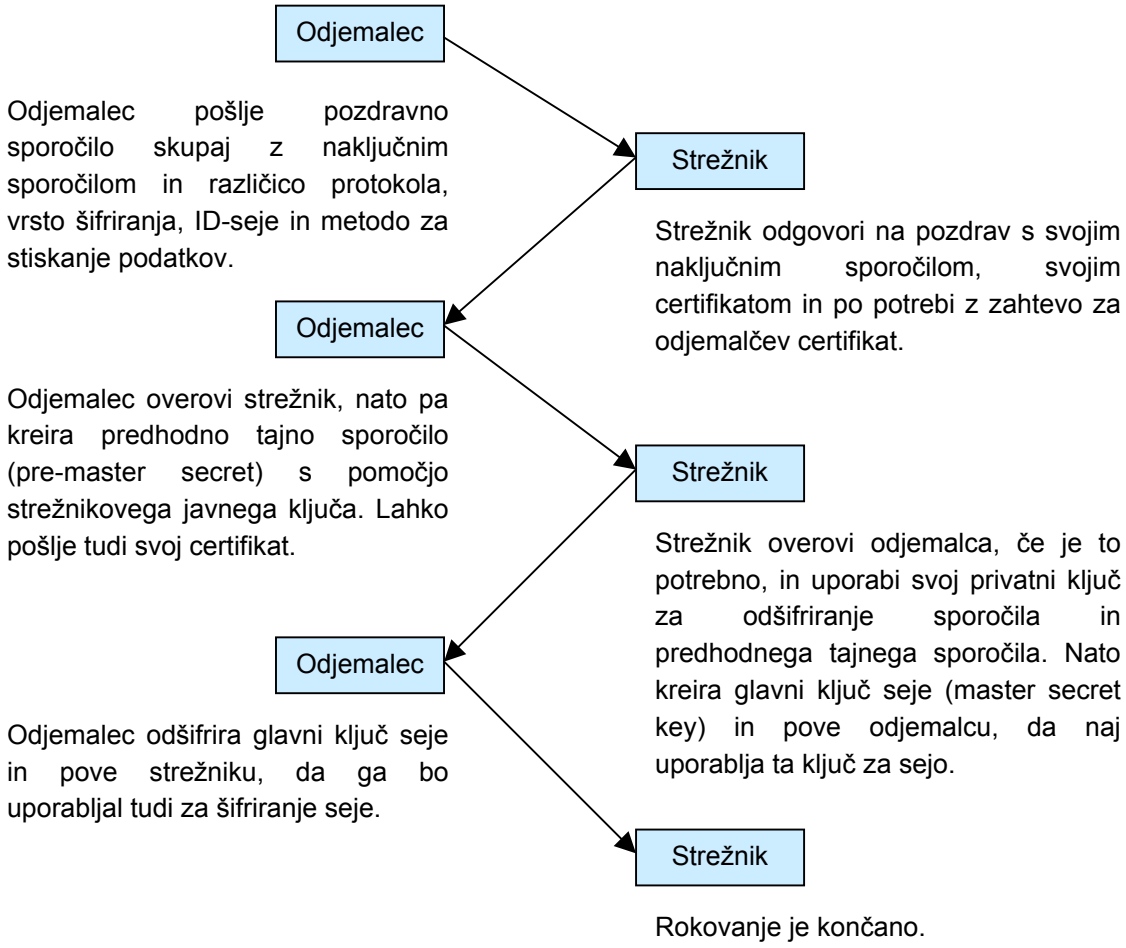
Protokol dopušča tri možnosti overjanja:

- obojestransko, vsak preveri certifikat nasprotne strani;
- enostransko, anonimni odjemalec preveri certifikat strežnika;
- overjanja ni, najslabša možnost, ker dopušča napad tipa »man-in-the-middle«, podatke, ki se sicer izmenjujejo šifrirani, lahko nekdo prestreže in spremeni.

Pri overjanju se uporabljajo digitalni certifikati tipa X.509v3. Nabor algoritmov, ki jih trenutno uporablja protokol, vsebuje 31 kombinacij asimetričnih in simetričnih algoritmov ter algoritmov za zgostitev podatkov, poleg teh pa obstajajo še algoritmi za stiskanje podatkov. Dokler se odjemalec in strežnik ne dogovorita za šifrirni algoritem, Record Protocol ne šifrira podatkov. Na začetku odjemalec pošlje nabor

algoritmov, ki jih podpira, strežnik pa izbere prvega tistega, ki ga podpira tudi sam. Če ne najdeta skupnega algoritma, podreta zvezo.
Protokol rokovanja (Handshake Protocol) poteka na naslednji način[24] (Slika 11):

Slika 11: Protokol rokovanja



Vir: Cavin, 2000

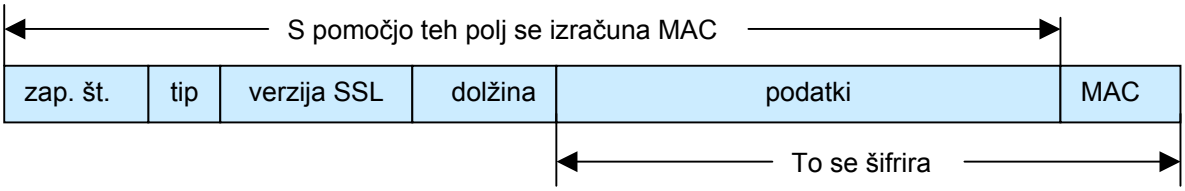
SSL loči podatke seje (neprekinjeno izmenjavo podatkov med odjemalcem in strežnikom) ter podatke povezave. Vsaki seji lahko pripada več povezav, ki so lahko tudi istočasne, vendar se za vsako povezavo uporablja drug ključ. Tako s ključem ene povezave ne moremo dešifrirati druge povezave. Po protokolu lahko traja ena seje največ 24 ur.

Change Cipher Spec Protocol je signal, ki ga odjemalec in strežnik pošljeta drug drugemu kot potrditev dogovorjenih parametrov. To se zgodi ob koncu protokola rokovanja, ko se preide iz načina brez šifriranja v način z dogovorjenim šifriranjem.
Alert Protocol pa skrbi za obveščanje sogovornika, da je prišlo do napake. Ob večji napaki se lahko povezava tudi prekine (če je na primer MAC-koda napačna).

[24] Cavin, 2000

Spodnji sloj (SSL Record protocol) razbije podatke na bloke določene dolžine ter vsakemu doda zaporedno številko sporočila, tip zapisa ter dolžino bloka podatkov. Nato iz teh polj in podatkov dobljenih iz višjih nivojev izračuna MAC (Message Authenticate Code), ki služi kontroli nespremenljivosti podatkov in za overjanje sporočila (Slika 12).

Slika 12: SSL Record protocol



Vir: Lah, 2000

Protokol poskrbi tudi za morebitno stiskanje podatkov pred šifriranjem. Nato se podatki in MAC zašifrirajo tako, kot je bilo dogovorjeno na zgornjem nivoju. SSL Record protocol nato preda podatke transportnemu nivoju pod sabo oziroma jih od njega sprejme.

Protokol SSL nima fiksno določenih algoritmov za šifriranje, tako da jih lahko določijo proizvajalci programskih produktov. Največkrat so implementirani asimetrični algoritmi za overjanje in izmenjavo ključev, kot je RSA, Fortezza in Diffie-Hellman ter simetrični za šifriranje DES, RC2, RC4, 3DES in IDEA. Naslednik tega protokola, TLS (Transport Layer Security), se od predhodnika le malo razlikuje.

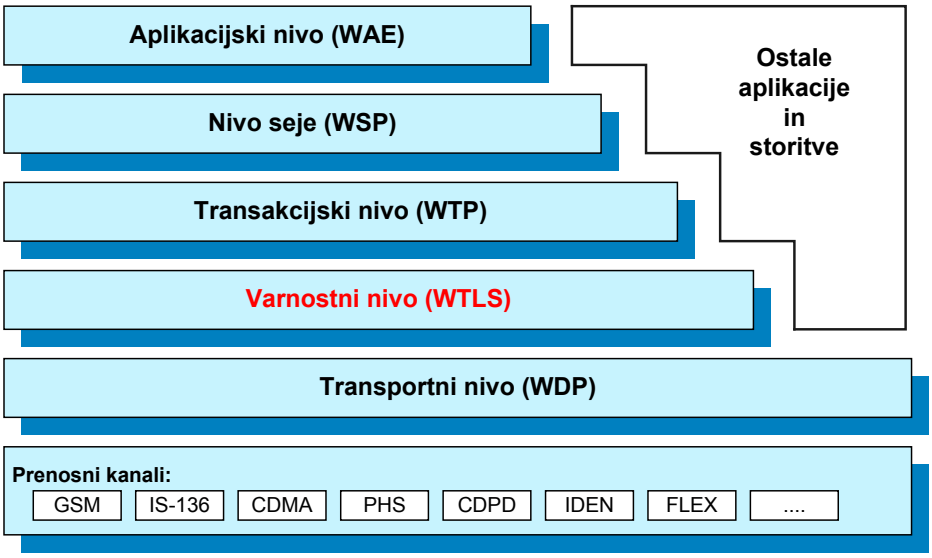
Primer uporabe protokola SSL v banki je aplikacija Klik. Tu se vsi podatki prenašajo prek protokola SSL, ta pa jih kodira s pomočjo algoritmov RSA (namenjen avtentikaciji in izmenjavi ključev) in RC4 (namenjen kodiranju podatkov). RC4 je tekoč šifrirni algoritem z variabilno dolžino ključa do 2048 bitov. Vgrajen je v brskalnike kot del protokola SSL oziroma TLS.

Protokol WTLS

Protokol WTLS (Wireless Transport Layer Security) predstavlja varnostni nivo protokola WAP (Wireless Application Protocol)[25]. Zasnovan je na standardnih protokolih SSL in TSL ter optimiziran za uporabo na ozko pasovnih komunikacijskih kanalih. Predstavlja de facto standard za zagotavljanje zasebnosti, neoporečnosti podatkov in overovljanje pri aplikacijah na mobilnih telefonih in drugih majhnih brezžičnih napravah.
V skladovnici WAP-protokolov (Slika 13) je WTLS umeščen med transportni in transakcijski protokol in zagotavlja višjim nivojem varen prenosni kanal[26].

[25] Šumak, 2000
[26] Jormalainen, 2000

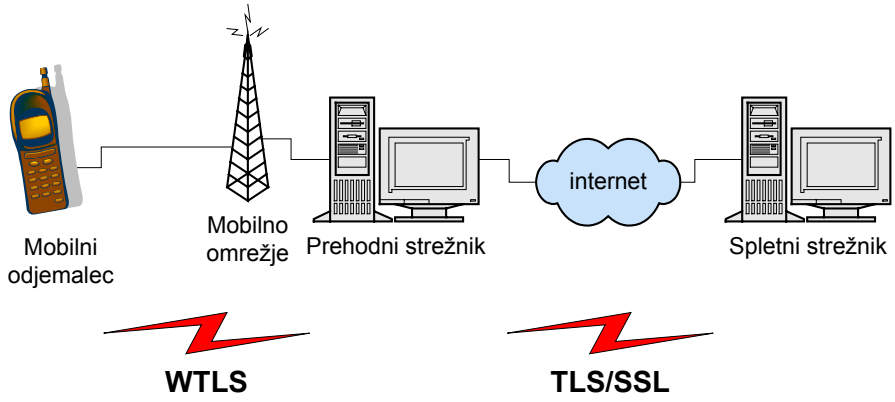
Slika 13: Skladovnica WAP protokolov



Vir: Jormalainen, 2000

Povezava med mobilno napravo in spletnim strežnikom poteka preko prehodnega strežnika – WAP-prehoda, kot kaže spodnja Slika 14. WTLS zagotavlja varnost WAP-protokola med dvema končnima točkama – mobilno napravo in WAP-prehodom (WAP Gateway).

Slika 14: Prenos podatkov med strežnikom in mobilno napravo



Vir: Šumak, 2000

WAP-prehod leži nekje na poti med WAP-odjemalcem in spletnim strežnikom. V bistvu nam WAP-prehod predstavlja most med internetom in brezžičnim svetom. Funkcije WAP-prehoda so naslednje:

- pretvarjanje WML-vsebine iz tekstovnega formata v binarni format, prilagojen tako, da ga WAP-naprava razume in interpretira;
- pretvarjanje zahteve po nekem naslovu, ki pride iz WAP-naprave v takšno obliko, ki je standardna v internetu in obratno;
- pretvarjanje med SSL kodirnimi metodami (ki se uporabljajo v internetu) in WTLS kodirnimi tehnikami (v svetu WAP-a).

Ko zakodirani podatki pridejo iz spleta v WAP-prehod, so zakodirani z uporabo protokola SSL. WAP-prehod jih mora dekodirati in zakodirati v obliko, ki jo narekuje protokol WTLS. To pa pomeni luknjo v varnosti. Prav zaradi te pretvorbe med SSL in protokolom WTLS so podatki določen čas na očem tistim, ki morebiti prisluškujejo WAP- prehodu. Če bi uporabili javno dostopen WAP-prehod, ne bi mogli zagotoviti popolne varnosti. Če pa uporabimo svoj WAP-prehod, ostanejo podatki v času, ko so dekodirani, v našem omrežju in pod našim nadzorom, zato je ta način bolj varen in uporabljen v banki.

Notranja arhitektura protokola WTLS je sestavljena iz dveh plasti, spodnjo plast predstavlja osnovni Record Protocol, na zgornji pa so štirje njegovi odjemalci:

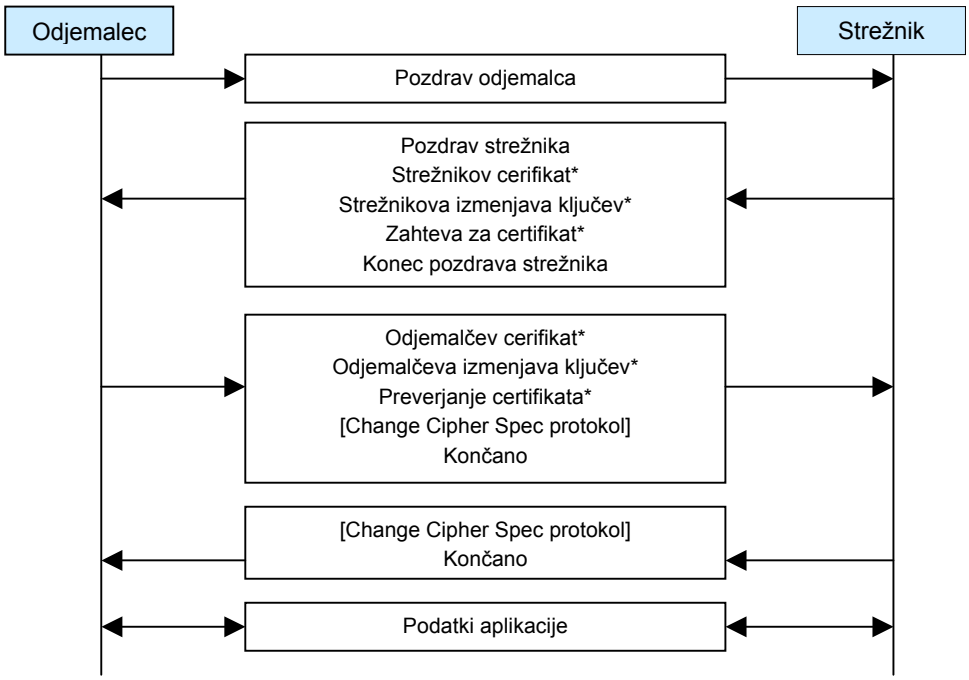
Tabela 2: Notranja arhitektura WTLS protokola

Hadshake Protocol	Alert Protocol	Application Protocol	Change Cipher Spec Protocol
Record Protocol			

Vir: Jormalainen, 2000

Protokol rokovanja (Handshake Protocol) je namenjen za izmenjavo varnostnih parametrov, kot so uporabljena verzija protokola, uporabljeni kriptografski algoritmi, informacije o uporabi overovljanja in tehnike uporabe javnega ključa. Poteka na naslednji način:

Slika 15: Diagram poteka Handshake protokola



Vir: Jormalainen, 2000

Alert Protocol poskrbi za morebitne napake in pošilja sporočila o napakah, Application Protocol pa je vmesnik za višje ravni v skladovnici WAP-protokolov.

Avtentikacija poteka s pomočjo certifikatov, je lahko obojestranska ali pa samo s strani odjemalca. Podprti so certifikati tipa X.509v3, X.9.68 ter certifikati tipa WTLS, ki so optimirani glede na velikost. Izmenjava ključev lahko poteka s pomočjo algoritmov RSA, Diffie-Hellman ali s pomočjo algoritmov eliptičnih krivulj Diffie-Hellman. Zasebnost WTLS zagotavlja s šifriranjem komunikacijskega kanala, uporablja pa naslednje bločne algoritme:

- RC5 s 40, 56 ali 128 bitov dolgimi ključi;
- DES, 3DES s 40 ali 56 bitnimi ključi;
- IDEA s 40, 56 ali 128 bitnimi ključi.

Za neoporečnost sporočil je poskrbljeno z uporabo MAC-kod (Message Authentication Codes), ki uporabljajo SHA ali MD5-algoritme, dolžina MAC-kod je lahko 0, 40 ali 80 bitov

Protokol je bil razvit za široko uporabo na vseh mobilnih napravah. Najšibkejše naprave ne morejo uporabljati močnejših kriptirnih metod, ker so omejene pri procesni moči, pomnilniku ter s širino komunikacijskega kanala. Varnost je seveda povezana z uporabljenimi metodami kriptiranja, zato je lahko pri šibkejših napravah omejena. Čeprav protokol dovoljuje tudi anonimno povezavo, je lahko varnostno precej tvegana, saj ne izključuje napada tretjega, ki lahko vpade med odjemalca in strežnik. Pomanjkljivost pri tem protokolu je lahko tudi zakonodaja, ki ne dovoljuje dovolj dolgih ključev, ki bi omogočili dovolj varno šifriranje sporočil. WTLS predvideva uporabo 168-bitnega ključa, vendar ne izven ZDA. Dolžina ključa 40 bitov danes ne zagotavlja varnosti.

Največja pomanjkljivost tega protokola pa je nedvomno to, da dovoli uporabnikom izbiro šibkih kriptirnih algoritmov oziroma celo dopušča možnost brez kriptiranja. Kljub nekaterim manjšim pomanjkljivostim pa niso znane kakšne pomembnejše varnostne luknje, zato lahko zaključimo, da ob primerni varnostni politiki protokol sicer ni idealen, vendar pa zadošča potrebam in zahtevam po varnosti.

Banka uporablja podoben protokol pri svoji poslovni aplikaciji Moba NLB, kjer lahko uporabniki s pomočjo svojega mobilnega telefona opravljajo veliko število bančnih storitev.

3.3 Operacijski sistemi in okolja

3.3.1 Uvod

Varnost celotnega sistema je v veliki meri odvisna tudi od operacijskega sistema, ki teče na računalniku. V začetnem obdobju razvoja osebnih računalnikov je računalnike poganjal v glavnem operacijski sistem DOS, katerega varnost je bila praktično nična. Vsakdo, ki je imel dostop do računalnika, je lahko dostopal do vseh podatkov. Na velikih računalnikih je bilo že v zgodnji dobi razvoja veliko bolje poskrbljeno za zaščito, uporabnik se je moral operacijskemu sistemu predstaviti s svojo uporabniško identiteto ter geslom. Z uveljavitvijo grafičnih okolij in začetkom povezovanja v omrežja se je tudi na področju osebnih računalnikov varnost izboljšala.

3.3.2 Okolje OS/390 - IBM S/390

Računalniki IBM S/390 predstavljajo danes eno izmed najbolj varnih platform. Skupaj z operacijskim sistemom OS/390 ponujajo dobro osnovo za zaščito kritičnih poslovnih potreb. Glavne odlike OS/390 so naslednje[27]:

- večopravilnost, ki je vgrajena v operacijski sistem je podprta na strojnem nivoju;
- dostopi do sistema in vseh virov, kot so baze podatkov, programi, transakcijski sistemi, omrežje, UNIX programi in drugo, so nadzorovani preko varnostnega modula z imenom OS/390 Security Server;
- robustni sistem zagotavlja sistemsko celovitost;
- sistem odgovarja po merilih ameriškega instituta za računalniško varnost (NCSC) nivoju varnosti C2/B1 ali po evropskih merilih ITSEC nivoju E4 za varnost (glej poglavje 4.1.2 Formalni modeli komercialnih sistemov);
- kriptografija in certificiranje sta sestavni del operacijskega sistema OS/390 V2, podprta sta tudi na strojnem nivoju;
- operacijski sistem vsebuje v svojih modulih tudi požarni zid in podpira navidezna zasebna omrežja (virtual private networks);
- OS/390 vključuje tudi LDAP strežnik (Lightweight Directory Access Protocol), ki zagotavlja varen dostop do informacij, ki jih hrani OS/390.

Zaščita v okolju OS/390 na IBM osrednjem sistemu[28] je izvedena z uporabo zaščitnega paketa Top Secret in obsega zaščito dostopa s pristopnimi identifikatorji in gesli, zaščito tabel, datotek, diskov, programov in transakcij. Uporablja se zaklepanje terminalov, glavna konzola pa je pred izvajanjem občutljivih rutin še posebej zaščitena. Vključen so varnosti alarmi v realnem času in varnostni zapisi za

[27] S/390 Security

[28] Predpis zaščite informacij v direkciji za informatiko, 2001, str. 13

vse kršitve dostopov in spremembe varnostnega okolja. Varnostni alarmi so kritični dogodki, ki sprožajo opozorila v sistemu na osnovi posebnih dogodkov. Taki dogodki so:

- nepooblaščeni dostopi do datotek, direktorijev, objektov …;
- prijave, odjave in poskusi vdora v sistem;
- spremembe v seznamu gesel in pooblastil;
- izvajanja brez varnostnih mehanizmov;
- poškodbe varnostnih mehanizmov.

Za preverjanje zaščite v okolju OS/390 pa se uporabljajo razna orodja za:

- beleženje delovanja;
- analiziranje varnostnih sporočil;
- spremljanje sprememb varnostnih parametrov;
- kontrolo dostopa;
- spremljanje uporabe;
- kontrolo mreže;
- preverjanje veljavnosti diskov.

3.3.3 Okolje AIX 4.3 – IBM RS/6000 strežniki

AIX je odprto okolje UNIX, ki zagotavlja dobro integracijo, prilagodljivost in zanesljivost[29]. Kot tako ustreza visokim zahtevam sodobnega elektronskega poslovanja. Podpira 32 in 64-bitno strojno opremo sistemov RS/6000, podpira razširljivost in ključne internetne tehnologije kot je Java. Na 64-bitnih sistemih AIX 4.3 zagotavlja polno večopravilnost in poganjanje 32 in 64-bitnih aplikacij s procesi, ki so lahko konkurenčni ali kooperativni, ter skupno rabo dostopa do datotek, pomnilnika in zunanjih naprav.
Operacijski sistem AIX je prvi 64-bitni operacijski sistem UNIX, ki je prejel C2 varnostni certifikat po TCSEC[30]. Tudi v Evropi so mu podelili certifikat E3/F-C2 po ITSEC. Operacijski sistem vsebuje mehanizem samovoljne kontrole dostopa do objektov, ki dovoljuje skupno rabo informacij vnaprej določenim uporabnikom.

Logična zaščita dostopa v okolju AIX pa zajema:

- definiranje uporabnikov v okolju OS;
- zaščito dostopa z uporabo programa za varno prijavljanje preko mreže;
- omejevanje priključevanja preko mreže;
- beleženje vključitev na sistem;
- zaščito konzole z geslom;
- nadzor nad spremembami varnostnega okolja.

[29] Strengthening AIX Security, 2002, str. 1
[30] IBM AIX: First UNIX…

Za nadzor v okolju operacijskega sistema se uporabljajo orodja za beleženje dostopov v sistem, beleženje dela uporabnikov, nadzor sprememb varnostnega okolja ter pregledovanje datotek napak in informativnih datotek.

3.3.4 Okolje OpenVMS – DEC Alpha

Operacijskemu sistemu OpenVMS je ITSEC dodelil varnostni nivo E3. Tudi v Ameriki mu je bil podeljen naziv C2 po TCSEC.

Zaščita v okolju OpenVMS je izvedena z uporabo zaščitnih mehanizmov operacijskega sistema:

- zaščita dostopa z obvezno uporabo identifikacijske kode uporabnika (UIC) in po potrebi kontrolne liste pristopov (ACL);
- zaščiteni elementi so datoteke, direktoriji, objekti in enote;
- za vse privilegirane uporabnike morajo biti gesla naključno generirana, datoteka gesel mora biti šifrirana, veljavnost gesel je časovno omejena;
- omejitve za prijavljanje glede na izvor zahtevka;
- uporablja se zaklepanje terminalov;
- uporablja se varnostni alarm in varnostni zapis v realnem času;
- selektivni nadzor za izbrane datoteke.

V operacijskem sistemu se lahko beležijo naslednji dogodki:

- neuspešen dostop do zaščitenega objekta;
- neuspešna uporaba privilegija ali identifikatorja;
- poskusi vdorov vseh vrst;
- sprememba v datoteki s podatki o pooblastilih;
- spremembe sistema;
- spremembe uporabnikovih gesel;
- sprememba sistemskega časa;
- sprememba datoteke sistemskih parametrov;
- spremembe privilegijev ali varnostnih atributov zaščitenih objektov;
- dostop do datoteke s pomočjo privilegijev;
- izvajanje privilegiranih ukazov.

Za preverjanje zaščite v okolju OpenVMS se uporabljajo naslednja orodja za:

- beleženje delovanja;
- analiziranje varnostnih poročil;
- spremljanje sprememb sistemskih parametrov;
- preverjanje čitljivosti diskovnih volumnov;
- kontrolo dostopa in spremljanje uporabe;
- pregled datoteke napak;
- kontrolo mreže.

Poleg tega pa se uporabljajo še sistemske rutine in programi za nadzor protokola.

3.3.5 Okolje Windows NT in Windows 2000 – strežniki Compaq

Banka razpolaga z več deset strežniki Compaq, različnih modelov družine Proliant, ki se tudi po zmogljivostih precej razlikujejo glede na naloge, ki jih opravljajo. Strežniki Compaq predstavljajo danes zagotovo eno najbolj zanesljivih platform za Microsoft Windows okolje. Vsebujejo razne tehnologije, ki povečajo zanesljivost delovanja, kot je[31]:

- uporaba pomnilnika ECC (paritetni bit omogoča avtomatsko popravljanje napak);
- RAID polja, RAID 1, RAID 5 in RAID 1+0 z redundantnimi diski povečajo odpornost sistema pri izpadih delovanja diskov;
- redundantni napajalniki, mrežne kartice, ventilatorji;
- enote za arhiviranje, tračne enote, robotske knjižnice s tračnimi enotami.

Poleg tega so vsi strežniki priključeni na sistem neprekinjenega napajanja, ki omili težave v primeru izpada dobave električne energije.

Strežniki so opremljeni z operacijskim sistemom Microsoft Windows NT 4.0 ali pa Microsoft Windows 2000 Server oziroma Advanced server. Trenutno poteka faza migracije iz operacijskega sistema NT na 2000, zato je okolje mešano, čeprav sta si oba sistema po funkcionalnosti zelo podobna.
Oba operacijska sistema se ponašata z določenim nivojem varnosti. Microsoft Windows NT 4.0 Server je leta 1999 dobil naziv E3/F-C2 po ITSEC[32], kar je v bistvu tudi najvišji naziv za operacijske sisteme v splošni rabi. Prav tako mu je ameriški NCSC podelil oceno nivoja varnosti C2 po TCSEC.
Microsoft Windows 2000 pa je dobil tudi priznanje po novi shemi za vrednotenje varnosti informacijske tehnologije CCITSE, bolj znani kot Common Criteria ali CC. CC je mednarodni standard ISO/IEC 15408, ki naj bi nadomestil ITSEC in TCSEC. Microsoft Windows 2000 odgovarja zahtevam za CAPP (Controlled Access Protection Profile), kar je približno podobno zahtevam C2 po TCSEC ali F-C2 po ITSEC.

Logična zaščita v okolju Windows zajema:

- definiranje uporabnikov v okolju;
- zaščito elementov, kot so datoteke, direktoriji, objekti …;
- beleženje dostopov iz okolja;
- varnostno politiko v zvezi z gesli.

Strežnik z operacijskim sistemom Windows vsebuje orodja za beleženje dostopov v sistem, orodja za beleženje dela uporabnikov, nastaviti pa je mogoče tudi vrsto varnostnih alarmov, ki se prožijo ob različnih varnostnih dogodkih.

