UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

DARINKA OŠLAK

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VARNOST ELEKTRONSKEGA POSLOVANJA V SLOVENSKEM BANČNIŠTVU

Ljubljana, februar 2005 **DARINKA OŠLAK**

IZJAVA

Študentka Darinka OŠLAK izjavljam, da sem avtorica tega magistrskega dela, ki sem ga napisala pod mentorstvom prof. dr. Mira GRADIŠARJA in somentorstvom prof. dr. Borke JERMAN BLAŽIČ ter skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 14.02.2005

Podpis: _____

KAZALO

KRATICE IN OZNAKE

AC - Agencija za certificiranje javnih ključev
AES - Advanced Encryption Standard
AJPES - Agencijo za javno pravne evidence
APP - Agencijo za plačilni promet
ARPA - Advanced Research Projects Agency
ASBH - Agencija za sanacijo bank in hranilnic
BPRČ - Bruto poravnava v realnem času
CVI - Center vlade za informiranje
DES - Data Encryption Standard
FTP – File Transfer Protocol
IDEA - International Data Encryption Algorithm,
MAC - Message Authentical Code
MIT - Massachusetts Institute of Technology
NIST - National Institute of Standards and Technology
NSF - National Science Fundation
PIN – Personal Identifay Number
PUB - Pilotskega usposabljanja bank
RA - Uradi za registriranje
RIP – Računalniška izmenjava podatkov
RSA - Rivers, Shamir, Adleman
S.W.I.F.T. - Society to Worldwide Interbank Financial Transakcion
SEB – Sistem za elektronsko poslovanje
SET - Secure Electronic Transaction
SFNB - Security Firs Network Bank
SIGEN-CA - Slovenian GENeral Certification Authority
SIGOV-CA - Slovenian GOVernmental Certification Authority
SSL - Secur Sockets Layer
TCP/IP - Transport Control Protocol / Internet Protocol
TLS - Transport Layer Security – TLS
UJP - Upravo za javna plačila
VAN – Value Added Natwork
WAP - Wireless Aplication Protokol
WTLS - Wireless Transport Layer Security
WWW – World Wide Web
ZEPEP - Zakon o elektronskem poslovanju in elektronskem podpisu

SEZNAM SLIK IN TABEL

UVOD

Ali je današnji delovni dan sploh mogoč brez uporabe računalnika? Ali je danes sploh mogoče operirati s podatki brez informacijskega sistema? Kakšna je prihodnost zaprte organizacije, ki ni povezana z javnim omrežjem? Iz tega bi lahko zaključila, da si z razvojem računalniške in informacijske tehnologije naprednih storitvenih in proizvodnih organizacij, ki te tehnologije ne bi uporabljale, ne moremo več predstavljati. Praktično lahko ugotovimo, da je že v vsaki gospodarski družbi prisoten vsaj enostaven informacijski sistem.

Pri proizvodnih družbah so informacijski sistemi pomembni predvsem pri načrtovanju, vodenju in izvajanju proizvodnih procesov. Pri storitvenih organizacijah pa informacijski sistem predstavlja že pogoj in temelj uspešnega poslovanja. To je še posebej razvidno iz poslovanja finančnih institucij, ki si svojega delovanja brez uporabe elektronskega poslovanja ne morejo več predstavljati. Z globalizacijo trgov so finančne storitve ponujene različnim uporabnikom s celega sveta. Odvisne so od informacij iz vsega sveta, za svoj in za račun svojih komitentov pa opravljajo storitve, ki ne poznajo državnih meja in potekajo po medmrežju. Prehod na elektronsko poslovanje počasi izpodriva klasičen način bančništva in postavlja nove temelje in pravila obnašanja, s čimer se pojavlja tudi dvom glede varnosti in zaščite podatkov.

Za varno elektronsko poslovanja mora organizacija zagotoviti varnostnim zahtevam, ki omogočajo podatkom varno in zanesljivo potovanje po globalnem omrežju. Z uporabo najrazličnejših varnostnih mehanizmov lahko uporabnik prepreči napade vsiljivcev, ki nepooblaščeno uporabijo vire omrežja. Pogosti vzrok žrtev napada je prav slaba priprava na uporabo storitev elektronskega poslovanja. Nepoznavanje delovanja sistema kot tudi slaba zaščita pripelje uporabnike do nezaupanja v uporabo elektronskega poslovanja.

Namen magistrskega dela je obravnavati problematiko varnosti elektronskega poslovanja v slovenskem bančništvu ob uveljavitvi reformiranega plačilnega sistema in analizirati bančno ponudbo elektronskih storitev preko interneta za pravne osebe. S pomočjo raziskave, želim z vidika varnosti izpostaviti ključna šibka področja elektronskega bančništva, ki kljub najrazličnejših varnostnih mehanizmov, še vedno omogočajo storilcem zlorabo virov informacijskega sistema. V svetu elektronskega bančništva prežijo na uporabnike in ponudnike storitev drugačne nevarnosti kot v klasičnem poslovanju, zato so potrebni tudi drugačni varnostni ukrepi in orodja, ki poskušajo odvrniti napad morebitnih napadalcev.

Cilji magistrskega dela so predvsem naslednji:

- predstaviti elektronsko poslovanje in elektronsko bančništvo,
- preučiti varnostno tehnologijo v elektronskem poslovanju,
- oceniti ponudbo elektronskega bančništva v slovenskih bankah,
- sistematično ugotoviti stopnjo ranljivosti virov elektronskega poslovanja pri

elektronskem plačilnem sistemu in
- izpostaviti morebitne kritične pomanjkljivosti varnostni elektronskega plačilnega sistema ter pripraviti ukrepe in navodila za odpravo le teh.

V nalogi sem se dotaknila problematike, kako zaščititi finančne podatke pri elektronskem bančništvu. Glede na to, da je elektronsko bančništvo preko interneta z uvedbo transakcijskih in osebnih računov dobilo na večji veljavi, sem v nalogi analizirala varnost pri izmenjavi finančnih podatkov preko interneta med banko in podjetjem in opredelila ključne prednosti in nevarnosti ter identificira potencialne grožnje na vire v sistemu elektronskega plačevanja.

V prvem delu sem v treh poglavjih strnila teoretično osnovo, ki jo je potrebno osvojiti in razumeti, preden pristopimo k varni uporabi elektronskega bančništva. Prvo poglavje je namenjeno grobi predstavitvi elektronskega poslovanja, kjer sem podala nekaj ključnih klasifikacij in lastnosti. V drugem poglavju sem zajela bistvene lastnosti elektronskega bančništva, ki predstavlja jedro naloge v okviru katerega sem podrobneje izpostavila način elektronskega plačevanja preko interneta med bankami in podjetji. To je le eden izmed možnih načinov storitev elektronskega bančništva. Poznamo še druge načine, ki so namenjeni fizičnim osebam in bi z vključitvijo v mojo nalogo presegli potreben okvir magistrskega dela.

Tretje teoretično poglavje, ki je po vsebini najobsežnejše, zajema varnostne mehanizme pri elektronskem poslovanju s poudarkom na elektronskem bančništvu. V tem poglavju sem poleg metod varovanja izpostavila tudi glavne nevarnosti in grožnje ter njihove akterje, ki v današnjem svetu pišejo nova poglavja o računalniškem kriminalu. V nalogo sem zajela najpogosteje uporabljene tehnike varnostnih mehanizmov, ki se dopolnjujejo v kombinaciji z drugimi. Varnost je pomembna na vseh korakih, saj ti dobro zaklenjena vhodna vrata z dvojno ključavnico in verigo ne pomagajo dosti, če imaš odprto okno in s tem omogočiš napadalcem prosti vstop. Hiša je varna, kot je varen njen najšibkejši člen.

V četrtem poglavju se naloga prevesi v drugi del, kjer je vsebina empirično zasnovana. V tem poglavju analiziram stanje bančništva v Sloveniji v povezavi s pravnimi subjekti. V začetku sem predstavila zgodovinski vidik in razvoj bančništva, ki je leta 1997 doživel drastične spremembe na področju plačilnega prometa. Številna podjetja so se z reformo plačilnega prometa odločila za uporabo elektronskega poslovanje z bankami. Prav slednja novost je odločujoče vplivala na izbiro ideje za temo magistrskega dela.

V zadnjem poglavju, ki je raziskovalne narave, sem poskušala teoretični izsledke iz prvega dela združiti s stanjem elektronskega bančništva v Sloveniji. Za varno uporabo elektronskega bančništva je potrebno za varnost poskrbeti tako na strani podjetja in banke kot tudi v sami distribucijski poti. Z analizo tveganja varnosti elektronskega plačilnega sistema sem izluščila ključne vire v podjetju, banki in v komunikacijski povezavi. Na podlagi ocen ocenjevalcev, ki so sodelovali pri raziskavi, sem ocenila vire in potencialne grožnje ter tako dobila najbolj ranljive vire. Z analizo sem prišla do zaključka, ki potrjuje zastavljen cilj naloge, da se stopnja

varnosti lahko poveča s preudarnim, pazljivim pristopom, ki v prvi vrsti temelji na dobrem razumevanju sistema in zavedanju nevarnosti na vseh ravneh uporabe.

V nalogi sem uporabila pridobljeno zanje na podiplomskem študiju Informacijsko upravljaljskih ved na Ekonomski fakulteti v Ljubljani. V prvem delu naloge sem z deskriptivno metodo na osnovi študija domače in tuje literature ter člankov, ki objavljajo novosti v podjetjih in bankah po Sloveniji, povzela teoretično problematiko, ki sistematično zajema vsa ključna področja elektronskega poslovanja. Prevladujejo viri iz interneta, ki so pogosto veliko bolj ažurni kot pa literatura, saj je narava tematike zelo dinamična in doživlja še veliko sprememb in novosti. V teoretičnem delu sem opisala uveljavljene pristope, metode in tehnike elektronskega poslovanja s poudarkom na zagotavljanju varnosti. Z metodo primerjalne analize sem v nekaterih delih naloge primerjala slovensko stanje z razmerami drugod v Evropski uniji.

V drugem delu sem z empiričnim pristopom teoretični prispevek iz prvega dela podkrepila s praktičnim primerom elektronskega bančništva. Naredila sem presek ponudbe elektronskega bančništva v Sloveniji in ponudnikov bančnih aplikacij. V zaključku sem na osnovi vprašalnika analizirala tako pridobljene podatke in na podlagi ocen izluščila ključna ozka grla glede varnosti pri prenosu finančnih transakcij med podjetjem in banko.

Vsebina naloge obsega le delček delovanja celotnega področja elektronskega poslovanja, ki v zadnjih letih intenzivno narekuje in usmerja sodobne internetne storitev, ki kar najširšemu segmentu uporabnikov omogočajo racionalizacijo poslovanja, pogojeno z zahtevami sodobnega načina zasebnega in poslovnega življenja. Pričakovanja po varnih, zanesljivih in dostopnih storitvah pogojujejo tehnološko zasnovo, ki omogoča zanesljivo in dosledno uporabo. Prav zato so informacijske rešitve za podporo poslovanju različne za različne tipe komitentov. Vse pa črpajo iz osnov, ki so zajete v tej nalogi in so podlaga za gradijo zahtevnejših oblik informacijskih sistemov.

1 ELEKTRONSKO POSLOVANJE

1.1 OPREDELITEV ELEKTRONSKEGA POSLOVANJA

Elektronsko poslovanje (v nadaljevanju e-poslovanje) je že nekaj časa pomemben del informatike. Z razvojem računalniških omrežij in komunikacij ter z razvojem novih tehnologij in interneta se postavljajo nova pravila in skupne podlage za elektronsko sodelovanje med partnerji, ki je tako postalo preprostejše, učinkovitejše, hitrejše in tudi cenejše.

V pogledu definicij e-poslovanja obstaja širok spekter razlag. Sam pojem v angleščini ("electronic commerce") se bolj kot v slovenščini navezuje na napačno razumevanje v smislu elektronske prodaje, kar oznaka e-poslovanja vsekakor presega in vključuje še vrsto drugih oblik uporabe. V najširšem smislu e-poslovanje vključuje uporabo vseh oblik informacijske in komunikacijske tehnologije v poslovnih odnosih. Sem sodijo trgovinske, proizvodne in storitvene organizacije kot tudi ponudniki informacij, potrošniki in državna uprava (Jerman Blažič, 2001, str 13).

Ena izmed definicij e-poslovanja opredeljuje kot izmenjavo poslovnih informacij preko omrežij s pomočjo računalniške izmenjave podatkov[1] in vseh podobnih tehnologij[2]. Novejše razlage, ki vključujejo internet kot omrežno okolje, definirajo e-poslovanje kot proces kupovanja, prodaje ali zamenjave proizvodov, storitev ali informacij preko računalniškega omrežja. E-poslovanje lahko preprosto definiramo kot »poslovati elektronsko«. Glede na obsežnost pojma e-poslovanja lahko razlage e-poslovanja proučujemo iz različnih spektrov (Kalakota, 1997, str.3):

1. Komunikacijski pogled: je prenos informacij, proizvodov in storitev preko telefonskih linij, računalniškega omrežja ali drugih komunikacijskih povezav.
2. Poslovno procesni pogled: v poslovni proces s pomočjo programskih aplikacij vnaša avtomatizacijo procesov in transakcij.
3. Storitveni pogled: omogoča večjo učinkovitost poslovanja z znižanjem stroškov, boljšo kvaliteto in hitrejšo dobavo oz. izvedbo storitve.
4. Povezovalni pogled: deluje v omrežjih, ki so med seboj povezane in delujejo neposredno.

[1] RIP oz. EDI – Electronic Data Interchange pomeni izmenjavo standardiziranih, kodiranih sporočil med dvema računalniškima aplikacijama (Toplišek, 1998, str. 13).
[2] Elektronsko poslovanje. Definicije. [URL: http://www.e-poslovanje.net/poglej_clanek.asp?ID=25], 26.06.2002.

1.2 ZGODOVINSKO OZADJE IN RAZVOJ E-POSLOVANJA

Začetki e-poslovanja segajo v leto 1968, ko se je začel razvoj računalniških omrežij in interneta, združevanja informacijske in telekomunikacijske tehnologije ter z uvajanjem standardov za RIP. Računalniška tehnologija, ki je bila v začetku namenjena le računalniškim strokovnjakom in znanstvenikom, je z leti postala veliko bolj uporabna in prijazna tudi širšim uporabnikom.

V 70. letih se je s pojavom elektronskih finančnih prenosov med bankami prek varnih zasebnih omrežji[3] spremenil način poslovanja na finančnem trgu. Precej podatkov je iz papirnate oblike prešlo na elektronsko obliko, ki so se znotraj podjetja prenašali preko raznih sistemov za prenos podatkov in po elektronski pošti. V poznih 70. in zgodnjih 80. letih se je e-poslovanje razširilo v okviru podjetij v obliki sistemov za prenos datotek, RIP in elektronske pošte. S tem so podjetja zmanjšala obseg papirnega dela in povečala se je avtomatizacija pisarniškega poslovanja. V poznih 80. in zgodnjih 90. letih so sistemi za izmenjavo sporočil postali integralni del računalniških sistemov in omrežij (Jerman Blažič, 2001, str. 13-14).

Dotedanja praksa izmenjave podatkov je pokazala nekaj slabosti in usmerila nadaljnji razvoj (Škrlec, 2002, str. 18):

- Gradila je na specifičnih komunikacijskih povezavah med podjetji, ki so bila draga in nedostopna za majhna podjetja.
- Natančno določena oblika podatkov in dokumentov, ki se izmenjujejo med različnimi aplikacijami na podlagi natančno določenih standardov. Preslikava v želeno obliko je bila draga in zapletena.
- Težje dostopna in razumna za širši krog uporabnikov.

Kljub pomanjkljivosti, ki jih je sistem dajal, je bila dobra stran standardizacije in izgradnje komunikacijske infrastrukture v avtomatizaciji procesov, ki je skrajšala čas obdelave podatkov in zmanjšala stroške prenosa. To se je dogradilo v nadaljnjem razvoju, ki je bil hiter in učinkovit. Nove rešitve se dopolnjujejo s staro tehnologijo, kar podjetjem omogoča cenovno ugodno nadgradnjo sistema. 90. leta so z razvojem interneta[4] ter s pojavom svetovnega spleta na internetu prinesle preobrat, ki je sprožil razvoj e-poslovanja na vse oblike uporabe, ki so poznane tudi danes in so se razširile med številne uporabnike. Njihovi temelji enostavne in preproste uporabe izhajajo iz ključnih predpostavk, ki gradijo internet. Te so:

[3] S.W.I.F.T. - Society to Worldwide Interbank Financial Transakcion - omrežje bančnih organizacij.

[4] Internet je danes najbolj razvito in tudi obiskano javno omrežje. Začetki interneta segajo v obdobje oboroževalne tekme med tedanjima velesilama Sovjetsko zvezo in ZDA. V času, ko so ljudje živeli v strahu pred vojno, so Rusi presenetili svet z izstrelitvijo prvega umetnega satelita Sputnik v vesolje. Američani so v odgovor ruskim strokovnjakom ustanovili vojaško raziskovalno ustanovo ARPA (Advanced Research Projects Agency), ki naj bi jim omogočila hitrejše osvajanje vesolja in razvoj morilskih naprav. Leta 1969 so se različni oddelki ARPA povezali v računalniško omrežje ARPAnet, ki je z leti preimenoval v internet. Leta 1986 je ARPA nadaljnji razvoj omrežja predala znanstveni organizaciji NSF (National Science Fundation), ki je v omrežje povezala pet velikih računalniških središč v Ameriki. NSF je spodbujala raziskovalne organizacije pa tudi podjetja po svetu, naj se povežejo v omrežje in s tem izmenjujejo zamisli z drugimi. Leta 1995 je bil internet že neustavljivo naraščajoč in NSF deluje kot hrbtenica, ki povezuje velika računalniška središča v Ameriki in je le del vseobsegajočega interneta, dosegljivega v več kot 130 državah sveta.

- lokacijsko neodvisna in strankam dosegljivo omrežje kjerkoli in kadarkoli,
- povezava množice navzven odprtih manjših računalniških omrežij, ki nimajo skupnega lastnika ali osrednjega nadzornega organa,
- preprosta uporaba z vnaprej določenimi scenariji in
- strojna ter programska neodvisnost.

Komunikacija je izvedljiva po istih pravilih sporazumevanja, ki so poznane vsem uporabnikom. S tem je internet znižal stroške za učinkovito komuniciranje, odprl pot do novega načina poslovanja in novih trgov, povečal učinkovitost, skrajšal čas posameznih poslovnih postopkov, omogočil vpeljavo večpredstavnih storitev ter večjo prilagodljivost spremembam na trgu in zagotovil, da je ekonomija postala globalna, gospodarske organizacije pa globalno povezane.

1.3 KLASIFIKACIJE E-POSLOVANJA

Kot je razbrati iz definicij, je e-poslovanje globalni pojem, ki vključuje vrsto področji in omogoča uporabnikom dostop do informacij, ki so zbrane na drugih delovnih postajah. Računalniška omrežja, sestavljena iz omrežji računalnikov in vmesnikov, predstavljajo infrastrukturo e-poslovanja, ki ga delimo na:

- internet – je globalno, javno omrežno okolje,
- intranet – je poslovno okolje, ki povezuje nekaj organizacij v zaprtem okolju,
- ekstranet – omrežje, ki povezuje različne intranete poslovnih partnerjev preko interneta ter
- privatna omrežja.

Tehnologija interneta in na njo vezane aplikacije so pospešile razvoj e-poslovanje, ki je svoj meteorski vzpon doživela v letu 1996, ko je uporaba e-poslovanja prešla v uporabo med vse uporabnike. Glede na področje uporabe e-poslovanja delimo na (Turban, 2003, str. 7-8):

- poslovanje med podjetji (B2B),
- poslovanje med podjetji in strankami (B2C) in obratno (C2B),
- poslovanje med strankami (C2C),
- poslovanje med vlado in podjetji ter strankami (G2B oz. G2C) ter
- drugi načini (B2B2C, m-poslovanje, intrabusiness poslovanje, podjetje in zaposleni B2E, nonbusiness poslovanje in exchange-to-exchange E2E).

Uvedba e-poslovanja vpliva na poslovni proces s spremembami v oskrbovalni verigi kot tudi v spremembi marketinškega spleta. Vse to za seboj potegne posebno strategijo e-poslovanja, ki so odraža v celostni strategiji podjetja. Podjetje lahko v elektronskem okolje komunicira

med zgoraj naštetimi subjekti na različne načine in z različnim namenom. Najbolj znani in razširjeni načini e-poslovanja so:

- elektronska pošta,
- prenos datotek - FTP[5],
- svetovni splet - WWW[6],
- omrežne novice,
- priključitev na oddaljen računalnik (TELNET) in
- videokonferenca.

Omrežni trg nudi, da se z uporabo zgoraj navedenih načinov e-poslovanja zbrišejo nacionalne meje in časovne omejitve ter omogočijo, da se podjetja čez noč spremenijo iz lokalnih v globalna podjetja. Omrežni trg ne priznava malih in velikih podjetji iz realnega sveta, ampak postavlja drugačne kriterije, ki ločijo dobra od slabih podjetji. Katera so dobra in katera slaba, pa je odvisno, kako hitro izkoristijo konkurenčne prednosti, ki jih ponuja e-poslovanje in se izognejo morebitnim nevarnostim. V informacijski tehnologiji se je rek, da velike ribe jedo male, preoblikoval, da hitre ribe jedo počasne.

1.4 PREDNOSTI IN SLABOSTI E-POSLOVANJA

Novosti, ki jih prinaša uporaba e-poslovanja jih nekateri primerjajo s spremembami, ki jih je prinesla industrijska revolucija. Spremembe se odražajo v prednostih in slabostih uporabe e-poslovanja posameznika, družbe in podjetij (glej Tabela 1 in Tabela 2).

Tabela 1: Prednosti e-poslovanja za podjetja, posameznika in družbo

PREDNOSTI ZA PODJETJA	• razširitev trga, globalizacija,
	• zmanjšanje stroškov poslovanja, zalog,
	• prilagoditev proizvodov željam kupca,
	• skrajševanje proizvodnega cikla,
	• prenova poslovnih procesov, reinžiniring,
	• zmanjšanje telekomunikacijskih stroškov.
PREDNOSTI ZA STRANKO	• možna hitra primerjava cene in kvalitete,
	• hitra dobava digitalnih proizvodov,
	• večja informiranost, konkurenca, večje ugodnosti,
	• izmenjava mnenj med kupci.
PREDNOSTI ZA DRUŽBO	• možnost dela preko doma, manj potovanja, manjši promet in manjše onesnaževanje,
	• ugodnosti povečujejo življenjski standard,
	• razvojne možnosti za tretji svet,
	• pospešuje dostavo javnih storitev .

Vir: Turban, 2003, str. 16-20.

[5] FTP – File Transfer Protocol
[6] WWW – World Wide Web

Tabela 2: Tehnične in netehnične omejitve, ki jih prinaša e-poslovanje

TEHNIČNE OMEJITVE	• pomanjkanje zanesljivosti, varnosti in tajnosti,
	• slab komunikacijski prenos,
	• nekompatibilnost opreme in hitre programske spremembe,
	• hitre spremembe tehnologije,
	• dodatni stroški za tehnično podporo.
NETEHNIČNE OMEJITVE	• stroški nabave računalniške opreme,
	• nezaupanje v varnost,
	• nezaupanje v obstoj podjetij,
	• različna zakonodaja in standardi.

Vir: Turban, 2003, str.20-21.

Zaradi številnih konkurenčnih prednosti, ki jih je moč dobiti z vstopom v e-poslovanje, se širi razkorak med uspešnimi in manj uspešnimi. Tempo razvoja pogosto sili podjetja, da sprejmejo nekaj novega, kar še ni povsem uveljavljeno in preizkušeno. Podjetja se v konkurenčnem boju za višji tržni delež ne malokdaj zatečejo k hitrim in nekvalitetnim rešitvam, ki za seboj puščajo slab in negativen rezultat. Neuspeli poskusi v e-poslovanju mečejo slabo luč na celotno področje in ljudje postanejo nezaupljivi. Pregledna raziskava na osnovi anketnega vprašalnika v okviru magistrskega dela na Fakulteti za organizacijske vede v Kranju je pokazala, da je 94% anketiranih kot težavo v e-poslovanju navedlo varnost finančnih podatkov, 93% zaupnost transakcij ter druge splošne zadeve varnosti (Puciher, 1999, str. 7-13).

Seveda si pred varnostjo in zaščito ne moremo zatiskati oči, saj je skrb za varnost podatkov pred razkritjem in zlorabo opravičena. Že en vdor v sistem pusti pri uporabnikih nezaupanje v digitalno obliko poslovanja in pusti za seboj veliko škodo. Zato se informatiki trudijo razvijati in graditi sisteme, ki bi zagotavljali želeno stopnjo varnosti in bi zagotavljali zadostno raven funkcionalnosti sistema. Računalniška varnost vključuje tako varnost fizičnega sistema, omrežnih in računalniških povezav kot tudi pravilno ravnanje uporabnikov. Dosežemo jo z učinkovitim procesom planiranja, uvajanja in preverjanja sistema varovanja pred vsiljivci[7]. Za zagotovitev le-te so na voljo različne kombinacije programske in strojne opreme ter fizično varovanje. Oblika zaščite je odvisna od varnostne politike organizacije in odnosa, ki ga v organizaciji gojijo do pomena varnosti in zaupnosti.

1.5 RAZSEŽNOST UPORABE E-POSLOVANJA

Za zagon e-poslovanja je potrebna namestitev in uvedba ključnih tehnoloških sestavin varnega e-poslovanja z vidika infrastrukture ter strojne in programske opreme. Postavitev ni majhen zalogaj in zahteva velika vlaganja tako v tehnologijo kot v znanje zaposlenih, ki se na daljši rok povrne. Pogoji za uspešno realizacijo e-poslovanja so (Jerman Blažič, 2001, str. 60):

- ustrezna infrastruktura in tehnološke komponente,

[7]Introduction to network security. SupportNet Online. [URL: http:/supportnet.merit.edu/m-intsec], 12.06.2002.

- ustrezno tehnološko znanje in sposobnost nadzora nad uporabo sistema e-poslovanja,
- nadzor nad upravljanjem z informacijami ter znanjem za potrebe odločanja,
- osvojitev postopkov za upravljanje z informacijami,
- upoštevanje vizije podjetja v poslovni strategiji in izbranega poslovnega modela ter
- obvladovanje okolja in demografske karakteristike potencialnega trga.

Potrebni pogoji za uspeh so enaki po vsem svetu, kar še ne pomeni, da so rezultati kot tudi obnašanje in pričakovanja podjetij med seboj enaka. E-poslovanje je poznano po vsem svetu, vendar se profil podjetij, ki uporabljajo takšen način poslovanja med celinami razlikuje, kot tudi pristopi pri uvajanju po svetu nimajo enakega scenarija. Na področju e-poslovanja so ameriška podjetja bolj usmerjena h končnemu potrošniku (več kot 50% ameriških podjetji, ki posluje na internetu posluje z individualnimi strankami), medtem ko imajo evropska podjetja za stranke pretežno podjetja (B2B) in so bolj usmerjena k medsebojnemu sodelovanju podjetji (Jerman Blažič, 2001, str. 24). Analize na strani uporabe interneta in e-poslovanja v podjetjih kažejo, da ima 80% velikih podjetji svojo predstavitveno stran na internetu, na kateri ponujajo splošne informacije, le 56% jih še ponuja kakšno drugo storitev preko spleta in le 45 % podjetji vključuje plačilni sistem (Škrlec, 2002, str. 18). Slovenija je v tem segmentu manj razvita, čeprav jo zaradi elektronskega plačilnega prometa z Agencijo za plačilni promet (APP) ocenjujejo kot razvito. Veliko bolj razvito je področje poslovanja s končnimi uporabniki, kjer je ponudba storitev veliko bolj pestra.

Razširjenost uporabe interneta se kaže v deležu uporabnikov internetnih storitev, po katerih se Slovenija uvršča med srednje razvite države. V letu 2001 se je več kot 31% celotnega prebivalstva posluževalo storitev preko interneta. Na lestvici se uvrščamo pred državami, ki smo maja leta 2004 vstopile v Evropsko Unijo (EU) prav tako prekašamo nekatere stare članice EU (Španija, Grčija, Francija). Največ uporabnikov imajo v skandinavskih državah, Švici, Veliki Britaniji in na Nizozemskem[8].

Med glavne spodbujevalce razvoja in odločanja za e-poslovanja v Sloveniji uvršamo[9]:

- skrajšanje odzivnih časov in izboljšanje učinkovitosti,
- povečanje fleksibilnosti podjetja,
- izboljšanje upravljanje informacijskega sistema in
- izboljšanje storitev za kupce.

Na drugi strani pa med zaviralne vzroke počasnega razvoja e-poslovanja uvrščamo:

- pomanjkanje ustreznih kombinacij znanj,
- finančne omejitve,
- panoge, v kateri podjetje deluje – standardizacija,

[8] Spletna stran NUA. [URL: www.nua.com], 01.01.03.
[9] Prodnik Pepevnik Vesna: Marketinški vidik uvajanja elektronskega poslovanja v slovenska podjetja. Ministrstvo za informacijsko družbo. [URL: www.merkur.si], 10.02.2004.

- odpor uporabnikov znotraj podjetja in
- zakonodaja.

Slednja prav zaradi brisanja mej in nastopanja na skupnem globalnem trgu ob novih oblikah poslovanja zahteva ureditev skupne pravne podlage in pravne regulative. Zaradi številnih možnosti zlorab in kršitev (javnega reda, avtorskih pravic, pravic potrošnikov) je področje nujno pravno urediti v tolikšni meri, da gospodarskega razvoja ne ohromi in zavre ter da možnosti za učinkovito delovanje in razvoj gospodarstva.

1.6 PRAVNA UREDITEV E-POSLOVANJA

Uporaba informacijske tehnologije in z njo povezanega elektronskega izmenjevanja sporočil ter hranjenja pomembnih dokumentov v digitalni obliki v vsakodnevnem gospodarskem in upravnem poslovanju je vse večja in z uveljavitvijo interneta dobiva še močnejši zagon. Vendar pa pomanjkanje ustrezne zakonske ureditve lahko znatno ovira sporočanje pravno pomembnih in zavezujočih informacij v elektronski obliki in povzroči splošno pravno negotovost. Zato je nujno zagotoviti pravno varnost najširše uporabe e-poslovanja v domačem in mednarodnem gospodarstvu. Na to dejstvo opozarjajo tudi različna priporočila vseh pomembnejših mednarodnih organizacij, kot so Organizacija združenih narodov, EU, Svet Evrope in druge.

Gre za pravno problematiko, ki ureja splošno in zelo široko področje, ki obsega prenos podatkov med računalniki, med pogodbenimi partnerji v dogovorjenem standardu, izmenjavo elektronskih sporočil z uporabo javnih ali lastninskih standardov preko javnih ali zasebnih omrežij oziroma najbolj splošno prenašanje golega besedila v elektronski obliki (npr. preko interneta). Zaradi širine področja je ureditev vplivala na izvajanje velikega števila zakonov in drugih predpisov. Področje namreč ni izredno široko samo zaradi raznovrstnih možnosti uporabe e-poslovanja v gospodarstvu, državni upravi in drugod, temveč zakonodajno urejanje e-poslovanja posega tudi v zelo obširen spekter obstoječe zakonodaje, saj spreminja temeljne pravne pojme, kot so izvirnik oziroma original, pisna oblika, lastnoročni podpis pogodbenih strank in podobni pojmi, ki jih zasledimo v večini slovenskih zakonov.

Ob upoštevanju gospodarskih potreb je bilo v EU sprejeto vrsto direktiv, ki se neposredno ali posredno dotikajo e-poslovanja. Poleg Direktive o standardih in pravilih za storitve informacijske družbe ter Direktive o elektronskih podpisih je ena najpomembnejših Direktiva o elektronskem poslovanju[10]. Njena določila so sprejele vse članice v svojo nacionalno zakonodajo.

Direktiva o elektronskem poslovanju obsega področja informacijske družbe skupnega trga. Skupaj z Direktivo o elektronskih podpisih postavlja temeljna pravila za poslovanje preko

[10] Directive on Electronic Commerce - Direcive 2000/3 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society service, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

interneta v državah članicah EU. Z direktivami so se postavila pravila, ki omogočajo delovanje skupnega trga na področju informacijske družbe (prost pretok storitev) z vsemi vrstami transakcij med uporabniki (B2B, B2C, C2C, G2C) pod enakimi pogoji ne glede na državne meje v EU. S tem zagotavljajo enoten režim pravil za ponudnike elektronskih storitev, za oglaševanje, sklepanje elektronskih pogodb, itd. Iz obsega direktiv pa so izrecno izvzeta nekatera področja (davki, varstvo podatkov, karteli) ter nekatere dejavnosti (notarske storitve, zastopanje na sodišču, igre na srečo, itd), ki se urejajo na državni ravni (Milenkovič, 2001, str. 96-98).

Slovenija se je s sprejemom Evropskega pridružitvenega sporazuma obvezala, da bo zakonodajo postopno uskladila s pravom EU. Junija leta 2000 je bil sprejet Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) (Uradni list RS, št. 57/2000) in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 ter št. 2/2001).

ZEPEP ureja e-poslovanje, ki zajema poslovanje v elektronski obliki na daljavo z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi e-poslovanje v sodnih, upravnih in drugih podobnih postopkih (1. člen ZEPEP).

ZEPEP v skladu z zgoraj omenjeno direktivo EU prav tako razlikuje med elektronskim in varnim elektronskim podpisom ter med navadnim in kvalificiranim digitalnim potrdilom. 15. člen ZEPEP določa, kateri elektronski podpis[11] je enakovreden lastnoročnemu podpisu. Zakon predpisuje, da je varen elektronski podpis[12], oblikovan z uporabo sredstev za varno elektronsko poslovanje, podpisnik, ki je podpis oblikoval, pa mora imeti kvalificirano potrdilo. Z varnim elektronskim podpisom in digitalnim potrdilom pošiljatelj zagotavlja naslovniku pristnost podpisanih podatkov in prepoznavanje podpisnika na daljavo (Pavliha, 2002, str. 76-77).

Zakon med drugimi tudi določa (ZEPEP, Uradni list RS, št. 57/2000):

- podatke, ki morajo biti ugotovljivi iz kvalificiranega potrdila,
- pogoje, ki jih morajo izpolnjevati ponudniki in uporabniki storitev, ki so v zvezi z overjanjem javnih ključev ali elektronskimi podpisi,
- odgovornost overiteljev,
- naloge in pristojnosti inšpekcijskih organov,
- prostovoljno akreditacijsko shemo ter
- kazenske določbe za prekrške overiteljev, imetnikov potrdil in posameznikov.

[11] Razlika med elektronskim in digitalnim podpisom je v tem, da je e-podpis oblika podpisa, dobljena z elektronsko tehnologijo, medtem ko je digitalni podpis le tisti, ki ga dobimo s šifrirnimi postopki, ki je šifriran na način asimetričnega dvojnega ključa (Toplišek, 1998, str.30).

[12] Varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve (4.točka 2.člena ZEPEP): da je povezan izključno s podpisnikom, da je iz njega mogoče zanesljivo ugotoviti podpisnika, da je ustvarjen s sredstvi za varno e-podpisovanje, ki so izključno pod podpisnikovim nadzorom, da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

Zakon je tehnično nevtralen, saj se tehnologija varovanja podatkov v e-poslovanju zelo hitro spreminja. Vlada RS je s podzakonskimi določili predpisala podrobnejša merila za izpolnjevanje zahtev glede postopkov, sredstev in drugih določil, ki jih zahteva ZEPEP.

Na podlagi komentarjev zakona ZEPEP in novih Smernic v evropskem prostoru[13] je vlada RS leta 2004 potrdila Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 25/2004), ki je bil pozneje sprejet v državnem zboru (v nadaljevanju ZEPEP-A). Razloge za sprejetje novela ZEPEP-A lahko razdelimo v tri skupine (Pernovšek, 2004, str. 28):

- uskladitev slovenskega pravnega reda s pravnim redom EU,
- odprava nekaterih sistemskih in tehničnih pomanjkljivosti ZEPEP iz leta 2000 in
- določitev pravne podlage za vzpostavitev oziroma vključitev digitalnih potrdil na osebne in druge identifikacijske dokumente.

Zagotovitev zakonske podlage še me zagotavlja, da je problematika varnosti v e-poslovanju rešena. Podana so le minimalna določila e-poslovanja, ki se glede na področja delovanja dopolnjujejo še z drugimi zakoni in predpisi, ki podrobneje predpisujejo način delovanja. Zakon o bančništvu je krovni zakon na področju bančništva, ki v povezavi z drugimi zakoni na področju finančnega poslovanja in elektronskega poslovanja, določajo pravno podlago za vzpostavitev e-bančništva.

[13] Smernica o elektronskem poslovanju se na splošno ukvarja s pravilnim delovanjem notranjega trga Evropske unije z zagotavljanjem prostega pretoka storitev informacijske družbe med državami članicami in zavezuje ponudnike teh storitev s sedežem v EU.

2 ELEKTRONSKO BANČNIŠTVO

2.1 OPREDELITEV ELEKTRONSKEGA BANČNIŠTVA

Deregulacija trgov, globalizacija in strateški vpliv informacijske tehnologije so povzročili drastične spremembe v bančnem sektorju. Vse večja globalizacija in povečanje konkurence spreminja osnovne značilnosti finančnih trgov. Gonilna sila, ki vodi v inovacije in teži k prilagajanju novim trendom, je digitalna tehnologija, katere jedro sprememb je e-bančništvo.

E-bančništvo lahko opredelimo kot kakršenkoli način poslovanje stranke z banko, ki je neodvisen od poslovalnic bank in temelji na informacijski tehnologiji in elektronskih medijih. V širšo razlago vključujemo vse bančne storitve, ki se opravljajo po elektronski poti (Miš Svoljšak, 1997, str.12):

- bančne avtomate,
- elektronsko bančništvo preko interneta,
- telefonsko bančništvo,
- mobilno bančništvo in
- kartično poslovanje.

Ožja razlaga e-bančništva se nanaša le na storitve, ki jih uporabljamo preko interneta in na katere sem se v povezavi s podjetji omejila v vsebini mojega magistrskega dela. V nadaljevanju bom z izrazom e-bančništvo aplicirala na del, ki se izvaja preko interneta, oziroma se izvaja preko odjemnega programa preko interneta .

2.2 ZNAČILNOSTI E-BANČNIŠTVA

Banke so z novimi načini dostopa do finančnih posrednikov korenito spremenile podobo tradicionalnega načina poslovanja. Sodobni življenjski ritem in tehnološke novosti izredno vplivajo na razvoj bančnega poslovanja. Nenehna dostopnost raznolikih, prilagodljivih in cenovno konkurenčnih bančnih storitev z uporabo številnih tržnih poti, postaja temelj današnjega bančništva. Storitve sodobnega e-bančništva morajo zagotoviti bančno tajnost, varnost, anonimnost prenosov, možnost opravljanja storitev kjerkoli in kadarkoli.