---

[31] Priporočila za strežniško infrastrukturo, 2000, str. 3
[32] Microsoft: Security, 2002

3.3.6 Okolje Windows NT 4.0 Professional ter Windows 2000 – osebni računalniki Compaq in IBM

Banka uporablja pri svojem poslovanju okrog 5000 osebnih računalnikov znamk Compaq in IBM, ki temeljijo na procesorjih Intel Pentium II do Pentium 4. Takšna količina računalnikov bi bila težko obvladljiva, če ne bi banka uvedla politiko standardne delovne postaje, tako da je velika večina računalnikov konfigurirana na popolnoma enak način. Banka določi vsako leto standardno delovno postajo in kupuje večje količine računalnikov z enako strojno in programsko opremo. Vsak model računalnika se pred uvedbo v produkcijsko okolje dodobra testira z vsemi naloženimi aplikacijami, ki se uporabljajo pri poslovanju. Po končanem testu se izdela slika diska standardne delovne postaje. Ostale delovne postaje se namestijo s preprostim kopiranjem slik diskov in dodatnimi nastavitvami, ki ustrezajo določenemu uporabniku. Z varnostnega stališča je takšna politika zelo primerna, saj omogoča hitro okrevanje pri možnem scenariju napada zlonamernega programa, ki bi uničil vse podatke na disku in prizadel veliko število računalnikov.

Na standardnih delovnih postajah se uporablja operacijski sistem Windows 2000, nekaj starejših delovnih postaj pa uporablja še Windows NT 4.0 Professional. Prav tako kot pri strežnikih poteka migracija na okolje Windows 2000.

Za logično zaščito osebnih računalnikov banka uporablja:

- začetno geslo pri zagonu (power on);
- zaščito BIOS-a z geslom;
- onemogočanje zagona s pomočjo diskete;
- zaklepanje ekrana z geslom;
- dostop do podatkov na osebnem računalniku imajo samo definirani uporabniki v NT okolju;
- na računalnikih mora biti vključeno zapisovanje dogodkov o pristopih.

Na osebnih računalnikih z občutljivimi podatki je dodatno poskrbljeno še za:

- zaščito varnostno občutljivih datotek s pomočjo kriptiranja;
- nadomestno opremo v primeru okvare;
- avtomatizirane postopke arhiviranja;
- neprekinjeno napajanje.

Vsi Microsoftovi operacijski sistemi Windows so danes zelo razširjeni, saj so nameščeni na milijonih računalnikov po svetu. Glede varnosti je to gotovo slabost, saj so s tem bolj izpostavljeni večjemu številu napadalcev, ker jim je sistem bolj domač, prav tako pa obstaja za te operacijske sisteme bistveno večje število programov z zlonamernim delovanjem (predvsem virusov in internetnih črvov), kot na primer za operacijski sistem IBM AIX.

3.3.7 Okolje OS/2 – osebni računalniki in strežniki

Na banki je tudi nekaj računalnikov IBM, na katerih teče operacijski sistem OS/2 Warp. Čeprav se operacijski sistem ne razvija več in je v zatonu, pa vseeno ni slab, kar se tiče varnosti. Varnost operacijskega sistema je na istem nivoju kot pri Microsoftih operacijski sistemih, odgovarja varnostnemu razredu C2 po TCSEC. OS/2 se je veliko uporabljal na tako imenovanih univerzalnih delovnih postajah, ki so bile namenjene poslovanju na bančnih okencih, pred kratkim pa so ti računalniki prešli na operacijski sistem Windows 2000 Professional.

3.3.8 Prenosni računalniki

Na prenosnih računalnikih je poleg Windows NT 4.0 in Windows 2000 dovoljena uporaba tudi drugih operacijskih sistemov kot je Windows 98, Windows ME ali Windows XP Pro. Zavedati pa se je potrebno, da operacijska sistema Windows 98 in Windows ME ne nudita ustrezne varnostne zaščite in imata kljub nekaterim izboljšavam in varnostnim ukrepom še vedno veliko varnostnih lukenj. Zato je banka določila poleg vseh ukrepov, ki veljajo za osebne računalnike, obvezno kriptiranje varnostno občutljivih podatkov na računalnikih s tem operacijskim sistemom. Na prenosnih računalnikih v javni uporabi pa ne sme biti varnostno občutljivih podatkov.

3.4 Baze podatkov

Baze podatkov predstavljajo nedvomno enega najpomembnejših virov podjetja, saj hranijo vse mogoče podatke, ki jih podjetje uporablja pri vsakdanjem poslovanju. Zato je treba podatke v bazah ustrezno zaščititi. Problematika varnosti baz podatkov je še nekoliko širša od problematike varnosti operacijskih sistemov[33]. Od nje se razlikuje po tem, da je treba pri bazah zaščititi več objektov, ukvarja se z različnimi nivoji razdrobljenosti, kot so datoteke, zapisi in polja. Objekti so lahko zapletene logične strukture, ki kažejo na iste fizične podatkovne objekte, zato je treba pri varnosti baz podatkov poskrbeti tako za varnost pomena podatkov, kot tudi za fizično varnost. Je pa res, da je varnost baz podatkov odvisna tudi od varnosti samega operacijskega sistema, na katerem teče baza.

Prav tako kot drugod, so tudi tu zaupnost, neoporečnost ter razpoložljivost podatkov najpomembnejša področja varnosti in zaščite. Potrebno je poskrbeti, da bodo podatki v bazi na razpolago le pooblaščenim, pri tem pa se lahko pojavi problem, ki ga pri varnosti operacijskih sistemov ne poznamo. Napadalec lahko iz podatkov, ki jih sicer lahko upravičeno dobi, sklepa o podatkih, do katerih ni upravičen. Sistem za upravljanje baz podatkov mora poskrbeti tudi za take probleme. Mehanizmi, s katerimi se zagotavlja zaupnost, so podobni kot drugod. Med nje spadajo:

[33] Hua, 2002

- preverjanje uporabnikov na nivoju operacijskega sistema, baze ali obojega;
- samovoljna kontrola dostopa na osnovi pravic (na sistemu in objektih) ter pravil;
- obvezna kontrola dostopa na osnovi občutljivosti podatkov, ki je lahko tudi več nivojska;
- kriptiranje, navadno na nivoju vrstice ali stolpca tabele.

Neoporečnosti podatkov v bazi zahteva poleg zagotovitve fizične tudi logično celovitost podatkov, zato je treba podatke po potrebi zaklepati. Poleg tega pa se lahko kot dodaten varnostni ukrep uporablja še porazdeljevanje podatkov v različne baze glede na zaupnost ter delo s pogledi na podatke namesto s podatki. Podatki morajo biti tudi vedno pravočasno na razpolago, kar je včasih precej zahtevna naloga, še posebej, če je količina podatkov velika in je baza porazdeljena. Varnostni ukrepi se morajo posvetiti tudi zavarovanju podatkov v primerih napak ali odpovedi ter zagotoviti redno arhiviranje in postopke okrevanja tudi na ravni posamezne baze. Tudi varnosti arhiva je potrebno posvetiti ustrezno pozornost, saj lahko napadalec pride do vseh podatkov, če ima dostop do arhiva. Zato je za zagotovitev varnosti smiselno poleg fizičnega varovanja arhivskega medija tudi šifrirati celotno bazo podatkov na arhivskem mediju.

3.4.1 DB/2

DB2 je univerzalna relacijska baza, ki deluje na različnih operacijskih sistemih. V banki se pojavlja na centralnem sistemu S390 ter na strežnikih, ki temeljijo na sistemih AIX, OS/2, Windows NT 4.0 Server in Windows 2000 Server.
Posebna pozornost pri bazi DB2 je posvečena ključnim področjem, kot so overjanje, pooblaščanje, pravice ter neoporečnost[34]. Pri overjanju DB2 uporablja usluge operacijskega sistema, ki preverja uporabnike in si pomaga z metodami, kot so zaupni odjemalec, kriptiranje odjemalca ter porazdeljeno okolje. Pravice v bazi se lahko dokaj podrobno definirajo na nivoju vrstice v tabeli. Neoporečnost baze je zagotovljena s pomočjo mehanizmov za referenčno celovitost, vsiljevanjem pravil ter s sprožilniki.

3.4.2 SQL Server 2000

V zadnjem času banka uvaja tudi bazo SQL Server 2000, ki je Microsoftov produkt in se zaradi tega posebej dobro sklada z operacijskim sistemom Windows. Varnost lahko v tem primeru temelji na varnosti same baze, lahko pa izkorišča prednosti operacijskega sistema Windows 2000 ter uporablja njegove mehanizme zaščite, kar priporoča tudi proizvajalec. Sicer pa je produkt dobil oceno ustreznosti C2 po TCSEC leta 2000 in zagotavlja[35]:

- obvezno identificiranje in overjanje vseh uporabnikov na sistemu, dostop do podatkov je dovoljen samo overjenim uporabnikom;

[34] IBM DB2 Universal database, 2002
[35] Microsoft: Security

- samovoljen nadzor dostopa – zmožnost, da lahko uporabniki zaščitijo podatke, kot želijo;
- odgovornost in revizijsko sled;
- ponovno uporabnost objektov.

3.4.3 Ostalo

V banki je v uporabi tudi nekaj drugih starejših baz podatkov oziroma bolj zbirk tabel ali preglednic kot pravih relacijskih baz. Izvirajo iz obdobja začetka množične uporabe osebnih računalnikov, v glavnem pa so namenjene bolj preprostim programom. Med take baze sodijo Access in Excel, ki se dobita skupaj z Microsoftovim pisarniškim paketom Office ter Dbase. O posebni varnosti pri teh bazah ne moremo govoriti, v kolikor obstajajo varnostni mehanizmi, so precej preprosti. V glavnem si pri takih bazah podatkov pomagamo z varnostnimi mehanizmi operacijskega sistema.

3.5 Aplikativna, komercialna in pomožna programska oprema

Množica programov, ki se izvajajo v banki, je zelo široka. Poleg operacijskih sistemov ter sistemov za upravljanje z bazami podatkov, ki so omenjeni v prejšnjih poglavjih, obstaja veliko število orodij, odjemalskih programov, komercialno dostopnih programskih paketov ter namenskih aplikacij.

3.5.1 Odjemalski programi

Odjemalski programi predstavljajo most med različnimi sistemi, od glavnih računalnikov in strežnikov sprejemajo oziroma jim dajejo podatke ter jih posredujejo drugim aplikacijam. V banki se uporabljajo naslednji odjemalci (Tabela 3):

Tabela 3: Odjemalski programi

Naziv odjemalca	Namen	Povezava na sistem
Microsoft Internet Explorer	Brskalnik za dostop do svetovnega spleta	Internet
IBM DB/2 client	Odjemalec za bazo DB/2	IBM
IBM CICS client	Odjemalec za IBM	IBM
Connect Direct	Povezava DEC - IBM	IBM
Microsoft Exchange	Odjemalski program elektronske pošte	Exchange Server
CLIME - client	Odjemalec aplikacije Clime	Clime
Host Explorer	Simulacija terminala in odjemalec za DEC	Alpha DEC
Communications Server	Odjemalec za IBM komunikacijski strežnik	Internet
Microsoft SMS	Nadzorni in distribucijski odjemalec	SQL Server

Vir: LBNET

3.5.2 Komercialni programski paketi

Banka uporablja tudi veliko število komercialnih paketov kot so razna pisarniška orodja in drugi pomožni programi. Glede na obseg so ti programi najbolj razširjeni, saj gre število licenc za nekatere programske pakete v tisoče. Nekateri najbolj znani, kot je Microsoftov Office, so zaradi razširjenosti še posebej dovzetni za napade zlonamerne programske opreme, saj obstaja kar nekaj makro virusov, ki so napisani nalašč za te programe.
Glavni paketi, ki se uporabljajo v banki, so našteti v spodnji tabeli (Tabela 4):

Tabela 4: Komercialni paketi

Ime programskega paketa	Namen
Microsoft Office	Pisarniški paket (Word, Excel, Power point, Outlook, Access)
Sophos Sweep	Protivirusna zaščita
Activ Card Gold	Program za uporabo čitalcev pametnih kartic
Symantec Norton Ghost	Orodje za delo z diski
DISS - (Continuity Action Planning Tool)	Orodje za načrtovanje neprekinjenega poslovanja
PowerSync	Replikacija datotek
Microsoft Visio	Orodje za načrtovanje
Microsoft Front Page	Orodje za izdelavo spletnih strani
Microsoft Project	Orodje za organizacijo
Corel Draw	Orodje za oblikovanje
Adobe Acrobat	Urejevalnik
PGP	Paket za kriptiranje
Key for Enterprise	Kriptiranje za OS/2
Adobe Photoshop 6.0	Orodje za oblikovanje
Recognita Plus 5.0	Orodje za optično razpoznavanje besedil
Entrust Desktop Solutions	Paket za kriptiranje
IBON	Boniteta poslovanja za slovenska podjetja
IPIS	Poslovni register Slovenije

Vir: LBNET

3.5.3 Namenske aplikacije

Najvažnejše za poslovanje so nedvomno namenske aplikacije, saj le-te neposredno operirajo s podatki. Zato je bilo v razvoju teh programov vloženega tudi veliko truda in skrbi za varnost. Programi morajo odgovarjati internim standardom varnosti[36] in kakovosti[37], pa naj gre za rešitve, ki so bile razvite znotraj banke ali pa kupljene. Za namenske aplikacije v banki velja, da mora biti vsak uporabnik pooblaščen. Zato se poleg zaščit, ki jih nudi operacijski sistem, uporablja dodatno uporabniško ime in geslo za vsako aplikacijo. Pri bolj občutljivih aplikacijah, ki vsebujejo finančne

[36] Interni standard informacijske zaščite, 2001
[37] Interni standard o uporabi razvojnih orodij, 2002, Interni standard podatkovnega modeliranja, 2001

transakcije, je upoštevan tudi princip ločevanja nalog, tako da posameznik ne more sam izvršiti poneverbe. Za vsako namensko aplikacijo je uveden tudi sistem skrbništva, ki se loči na sistemski del, ki skrbi za tehnični vidik, ter uporabniški del, ki ureja pravice dostopa in podobno.
Pomembnejše namenske aplikacije so zbrane v spodnji tabeli (Tabela 5):

Tabela 5: Namenska aplikativna programska oprema

Ime aplikacije	Namen	Dostop do baze	Sistem
Pranje	Aplikacija za preprečevanje pranja denarja	DB2	IBM
Storitve	Podpora storitvam banke	DB2	IBM
Register	Register komitentov	DB2	IBM
MASA	Zbiranje vseh podatkov o poslovanju komitentov	DB2	IBM
MUNDUS	Podpora za centralni register transakcijskih računov	DB2	IBM
Vmesnik	Vmesnik za plačilni promet	DB2	IBM
POND	Podpora odobravanju naložb in depozitov	DB2	IBM
SOD_PIS	Sodobna pisarna – poslovanje brez papirja	DB2	IBM
Študentski krediti	Podpora odobravanju študentskih kreditov	DB2	IBM
Plačilni promet	Podpora za plačilni promet	DB2	IBM
BTM 2000	Podpora za kredite in depozite	DB2	IBM
BTM Correspondence	Izpisi za kredite in depozite	DB2	IBM
EPI@BS	Podpora za poslovanje z vrednostnimi papirji	DB2	IBM
GLOBUS	Podpora tržnikom	DB2	IBM
Imago	Zajem in optično razpoznavanje dokumentov	SQL Server	Compaq strežnik
Depozit	Podpora za depozite na bankomatu	Dbase-lokalno	PC
Krediti	Podpora za dolgoročne kredite občanov	Dbase-lokalno	PC
Pilot Excel	Informacijski sistem za planiranje	Excel-lokalno	PC
EOM	Izračun efektivne obrestne mere	Excel-lokalno	PC
Hipotekarni krediti	Podpora za hipotekarne kredite	Excel-lokalno	PC
Naročila IB	Naročila investicijskega bančništva	Excel-lokalno	PC
PCTEAM	Intranetna aplikacija za podporo oddelka za osebne računalnike		WEB
EIS	Elektronski IS za direktorje		WEB
LBNET	Intranetne strani banke		WEB
Klik	Internetna aplikacija za podporo poslovanja s fizičnimi osebami		WEB
Proklik	Internetna aplikacija za podporo poslovanja s pravnimi osebami		WEB
Proklik^{+}	Internetna aplikacija za podporo poslovanja s pravnimi osebami		WEB
Moba	Internetna aplikacija za podporo poslovanja s fizičnimi osebami preko mobilnega telefona		WEB

Vir: LBNET

3.6 Zlonamerna programska oprema

3.6.1 Uvod

Obstoj programov, ki se lahko sami reproducirajo, je ugotovil že matematik John von Neumann leta 1949[38]. Prvi računalniški zlonamerni programi so se pojavili že v 60. letih prejšnjega stoletja na večjih sistemih. Leta 1984 pa se je pojavil prvi računalniški virus imenovan Brain, ki je lahko okužil osebne računalnike. Takrat se je začel tudi buren razvoj programov z zlonamernim delovanjem. Prvi taki programi so se širili preko disket, zato je bilo njihovo razširjanje za današnje razmere počasno, kasneje pa so začeli izkoriščati omrežja in se širiti preko interneta in elektronske pošte. Kako nevarni so lahko zlonamerni programi se lahko prepričamo večkrat na leto, ko kakšen nov virus v enem samem dnevu preplavi ves svet.

3.6.2 Vrste zlonamerne programske opreme

Zlonamerno programsko opremo lahko definiramo kot programsko opremo, ki ima za osnovni namen povzročanje škode, izgube ali vohunjenje. Razdelimo jo lahko na naslednje skupine[39]:

- virusi,
- črvi (worms),
- trojanski konji,
- miselni virusi,
- kombinirani virusi.

Virusi

Najbolj znana skupina so nedvomno računalniški virusi. To so programčki, ki za svoje razširjanje potrebujejo druge programe, zato okužijo izvajalne datoteke. Nekateri virusi so narejeni tako, da sprožijo svoje uničujoče aktivnosti ob določenem času – časovne bombe, ali pa, ko je izpolnjen določen pogoj – logične bombe. Včasih so se virusi širili predvsem s pomočjo prenosnih medijev, danes pa v glavnem s priponami elektronske pošte ali pa preko datotek, ki jih dobimo preko interneta. Primer takega virusa sta virusa Melissa (marec 1999) in Love Letter (maj 2000), ki sta prizadela ves svet.
Posebni primeri virusov so makro virusi, ki se širijo preko aplikacij, kot so urejevalniki besedil ali preglednice, še posebno veliko pa jih za svoje razširjanje uporablja Microsoft Word in Excel.
Zanimiv je primer, ko je podjetje odpustilo delavca, ta pa je namestil virus - logično bombo, ki se sprožila po njegovem odhodu in naredila preko 10 milijonov dolarjev škode[40].

---

[38] Computer viruses demystified, 2001, str. 18
[39] Pečenko, 2002, str. 62
[40] Gupta, 2000, str. 337

Črvi

Črvi za razliko od virusov za svoje delovanje ne rabijo gostiteljskega programa. Poleg tega jim tudi ni treba ročno pomagati, saj se znajo širiti kar sami. Črvi izdelajo svoje kopije in za širjenje izkoriščajo obstoječe povezave med računalniki. Ker je danes večina računalnikov povezanih v omrežje kot je internet, se lahko preko omrežja v zelo kratkem času okuži ogromno računalnikov.
Primer takega črva je črv Nimda, ki spreminja vsebino spletnih strani tako, da se uporabnik okuži z obiskom spletne strani. Črv z uporabniških računalnikov napada ranljive spletne strežnike Internet Information Server preko napake v IIS.

Trojanski konji

Trojanski konji se ne znajo sami razmnoževati. Namesto tega ponudijo uporabniku kakšno zanimivost, v ozadju pa počno druge nedovoljene reči, npr. sporočajo podatke iz računalnika, omogočijo dostop do računalnika napadalcu, počnejo določene stvari v imenu uporabnika in podobno. V zadnjem času je eden bolj znanih takih programov Go!Zilla, ki je namenjen iskanju programov in drugih datotek v svetovnem spletu, poleg tega pa še pridno zbira podatke o gostiteljevem računalniku.

V mesecu oktobru 2002 se je ravno v zvezi z Novo Ljubljansko banko pojavil razvpit primer trojanskega konja, s katerim je skušal posameznik izsiljevati banko za 100 milijonov tolarjev, s tem ko je skušal prodati trojanskega konja skupaj z načinom zaščite pred njim. Omenjeni trojanski konj ni bil v bistvu nič drugega, kot programček, ki je izkoriščal določeno funkcionalnost brskalnika Internet Explorer in oponašal obnašanje človeka pri uporabi spletne aplikacije Klik NLB. S tem se mu ni bilo treba ukvarjati z razbijanjem šifriranja in protokola SSL, saj mu je uporabnik kar sam priskrbel vse potrebno. Vendar pa je bil ta trojanski konj precej preprost, saj si ga je moral uporabnik sam namestiti na računalnik, poleg pa je moral imeti v možnostih brskalnika nastavljeno možnost, da lahko tretji program prevzame nadzor nad brskalnikom (kar je sicer privzeta nastavitev). S tem bi bila lahko ogrožena varnost Klik-a pri uporabniku, ne pa pri banki, kot so napačno navedli nekateri novinarji v nekaterih medijih. V tem primeru velja prav tako kot za ostalo zlonamerno programsko opremo, da je treba upoštevati splošne varnostne ukrepe tudi na strani uporabnika, ne samo na strani banke, da bo elektronsko poslovanje varno.

Miselni virusi

Poleg naštetih vrst zlonamerne programske opreme pa poznamo še tako imenovane miselne viruse ali potegavščine (hoaxes). To so razna obvestila, v slogu:

Pojavil se je nov nevaren virus, ki lahko pobriše vse podatke v računalniku. Preglejte, če je ta in ta datoteka na vašem računalniku in jo nemudoma pobrišite ...

Navadno taka besedila navajajo kakšno znano računalniško podjetje, preveč poveličujejo zmožnosti virusa in svetujejo, da sporočilo takoj pošljete prijateljem. Taka obvestila niso nič manj nevarna kot virusi, saj lahko z njihovo "pomočjo" uporabnik sam onesposobi računalnik, tako da si pobriše kakšno pomembno datoteko, ki je potrebna za delovanje računalnika.

3.6.3 Tveganja povezana z zlonamerno programsko opremo

PandaSoftware, podjetje ki se ukvarja s protivirusno zaščito, ponuja preprosto tabelo[41] (Tabela 6), s katero si lahko sami ocenimo tveganje v zvezi z zlonamerno programsko opremo, če nimamo nameščene protivirusne programske opreme:

Tabela 6: Tabela ocenjevanja tveganj v zvezi z zlonamerno programsko opremo

Število računalnikov	Točke
1-10 (1 točka)	
11-50 (2 točki)	
več kot 50 (3 točke)	3
Vrsta povezav med računalniki	
Posamezne povezave (1 točka)	
Omrežje (3 točke)	3
Vhodne točke	
Diskete in CD ROM (1 točka)	1
Internet (2 točki)	2
Elektronska pošta (3 točke)	3
VSOTA	12

Indeks tveganja	
Od 1 do 3 točke	Nizko tveganje
Od 4 do 6 točk	Srednje tveganje
Več kot 6 točk	Visoko tveganje

Vir: Pandin vodnik, 2002, str. 3

Preprost izračun nam prikaže, da je tveganje v običajnem srednje velikem podjetju kot je banka, zelo veliko. Ankete istega podjetja tudi kažejo, da pride iz leta v leto več okužb preko elektronske pošte in interneta. Najtežje posledice okužb z virusi pa so onesposobitev računalnika (70%), upad produktivnosti (69%), popačenost datotek (55%), izguba dostopa do podatkov (41%), izguba podatkov (37%) ter upad zaupanja uporabnikov (33%).
Po podatkih raziskav analitske skupine IDC[42] je v letu 2000 v Evropi uporabljalo protivirusno zaščito 97% podjetij. Banka je kot finančna ustanova še posebej občutljiva glede svojih podatkov, zato mora obvezno uporabljati protivirusno zaščito.

[41] Pandin vodnik, 2002, str. 3
[42] Virusi in vdori, 2000, str.6

3.6.4 Zaščita pred zlonamerno programsko opremo

Za zaščito pred zlonamerno programsko opremo je banka sprejela naslednje varnostne ukrepe[43]:

- uporaba protivirusnih programov s centralno administracijo, ki se redno obnavljajo na vseh glavnih računalnikih, strežnikih, osebnih in prenosnih računalnikih ter na požarnem zidu;
- blokiranje nekaterih pripon elektronske pošte na požarnem zidu, ki so potencialne nosilke virusa;
- protivirusno pregledovanje elektronske pošte na poštnem strežniku;
- striktna uporaba interneta v poslovne namene, blokiranje določenih spletnih strani in vsebin;
- dosledna uporaba licenčne programske opreme;
- prepoved uporabe programov v javni lasti in preprečitev samovoljnih namestitev uporabnikom;
- pregledovanje vseh digitalnih medijev (disket, CD ROM-ov …), ki vstopajo v banko na posebnem računalniku, ki ni povezan v omrežje.

3.7 Motnje v delovanju in naravne nesreče

3.7.1 Motnje v delovanju

Vzrokov, zakaj prihaja do motenj pri delovanju računalniških sistemov, je več. Skupna lastnost vseh je, da je z njimi neposredno ali pa posredno povezan človek. Posledice teh motenj so lahko katastrofalne, če gre za jedrsko centralo, pri banki pa se kažejo predvsem kot finančne izgube.

Vzroki za motnje v delovanju so lahko[44]:

- **Človeške napake**
  Človeške napake so najpogostejše, raziskave kažejo, da je kar 60% do 80% nesreč pri računalniških sistemih, ki jim botruje človeška napaka. Problem pri tem pa je, da vseh napak preprosto ni mogoče predvideti, da bi se ustrezno zaščitili pred njimi. Zaustavitev glavnega računalnika zaradi administratorjeve napake bi pomenila izpad celotne mreže banke po vsej Sloveniji.

- **Slabo delovanje strojne opreme**
  Računalniška oprema je dokaj zanesljiva, včasih pa vseeno odpove. Pri osebnih računalnikih lahko opazujemo oster boj konkurentov, ki izdelujejo posamezne komponente. Razvoj procesorjev in grafičnih čipov je v zadnjem

[43] Interni standard NLB za informacijsko zaščito, 2001, str. 10
[44] Gradišar, 2001, str. 449

obdobju naravnost fantastičen, saj se zmogljivost podvoji kar vsakih 6 do 12 mesecev. Tako izredno kratki razvojni cikli pa imajo za posledico krajši čas testiranja proizvodov in s tem povezane napake pri delovanju. Najbolj znana takšna napaka je bila napačno delovanje procesorjev Intel Pentium pri deljenju določenih števil. Pogosto prihaja do težav in nepravilnega delovanja tudi zaradi manjših nekompatibilnosti komponent sistema.

- **Napake programske opreme**
  Pri programski opremi so problemi zaradi napak še veliko hujši, kot pri strojni opremi. Čeprav je programska oprema navadno dobro testirana, so testi veliko manj strogi kot pri strojni opremi. Zaradi obsežnost programov niso nikoli preverjeni prav vsi parametri in vsi možni dogodki, ki se lahko zgodijo. Za popolno testiranje bi morali preveriti prav vsako vrstico kode, to pa z današnjo tehnologijo preprosto ni mogoče niti z najmočnejšimi računalniki[45]. Ponavadi so tudi roki za izdelavo programov kratki in velikokrat se zgodi, da se programi začnejo uporabljati, preden so do konca preizkušeni. Primer take programske opreme je operacijski sistem Microsoft Windows 95. Računalniki, ki so imeli nameščen ta operacijski sistem, so se pogosto zaustavljali in javljali napake.

- **Podatkovne napake**
  Problem pri podatkih je ta, da jih ni mogoče popolnoma preveriti. Večkrat ne moremo preverjati vrednosti, ki so sicer dovoljene, niso pa pravilne.

- **Fizične poškodbe računalniške opreme**
  Računalniška in komunikacijska oprema je občutljiva za razne zunanje dejavnike. Zaradi pregretja lahko pride do odpovedi delovanja raznih komponent, diski so še vedno dokaj občutljivi na udarce in tresljaje, vlaga lahko pomeni kratek stik in podobno. Tudi komunikacijske naprave in vodi se lahko hitro poškodujejo, že zaradi zelo banalnih vzrokov kot je recimo ta, da glodalci uničijo kable. Leta 1998 je bila Banka Velenje za več ur odrezana od sveta, ker je bager pri kopanju ceste pretrgal glavni komunikacijski vod.

- **Neprimerna zmogljivost sistema**
  O neprimerni zmogljivosti sistema govorimo takrat, ko sistem ni sposoben izvesti naloge, za katero je namenjen. Današnji sistemi lahko hitro pridejo do preobremenitve, če so povezani v svetovni splet. Več sto ali tisoč hkratnih zahtev po strežbi lahko strežnik hitro zasiti, tako da ne zmore odgovoriti vsem zahtevam.

[45] Laudon, 1999, str. 442

- **Napadi zlonamerne programske opreme**
  Statistika v zadnjih letih priča, da sodijo med resne grožnje delovanju informacijskih sistemov tudi napadi zlonamerne programske opreme. Škoda, ki jo lahko povzročijo, je lahko na svetovni ravni gromozanska. Najodmevnejši je bil nedvomno virus Code Red z 2,6 milijardama dolarjev škode.

- **Namerno uničevanje**
  V takih primerih je neposredni krivec za motnje v delovanju človek, pa naj gre za manjše oblike sabotaže v podjetju, ki jih povzročijo sedanji ali nekdanji nezadovoljni uslužbenci ali hekerji, ali za katastrofalne oblike, kot je bil teroristični napad na poslopje svetovnega trgovinskega centra 11. septembra 2001 v ZDA.