»Kupec je kralj« je rek, ki velja tudi v bančnem okolju. Banke strmijo k zadovoljitvi želja strank in hkrati k znižanju stroškov poslovanja. Iz tega lahko izluščimo dva glavna vzroka uvajanja e-bančništvo:

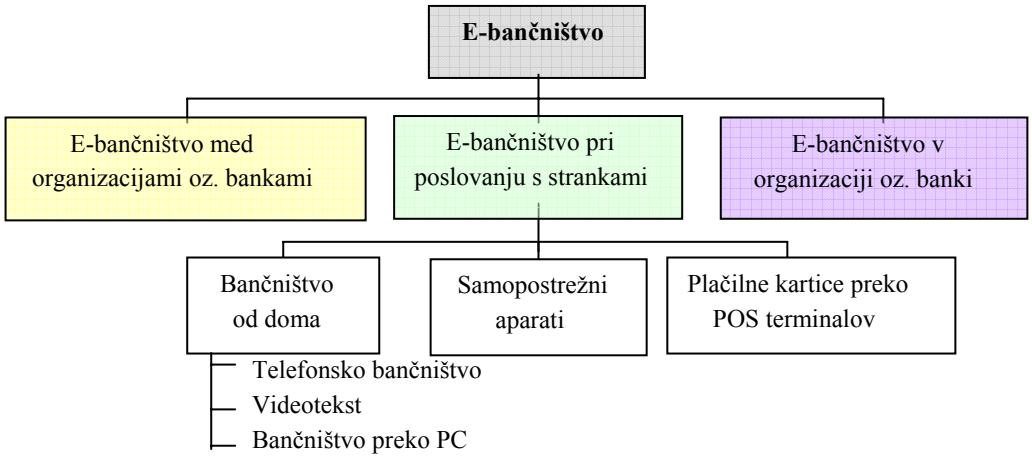
- Banke so želele odstraniti čakajoče vrste v bankah, znižati stroške poslovanja in masovne posle prenesti z bančnih okenc ter ta čas porabiti za svetovanje strankam in

opravljanje zahtevnejših poslov.

- Želele so prilagoditi strankam za delo z bančnimi posli od doma in jim skrajšati čas in napor v bankah.

Banke nudijo svoje storitve preko digitalnega medija različnim segmentom uporabnikom. Med uporabniki so tako fizične kot pravne osebe, ki imajo možnost izbirati med različnimi oblikami e-bančništva, ki nadomeščajo tradicionalni načine poslovanja (glej Slika 1).

Slika 1: Oblike e-bančništva



Vir: Miš Svoljšak, 1997, str. 12.

Elektronske bančne storitve so najbolj razvite v poslovanju s prebivalstvom. Za razliko od pravnih oseb jim je poleg finančnih prenosov in plačilnega prometa omogočena uporaba potrošniškega plačevanja z raznimi plastičnimi in kreditnimi karticami, uporaba bančnega avtomata kot tudi domače bančništvo.

2.2.1 Domače bančništvo

Domače bančništvo je oblika dostopanja do bančnih storitev preko raznih povezav od doma. Prvi začetki segajo v leto 1970, ko se je pojavila prva oblika domačega bančništva – telefonsko bančništvo. Najbolj popularen pristop je bil s pomočjo digitalnih telefonov na gumbe, s katerimi so stranke prihajale do bančnih uslug. Vendar so kljub začetnemu optimizmu rezultati prinesli veliko razočaranje. Zaradi nezmožnosti vizualne verifikacije in omejene uporabe digitalnih telefonov v 70-ih je to obliko uporabe v 80-ih letih kot možen medij za domače bančništvo zamenjala kabelska televizija. Čeprav so s tem rešili grafične omejitve telefonije, je imela druge pomanjkljivosti. Le nekateri ameriški uporabniki so imeli dvosmerni kabel, ki je bil potreben za izvedbo operacije. Ker je imel računalnik tako možnost vizualizacije kot dvosmerno komunikacijo, je postal nosilni medij za domače bančništvo. Ovira je postala pomanjkanje računalnikov v družinah. Danes se stvari obračajo na boljše in s

tem v prid domačemu bančništvu. Računalniki so postali vsesplošno uporabni, računalniška pismenost je danes nekaj vsakdanjega in uporabniki lahko lažje komunicirajo s svojimi dobavitelji finančnih uslug (Kalakota, 1997, str. 188).
Ponudba e-bančništva s pravnimi osebami je v primerjavi s fizičnimi osebami precej bolj okrnjena. Podjetja imajo možnost dostopa v banko na tradicionalni način ali preko interneta. Banke so v sodelovanju s telekomunikacijskimi in informacijsko tehnološkimi podjetji, uporabnikom odprle nove poti za dostop do njihovih storitev, ne da bi za to morali oditi fizično v poslovalnico. Internetni dostop do storitev je v razvoju e-bančništva naredil velik korak naprej. Podjetja lahko pri e-plačilnem prometu podatke z banko izmenjajo na tri načine (Hrovat, 2000, str.54):

- izmenjava preko e-pošte,
- preko interneta ali
- preko odjemalnega programa.

Vsi trije načini se izvajajo preko internetnega omrežja, za kar jih lahko poimenujemo internetno bančništvo.

2.2.2 Internetno bančništvo

Internetno bančništvo omogoča opravljanje bančnih storitev kadarkoli (ne glede na delovni čas banke) in brez neposredne pomoči bančnega uslužbenca. S podporo sistemov bančništva na daljavo, lahko komitent opravlja vse negotovinske transakcije preko svojega računalnika, pregleduje stanje na svojih računih, izpisuje prometne postavke za izbrano obdobje, prenaša sredstva med svojimi računi itd. Vse transakcije, ki jih uporabnik sproži s svojega računalnika, potujejo neposredno v centralni bančni sistem brez posredovanja bančnega uslužbenca, ki je obveščen le o takšnih zahtevah komitenta, pri katerih so potrebne dodatne odločitve ali sodelovanje človeka. Internetno bančništvo koristi tako bankam kot podjetjem, saj se s tem znižujejo stroški storitev. Bankam predstavlja dodatno distribucijsko pot, ki jih nudi vrsto prednosti kot tudi groženj pred izgubo komitentov, saj zaradi nižjih vstopnih ovir prihajajo drugi nebančni finančni posredniki, ki predstavljajo bankam novo konkurenco.

Prva internetna banka, ki je omogočila elektronske bančne storitve za uporabnike preko interneta, je bila Security First Network Bank (SFNB[14]). Preden je dobila dovoljenje za poslovanje kot spletna banka, je morala zadovoljiti mnogim strogim predpisom. Tako je leta 1995 končno dobila zeleno luč, da je kot nekdanja First Federal Savings Bank of Pineville iz Kentuckija, sedaj kot SFNB, vstopila v virtualni svet e-bančnega poslovanja (Kalakota, 1997, str. 202).

Največ uporabnikov internetnega bančništva imajo v skandinavskih državah; na Švedskem štejejo kar 31% prebivalcev. Presenetljivo majhen delež ameriškega prebivalstva posega po

[1]8 Spletna stran Security Firs Network Bank. [URL: http://www.sfnb.com], 01.01.03.

omenjenih storitvah, za kar lahko vzroke iščemo v velikemu številu bank in njihovih podružnic, ki so dostopne na vsakem koraku. Po številu uporabnikov internetnega bančništva na vrhu pred vsemi vodi skandinavska banka Nordea največja regionalna banka v Evropi. Banka je rezultat uspešne čezmejne konsolidacije med finsko banko Merita, švedsko Nordbanken, dansko Unidanmark in norveško banko Christiania (Oman, 2002, str.17-21). Poleg skandinavske konsolidirane banke so najnaprednejše evropske banke na področju e-bančništva še angleška Barclays, švicarski Credit Suisse in UBS, španska Bankinter in nemška Deutsche Bank (Grenko, 2000b, str. 65-69.).

2.3 PREDNOSTI E-BANČNIŠTVA

Za bančništvo se postavljajo nove meje in novi izzivi; poslovanje s prebivalstvom, informiranje, fakturiranje in plačevanje računov bo postalo rutina, ki jo bo prevzemala avtomatizacija, papir bo izginil. Banke se bodo posvetile planiranju, analitičnim poslom in iskanju novih priložnosti. E-bančništvo je tako postalo obvezno. Banke ga uvajajo predvsem zaradi naraščajočega konkurenčnega pritiska. Glavne dejavnike za investiranje v rešitve e–bančništva lahko strnemo v tri kategorije (Škedelj, 2002):

- orientacija k sodobnim tržnim potem,
- izboljšane storitev strankam in
- razširitvijo strategija e-poslovanja.

Banke pozicionirajo e-bančništvo kot del celovite strategije tržne poti. Najnaprednejše banke gledajo na e-bančništvo kot na osnovo za širšo strategijo e-poslovanja. Ne glede na strategijo mora banka imeti realna pričakovanja. Nikakor se račun ne izide, če pričakuje povrnitev stroškov investiranja v e-bančništvo čez noč. Koristi se ne pokažejo takoj, ampak jih lahko pričakuje v daljšem časovnem razmiku. Tako lahko koristi rangiramo glede na čas. Kratkoročne koristi bančnega sektorja so v konkurenčni enakosti, zadrževanju komitentov ter pridobivanju novih strank. Srednjeročne priložnosti so integracija tržnih poti, upravljanje informacij, celovit pogled na komitenta, migracija komitentov na ustrezne kanale ter tudi znižanje stroškov. Pozitivni rezultati investicije v e-bančništvo se pokažejo šele po 18. mesecih, tako glede zmanjševanja stroškov kot povečanja prihodka (Škedelj, 2002).

Uporaba e-bančništva prinaša prednosti tudi za uporabnike bančnih storitev. Prednosti e-bančništva, ki jih z uporabo informacijske tehnologije vnaša v bančni sektor, so (Sjekloča, 1999, str 31-33):

- zmanjšanje stroškov bančnega poslovanja; manj papirja, nižje provizije,
- hitrejše, cenejše in kvalitetnejše poslovanje brez vrst pred bančnimi okenci,
- nove distribucijske poti uporabe storitev,
- širša ponudba uslug in storitev,

- povečanje učinkovitosti in transparentnosti trgov,
- zaradi multimedijske komunikacije je zanesljivost informacij enostavno preverljiva,
- hitrejše kroženje denarja in bolj redno plačevanje obveznosti,
- spreminjanje profila zaposlenih v bankah ter
- odpirajo se novi trgi, kjer izginjajo fizične meje.

Med končnimi uporabniki je z uvedbo e-bančništva prisotna določena mera razočaranja, ker ni pričakovanega takojšnjega zmanjševanja stroškov in povečanja prihodkov. Vendar lahko koristi pričakujemo le na dolgi rok in so tako kot pri bankah kratkoročne koristi vidne v nemerljivih dejavnikih.

2.4 RAZVOJNI TRENDI IN STRATEGIJE V E-BANČNIŠTVU

V 90. letih je celotno evropsko celino zajel proces koncentracije, močne konsolidacije bančne industrije in pospešen razvoj elektronskih distribucijskih poti, kar je bistveno spremenilo podobo evropskega trga finančnih storitev.

Razvojni trendi v evropskem bančništvu so usmerjeni predvsem v (Grenko, 2000a, str.36-41):

- konsolidacijo znotraj državnih meja ter prevzemi in združevanja med bankami različnih držav,
- pospešen razvoj elektronskih distribucijskih poti in
- usmerjanje v investicijsko bančništvo.

Temeljni razlogi za združevanja in prevzeme v bančni industriji so povečanje tržnega deleža, izboljšanje poslovanja družbe in s tem povečanje premoženja njihovih delničarjev. Banke želijo z združevanjem zmanjšati stroške, povečati produktivnost, zvišati dobiček in povečati kapital kot tudi racionalizirati poslovanje z učinkovito uporabo nove tehnologije, ki bankam omogočajo diverzifikacijo pri poslovanju in večjo fleksibilnost pri ponudbi storitev. Na evropskem bančnem trgu obstajajo številne ovire med posameznimi državami (različna podjetniška kultura, pravna ureditev, davčna zakonodaja), kar otežuje čezmejne združitve bank. Doslej je večina bančnih združitev v svetu potekala znotraj državnih meja med podobnimi institucijami.

Pospešen razvoj elektronskih distribucijskih poti je močno spremenil evropski bančni prostor. Prihodnost bank bo vse manj odvisna od razvoja samih bank, ampak vse bolj od tehnološkega napredka, saj bo sodobno bančništvo vse bolj odvisno od učinkovite izrabe informacijske tehnologije.

Z razvojem interneta bančništvo je oz. bo elektronski medij zamenjal tradicionalni model bančnega poslovanja prek bančnih poslovalnic e-bančništva. Banke, ki se bodo uspešno

vključile v trend virtualnosti, bodo lahko izkoristile ključne dejavnike in jih izkoristile v konkurenčni tekmi, ki poteka na evropskem trgu.

Banke glede na prihodnost e-bančništva lahko razdelimo v 4 kategorije (Škedelj, 2002):

- internetne banke,
- banke, ki ne nudijo e-bančništva,
- banke, ki nudijo osnovno e-bančništvo in
- pionirske banke.

Virtualne banke prinašajo vrsto prednosti; od lažjega premagovanja daljave, zniževanja stroškov poslovanja - do povečanja konkurenčnosti. Trend uspeha se kaže v reorganizaciji bank in sledenju novim strategijam, ki jih obdrži v boju za preživetje, kjer konkurenca prihaja tudi zunaj meja. Večje evropske banke si bodo prizadevale utrjevati tržni delež s povezovanjem z glavnimi internetnimi portali, tehnologijami in telekomunikacijskimi družbami. Nova razvojna pot žene banke, da si razširijo storitveni asortima z vključitvijo oz. povezavo z mobilnimi telekomunikacijskimi družbami, ki strankam omogočajo dostop do internetnih finančnih storitev z uporabo protokola WAP[15]. Pričakujemo lahko, da bo obdobju e-bančništva sledilo obdobje m-bančništva[16].

Konkurenca evropskih bank na področju internetnega bančništva se z internetno revolucijo posledično stopnjuje. Za ohranitev sedanjega tržnega deleža in krepitev odnosa s strankami je potreben prijazen nastop do uporabnikov s ponudbo cenejših in pestrejših bančnih storitev. Predvsem je pomembno »biti prvi«, kar zahteva od bank veliko inovativnost. V prihodnje bodo banke prek interneta ponujale nove vrste poslov, ki bodo povečali tržni delež. Strateške usmeritve na področju internetnega bančništva pa so usmerjene v (Grenko, 2000b, str. 65-69.):

- ustvarjanje novih prodajnih poti,
- vstop na nove geografske trge,
- povečanje tržnega deleža na domačem trgu in
- razvoj vloge interneta in dohodkovnih poti zunaj tradicionalnega poslovnega modela.

[15] Wireless Aplication Protocol – protokol, ki zagotavlja komuniciranje mobilnega telefona s svetovnim spletom.
[16] M-bančništvo je opravljanje bančnih storitev s pomočjo mobilnih naprav, kjer koli in kadar koli, saj tehnika temelji na brezžični povezavi preko WAP portala.

3 VARNOST ELEKTRONSKEGA POSLOVANJA

Z nastankom interneta se je razvil nov družbeni prostor, ki ga je nemogoče nadzorovati v celoti in ki omogoča tako stare kot tudi povsem nove oblike računalniške kriminalitete[17]. Omrežje internet samo po sebi ne zagotavlja potrebnih pogojev za varno komunikacijo in e-poslovanje. Varnost računalniških sistemov in drugih pomembnih virov, ki jih obravnavamo v sklopu računalniškega omrežja, je potrebno zaščititi z izbiro ustreznih tehnologij, metod in rešitev, s kombinacijo ukrepov ter jih povezati v celoto tako, da bo varnost komunikacije prek interneta največja.

Število možnih žrtev računalniške kriminalitete raste iz dneva v dan. Tako je že vsak uporabnik interneta postal potencialna možna žrtev (Power, 1998). Pri tem je opaziti, da naraščata tako obseg kot tudi raznovrstnost načinov in oblik izvajanja računalniškega kriminala. Zato nekatere, zlasti razvite države, ki so se že soočile z njimi, razmišljajo o zakonodajnih rešitvah, ki bi omogočile pregon tovrstnih kaznivih dejanj.

3.1 ZAKONSKI IN SODNI PREGON KAZNIVIH DEJANJ

Naloga sodobne kazenske teorije in prakse je, da te negativne pojave ugotovi in da jih predvidi v zakonodaji. Eden izmed takšnih pojavov je računalniška kriminaliteta. Računalniški kriminal je prisoten zlasti v gospodarsko bolj razvitih okoljih. Storilci tovrstnih kaznivih dejanj so deležni milejših kazni kot storilci klasičnih kaznivih dejanj, čeravno je škoda, povzročena z računalniškim kriminalom lahko izredno visoka.

Kazenski zakonik Republike Slovenije (v nadaljnjem besedilu KZ RS) dokaj natančno ureja kazniva dejanja, ki spadajo v sklop kriminalitete v zvezi z računalniki (KZ RS, april 1999):

- vdor v računalniško vodeno zbirko osebnih podatkov (drugi odstavek 154. člena),
- poškodovanje računalniških podatkov in programov (225. člen),
- vdor v informacijski sistem (242. člen),
- izdelovanje in pridobivanje pripomočkov, ki so namenjeni za vdor v informacijski sistem (tretji odstavek 309. člena) in
- neupravičeno izkoriščanje avtorskega dela - piratstvo (159. členu).

Kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali z zaporom do enega leta. Enako se kaznuje, kdor vdre v

[17] Računalniški kriminal je nasilno dejanja na računalniku, s čimer trpi žrtev zaradi nezakonite namere kršitelja. Računalniški kriminal je relativno nov pojem, ki se pojavil zaradi povečane uporabe računalniških sistemov za shranjevanje podatkov. Vse oblike organizacij, ki uporabljajo računalniške sisteme, so potencialne žrtve napada računalniškega napada (Forcht, 1994, str. 297). Danes se pojavljajo poleg klasičnih načinov kriminala tudi novejše oblike, ki so povezane s trendom v digitalni tehnologije. Glavne oblike nasilja računalniškega kriminala so: telekomunikacijske prevare, poneverbe kreditnih kartic in drugo, vdori v sisteme, nepooblaščeno reproduciranje izdelkov, otroška pornografija, organiziran kriminal, itd.

računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. Če stori dejanje uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

Kdor neupravičeno spremeni, zbriše ali kako drugače napravi podatke neuporabne, se kaznuje z zaporom do dveh let. Prav tako je poskus kazniv in se storilca kaznuje z zaporom od treh mesecev do petih let, če je pri tem povzročena velika premoženjska škoda.

Kdor pri gospodarskem poslovanju neupravičeno vnese, spremeni, skrije, izbriše ali uniči računalniške podatke ali programe, ali kako drugače vdre v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let. Če je bila s tem pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda, se storilec kaznuje z zaporom do petih let. Kdor izdela, si pridobi, proda ali da v uporabo pripomočke, ki so namenjeni za vdor v računalniški sistem, se kaznuje z zaporom do treh let.

Kot je iz opisanega mogoče razbrati, so kazni zelo mile in tudi klasifikacija kaznivih dejanj ne pokriva vseh kaznivih dejanj na področju računalniškega kriminala. Ker se te vrste kaznivih dejanj močno širijo je potrebno v prihodnje razširiti kvalifikacije kaznivih dejanj in dosledno zajeti vse načine nelegalnega delovanja z računalniško opremo.

3.2 GROŽNJE IN NEVARNOSTI INTERNETA

Predpisane kazni na področju računalniške kriminalitete ne zagotavljajo, da bi storilce teh vrst kaznivih dejanj odvrnile od nelegalnih dejanj, zato je potrebno za zagotavljanje varnosti in zaščite podatkov za vzpostavitev varnega elektronskega poslovanja, namestiti še druge učinkovite načine varovanja. Način zagotavljanja varnosti je odvisen od vrednosti virov, potencialnih groženj in učinkov groženj. Z razvojem e-poslovanja je globalna značilnost digitalnih in omrežnih tehnologij pospešila izmenjavo informacij, olajšala dostop, obdelavo in shranjevanje podatkov. Največkrat poteka posredovanje podatkov neposredno preko interneta, kar povečuje možnost zlorabe zbranih podatkov (Perše, 2000, str. 11).

Računalniški kriminal je splošen izraz za kakršnokoli uporabo računalniških sistemov pri nezakonitih dejanjih. Razdelimo ga lahko na dvoje glavnih področij:

- tatvina s pomočjo informacijskega sistema,
- sabotaža in vandalizem.

Med najpogostejšimi načini tatvin s pomočjo informacijski sistem uvrščamo; tatvine s pomočjo informacijskega sistema, tatvine z vnosom napačnih podatkov, s spremembo računalniškega programa in s tatvino podatkov iz informacijskega sistema. Zlonamerna

programska oprema je način vandalizma ali sabotaže, ki ima za osnovni namen povzročanje škode, izgube ali vohunjenje.

Že leta 1949 je matematik John von Neumann ugotovil obstoj programov, ki se lahko sami reproducirajo. 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 e-pošte. Prevladujoče skupine zlonamerne programske opreme so (Pečenko, 2002, str. 62):

- virusi,
- trojanski konji,
- črvi in
- kombinirani virusi.

Računalniški virusi so najbolj znana skupina zlonamerne programske opreme, ki se lahko razmnožujejo in širijo podobno kot biološki virus. Z okužitvijo izvajalne datoteke se virus razširi na druge programe. Nekateri virusi so narejeni tako, da sprožijo svoje uničujoče aktivnosti ob določenem času (časovne bombe) ali ko je izpolnjen določen pogoj (logične bombe). Včasih so se virusi širili predvsem s pomočjo prenosnih medijev, danes pa v glavnem s priponami e-pošte ali pa preko datotek, ki jih dobimo preko interneta[18], kot tudi z uporabo nelegalnih računalniških programov.

Trojanski konj je računalniški program, ki vsebuje skrite ukaze, ki se izvršujejo v primeru, ko je izpolnjen določen pogoj. Program se ne zna sam razmnoževati kot pri virusu. Namesto tega ponudijo uporabniku kakšno zanimivost, v ozadju pa počno druge nedovoljene reči, npr. ko je v obdelavi zapis z določenim bančnim računom, pride do nepričakovanih posledic, ki lahko ostanejo skrite in jih napadalec v ozadju počne v imenu uporabnika[19].

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[20].

---

18 Primer takega virusa sta virusa Melissa (marec 1999) in Love Letter (maj 2000).

19 V mesecu oktobru 2002 se je v zvezi z Novo ljubljansko banko pojavil 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 je bil 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, saj mu je uporabnik kar sam priskrbel vse potrebno. Trojanski konj je bil 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. S tem bi bila lahko ogrožena varnost Klik-a pri uporabniku, ne pa pri banki.

20 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.

Omenjene skupine zlonamerne programske opreme so le ena vrsta groženj, ki ogrožajo varnost računalniškega sistema. Grožnje zlorabe virov so lahko naključnega ali namernega značaja ter lahko delujejo pasivno ali aktivno. Slednje pomeni, da nekdo aktivno uporablja pridobljene podatke, jih pretvarja, ponareja, nepooblaščeno uporablja vire, spreminja in onemogoča delo z njimi ali pa jih pasivno zlorablja s prisluškovanjem (Jerman Blažič, 2001, str. 100).

Storilci računalniškega kriminala so najbolj pogosto programerji, uradniki, študenti, managerji, sistemski analitiki, operaterji in drugi uporabniki informacijskih sistemov. Razvrstimo jih lahko v tri skupine:

1. zaposleni v institucijah
2. storilci izven institucij (krekerji) in
3. računalniški zagnanci (hekerji).

Statistika dokazuje, da več kot polovico nedovoljenih dostopov do podatkov zagrešijo uslužbenci v podjetju. Podjetja vse pogosto ne zasledujejo miselnosti razvoju tehnologije. Lep primer takšne miselnosti so podjetja, ki so obdana s takšno ali drugačno ograjo, ki jo skrbno nadzorujejo varnostniki, medtem ko za varnost elektronskih podatkov ne skrbi nihče. Večina varnosti je namenjena zunanjim grožnjam, medtem ko na notranje napade vse pogosto pozabljajo. Zaposleni v institucijah poznajo način poslovanja in imajo dostop do informacijskih sistemov, ki jih nepooblaščeno izkoriščajo za svoja nelegalna dejanja. Storilcem izven institucije je težje, ker morajo prodreti v informacijski sitem, za katerega ne vedo, kako delujejo.

Za računalniške zanesenjake (hekerji) pa je značilno, da jih v računalniški kriminal ne vodi osebna korist ali škoda, ki jo povzročijo, ampak gre pri njih za intelektualni izziv in v informacijski sistem vdirajo za zabavo. Pogosto se zamenjuje pojem heker in kreker, ki se pogosto pojavljata kot glavna akterja pri zlorabah interneta. Glavna razlika med njima je, da hekerja definiramo kot osebo, ki pogosto dokazuje svoje sposobnosti, moč in dovršenost ter odkriva luknje v računalniških sistemih iz različnih vzrokov. Hekerji tako nenehno težijo k iskanju novega znanja, k dokazovanju svojih sposobnosti, ki pa znanje pogosto delijo z ostalimi, pri tem pa ne uničujejo in si ne prilaščajo oz. koristijo podatkov, ki bi lahko škodili ostalim udeležencem na internetu. Zato so hekerji pogosto osebe, ki so strokovnjaki s področja programskega jezika in računalniških sistemov. Ker pa jih ljudje pogosto ocenjujejo kot negativne osebe, da nezakonito vdirajo v sisteme, jih nekateri delijo na »white-hat« in na »black-hat«, glede na njihov motiv (Turban, 2003, str. 393). Krekerja lahko prav tako definiramo ko osebo, ki vdira v računalniška omrežja, vendar ne z namenom iskanja novega znanja temveč z namenom povzročati težave svojim »tarčam«, uničiti sistem ali izvajati nezakonite aktivnosti, kot sta kraja in vandalizem.

Na informacijski sistem ne pretijo le kriminalci, ampak tudi nevarnosti uničenja sistema, zaradi naravnih nesreč ali tehničnih okvar.

3.3 OPREDELITEV VARNOSTNIH KOMPONENT

Za zagotovitev varnosti so na voljo različne kombinacije programske in strojne opreme ter fizičnega varovanja. Vodstvo je odgovorno za postavitev temeljne varnostne politike, kjer mora jasno definirati, kaj ščiti in zakaj ter določiti, koliko sredstev je potrebno vložiti v varnostne ukrepe. Ukrepi morajo biti postavljeni široko, saj je težko vnaprej predvideti smer napada. Obseg varnostnih komponent je odvisen od stopnje zahtevane zaščite in oblike sistema.

Varnostna politika je kompromis med stroški in tveganji. Sistem je varen, ko imajo napadalci večje stroške od koristi vdora v sistem. V bančnih krogih je ta problematika še toliko bolj pomembna in občutljiva, saj operirajo s finančnimi podatki od svojih komitentov. Stroški vdora v bančni sistem imajo lahko za posledice vidne (prenos denarja, koristoljubnost, izguba komitentov, izguba poslov, zloraba podatkov, itd.) kot tudi nevidne (nezaupanje, zmanjšanje ugleda, itd.) posledice, ki pogosto rezultirajo posredno na vidne stroške (Kuščar, 2002, str. 8).

Osrednja točka varovanja pri e-poslovanju so viri[21], zoper katere preti nevarnost in imajo za lastnika določeno vrednost. Organizacija mora za zagotavljanje varnosti zadostiti naslednjim varnostnim storitvam (Jerman Blažič, 2001, str. 101):

- overjanje; možnost preveriti identiteto subjekta,
- zaupnost; informacije ne smejo biti razkrite nepooblaščenim osebam,
- neokrnjenost; ohranjanje pristnosti podatkov,
- nadzor dostopa; preprečevanje nepooblaščene uporabe,
- preprečevanje zanikanja o sodelovanju v aktivnostih e-poslovanja ter
- razpoložljivost; storitve e-poslovanja stalno na voljo.

Za zagotovitev omenjenih varnostnih storitev so na voljo različne metode. Njihova izbira je odvisna od zahtevanih varnostnih storitev, stopnje zaščite in oblike sistema. Vrste metod za zagotovitev varnosti v e-poslovanju so:

- kriptografija,
- elektronski podpis,
- požarni zid,
- gesla in drugo.

[21] Splošne kategorije virov so: podatki, informacije pri prenosu in hranjenju, strojna in programska oprema, uporabniki in odnosi med njimi ter dokumentacija o postopkih, strojne in programske opreme v sistemu ali omrežju (Jerman Blažič, 2001, str. 100).

3.4 KRIPTOGRAFIJA

Kriptografija (tajnopisje, šifriranje, kodiranje) je veda o tajnosti, šifriranju, zakrivanju sporočil in o razkrivanju šifriranih podatkov (kriptoanaliza) s pomočjo matematičnih postopkov. Uporablja se za zaščito občutljivih informacij med prenosom po javnih omrežjih in zagotavlja zaupnost podatkov in kontrolo dostopa. V kriptografskem sistemu se sporočilo šifrira s pomočjo kriptografskega algoritma in ključa. Uporabljajo se kode in šifre za preoblikovanje sporočil, tako da jih lahko prebere le naslovnik, ki pozna način za dešifriranje.

3.4.1 Zgodovina šifriranja

Šifriranje se je razvilo za vojaške potrebe, za tajno pošiljanje sporočil. Vendar je eden prvih kriptografov bil Julij Cezar, ki naj bi svojim prijateljem pisal z uporabo preproste zamenjalne šifre, ki vsako črko zamenja s črko, ki je v abecedi za tri mesta za njo. Danes pojmujemo Cezarjevo šifro vsako šifro, v kateri je določena abecedna razdalja od običajne črke do šifrirane črke.

V 2. svetovni vojni so Nemci za šifriranje uporabljali močnejši kriptografski sistem s poliabecedno šifro[22]. Za šifriranje sporočil so uporabljali zelo zapleten šifrirni stroj Enigma[23]. Angležem je kljub zagotovilom, da sporočil ni mogoče dešifrirati jim je pod vodstvom Alana Turinga to uspelo.

3.4.2 Delitev šifrirnih sistemov

V preteklosti so razvili več vrst različnih šifrirnih sistemov. V grobem lahko ločimo dve vrsti:

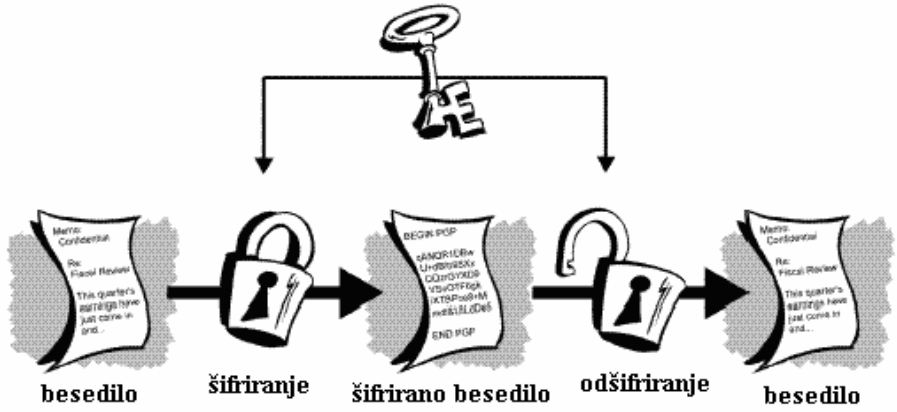
- simetrična kriptografija - kriptografija z zasebnim ključem in
- asimetrična kriptografija - kriptografija s parom ključev.

Doslej našteti algoritmi, ki so se v pretežni meri uporabljali v zgodovini, spadajo pod simetrične algoritme ali algoritme z zasebnim ključem. Imamo samo en ključ, katerega uporabljamo za šifriranje in dešifriranje sporočil (glej Slika 2).

[22] Način šifriranja, kjer so črke v abecedi v običajnem besedilu nadomestile različne črke v šifriranem besedilu glede na njihov položaj v sporočilu. Te šifre uporabljajo ključ – število, ki ga morata poznati pošiljatelj kot prejemnik.

[23] Stroj je bil sestavljen iz baterije, tipke za črke kot pri pisalnem stroju, luči za vsako črko in treh rotorjev, ki so predstavljali srce stroja. Vsak rotor je bil plošča z obročem električnih priključkov na vsaki strani. Rotor je imel na vsaki ploskvi dvakrat po 26 kontaktov (kolikor je črk), v notranjosti valja povezanih med seboj z žicami, ki so prenašale električne signale od priključka na eni strani, vse do priključka na drugi strani zadnjega rotorja, vendar ne urejeno (kontakt št.1 na prvi ploskvi ni bil povezan s kontaktom 1 na drugi ploskvi). Operator je vtipkal sporočilo na tipkovnico. Ko je vtipkal posamično črko, se je prižgala žarnica, ki je kazala šifrirano črko. Ko je šifrirano sporočilo doseglo cilj, so stroj nastavili tako kot prvega. Šifrirano sporočilo so vtipkali na tipkovnico in na žarnicah se je pojavil izvirnik (Wright, 2002, str. 154-155).

Slika 2: Simetrično šifriranje z enim samim ključem

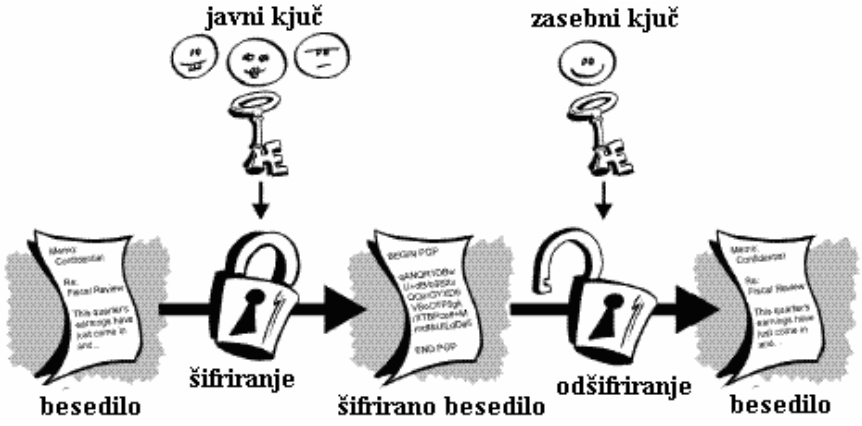


Vir: NA, 1999, str. 15.

Prednosti simetričnih šifrirnih sistemov je v hitrosti in omogoča šifriranje večje količine podatkov. Slabost se kaže v težavah pri distribuciji ključev. Zato simetrično šifriranje uporabljajo predvsem v vojski in bankah, kjer je mogoče te skrivne ključe razpečevati po posebnih varnih kanalih. Druga težava, ki se pojavlja pri simetričnih postopkih šifriranja, je kopičenje skrivnih ključev. Kajti pri simetričnih postopkih šifriranja uporabljamo samo en ključ za šifriranje in dešifriranje, tako moramo za vsakega poslovnega partnerja uporabiti drugačen skrivni ključ. Število ključev tako postane neobvladljivo že pri majhnem številu uporabnikov. Uporabni so v kombinaciji z drugimi algoritmi, ki omogočajo varno izmenjavo ključev, ali v manjši skupini uporabnikov, kjer problem izmenjave ključev ni problematičen. Slabost se kaže tudi v nezmožnosti uporabe za digitalni podpis. Ravno zaradi teh slabosti so se razvile asimetrične metode ali algoritmi z javnim ključem.

Začetki uporabe asimetričnih šifrirnih sistemov segajo v leto 1975. Zgrajeni so iz dveh ključev v paru (glej Slika 3). Eden je zasebni, ki je poznan le uporabniku, in javni, ki je dostopen vsem (kot telefonska številka v imeniku).

Slika 3: Asimetrično šifriranje z dvema ključema



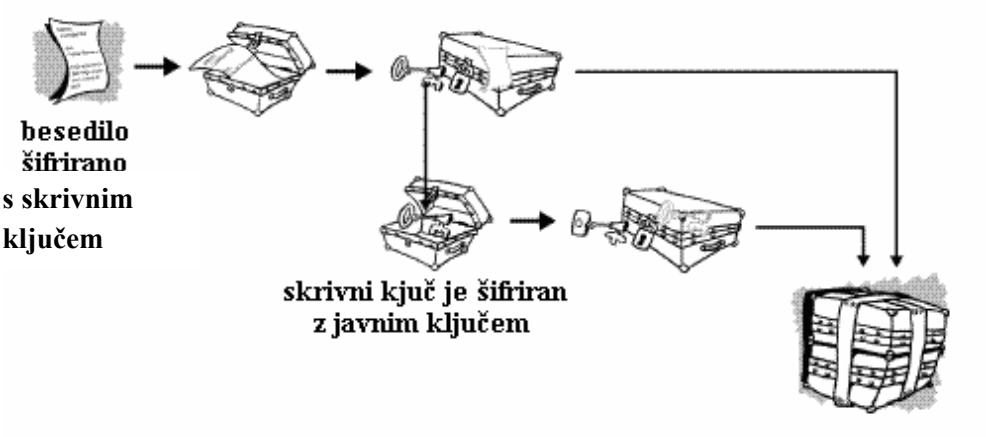
Vir: NA, 1999, str. 15.

Ključi nastopajo v parih, ki so povezani s konkretno matematično funkcijo, imajo pa lastnost, da iz enega ključa brez poznavanja dodatnih informacij, ni mogoče določiti preostalega. Javni ključ javno objavimo, drugi ključ iz para - zasebni ključ, mora biti varno shranjen pri lastniku (Blažič Jerman, 2001, str.103).

Prednost asimetrične kriptografije je v relativno enostavni distribuciji ključev. Ne glede na število vseh uporabnikov imamo le en par ključev. Zaradi računsko bolj zahtevnih metod, poteka šifriranje in dešifriranje relativno počasi in je neprimerno za večjo količino podatkov. Uporabljajo se v kombinaciji z drugimi načini.

Danes je najbolj razširjen način šifriranje, kombinirano šifriranje, ki združuje prednosti obeh pristopov. Pri tem postopku šifriramo dokumente po klasičnem simetričnem postopku. Ker je postopek šifriranja simetričen, naključno izbrani ključ asimetrično šifriramo z javnim ključem prejemnika in mu ga pošljemo skupaj s šifriranim dokumentom. Prejemnik najprej s svojim zasebnim ključem dešifrira simetrični ključ in šele s pomočjo tega ključa nato dešifrira dokument (glej Slika 4). Tako smo ohranili vse prednosti asimetričnega postopka in pridobili na hitrosti, ki je sedaj enaka klasičnim simetričnim postopkom.