3.7.2 Naravne nesreče

Za naravne nesreče ni mogoče reči, da je z njimi neposredno povezan človek, večinoma so posledica narave. Nanje ne moremo niti vplivati, niti jih ne moremo zanesljivo vnaprej napovedati. Med naravne katastrofe spadajo:

- potresi,
- poplave,
- orkani in viharji,
- udari strele,
- požari,
- neurja.

Naravne katastrofe lahko popolnoma uničijo računalniški sistem in vse podatke na njem, kar ima lahko za posledico v najslabšem primeru tudi propad podjetja. Zato se morajo podjetja vprašati, kakšno izgubo lahko prinesejo nesreče, kako bodo reagirale stranke, dobavitelji in delničarji ter kakšne bodo finančne izgube. Vsekakor pa morajo upoštevati možnost, da se tak dogodek zgodi, pa naj bo verjetnost videti še tako majhna.

Zagotavljanje neprekinjenega poslovanja in okrevanja po nesreči

Včasih ni mogoče vnaprej predvideti vseh groženj ali pa bi preventivno delovanje pomenilo preveliko oviro poslovanju ali zahtevalo prevelike stroške, zato mora podjetje, ki je močno odvisno od informacijskega sistema nujno izdelati načrt, kako bo ukrepalo po nesreči. Večkrat se pri tem pojavi problem, kako prepričati vodstvo podjetja, da odobri sredstva, ki so potrebna za izvedbo takšnega načrta[46], saj le-ta navadno pomeni kar precejšen finančni zalogaj. Vodstvo je največkrat mnenja, da vlaganje v prostore, infrastrukturo in opremo, ki bi služila samo za rezervo, predstavlja mrtvi kapital. Zato mu je potrebno pokazati, da imajo takšne investicije

[46] Hvala, 2002, str. 25

podoben značaj kot zavarovanje stavb in avtomobilov pri zavarovalnici (o smotrnosti slednjega se nihče ne sprašuje, ampak jemlje to kot samoumevno).

Načrt opredeljuje ukrepanje in odločanje od pojava motnje do obnovitve delovanja. Njegov namen je preprečiti paniko in nenadzorovano delovanje, ki bi lahko samo še poslabšalo stanje in naredilo še več škode[47]. Priprava načrtov pa v prvi fazi pomeni urejanje dokumentacije o procesih v sistemu, kar zajema dokumentiranje vseh virov kot so računalniki, programska oprema, postopki, mediji in podobno. Dokumentacijo je treba varno hraniti na več mestih, da je res na voljo v primeru nesreče. Nato je treba razvrstiti glavne poslovne procese po pomembnosti, da se v primeru izrednih dogodkov najprej posvetimo najvažnejšim procesom. Sledi opredelitev možnega vpliva različnih nesreč, ki lahko ogrozijo poslovanje. Pozornost je treba posvetiti tako pojavom odpovedi strojne opreme, kot možnosti, da bo potres popolnoma uničil glavno zgradbo podjetja.
Naslednji korak mora zagotoviti ukrepe, s katerimi skušamo zmanjšati možnosti odpovedi celotnega sistema. Tak ukrep je v prvi vrsti varnostno arhiviranje podatkov in shranjevanje na dovolj oddaljeni rezervni lokaciji, da je ne bi prizadel isti neljubi dogodek kot glavno lokacijo. Ne smemo pozabiti tudi na rezervno opremo, zagotavljanje neprekinjene oskrbe z električno energijo in podobno. Predvsem pa mora načrt vsebovati ljudi, ki bodo sodelovali v primeru izrednih dogodkov, ter opredeliti njihove naloge in odgovornosti. Vsi sodelujoči se morajo zavedati pomembnosti svojih nalog ter biti primerno usposobljeni in pripravljeni za izvajanje načrta.
Od posamezne organizacije je odvisno, ali bo sama skušala pripraviti načrt ali pa bo to nalogo zaupala bolj usposobljenim zunanjim izvajalcem. Praviloma imajo večja podjetja na razpolago več za to primerno usposobljenih strokovnjakov, ki lahko sami izdelajo načrt neprekinjenega poslovanja. Za manjša podjetja pa je navadno bolj smiselno in ceneje, če nalogo prepustijo drugim.
Zadnji korak je preverjanje in dopolnjevanje načrta. Načrt je potrebno periodično preizkušati, testiranje pa je lahko bolj ali manj zapleteno. Lahko preizkušamo samo postopke za vračanje podatkov iz arhiva rezervne kopije ali pa scenarij prehoda na rezervno lokacijo poslovanja. S tem se ugotovi, ali so aktivnosti in z njimi povezani rezultati v skladu z načrtovanimi postopki. O ugotovitvah je potrebno poročati nadrejenim, da le-ti ugotovijo, kakšne tveganja še vedno obstajajo in kaj bi bilo potrebno izboljšati. Pomembno je tudi, da se načrt neprekinjenega poslovanja in obnovitve delovanja po nesreči neprestano obnavlja skladno z razvojem poslovnih procesov in razvojem tehnologije. Še tako dober načrt bo popolnoma neuporaben, če bodo podatki v njem veljali za stanje, kakršno je bilo v podjetju pred tremi leti.

Glavne sestavine načrta v banki so:

- postopki v sili - nujni ukrepi ob večji nesreči;

[47] PSIST BS 7799, 1997, str. 98

- postopki za rezervno delovanje - selitev glavnih poslovnih dejavnosti na rezervno lokacijo;
- postopki za ponovno delovanje - za ponovno delovanje na prvotnem mestu.

Banka ima izdelan načrt za okrevanje po nesreči[48], ki ga testira vsakih 6 mesecev. V njem so popisani viri (osrednji računalniki, strežniki in omrežni sistemi), skrbniki (skrbniki sistema, aplikacij in elementov informacijskega sistema) ter kontaktne informacije za krizne skupine. Dokument opisuje vrste nesreč in ukrepe za vsako od teh nesreč, sistem obveščanja, postopke in potreben čas za vzpostavitev stanja pred nesrečo ali motnjo, postopke v primeru okvare strojne opreme, sistemske ali aplikacijske napake. Načrt okrevanja obravnava tudi dokumentiranje aktivnosti ob incidentu, kar pomaga zagotoviti sled v kasnejših analizah in poiskati morebitne pomanjkljivost ter na osnovi tega izdelati izboljšan obnovitveni načrt.

3.7.3 Varnostno kopiranje

Varnostna kopija je lahko edina stvar, ki nam ostane po izrednih situacijah, kot so odpovedi diskov, brisanje diska zaradi napada virusov, uničenje podatkov zaradi napada preko omrežja ali pa po naravni nesreči. Zato je pomembno, da je varnostna kopija shranjena na varnem mestu, na oddaljeni lokaciji, da nesreča ne prizadene tudi nje, če pride do uničenja prostora s strojno opremo. Nujno je redno in sistematično izdelovanje varnostnih kopij. Če dobi v roke varnostno kopijo nepooblaščena oseba, lahko z njeno pomočjo obnovi vse podatke, ki so bili na računalniku. Zato mora zanjo veljati ista varnostna politika in pravila zaščite, kot za računalnike, na katerih je bila izdelana.

Banka ima tudi na tem področju ustrezno varnostno politiko[49]. Varnostne kopije se izdelujejo za podatkovno, aplikativno programsko in sistemsko programsko področje:

- Osnovne varnostne kopije podatkovnega področja (varnostne kopije baz in arhivov) se izvajajo dnevno, poleg tega pa tudi ciklično tedensko, desetdnevno, mesečno, kvartalno, polletno, letno in občasno, glede na zahteve poslovnega področja banke. Vsaka varnostna kopija podatkovnega področja se hrani vsaj do kopije naslednjega višjega cikla.
- Varnostne kopije aplikativnih in sistemskih programov se izdelajo ob vsaki spremembi.
- Za področje osebnih računalnikov velja za sistemsko in aplikativno programsko področje enaka ureditev. Za podatkovno področje pa je ureditev nekoliko drugačna; vsak uporabnik ima zagotovljen svoj zasebni podatkovni prostor na strežniku, kjer je zagotovljeno tudi zavarovanje teh podatkov. Za varnostno kopiranje podatkov je odgovoren vsak uporabnik osebnega računalnika sam. Varnostno kopijo podatkov hrani na varnem prostoru toliko časa, kolikor sam oceni, da je potrebno.

[48] Okrevalni načrt, 2002

[49] Postopek varnostnega kopiranja, 2001

3.8 Razpoložljivost

Obstaja več načinov, kako se doseže visoko razpoložljivost[50]. Najbolj običajen in preprost način je s podvajanjem komponent sistema. Pri računalnikih se v ta namen podvajajo diski (zrcaljenje), napajalniki, ventilatorji ali mrežne kartice, sistem pa deluje tako, da se dodatne komponente vključijo takoj, ko računalnik zazna izpad primarnih in računalnik deluje tako, kot da se ni nič zgodilo. Za zagotavljanje dobre razpoložljivosti je potrebno poskrbeti za alternativne načine električnega napajanja naprav v primeru izpada glavnega napajanja. Največkrat za to poskrbijo naprave za neprekinjeno napajanje (UPS) in agregati, ki se ob izpadu avtomatsko vključijo.
Lahko pa se zgodi, da odpove celoten računalnik ali pa njegova ključna komponenta, ki ni podvojena. V tem primeru je rešitev dodaten računalnik, ki deluje v gruči s prvim (cluster). Ta računalnik prevzame vse naloge prvega v primeru okvare. Take rešitve se pogosto pojavljajo v strežniških infrastrukturah.
Vendar tudi ta rešitev ne rešuje problema razpoložljivosti v celoti. Lahko se zaradi različnih razlogov, kot je na primer požar v računalniški sobi, ustavijo vsi računalniki v njej. V tem primeru pride v poštev samo rezervna lokacija, na kateri se lahko izvajajo iste operacije, kot na osnovni. Ta zagotavlja neprekinjeno delovanje v primeru večje nesreče in s tem neprekinjeno razpoložljivost sistema. Smiselno je, da je rezervna lokacija precej oddaljena od glavnega računalniškega centra, da je ne bi prizadela ista nesreča kot sam glavni računalniški center (potres). Kakšno prekinitev poslovanja brez ustrezne informacijske podpore (in s tem nerazpoložljivost) si lahko privošči podjetje, opredeli vodstvo glede na posledice in tip poslovanja. Ločimo:

- Hladno rezervno lokacijo – imamo rezervni računalniški center, v katerem so računalniki pripravljeni na delovanje, vendar niso stalno vključeni in popolnoma konfigurirani. Zagon traja dlje časa zaradi zagona vseh računalnikov, potrebnih manjših prilagoditev ter restavriranja podatkov iz rezervnih kopij. To je najcenejša in najenostavnejša rešitev.
- Toplo rezervno lokacijo – tu računalniki sicer delujejo, vendar niso razpoložljivi v trenutku, podatki se prenašajo preko komunikacijskih povezav, vendar niso takoj restavrirani.
- Vročo rezervno lokacijo – ki je popolna kopija računalniškega centra in lahko takoj prevzame vse njegove funkcije. Zagotovljena je sinhroniziranost glavnega in rezervnega računalniškega centra, saj se podatki sproti prenašajo tudi v rezervni center. Razpoložljivost takega sistema je dobra.
- Razžarjeno rezervno lokacijo – ta je popolnoma enakovredna glavni lokaciji, lokaciji stalno nadzorujeta druga drugo in v primeru izpada samostojno prevzameta nalogo. Posebne tehnike poskrbijo za morebitne nevšečnosti, ki bi lahko nastale pri tem. Taka rešitev je najboljša, zagotavlja najboljšo razpoložljivost, vendar je tudi najbolj zapletena in je zaradi tega tudi najdražja.

[50] Hvala, 2002, str. 26

Banka nedvomno sodi med tiste organizacije, ki bi nujno morale imeti vsaj hladno rezervno lokacijo. Zaradi tega je bila jeseni lanskega leta vzpostavljena rezervna lokacija, ki je s centralo povezana z optičnim omrežjem. Na žalost pa je rezervna lokacija od glavne oddaljena le nekaj kilometrov, kar je slabo v primeru naravne katastrofe širših razsežnost, kot je potres, saj še vedno preti grožnja popolnega izpada centralnega računalniškega centra. Razpoložljivost centralnih sistemov v banki se je v letu 2001 po uvedbi sistema ISO 9001/TickIT statistično znatno izboljšala in je po izkušnjah IBM-a na nivoju večjih avstrijskih bank[51].

V današnjem času veliko podjetij ponuja sisteme, predvsem tiste namenjene spletnemu poslovanju, ki obljubljajo zelo visoko razpoložljivost, kar 99.999%[52]. Takšna razpoložljivost pomeni, da so sistemi nerazpoložljivi v celem letu samo 5 minut ali 24 sekund na mesec. Seveda je to le tržni trik prodajalcev in je kaj takšnega v praksi skoraj nemogoče doseči, saj denimo sistemi za vesoljske polete odgovarjajo zahtevam po 99.9% razpoložljivosti. Postavlja pa se vprašanje, kakšna razpoložljivost je dobra za banko, ki nudi svoje storitve 24 ur na dan in 365 dni na leto preko bankomatov, interneta, mobilnih telefonov in drugega. Glede na to, da se celotno poslovanje odvija v državi, ki je relativno majhna, je zelo važno, da so ti sistemi neprekinjeno razpoložljivi predvsem v času od 6 do 24 ure, ko se opravi več kot 99% prometa. Redna vzdrževalna dela in posodabljanje opreme pa se izvajajo v času med 24 in 6 uro zjutraj, pa še to samo enkrat ali nekajkrat na leto s tem, da so vnaprej napovedana. Med vsemi “on line” sistemi imajo največ izpadov bankomati, vendar problem ni tako pereč, saj je v bankomatsko omrežje vključenih več bank. V vsakem večjem kraju je več konkurenčnih bank, ki so s centri povezane po različnih poteh, tako da, razen v redkih izjemah, deluje vsaj nekaj bankomatov. Za sisteme, ki delujejo preko interneta, pa lahko rečemo, da je razpoložljivost kar dobra.

Za zmanjševanje nerazpoložljivosti sistemov je dobro poskrbeti tudi z ustreznimi vzdrževalnimi pogodbami za ključne sisteme. Zato ima banka podpisane dokaj stroge vzdrževalne pogodbe, ki določajo čas za funkcionalno odpravo napake dve do štiri ure in za popolno odpravo napake največ dva dneva. Pogodbeni dobavitelji morajo imeti zato na voljo redundantne sisteme, ki lahko v primeru okvare nadomestijo okvarjene sisteme v banki. Med sisteme, za katere je poskrbljeno s takšnimi vzdrževalnimi pogodbami, spadajo požarni zid, glavni računalniki IBM in DEC, strežniki IBM in Compaq ter usmerjevalniki v omrežju banke.

[51] nIT, 2002, str. 7
[52] Slapar, 2002, str. 22

3.9 Zaščita sodobnega elektronskega poslovanja NLB

3.9.1 Sistem plačevanja velikih vrednosti – SWIFT

Sistem plačevanja med komitenti različnih bank v naši državi se v grobem deli na dva dela:

- BPRČ – bruto poravnava v realnem času,
- SMPV – sistem plačil malih vrednosti.

BPRČ sistem pomeni po številu transakcij 10%, vrednostno pa kar preko 90%, obratno pa zajema SMPV 90% transakcij in manj kot 10% vrednosti prometa.

Banka uporablja za bruto poravnavo v realnem času svetovno medbančno omrežje S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunications). Ker se preko tega sistema prenašajo ogromni zneski, je tudi zelo zanimiv za zlorabe. To je popolnoma zaprt sistem, njegovi udeleženci pa so banke po vsem svetu. S.W.I.F.T. uporablja kriptiranje na različnih segmentih omrežja. Omrežje vsebuje vozlišča in regionalne S.W.I.F.T.-centre, ki vsebujejo vhodne in izhodne regionalne procesorje, sektorske in sistemske kontrolne procesorje[53].
Vsak uporabnik tega sistema ima najmanj dva posebna čitalca pametnih kartic in komplete kartic, ki jih dobi neposredno iz tovarne po preverjanju istovetnosti. Uporabnik ima na voljo več različnih pametnih kartic, vsaka pa je namenjena za določena opravila:

- uporabniška kartica, za normalno delo;
- kartica za izmenjavo ključev;
- kartica za administriranje.

Na kartico so vezane tudi pravice, kaj lahko posameznik v sistemu počne. Kartice je možno v vsakem trenutku blokirati in razveljaviti certifikat, če pride do suma zlorabe.

Na začetku mora vsaka banka pridobiti certifikat od S.W.I.F.T.-centra, ki potrjuje, da je javni ključ banke izviren. Nato mora z vsako banko, s katero želi poslovati, izmenjati ključe. Ključi so dolgi 16 heksadecimalnik znakov in se izmenjujejo na bilateralni osnovi s pomočjo varnostnega ključa za prenos. Življenjska doba ključev je omejena. Avtentikacijski algoritem je razvil S.W.I.F.T. in ni javno znan. Ko so izmenjani ključi, lahko začne banka izmenjavati sporočila finančne ali nefinančne narave s svojimi partnerji. Sistem S.W.I.F.T. vsebuje mehanizme, ki zagotavljajo celovitost sporočil[54], preprečujejo izgubo, podvajanje ali ponavljanje transakcij. To je narejeno s pomočjo dodeljevanja edinstvenega para vhodnih in izhodnih zaporednih številk vsake transakcije.

[53] Oblak, 1997, str. 8
[54] Caelli, 1994, str. 698

Sistem vsebuje tudi varnostne mehanizme, ki preprečujejo grožnjo “maskiranega” napada, tako da bi nepooblaščen uporabnik prestregel sporočilo in ga še enkrat poslal. To je doseženo tako, da vsebuje vsak terminal zaporedno množico gesel. Ob vsaki novi seji se avtomatsko uporabi naslednje geslo iz množice, S.W.I.F.T. pa pošlje nazaj odgovarjajoče edinstveno geslo.
Zaradi zanesljivosti in testiranja delovanja ob uvedbi novosti mora imeti tudi vsak uporabnik podvojen sistem, prvi je namenjen samo testiranju, drugi pa za redno delo.

Slika 16: Pametna kartica, sistem S.W.I.F.T.

3.9.2 Sistem plačevanja malih vrednosti – GIRO

Sistem plačevanja malih vrednosti ali tako imenovani giro kliring[55] predstavlja zaradi manjših zneskov s stališča tveganja manjši problem kot BPRČ. Je pa zaradi obsega dela, raznolikosti in računalniške opreme bolj zapleten. V omrežje SMPV so vključene vse banke in ostale finančne institucije in firme, ki se neposredno vključujejo v sistem za izmenjavo plačilnih nalogov.

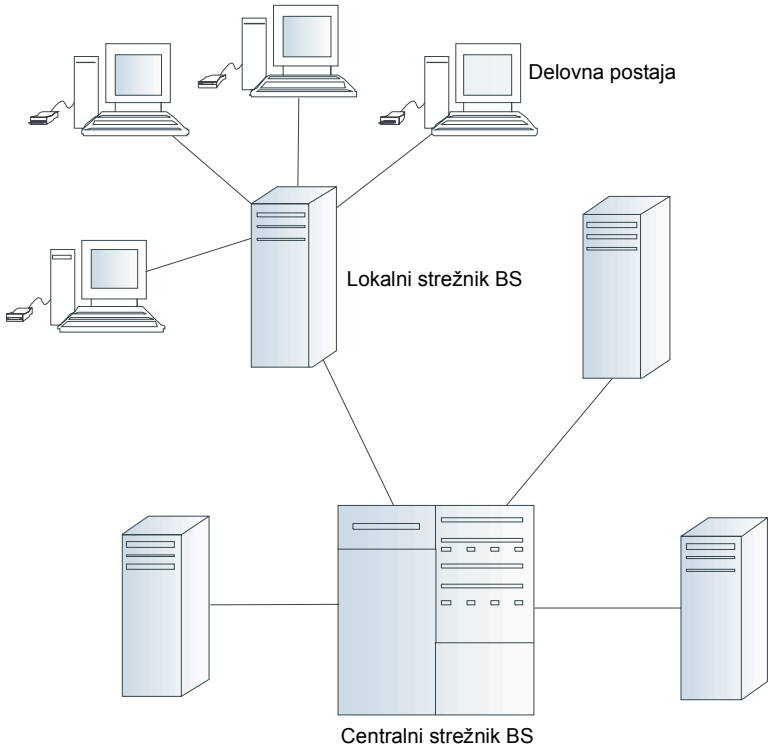
Arhitektura sistema je naslednja (Slika 17):

- V Banki Slovenije je komunikacijsko avtentikacijski center in glavni strežnik, na katerem teče kliring. Center je zaradi varnosti podvojen na različnih lokacijah.
- V vsaki banki je strežnik Banke Slovenije, (ki ga tudi administrira), na katerega so povezane banke. Nanj odlagajo in na njem sprejemajo plačilne naloge.
- Vsaka banka ima za opravljanje plačilnega prometa osebne računalnike, opremljene s čitalci pametnih kartic, kartice, na katerih so shranjeni certifikati potrebni za avtentikacijo ter namensko razvito programsko opremo za šifriranje plačilnih nalogov.
- Vse skupaj povezujejo stalne najete linije.

Oblika plačilnih nalogov se zgleduje po standardih S.W.I.F.T.-a.

[55] Študija za postavitev “giro” klirinškega sistema, 1997, str. 1

Slika 17: Shema omrežja za plačilni promet



3.9.3 Proklik NLB

Proklik NLB je elektronska banka, namenjena podjetjem in samostojnim podjetnikom, ki imajo v NLB odprt poslovni račun. Omogoča opravljanje tolarskega in deviznega plačilnega prometa preko klicne povezave. Obstajata dve različici Proklika – enouporabniška in večuporabniška (mrežna). Večuporabniška različica deluje v načinu odjemalec/strežnik in rabi za delovanje lokalno omrežje, strežnik ter komunikacijski protokol TCP/IP.

NLB zagotavlja uporabniku Proklika NLB povezavo do strežnika elektronskega bančništva prek lastne vstopne točke. Za varno poslovanje prek Proklika NLB je poskrbljeno s šifriranjem in elektronskim podpisovanjem sporočil med uporabnikom in banko. Tako banka kot uporabnik za šifriranje in elektronsko podpisovanje sporočil uporabljata metodologijo dvojnih ključev (RSA, 2048 bitni na strani strežnika in 1024 bitni na strani odjemalca) in metodologijo tajnega zapisa (kriptografija - 3DES). Identifikacija uporabnika in elektronsko podpisovanje potekata prek zaščitne kartice, ki hrani digitalni certifikat po standardih PKI in zasebni ključ. Uporabnik zaščitne kartice mora poznati osebno identifikacijsko številko (PIN). Kartica se samodejno uniči po treh napačno vpisanih osebnih številkah.

3.9.4 Proklik+ NLB

Proklik+ je prav tako kot Proklik elektronska banka, namenjena podjetjem in samostojnim podjetnikom, za razliko pa omogoča opravljanje tolarskega in deviznega plačilnega prometa preko svetovnega spleta.

Uporabnik potrebuje za svoje delo osebni računalnik opremljen s čitalcem pametnih kartic in spletnim brskalnikom. Pred prvo prijavo v Proklik+ mora prejeti digitalni certifikat. Banka mu po dveh različnih poteh (po navadni in elektronski pošti) pošlje dve začasni gesli za prevzem digitalnega certifikata. Uporabnik se s spletnim brskalnikom prijavi na naslov, ki mu ga sporoči banka, in vnese obe začasni gesli ter prevzame digitalni certifikat. Med postopkom za izdajo digitalnega certifikata in prevzema s strani uporabnika se na uporabnikovi kartici Proklik+ ustvarita uporabnikov zasebni in javni ključ. Varovanje zasebnega ključa je temelj uporabnikove varnosti. Javni ključ je del uporabnikovega digitalnega certifikata in je načeloma dostopen vsakomur. Zasebni ključ pa je tajen in je shranjen samo na uporabnikovi kartici Proklik+.

Uporabnik se identificira s svojim digitalnim certifikatom, ki je varno shranjen na njegovi kartici Proklik+. Banka se prav tako identificira s svojim certifikatom. Dostop do podatkov na kartici Proklik+ je zaščiten z osebnim geslom (PIN), ki ga pozna samo pooblaščeni uporabnik kartice. Vsa sporočila, ki si jih izmenjujeta uporabnik in banka, so kodirana tako, da jih morebitni prisluškovalci tako rekoč ne morejo odkodirati. Podatki med banko in uporabnikom se prenašajo po protokolu SSL. Ta jih kodira s pomočjo algoritmov RSA (1024-bitni, namenjen avtentikaciji in izmenjavi ključev) in RC4 (128-bitni, namenjen kodiranju podatkov). Vsakič, ko se uporabnik prijavi v sistem Proklik+, se samodejno izvede preverjanje digitalnih certifikatov v okviru protokola SSL.

Kodiran prenos, digitalni certifikat na kartici Proklik+ in osebno geslo omogočajo celo varnejše poslovanje kot v tradicionalnem bančništvu. Za varnost poslovanja s Proklik+ je bistvenega pomena tudi varnost okolja, v katerem so nameščeni računalniki, s katerih delajo uporabniki. Raven varnosti se bistveno dvigne z uporabo pravilno nameščene požarne pregrade in s sistematičnim zagotavljanjem protivirusne zaščite v podjetju.

3.9.5 Klik NLB

Klik NLB je spletna poslovalnica, namenjena fizičnim osebam. Ponuja praktično vse najpogostejše storitve, ki jih opravljajo uporabniki pred bančnim okencem. Delovanje in zaščita tega sistema je precej podobno delovanju Proklika+, prav tako mora uporabnik na začetku prejeti digitalni certifikat. Razlika je le v tem, da pri Kliku čitalec pametnih kartic in kartica nista obvezna, sta pa priporočljiva. Če ni pametne kartice,

se digitalni certifikat in zasebni ključ nahajata v obliki datoteke na disku računalnika, zato je potrebno z geslom v brskalniku preprečiti možnost, da še kdo drug dobi dostop do vsebine datoteke. Do spletne poslovalnice Klik NLB je od 1. 10. 2002 naprej možno dostopati samo z brskalniki, ki podpirajo 128-bitno šifriranje. Kot dodaten dejavnik verodostojnosti mora uporabnik pri prijavi v Klik vtipkati še svoje osebno geslo. Pri petem napačno vnesenem geslu se uporaba Klika zaklene, kar je dodatna zaščita v primeru, če bi nepooblaščena oseba skušala zlorabiti uporabnikov certifikat.
Kot pri Prokliku^{+} se vsi podatki prenašajo prek protokola SSL, ta pa jih kodira s pomočjo algoritmov RSA in RC4.

3.9.6 Moba NLB

Moba[56] je storitev NLB, ki omogoča uporabnikom opravljanje osnovnih bančnih storitev z uporabo mobilnega telefona kadarkoli in kjerkoli. Je rezultat skupnega razvojnega projekta Nove Ljubljanske banke in družbe Mobitel.

Za delovanje mora imeti mobilni telefon nameščeno pametno SIM-kartico. Vsa sporočila med uporabnikom in banko so šifrirana, da jih morebitni prisluškovalci ne morejo zlorabiti. Vsaka kartica SIM mobilnega telefona, ki je prijavljena za uporabo storitev mobilne banke, je enolično določena in za komunikacijo z banko uporablja svoj neponovljivi šifrirni ključ. Za vsak posamezni dostop do banke prek mobilnega telefona se oblikuje nov ključ. Pri prijavi banke na mobilnem telefonu se mora uporabnik identificirati z unikatno določeno uporabniško številko in osebno dodeljenim bančnim PIN-om. Bančni PIN služi tudi za identifikacijo uporabnika pri opravljanju transakcij preko Mobe NLB, podobno kot pri poslovanju preko bančnega avtomata. Po trikratnem napačnem vnosu bančnega PIN-a se uporaba storitev Mobe NLB zaradi varnostnih razlogov blokira, za nadaljevanje uporabe pa je treba naročiti nov PIN.

Komunikacija poteka preko protokola SSL ter posebnega protokola za šifriranje, ki je precej podoben protokolu WTLS. Protokola poskrbita za izmenjavo ključev ter za ustrezno šifriranje podatkov. Namenske aplikacije, ki tečejo na računalnikih in v mobilnem telefonu, skrbijo za varen prenos podatkov od uporabnika do banke. Pametna kartica v telefonu vsebuje svoj procesor, ki izvaja kodirne in dekodirne algoritme in varno shranjuje podatke, kot so zasebni ključi, certifikat in podobno.

[56] M-bančništvo NLB – uporabniški priročnik

4 METODE PREUČEVANJA TVEGANJ

4.1 Pregled teorij o ocenjevanju varnosti informacijskih sistemov

4.1.1 Razvoj

Začetki poskusov zagotavljanja določene varnosti informacijskih sistemov segajo desetletja nazaj, ko so v vojaške namene začeli razvijati varnostne sisteme za zaščito podatkov. Črpali so iz izkušenj, ki so jih imeli pri zaupnih dokumentih in jih uporabili ter prilagodili tako, da so bili primerni za računalniške sisteme. Računalniška varnost je bila takrat enačena v glavnem z zaščito pred nepooblaščenim dostopom.
V letih 1970 do 1980 je bil najbolj znan model Bell La Padula[57], ki je bil razvit predvsem v vojaške namene in ni bil omejen le na računalniške sisteme, ampak je lahko obravnaval tako fizično kot postopkovno varnost. Predstavljal je temelj za kasnejše modele, kot so model neoporečnosti Biba, model ločljivost Rushby in Take-Grantov model.
Leta 1983 je izdala vlada ZDA navodila za vrednotenje in razvoj zaupnih računalniških sistemov TCSEC, imenovan tudi oranžna knjiga. Pomenila je pomemben korak v potrjevanju varnosti računalniških sistemov. Ker pa je bila precej povezana z modelom Bell La Padula, so se pojavljali dvomi o primernosti teh kriterijev za komercialne namene.
Zato sta se razvila Clark-Wilsonov in Brever–Nashov modela za ocenjevanje varnosti komercialnih sistemov. Tudi v Evropi niso stali križem rok, zato so se predvsem v Veliki Britaniji in Nemčiji pojavila navodila za računalniško varnost. Zaradi potrebe po enotnosti in skladnosti teh navodil je pobudo prevzela Evropska unija in leta 1990 izdala vrsto kriterijev, imenovanih ITSEC. Nazadnje se je zaradi potrebe po poenotenju standardov pojavil nov mednaroden ISO standard, imenovan Common Criteria.

4.1.2 Formalni modeli komercialnih sistemov

Model Clark Wilson

Clark in Wilson[58] sta razvila model varnosti za komercialne sisteme, ki je bil različen od vseh prej znanih modelov, ki so se ukvarjali predvsem z vojaškimi potrebami. Model zagotavlja celovitost finančnih zapisov s predpostavko, da je potrebno zagotoviti ločevanje nalog, vsili pa tudi obvezno kontrolo dostopa. V začetku je potrebno zagotoviti štiri glavne varnostne zahteve:

[57] Caelli, 1994, str. 708
[58] Caelli, 1994, str. 743

- identifikacija in avtentikacija vsakega uporabnika;
- zagotovitev, da lahko na določen podatek vpliva le omejena množica programov;
- sistem mora vsakemu uporabniku dovoliti zaganjanje samo določene množice programov;
- sistem mora vzdrževati revizijsko sled, ki beleži vsak program, ki se je izvedel in uporabnika, ki ga je izvajal.

Poleg tega pa mora računalniški sistem vsiliti pravila in biti zaščiten pred nepooblaščenimi spremembami.

Model definira omejene podatkovne objekte CDI (Constrained Data Item). Če sistem ustreza prej naštetim varnostnim zahtevam, je v začetnem varnem stanju, primerljivim z množico uravnoteženih knjig v knjigovodstvu. Nato model definira množico procedur za vrednotenje celovitosti IVP (Integrity Validation Procedures). Uporaba IVP-jev na CDI zagotavlja varno stanje, primerljivo s preverjanjem knjigovodstva. Vse spremembe na CDI-jih morajo biti take, da sistem prehaja iz enega varnostnega stanja v drugo. To dosežemo z omejevanjem akcij na CDI-jih, z dobro definiranimi transformacijskimi postopki TP (Transformation procedures). To ustreza, na primer, transakciji dveh vnosov v knjigovodstvu. Pomembno je tudi, da so podatki v sistem vneseni pravilno, zato jih je treba pri vnosu preveriti in potrditi ali pa zavrniti.
Model zagotavlja računalniško varnost ob začetnem varnem stanju in varnih prehodih iz enega stanja v drugo.
Da je temu res tako, mora model ustrezati dvema pogledoma na varnost:

- zagotovitev takih postopkov potrjevanja, da IVP-ji in TP-ji v resnici zagotavljajo take varne akcije;
- oblikovanje ustrezne varnostne politike za prisilo.

Clark Wilsonov model predstavlja enega od največjih korakov v razvoju formalnih modelov. Pri vrednotenju računalniških sistemov pa se pojavi problem, kako testirati sistem, da ugotovimo, če ustreza temu modelu.

Model Brewer Nash – model kitajskega zidu

Model Brewer Nash[59] je zamišljen kot neka organizacija, ki opravlja storitve za več strank - organizacij, o katerih hrani podatke. Varnostna politika je naslednja:

- Uporabnik (subjekt) lahko na začetku dostopa do katerih koli podatkov (objektov), recimo do podatkov o turistični organizaciji A.
- Uporabnik lahko sedaj poljubno dostopa do podatkov te turistične organizacije, ne more pa več dostopati do podatkov turistične organizacije B,

[59] Caelli, 1994, str. 750

ker bi lahko poznavanje podatkov organizacije A pomenilo konflikt v interesih. Turistični agenciji A in B predstavljata konfliktni razred.
- Uporabnik lahko dostopa tudi do podatkov o pekarni C, ker turistična organizacija A in pekarna C nista v konfliktnem razredu. Vendar pa spet ne more dostopati do nobene pekarne več.

Tako omejevanje podatkov za uporabnika, takoj ko dostopa do podatkov, je podobno gradnji zidu okoli njih, zato je model znan tudi pod imenom model kitajskega zidu. Ta model vsili zelo strogo kontrolo dostopa objektov do subjekta.

Težave, ki lahko nastopijo pri tem modelu, so naslednje. Če je organizacija A v konfliktu z organizacijo B in organizacija B v konfliktu z organizacijo C, potem iz modela sledi, da je tudi organizacija A v konfliktu z organizacijo C, vendar pa ta tranzitivna relacija v praksi ni vedno nujna.

TCSEC

Leta 1983 je ameriško obrambno ministrstvo, pravzaprav National Computer Security Centre, izdalo prvo verzijo TCSEC (Trusted Computer Security Evaluation Criteria) imenovano po barvi platnic tudi Oranžna knjiga. Leta 1985 je bila obnovljena in objavljena kot standard. Oranžna knjiga so pravzaprav navodila za vrednotenje in razvoj zaupnih računalniških sistemov[60]:

- Sisteme deli na 4 hierarhične skupine, od A, B, C in D, nekatere pa so razdeljene še na podrazrede B1, B2, B3 ter C1 in C2. Razred A pri tem pomeni najbolj varen sistem, razred D pa najmanj varen sistem.
- Vsak razred obravnava varnostno politiko, identifikacijo, označevanje, odgovornost, zavarovanje ter sovisno zaščito.
- Osnovna razlika med razredoma B in C je področje nadzora dostopa. Pri razredu C2 lastniki objektov odločajo, kdo lahko dostopa do objekta in s kakšnimi pooblastili. To se imenuje tudi samovoljna kontrola dostopa (Discretionary Access Control - DAC). Pri razredu B pa je varnostni razred objekta neodvisen od njegovega lastnika, to pa se imenuje obvezna kontrola dostopa (Mandatory Access Control – MAC). Zaradi tega mora sistem označevati podatke.

Osnovna ideja TCSEC je uporaba zaupnega računalniškega jedra (Trusted Computing Base - TCB), ki ne dopušča vmešavanje v TBC ter zagotavlja ločevanje naslovnega prostora, zaupne poti, princip najmanj enakih pravic in neokrnjenost operacij.
Ocenjevanje opravlja ameriška vladna organizacija National Security Agency – NSA, katera tudi podeli ustrezen naziv. Komercialni sistemi so običajno v razredu C2. Sistemi razreda B so redkejši, razviti pa so predvsem za vojaške namene.

[60] IT Security Cookbook, 2002

Zavedati se je potrebno, da sistem, ki je bil ocenjen pri NSA z nazivom B1, ne zagotavlja nujno takšne varnosti, če je sistem v praksi izpostavljen drugačnim pogojem kot pri ocenjevanju.

ITSEC

ITSEC[61] (Information Technology Security Evaluation Criteria) je kriterij za ocenjevanje varnosti računalniških sistemov, ki je nastal kot združitev varnostnih standardov Nemčije, Francije, Nizozemske in Velike Britanije. Evropska unija ga je objavila kot standard za vse članice aprila 1995. ITSEC precej povzema TCSEC, vendar pa je od njega širši, saj ločuje vrednotenje funkcionalnosti od stopnje zavarovanja (assurance). Predpostavlja 7 nivojev zavarovanja (E0-E6) in 10 funkcionalnih nivojev (F1-F10). Ukvarja se z varnostnim ocenjevanjem tako sistemov kot produktov zanje. Za funkcionalnost priporoča obravnavanje osmih splošnih poglavij:

- identifikacija in avtentikacija,
- nadzor dostopa,
- odgovornost,
- revizija,
- ponovno uporabo objektov,
- točnost,
- zanesljivost,
- izmenjavo podatkov.

Pri zavarovanju pa pozna 7 nivojev, od E0, ki predstavlja nezadostno zavarovanje, pa vse do E6, ki zahteva formalno opisano varnostno arhitekturo in skladnost s formalno varnostno politiko.

ITSEC definira 10 funkcionalnih razredov, primere funkcionalnih razredov F-C1, F-C2, F-B1, F-B2 in F-B3, ki so podobni TCSEC ter nove razrede IN, AV, DI, DC in DX. Pri primerih razredov je poveza med ITSEC IN TCSEC naslednja:

Tabela 7: Povezava med ITSEC in TCSEC

ITSEC	TCSEC
E1, F-C1	C1
E2, F-C2	C2
E3, F-B1	B1
E4, F-B2	B2
E5, F-B3	B3
E6, F-B3	A1

Vir: IT Security Cookbook, 2002

[61] Caelli, 1994, str. 764

Novi razredi, ki so zanimivi predvsem zato, ker vključujejo tudi omrežja, katera manjkajo v TCSEC, so:

- F-IN – sistemi z visokimi zahtevami glede neoporečnosti in celovitosti za programe in podatke;
- F-AV – visoko razpoložljivi sistemi;
- F-DI – sistemi, z visokimi zahtevami glede neoporečnosti podatkov pri prenosu;
- F-DC – sistemi z visokimi zahtevami glede zaupnosti podatkov pri prenosu;
- F-DX – sistemi z visokimi zahtevami glede neoporečnosti in zaupnosti za podatke.

Common Criteria

Ker sta merili vrednotenja računalniških sistemov ITSEC IN TCSEC precej podobni in so vrednotili iste sisteme tako v Evropi kot v Ameriki, so uvedli nov mednarodni standard, v katerem so združili kriterije Evropske unije, ZDA in Kanade v novo shemo za vrednotenje varnosti informacijske tehnologije CCITSE (Common Criteria for Information Technology Security Evaluation), bolj znani kot Common Criteria. Groba primerjava med ITSEC, TCSEC in CC je v spodnji tabeli (Tabela 8):

Tabela 8: Primerjava med CC, ITSEC in TCSEC

Evaluation Assurance Level (CC)		ITSEC	TCSEC
EAL1	Funkcionalno testirano	E0	D
EAL2	Strukturalno testirano	E1, F-C1	C1
EAL3	Metodično testirano in preverjeno	E2, F-C2	C2
EAL4	Metodično modelirano, testirano in ocenjeno	E3, F-B1	B1
EAL5	Polformalen model in testirano	E4, F-B2	B2
EAL6	Polformalno potrjen model in testirano	E5, F-B3	B3
EAL7	Formalno potrjen model in testirano	E6, F-B3	A1

Vir: Zdravkovič, 2002, Hua, 2002

4.1.3 Kako ocenjevati?

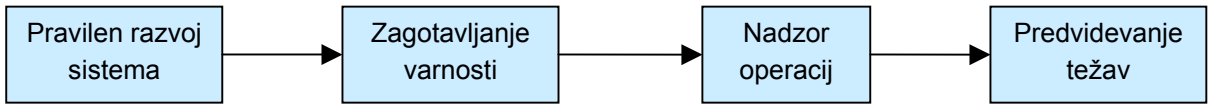
Namen formalnih modelov je pomoč pri ocenjevanju varnosti računalniških sistemov. Vendar pa je ocenjevanje varnosti zelo težko opravilo. V dokumentaciji ITSEC je omenjena celo nevarnost preveč vnetega ocenjevalca. Najzahtevnejše opravilo je gotovo povezava kriterija vrednotenja z živim okoljem zapletenega sistema, ki je sestavljen iz strojne in programske opreme, omrežij in ljudi. Kljub temu, da lahko v sistem vložimo ogromno, da odgovarja klasifikaciji razreda A1 po TCSEC, pa lahko pride do razkritja zaupnih podatkov, če uporabnik z visokimi pooblastili ne upošteva varnostne politike.
Zato ni presenetljivo, da odgovarja Denis Longley[62] na vprašanje “Kako meriti varnost?” z besedami “S precejšnjimi težavami!”.

[62] Caelli, 1994, str. 775

4.2 Metoda za zmanjševanje tveganj v informacijskem sistemu

Organizacija mora sama dobro poskrbeti za zagotavljanje in vzdrževanje varnosti svojega informacijskega sistema. Pravilna pot pri tem je prikazana z vrednostno verigo na spodnji sliki (Slika 18)[63]:

Slika 18: Vrednostna veriga za varen in nadzorovan sistem



Vir: Alter, 1999, str. 475

4.2.1 Pravilen razvoj sistema

Pravilen razvoj sistema pomeni zagotavljanje kvalitetne programske opreme. To pa se lahko doseže le s kvalitetno opravljenim preizkušanjem vse programske opreme, ki gre v produkcijsko okolje. Vsi novi programi, ne glede na to, ali so bili razviti v sami organizaciji ali pa zunaj nje, morajo biti pred uporabo dodobra preizkušeni, da že v fazi testiranja odkrijemo morebitne napake in pomanjkljivost, ki bi utegnile v produkciji povzročati precejšnje težave. Taki testi morajo poleg ostalega zajemati tudi varnostno testiranje, ki lahko prepreči vnos programske opreme s zlonamernim delovanjem, kot so razni virusi, še posebej pa se je treba posvetiti odkrivanju morebitnih trojanskih konjev skritih v programih. K vsakemu programu sodi tudi dobra dokumentacija. V vseh fazah testiranja mora odražati vse, kar se je dogajalo s programom, opisovati mora vse spremembe in popravke ter vsebovati zgodovino o programu.
Podobno kot za programsko opremo velja tudi za preizkušanje strojne opreme pred uvedbo v produkcijsko okolje.

4.2.2 Zagotavljanje varnosti

Zagotavljanje varnosti pa zajema:

- izobraževanje zaposlenih o varnosti;
- vzdrževanje fizične varnosti;
- nadzor dostopa do podatkov, računalnikov in omrežja.

Organizacija mora dobro poskrbeti za izobraževanje vseh zaposlenih glede varnosti. Zato ni dovolj, da samo sprejme varnostno politiko, ki je ponavadi, razen redkih

[63] Alter, 1999, str. 475

izjem, tako nihče ne prebere, ampak mora ljudi motivirati, da posvečajo ustrezno pozornost varnostnim problemom. Zaposlenim je potrebno razložiti, zakaj je pomembna varnost, zakaj so potrebne razne omejitve in kako prepoznajo sumljive aktivnosti v postopkih poslovanja. Veliko problemov si lahko na primer prihranimo že z obveščanjem uporabnikov o nevarnostih povezanih z virusi, ki jih lahko dobijo preko elektronske pošte ali preko interneta. Organizacija mora imeti glede na velikost tudi ustrezne posebej izšolane strokovnjake ali službe, ki se posvetijo problematiki varnosti v podjetju, katerim lahko tudi ostali zaposleni sporočajo probleme in opažanja povezana z varnostjo.

Splošno načelo pri zagotavljanju fizične varnosti je, da morajo biti računalniška in komunikacijska oprema izven dosega nepooblaščenih oseb. Zato mora organizacija uvesti ločene prostore, ki fizično omejujejo dostop. S tem se precej zmanjša možnost nesrečnega ali namernega poškodovanja naprav. V bolj občutljivih okoljih je smiselno uvesti varnostne cone z različnimi stopnjami varovanja glede na strojno opremo.

Poleg tega pa je treba nadzorovati dostop do podatkov, računalnikov in omrežja. Poskrbeti je treba za osnovno pravilo “čiste” mize, to pomeni, da uporabniki po končanem delu ne smejo puščati dokumentov s podatki na mizi in da morajo zaklepati predale in omare, kjer hranijo podatke. Ko se podatki ne potrebujejo več, je treba poskrbeti za uničevanje dokumentov s sežiganjem ali razrezanjem oziroma za zanesljivo brisanje ponovno uporabnih nosilcev podatkov. Omejiti je treba pravice dostopa tako do računalnikov kot do podatkov na njem ter zagotoviti nadzor nad prihajajočimi in odhajajočimi podatki iz drugih omrežij in medijev. Pri tem se uporabljajo različne tehnike in metode, ki so opisane v prejšnjih poglavjih.

4.2.3 Nadzor operacij

Nadzor operacij pa zajema:

- nadzor obdelave transakcij;
- spodbujanje učinkovitih in zmogljivih operacij;
- revizijo sistema.

Nadzor obdelave transakcij obsega nadzor nad zbiranjem podatkov, preverjanje podatkov in preverjanje njihovega arhiviranja. Pri zajemu podatkov lahko uporabimo metodo ločevanja dolžnosti, ki zahteva vpletenost več oseb, kar zmanjša možnost kriminalnih dejanj. Poskrbeti je treba za preverjanje pravilnosti vnesenih podatkov, vendar se je treba zavedati, da se lahko preverjajo samo sintaktične, ne pa tudi semantične napake. Na koncu je potrebno poskrbeti tudi za varnostno shranjevanje in po potrebi vračanje transakcij in podatkov v sistem ter po možnosti za zagotovitev revizijske sledi, ki pride še kako v pomoč pri odkrivanju kriminalnih dejanj.

Za zagotavljanje učinkovitost in ustrezne zmogljivosti je treba občasno izvajati meritve na računalniških sistemih. Meritve zajemajo merjenje zmogljivosti tako za poslovni proces kot tudi za sam informacijski sistem. Le tako se lahko prepričamo, ali sistem deluje optimalno, lahko ugotovimo, kje so ozka grla in tudi predvidevamo morebitne težave v prihodnje. Te ugotovitve so dobra osnova za kasnejše razširitve in posodabljanje sistema. Seveda pa je potrebno opažanja na primeren način posredovati ustreznim odgovornim osebam. Poleg vsega naštetega pa je treba uporabnike seznaniti s stroški informacijskega sistema z namenom, da se vzbudi zavest smotrne uporabe. Uporabniki se morajo zavedati, da v času, ko uporabljajo internet v zasebne namene, ne samo ne opravljajo svojega dela, ampak zasedajo tudi pomembne vire podjetja in celo ovirajo druge upravičene uporabnike pri delu.

Revizija računalniških sistemov se deli na:

- Splošen nadzor, ki ugotavlja, kako je poskrbljeno za varnost poslovanja, kako se upoštevajo pravilniki in standardi, kako je poskrbljeno za uporabo raznih varnostnih metod, kakšni so postopki itd..
- Aplikacijski nadzor, ki preverja pravilnost shranjevanja, procesiranja podatkov in poročanja, še posebej pri finančnih transakcijah. Pri tem se uporabljata dve metodi, revidiranje okrog računalnika in revidiranje skozi računalnik. Pri revidiranju okrog računalnika jemlje revizor računalnik kot črno škatlo ter primerja, če so rezultati v skladu s pričakovanji glede na vhodne podatke. Taka metoda večkrat ne odkrije vseh zlorab. Zaradi tega je boljša metoda revidiranje skozi računalnik, ki zahteva, da je revizor dober strokovnjak za računalništvo in preverja postopke in programe v računalniku. Zaradi zahtevnosti pa je druga metoda precej dražja od prve.

4.2.4 Predvidevanje težav

Vsak informacijski sistem je slej ko prej izpostavljen težavam. Dober informacijski sistem jih pričakuje in ima že vnaprej pripravljene postopke, s katerimi skuša omiliti težave ali obnoviti svoje delovanje. Zato je treba pravočasno sestaviti dober načrt priprave na katastrofo ter zagotoviti dodatne kapacite, ki pridejo v poštev v primeru večje nesreče. Kako je ta načrt potreben, smo bili priča v primeru znanega problema z letnico 2000 (Y2K).

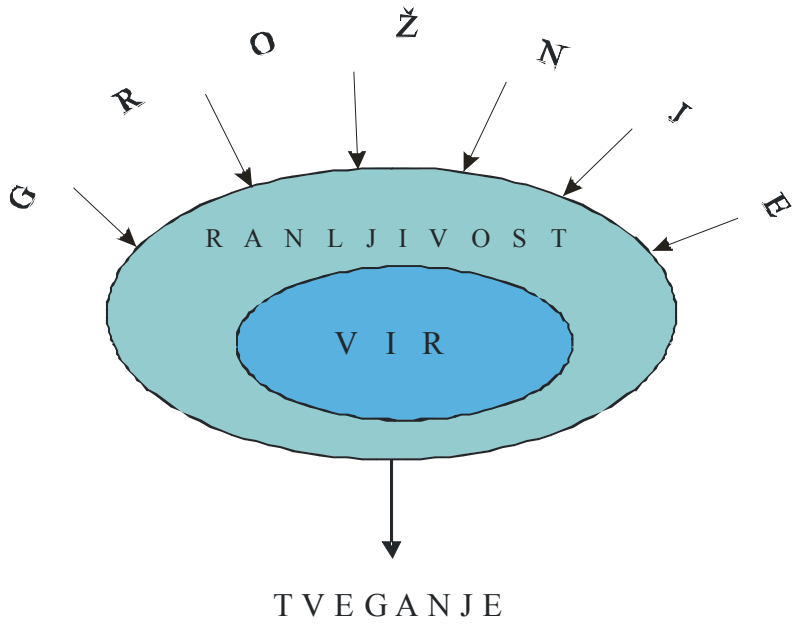
4.3 Analiza tveganja

4.3.1 Uvod

Na začetku je treba razjasniti nekaj osnovnih pojmov pri analizi tveganj:

- Vir: je stvar oziroma predmet, ki jo obravnavamo pri analizi tveganj. Vir je lahko računalnik, program, informacijski podsistem, posamezna komponenta v računalniku in podobno.
- Grožnja: je dogodek, ki lahko povzroči škodo ali izgubo na virih ali pri poslovanju. Grožnje so lahko namerne, kot je vdor hekerja v računalnik ali pa slučajne, kot je na primer potres.
- Ranljivost: je slabost posameznega vira, ki jo izkoristi grožnja. Komunikacijski vodi so na primer ranljivi glede prisluškovanja,.
- Tveganje: predstavlja možnost oziroma verjetnost, da se bo zaradi ranljivosti vira grožnja uresničila. Tveganja lahko skoraj poljubno zmanjšamo, ne moremo pa se jim v celoti izogniti.

Slika 19: Grožnje, ranljivosti, tveganje



Za primer lahko vzamemo, da je vir posamezen osebni računalnik. Grožnjo predstavlja okužba z zlonamerno programsko opremo kot je virus. Ranljivost računalnika je občutljivost na okužbo z virusom. Če je računalnik priključen v omrežje, je bolj ranljiv, kot če ni. Iz tega izhaja tudi večje tveganje, da bo do okužbe prišlo. Ranljivost pa lahko tudi zmanjšamo tako, da na računalnik namestimo protivirusni program in ga redno posodabljamo ter poskrbimo za ustrezno osveščanje uporabnikov glede zlonamerne programske opreme. Zmanjšanje ranljivost pa ima za posledico tudi manjše tveganje v zvezi s to grožnjo.

4.3.2 Analiza

Analiza tveganja je temeljni postopek, s katerim sistematično ugotovimo, s katerimi viri razpolagamo, jih opredelimo, opravimo pregled groženj, katerim so ti viri podvrženi in ocenimo tveganja, ki nastanejo. Ta analiza je temelj za kasnejše ukrepanje, saj nam pove, kje so največje varnostne luknje v informacijskem sistemu. Na njeni osnovi izdelamo varovalne ukrepe.
Informacijska tehnologija mora podpirati poslovni proces tako, da bodo vse informacije in postopki, ki jih poslovni sistem uporablja, zadoščale najmanj trem kriterijem, ki jih opredeljujeta tudi mednarodni standard ISO/IEC 17799:2000 in britanski standard BS 7799-2[64], to pa so:

- zaupnost (confidentiality) – označena z Z;
- neoporečnost, celovitost (integrity) – označena z N;
- razpoložljivost (availability) – označena z R.

Vsaka informacija, ki se prenaša v elektronski obliki, je potencialno lahko ukradena in razkrita drugim, če se lahko nekdo nepooblaščeno prijavi v sistem ali pa prisluškuje izmenjavi podatkov. Posledice take kraje podatkov so lahko pri finančnih institucijah tudi kritične, zato je ključen kriterij kakovosti v banki med drugim tudi to, da imajo dostop do informacij izključno pooblaščene osebe. Zaščita zaupnost pri informacijah pomeni ščitenje informacij pred nepooblaščenim razkritjem ali prestrezanjem njihovega pomena.

Neoporečnost informacij pove, da so informacije celovite in pravilne, zagotavlja, da ni prišlo do nekontroliranih sprememb. Cena, ki jo lahko podjetje plača zaradi neoporečnosti informacij, je praviloma zelo visoka. Odraža se v izgubi ugleda in nezaupanju strank in s tem posledično izgubi strank in dohodka. Zaščita neoporečnosti pomeni varovanje točnosti in popolnosti informacij ter računalniške in programske opreme.

Tudi razpoložljivost informacij je pomemben dejavnik, še posebej se ga organizacija zaveda takrat, ko so neke informacije ali storitve zaradi napak, odpovedi, nadgradenj in podobnega nedostopne. V sedanjem času, ko sistemi temeljijo na računalniški tehnologiji in so sistemi zelo medsebojno povezani, so lahko izgube zaradi nerazpoložljivosti velike. Zagotavljanje razpoložljivosti pomeni zagotavljanje, da so informacije in računalniške storitve vedno na voljo uporabnikom, ko jih potrebujejo.

Na teh treh kriterijih varovanja informacij sloni tudi metoda analize tveganj. Obstaja več različic te metode, vse pa so si do neke mere podobne. Metoda, ki jo bom opisal v nadaljevanju, se nekoliko razlikuje od ostalih, ki jih najdemo v literaturi, pa tudi od tiste, ki je v uporabi v banki. Nastala je na podlagi mojih izkušenj s to problematiko in na osnovi podobnih metod.

[64] British standard, 1999, str. 12

4.3.3 Postopek

Področje analize

Prvi korak je izbor področja analize. Odločiti se moramo, kaj bomo analizirali. To je lahko celoten poslovni sistem, poslovno področje, samo glavni računalnik ali pa samo eden od programov. Smiselno je, da je analiza ozkega področja bolj podrobna, pri širšem področju pa bolj površinska. Možno pa je tudi najprej opraviti analizo širšega področja, poiskati šibke točke v sistemu ter le-te kasneje še enkrat obdelati z bolj podrobno analizo.

Popis virov

V drugem koraku se popišejo viri, ki sodijo v področje analize. Vire pa lahko razporedimo v več skupin[65]:

- informacije in podatki,
- strojna oprema,
- programska oprema,
- infrastruktura,
- dokumentacija,
- ostalo,
- ljudje (pogojno).

Prvo skupino sestavljajo informacije in podatki na različnih medijih, tako v elektronskih kot papirnih in drugih. Pod strojno opremo sodijo računalniki, komunikacijska oprema, mrežna oprema, mediji in podobno. Pod programsko opremo pa sodi sistemska programska oprema, strojna programska oprema, aplikacijska programska oprema, sistemi za upravljanje baz podatkov in razvojna programska oprema. Infrastrukturo sestavljajo prostori, napeljave, klima naprave, protipožarna oprema itd. Pod dokumentacijo spadajo vsi opisi postopkov, delovna navodila, natisnjeni programi in podobno. Dokumentacija se lahko nahaja na papirju, mikrofilmu, disku ali na kakšnem drugem mediju.
Pri popisu virov si pomagamo s tabelo (Tabela 9), ki vsebuje naslednje podatke: naziv vira, njegov opis ter oceno glede zahtevane zaupnosti, neoporečnosti in razpoložljivosti (ocena Z-N-R).

Tabela 9: Tabela virov

Naziv vira	Opis	Ocena Z - N - R
		Z:
		N:
		R:

[65] Obvladovanje informacij v skladu s standardom BS7799, 2001, str. 20

Ocena virov glede zahtevane stopnje varnosti (Z-N-R)

V tretjem koraku ocenimo vire glede na zahtevano zaupnosti, neoporečnosti in razpoložljivosti pri poslovanju. Ocene za vire glede Z-N-R so naslednje:

- 4 – bistven,
- 3 – zelo pomemben,
- 2 – pomemben,
- 1 – malo pomemben,
- 0 – nepomemben.

Ocenjevanje poteka na osnovi pomembnosti virov za poslovno področje, zato morajo oceno dati ustrezne osebe s tega poslovnega področja, za razliko od vseh nadaljnjih ocen, ki jih dajo strokovnjaki s področja informacijske tehnologije.