Slika 4: Prikaz kombiniranega šifriranja



Vir: NA, 1999, str. 16.

3.4.3 Vrste algoritmov

Za šifriranje podatkov v e-poslovanju so na voljo številni algoritmi. Najbolj znani simetrični algoritmi so[24]:

- DES - Data Encryption Standard,
- trojni DES,
- RC2, RC4, RC5,

[24] Osnovni pojmi in nekaj primerov. Simetrični algoritmi. [URL: http://www.sigov.si/tecaj/seminar.html], 30.08.2002

- IDEA - International Data Encryption Algorithm,
- AES - Advanced Encryption Standard in
- drugi: Blowfish, CAST, ipd.

Algoritem DES je uporabljal ključ velik 56 bitov, 2^{56} je vseh ključev oz. približno 10^{17}. To je premajhna količina ključev za današnje zmogljive računalnike, saj lahko napadalec preizkusi vse možne ključe v enem dnevu in odkrije tistega, ki dešifrira sporočilo. Algoritem DES zaradi prekratkih ključev ni več priporočljivo uporabljati. Zato je Ameriški nacionalni inštitut za standarde in tehnologijo vladne administracije NIST (National Institute of Standards and Technology) septembra leta 1997 razpisal natečaj za naslednika algoritma DES, ki naj bi bil močnejši in hitrejši od trojnega DES. Izbran je bil algoritem AES, ki ponuja možnost treh dolžin ključev: 128, 192 in 256 bitov. Simetrični algoritem RC4 je vgrajen v brskalnike kot del protokola SSL[25] oziroma TLS[26]. Je tekoč z variabilno dolžino ključa do 2048 bitov. RC5 je bil objavljen leta 1994, pri katerem lahko uporabnik sam določi dolžino ključa, velikost bloka in število ponovitev šifrirnega postopka. Kriptosistem IDEA se uporablja pri šifriranju sporočil e-pošte. Uporablja ključ velikosti 128 bitov na 64 bitov dolgih blokih. Dolžina ključa je dovolj velika, da z navadnim računalnikom ni moč poiskati pravilnega ključa.

Najbolj uporabljen asimetrični kriptosistem je RSA, ki je dobil ime po avtorjih Rivers, Shamir, Adleman in je bil zasnovan leta 1968 na ameriškem inštitutu MIT[27]. Algoritem temelji na celoštevični algebri in izkorišča lastnosti velikih praštevil. Prednost algoritma je v tem, da uporabniku ob menjavi ključa ni potrebno razpošiljati novega ključa po vsem sistemu, ampak zgolj lokalno ponovi izračun in objavi spremenjen javni ključ. Šibka točka algoritma je počasnost. Vzrok zato tiči v potenciranju dveh zelo velikih števil, ki jih potrebujemo za šifriranje in dešifriranje. Računska operacija je zelo zahtevna in zato tudi počasna.

Za varnost je zelo pomembno, da je velikost ključev čim večja in s tem tudi število ključev, ki so na voljo za preizkušanje. Minimalna velikost ključev se z leti povečuje, zaradi vedno bolj zmogljivih računalnikov. Za varovanje zaupnih podatkov so potrebni algoritmi z velikimi ključi. Pri šifriranju je zaželeno, da se uporablja vsaj 73 bitov velik simetrični ključ ali pri asimetričnih algoritmih ključ velikosti 1108 bitov za uporabo v organizacijah oziroma ključ dolžine 2048 bitov v izredno pomembnih operacijah.

Lenstra in Verhuel sta pripravila tabelo za primerjavo varnosti različnih postopkov. S pomočjo tabele lahko enostavno ugotovimo, katere postopke za šifriranje še lahko uporabljamo, katerih pa ne več (glej Tabela 3).

[25] Secur Sockets Layer
[26] Transport Layer Security
[27] Massachusetts Institute of Technology.

Tabela 3: Primerjava dolžin ključev ob enaki varnosti glede na leto

Obdobje zaščite podatkov	Najnižji nivo varnosti za simetrične algoritme	Najnižji nivo varnosti za asimimetrične algoritme
1982	56	417
1990	63	622
2000	70	952
2002	72	1028
2004	**73**	**1108**
2010	78	1369
2020	86	1881
2030	93	2493
2040	101	3214

Vir: Lenstra, Verhaul,1999.

3.5 ELEKTRONSKI PODPIS

Pri uporabi simetrične kriptografije so se pokazale tri osnovne pomanjkljivosti:

- problem razpošiljanja simetričnih ključev,
- problem preprečevanja zanikanja in
- problem neokrnjenosti podatkov.

Samo šifriranje sporočil na omrežju ne zagotavlja vse potrebne varnostne storitve, ki sem jih omenila kot potrebne varnostne zahteve za varno in zanesljivo pošiljanje informacij po omrežju. Z uporabo sistema asimetrične kriptografije, odpravimo problem razpošiljanje ključev. Še vedno pa obstaja nevarnost in dvom, da je bilo sporočilo med prenosom spremenjeno kot tudi problem ugotavljanja identitete subjekta s katerim komuniciramo. Prejemnik nima zagotovila, da je na drugi strani tista oseba, za koga se izdaja. Zato se je razvilo elektronsko podpisovanje sporočil, kjer elektronski podpis nadomesti lastnoročnega ter zagotavlja pristnost podatkov kot tudi identifikacijo podpisnika.

Poznamo več oblik elektronskega podpisovanja. Enostavne metode na podlagi simetričnih algoritmov, ne zagotavljajo visoke stopnje varnosti kot to omogočajo metode na podlagi asimetričnih ključev. Elektronski podpis, ki je dobljen z elektronsko tehnologijo, za razliko od digitalnega podpisa, ki pa ga dobimo z asimetričnim šifrirnim postopkom, ne omogoča neokrnjenost podpisanega dokumenta in identifikacije podpisnika (Toplišek, 1998, str. 30).

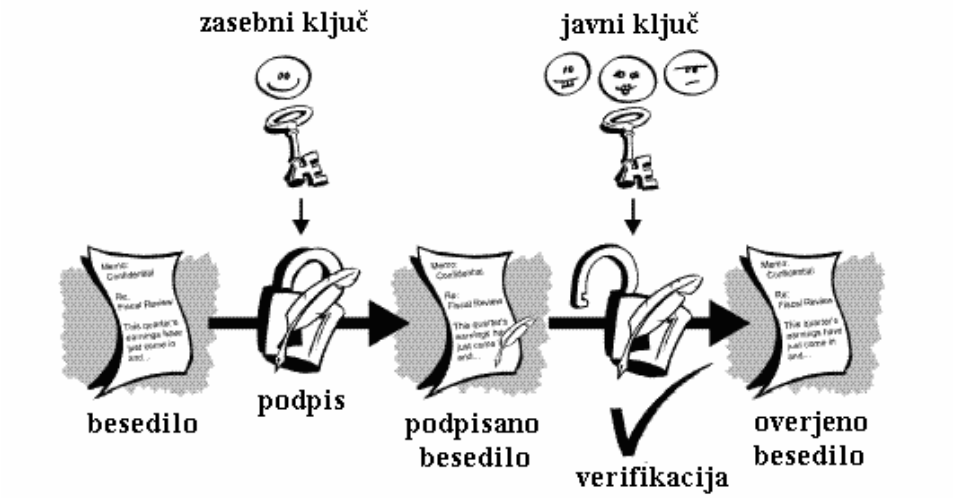
Da bi zagotovili istovetnost lastnoročnega podpisa z digitalnim podpisom, mora podpis zadostiti naslednjim zahtevam:

- avtentičnost,
- podpisa se ne da ponarediti,

- podpisa se ne da kopirati,
- podpisanega dokumenta se ne da spremeniti in
- podpisa se ne da zanikati.

Podpisovanje dokumenta poteka v dveh fazah. V prvi fazi podatke skrčimo z eno izmed enosmernih zgoščevalnih funkcij, ki poljubno dolgo besedilo preslika v blok konstantne dolžine. Dobljen blok, ki predstavlja »prstni odtis« besedila šifriramo s svojim zasebnim ključem in tako dobimo digitalni podpis. Pri preverjanju podpisa naslovnik z javnim ključem pošiljatelja (podpisnika) dešifrira podpis in dobi povzetek. Ponovno izračuna povzetek pisma, ki je bilo poslano v nešifrirani obliki z isto zgoščevalno funkcijo kot pošiljatelj. Če se ujemata, pomeni, da je dobil tak dokument, kot ga je pošiljatelj podpisal. Če pa sta različna, je dokument podpisal nekdo drug ali je bila vsebina dokumenta spremenjena. Bistvo poteka digitalnega podpisovanja je, da podpisujemo s svojim zasebnim ključem, podpis pa preverimo z javnim ključem podpisnika.

Slika 5: Prikaz podpisovanja elektronskih dokumentov



Vir: NA, 1999, str. 19.

Uporabnik lahko uporablja isti par ključev za šifriranje in digitalno podpisovanje, vendar to ni priporočljivo, ker se varnostne zahteve v obeh primerih razlikujejo. Zasebni ključ, ki ga uporablja za podpisovanje mora generirati in poznati le njegov lastnik, saj le tako lahko podpis dejansko določa podpisnika. Zasebni ključ, ki se uporablja za šifriranje, pa je včasih nujno, da ga pozna še kdo drug. Tukaj zasebni ključ ne identificira subjekta, ampak omogoča izdelavo šifriranih podatkov.

Z digitalnim podpisom zagotovimo pristnost podatkov in s tem tudi identifikacijo osebe. Vendar se pri tem postavljajo vprašanja, ali smo prepričani, da ključ res pripada naslovniku šifriranega sporočila oz. domnevnemu podpisniku podpisanega sporočila.

3.5.1 Digitalno potrdilo

Digitalno potrdilo je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo ali institucijo ali strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Je sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica), s specifičnim namenom; zagotavljanje varnega in legitimnega e-poslovanja. Potrdilo vsebuje javni ključ in informacijo o njegovem imetniku, ki jo podpiše oseba ali institucija, ki ji zaupamo. Potrdila so objavljena v splošno dostopnih imenikih ali na spletnih straneh.

Digitalno potrdilo je digitalno podpisan računalniški zapis, ki vsebuje naslednje podatke:

- različica formata,
- serijska številka potrdila,
- identifikator algoritmov,
- ime agencije, ki izdala potrdilo,
- obdobje veljavnosti potrdilo,
- ime lastnika javnega ključa,
- javni ključ in identifikator lastnika,
- enolična oznaka uporabnika (samo v verzijah 2 in 3),
- razširitve in
- digitalen podpis teh podatkov, ki je narejen z zasebnim ključem.

Overjanje javnih ključev je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetrični kriptografiji. Preverjanje povezave med uporabnikom in njegovim ključem omogočajo v e-poslovanju posebne ustanove, imenovane overitelji javnih ključev.

3.5.2 Overitelj javnih ključev

Overitelj oz. agencija za certificiranje javnih ključev (AC) predstavlja ustanovo, kateri zaupajo njeni komitenti - imetniki digitalnih potrdil. S tem jo tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Overitelj izdaja lastniku javnega ključa digitalno potrdilo, s katerim zagotavlja drugim uporabnikom avtentičnost ključa oziroma neločljivo veže uporabnika in njegov javni ključ. S pomočjo tega potrdila lahko lastnik dokaže lastništvo ključa in s tem tudi svojo identiteto[28].

Poleg agencij za overjanje javnih ključev imajo pomembno vlogo tudi uradi za registriranje (RA), ki sodelujejo pri izvajanju nalog CA. Razlika med agencijama (CA) in uradi (RA) je v tem, da agencija izda uporabniku digitalno potrdilo, s katerim jamči, da javni ključ res pripada lastniku potrdila, medtem ko so RA uradi, ki ne izdajajo potrdilo, ampak preverjajo

[28] Osnove tehnologije elektronskega poslovanja in elektronskega podpisa. URL:http://www.gov.si/cvi/slo/index_slo.htm, 20.06.2002.

dokumente in registrirajo naročnika, ki zaprosi za potrdilo, preverijo njegovo identiteto in poznavanje javnemu ključu pripadajočega zasebnega ključa.

V svetu obstaja veliko različnih agencij za certificiranje javnih ključev. V Sloveniji imamo kar nekaj overiteljev javnih ključev, ki izdajajo potrdila za posamezna področja. Za potrebe javne uprave in za uresničevanje projekta e-poslovanja javne uprave, je bil ustanovljen overitelj digitalnih potrdil na Centru vlade RS za informiranje (CVI), ki izdaja dve različici digitalnih potrdil:

- SIGOV-CA (Slovenian GOVernmental Certification Authority), katerih digitalna potrdila so namenjena uporabi v javni upravi ter
- SIGEN-CA (Slovenian GENeral Certification Authority), katerih digitalna potrdila so namenjena pravnim in fizičnim osebam za izmenjavo podatkov z institucijami javne uprave in za dostop do podatkov, ki so v skrbništvu javne uprave.

Za komercialne potrebe izdajajo potrdila na Trade point Slovenija ter še nekatere komercialne organizacije, kot so banke, ki izdajajo CA svojim klientom za varno e-bančništvo. V Sloveniji sta jih kot prvi začeli uporabljati NLB (1999) v aplikaciji KLIK in SKB v aplikaciji SKBNet. Vsaka banka ima svojo službo za izdajanje digitalnih potrdil in izdano potrdilo je uporabno samo za dostop do bančnih aplikacij ustrezne banke.

3.5.3 Infrastruktura javnih ključev

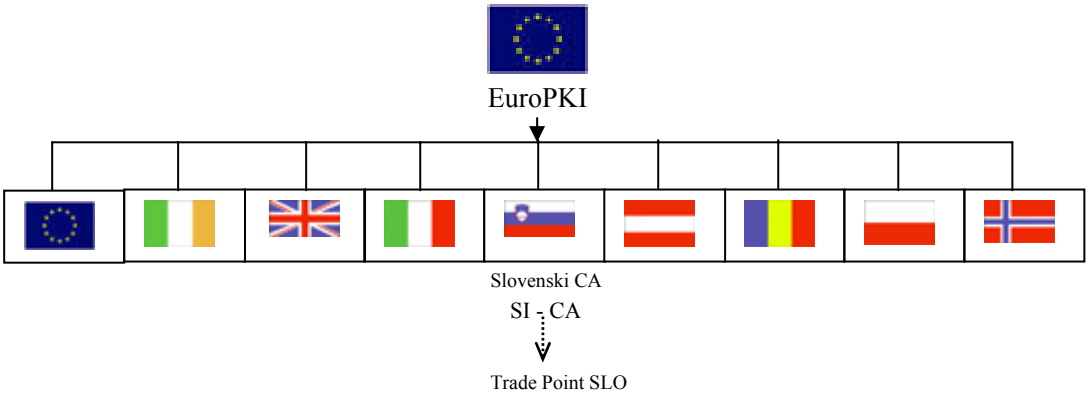
Infrastruktura javnih ključev (PKI – Public Kay Infrastructure) je sistem za upravljanje s ključi in digitalnimi potrdili, ki omogočajo vzpostavitev potrebnega zaupanja za e-poslovanje. Je kombinacija programske in strojne računalniške opreme ter politike in pravil certificiranja. Osnovna naloga PKI je omogočati varno e-poslovanje uporabnikom, ki se med seboj ne poznajo in želijo varno komunicirati z uporabo asimetrične kriptografije. Podobno kot je nastajal sistem elektronskih naslovov in imen računalnikov, so začele nastajati posamezne infrastrukture javnih ključev, ki jih vpeljujejo vlade (Kanada, ZDA, Singapur, nekatere evropske države) ali posebne organizacije (Verisign, Thawte, EuroTrust). Te doslej še niso povezane med seboj, tako da lahko komunicirajo med seboj samo člani posamezne infrastrukture.

Pomembnejše storitve PKI so:

- generiranje, upravljanje, distribucija in hranjenje javnih ključev
- overjanje ključev in izdajanje digitalnih potrdil javnih ključev,
- objavljanje digitalnih potrdil,
- preklicevanje digitalnih potrdil in
- časovna označitev postopkov.

Ključi se lahko uporabljajo za različne namene in v različnih okoljih (e-bančništvo, državna uprava, medorganizacijsko poslovanje, vojska, itd.). Vsako okolje zahteva različno stopnjo varnosti in specifično strukturo PKI. Ena redkih PKI, katerih namen je združevanje CA iz različnih držav, je EuroPKI, ki je vrhovna agencija (glej Slika 6).

Slika 6: Struktura EuroPKI



VIR: Spletna stran Europki, 29.01.2003.

Del te infrastrukture je tudi slovenska agencija za certificiranje SI-CA, katera podpisuje javne ključe drugih slovenskih overiteljev.

PKI je potrebna za vse storitve, katerih varnost se zagotavlja na podlagi asimetrične kriptografije, med njimi je tudi e-bančništvo. Na tem področju je ustanovljena vrhovna agencija - Identrus, ki so jo ustanovile največje svetovne finančne organizacije z namenom ponujanja globalnih storitev e-poslovanja med podjetji. Ključne lastnosti so globalni pristop, uporaba standardov odprtih sistemov, konsistentni poslovni proces in ocena tveganja pri e-poslovanju. Sistem je zasnovan na hierarhični infrastrukturi javnih ključev, ki povezuje sodelujoče banke s celega sveta (Jerman Blažič, 2001, str 152).

Uporaba kriptografije za zagotavljanje varnosti, danes ne zadostuje, zato si organizacije pomagajo še z dodatnimi mehanizmi, ki zaokrožajo neko varnostno celoto. Te so požarni zid, pametna kartica, uporaba gesel, varnostni protokoli itd.

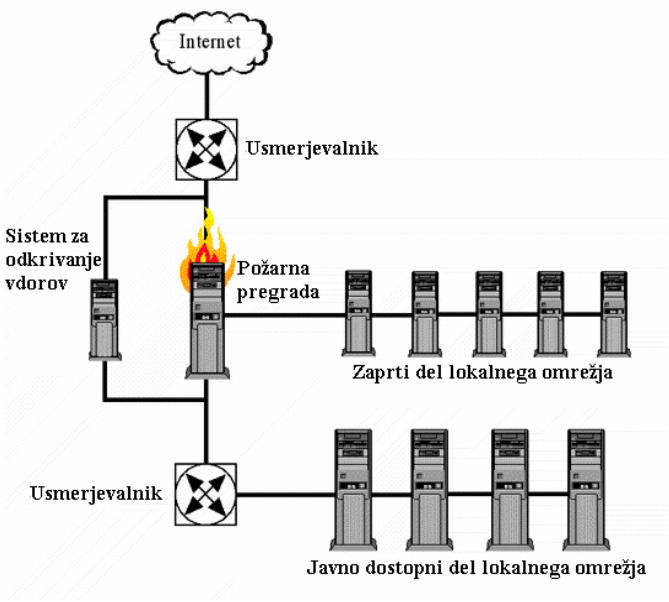
3.6 POŽARNI ZID

Požarni zid si lahko predstavljamo kot varnostna vrata ali vratarja, ki nepooblaščenim osebam ne dovoli vstopa v sistem, po drugi strani pa ne dopušča odnašanja podatkov iz sistema. Požarni zid z ustrezno strojno in programsko opremo implementira varnostno politiko v zvezi z uporabo virov in sistemov v internem lokalnem omrežju.

Osnovna zahteva pri postavitvi požarne pregrade je, da imajo vsi uporabniki lokalnega

omrežja čim manj oviran dostop do javnega omrežja, iz omrežja internet pa v lokalno omrežje prepuščamo le povezave do javnih strežnikov (glej Slika 7).

Slika 7: Osnovni model zaščite lokalnega omrežja



Vir: Young-Seock, 2000.