Ocenjevalci se morajo vprašati predvsem naslednje[66]:

- glede zaupnosti:
  - ali lahko razkritje informacij (konkurenci) vpliva na izgubo konkurenčne prednosti;
  - ali lahko vpliva razkritje informacij na izgubo posla;
  - kakšen vpliv ima razkritje informacij na zaupanje strank in javnosti;
  - ali razkritje informacij povzroči dodatne stroške;
  - kakšna je zakonska odgovornost v primeru razkritja;

- glede neoporečnosti:
  - kakšen je vpliv oporečnih informacij na odločitve vodstva;
  - ali lahko spremembe vplivajo na prekinitve poslovanja;
  - kakšen je vpliv oporečnih informacij na zaupanje javnosti;
  - kakšne so zakonske odgovornosti v primeru oporečnosti;
  - ali so pooblaščene spremembe informacij v resnici goljufija;
  - ali lahko oporečne informacije povzročijo dodatne stroške;

- glede razpoložljivost:
  - ali lahko nerazpoložljivost sistemov vpliva na odločitve vodstva;
  - ali lahko zaradi nerazpoložljivosti izgubimo posel;
  - ali je omajano zaupanje javnosti in komitentov zaradi nerazpoložljivosti;
  - ali nastanejo kakšni dodatni stroški;
  - kakšna je zakonska odgovornost organizacije zaradi prekinitev;
  - kakšne posledice nastanejo zaradi prekinitve dela.

[66] Pravilnik o analizi IT tveganj, 2002

Primer:

Za primer lahko vzamemo majhno internetno trgovino. Podjetje ima spletni strežnik, na katerem teče spletna aplikacija za naročila preko interneta, domenski strežnik in 3 osebne računalnike, povezane v mrežo, ki jih uporabljajo pri poslovanju. Težave na spletnem strežniku bi bile za podjetje zelo hude, medtem ko bi nedelovanje enega od osebnih računalnikov pomenilo manjše težave. Razkritje kakršnih koli podatkov bi bilo zelo problematično, prav tako bi neoporečni podatki predstavljali veliko oviro:

Tabela 10: Primer ocenjevanja virov

Naziv vira	Opis	Ocena Z – N - R
Spletni strežnik	Spletni strežnik, na katerem teče spletna trgovina	Z: 4
		N: 4
		R: 4
Domenski strežnik	Domenski strežnik	Z: 2
		N: 3
		R: 4
Spletna aplikacija	Aplikacija za naročanje artiklov preko interneta	Z: 4
		N: 4
		R: 4
Osebni računalnik	Osebni računalnik, ki se uporablja pri poslovanju	Z: 4
		N: 4
		R: 2

Ocena ogroženosti

Oceno ogroženosti izdelajo ustrezni strokovnjaki informacijske tehnologije. Najprej je potrebno identificirati grožnje, ki obstajajo za vsak vir. Opozoriti je potrebno, da vsakemu viru grozijo različne grožnje. Na primer poplava lahko grozi računalniku, računalniški virus programski opremi in podatkom, kraja pa lahko grozi vsemu. Pri opisu groženj si pomagamo s spodnjo tabelo ogroženost, kamor vpišemo podatke, pri tem pa si pomagamo s tabelo virov.

Tabela 11: Tabela ogroženosti

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
			Z:	Z:
			N:	N:
			R:	R:

Ocenimo grožnjo:

- 0 – zanemarljiva,
- 1 – zelo majhna,
- 2 – majhna,

- 3 – srednja,
- 4 – velika.

Nato ocenimo ranljivost vira. Spet vzamemo za ocenjevanje številke:

- 0 – neranljiv, neobčutljiv vir,
- 1 – zelo malo ranljiv,
- 2 – delno ranljiv,
- 3 – srednje ranljiv,
- 4 – zelo ranljiv.

Če vzamemo za primer nosilce podatkov in grožnjo nenamerno brisanje podatkov, je disk zelo ranljiv za brisanje podatkov po nesreči, CD ROM pa neranljiv.

Od tod dalje dobimo oceno ogroženosti tako, da preprosto seštejemo številčne vrednosti teh dveh ocen. Vrednost se tako lahko giblje med 0 in 8.

Primer:
Recimo, da obstajata dve grožnji:

- *odpoved diskov v računalniku,*
- *vdor v računalnik preko interneta.*

Strežnik ima diske v RAID-polju, se pravi da vsebuje redundantne diske in je zato manj občutljiv glede odpovedi diskov. Verjetnost, da bosta hkrati odpovedala najmanj dva diska je majhna. Računalnik ima le en disk, zato so lahko ob okvari izgubljeni vsi podatki in traja dlje časa, da ga ponovno usposobimo za delo. Strežnik in računalnik sta povezana v omrežje in zaščitena s preprostim požarnim zidom.

Tabela 12: Primer ocene ogroženosti

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Spletni strežnik	okvara diska	1	Z: 0	Z: 1
			N: 1	N: 2
			R: 1	R: 2
Osebni računalnik	okvara diska	1	Z: 0	Z: 1
			N: 2	N: 3
			R: 4	R: 5
Spletni strežnik	vdor preko interneta	2	Z: 3	Z: 5
			N: 3	N: 5
			R: 3	R: 5
Osebni računalnik	vdor preko interneta	2	Z: 3	Z: 5
			N: 3	N: 5
			R: 1	R: 3

Ocenjevanje tveganj

Ocena tveganj je kombinacija ocene poslovnega sektorja (ocena zahtevane stopnje varnosti Z-N-R) in informacijskega sektorja (ocena ogroženosti). Tabela virov in tabela ogroženosti sta osnova za izdelavo ocene tveganj. Podatke iz teh dveh tabel vnesemo v novo tabelo:

Tabela 13: Tabela ocenjevanja tveganj

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
		Z:	Z:	Z:
		N:	N:	N:
		R:	R:	R:

Oceno tveganja dobimo s pomočjo prevajalne tabele:

Tabela 14: Prevajalna tabela

Ocena Z-N-R	Ocena ogroženosti								
	0	1	2	3	4	5	6	7	8
0	0	1	1	2	2	3	3	4	4
1	1	1	2	2	3	3	4	5	6
2	1	2	2	3	4	5	6	7	8
3	2	2	3	4	5	6	7	8	9
4	2	3	4	5	6	7	8	9	10

Vrednosti ocen tveganja se gibljejo med 0 in 10. Postaviti je potrebno merilo, kdaj je tveganje še sprejemljivo.

Kriterij je naslednji:

- od 0 do 2 točki: tveganja ni ali pa je zanemarljivo;
- 3 točke tveganje je majhno;
- od 4 do 5 točk: tveganje je sprejemljivo;
- 6 točk: tveganje je pogojno sprejemljivo, razmisliti je treba o ukrepih;
- 7 točk: tveganje je zelo pogojno sprejemljivo, priporočljivi so ukrepi;
- od 8 do 10 točk: tveganje je nesprejemljivo, ukrepi so nujni.

Primer:

Za naš primer bi tabela ocenjevanja tveganj izgledala takole (Tabela 15):

Tabela 15: Primer tabele ocenjevanja tveganj

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Spletni strežnik	okvara diska	Z: 1	Z: 4	Z: 3
		N: 2	N: 4	N: 4
		R: 2	R: 4	R: 4
Osebni računalnik	okvara diska	Z: 1	Z: 4	Z: 3
		N: 3	N: 4	N: 5
		R: 5	R: 2	R: 5
Spletni strežnik	vdor preko interneta	Z: 5	Z: 4	Z: **7**
		N: 5	N: 4	N: **7**
		R: 5	R: 4	R: **7**
Osebni računalnik	vdor preko interneta	Z: 5	Z: 4	Z: **7**
		N: 5	N: 4	N: **7**
		R: 3	R: 2	R: 3

Vidimo, da je v tabeli kar nekaj sedmic pri ocenah tveganja – se pravi, da je ocenjeno, da bi bilo lahko poslovanje prizadeto zaradi vdora v spletni strežnik ali osebni računalnik preko interneta. To pomeni, da je tveganje zelo pogojno sprejemljivo in da je priporočljivo na tem področju ukrepati, na primer z izboljšanjem požarne pregrade. Tudi dve petici sta se pojavili pri okvari diska osebnega računalnika, v tem primeru bi lahko razmislili, ali so podatki na osebnih računalnikih takšnega pomena, da bi bilo potrebno redno izdelovanju rezervnih kopij podatkov tudi na teh računalnikih.

4.3.4 Avtomatizacija metode in njena uporaba

Metoda je zasnovana na način, ki omogoča zelo enostavno pretvorbo v program ali v preglednico kot je npr. Microsoft Excel. Glede na to, da metoda vsebuje veliko enostavnih in enoličnih opravil, ki zahtevajo precej časa, kar kliče po avtomatizaciji. Programska rešitev bi lahko vsebovala seznam že vnaprej vnesenih virov, ki bi ga lahko poljubno dopolnjevali ter tipične grožnje, ki so povezane s temi viri. V okviru programske rešitve bi bilo možno izdelati tudi povezave med splošnejšo analizo nekega področja ter podrobnejšimi analizami posameznih bolj ozkih podpodročij.

Bistven del, to je ocene, pa je treba v vsakem primeru vnašati ročno, saj zahteva ta korak tehtno presojo in kar nekaj občutka. Ocenjevalec mora zavzeti kritično izhodišče, ki ne sme biti niti pretirano strogo, niti preveč ohlapno. Predvsem pa mora dobro poznati področje, ki ga proučuje, če hočemo, da so ocene uporabne.

5 OCENA VARNOSTI Z UPORABO METODE ANALIZE TVEGANJ

Za oceno varnosti informacijskega sistema sem izbral metodo analize tveganj zaradi večih razlogov. Prvi je nedvomno ta, da je metoda dovolj enostavna, da jo lahko uporabimo na tako zapletenem področju kot je informacijska tehnologija banke. Je tudi dovolj splošna, da jo lahko prilagodimo na problematiko, ki me zanima, to pa je ocena, kako dobro je tehnološko zaščiten informacijski sistem banke. Tretji razlog je, da bi bila uporaba kakšnega standardnega kriterija vrednotenja varnosti informacijskega sistema (ITCES, TCSEC…) za enega človeka preprosto neobvladljiva naloga, na razpolago pa bi moral imeti bistveno več podatkov o informacijskem sistemu, kar pa je glede na občutljivost področja tudi iluzorno pričakovati.

Področje analize je možno izbrati zelo različno. Lahko izberemo področje iz poslovnega vidika, na banki recimo poslovanje z vrednostnimi papirji ali poslovanje z gospodarskimi družbami, lahko pa se odločimo samo za del področja ali pa za celotno poslovanje. Ker naloga preučuje varnost sistema in predvsem njegov tehnološki vidik, sem se odločil, da bo glavno področje analize informacijski sistem. Predvsem je poudarek na strojni in programski opremi ter infrastrukturi in dokumentaciji povezani s tem.

V zadnjem delu tega poglavja (podpoglavje 5.3) pa sem za primerjavo izdelal analizo tveganj samo enega poslovnega področja in pokazal dejansko uporabnost metode. Izbral sem plačilni promet banke, kateri predstavlja precej kompleksno področje poslovanja.

5.1 Analiza tveganj informacijskega sistema banke

5.1.1 Področje analize

Področje analize je v tem primeru izbrano precej na široko, saj opazujemo celoten informacijski sistem. Glavna področja analize so tako:

1. računalniško omrežje,
2. računalniki,
3. operacijski sistemi,
4. baze podatkov,
5. programska oprema.

Poleg tega pa se upošteva s temi področji povezana infrastruktura ter dokumentacija.

5.1.2 Popis virov IT

1. računalniško omrežje
    a. komunikacijska infrastruktura,
    b. usmerjevalniki, preklopniki in druga komunikacijska oprema,
    c. požarni zid;

2. računalniki
    a. glavni računalniki IBM S/390,
    b. računalniki DEC Alpha,
    c. strežniki IBM RS/6000,
    d. strežniki Compaq,
    e. osebni računalniki,
    f. prenosni računalniki;

3. operacijski sistemi
    a. OS/390,
    b. OpenVMS,
    c. AIX,
    d. Windows 2000,
    e. Windows NT,
    f. Windows 9x,
    g. OS/2;

4. sistemi za upravljanje baz podatkov ter baze podatkov
    a. DB2,
    b. SQL Server,
    c. Access,
    d. Dbase,
    e. Excel;

5. programska oprema
    a. namenske aplikacije,
    b. komercialni paketi,
    c. odjemalski in komunikacijski programi.

5.1.3 Ocena glede zahtevane stopnje varnosti

Naslednja tabela (Tabela 16) podaja le zbirno tabelo ocen glede Z-N-R, podrobnosti pa so v prilogi.
Računalniško omrežje (priloga Tabela 19) je gotovo nepogrešljiv del prav na vseh področjih poslovanja. Posebej pomembni za poslovanje so požarni zid, ki skrbi za zaščito povezave v internet, ter usmerjevalniki in najete povezave.

Računalniki (priloga Tabela 20) nedvomno predstavljajo srce informacijskega sistema. Najpomembnejši so glavni računalniki IBM in DEC, ki so nepogrešljivi pri poslovanju, takoj za njimi pa strežniki IBM in Compaq. Pomembnost osebnih računalnikov je manjša, saj jih je okrog 4000, pa še hitro se jih da nadomestiti. Tudi prenosniki spadajo med manj pomembne računalnike.

Operacijski sistemi (priloga Tabela 21) so temelj varnosti za podatke na računalniku, zato se zahteva za operacijske sisteme na pomembnejših računalnikih visoka stopnja zaupnosti, neoporečnosti in celovitosti, na manj pomembnih pa nekoliko nižja.

Tabela 16: Skupna ocena zahtevane stopnje varnosti (Z-N-R)

Naziv vira	Opis	Ocena Z - N – R
Računalniško omrežje	Požarni zid, glavni in manjši usmerjevalniki, najete povezave, ožičenje LAN, stikala in preklopniki	Z:2-4
		N:2-4
		R:3-4
Pomembnejši računalniki	Glavni računalniki IBM in DEC, strežniki IBM in Compaq, delovne postaje in prenosniki	Z:3-4
		N:3-4
		R:3-4
Ostali računalniki	Delovne postaje in prenosniki	Z:1-4
		N:1-4
		R:0-3
Operacijski sistemi na pomembnejših računalnikih	OS/390, Open VMS, AIX, Windows 2000 Server, Windows NT 4.0 Server	Z:4
		N:4
		R:3-4
Operacijski sistemi na PC in prenosnikih	Windows 2000 Server, Windows NT 4.0 Server, Windows 9x, OS/2	Z:3
		N:3
		R:2-3
Sistemi za upravljanje baz podatkov	DB2, SQL Server	Z:4
		N:4
		R:4
Baze podatkov	Dbase, Excel, Acess	Z:3
		N:3
		R:3
Programska oprema - namenske aplikacije	Namenske aplikacije za podporo poslovanju banke	Z:2-4
		N:2-4
		R:2-4
Programska oprema – odjemalski in komunikac. programi	Odjemalski in komunikacijski programi, ki povezujejo sisteme	Z:2-4
		N:2-4
		R:1-4
Programska oprema – komercialni paketi	Komercialni paketi	Z:1-4
		N:1-4
		R:1-4

Baze podatkov (priloga Tabela 22) hranijo bolj ali manj zaupne podatke o poslovanju banke ter o njenih komitentih, zato se zahteva v glavnem zelo visoka stopnja zaupnosti, neoporečnosti in celovitosti.

Programsko opremo sem razdelil na tri dele. Za večino namenskih aplikacij (priloga Tabela 23) se zahteva visoka stopnja zaupnosti, neoporečnosti in razpoložljivosti, so pa tudi takšne, kjer to ni ravno nujno. Odjemalski in komunikacijski programi (priloga Tabela 24) so tudi zelo pomembni, saj predstavljajo most med posameznimi sistemi, ker se preko njih prenašajo zaupni podatki. Komercialni paketi (priloga Tabela 25) pa so razmeroma različne narave. Nekateri, kot so programi za kriptiranje, so nujno potrebni za nemoteno poslovanje banke, drugi pa s stališča poslovanja niso zelo pomembni.

5.1.4 Ocena ogroženosti

Glavne grožnje v računalniškem omrežju (priloga Tabela 26) so naravne nesreče, odpoved strojne opreme, prekinitve zvez, slabo delo skrbnikov, vdor preko požarnega zidu, prisluškovanje na komunikacijskih kanalih ter pomanjkljiva dokumentacija in delovni postopki. Za zmanjšanje grožnje odpovedi opreme so sklenjene vzdrževalne pogodbe, po katerih je hitro zagotovljena nadomestna naprava. Za zaščito omrežja skrbi dokaj dober požarni zid, zato ocenjujem, da tu tveganje ni preveliko. Žal pa obstaja dokaj velika ogroženost in ranljivost komunikacijskih kanalov zunanjega omrežja glede prisluškovanja in velika ranljivost glede naravnih nesreč, ki bi prizadele omrežje.
Pri računalnikih (priloga Tabela 27) predstavljajo glavne grožnje naravne nesreče, sabotaža, slabo vzdrževanje, okvare, preobremenitev, izpad napajanja, neprimerna zmogljivost, kraja in podobno. Te grožnje imajo največji vpliv na razpoložljivost sistema. Pomembnejši računalniki so v posebej zaščitenih in klimatiziranih prostorih, zato so manj občutljivi na izpade napajanja, zunanje vplive in vandalizem. Vzdrževalne pogodbe tudi zagotavljajo manjše težave pri okvarah. Obstaja pa večja ogroženost v primeru velikih naravnih nesreč ter človeških napak. Ostali računalniki pa so bolj občutljivi glede okvar, neprimernega okolja, izpadov napajanja in podobnega. Imajo pa prednost v številu, zato okvara na manjšem računalniku ni tako usodna za poslovanje kot na večjem. Pri prenosnikih je potrebno med pomembnejšimi grožnjami omeniti še grožnjo kraje prenosnega računalnika.
Operacijski sistem OS/390 (priloga Tabela 28) zagotavlja skupaj z ustrezno strojno opremo dokaj dobro zaščito glede nepooblaščenih dostopov. Open VMS, AIX in OS/390 so tudi glede napadov zlonamerne programske opreme manj občutljivi, ker obstaja neprimerno manj virusov za te operacijske sisteme. Po drugi strani pa so operacijski sistemi družine Windows zelo dovzetni za take napade, pa tudi varnost je pri teh sistemih nekoliko manjša. Še posebej neprimerni za bančno okolje pa so operacijski sistemi Windows 9x, ker imajo vgrajenih zelo malo mehanizmov, ki bi preprečevali vdore in zlorabe.
Sistemi za upravljanje baz (priloga Tabela 29) so veliko manj ogroženi kot navadne preglednice ali sistemi, ki temeljijo predvsem na datotekah.
Pri namenskih aplikacijah (priloga Tabela 30) obstaja največja ogroženost zaradi skritih napak v aplikacijah, velika ogroženost je tudi zaradi zlonamerne programske

opreme, obstaja ogroženost zaradi vdorov pri internetnih aplikacijah in ogroženost aplikacij napisanih za operacijski sistem DOS.
Pri odjemalskih in komunikacijskih programih (priloga Tabela 31) so največja grožnja napake v programih. Pri Microsoftovih produktih obstaja večja ogroženost tudi zaradi delovanja zlonamerne programske opreme, ki še posebej rada izkorišča varnostne luknje v teh produktih. Komercialni paketi pa, razen paketov Microsoft Office, ne predstavljajo velike ogroženosti (priloga Tabela 32).

Tabela 17: Skupna ocena ogroženosti

Naziv vira	Grožnje	Ocena ogroženosti
Računalniško omrežje	Naravne nesreče, odpoved opreme, slabo delo skrbnikov, prekinitve zvez, vdori, prisluškovanja …	Z:2-7
		N:1-6
		R:1-6
Pomembnejši računalniki	Naravne nesreče, sabotaža, slabo vzdrževanje, okvare ….	Z:1-3
		N:1-5
		R:3-6
Ostali računalniki	Okvare, odpoved diska, neprimerna zmogljivost, slabo ravnanje z računalnikom, izpad napajanja, kraja …	Z:2-5
		N:2-5
		R:4-6
Operacijski sistemi na pomembnejših računalnikih	Slaba administracija, nepooblaščen dostop, sabotaža	Z:2-5
		N:2-5
		R:2-5
Operacijski sistemi na PC in prenosnikih	Napad zlonamerne programske opreme, nepooblaščen dostop …	Z:4-6
		N:4-6
		R:3-4
SUBP in baze podatkov	Nepooblaščen dostop do podatkov	Z:4
		N:4
		R:3
Dbase, Excel, Acess	Nepooblaščen dostop do podatkov, napad virusov	Z:4-6
		N:4-6
		R:3-4
Programska oprema - namenske aplikacije	Programske napake v aplikacijah, izpad baz in računalnikov, vdor v aplikacije, napad zlonamerne programske opreme …	Z:1-5
		N:1-5
		R:2-5
Programska oprema – odjemalski in komunikac. programi	Napake v programih, zlonamerna programska oprema	Z:1-6
		N:1-5
		R:3-6
Programska oprema – komercialni paketi	Napake v programih, napadi na šifrirne sisteme, zlonamerna programska oprema	Z:2-5
		N:2-5
		R:1-5

5.1.5 Ocena tveganja v IT banke

V zadnjem koraku analize tveganja pridemo do želenih rezultatov, povzetek je zbran v naslednji tabeli (Tabela 18), podrobnosti pa so v prilogi (Tabela 33 - Tabela 39):

Tabela 18: Skupna ocena tveganj

Vir	Grožnje	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Računalniško omrežje	Naravne nesreče, odpoved opreme, slabo delo skrbnikov, prekinitve zvez, vdori, prisluškovanja	Z:2-7	Z:2-4	Z:2-9
		N:1-6	N:2-4	N:2-8
		R:1-6	R:3-4	R:2-8
Pomembnejši računalniki	Naravne nesreče, sabotaža, slabo vzdrževanje, okvare …	Z:1-3	Z:3-4	Z:3-5
		N:1-5	N:3-4	N:3-7
		R:3-6	R:3-4	R:5-8
Ostali računalniki	Okvare, odpoved diska, neprimerna zmogljivost, slabo ravnanje z računalnikom, izpad napajanja, kraja …	Z:2-5	Z:1-4	Z:2-7
		N:2-5	N:1-4	N:2-7
		R:4-6	R:0-3	R:3-7
Oper. sistemi na glavnih računalnikih	Slaba administracija, nepooblaščen dostop, sabotaža	Z:2-5	Z:4	Z:4-7
		N:2-5	N:4	N:4-7
		R:2-5	R:3-4	R:4-7
Operacijski sistemi na PC in prenosnikih	Napad zlonamerne programske opreme, nepooblaščen dostop …	Z:4-6	Z:3	Z:5-7
		N:4-6	N:3	N:5-7
		R:3-4	R:2-3	R:4-7
SUBP in baze podatkov	Nepooblaščen dostop do podatkov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
Dbase, Excel, Acess	Nepooblaščen dostop do podatkov, napad virusov	Z:4-6	Z:3	Z:5-7
		N:4-6	N:3	N:5-7
		R:3-4	R:3	R:4-7
Progr. oprema - namenske aplikacije	Programske napake v aplikacijah, izpad baz in računalnikov, vdor v aplikacije, napad zlonamerne programske opreme	Z:1-5	Z:2-4	Z:2-7
		N:1-5	N:2-4	N:2-7
		R:2-5	R:2-4	R:2-7
Progr. oprema – odjemalski in komun. programi	Napake v programih, zlonamerna programska oprema	Z:1-6	Z:2-4	Z:3-7
		N:1-5	N:2-4	N:3-7
		R:3-6	R:1-4	R:3-7
Progr. oprema – komercialni paketi	Napake v programih, napadi na šifrirne sisteme, zlonamerna programska oprema	Z:2-5	Z:1-4	Z:2-6
		N:2-5	N:1-4	N:2-6
		R:1-5	R:1-4	R:3-6

Analiza najde kar nekaj tveganj, med katerimi izstopajo:

a. <u>Pri računalniškem omrežju</u>
   - **9**: zelo visoko tveganje za komunikacijske kanale glede zaupnosti (možnost prisluškovanja);
   - **8**: visoko tveganje za komunikacijske kanale glede zaupnosti in neoporečnosti podatkov, ki se prenašajo (možnost prestrezanja in ponarejanja);
   - **8**: visoko tveganje zaradi razpoložljivosti požarnega zidu in glavnih usmerjevalnikov v primeru večje nesreče (na primer potres);
   - **7**: tveganje glede zaupnosti in neoporečnosti zaradi vdora v omrežje skozi požarni zid;
   - **7**: tveganje glede razpoložljivosti pri odpovedi strojne opreme požarnega zidu;

- **7**: tveganje glede razpoložljivosti povezave v primeru prekinitev komunikacijskih kanalov.

b. Pri računalnikih:
   - **8**: visoko tveganje zaradi razpoložljivosti v primeru naravnih nesreč pri glavnih računalnikih;
   - **8**: visoko tveganje zaradi razpoložljivosti pri človeških napakah pri glavnih računalnikih;
   - **7**: tveganje glede razpoložljivosti v primeru sabotaže pri glavnih računalnikih;
   - **7**: tveganje glede razpoložljivosti, če je strežnik premalo zmogljiv;
   - **7**: tveganje v primeru naravnih nesreč glede razpoložljivosti strežnikov;
   - **7**: tveganje glede zaupnosti in neoporečnosti podatkov pri kraji pomembnejše delovne postaje ali prenosne delovne postaje;
   - **7**: tveganje glede razpoložljivosti pomembnejših delovnih postaj v primeru prekinitve napajanja;
   - **7**: tveganje glede razpoložljivosti pomembnejših delovnih postaj zaradi slabega ravnanja uporabnika z računalnikom.

c. Pri operacijskih sistemih:
   - **7**: tveganje glede zaupnosti, neoporečnosti in celovitosti pri vseh operacijskih sistemih zaradi slabe administracije;
   - **7**: tveganje glede zaupnosti, neoporečnosti in celovitosti pri vseh operacijskih sistemih zaradi sabotaže;
   - **7**: tveganje glede zaupnosti in neoporečnosti pri operacijskih sistemih Windows 9x zaradi nepooblaščenega dostopa.

d. Pri sistemih za upravljanje baz podatkov in bazah podatkov:
   - **7**: tveganje glede zaupnosti in neoporečnosti podatkov v Dbase in Excel zaradi možnosti nepooblaščenega dostopa.

e. Pri programski opremi:
   1. Namenske aplikacije
      - **7**: tveganje glede zaupnosti, neoporečnosti in razpoložljivosti zaradi napak v aplikacijah;
      - **7**: tveganje glede zaupnosti in neoporečnosti zaradi nepooblaščenega dostopa v nekatere pomembnejše aplikacije, ki temeljijo na Dbase in Excel-u;
      - **7**: tveganje glede razpoložljivosti internetnih aplikacij v primeru napada odklonitve storitve na spletni portal.
   2. Odjemalski in komunikacijski programi

- **7**: tveganje glede zaupnosti in neoporečnosti v primeru napada zlonamerne programske opreme pri programu Microsoft Internet Explorer;
- **7**: tveganje glede zaupnosti in razpoložljivosti v primeru napada zlonamerne programske opreme na strežnik za elektronsko pošto Microsoft Exchange.

3. Komercialni paketi
   - programi niso tako pomembni, da bi predstavljali visoko tveganje ali pa so grožnje premajhne, da bi prišlo do visokega tveganja

5.2 Nujni ter priporočljivi ukrepi

***9**: Zelo visoko tveganje za komunikacijske kanale glede zaupnosti zaradi možnosti prisluškovanja.*

Analiza je pokazala zelo veliko tveganje glede zaupnosti podatkov, ki se prenašajo preko zunanjega računalniškega omrežja. Ker je omrežje zelo prostrano, je možnosti, kjer bi lahko napadalec prisluškoval, veliko. Zato bo treba nujno ukrepati na enega od dveh načinov:

- Šifriranje podatkov na prenosni liniji.
  Šifriranje je možno izvesti s pomočjo usmerjevalnikov, od enega usmerjevalnika do drugega, šifriranje poteka na nižjih nivojih TCP/IP protokola, pri tem pa se šifrira ves promet.
- Šifriranje podatkov na aplikativnem nivoju.
  Za šifriranje je lahko poskrbljeno v poslovnih aplikacijah, šifriranje poteka na aplikativnem nivoju. Pri tem ni nujno, da se šifrirajo vsi podatki, lahko se le tisti, katere je potrebno zaščititi.

Drugi način je boljši od prvega, ker rešuje probleme prisluškovanja tudi na lokalnem omrežju, čeprav si je mogoče tudi v okviru lokalnega omrežja pomagati s strojnimi rešitvami, kot so mrežne kartice, ki podpirajo šifriranje. Pomanjkljivost drugega načina pa so kar precejšnje spremembe v vseh aplikacijah, ki se ukvarjajo z zaupnimi podatki.

***8**: Visoko tveganje za komunikacijske kanale glede zaupnosti in neoporečnosti podatkov, ki se prenašajo, zaradi možnosti prestrezanja in ponarejanja.*

Ker so podatki, ki se pošiljajo po zunanjemu omrežju tudi finančne narave, so zelo zanimivi za potencialne napadalce, ki bi jih lahko zlorabili. Uporaba kriptografskih metod za prenos po komunikacijskem kanalu bi avtomatsko rešila tudi problem neoporečnosti podatkov. Kriptiranje je sicer že zagotovljeno na področju plačilnega prometa na aplikativnem nivoju, drugod pa zaenkrat še ne.

***8**: Visoko tveganje zaradi razpoložljivosti požarnega zidu in glavnih usmerjevalnikov v primeru večje nesreče (na primer potres).*

7: Tveganje glede razpoložljivosti pri odpovedi strojne opreme požarnega zidu.

Problem razpoložljivosti požarnega zidu v primeru velikih naravnih nesreč bi najbolje rešila rezervna lokacija, ki bi se avtomatično vključila v primeru izpada glavne lokacije. Taka rešitev bi pomagala izboljšati razpoložljivosti tudi v primeru okvare strojne opreme na požarnem zidu.

7: Tveganje glede zaupnosti in neoporečnosti zaradi vdora v omrežje skozi požarni zid.

Zaradi velikega tveganja je potreben stalen in učinkovit nadzor nad dogajanjem v omrežju in na požarnem zidu. Opremo in znanje je potrebno neprestano nadgrajevati ter se tako preventivno pripravljati, da ne bi prišlo do vdora. Preveriti in dopolniti je potrebno tudi vse postopke, ki pridejo v poštev v primeru odkritja vdora.

7: Tveganje glede razpoložljivosti povezave v primeru prekinitev komunikacijskih kanalov.

Večje tveganje, ki se pojavi v primeru prekinitev komunikacijskih kanalov, bi bilo možno rešiti z izborom vsaj dveh neodvisnih ponudnikov komunikacijskih storitev. Tako bi zagotovili različne poti, po katerih poteka komunikacija, in zmanjšali nevarnost hkratne prekinitve glavne in rezervne povezave (primer rešitve: glavni komunikacijski vodi najeti pri Telekomu, rezervni pa pri Elesu).

***8**: Visoko tveganje glede razpoložljivosti v primeru naravnih nesreč pri glavnih računalnikih.*

7: Tveganje v primeru naravnih nesreč glede razpoložljivosti strežnikov.

Večji potres bi lahko popolnoma onemogočil poslovanje banke, poleg tega pa še poslovanje drugih bank, ki so povezane z NLB. Rezervna lokacija, ki jo ima banka v Ljubljani, bi bila v primeru take nesreče popolnoma nekoristna, saj bi bila ravno tako porušena. Zato bi bilo potrebno razmisliti o rezervni lokaciji, ki bi bila več kot 50 km oddaljena od glavne, saj bi s tem zelo zmanjšali tveganje velikih naravnih nesreč in zagotovili dokaj neprizadeto poslovanje. Obstoječa rezervna lokacija je hladna (glej poglavje Razpoložljivost), zato bi tudi prenos vseh obdelav in vzpostavitev vseh potrebnih procesov trajal precej dolgo. Z varnostnega in poslovnega stališča bi bila veliko boljša rešitev topla ali pa celo vroča rezervna lokacija, saj bi omogočila hiter prenos informacijske podpore poslovanju v center, ki ni ogrožen.

***8**: Visoko tveganje glede razpoložljivosti pri človeških napakah pri glavnih računalnikih.*

Človeške napake so večkrat vzrok za prekinitve delovanja pri računalnikih, so pa še posebej problematične zato, ker jih ni možno vselej vnaprej predvideti in se zato nanje ne moremo pripraviti. Včasih se da zmanjšati število napak že s tem, da imajo zaposleni dovolj časa, da lahko v miru opravljajo svoje delo in da niso podvrženi zunanjim vplivom, ki bi zmanjševali njihovo zbranost. Tveganja bi zmanjšale tudi dodatne kontrole, ki bi poskrbele, da bi prihajalo do napak redkeje (na primer bolj strog nadzor). Potrebno bi bilo tudi pregledati, dopolniti ali na novo napisati navodila za delo rezervnih skrbnikov v primeru odsotnosti glavnih skrbnikov sistemov.

7: Tveganje glede razpoložljivosti v primeru sabotaže pri glavnih računalnikih.

7: Tveganje glede zaupnosti, neoporečnosti in celovitosti pri vseh operacijskih sistemih zaradi sabotaže.

Sabotaža predstavlja svojevrsten problem v organizaciji. Dobra zaščita pred njo so zadovoljni zaposleni, ki jim ni v interesu takšno dejanje, zato je potrebno poskrbeti za ustrezno nagrajevanje dela in ustrezne pogoje dela zaposlenih. Na zelo pomembnih področjih, kot so glavni računalniki, je treba poskrbeti za preizkušene kadre, ki jih dobro poznamo in jim zaupamo. Ne gre pa pozabiti na pomen ustreznega nadzora dela skrbnikov sistemov.

7: Tveganje glede razpoložljivost, če je strežnik premalo zmogljiv.

Neprestani nadzor nad delovanjem strežnika zagotavlja pravočasno ugotavljanje ozkih grl glede zmogljivosti in razpoložljivosti strežnikov. Potrebno je zagotoviti alarme, ki javljajo zmanjšanje in pomanjkanje virov na strežniku in avtomatsko pošiljanje obvestil skrbnikom, da se pravočasno zagotovijo močnejši strežniki.

7: Tveganje glede zaupnosti in neoporečnosti podatkov zaradi kraje pomembnejše delovne postaje ali prenosne delovne postaje.

Medtem ko ne obstaja velika verjetnost za krajo delovne postaje, pa obstaja kar precejšnja verjetnost kraje prenosnika. Zaradi tega bi bilo potrebno na vse prenosnike, ki so dovolj sposobni, namestiti operacijski sistem Windows 2000 ali Windows XP ter vključiti kriptiranje podatkov, kar vsebuje že operacijski sistem sam. Manj zmogljivi prenosniki, ki imajo nameščen OS Windows 9x, pa ne bi smeli vsebovati občutljivih podatkov, v kolikor na njih ni nameščena programska oprema za kriptiranje.

7: Tveganje glede razpoložljivosti pomembnejših delovnih postaj v primeru prekinitve napajanja.

Za vse pomembnejše postaje, ki še niso priključene na neprekinjeno napajanje, je treba zagotoviti enote za neprekinjeno napajanje (UPS). Poleg tega je potrebno zagotoviti rezervno napajanje tudi za vso morebitno pomožno opremo, ki je prav tako potrebna za neprekinjen delovni proces (tiskalniki, optični bralniki …).

7: Tveganje glede razpoložljivosti pomembnejših delovnih postaj zaradi slabega ravnanja uporabnika z računalnikom.

Uporabnike je potrebno neprestano izobraževati in opozarjati na pomen in posledice ravnanja z računalniško opremo. Malomarno delo ima lahko za posledico prekinjen delovni proces (npr. prevrnjena skodelica s kavo lahko v najslabšem primeru pokvari prenosni računalnik).

7: Tveganje glede zaupnosti, neoporečnosti in celovitosti pri vseh operacijskih sistemih zaradi slabe administracije.

Slaba administracija lahko izniči vse napore in mehanizme, ki so namenjeni za zaščito informacij. Zato je potrebno vzpostaviti nadzor nad delom administratorjev računalnikov ter vzpodbujati kvalitetno delo. Prav tako pa je treba vzpodbujati izobraževanje in slediti novostim pri razvoju na tem področju.

7: Tveganje glede zaupnosti in neoporečnosti pri operacijskih sistemih Windows 9x zaradi nepooblaščenega dostopa.

Na vseh računalnikih, ki še imajo nameščen OS Windows 9x, je potrebno takoj zamenjati operacijski sistem, ker le-ta ni varen in tako ni primeren za poslovno rabo. Če je računalnik preslab, da bi bilo mogoče na njega namestiti OS Windows 2000 ali XP, ga je potrebno nadgraditi, ali pa zamenjati, če nadgradnja ne pride v poštev.

7: Tveganje glede zaupnosti in neoporečnosti podatkov v Dbase in Excel-u zaradi možnosti nepooblaščenega dostopa.

7: Tveganje glede zaupnosti in neoporečnosti zaradi nepooblaščenega dostopa v nekatere pomembnejše aplikacije, ki temeljijo na Dbase in Excel-u.

Podatki in aplikacije, ki temeljijo na Dbase ali Excel-u niso dovolj varni, da bi zadoščali kriterijem dobre varnosti, zato je treba razmisliti o prehodu na bolj varno bazo podatkov. Nekatere varnostne mehanizme, s katerimi lahko zaščitimo podatke v takšnih bazah, lahko sicer zagotovijo operacijski sistemi, vendar pa to ni vedno dovolj. Razmisliti je potrebno tudi o prenosu aplikacij iz okolja DOS na sodobnejša okolja.

7: Tveganje glede zaupnosti, neoporečnosti in razpoložljivosti zaradi napak v aplikacijah.

Aplikacije predstavljajo velik vir napak, predvsem zato, ker so premalo testirane. Zato je treba več časa posvetiti testiranju in odpravljanju napak in zadostiti vsem kriterijem po varnosti in zahtevani funkcionalnosti. Nobena aplikacija ne sme v produkcijsko okolje, dokler niso končani vsi testi in ni ocenjeno, da je aplikacija primerna za delo. Sedanja praksa se ne drži vedno tega načela.

7: Tveganje glede razpoložljivosti internetnih aplikacij v primeru napada odklonitve storitve na spletni portal.

Tak napad bi pomenil zmanjšanje razpoložljivost ali celo odpoved strežbe spletnih strežnikov, ki so namenjeni za opravljanje elektronskega bančništva preko interneta. Nekoliko bi se lahko pred tem zavarovali z dovolj zmogljivimi strežniki, ki bi bili sposobni odgovarjati na veliko število zahtev in bi bili tako odporni proti manjšim napadom. V primeru dobro organiziranega napada z zelo velikim številom hkratnih napadalcev pa se veliko preventivnega ne da storiti.

7: Tveganje glede zaupnosti in neoporečnosti v primeru napada zlonamerne programske opreme pri programu Microsoft Internet Explorer.

7: Tveganje glede zaupnosti in razpoložljivosti v primeru napada zlonamerne programske opreme na strežnik za elektronsko pošto Microsoft Exchange.

Spletni odjemalci so še posebej občutljivi za napade zlonamerne programske opreme, saj je veliko strani na internetu okuženih z virusi, trojanskimi konji in internetnimi črvi. Microsoftova programska oprema je zaradi želje po razvajanju uporabnikov z vsemi mogočimi dodatki, ki naj bi jim olajšali delo, še posebej oprta in premalo zaščitena, zato je na požarnem zidu onemogočen prenos datotek, ki vsebujejo izvršljivo kodo, poleg tega pa se protivirusno preverja promet. Največkrat pa pride do okužbe preko elektronske pošte, kjer se uporabniki navadno okužijo tako, da odprejo pripone, ki prihajajo skupaj z elektronsko pošto. Zato je potrebno, da imajo uporabniki izključeno možnost avtomatskega predogleda in odpiranja pripon ter da se vsa prihajajoča in odhajajoča pošta protivirusno pregleduje tudi na poštnem strežniku in po potrebi zadrži. To je sicer že stalna praksa na banki, vendar pa bi bilo mogoče kaj več storiti pri sprotnem obveščanju uporabnikov s kratkimi in jedrnatimi opozorili o nekaterih novih nevarnih virusih, na primer, kako lahko pride do okužbe in kako ukrepati v primeru, če je do nje že prišlo. Potrebno bi bilo uvesti mehanizem, ki bi vsilil redno varnostno kopiranje uporabniških podatkov na strežnik, saj bi to omogočilo lažje in hitrejše okrevanje v primeru katastrofalnega napada virusov, ki bi zbrisal vse podatke na računalnikih. Na strežnikih bi bilo mogoče uvesti tudi dvojno filtriranje prometa z dvema neodvisnima programoma za zaščito pred virusi.

5.3 Analiza tveganj in ukrepi pri plačilnem prometu

Plačilni promet v banki predstavlja enega od širših in bolj zapletenih področij poslovanja. Sestavljajo ga tudi sistemi in omrežja, ki so izven banke, kot je BSNET - omrežje za plačilni promet v domovini ter S.W.I.F.T. - svetovno bančno omrežje. Poleg tega pa zajema tudi sisteme za elektronsko poslovanje, kot so Klik, Proklik, Proklik^{+} in Moba ter Teledom. V plačilni promet je vpletenih več deset računalnikov, vse od glavnih računalnikov, več različnih strežnikov (tako glede proizvajalca kot tudi glede namena) vse do osebnih računalnikov. Področje je dovolj široko, da bi ga bilo mogoče razbiti na več podpodročij, vendar pa moj namen ni bil poglabljanje v takšne podrobnosti. Želel sem izdelati grobo analizo tveganj celotnega plačilnega prometa in prikazati uporabnost metode na določenemu poslovnemu področju.

Pri ocenjevanju je treba upoštevati:

- vso strojno opremo (glavne računalnike, strežnike, osebne računalnike, komunikacijske poti, zunanja omrežja, opremo za šifriranje in drugo);
- programsko opremo (od sistemske programske opreme preko komunikacijskih programov do namenskih aplikacij in pomožnih programov za šifriranje in digitalno podpisovanje);
- navodila za delo.

Podrobnosti analize so podane v prilogi. Tabela (Tabela 40) vsebuje spisek in oceno virov plačilnega prometa glede zahtevane stopnje varnosti. V naslednji tabeli (Tabela 41) je ocenjena ogroženost posameznih virov glede na nekatere najbolj značilne

grožnje, ki se pojavljajo v zvezi s temi viri. Zadnja tabela v prilogi (Tabela 42) pa vsebuje ocene tveganj za plačilni promet.

Izrazito velikih tveganj na tem področju ni najti, je pa nekaj pomembnih tveganj:

- 7: *Tveganje glede zaupnosti, neoporečnosti in razpoložljivosti zaradi nedovoljenega fizičnega dostopa do računalnika.*

  Razmisliti bi bilo potrebno o dodatnih fizičnih zaščitah osebnih računalnikov, ki so namenjeni plačilnemu prometu.

- 7: *Tveganje glede razpoložljivosti komunikacijskih povezav zaradi prekinitve.*

  Komunikacije bi lahko potekale preko dveh neodvisnih poti in ne da jih ima v rokah le en ponudnik.

- 7: *Tveganje glede nerazpoložljivosti sistemov Bancs in Globus zaradi nedostopnosti Registra komitentov.*

  Pri večih zaporedno povezanih sistemih vedno nastopi nevarnost, da celotna veriga ne bo delovala zaradi izpada enega člena. Zato je treba najti alternativno pot ali pa okrepiti najšibkejši člen, v tem primeru dostop do Registra komitentov.

- 7: *Tveganje glede zaupnosti, neoporečnosti in razpoložljivosti zaradi vdora preko interneta*.

  Podatki, ki se pošiljajo za namen plačilnega prometa, so dokaj dobro zavarovani, saj so šifrirani s solidnim kriptirnim sistemom. Še vedno pa obstaja možnost vdora preko stranskih vrat, na primer preko drugih sistemov, ki so povezani s plačilnim prometom, ki pa ne vsebujejo šifriranih podatkov. Rešitev bi bila šifriranje vseh zaupnih podatkov v informacijskem sistemu.

- 7: *Zloraba opreme za šifriranje.*

  Opremo, potrebno za šifriranje podatkov, je potrebno v primeru, da ni v posebej varovanih prostorih, zaščititi. To pomeni dosledno shranjevanje pametnih kartic, ki vsebujejo digitalni certifikat, v zaklenjene ognjevarne omare. S tem to opremo zavarujemo pred krajo, uničenjem ali poškodbami.

- 7: *Nerazpoložljivost sistemov zaradi nepopolnih operaterskih in uporabniških navodil.*

  Nepopolna ali neažurirana operaterska ali uporabniška navodila so večkrat kriva za nerazpoložljivost sistemov, še posebej, če pride do nepričakovanih težav pri delovanju. Zato je potrebno poskrbeti za vestno dopolnjevanje in spreminjanje teh navodil ob vsaki spremembi strojne in programske opreme ali delovnih postopkov.

6 SKLEP

Na koncu lahko zaključim, da sem dosegel v uvodu zastavljene cilje in prišel do želenega rezultata. Predvsem v tretjem poglavju sem proučil večja varnostna tveganja, ki se pojavljajo pri informacijski tehnologiji bančnega poslovanja ter predstavil in proučil varnostne tehnologije, ki se pri tem uporabljajo. Banka spremlja novejše trende na varnostnem področju, pri uvajanju novosti, predvsem mislim s tem elektronsko poslovanje, pa je dovolj prožna, da skrbi za svoje konkurenčne prednosti v primerjavi z ostalimi slovenskimi bankami. Hkrati pa je pri uvajanju novosti, mogoče tudi zaradi njene velikosti, dovolj konservativna, tako da so uvedene rešitve v praksi že preizkušene v svetu. Hitro uvajanje sprememb se je v preteklosti že velikokrat pokazalo kot dvorezen meč, saj je poleg dobrot s seboj prineslo tudi nove varnostne grožnje, katere so bile pred uvedbo skrite.
V četrtem poglavju sem predstavil metodo analize tveganj, ki je ključna za ugotavljanje varnostnih tveganj. Metoda, ki se trenutno uporablja v banki, je po mojem mnenju preveč zapletena in nepraktična za uporabo, zato sem na njeni osnovi izdelal novo izboljšano metodo. Stari metodi sem odstranil nekatere nepotrebne korake, ki pravzaprav k njeni učinkovitosti in uporabnosti niso nič doprinesli, ostale korake pa spremenil in dopolnil tako, da nudi moja metoda ob enostavnejši uporabi enako funkcionalnost in daje enake rezultate.
V petem poglavju sem s pomočjo te metode ugotavljal stopnjo varnosti informacijskega sistema in prišel do določenih ugotovitev. Na podlagi teh ugotovitev sem v nadaljevanju podal predloge ukrepov, za katere sem menil, da bi bili glede na grožnje, okoliščine in ceno najbolj upravičeni. Če še enkrat na kratko povzamem, so moje ugotovitve naslednje:

- Največjo hibo glede prisluškovanja in spreminjanja podatkov na komunikacijskih kanalih, ki preti iz zunanjega omrežja, bi bilo mogoče rešiti v dokaj kratkem času z zelo dobro znanimi kriptirnimi tehnikami.

- Za identifikacijo in overjanje uporabnikov, tako komitentov, ki uporabljajo sodobne elektronske poti, kot tudi zaposlenih, je dobro poskrbljeno. Tehnike in tehnologija, ki se uporabljajo pri tem, sledijo priporočilom standardov za varnost IS (kot je BS 7799:2 ali ISO 17799:2000), pa tudi v praksi se delo dokaj dobro izvaja, kakor kažejo revizijska poročila. Načini kriptiranja, ki se uporabljajo v banki, so standardni, dobro preizkušeni v svetu in kolikor je znano, ne vsebujejo varnostnih vrzeli. Dolžine ključev, ki so trenutno v uporabi, so takšne, da bi razbijanje kriptiranih sporočil zahtevalo veliko časa in denarja, veliko več, kot pa bi bila vredna odkrita informacija. Certifikati, ki jih izdaja Agencija za certificiranje NLB, zagotavljajo še dodatno zaščito. Seveda se lahko pri elektronskem poslovanju pojavijo določene težave, vendar pa so te povezane predvsem z neupoštevanjem varnostne politike ali z nepazljivim ravnanjem uporabnikov.

- V prihodnosti se pričakuje vedno večja grožnja s strani interneta, zato je treba temu področju posvetiti največjo pozornost ter poskrbeti, da bo varovanje omrežja s požarnim zidom ostalo na sedanji dokaj visoki ravni. Poskrbeti bo potrebno za neprestano izobraževanje in seznanjanje z novimi grožnjami, da bomo kos vedno novim napadom, ki pretijo z interneta. Vendar pa samo tehnična znanja ne bodo zadostovala. Veliko več, kot je bilo storjenega do sedaj, je moč storiti pri osveščanju zaposlenih. Zaposleni v banki lahko pomagajo napadalcem že z neupoštevanjem varnostne politike ali pa nehote ogrožajo zaupnost podatkov v banki tako, da jih pošiljajo na svoj domači elektronski naslov v nekriptirani obliki. Uvesti je potrebno mehanizme, ki bodo vsilili kriptiranje vseh podatkov, ki gredo iz banke. Slaba "internetna kultura" lahko naredi banki veliko škode, tako neposredne kot tudi posredne, s kvarjenjem njenega ugleda.

- Trši oreh predstavlja razpoložljivost informacijskega sistema banke v primeru velikih naravnih nesreč. Naložbe v izgradnjo rezervnega računalniškega centra so običajno zelo velike, vendar pa opravičijo svoj strošek, saj bistveno zmanjšajo grožnjo in tveganja glede odpovedi celotnega sistema. Postavitev rezervne lokacije le nekaj kilometrov stran od glavne lokacije bi lahko imenovali slaba naložba v primeru močnejšega potresa ali velike poplave. Verjetno bi bilo vredno razmisliti o rezervni lokaciji v kakšnem večjem mestu v Sloveniji. Mogoče je razlog, da temu ni tako, bojazen pred decentralizacijo ali pa bodoče tesnejše povezovanje z močnejšo bančno-zavarovalniško skupino, ki ima v lasti precejšen delež banke.
  Sicer pa ima banka izdelan načrt okrevanja po nesreči, ki predpisuje ravnanje zaposlenih v kritičnih razmerah. Načrt se neprenehoma dopolnjuje in prenavlja, poleg tega pa se periodično preizkuša, da se preverja seznanjenost zaposlenih z načrtom ter praktično izvajanje.
  Za varnostno kopiranje podatkov v banki je dobro poskrbljeno, saj ima banka že zaradi svoje tesne povezanosti s podatki zelo vesten odnos do njih in uporablja cel niz varnostnih ukrepov, ki zagotavljajo, da se res noben podatek po pomoti ne izgubi ali spremeni. Delovni postopki in nadzorovana avtomatizirana strojna oprema zagotavljata izdelovanje varnostnih kopij, ki se tudi varno hranijo na primernih mestih. Mogoče bi bilo potrebno v zvezi s tem omeniti samo to, da bi bilo dobro poskrbeti za nek mehanizem, ki bi vsilil redno shranjevanje podatkov uporabnikov iz osebnih računalnikih na uporabniške imenike na strežnikih.

- Poleg zunanjih nevarnosti pa je treba upoštevati tudi nevarnosti, ki izvirajo s strani zaposlenih. Nadzor v banki je dokaj dober, saj se izvaja tako s strani zunanjih institucij, kot so Banka Slovenije in razne revizorske hiše, kot tudi s strani ustrezno usposobljene notranje kontrole za informacijske sisteme.

Ločevanje nalog, ki predstavlja enega od načinov kontrol, je v banki dokaj razvito že zaradi velikosti banke. Nekoliko slabše, čeprav še vedno dobro, pa je opredeljena posameznikova odgovornost, zato bi bilo potrebno preučiti in dopolniti nekatere pravilnike o delu, predvsem za administratorje sistemov, prav tako pa dobro opredeliti odgovornosti v zvezi z elektronsko pošto, dostopom do interneta in podobno.

- Strojna oprema, predvsem so tu mišljeni računalniki, je moderna in od priznanih proizvajalcev, tako da z varnostnega stališča ne predstavlja večjih tveganj glede odpovedi. Vzdrževanje je strokovno in redno, saj za opremo skrbijo ustrezno usposobljeni zaposleni in bolj znana slovenska podjetja iz tega področja.
  Politika IT banke, ki vztraja na dejstvu, da predstavlja temelj glavni računalniških sistem na preizkušeni IBM platformi, kjer teče tudi jedro programske opreme in kjer je tudi sistem za upravljanje z bazami podatkov ter večina občutljivih podatkov, se izkaže z varnostnega stališča za zelo dobro. Spreminjanje te platforme s precej cenejšo strežniško platformo z Microsoftovo opremo bi prineslo s sabo veliko tveganj, ki so pri platformi IBM bistveno manjša (na primer tveganja v zvezi z zlonamerno programsko opremo, tveganja glede zaupnosti in neoporečnosti podatkov, tveganja glede programskih napak v sistemski programski opremi …).

- Aplikacije, ki se uporabljajo v banki, so pred vstopom v produkcijsko okolje podvržene večstopenjskim strogim testom, ki zagotavljajo, da se velika večina napak odkrije in popravi že v fazi testiranja. Poleg iskanja napak imajo testi namen preveriti tudi funkcionalnost programov in ugotoviti, ali ustrezajo standardom kakovosti ter varnostnim kriterijem. Analiza tveganja je pokazala tudi določene varnostne vrzeli in posledično večja tveganja pri nekaterih aplikacijah, ki uporabljajo za osnovo nekatere starejše baze podatkov, ki ne izpolnjujejo vseh varnostnih kriterijev. Te aplikacije bodo zamenjane v bližnji prihodnosti z aplikacijami projekta Sigma ali pa bodo opuščene, v kolikor ne bodo več potrebne.
  Svojevrsten problem predstavlja programska oprema Microsoft. Zaradi vsesplošne razširjenosti in zaradi cele vrste napak in varnostnih vrzeli zahteva skoraj posebno obravnavo. Politika počasnejšega uvajanja te programske opreme, ko so na voljo ustrezni popravki, se izkaže v tem primeru za pravilno in je bistveno boljša, kot pa hitenje z uvajanjem vsake nove različice, ki pride na trg. Glede na to, da je ta oprema de facto standard, ker jo uporabljajo skoraj vse organizacije v državi, je potrebna zaradi kompatibilnosti, zato se na tem področju kaj več ne da storiti.

- Grožnjo glede zlonamerne programske opreme, ki predstavlja precejšnjo nevarnost za zaupnost, neoporečnost in razpoložljivost podatkov, banka obravnava zelo resno. Požarni zid, nadzor elektronske pošte, protivirusna

oprema na osebnih računalnikih ter redno posodabljanje protivirusne opreme so do sedaj preprečevali napade, tako da kakšne posebne škode v zvezi s tem ni bilo. Seveda pa to ni zagotovilo za prihodnost, zato je previdnost še kako na mestu. Več na tem področju bi bilo mogoče storiti v zvezi z informiranjem in opozarjanjem uporabnikov ter vzpostavitvijo dodatnih kontrol na večjih računalnikih, kjer ta problem ni tako pereč.

S tem lahko potrdim v uvodu postavljeno tezo, da je računalniški sistem Nove Ljubljanske banke razmeroma varen, res pa bi se dalo še nekaj stvari popraviti oziroma izboljšati. Varnost informacijskega sistema je zadovoljiva in mislim, da je bil v zadnjih nekaj letih storjen velik korak v pravo smer. Skupina, ki skrbi za varnost informacij v NLB ter bankah bančne skupine, se trudi slediti novejšim trendom glede varnosti in skrbi, da se varnostna politika banke oblikuje tako, da kar v največji meri minimizira varnostne grožnje. Verjetno v Sloveniji ni veliko organizacij, ki bi imele varnostno področje veliko boljše urejeno kot banka.

Na koncu lahko še rečem, da bi bil vesel, če bi kritična ocena katerega od področij vzpodbudila razmislek o pomenu varnosti v banki in obrodila konkretne sadove v izboljšavah.