Požarna pregrada je tako namenjena preverjanju podatkov, ki se prenašajo med lokalnim omrežjem in internetom. Filter je tista komponenta požarnega zidu, ki nad vsakim paketom izvede množico pravil iz varnostne politike, določenih s strani administratorja. Pravila temeljijo na selektivni osnovi, ki filtrira vhodne dostope v svoje omrežje, gleda na pravila, ki lahko temeljijo na uporabniških imenih, internetnih IP naslovov pošiljatelja ali prejemnika, imenih domen, številkah komunikacijskih vrat itd. (Kalakota, 1997, str. 125).

Požarni zid ne more varovati virov podjetja pred napadi notranjih sodelavcev, saj je le vmesnik med internim omrežjem podjetja in internetom ali vmesnik med posameznimi oddelki podjetja, kot je to običajno v večjih podjetjih. V vsakem primeru lahko zaposleni v podjetju ukrade ključne informacije podjetja in poškoduje poslovne vire, ne da bi se to prikazalo na požarnem zidu. Tovrstne nevarnosti moramo rešiti z ustreznimi overitvenimi postopki (Collin, 1998).

3.6.1 Vrste požarnih zidov

Poznamo več funkcijskih konceptov delovanja požarnih zidov. Ločimo jih glede na nivo kontrole paketov v modelu TCP/IP[29] v tri glavne kategorije (Cheswick, 1994, str.51):

[29] TCP/IP - Transport Control Protocol / Internet Protocol je komunikacijski protokol, ki je skupen dogovor za delovanje v omrežju internet. Sestavljen je iz 4 plasti: plast povezave gostitelj – omrežje, medomrežna plast, transportna plast in aplikacijska plast. Komunikacija v TCP/IP modelu se izvršuje preko treh agentov: procesi, gostitelj in omrežja. Glavna naloga osnovnega protokola TCP/IP je, da poskrbi za pravilen prenos paketov. Zato TCP/IP prelomi uporabniške podatke na majhne pakete. Paket je sestavljen iz uporabniških podatkov in ovojnice, ki vsebuje krmilne informacije, ki jih dobimo z enkapsulacijo in jih prenašamo z določenim protokolom. Vsak paket lahko potuje neodvisno, ker ima vgrajeno informacijo o naslovu.

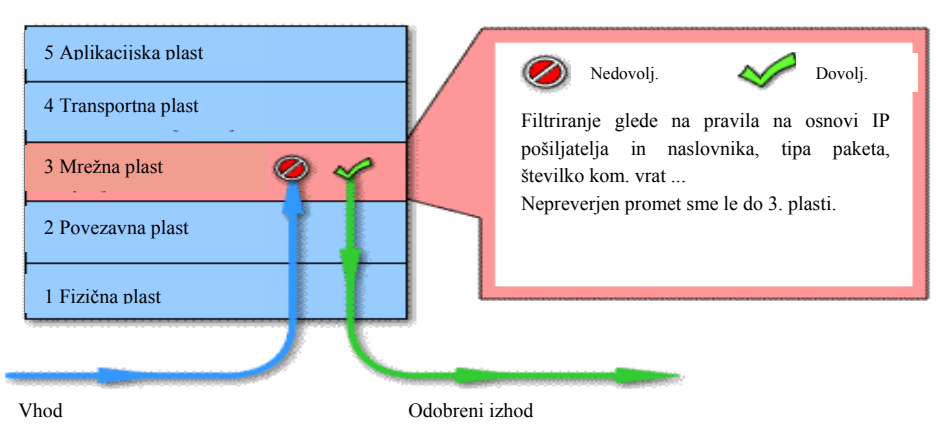
- filtriranje paketov,
- nadzor aplikacijskih prehodov in
- nadzor prehodov na nivoju povezave.

3.6.1.1 Funkcija filtriranja paketov

Prvi pristop poteka v mrežni plasti TCP/IP modela (glej Slika 8) in postavlja v ospredje funkcije filtriranja paketov, ki velja za najpreprostejšo metodo nadzora dostopa. Zanj je značilno relativno hitro izvajanje. Funkcija filtriranja je namenjena nadzoru legalnosti podatkovnih paketov, ki se porajajo znotraj omrežja in ga zapuščajo, obenem pa onemogoča nekontroliran vdor nezaželenih paketov v omrežje (Kranjc, 2002, str.57-58):

Funkcijo filtriranja pogosto opravlja eden ali več usmerjevalnikov. Glavna pomanjkljivost funkcij filtriranja je njihova ločenost od višjih komunikacijskih nivojev. Pakete, ki prihajajo ali odhajajo iz omrežja, lahko nadzorujemo samo na nivoju vrat za aplikacije (npr. e-pošta, FTP) in ne moremo preverjati vsebine paketov. Požarni zidovi tega tipa so osnova zaščite lokalnega omrežja in se uporabljajo tudi v kombinaciji z drugimi tipi požarnih zidov.

Slika 8: Prikaz požarnega zidu na mrežni plasti v TCP/IP modelu



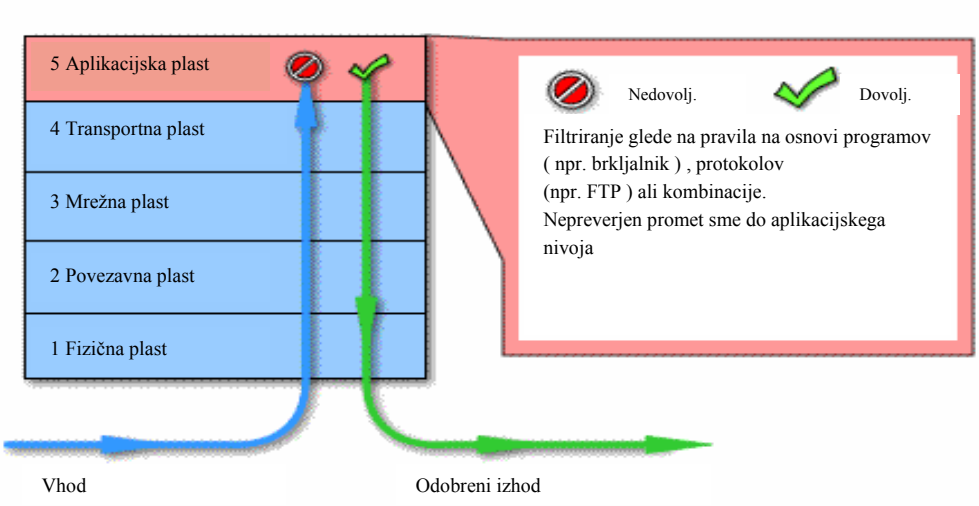
VIR: Vicomsoft, 2003.

3.6.1.2 Funkcija nadzora aplikacijskega nivoja

Funkcija nadzora aplikacijskih plasti omogoča na aplikacijski plasti nadzor storitev, ki naj bi se uporabljale v omrežju (glej Slika 9). Taki sistemi so v bistvu "namestniški" programi (proxy), ki prestrezajo, preverjajo in posredujejo ali blokirajo zahteve posameznim programom. Z večanjem števila procesov se veča tudi ranljivost sistema, na katerem tečejo ti procesi. Veča se tudi zahteva po procesorski moči, ki je potrebna za izvajanje vseh procesov.

Ta omogoča, da lahko veliko paketov potuje skozi omrežje in pri tem uporabljajo različne poti, navzlic temu pa vsak dospe na cilj v enem kosu. Pri pretoku informacij imajo pomembno vlogo t.i. stikala za usmerjanje paketov, ki ji imenujemo usmerjevalniki.

Slika 9: Prikaz požarnega zidu na aplikacijski plasti v TCP/IP modelu



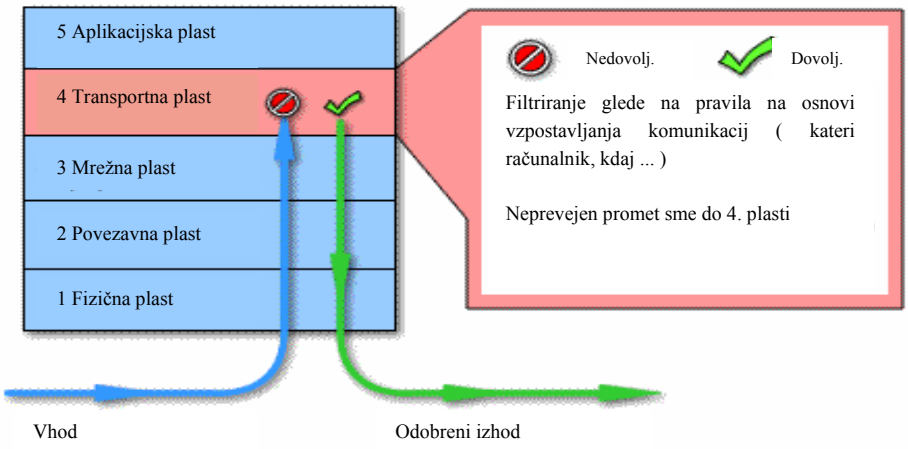
VIR: Vicomsoft, 2003.

Prednost požarnega zidu na aplikacijskem nivoju je popoln nadzor nad izvajanimi aplikacijami in s tem omogočanje visoke ravni varnosti. Slabost pa je opazna pri večji zahtevnosti pri nastavitvah in vzdrževanju kot tudi po potrebi večjih procesorskih moči ter slabše prilagodljivosti novim servisom**.**

3.6.1.3 Funkcija nadzora prehoda na nivoju povezave

Tak sistem je običajno nameščen na strežniku, preko katerega do zunanjega omrežja dostopajo drugi računalniki v lokalni mreži. Deluje v transportni plasti TCP/IP modela (glej Slika 10) in preverja ustreznost paketov glede na to, kdo vzpostavlja posamezne komunikacije in ali je komunikacija pravilno vzpostavljena. Nekateri taki sistemi lahko s spreminjanjem IP naslovov pošiljatelja tudi omogočajo skrivanje podatkov o notranji mreži. Iz zunanje mreže je videti, kot da vsi paketi prihajajo z istega naslova varnostnega strežnika.

Slika 10: Prikaz požarnega zidu na transportni ravni v TCP/IP modelu



VIR: Vicomsoft, 2003

3.7 PAMETNE KARTICE

Pametna kartica je plastična kartica z vgrajenim mikropocesorjem na čipu, ki se je v svetu prvič pojavila leta 1979. Pojem pametna kartica opisuje mikroračunalnik, ki je v ohišju kartice. Tehnologija pametnih kartic nam omogoča prenos in hranjenje informacij s pomočjo integriranega vezja, ki je vgrajen v kartici in na katerem lahko hranimo šifrirni ključ oz. digitalno potrdilo. Kartica poskrbi, da se podatki z zunanjim svetom izmenjujejo na varen in zanesljiv način. Na površini kartice se nahajajo priključki, ki so namenjeni izmenjavi podatkov med čitalcem in kartico. Tako je s pomočjo čitalca za te kartice mogoče poslovati kjer koli, s tem da je treba čitalec predhodno namestiti na računalnik.

Danes so pametne kartice nadomestile uporabo kartic z magnetnim zapisom, ki se na trgu pojavljajo že dlje časa in so cenejše ter slabše zaščitene pred zlorabami[30]. S pomočjo posebnih naprav je možno zapis z magnetne kartice enostavno prekopirati na drugo[31]. Magnetno kartico je tudi moč uporabiti brez poznavanja gesla (PIN), saj za uporabo zadošča že podpis, ki ga lahko oseba brez težav ponaredi. V primerjavi z magnetno kartico pametna kartica dovoli e-podpisovanje le z vnosom osebnega gesla, ki ga pozna samo imetnik kartice. Poleg tega tehnologija pametne kartice preveri, ali je terminal, preko katerega poteka plačilo originalen ter preveri pravilnost kartice in identifikacijo imetnika kartice z uporabo PIN kode. Takšen postopek je veliko varnejši, saj je pametna kartica brez ustreznega PIN-a praktično neuporabna in se ob treh napačnih poskusil gesla zablokira. To je tudi glavni razlog, zakaj je uporaba pametne kartice varnejša od uporabe magnetne kartice.

3.8 GESLA IN DRUGA ZAŠČITA

Najstarejši in najenostavnejši način preverjanja identitete je identifikacija s pomočjo gesla oz. določene informacije, ki določa neko osebo ali subjekt. V e-poslovanju kot tudi v e-bančništvu se z gesli ali identifikacijskimi številkami srečujemo praktično na vsakem koraku. Predstavljajo najenostavnejši način identifikacijske uporabnosti in so ključ dostopa do varovanih podatkov.

Gesla uvrščamo med šibkejšo zaščito varovanja zaradi naslednjih razlogov:

- uporabniki si večinoma sami izbirajo gesla, ki si jih je lažje zapomniti in katera se da tudi lažje razkriti. Ugotavljanje tujih gesel poteka s pomočjo elektronskih slovarjev, s poznavanjem uporabnikovih podatkov in s preizkuševanjem že uporabljenih gesel. Za daljše izbrana gesla si pogosto pred izgubo nekje zapišejo, kar je lahko lahek plen za nepridiprave;
- pri identifikaciji razkrijemo svoje geslo in tako omogočimo naslovniku, da se izdaja pod našim imenom;

[30] Izdajatelji kreditnih kartic so imeli v minulih letih veliko izgub zaradi najrazličnejših zlorab kreditnih kartic. Tovrstne zlorabe so se razvite zlasti v azijskih deželah in ZDA, kjer je organiziranemu kriminalu uspelo osvojiti celo tehnologijo proizvodnje magnetnega zapisa. Pri tem pa je nekaterim uspevalo, da so ponaredki zelo dobri in jih je moč prepoznati le s strani redkih strokovnjakov (Pinterič, 1995, str. 29).

[31] SCIMMING se imenuje naprava, ki prekopira magnetni zapis kartice na ponarejeno kartico. To je majhna naprava velikosti vžigalične škatlice, ki s potegom prekopira celotno vsebino na kartici. Kopiranje magnetne kartice se ponavadi zgodi pri plačevanju s kartico, ko lastnik ni fizično prisoten pri POS terminalih (v restavracijah in drugih gostinskih lokalih) (Lamberger, 2004, str 24).

- gesla se ponavadi prenašajo v nešifrirani obliki in so tako lahko tarča napadalcev. Tudi če so gesla predhodno šifrirana, jih napadalec lahko prestreže in uporablja v takšni obliki za kasnejše predstavljanje.

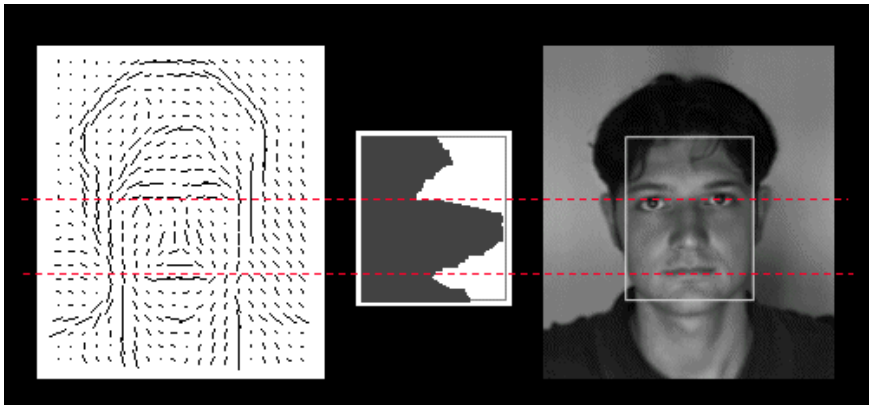
Zaradi navedenih razlogov šibko overjanje s pomočjo gesel ni primerno za preverjanje identitete v e-poslovanju, razen za dostop do lokalnega sistema ali aktiviranja določenih naprav (pametne kartice, internetnega brskalnika, itd.). Pogosto gesla zamenjujejo PIN kode, ki pa se uporabljajo za avtorizacijo pri bankomatih, POS terminalih ter v kombinaciji z magnetnimi in pametnimi karticami.

Varnost gesel v javnih omrežjih lahko izboljšamo z varnostjo z enkratnimi gesli. Posamezno geslo se uporabi le enkrat, zato prestrezanje gesel nima pravega pomena. Pri tem načinu je zelo pomembno, da se iz preteklih gesel ne da izračunati prihodnjega gesla. Najenostavnejši način brez uporabe kriptografskih algoritmov je uporaba enkratnih gesel z vnaprej generiranih določenih naključnih gesel. Slabost takšnega sistema je, da gesla shranimo v računalnik in jih za overjanje uporabljamo po seznamu.

Najbolj znan način za identifikacijo s pomočjo enkratnih gesel je uporaba kartice, ki vsebuje mikroprocesor in ekran ter je sinhroniziran z uro na strežniku. Lastnik kartice, ki želi izkazati svojo identiteto, vtipka na kartici geslo za njeno uporabo, algoritem pa nato na podlagi trenutnega časa generira geslo, katerega uporabnik pošlje na strežnik. Takšen način identifikacije uporabljajo nekatere banke v e-bančništvu za identifikacijo svojih komitentov (Jerman Blažič, 2001, str. 116).

Poleg enkratnih gesel poznamo še druge načine dokazovanja identitete uporabnika. Boljši načini dokazovanja identitete so na podlagi biometričnih lastnosti. Preverjanje uporabnika bo nekoč temeljilo na biometriki, ki se nanaša na poznavanje in razlikovanje fizičnih karakteristik posameznika. Uporabljala se bo lahko tehnologija prepoznavanja obraza (glej Slika 11), prstnih odtisov, prepoznavanje glasu ali celo zenice. Pri tehniki prepoznavanja obraza infra rdeča kamera skenira obraz in s tem dobi zapis žilnega sistema našega obraza, ki ga nato shrani kot obrazni termogram in vsakič, ko bomo hoteli poslovati s svojo banko, nam bo ta naprava skenirala in hkrati preverila, ali ustrezamo šabloni, zapisani v bazi dostopa.

Slika 11: Primer biometrične zaščite s prepoznavanjem obraza



3.9 VARNOSTNI PROTOKOLI

Internet združuje veliko množico najrazličnejših računalnikov in uporabnikov, da pa se lahko ti med seboj sporazumevajo, uporabljajo protokole. Protokoli tako predstavljajo množico pravil ali dogovorov o tem, kako komunicirati in kako razumeti preneseno sporočilo. V glavnem lahko uporabljene protokole na internetu delimo v skupine komunikacijskih, programskih in varnostnih protokolov. Pri komunikacijskih protokolih gre za vrsto pravil, po katerih si računalniki izmenjujejo informacije, medtem ko programski protokoli skrbijo za formatiranje zahtev, ki jih postavlja uporabnik ter prikaz podatkov, ki so odgovor na omenjene zahteve. Varnostni protokoli pa omogočajo vzpostavitev varne šifrirane povezave med dvema točkama (strežnik/odjemalec).

Varnost lahko v sistemu za e-poslovanje zagotovimo na različnih ravneh. Najpogosteje uporabljamo varnostne protokole v komunikacijskem protokolu TCP/IP, in to na aplikacijski, transportni in omrežni ravni.