7 SLOVARČEK

AES (Advanced Encryption Standard) - novejši kriptografski standard
availability – razpoložljivost
audit – pregled, revizija
audithing around the computer – revidiranje okrog računalnik, revizorska metoda
auditing through the computer – revidiranje skozi računalnik, revizorska metoda
authentication – overjanje, avtentikacija

CCITSE (Common Criteria for Information Technology Security Evaluation) – mednaroden standard za ocenjevanje varnosti informacijskih sistemov
certificate – certifikat, overjeno potrdilo
client - odjemalec
confidentiality – zaupnost
cryptography – kriptografija, tajnopisje

decryption – odšifriranje, dešifriranje
denial of service – odklonitev storitve (predvsem povezano z napadom na strežnik)
DES (Data Encryption Standard) – kriptografski standard
disaster recovery plan – načrt okrevanja po nesreči
discretionary access control - samovoljna kontrola dostopa

encryption - šifriranje

firewall – požarni zid, varnostni zid (za zaščito omrežja organizacije)

hacker – heker, oseba, ki skuša vdreti v računalnik druge osebe
handshake protocol - protokol rokovanja, postopek dogovarjanja
hoaxes – potegavščine, miselni virusi, sporočila, ki imajo za posledico škodljivo delovanje
host (computer) – gostitelj, centralni, glavni računalnik

identification – identifikacija, ugotavljanje istovetnosti
integrity – neoporečnost, celovitost
IT (information technology) – informacijska tehnologija
ITSEC (Information Technology Security Evaluation criteria) - kriterij za ocenjevanje varnosti informacijskih sistemov v Evropski uniji

key – ključ (npr. public key - javni ključ pri šifriranju)

LAN (Local Area Network) – lokalno omrežje

MAC (Message Authentication Codes) – koda za potrjevanje pravilnosti sporočila
mandatory access control – obvezna kontrola dostopa

Operating System (OS) – operacijski sistem

password - geslo
PIN (Personal Identification Number) – osebna identifikacijska številka
POS (Point Of Sale) terminal – terminali za plačevanje s plačilnimi karticami
proxy - program, ki dovoljuje ali ne dovoljuje dostop do določenih aplikacij med različnimi omrežji
RSA cryptigraphy (Rivest, Shamir, Adelman) – kriptografija z javnim ključem

security – varnost, zaščita
server – strežnik
smart card – pametna kartica (kartica s čipom)
SSL (Secure Socket Layer) – varnostni protokol v skladovnici TCP/IP protokolov

TCSEC (Trusted Computer Security Evaluation Criteria) – kriterij za ocenjevanje varnosti informacijskih sistemov v ZDA, imenovan tudi Oranžna knjiga
TLS (Transport Layer Security) – novejši varnostni protokol

virus – virus, računalniški program z zlonamernim delovanjem

WAN (Wide Area Network) – omrežje velikega dosega
WAP (Wireless Application Protocol) – komunikacijski protokol za brezžične povezave
worm – črv, računalniški program, ki se širi iz računalnika v računalnik in pri tem ne rabi nosilnega programa
WTLS (Wireless Transport Layer Security) – varnostni protokol za brezžična omrežja

8 LITERATURA

1. Alter Steven: Information Systems, A management perspective, third editon. New York: Addison-Wesley, 1999, str. 457-491
2. Brumen Boštjan, Welzer Tatjana: Modularna varnost v podatkovnih bazah. Portorož: Zbornik sedme Elektrotehniške in računalniške konference ERK'98, Zvezek B, 1998, str. 83-86
3. Caelli William, Longley Dennis, Shain Michael: Information Security Handbook, London: MacMillan, 1994. 833 str.
4. Cvjetović Srdjan: Računalniški kriminal, Sistem – priloga revije Monitor, Ljubljana: Infomediji, št. 5, maj 2001, str. 12-13
5. Eckel George, Steen William: Intranet Working: Network security. Indianapolis USA: New Riders Publishing, 1996, str. 419-438
6. Golob Izidor: Podatkovna skladišča - nevarnost zlorab. Portorož: Zbornik osme Elektrotehniške in računalniške konference ERK'99, Zvezek B, 1999, str. 93-96
7. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju, 1. natis. Ljubljana: Ekonomska fakulteta, 2001, str. 447-477
8. Guidelines for the security of information system. Paris: Organization for Economic Co-operation and Development, 1996. 49 str.
9. Gupta Uma G.: Information systems Success in the 21st Century. New Jersey: Prentice Hall, 2000, str. 327-351
10. Hvala Davor: Priprave na katastrofo. Sistem - priloga revije Monitor. Ljubljana: Infomediji, št 11, november 2002, str. 24-26
11. Jenkins Neil: Client/server Unleashed: Securing a client/server, Intranet Security, First edition. Indianapolis USA: Sams publishing, 1996, str. 483-500, 589-619
12. Jerman Blažič Borka s soavtorji: Elektronsko poslovanje na internetu. Ljubljana: Gospodarski vestnik, 2001. 188 str.
13. Kuščer Samo: O varnosti in odgovornosti. Monitor. Ljubljana:Infomediji, številka11, november 2002, str. 8
14. Laudon Kenneth C., Laudon Jane Price: Information system: A problem-solving approach, third edition. The Dryden Press, 1999, str. 432-469
15. Laudon Kenneth C.: Essentials of management information systems: organization and technology in the network enterprise, fourth edition. New Jersey: Prentice-Hall, 2001, str. 418-448
16. Oskrbovanje varovanja informacij. Revizor, letnik 12, št. 2 (februar 2001), str. 54-68
17. Pečenko Nikolaj: Virusi, PC&Mediji. Ljubljana: Infomediji, številka 02/VIII, februar 2002, str. 60-69
18. PSIST BS 7799, Kodeks varovanja informacij, slovenski standard. Ljubljana: Urad Republike Slovenije za standardizacijo in meroslovje pri Ministrstvu za znanost in tehnologijo, 1997. 135 str.
19. Slapar Damijan: Pet devetk v internetu (realnost visoke razpoložljivosti). Sistem - priloga revije Monitor. Ljubljana: Infomediji, št. 10, oktober 2002, str. 22-23
20. Šiška Arijan: (Ne)varna omrežja, Sistem - priloga revije Monitor. Ljubljana: Infomediji, št. 11, november 2002, str. 20-22
21. Šumak Bošjan: Mobilno poslovanje in WAP, Cotl' 2000, letnik 4, številka 9, poletje 2000. 8 str.
22. Vidmar Tone: Informacijsko-komunikacijski sistemi. Ljubljana: Pasadena, 2002. 823 str.
23. Vidmar Tone: Računalniška omrežja in storitve. Ljubljana: Atlantis, 1997, str. 159-180
24. Virusi in vdori, Sistem – priloga revije Monitor. Ljubljana: Infomediji, 10, maj 2000, str. 6

9 VIRI

1. An introduction to cryptography. [URL:http://download.nai.com/products/media/pgp/support/pgp/pgp71_win32/introtocrypto.pdf], Network Associates, 12. 9. 2002
2. Ant Allan: Improving Enterprise Security. [URL:http://www4.gartner.com/DisplayDocument?id=352376&acsFlg=accessBought], Gartner, 1. 2. 2002
3. British standard. BS 7799-2:1999, Information security management. London : BSI = British Standards Institution, cop., 1999. 44 str.
4. Cavin Stan: An introduction to Secure Sockets Layer (SSL). [URL:http://www.eecs.umich.edu/~aprakash/585/html/ssl-cavin-2000.ppt], EECS, 2000
5. Computer viruses demistyfied. [URL:http://www.sophos.com/sophos/docs/eng/refguide/viru_ben.pdf], Sophos Plc, 2001
6. Distributed.net completes rc5-64 project. [URL:http://www.distributed.net/pressroom/news-20020926.html], 9. 10. 2002
7. Firewalls: a technical overview. [URL:http://www.boran.com/security/it12-firewall.html], 1.9. 2002
8. Five keys to successfully protecting your E-mail. [URL:http://www.issa.org/PDF/FiveKeysGuide.pdf], TenFour US, 20. 4. 2002
9. Hua Shu: Database Security. [URL: http://www.cs.kau.se/~hua/dbsec.pdf], Karlstad University, 6. 11. 2002
10. IBM AIX: First UNIX Operating System in a 64-bit Environment to Receive C2 Security Certification. [URL: http://www-1.ibm.com/servers/aix/news/c2.html], 15. 10. 2002
11. IBM DB2 Universal Database: Providing privacy and security for customer information. [URL: http://www-3.ibm.com/software/data/db2/udb/factsheets/security], 11. 11. 2002
12. IT Security Cookbook – 21 Appendix C: reference material. [URL:http://www.boran.com/security/references.html], 9. 10. 2002
13. Interni standard NLB za informacijsko zaščito. Ljubljana: NLB, 3. izdaja, 30. 4. 2001. 13 str.
14. Interni standard podatkovnega modeliranja. Ljubljana: NLB, 2. izdaja, 16. 1. 2002. 5 str.
15. Interni standard o uporabi razvojnih orodij za IBM, Compaq (DEC,AXP) in C/S platformo, Ljubljana: NLB, 3. izdaja, 6. 6. 2002. 5 str.
16. Intrusion Detection Systems (IDSs): Perspective. [URL:http://www4.gartner.com/DisplayTechOverview?id=320015&acsFlg=accessBought], Gartner Research, 4. 1. 2002
17. Javna varnostna politika overitelja – agencije za certificiranje NLB. Ljubljana: NLB, 2001. 6 str.
18. Lah Pavla: Zaščita podatkov na internetu s šifriranjem. [URL:http://www.sigov.si/tecaj/kripto/index.htm], 2000
19. LBNET, intranetne strani Nove Ljubljanske banke, 2002
20. Microsoft: Security: Government Issues. [URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/issues.asp], 11. 11. 2002
21. M-bančništvo NLB – uporabniški priročnik. Ljubljana: NLB, 2002
22. NIT, novice informacijske tehnologije. Ljubljana: NLB, številka 26, 13. 09. 2002. 9 str.
23. Oblak Miro: S.W.I.F.T. osnove in sistemske operacije. Ljubljana, maj 1997. 10 str.
24. Obvladovanje dostopa do sistema – Obvladovanje dostopa do računalnika, 1. izdaja. Ljubljana: NLB, 2001
25. Obvladovanje informacij v skladu s standardom BS 7799, delovno gradivo. Ljubljana, 10. 10. 2001. 53. str

26. Okrevalni načrt – Navodilo za izvajanje postopka ponovnega zagona računalniških sistemov po motnjah v delovanju ali po nesreči. Ljubljana: NLB, 9. 8. 2002. 15. str

27. Operating Systems (OS) Overview. [URL: http://www.boran.com/security/it15-os-overview.html], 20. 6. 2000

28. Organization under attack, Sonicwall. [URL: http://www.sonicwall.com/security-planning-center/Under-Attack.html], 2002

29. Pescatore John: Develop a policy for reporting Cybercrime. [URL:http://www4.gartner.com/resources/105800/105891/105891.pdf], Gartner,10. 4. 2002

30. Pandin vodnik: Kako zagotoviti, da vaše podjetje ostane 100% brez virusov. [URL:http://www.pandasoftware.com], PandaSoftware, 2002

31. Poslovnik o varovanju informacij. Ljubljana: NLB, 5. 4. 2002. 12 str.

32. Postopek varnostnega kopiranja, 2. izdaja. Ljubljana: NLB, 30. 4. 2001. 5 str.

33. Pravilnik o analizi IT tveganj. Ljubljana: NLB, 5. 4. 2002, 14. str

34. Predstavitev banke na internetu. [URL:http://www.nlb.si], 2002

35. Predpis zaščite informacij v direkciji za informatiko, 2. izdaja. Ljubljana: NLB, 2001

36. Priporočila za strežniško infrastrukturo bank bančne skupine NLB, 1.izdaja. Ljubljana: NLB, 11. 9. 2000. 16 str.

37. Ranum J. Marcus: Thinking about firewals. [URL:http://www.mirrors.wiretapped.net/security/info/papers/firewalls/ranum-thinking-about-fw.pdf], 11. 11. 2002

38. Saarinen Markku-Juhani: Attacks against the WAP WTLS protocol. [URL:http://www.cc.jyu.fi/~mjos/wtls.pdp], Finska: University of Jyväskylä, 10. 4. 2002

39. Sami Jormalainen, Jouni Laine: Security in the WTLS. [URL:http://www.hut.fi/~jtlaine2/wtls], Helsinki: University of Technology, 10. 1. 2000

40. S/390 Parallel Enterprise Server and OS/390 Reference guide. [URL: http://www-1.ibm.com/servers/eserver/zseries/library/refguides/pdf/g3263070.pdf], IBM, maj 200

41. Smith Rick: Authentication. [URL:http://www.infosecuritymag.com/articles/august00/cover.shtml], Information Security Magazine, avgust 2000

42. Stiennon Richard, Malik William: Egghead Cracked: Companies Still Not Adequately Protecting Key Assets. [URL:http://www4.gartner.com/DisplayDocument?id=318684&acsFlg=accessBought], Gartner, 27. 12. 2000

43. Strengthening AIX Security: A System-Hardening Approach. [URL:http://www-1.ibm.com/servers/aix/whitepapers/aix_security.pdf], IBM, marec 2002

44. Študija za postavitev “giro” klirinškega sistema plačil malih vrednosti. Ljubljana: Banka Slovenije, 1997. 19 str.

45. Tehnološki standard za ugotavljanje revizijske sledi v informacijskih (pod)sistemih. Ljubljana: NLB, 1. izdaja, 26. 11. 2001

46. Wheatman Vic, Malik William: Security, Privacy and Risk Management: 2002 and Beyond. [URL:http://www4.gartner.com/DisplayDocument?id=351156&acsFlg=accessBought], Gartner, 2. 1. 2002

47. Wiggins Dion: Hong Kong’s Multiapplication Smart ID Card, [URL:http://www4.gartner.com/DisplayDocument?id=352895&acsFlg=accessBought], Gartner, 15. 2. 2002

48. ZEPEP, Zakon o elektronskem poslovanju in elektronskem podpisu. Ljubljana, 13. 6. 2000

49. Zdravkovič Gordan: Security model & DB security. [URL:http://www.hig.se/~gzc/security/sec_lecture6.ppt], 6. 11. 2002

1 PRILOGA – INFORMACIJSKI SISTEM BANKE

1.1 Ocena virov glede zahtevane stopnje varnosti (Z-N-R)

1.1.1 Računalniško omrežje

Tabela 19: Ocena glede zahtevane stopnje varnosti - računalniško omrežje

Naziv vira	Opis	Ocena Z - N – R
Požarni zid	Požarni zid banke	Z:4
		N:4
		R:4
Glavni usmerjevalniki	Usmerjevalniki na centrali in na večjih enotah	Z:4
		N:4
		R:4
Manjši usmerjevalniki	Usmerjevalniki na manjših enotah	Z:4
		N:4
		R:3
Komunikacijski kanali	Najete povezave med centralo ter podružničnimi bankami ter med poslovalnicami	Z:4
		N:4
		R:4
Stikala in preklopniki	Stikala in preklopniki po bankah	Z:2
		N:2
		R:3
Notranje ožičenje	Ožičenje v lokalnem omrežju	Z:2
		N:2
		R:3

1.1.2 Računalniki

Tabela 20: Ocena glede zahtevane stopnje varnosti - računalniki

Naziv vira	Opis	Ocena Z - N – R
IBM S/390	Glavni računalniki	Z:4
		N:4
		R:4
DEC Alpha	Glavni računalniki DEC	Z:4
		N:4
		R:4
IBM RS/6000	Strežniki IBM	Z:4
		N:4
		R:4
Strežniki Compaq	Strežniki, ki temeljijo na Intel platformi	Z:3-4
		N:3-4
		R:3
Delovne postaje	Osebni računalniki uporabnikov	Z:1-4
		N:1-4
		R:1-3
Prenosne delovne postaje	Prenosniki uporabnikov	Z:1-4
		N:1-4
		R:0-2

1.1.3 Operacijski sistemi

Tabela 21: Ocena glede zahtevane stopnje varnosti - operacijski sistemi

Naziv vira	Opis	Ocena Z - N – R
IBM OS/390	Operacijski sistem na glavnih računalnikih	Z:4
		N:4
		R:4
Open VMS	Operacijski sistem na DEC računalnikih	Z:4
		N:4
		R:4
IBM AIX	Operacijski sistem na IBM RS/6000 računalnikih	Z:4
		N:4
		R:3
Windows 2000 Server	Operacijski sistem na Intel strežnikih	Z:4
		N:4
		R:3
Windows NT 4.0 Server	Operacijski sistem na Intel strežnikih	Z:4
		N:4
		R:3
Windows 2000 Professional	Operacijski sistem na osebnih in prenosnih računalnikih	Z:3
		N:3
		R:3
Windows XP Professional	Operacijski sistem na osebnih in prenosnih računalnikih	Z:3
		N:3
		R:3
Windows 9x	Operacijski sistem na osebnih in prenosnih računalnikih	Z:3
		N:3
		R:2
OS/2	Operacijski sistem na osebnih računalnikih	Z:3
		N:3
		R:2

1.1.4 Sistemi za upravljanje baz podatkov ter baze podatkov

Tabela 22: Ocena glede zahtevane stopnje varnosti - baze podatkov

Naziv vira	Opis	Ocena Z - N – R
DB/2	Relacijska baza na IBM sistemih	Z:4
		N:4
		R:4
SQL Server	Relacijska baza na Intel strežnikih	Z:4
		N:4
		R:4
Access	Baza na osebnih računalnikih	Z:3
		N:3
		R:3
Dbase	Baza na osebnih računalnikih	Z:3
		N:3
		R:3
Excel	Preglednica na osebnih računalnikih	Z:3
		N:3
		R:3

1.1.5 Programska oprema

Namenske aplikacije

Tabela 23: Ocena glede zahtevane stopnje varnosti – programska oprema (namenske aplikacije)

Naziv vira	Opis	Ocena Z - N – R
Pranje	Aplikacija za preprečevanje pranja denarja	Z:4
		N:4
		R:2
Storitve	Podpora storitvam banke	Z:3
		N:3
		R:3
Register	Register komitentov	Z:4
		N:4
		R:4
MASA	Zbiranje vseh podatkov o poslovanju komitentov	Z:4
		N:4
		R:2
MUNDUS	Podpora centralnemu registru transakcijskih računov	Z:4
		N:4
		R:3
Vmesnik	Vmesnik za plačilni promet	Z:4
		N:4
		R:4
POND	Podpora odobravanju naložb in depozitov	Z:3
		N:3
		R:3
SOD_PIS	Sodobna pisarna – poslovanje brez papirja	Z:3
		N:3
		R:2
Študentski krediti	Podpora odobravanju študentskih kreditov	Z:4
		N:4
		R:2
Plačilni promet	Podpora za plačilni promet	Z:4
		N:4
		R:4
BTM 2000	Podpora kreditom in depozitom	Z:4
		N:4
		R:3
BTM Correspondence	Izpisi kreditov in depozitov	Z:4
		N:4
		R:3
EPI@BS	Podpora poslovanju z vrednostnimi papirji	Z:4
		N:4
		R:4
GLOBUS	Podpora tržnikom	Z:4
		N:4
		R:3
Imago	Zajem in optično razpoznavanje dokumentov	Z:3
		N:3
		R:2
Depozit	Podpora za depozite na bankomatu	Z:3
		N:3
		R:2
Krediti	Podpora za dolgoročne kredite občanov	Z:4
		N:4
		R:3

Tabela 23 - nadaljevanje

Pilot Excel	informacijski sistem za planiranje	Z:3
		N:3
		R:2
EOM	Izračun efektivne obrestne mere	Z:2
		N:2
		R:2
Hipotekarni krediti	Podpora za hipotekarne kredite	Z:4
		N:4
		R:3
Naročila IB	Naročila investicijskega bančništva	Z:3
		N:3
		R:2
PCTEAM	Intranetna aplikacija za podporo oddelka za osebne računalnike	Z:2
		N:2
		R:2
EIS	Elektronski informacijski sistem za direktorje	Z:3
		N:3
		R:2
LBNET	Intranetne strani banke	Z:3
		N:3
		R:2
Klik	Internetna aplikacija za podporo poslovanja s fizičnimi osebami	Z:4
		N:4
		R:4
Proklik	Internetna aplikacija za podporo poslovanja s pravnimi osebami	Z:4
		N:4
		R:4
Proklik^{+}	Internetna aplikacija za podporo poslovanja s pravnimi osebami	Z:4
		N:4
		R:4
Moba	Internetna aplikacija za podporo poslovanja s fizičnimi osebami preko mobilnega telefona	Z:4
		N:4
		R:4

Odjemalski in komunikacijski programi

Tabela 24: Ocena glede zahtevane stopnje varnosti - programska oprema (odjemalski programi)

Naziv Vira	Opis	Ocena Z - N – R
Microsoft Internet Explorer	Brskalnik za dostop do svetovnega spleta	Z:4
		N:4
		R:1-3
IBM DB/2 client	Odjemalec za bazo DB/2	Z:4
		N:4
		R:3
IBM CICS client	Odjemalec za IBM	Z:4
		N:4
		R:3
Connect Direct	Povezava DEC – IBM	Z:4
		N:4
		R:4
Microsoft Exchange	Strežnik za elektronsko pošto	Z:3
		N:3
		R:3
CLIME - client	Odjemalec aplikacije Clime	Z:4
		N:4
		R:2
Host Explorer	Simulacija terminala in odjemalec za DEC	Z:4
		N:4
		R:2
Communications Server	Odjemalec za IBM komunikacijski strežnik	Z:4
		N:4
		R:2
Microsoft SMS	Nadzorni in distribucijski program SMS strežnik	Z:2
		N:2
		R:1-2

Komercialni paketi

Tabela 25: Ocena glede zahtevane stopnje varnosti – programska oprema (komercialni paketi)

Naziv vira	Opis	Ocena Z - N – R
Microsoft Office	Pisarniški paket (Word, Excel, Power point, Outlook, Access)	Z:2-3
		N:2-3
		R:2-3
Sophos Sweep	Protivirusna zaščita	Z:4
		N:4
		R:4
Activ Card Gold	Program za uporabo čitalcev	Z:4
		N:4
		R:4
Symantec Norton Ghost	Orodje za delo z diski	Z:1
		N:1
		R:2
DISS - (Continuity Action Plann. Tool)	Orodje za načrtovanje neprekinjenega poslovanja	Z:2
		N:2
		R:2
PowerSync	Orodje za replikacijo datotek	Z:2
		N:2
		R:2

Tabela 25 – nadaljevanje

Microsoft Visio	Orodje za načrtovanje	Z:1
		N:1
		R:1
Microsoft Front Page	Orodje za izdelavo spletnih strani	Z:2
		N:2
		R:2
Microsoft Project	Orodje za organizacijo	Z:1
		N:1
		R:1
Corel Draw	Orodje za oblikovanje	Z:1
		N:1
		R:1
Adobe Acrobat	Urejevalnik	Z:1
		N:1
		R:1
PGP	Paket za kriptiranje	Z:4
		N:4
		R:4
Key for Enterprise	Kriptiranje za OS/2	Z:4
		N:4
		R:4
Adobe Photoshop 6.0	Orodje za oblikovanje	Z:1
		N:1
		R:1
Recognita Plus 5.0	Orodje za optično razpoznavanje besedil	Z:1
		N:1
		R:1
Entrust Desktop Solutions	Paket za kriptiranje	Z:4
		N:4
		R:4
IBON	Boniteta poslovanja za slovenska podjetja	Z:1
		N:1
		R:2
IPIS	Poslovni register Slovenije	Z:1
		N:1
		R:2

1.2 Ocena ogroženosti

1.2.1 Računalniško omrežje

Tabela 26: Ocena ogroženosti – računalniško omrežje

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Požarni zid	Naravne nesreče	2	Z:0	Z:2
			N:0	N:2
			R:4	R:6
Požarni zid	Vdor v omrežje preko požarnega zidu	3	Z:2	Z:5
			N:2	N:5
			R:1	R:4
Požarni zid	Slaba administracija	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Požarni zid	Pomanjkljiva delovna navodila	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Požarni zid	Odpoved strojne opreme	3	Z:0	Z:3
			N:0	N:3
			R:2	R:5
Glavni usmerjevalniki	Odpoved usmerjevalnika	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Glavni usmerjevalniki	Slabo delo skrbnikov	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Glavni usmerjevalniki	Naravne nesreče	2	Z:0	Z:2
			N:0	N:2
			R:4	R:6
Manjši usmerjevalniki	Odpoved usmerjevalnika	2	Z:1	Z:3
			N:1	N:3
			R:2	R:4
Manjši usmerjevalniki	Slaba administracija	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Komunikacijski kanali	Prekinitev zveze	3	Z:0	Z:3
			N:0	N:3
			R:2	R:5
Komunikacijski kanali	Prisluškovanje na kanalu	3	Z:4	Z:7
			N:0	N:3
			R:0	R:3
Komunikacijski kanali	Prestrezanje in spreminjanje podatkov na kanalu	2	Z:4	Z:6
			N:4	N:6
			R:2	R:4
Stikala in preklopniki	Okvara na opremi	3	Z:1	Z:4
			N:1	N:4
			R:2	R:5
Stikala in preklopniki	Slaba dokumentacija	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Notranje ožičenje	Prisluškovanje znotraj banke	1	Z:4	Z:5
			N:0	N:1
			R:0	R:1

1.2.2 Računalniki

Tabela 27: Ocena ogroženosti – računalniki

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
IBM S/390, DEC Alpha, IBM RS/6000	Namerno uničenje računalnika	1	Z:0	Z:1
			N:0	N:1
			R:2	R:3
IBM S/390, DEC Alpha, IBM RS/6000	Naravne nesreče	2	Z:0	Z:2
			N:0	N:2
			R:4	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Sabotaža	1	Z:0	Z:1
			N:0	N:1
			R:4	R:5
IBM S/390, DEC Alpha, IBM RS/6000	Okvara	2	Z:0	Z:2
			N:2	N:4
			R:2	R:4
IBM S/390, DEC Alpha, IBM RS/6000	Človeške napake	3	Z:0	Z:3
			N:2	N:5
			R:3	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Preobremenitev	1	Z:0	Z:1
			N:1	N:2
			R:3	R:4
IBM S/390, DEC Alpha, IBM RS/6000	Izpad napajanja	3	Z:0	Z:3
			N:0	N:3
			R:1	R:4
IBM S/390, DEC Alpha, IBM RS/6000	Slabo vzdrževanje	2	Z:0	Z:2
			N:2	N:4
			R:2	R:4
IBM S/390, DEC Alpha, IBM RS/6000	Slabi delovni postopki	2	Z:1	Z:3
			N:2	N:4
			R:2	R:4
Strežnik Compaq	Okvara	2	Z:0	Z:2
			N:2	N:4
			R:2	R:4
Strežnik Compaq	Neprimerna zmogljivost	3	Z:0	Z:3
			N:1	N:4
			R:3	R:6
Strežnik Compaq	Slabo vzdrževanje	2	Z:0	Z:2
			N:2	N:4
			R:2	R:4
Strežnik Compaq	Naravne nesreče	2	Z:0	Z:2
			N:0	N:2
			R:4	R:6
Strežnik Compaq	Odpoved diska	3	Z:0	Z:3
			N:1	N:4
			R:1	R:4
Strežnik Compaq	Izpad napajanja	3	Z:0	Z:3
			N:0	N:3
			R:1	R:4
Delovna postaja	Okvara	3	Z:0	Z:3
			N:1	N:4
			R:3	R:6
Delovna postaja	Odpoved diska	3	Z:0	Z:3
			N:1	N:4
			R:3	R:6

Tabela 27 - nadaljevanje

Delovna postaja	Kraja računalnika	1	Z:4	Z:5
			N:4	N:5
			R:4	R:5
Delovna postaja	Izpad napajanja	3	Z:0	Z:3
			N:0	N:3
			R:3	R:6
Delovna postaja	Neprimerna zmogljivost računalnika	2	Z:0	Z:2
			N:0	N:2
			R:3	R:5
Delovna postaja	Slabo ravnanje uporabnika z računalnikom	3	Z:0	Z:3
			N:0	N:3
			R:3	R:6
Prenosna delovna postaja	Okvara	3	Z:0	Z:3
			N:1	N:4
			R:2	R:5
Prenosna delovna postaja	Odpoved diska	3	Z:0	Z:3
			N:1	N:4
			R:2	R:5
Prenosna delovna postaja	Kraja računalnika	3	Z:2	Z:5
			N:2	N:5
			R:3	R:6
Prenosna delovna postaja	Izpad napajanja	3	Z:0	Z:3
			N:0	N:3
			R:1	R:4
Prenosna delovna postaja	Neprimerna zmogljivost računalnika	2	Z:0	Z:2
			N:0	N:2
			R:3	R:5
Prenosna delovna postaja	Slabo ravnanje uporabnika z računalnikom	3	Z:0	Z:3
			N:1	N:4
			R:3	R:6

1.2.3 Operacijski sistemi

Tabela 28: Ocena ogroženosti – operacijski sistemi

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
OS/390, Open VMS, AIX, Windows	Slaba administracija	2	Z:3	Z:5
			N:3	N:5
			R:3	R:5
OS/390, Open VMS, AIX, Windows	Sabotaža	1	Z:4	Z:5
			N:4	N:5
			R:4	R:5
OS/390	Nepooblaščen dostop	2	Z:1	Z:3
			N:1	N:3
			R:0	R:2
OS/390	Napad zlonamerne programske opreme	1	Z:1	Z:2
			N:1	N:2
			R:1	R:2
Open VMS, AIX	Nepooblaščen dostop	3	Z:1	Z:4
			N:1	N:4
			R:0	R:3
Open VMS, AIX	Napad zlonamerne programske opreme	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
Windows NT, 2000, XP, OS/2	Nepooblaščen dostop	3	Z:1	Z:4
			N:1	N:4
			R:0	R:3
Windows NT, 2000, XP, OS/2	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Windows 9x	Nepooblaščen dostop	3	Z:3	Z:6
			N:3	N:6
			R:1	R:4
Windows 9x	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4

1.2.4 Sistemi za upravljanje baz podatkov ter baze podatkov

Tabela 29: Ocena ogroženosti – baze podatkov

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
DB/2	Nepooblaščen dostop do podatkov	3	Z:1	Z:4
			N:1	N:4
			R:0	R:3
SQL Server	Nepooblaščen dostop do podatkov	3	Z:1	Z:4
			N:1	N:4
			R:0	R:3
Access	Nepooblaščen dostop do podatkov	3	Z:2	Z:5
			N:2	N:5
			R:0	R:3
Dbase	Nepooblaščen dostop do podatkov	3	Z:3	Z:6
			N:3	N:6
			R:0	R:3
Excel	Napad makro virusa	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Excel	Nepooblaščen dostop do podatkov	3	Z:3	Z:6
			N:3	N:6
			R:0	R:3

1.2.5 Programska oprema

Namenske aplikacije

Tabela 30: Ocena ogroženosti – programska oprema (namenske aplikacije)