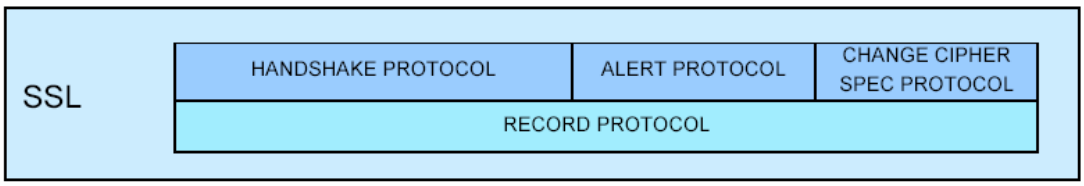
3.9.1 Secure Sockets Layer - SSL

SSL protokol je varnostni protokol med transportnim in aplikativnim nivojem, ki ga je razvilo podjetje Netscape, da bi zagotovilo varno povezavo med odjemalcem in strežnikom, ki komunicirata prek javnega kanala. Implementiran je v večino najpogosteje uporabljanih brskalnikov in internet strežnikov (Robinson, 2001).

Protokol SSL pogosto uporabljajo banke v e-bančništvu. Uporabnik se najprej prepriča, ali res komunicira s pravim končnim strežnikom. Protokol SSL zagotavlja:

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

Slika 12: Arhitektura protokola SSL



Vir: Zapiski predavanj - Komunikacijska tehnologija, 2001

Protokol SSL je sestavljen iz dveh delov (glej Slika 12)[32] :

1. Zgornji sloj
   - SSL Handshake Protocol – so protokoli, ki poskrbijo za to, da se stražnik in odjemalec medsebojno preverita, se dogovorita za način šifriranja podatkov, si varno izmenjata simetrični ključ in dogovorita ter uskladita algoritme;
   - SSL Alert Protocol – skrbi za obveščanje o napakah ali prekinitvah na povezavah pri komunikaciji;
   - SSL Change Cipher Spec Protocol – namenjen zamenjavi šifriranja in za potrjevanje o dogovorjenih parametrih med strežnikom in odjemalcem.

2. Spodnji sloj
   - SSL Record Protocol – deluje kot nivo pod vsemi sporočili SSL in določa način šifriranja in zaščito celovitosti, ki se bodo uporabili. Podatke razbije na bloke določene dolžine ter vsakemu doda zaporedno številko sporočila, tip zapisa ter dolžino bloka podatka. Iz teh podatkov se izračuna MAC (Message Authentical Code), ki služi kontroli nespremenljivosti podatkov in za overjanje sporočila.

Strežnik in odjemalec pri vzpostavitvi povezave najprej na podlagi prvega protokola preverita identiteto drug drugega, uskladita kriptografske algoritme ter si varno izmenjata ključ seje in ostale podatke, ki so potrebni za morebitne kasnejše šifriranje (Blažič Jerman, 2001, str. 120).

Protokol SSL nima fiksno določenih algoritmov za šifriranje, tako da jih lahko določijo proizvajalci programskih aplikacij sami. V NLB uporabljajo šifriranje s pomočjo algoritma RSA (namenjen overjanju in izmenjavi ključev) in RC4 (namenjen za kodiranje podatkov).

3.9.2 Transport Layer Security - TLS, Wireless Transport Layer Security - WTLS

Bistvo protokola varnosti na transportni ravni in protokola varnosti za brezžične povezave je, da vzpostavijo varen kanal med strežnikom in odjemalcem (spletnim brskalnikom). WTLS je namenjen za brezžične povezave v okolju m–bančništva. Zasnovan je na protokolu SSL in TLS ter optimiziran za uporabo na ozkih pasovnih komunikacijskih kanalih. Postavljajo de facto standard za zagotavljanje zasebnosti, neoporečnosti podatkov in overovljenje pri aplikacijah na mobilnih telefonih in drugih majhnih brezžičnih napravah.

SSL, TLS in WLTS zagotavlja varen prenos podatkov, ne morejo pa zagotavljati njihove varnosti na strežniku in brskalniku.

[32] SSL. [URL: http://www.sigov.si/tecaj/kripto/kr-ssl.htm], 26.06.2002.

3.9.3 Secure Electronic Transaction - SET

Protokol SET se uporablja v sistemu za varno elektronsko plačevanje z bančnimi karticami v svetovnem spletu. SET je bil razvit z namenom, da bi vsem udeležencem v elektronskem trgovanju zagotovil visok nivo varnosti ter preprečil zlorabe pri plačilnih transakcijah s plačilnimi karticami preko interneta. SET protokol je načrtovan tako, da poveča zaupanje v plačilnem procesu e-poslovanja v svetovnem spletu. SET zagotovi, da so trgovci, ki sprejemajo kartice, za to avtorizirani, istočasno pa trgovcu zagotavljajo pravilno identiteto lastnika kartice.

Pri plačevanju s kreditnimi karticami v protokolu SET so vedno udeležene 4 stranke. Med njimi se zagotavlja vmesna vrata med nezavarovanim delom omrežja in varnim omrežjem bank. Zaupne informacije potujejo skozi varno omrežje, z uporabo sodobnega asimetričnega šifrirnega algoritma in z uporabo sistema javnega ključa.

SET podpira vrsto organizacij za izdajo kreditnih kartic, vendar zaradi kompleksnosti in pomanjkljivosti infrastrukture javnih overiteljev elektronskih podpisov ni prišlo do množične uporabe. Drug problem je nekompatibilnost programske in strojne opreme različnih dobaviteljev.

4 BANČNIŠTVO V SLOVENIJI

4.1 ZGODOVINA BANČNIŠTVA V SLOVENIJI

Slovenija je po osamosvojitvi počasi spreminjala podobo v bančnem prostoru. V 70. in 80. letih so bile banke v jugoslovanskem prostoru v lasti podjetij, ki so delovala v geografsko omejenih trgih. Pogosto so na podlagi vladnih gospodarskih ciljev zagotavljale kredite lokalnim podjetjem v družbeni lasti. Leta 1991 je v slovenskem bančnem prostoru dominirala skupina Ljubljanske banke, ki je bila sestavljena iz 13 bank članic in banke matere (LB d.d.). Istega leta je bila ustanovljena Banka Slovenija in sprejet je bil Zakon o bankah in hranilnicah. Začelo se je novo obdobje v bančništvu s sanacijo bank, ki je bila posledica ekonomskega sistema bivše države. Nezaupanje v bančni sektor so začeli reševati s sanacijo, ki jo je prevzela Agencija za sanacijo bank in hranilnic (ASBH). Vloga ASBH je obsegala predvsem področje nadzora nad bankami v sanaciji, upravljanje s slabo aktivo in upravljanje z delom javnega dolga. V sanacijskem postopku sta bili ustanovljeni dve novi banki Nova Ljubljanska Banka d.d. in Nova Kreditna Banka Maribor d.d., ki sta nastali po prevzetju slabih terjatev LB d.d. in KBM d.d. od ASBH. Sanacija se je zaključila z letom 1997, ko je BS ugotovila zadostno kapitalsko ustreznost, zadostnost jamstvenega kapitala kot tudi zadovoljivost drugih kriterijev varnega bančnega poslovanja (Šega, 2001, 54-58).

Trenutno v Sloveniji posluje 19 poslovnih bank (3 so v povezavi z NLB, 1 v likvidaciji)[33]. Za majhen slovenski prostor je bank glede na število prebivalstva preveč in banke težje konkurirajo v evropskem prostoru. Pojavljajo se težnje k povezovanju bančnega sektorja z drugimi finančnimi institucijami kot tudi k širitvi ponudbenega asortimana. Ena izmed sodobnejših načinov pridobivanja novih komitentov in utrjevanje položaja na trgu je uvajanje poslovanja preko interneta.

4.2 RAZVOJ E-BANČNIŠTVA V SLOVENIJI

Slovenske banke so se priprav na e-poslovanje lotile po svojih zmožnostih. Postavitev e-bančništva ni majhen zalogaj in potrebuje velika vlaganja tako v tehnologijo kot v znanje zaposlenih. Pri ozaveščenju gospodarstva za uporabo e-bančništva je prvi korak naredila APP. Uvajanje e-bančništva je začela že pred nekaj leti, ko so bili pogoji precej bolj neugodni, saj ni obstajalo močno javno omrežje, ki bi vključevalo širok krog uporabnikov, prav tako pa še ni bilo primernih tehnologij za zaščito podatkov. APP se je za pošiljanje plačilnih nalogov po e-pošti odločila zaradi velikega prihranka časa uporabnikov, prihranek pri stroških obrazcev in časa, izogibanju možnih napak zaradi večkratnih vnosov kot tudi nižje cene teh storitev. Podjetja so s finančnim aplikativnim programom, ki ga je posredovala APP, prenašala naloge

[33] Banka Slovenije: Seznam poslovnih bank. URL: http://www.bsi.si/html/povezave/seznam_bank.html], 26.08.2004.

s pomočjo poljubnega odjemalca za e-pošto. Zagotovljena je bila uporaba sistema javnega in zasebnega ključa, ki je bil varovan z geslom, ki ga je poznal samo lastnik. Digitalno potrdilo se je hranilo na trdem disku na lokalnem računalniku[34], kar je za današnje razmere nesprejemljivo.

V bančnem prostoru je e-bančništvo kot prva začela uvajati Hipotekarna banka Brežice, ki sedaj ne posluje več. Prvi uspešni začetki segajo v leto 1993, ko se je SKB banka vključila v slovenski javni sistem VINET (videotekstno omrežje). Na tej osnovi je bil zgrajen SKB Telebanking kot prvi način bančništva od doma, ki so ga uporabnikom testno ponudili leta 1995. Ta projekt je postavil temelje internetnega bančništva za fizične osebe, ki so ga uporabniki lahko začeli uporabljati septembra 1997.

E-bančništvo se tako v Sloveniji kot po svetu pretežno uporablja za izvajanje plačilnega prometa. Do nedavnega je bil ta segment poslovanja med podjetji in bankami zelo slabo razvit in neurejen. Vzroke lahko iščemo v starem načinu plačilnega sistema, ki ni bil prilagojen evropskim smernicam, kot tudi ni bil tržno in konkurenčno naravnan. Deloval je v monopolnem okolju, kjer je država imela popoln nadzor nad denarnimi transakcijami. Z reformo plačilnega prometa je Slovenija na novo uredila plačilni sistem, ki je primerljiv z državami EU in podpira smernice Evropske Unije.

4.3 REFORMA PLAČILNEGA SISTEMA

4.3.1 Zgodovinski razvoj slovenskega plačilnega sistema

Zametki slovenskega plačilnega sistema segajo v nekdanjo Jugoslavijo, kjer se je leta 1962 iz tedanje Narodne banke Jugoslavije izločil sektor za opravljanje plačilnega prometa, ki so ga z zakonom organizirali kot Službo družbenega knjigovodstva (SDK). Vzroki za odvzem opravljanja plačilnega prometa s pravnimi osebami centralni banki je bil predvsem politične narave, saj je politika želela ohraniti nadzor nad gospodarskimi in predvsem finančnimi tokovi.

Temeljne značilnosti starega sistema so bile:

- družbena lastnina,
- pravica države do stalne kontrole pravnih oseb,
- zamegljena vloga denarja kot zakonitega plačilnega sredstva[35] in
- odvisnost centralne banke od politike.

[34] Pošiljanje plačilnih nalogov po elektronski pošti. Združenja bank Slovenije. [URL: http://www.zbs.giz.si], 10.09.2002.
[35] V zahodnih državah je zakonito plačilno sredstvo tisto, ki ga izdaja centralna banka, ne pa tudi denar na žiro računih, ki je t.i. opcijski denar, ki ga posameznik seveda lahko sprejme v plačilo, ni pa v to obvezan.

Leta 1992 je BS začela s projektom prenove plačilnega sistema, ki je v skladu s sistemom tržnega gospodarstva in je primerljiv z drugimi evropskimi državami.

Prenova plačilnih sistemov je bila nujna iz več razlogov (Marinšek, Cepec, 2002):

- V prejšnjem sistemu ni bilo konkurence, ker je ves tolarski promet opravljala APP. Storitve so bile sorazmerno drage in tarifna politika je upoštevala nominalno vrednost transakcije, kar ni ekonomsko smotrno.
- Ločeno sta se izvajala tolarski in devizni plačilni promet. Tolarski plačilni promet med pravnimi osebami je opravljala APP, tolarski kot tudi devizni plačilni promet med fizičnimi osebami ter devizni plačilni promet s tujino za pravne osebe pa banke. To je v praksi pomenilo, da so podjetja kljub blokiranemu žiro računu pri APP še vedno uporabljala sredstva s svojih deviznih računov.
- Z zakonom je bilo omejeno plačevanje z gotovino med pravnimi osebami, medtem ko je bilo kot obvezno plačilno sredstvo določen denar z računa (žiralni denar), ki v razvitem svetu velja za tvegano plačilno sredstvo.
- E-poslovanje, ki ga je omogočila APP preko e-pošte, ni ustrezalo strogim varnostnim zahtevam.
- Neprilagojenost z EU je povzročalo bankam težave pri vključevanju v evropski sistem bruto poravnave v realnem času.

Iz vsega omenjenega je moč izluščiti nekaj temeljnih ciljev prenove z makroekonomskega vidika. Potrebno je bilo odpraviti monopolni položaj APP in razviti poslovno okolje za racionalno poslovanje bank. BS mora prevzeti kontrolo nad denarno politiko in tveganjem v plačilnem prometu ter s tem pridobiti boljši pregled nad bonitetami podjetij ter njihovo likvidnostjo in solventnostjo. Konkurenčno okolje bo sililo v zagotovitev boljših storitev in nižjih cen ter možnost izbire banke glede hitrosti, cene in kakovosti teh storitev.

4.3.2 Faze reforme plačilnega prometa

Reforma plačilnega prometa je potekala v več fazah. Faze so sistematično odpravljale star sistem in tako niso ogrozile nemotenega in kontinuiranega delovanja plačilnega sistema. Prehod je omogočil postopno integracijo domačega plačilnega prometa s plačilnim prometom v tujini in omogočil zagotavljanje sprotne ustrezne statistične in davčne informacije ter prilagoditev zakonodaje. Reforma plačilnega prometa je potekala v 6 - fazah[36]:

1. prenos računov obvezne rezerve poslovnih bank v BS (marec 1997),
2. prenos računov bank v BS in vpeljava sistema bruto poravnave v realnem času (BPRČ) in žiro kliring za medbančna plačila (april in oktober 1998),

[36] Plačilni sistemi: Nekaj informacij o reformi plačilnih sistemov v Sloveniji. [URL:http://www.bsi.si/html/ps/nekaj_info.html], 21.06.2002.

3. prevzem plačilnega prometa pravnih oseb s strani poslovnih bank in začetek »pilotskega usposabljanja bank« (PUB) ,[37]
4. posamezne banke ukinejo bančne račune pri APP in prevzemajo plačila vseh svojih komitentov. S tem si pridobijo popolni nadzor nad sredstvi, s katerimi upravljajo, ter združijo plačilni promet pravnih in fizičnih oseb (do 30.06.2002),
5. prenehanje poslovanja posameznih podružnic APP, ki nimajo komitentov,
6. popolna ukinitev podružnic APP, plačilni promet se opravlja le preko bank. Del nalog APP se prenese na dve novi državni instituciji: Agencijo za javno pravne evidence (AJPE) in Upravo za javna plačila (UJP)[38].

4.3.3 Lastnosti reformiranega plačilnega sistema

Makroekonomski razlogi so botrovali k nekaj bistvenim spremembam, ki se odražajo pri dnevnih plačevanjih kot tudi pri splošnih pravilih delovanja. Glavne spremembe reformiranega plačilnega sistema so:

- odprava žiro računov pri APP in odprtje transakcijskih računov pri bankah,
- možnost imeti več računov pri več bankah, vendar le enega pri posamezni banki,
- dva načina plačevanje nalogov; bruto poravnava v realnem času (BPRČ) in sistem žiro kliringa[39],
- poravnava med bankami poteka v sistemu BPRČ, kjer ima BS vlogo poravnalne hiše,
- tarifna politika temelji na številu poslanih nalogov in ne na nominalni vrednosti transakcij,
- sistematičen način določanja številke računa pri banki (glej Tabela 4.), ki ima svojo identifikacijsko številko, ki jo določi BS (npr. 30000-0003029005 računa Volksbank-Ljudske banke).

Tabela 4: Struktura transakcijskega računa

xx	yyy	Zzzzzzzz	kk
ID – šifra banke	**Organizacijska enota banke**	**ID komitenta, št. poravnalnega računa**	**Kontrolna številka**

Vir: Spletna stran Banke Slovenije, 2004.

[37] Pilotsko usposabljanje je proces, v katerem posamezno podjetje z banko preizkusi delovanje sistema. V prvi fazi poteka informacijski tok vzporedno. Podjetja pošiljajo naloge tako Agenciji kot poslovni banki, upošteva pa se nalog, ki je poslan banki. Po potrditvi uspešnosti poslovanja prične podjetje poslovati neposredno z banko, vzporedni informacijski tok z Agencijo pa postane nepotreben.

[38] Naloge AJPES so: zbiranje, obdelovanje in posredovanje podatkov iz letnih poročil vseh poslovnih subjektov, vodenje različnih registrov in evidenc ter povezovanje podatkov med njimi, izdelovanje informacij o boniteti poslovanja posameznih poslovnih subjektov, itd. UJP je organ za vodenje registrov in računov proračunskih uporabnikov, zagotavljanje podatkov o javno finančnih prihodkih in o poravnavanju obveznosti proračunskih uporabnikov, zagotavljanje tehnološke podpore zakladniškemu poslovanju (Valher, 2002, 26-28 str.).

[39] BPRČ je sistem, kjer se transakcija izvede v realnem času in kjer banke za vsa medbančna plačila velikih vrednosti preko SWIFT omrežja pošlje nalog v poravnavo BS. Za ostala plačila je vpeljan sistem žiro kliring, ki je namenjen medbančni poravnavi nenujnih plačil malih vrednosti. Poslovne banke zbirajo plačilne naloge posameznih družb, in jih v zbirni obliki posredujejo BS. Bistvena razlika med sistemoma BPRČ in ŽK je v času poravnave posamezne transakcije. Medtem ko je v sistemu BPRČ transakcija poravnana takoj (on-line), pa je v sistemu ŽK dokončna poravnava izvedena šele v okviru neto poravnave med bankami neto dolžnicami in bankami neto upnicami, ki se izvaja nekajkrat v okviru posameznega dneva.

4.3.4 Prednosti in pomanjkljivosti reforme

Nov sodobno tržno usmerjen reformiran plačilni sistem prinaša tako prednosti kot tudi slabosti za uporabnike novega sistema (BS, banke in hranilnice, podjetja in druge pravne osebe, fizične osebe).

1. Prednosti in pomanjkljivosti za podjetja:

+ nižji stroški, večja hitrost, boljša kakovost,
+ direktno finančno svetovanje,
+ boljša varnost e-poslovanja,
- slabša preglednost denarnih sredstev in
- nestandardizirane programske rešitve.

2. Prednosti in pomanjkljivosti za banke:

+ konkurenčnost,
+ prilagajanje sistemu EU,
+ direktno bančništvo,
+ sprememba profila zaposlenih in
- nepoenotenost med pristojnimi službami.

4.4 BANČNI PREGLED PONUDBE E-BANČNIŠTVA

V preteklih desetletjih je razvoj finančnega poslovanja podjetij skokovito napredoval. Pred tridesetimi leti so zaposleni prejemali plačo v gotovini pri blagajni podjetja, knjigovodstvo in računovodstvo pa so vodili s kartotekami. Še pred desetletjem je kurir vsak dan odšel na SDK z mapo virmanov in nalogov, v finančnih sektorjih pa so se ubadali s prvimi računalniškimi programi za knjiženje. Danes je večina finančnega poslovanja avtomatizirana. V svetu denarja so se udomačili računalniki in posledično tega tudi razvoj e-bančništva. Finančne institucije vse bolj uvajajo storitve e-bančništva, ki omogočajo opravljanje osnovnih finančnih storitev brez obiska finančne institucije oz. kar z domačega računalnika.