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Vse aplikacije	Napake v aplikaciji	3	Z:2	Z:5
			N:2	N:5
			R:2	R:5
Aplikacije, odjemalci baze DB2	Izpad delovanja računalnika IBM ali baze DB2	1	Z:0	Z:1
			N:0	N:1
			R:2	R:3
Aplikacije, odjemalci baze DB2	Napad zlonamerne programske opreme	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
Aplikacije, odjemalci baze DB2	Nepooblaščen dostop v program	2	Z:2	Z:4
			N:2	N:4
			R:0	R:2
Aplikacije na osnovi SQL strežnika	Izpad delovanja SUBP SQL Server ali strežnika	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Aplikacije na osnovi SQL strežnika	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Aplikacije na osnovi SQL strežnika	Nepooblaščen dostop v program	2	Z:2	Z:4
			N:2	N:4
			R:0	R:2
DOS aplikacije in aplikacije na osnovi DBase	Napake na bazi	2	Z:1	Z:3
			N:2	N:4
			R:3	R:5
DOS aplikacije in aplikacije na osnovi DBase	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
DOS aplikacije in aplikacije na osnovi DBase	Nepooblaščen dostop v program	2	Z:3	Z:5
			N:3	N:5
			R:1	R:3
Aplikacije na osnovi Excel-a	Nepooblaščen dostop v program	2	Z:3	Z:5
			N:3	N:5
			R:0	R:2
Internetne aplikacije za interno uporabo	Izpad delovanja spletnega strežnika	1	Z:0	Z:1
			N:0	N:1
			R:2	R:3
Internetne aplikacije za interno uporabo	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Internetne aplikacije za interno uporabo	Nepooblaščen dostop v internetno aplikacijo	2	Z:2	Z:4
			N:2	N:4
			R:1	R:3
Internetne aplikacije za komitente	Izpad delovanja baze DB2	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Internetne aplikacije za komitente	Izpad delovanja računalnika IBM	1	Z:0	Z:1
			N:0	N:1
			R:1	R:2

Tabela 30 - nadaljevanje

Internetne aplikacije za komitente	Izpad spletnega strežnika	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Internetne aplikacije za komitente	Napad na spletni portal s pošiljanjem velike količine zahtev	3	Z:1	Z:4
			N:1	N:4
			R:2	R:5
Internetne aplikacije za komitente	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Internetne aplikacije za komitente	Nepooblaščen dostop v program	2	Z:1	Z:3
			N:1	N:3
			R:0	R:2

Odjemalski in komunikacijski programi

Tabela 31: Ocena ogroženosti – programska oprema (odjemalski, komunikacijski programi)

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Microsoft Internet Explorer	Napad zlonamerne programske opreme	3	Z:2	Z:5
			N:2	N:5
			R:2	R:5
Microsoft Internet Explorer	Napake v programu	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Komunikacijski programi	Nedelovanje programa	1	Z:0	Z:1
			N:0	N:1
			R:2	R:3
Komunikacijski programi	Napake v programih	2	Z:1	Z:3
			N:1	N:3
			R:2	R:4
Microsoft Exchange	Napad zlonamerne programske opreme	3	Z:3	Z:6
			N:2	N:5
			R:3	R:6

Komercialni paketi

Tabela 32: Ocena ogroženosti – programska oprema (komercialni paketi)

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Programi za kriptiranje	Napadi na kriptirne sisteme	1	Z:2	Z:3
			N:2	N:3
			R:0	R:1
Programi za kriptiranje	Napadi, ki skušajo obiti kriptirne sisteme	1	Z:2	Z:3
			N:2	N:3
			R:0	R:1
Programi za kriptiranje	Napake v programih	2	Z:1	Z:3
			N:1	N:3
			R:2	R:4
Microsoft Office	Napake v programih	2	Z:1	Z:3
			N:2	N:4
			R:2	R:4
Microsoft Office	Napadi zlonamerne programske opreme	3	Z:2	Z:5
			N:2	N:5
			R:2	R:5
Programerska in načrtovalna orodja	Napake v programih	2	Z:1	Z:3
			N:2	N:4
			R:2	R:4
Programi za oblikovanje	Napake v programih	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Pomožni programi	Napake v programih	2	Z:1	Z:3
			N:1	N:3
			R:2	R:4
Vzdrževalna orodja	Napake v programih	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
Protivirusna zaščita	Nedelovanje programa	2	Z:0	Z:2
			N:2	N:4
			R:2	R:4

1.3 Ocenjevanje tveganj

1.3.1 Računalniško omrežje

Tabela 33: Ocenjevanje tveganja – računalniško omrežje

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Požarni zid	Naravne nesreče	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:6	R:4	R:8
Požarni zid	Vdor v omrežje preko požarnega zidu	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:4	R:4	R:6
Požarni zid	Slaba administracija	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Požarni zid	Pomanjkljiva delovna navodila	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Požarni zid	Odpoved strojne opreme	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:5	R:4	R:7
Glavni usmerjevalniki	Odpoved usmerjevalnika	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
Glavni usmerjevalniki	Slabo delo skrbnikov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Glavni usmerjevalniki	Naravne nesreče	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:6	R:4	R:8
Manjši usmerjevalniki	Odpoved usmerjevalnika	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:4	R:3	R:5
Manjši usmerjevalniki	Slaba administracija	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:3	R:5
Komunikacijski kanali	Prekinitev zveze	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:5	R:4	R:7
Komunikacijski kanali	Prisluškovanje na kanalu	Z:7	Z:4	Z:9
		N:3	N:4	N:5
		R:3	R:4	R:5
Komunikacijski kanali	Prestrezanje in spreminjanje podatkov na kanalu	Z:6	Z:4	Z:8
		N:6	N:4	N:8
		R:4	R:4	R:6
Stikala in preklopniki	Okvara na opremi	Z:4	Z:2	Z:4
		N:4	N:2	N:4
		R:5	R:3	R:6
Stikala in preklopniki	Slaba dokumentacija	Z:2	Z:2	Z:2
		N:2	N:2	N:2
		R:4	R:3	R:5
Notranje ožičenje	Prisluškovanje znotraj banke	Z:5	Z:2	Z:5
		N:1	N:2	N:2
		R:1	R:3	R:2

1.3.2 Računalniki

Tabela 34: Ocenjevanje tveganja – računalniki

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
IBM S/390, DEC Alpha, IBM RS/6000	Namerno uničenje računalnika	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:3	R:4	R:5
IBM S/390, DEC Alpha, IBM RS/6000	Naravne nesreče	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:6	R:4	R:8
IBM S/390, DEC Alpha, IBM RS/6000	Sabotaža	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:5	R:4	R:7
IBM S/390, DEC Alpha, IBM RS/6000	Okvara	Z:2	Z:4	Z:4
		N:4	N:4	N:6
		R:4	R:4	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Človeške napake	Z:3	Z:4	Z:5
		N:5	N:4	N:7
		R:6	R:4	R:8
IBM S/390, DEC Alpha, IBM RS/6000	Preobremenitev	Z:1	Z:4	Z:3
		N:2	N:4	N:4
		R:4	R:4	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Izpad napajanja	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:4	R:4	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Slabo vzdrževanje	Z:2	Z:4	Z:4
		N:4	N:4	N:6
		R:4	R:4	R:6
IBM S/390, DEC Alpha, IBM RS/6000	Slabi delovni postopki	Z:3	Z:4	Z:5
		N:4	N:4	N:6
		R:4	R:4	R:6
Strežnik Compaq	Okvara	Z:2	Z:3-4	Z:3-4
		N:4	N:3-4	N:5-6
		R:4	R:3	R:5
Strežnik Compaq	Neprimerna zmogljivost	Z:3	Z:3-4	Z:4-5
		N:4	N:3-4	N:5-6
		R:6	R:3	R:7
Strežnik Compaq	Slabo vzdrževanje	Z:2	Z:3-4	Z:3-4
		N:4	N:3-4	N:5-6
		R:4	R:3	R:5
Strežnik Compaq	Naravne nesreče	Z:2	Z:3-4	Z:3-4
		N:2	N:3-4	N:3-4
		R:6	R:3	R:7
Strežnik Compaq	Odpoved diska	Z:3	Z:3-4	Z:4-5
		N:4	N:3-4	N:5-6
		R:4	R:3	R:5
Strežnik Compaq	Izpad napajanja	Z:3	Z:3-4	Z:4-5
		N:3	N:3-4	N:4-5
		R:4	R:3	R:5
Delovna postaja	Okvara	Z:3	Z:1-4	Z:2-5
		N:4	N:1-4	N:3-6
		R:5	R:1-3	R:3-6
Delovna postaja	Odpoved diska	Z:3	Z:1-4	Z:2-5
		N:4	N:1-4	N:3-6
		R:5	R:1-3	R:3-6

Tabela 34 - nadaljevanje

Delovna postaja	Kraja računalnika	Z:5	Z:1-4	Z:3-7
		N:5	N:1-4	N:3-7
		R:5	R:1-3	R:3-6
Delovna postaja	Izpad napajanja	Z:3	Z:1-4	Z:2-5
		N:3	N:1-4	N:2-5
		R:6	R:1-3	R:4-7
Delovna postaja	Neprimerna zmogljivost računalnika	Z:2	Z:1-4	Z:2-4
		N:2	N:1-4	N:2-4
		R:5	R:1-3	R:3-6
Delovna postaja	Slabo ravnanje uporabnika z računalnikom	Z:3	Z:1-4	Z:2-5
		N:3	N:1-4	N:2-5
		R:6	R:1-3	R:4-7
Prenosna delovna postaja	Okvara	Z:3	Z:1-4	Z:2-5
		N:4	N:1-4	N:3-6
		R:5	R:0-2	R:3-5
Prenosna delovna postaja	Odpoved diska	Z:3	Z:1-4	Z:2-5
		N:4	N:1-4	N:3-6
		R:5	R:0-2	R:3-5
Prenosna delovna postaja	Kraja računalnika	Z:5	Z:1-4	Z:3-7
		N:5	N:1-4	N:3-7
		R:6	R:0-2	R:3-6
Prenosna delovna postaja	Izpad napajanja	Z:3	Z:1-4	Z:2-5
		N:3	N:1-4	N:2-5
		R:4	R:0-2	R:2-4
Prenosna delovna postaja	Neprimerna zmogljivost računalnika	Z:2	Z:1-4	Z:2-4
		N:2	N:1-4	N:2-4
		R:5	R:0-2	R:3-5
Prenosna delovna postaja	Slabo ravnanje uporabnika z računalnikom	Z:3	Z:1-4	Z:2-5
		N:4	N:1-4	N:3-6
		R:6	R:0-2	R:3-6

1.3.3 Operacijski sistemi

Tabela 35: Ocenjevanje tveganja – operacijski sistemi

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
OS/390, Open VMS, AIX, Windows	Slaba administracija	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:3-4	R:6-7
OS/390, Open VMS, AIX, Windows	Sabotaža	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:3-4	R:6-7
OS/390	Nepooblaščen dostop	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:2	R:4	R:4
OS/390	Napad zlonamerne programske opreme	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:2	R:4	R:4
Open VMS, AIX	Nepooblaščen dostop	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:3-4	R:4-5
Open VMS, AIX	Napad zlonamerne programske opreme	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:3-4	R:4-5
Windows NT, 2000, XP,OS/2	Nepooblaščen dostop	Z:4	Z:3-4	Z:5-6
		N:4	N:3-4	N:5-6
		R:3	R:3-4	R:4-5
Windows NT, 2000, XP, OS/2	Napad zlonamerne programske opreme	Z:4	Z:3-4	Z:5-6
		N:4	N:3-4	N:5-6
		R:4	R:3-4	R:5-6
Windows 9x	Nepooblaščen dostop	Z:6	Z:3	Z:7
		N:6	N:3	N:7
		R:4	R:2	R:4
Windows 9x	Napad zlonamerne programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:4

1.3.4 Sistemi za upravljanje baz podatkov ter baze podatkov

Tabela 36: Ocenjevanje tveganja – baze podatkov

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
DB/2	Nepooblaščen dostop do podatkov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
SQL Server	Nepooblaščen dostop do podatkov	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
Access	Nepooblaščen dostop do podatkov	Z:5	Z:3	Z:6
		N:5	N:3	N:6
		R:3	R:3	R:4
Dbase	Nepooblaščen dostop do podatkov	Z:6	Z:3	Z:7
		N:6	N:3	N:7
		R:3	R:3	R:4
Excel	Napad makro virusa	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:3	R:5
Excel	Nepooblaščen dostop do podatkov	Z:6	Z:3	Z:7
		N:6	N:3	N:7
		R:3	R:3	R:4

1.3.5 Programska oprema

Namenske aplikacije

Tabela 37: Ocenjevanje tveganja – programska oprema (namenske aplikacije)

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Vse aplikacije	Napake v aplikaciji	Z:5	Z:2-4	Z:5-7
		N:5	N:2-4	N:5-7
		R:5	R:2-4	R:5-7
Aplikacije, odjemalci baze DB2	Izpad delovanja računalnika IBM ali baze DB2	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:3	R:4	R:5
Aplikacije, odjemalci baze DB2	Napad zlonamerne programske opreme	Z:3	Z:3-4	Z:4-5
		N:3	N:3-4	N:4-5
		R:3	R:3-4	R:4-5
Aplikacije, odjemalci baze DB2	Nepooblaščen dostop v program	Z:4	Z:3-4	Z:5-6
		N:4	N:3-4	N:5-6
		R:2	R:3-4	R:3-4
Aplikacije na osnovi SQL strežnika	Izpad delovanja SUBP SQL Server ali strežnika	Z:2	Z:3	Z:3
		N:2	N:3	N:3
		R:4	R:2	R:5
Aplikacije na osnovi SQL strežnika	Napad zlonamerne programske opreme	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:4	R:2	R:4
Aplikacije na osnovi SQL strežnika	Nepooblaščen dostop v program	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:2	R:2	R:2
DOS aplikacije in aplikacije na osnovi DBase	Napake na bazi	Z:3	Z:3-4	Z:4-5
		N:4	N:3-4	N:5-6
		R:5	R:2-3	R:5-6
DOS aplikacije in aplikacije na osnovi DBase	Napad zlonamerne programske opreme	Z:4	Z:3-4	Z:5-6
		N:4	N:3-4	N:5-6
		R:4	R:2-3	R:4-5
DOS aplikacije in aplikacije na osnovi DBase	Nepooblaščen dostop v program	Z:5	Z:3-4	Z:6-7
		N:5	N:3-4	N:6-7
		R:3	R:2-3	R:3-4
Aplikacije na osnovi Excel-a	Nepooblaščen dostop v program	Z:5	Z:2-4	Z:5-7
		N:5	N:2-4	N:5-7
		R:2	R:2-3	R:2-3
Internetne aplikacije za interno uporabo	Izpad delovanja spletnega strežnika	Z:1	Z:2-3	Z:2
		N:1	N:2-3	N:2
		R:3	R:2	R:3
Internetne aplikacije za interno uporabo	Napad zlonamerne programske opreme	Z:4	Z:2-3	Z:4-5
		N:4	N:2-3	N:4-5
		R:4	R:2	R:4
Internetne aplikacije za interno uporabo	Nepooblaščen dostop v internetno aplikacijo	Z:4	Z:2-3	Z:4-5
		N:4	N:2-3	N:4-5
		R:3	R:2	R:4
Internetne aplikacije za komitente	Izpad delovanja baze DB2	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
Internetne aplikacije za komitente	Izpad delovanja računalnika IBM	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:2	R:4	R:4

Tabela 37 - nadaljevanje

Internetne aplikacije za komitente	Izpad spletnega strežnika	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
Internetne aplikacije za komitente	Napad na spletni portal s pošiljanjem velike količine zahtev	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:5	R:4	R:7
Internetne aplikacije za komitente	Napad zlonamerne programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Internetne aplikacije za komitente	Nepooblaščen dostop v program	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:2	R:4	R:4

Odjemalski in komunikacijski programi

Tabela 38: Ocenjevanje tveganja – programska oprema (odjemalski in komun. programi)

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Microsoft Internet Explorer	Napad zlonamerne programske opreme	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:1-3	R:3-6
Microsoft Internet Explorer	Napake v programu	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:1-3	R:3-5
Komunikacijski programi	Nedelovanje programa	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:3	R:2-3	R:3-4
Komunikacijski programi	Napake v programih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:4	R:2-3	R:4-5
Microsoft Exchange	Napad zlonamerne programske opreme	Z:6	Z:3	Z:7
		N:5	N:3	N:6
		R:6	R:3	R:7

Komercialni paketi

Tabela 39: Ocenjevanje tveganja – programska oprema (komercialni paketi)

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Programi za kriptiranje	Napadi na kriptirne sisteme	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:1	R:4	R:3
Programi za kriptiranje	Napadi, ki skušajo obiti kriptirne sisteme	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:1	R:4	R:3
Programi za kriptiranje	Napake v programih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:4	R:4	R:6
Microsoft Office	Napake v programih	Z:3	Z:2-3	Z:3-4
		N:4	N:2-3	N:4-5
		R:4	R:2-3	R:4-5
Microsoft Office	Napadi zlonamerne programske opreme	Z:5	Z:2-3	Z:5-6
		N:5	N:2-3	N:5-6
		R:5	R:2-3	R:5-6
Programerska in načrtovalna orodja	Napake v programih	Z:3	Z:1-2	Z:2-3
		N:4	N:1-2	N:3-4
		R:4	R:1-2	R:3-4
Programi za oblikovanje	Napake v programih	Z:2	Z:1-2	Z:2
		N:2	N:1-2	N:2
		R:4	R:1-2	R:3-4
Pomožni programi	Napake v programih	Z:3	Z:1-2	Z:2-3
		N:3	N:1-2	N:2-3
		R:4	R:1-2	R:3-4
Vzdrževalna orodja	Napake v programih	Z:3	Z:1-2	Z:2-3
		N:3	N:1-2	N:2-3
		R:3	R:2	R:3
Protivirusna zaščita	Nedelovanje programa	Z:2	Z:4	Z:4
		N:4	N:4	N:6
		R:4	R:4	R:6

2 PRILOGA - PODROČJE PLAČILNEGA PROMETA

2.1 Ocena virov plačilnega prometa glede zahtevane stopnje varnosti

Tabela 40: Ocena glede zahtevane stopnje varnosti plačilnega prometa

Naziv vira	Opis	Ocena Z - N – R
Osebni računalnik	Strojna in programska oprema	Z:4
		N:4
		R:4
Sistem IBM	Strojna in programska oprema	Z:4
		N:4
		R:4
Komunikacijske povezave	Omrežje banke ter povezava na Banko Slovenije	Z:4
		N:4
		R:4
DB2 Vmesnik/ Predvmesnik	Programska oprema	Z:4
		N:4
		R:4
Povezovalno programje	Programska oprema	Z:4
		N:4
		R:4
NCAF (MEGA)	Strojna in programska oprema	Z:4
		N:4
		R:4
BSNET	Omrežje plačilnega sistema v Sloveniji za izmenjavo podatkov	Z:4
		N:4
		R:4
SWIFT / MERVA	Strojna in programska oprema	Z:4
		N:4
		R:4
Register	Strojna in programska oprema	Z:4
		N:4
		R:4
Vodenje TRR	Strojna in programska oprema	Z:4
		N:4
		R:4
Bancs	Strojna in programska oprema	Z:4
		N:4
		R:4
Klik, Proklik, Proklik +	Strojna in programska oprema za poslovanje preko interneta	Z:4
		N:4
		R:4
Teledom	Strojna in programska oprema	Z:4
		N:4
		R:4
Imago +	Strojna in programska oprema za optični zajem podatkov	Z:4
		N:4
		R:3
MOBA	Strojna in programska oprema za poslovanje preko mobilnih telefonov	Z:4
		N:4
		R:4
Oprema za šifriranje	Čitalci in pametne kartice za šifriranje in elektronsko podpisovanje podatkov	Z:4
		N:4
		R:4
Uporabniška navodila	Postopki in navodila za uporabnike	Z:3
		N:3
		R:4
Operaterska navodila	Postopki in navodila za delavce IT	Z:3
		N:3
		R:4

2.2 Ocena ogroženosti za plačilni promet

Tabela 41: Ocena ogroženosti za plačilni promet

Naziv vira	Grožnja	Ocena grožnje	Ocena ranljivosti vira	Ocena ogroženosti
Osebni računalnik	Odpoved strojne opreme	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Osebni računalnik	Nedovoljen fizični dostop	2	Z:3	Z:5
			N:3	N:5
			R:3	R:5
Osebni računalnik	Kršitev politike varovanja informacij	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
Osebni računalnik	Napake programske opreme	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Osebni računalnik	Izpad napajanja	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
Sistem IBM	Odpoved strojne opreme	2	Z:0	Z:2
			N:0	N:2
			R:1	R:3
Sistem IBM	Nedovoljen fizični dostop	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
Sistem IBM	Kršitev politike varovanja informacij (gesla, dostopi)	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
Sistem IBM	Napake programske opreme	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
Komunikacijske povezave	Prekinitev komunikacijskih povezav	3	Z:0	Z:3
			N:0	N:3
			R:2	R:5
Komunikacijske povezave	Prisluškovanje na povezavah	3	Z:1	Z:4
			N:0	N:3
			R:0	R:3
Komunikacijske povezave	Prestrezanje in spreminjanje podatkov na povezavah	3	Z:1	Z:4
			N:1	N:4
			R:0	R:3
DB2 vmesnik/ predvmesnik	Napake zaposlenih	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
DB2 vmesnik/ predvmesnik	Napake v programih	2	Z:1	Z:3
			N:1	N:3
			R:2	R:4
Povezovalno programje	Napake zaposlenih	1	Z:1	Z:2
			N:1	N:2
			R:2	R:3
Povezovalno programje	Napake v programih	1	Z:1	Z:2
			N:1	N:2
			R:2	R:3
NCAF (MEGA)	Odpoved strojne opreme	1	Z:0	Z:1
			N:0	N:1
			R:3	R:4

Tabela 41 - nadaljevanje

NCAF (MEGA)	Kršitev politike varovanja informacij (gesla, dostopi)	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
NCAF (MEGA)	Napake zaposlenih	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
BSNET	Izpad sistema BSNET	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
BSNET	Prekinitev na komunikacijskih povezavah z BSNET-om	2	Z:0	Z:2
			N:0	N:2
			R:1	R:3
BSNET	Odpoved strežnika BSNET	1	Z:0	Z:1
			N:0	N:1
			R:3	R:4
BSNET	Kršitev politike varovanja informacij (gesla, dostopi)	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
SWIFT / MERVA	Prekinitev na komunikacijskih povezavah s SWIFT-om	1	Z:0	Z:1
			N:0	N:1
			R:3	R:4
SWIFT / MERVA	Izpad delovanja SWIFT omrežja	0	Z:0	Z:0
			N:0	N:0
			R:3	R:3
SWIFT / MERVA	Napake na programski opremi Merva	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
Register	Nedostopnost sistemov Bancs in Globus iz Registra komitentov	3	Z:0	Z:3
			N:0	N:3
			R:2	R:5
Register, Vodenje TRR, Bancs	Kršitev politike varovanja informacij (gesla, dostopi)	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
Register, Vodenje TRR, Bancs	Napake programske opreme	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Register, Vodenje TRR, Bancs	Napake zaposlenih	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
Klik, Proklik, Proklik +	Prekinitev povezave banke z internetom	1	Z:0	Z:1
			N:0	N:1
			R:3	R:4
Klik, Proklik, Proklik +	Vdor iz interneta	3	Z:2	Z:5
			N:2	N:5
			R:2	R:5
Klik, Proklik, Proklik +	Napad zlonamerne programske opreme	3	Z:1	Z:4
			N:1	N:4
			R:1	R:4
Klik, Proklik, Moba, Proklik +	Napake programske opreme	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Klik, Proklik, Moba, Proklik +	Napake zaposlenih	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
Klik, Proklik, Moba, Proklik +	Kršitev politike varovanja informacij (gesla, dostopi)	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1

Tabela 41 - nadaljevanje

Teledom	Napake zaposlenih	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
Imago +	Odpoved optičnega čitalca	2	Z:0	Z:2
			N:0	N:2
			R:1	R:3
Imago +	Napake na programski opremi	2	Z:1	Z:3
			N:1	N:3
			R:1	R:3
MOBA	Nedelovanje javnega GSM omrežja	2	Z:0	Z:2
			N:0	N:2
			R:2	R:4
MOBA	Napake na WAP prehodu	1	Z:2	Z:3
			N:2	N:3
			R:2	R:3
MOBA	Vdori preko mobilnega omrežja	2	Z:2	Z:4
			N:2	N:4
			R:2	R:4
Oprema za šifriranje	Nerazpoložljivost opreme za šifriranje	1	Z:0	Z:1
			N:0	N:1
			R:3	R:4
Oprema za šifriranje	Zloraba opreme za šifriranje	1	Z:4	Z:5
			N:4	N:5
			R:4	R:5
Uporabniška in operaterska navodila	Nepopolna dokumentacija	2	Z:0	Z:2
			N:0	N:2
			R:3	R:5
Uporabniška navodila	Nedovoljen dostop do navodil	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1
Operaterska navodila	Nedovoljen dostop do navodil	1	Z:3	Z:4
			N:3	N:4
			R:0	R:1

2.3 Ocenjevanje tveganj za plačilni promet

Tabela 42: Ocenjevanje tveganj za plačilni promet

Vir	Grožnja	Ocena ogroženosti	Ocena Z-N-R	Ocena tveganja
Osebni računalnik	Odpoved strojne opreme	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
Osebni računalnik	Nedovoljen fizični dostop	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:4	R:7
Osebni računalnik	Kršitev politike varovanja informacij	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3
Osebni računalnik	Napake programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Osebni računalnik	Izpad napajanja	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
Sistem IBM	Odpoved strojne opreme	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:3	R:4	R:5
Sistem IBM	Nedovoljen fizični dostop	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Sistem IBM	Kršitev politike varovanja informacij (gesla, dostopi)	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3
Sistem IBM	Napake programske opreme	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Komunikacijske povezave	Prekinitev komunikacijskih povezav	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:5	R:4	R:7
Komunikacijske povezave	Prisluškovanje na povezavah	Z:4	Z:4	Z:6
		N:3	N:4	N:5
		R:3	R:4	R:5
Komunikacijske povezave	Prestrezanje in spreminjanje podatkov na povezavah	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:3	R:4	R:5
DB2 vmesnik/ predvmesnik	Napake zaposlenih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
DB2 vmesnik/ predvmesnik	Napake v programih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:4	R:4	R:6
Povezovalno programje	Napake zaposlenih	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:3	R:4	R:5
Povezovalno programje	Napake v programih	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:3	R:4	R:5
NCAF (MEGA)	Odpoved strojne opreme	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:4	R:4	R:6

Tabela 42 - nadaljevanje

NCAF (MEGA)	Kršitev politike varovanja informacij (gesla, dostopi)	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3
NCAF (MEGA)	Napake zaposlenih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
BSNET	Izpad sistema BSNET	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
BSNET	Prekinitev na komunikacijskih povezavah z BSNET-om	Z:2	Z:4	Z:6
		N:2	N:4	N:6
		R:3	R:4	R:5
BSNET	Odpoved strežnika BSNET	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:4	R:4	R:6
BSNET	Kršitev politike varovanja informacij (gesla, dostopi)	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3
SWIFT / MERVA	Prekinitev na komunikacijskih povezavah s SWIFT-om	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:4	R:4	R:6
SWIFT / MERVA	Izpad delovanja SWIFT omrežja	Z:0	Z:4	Z:2
		N:0	N:4	N:2
		R:3	R:4	R:5
SWIFT / MERVA	Napake na programski opremi Merva	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Register	Nedostopnost sistemov Bancs in Globus iz Registra komitentov	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:5	R:4	R:7
Register, Vodenje TRR, Bancs	Kršitev politike varovanja informacij (gesla, dostopi)	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3
Register, Vodenje TRR, Bancs	Napake programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Register, Vodenje TRR, Bancs	Napake zaposlenih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Klik, Proklik, Proklik +	Prekinitev povezave banke z internetom	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:4	R:4	R:6
Klik, Proklik, Proklik +	Vdor iz interneta	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:4	R:7
Klik, Proklik, Proklik +	Napad zlonamerne programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Klik, Proklik, Moba, Proklik +	Napake programske opreme	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Klik, Proklik, Moba, Proklik +	Napake zaposlenih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Klik, Proklik, Moba, Proklik +	Kršitev politike varovanja informacij (gesla, dostopi)	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:1	R:4	R:3

Tabela 42 - nadaljevanje

Teledom	Napake zaposlenih	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
Imago +	Odpoved optičnega čitalca	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:3	R:3	R:4
Imago +	Napake na programski opremi	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:3	R:4
MOBA	Nedelovanje javnega GSM omrežja	Z:2	Z:4	Z:4
		N:2	N:4	N:4
		R:4	R:4	R:6
MOBA	Napake na WAP prehodu	Z:3	Z:4	Z:5
		N:3	N:4	N:5
		R:3	R:4	R:5
MOBA	Vdori preko mobilnega omrežja	Z:4	Z:4	Z:6
		N:4	N:4	N:6
		R:4	R:4	R:6
Oprema za šifriranje	Nerazpoložljivost opreme za šifriranje	Z:1	Z:4	Z:3
		N:1	N:4	N:3
		R:4	R:4	R:6
Oprema za šifriranje	Zloraba opreme za šifriranje	Z:5	Z:4	Z:7
		N:5	N:4	N:7
		R:5	R:4	R:7
Uporabniška in operaterska navodila	Nepopolna dokumentacija	Z:2	Z:3	Z:3
		N:2	N:3	N:3
		R:5	R:4	R:7
Uporabniška navodila	Nedovoljen dostop do navodil	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:1	R:4	R:3
Operaterska navodila	Nedovoljen dostop do navodil	Z:4	Z:3	Z:5
		N:4	N:3	N:5
		R:1	R:4	R:3