Tehnološka preobrazba je prinesla mnogo novosti tako na strani podjetij kot tudi bank. Uporabnikom je dana možnost dodatnega racionalnega poslovanja pri izvajanju elektronskega plačila na daljavo preko interneta in avtomatske obdelave podatkov. Še pred kratkim so banke težile h glavnemu cilju poslovanja v zagotavljanju kvalitetne aktive kot tudi v kapitalizaciji, ki vpliva na čim večjo profitabilnost. Danes banke težijo za novimi načini, ki povečujejo prihodke in jim dajejo konkurenčno prednost pred njihovimi konkurenti. Pet ključnih faktorjev, ki so vplivali na spremembe v bančnem sektorju in prispevali k konkurenčnemu okolju, so (Kalakota, 1997, str.183):

- sprememba navad kupcev,
- zmanjševanje stroškov,
- demografski trendi,
- regulativne reforme in
- novi spletni finančni proizvodi.

Banke so se na nov način poslovanja pripravljale skozi faze reforme plačilnega prometa. Reforma je na nek način prisilila banke v hitrejši razvoj in ponudbo elektronskih bančnih storitev. Današnja slika ponudbe e-bančništva v slovenskih bankah je vidna iz spodnje tabele (glej Tabela 5). V vseh bankah ponujajo e-bančništvo za podjetja. V manjših bankah postavitev samostojnega sistema e-bančništva ni ekonomsko smotrno, saj je strošek na transakcijo previsok in je težje doseči kritično maso uporabnikom.

Tabela 5: Seznam bank, ki ponujajo storitve e-bančništva za prebivalstvo in podjetje

BANKA	ELEKTRONSKO BANČNIŠTVO (za prebivalstvo)	ELEKTRONSKO BANČNIŠTVO (za podjetja)
Abanka Vipa d.d.	ABANET	ABACOM
Bank Austria Creditanstalt d.d.	ONLINE B@NKA	MULTICASH, E-BANKA
Banka Celje d.d.	KLIK NLB	e-BANČNIŠTVO BC
Banka Koper d.d.	I-NET BANKA	POSLOVNA I-NET BANKA
Banka Domžale d.d.	KLIK NLB	PROKLIK NLB, PROKLIK +NLB
Banka Zasavje d.d.	KLIK NLB	PROKLIK NLB, PROKLIK +NLB
Deželna banka Slovenije, d.d.	SEZAM	SEZAM
Factor Banka d.d.		E-BANKA
Gorenjska banka d.d.	LINK	LINK +
Hypo Alpe Adria banka d.d.	HYPONET	HYPONET
Raiffeisen Krekova Banka d.d.	RaiffeisenNET	EUREKA
NKBM d.d.	BANK@NET	POSLOVNI BANK@NET
NLB d.d.	KLIK NLB	PROKLIK NLB, PROKLIK +NLB
Koroška Banka d.d.	KLIK NLB	PROKLIK NLB, PROKLIK +NLB
Poštna banka Slovenija d.d.	PBS.NET	POSLOVNI PBS.NET
Probanka d.d.	PROSPLET	POSLOVNI PROSPLET
SKB Banka d.d.	SKBNET	POSLOVNI SKBNET
Volksbank – Ljudska banka d.d.	VOLKSBANK – ONLINE	VOLKSBANK – ONLINE

Vir: Spletna stran BS, Halcom in Zaslon, 2002.

Število uporabnikov e-bančništva iz dneva v dan raste. Od leta 1997, ko je SKB banka kot prva ponudila e-bančništvo, se ji je z internetno ponudbo pridružila tudi velika večina ostalih slovenskih bank. Ocena uporabnikov omenjenih storitev je okoli 3.4% prebivalcev - 70.000 uporabnikov (uporabnikov interneta; 31% prebivalcev - 620.000 prebivalcev), vendar po raziskavi RIS-a ocenjujejo možni potencial uporabnikov na okoli 150.000[40]. Rezultati raziskave RIS o uporabi e-bančništva iz meseca decembra 2002 kažejo trend rasti. Na trgu pravnih oseb že več kot 91% velikih in srednjih podjetji in nekoliko manj majhnih uporablja storitve e-bančništva[41].

[40] Spletna stran Raba interneta v Sloveniji. [URL: http://www.ris.org], 20.07.2002.
[41] E-bančništvo. Povzetek. RIS 2002. URL:http://www.ris.org/publikacije/najnovejsa/e_bancnistvo2k2.html, 28.04.2003.

Podjetja v dveh tretjinah primerov uporabljajo eno samo banko, preko katere opravljajo e-plačilni promet. Večina med njimi (71%) jih napoveduje, da bo število bank, preko katerih opravljajo plačilni promet, v prihodnje ostalo enako, v preostalih pa prevladuje delež tistih, ki bodo število bank večali. Največji tržni delež zavzema NLB, predvsem kot glavna banka in manj kot druga banka. Druga najpomembnejša glavna banka med anketiranimi podjetji je SKB Societe Generale, sledita pa še NKBM ter A–Banka Vipa. Lojalnost glavni banki je med podjetji izredno visoka in se je v primerjavi z letom 2000 še povečala. V povprečju bi 30% podjetij zamenjalo banko, če bi konkurenčna banka ponudila boljše storitve e-bančništva. Kot glavno banko pa podjetja navajajo tisto, ki je najbolj razvila e-bančništvo[42].

Osnovna ponudba e-bančništva na svetovnem spletu omogoča naslednje storitve:

1. Domači plačilni promet
   - pregled osnovnih podatkov o TrR (transakcijski računi - limiti, obrestne mere),
   - pregled prometa in stanja na TrR (prilivi/odlivi, možnost pregleda tudi posameznega naloga),
   - vnos plačilnega naloga,
   - posredovanje nalogov v banko preko ročne ali paketne obdelave nalogov,
   - pregled neobdelanih nalogov,
   - oblikovanje čakalne vrste,
   - informativni izračun,
   - izpis prometa na računu po različnih kriterijih,
   - pregledovanje podatkov o posameznem plačilnemu nalogu,
   - pregledovanje arhiva prometa,
   - reševanje reklamacij in pošiljanje vprašanj kontaktni osebi v banki;

2. Devizno poslovanje
   - pregled dnevno prispelih prilivov iz tujine,
   - razpored prilivov iz datoteke,
   - pregled prilivov in odlivov v izbranem obdobju,
   - pregled odprtih akreditivov s prometom,
   - pregled čakajočih črpanj po akredetivih;

3. Kreditno in depozitno poslovanje
   - vpogledi v posamezne kreditne in depozitne pogodbe, stanja, promet;

4. Tečajnice
   - pregled tečajnice za trenutni datum
   - pregled tečajnice za poljubni datum

[42] E-bančništvo. Povzetek. RIS 2002. URL:http://www.ris.org/publikacije/najnovejsa/e_bancnistvo2k2.html, 28.04.2003

Podjetjem, ki so se odločila za uporabo storitev e-bančništva, banke nudijo dva različna načina dostopa do spletne poslovalnice, glede na njihove potrebe:

- preko fiksnega omrežja; večina bank ponuja dostop preko interneta, kjer s prijavo v bančni sistem direktno povežejo na spletni strežnik. Omogoča mobilnost uporabnika, saj se lahko z bančnim strežnikom poveže kadarkoli in povsod tam, kjer ima na osebnem računalniku omogočen dostop do interneta. Baza podatkov se oblikuje na bančnem strežniku in zanjo skrbi banka. Ta različica je posebej primerna za vsa podjetja, ki imajo v svojem informacijskem sistemu možnost medsebojnega paketnega posredovanja podatkov (npr. seznama plačilnih nalogov v elektronski obliki, izpiski prometa) in sistem uporabljajo predvsem za hiter pregled ali paketno posredovanje podatkov ali pa poslujejo z manjšim številom ročno vnesenih plačilnih nalogov;

- preko modemske povezave; drugi način je s pomočjo programske aplikacije, ki si jo uporabnik namesti na svoj računalnik in se preko modemske povezave priklopi na bančni strežnik. Omogoča opravljanje številnih funkcij brez stalne internetne povezave, saj uporabnik lahko pripravi in pregleda plačilne naloge, pregleda bazo starih izpiskov, pripravi statistike brez uporabe interneta, z bančnim strežnikom pa se poveže le pri pošiljanju in sprejemanju podatkov. Baza podatkov se oblikuje pri uporabniku, ki zanjo tudi skrbi. Lokalna različica je primerna predvsem za srednje velika in velika podjetja. Odvisno od narave dela v podjetju je možno uporabljati tudi kombinacijo obeh različic.

Most, ki povezuje banko in podjetje, je uporabniški vmesnik, kamor podjetja vnašajo želene transakcije, banke pa jih izvajajo. Uporabniški vmesnik je programska zasnova, ki omogoča dostop do sistema e-banke, kjer si izmenjujejo podatke z bančnim informacijskim sistemom.

4.4.1 Programska zasnova e-bančništva

Banke so se pri zasnovanju in razvijanju sistema e-bančništva posluževale lastnega kadra v banki, oz. so programske rešitve kupili od specializiranih ponudnikov (Halcom Informatika, Zaslon – Hermes Soflab, Hmezad računalniški center, Zrcalo, Adacta, itd.). Konkurenca programskih aplikacij za e-bančništvo je precejšnja (glej Tabela 6), kar ima za posledico dobre kot tudi slabe lastnosti. Ponudniki so prisiljeni izdelati čim bolj kvalitetno rešitev, ki naj bi bila zasnovana na čim večji varnosti in bi zagotavljala enostavno funkcionalnost in preglednost.

Slabost se kaže v nepovezanem razvoju. Proizvajalci ponujajo različne programske aplikacije, ki podpirajo različne programske vmesnike in uporabnikom, ki poslujejo z več bankami hkrati, otežujejo delo, ker so prisiljeni nameščati in vzdrževati več sistemov. Posledica tega je precej različna in bolj ali manj nezdružljiva programska oprema e-bančništva.

Tabela 6: Sistemi e-bančništva v Sloveniji

APLIKACIJA	BANKE
E-banka (Halcom)	Skupina NLB (Proklik), Abanka (Abacom), BACA (E-banka), Raiffeinsen Krekova banka, Faktor Banka, Kartner Sparkasse
SEB (Hermes Softlab)	SKB (BAPPlus), Gorenjska banka (Link), Poštna banka Slovenije, NKBM, HYPO Alpe Adria (HYPO Onet), NLB (Proklk +)
EPP (Zrcalo)	NKBM, SIB, Volksbank – Ljudska banka, Banka Celje
Adacta	Banka Koper, Volksbank – Ljudska banka
HRC	Factor banka, Banka Celje
Multi Cash (Omikron)	BACA, *Societe General – SKB (Multi SKB Net)*
Lastni razvoj	VIPA, Probanka, Krekova banka

VIR: Bratož, 2002, str.7.

Bančna platforma igra vlogo vmesnika, ki s pomočjo sodobne distribuirane objektne tehnologije omogoča v realnem času dostop do obstoječih bančnih aplikacij na način, ki najbolj ustreza sodobnim oblikam e-poslovanja. Med poglavitnimi ponudniki bančnih platform so Halcom Informatika, Hermes Softlab, Zrcalo in Adacta.

4.4.1.1 Halcom Informatika - E-BANKA[43]

E-banka je sistem za e-bančništvo, zasnovan pri podjetju Halcom Informatika. V Sloveniji ga uporablja preko 40.000 podjetij pod različnimi imeni (Proklik NLB, Abacom, E-bank). Že na samem začetku, ki sega v leto 1996, so dajali velik pomen varnosti. V svoje izdelke so vgrajevati vse tri komponente varnosti, ki jih predvideva PKI sistem zaščite. Te so:

- zagotavljanje zasebnosti na osnovi šifriranja,
- preverjanje istovetnosti uporabnika na osnovi digitalnega potrdila ter
- preverjanje verodostojnosti podatkov na osnovi digitalnega podpisa.

Uporaba vseh treh varnostnih komponent skupaj omogoča, da je varnost nadzorovana in neodvisna od varnosti trenutnih različnih brskalnikov ali drugih elementov operacijskega sistema.

Pri E-bank gre za princip varovanja samega plačilnega naloga z digitalnim podpisom. Uporabnik vsak nalog digitalno podpiše s svojim zasebnim ključem, ki ga ima shranjenega na pametni kartici in ne na računalniku, kar omogoča banki nedvoumno ugotavljanje pristnosti podatkov. Banka za vsak plačilni nalog preveri istovetnost uporabnika. Princip pošiljanja podatkov in digitalno podpisovanje je zasnovano na kombiniranem šifrirnem načinu podobno SSL-u. Na začetku izmenjave podatkov bančni strežnik in uporabnikov programski paket tvorita simetrični ključ, ki si ga izmenjata z uporabo svojih javnih ključev z algoritmom RSA (1024 bitni ključ na strani podjetja in 2048 bitni ključ v banki). S simetričnim ključem se podatki s pomočjo algoritma 3DES zašifrirajo in na strani banke odšifrirajo z istim ključem.

[43] Povzeto po spletni strani Halcom Informatika. [URL: http://www.halcom.si], 2002.

Identifikacija uporabnika in elektronsko podpisovanje potekata prek zaščitne kartice, ki hrani digitalno potrdilo in zasebni ključ. Digitalna potrdila izdaja podjetje Halcom, saj ima lastno agencijo za certificiranje.

Halcomovi poslovni bančni partnerji, ki uporabljajo njihovo različico, so: Abanka, skupina NLB, SKB in BACA. Način dostopa do spletne banke je možen preko klicnega dostopa ali preko internetnega brskalnika, za kar se varnost kot tudi programska oblika ne spremeni.

4.4.1.2 Hermes Softlab - SEB[44]

SEB – sistem za elektronsko poslovanje je rešitev podjetja ZASLON - hčerinsko podjetje Hermes Softlab. Namenjen je za poslovanje s podjetji in omogoča banki enoten način e-poslovanja pravnih oseb z banko. Banke, ki uporabljajo SEB za potrebe e-bančništva za podjetja, so: SKB banka, Nova KBM, NLB, Gorenjska banka, HYPO Alpe Adria Bank, Poštna banka Slovenije in Slovenska zadružna kmetijska banka.

Podjetje se lahko na podlagi svojih potreb odloči med dvema načinoma e-poslovanja z banko prek interneta:

- Bančni asistent 2000+ za podjetja (BAP+): je modularni sistem, ki je nameščen na strani podjetja in je namenjen izvajanju negotovinskih bančnih opravil. Ciljna skupina so predvsem velika in srednje velika podjetja.
- Bančni asistent 2000 za podjetja (BAP): je spletni uporabniški vmesnik, ki omogoča, da bančne stranke – podjetja z uporabo brskalnika (npr. MS Internet Explorer) izvajajo negotovinska bančna opravila. Ciljna skupina so predvsem mala in srednje velika podjetja, za izvajanje posameznih opravil pa tudi velika podjetja.

Modularna zasnova SEB omogoča banki preprosto dodajanje podpore novim tržnim potem (GSM mobilno bančništvo, telefonski odzivniki, klicni center, informacijski terminal ipd.). SEB je sistem e-bančništva druge generacije in ima vgrajeno podporo za večbančništvo, saj podjetja zahtevajo enoten način dela z različnimi bankami. Podjetja, ki imajo odprt transakcijski račun pri večih bankah, lahko za izmenjavo podatkov z bankami s postavljenim SEB uporabljajo enotno odjemalsko programsko opremo BAP+[45].

Za pretok informacij med banko in uporabnikom uporabljajo protokola SSL. Uporabnik lahko uporablja katerikoli spletni brskalnik, ki podpira SSL protokol in je možna 128 bitna zaščita šifriranja. Povezava med podjetjem in banko je zagotovljena z overjanjem identitete s pomočjo digitalnega potrdila.

[44] Povzeto po spletni strani Zaslon. [URL: http://www.zaslon.si], 2002.
[45] Sistem elektronskega bančništva (SEB). Zaslon. [URL: http://www.zaslon.si/elba/seb.html]. 20.06.2002.

Banka izda svojim komitentom digitalna potrdila. Izdajanje digitalnih potrdil je odvisno od politike bank. Pogost je postopek, kjer banka po dveh različnih kanalih pošlje dve začasni gesli za prevzem zasebnega ključa. Med postopkom za izdajo digitalnega potrdila in prevzema s strani uporabnika se na uporabnikovi kartici ustvarita uporabnikov zasebni in javni ključ. Javni ključ je del uporabnikovega digitalnega potrdila in je dostopen vsakomur. Zasebni ključ pa je tajen in je shranjen samo na uporabnikovi kartici. Uporabnik se identificira s svojim digitalnim potrdilom. Banka se prav tako identificira s svojim potrdilom. Dostop do podatkov na kartici 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 ne morejo odkodirati.

4.4.1.3 Zrcalo - EPP[46]

Programska rešitev e-bančništva EPP, uporabnikom ponuja dva različna paketa, ki so jih v družbi ZRCALO poimenovali debeli in tanek klient. Uporaba debelega klienta EPP omogoča uporabniku izgradnjo lastne baze podatkov in njihovo obdelavo na svojem računalniku. Primerna je predvsem za večja podjetja z večimi uporabniki. Z uporabo tankega klienta EPP uporabnik v celoti posluje preko interneta, tako da na računalniku na katerem dela nima nobenih podatkov. Programski paket je primeren za tiste uporabnike, ki želijo uporabljati storitve e-plačilnega prometa z različnih lokacij in računalnikov.

Različica EPP 3 je prenovljena, poenostavljena in nadgrajena v varnosti. Omogoča podpisovanje nalogov z vsemi vrstami varnostnih certifikatov, ki jih podpira operacijski sistem Windows. EPP 3 omogoča tudi devizno poslovanje s tujimi poslovnimi partnerji.

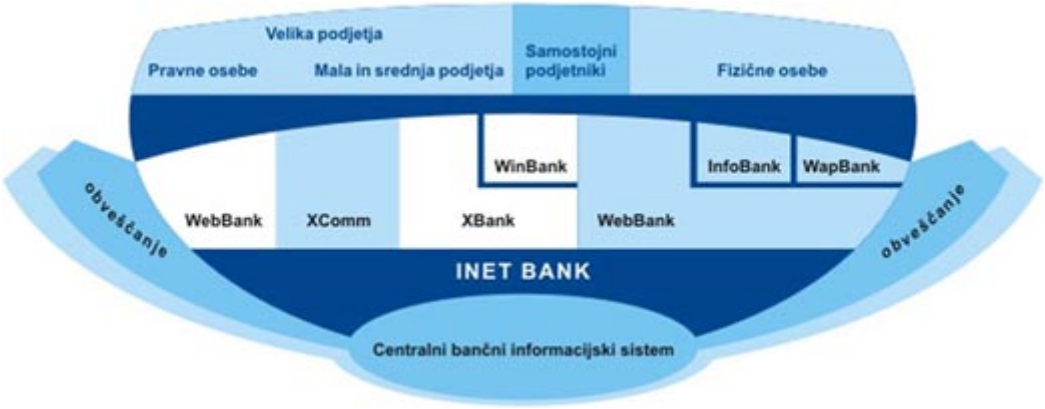
Zrcalo je s svojim programom EPP prisoten v SKB Banki, kot SKB net, SIB, Volksbank – Ljudska banka in Banka Celje.

4.4.1.4 Adacta – I-NET BANK[47]

I-net Bank je celovita rešitev za e-bančništvo za pravne in fizične osebe. S programsko rešitvijo I-net Bank lahko bančni poslovni sistem vzpostavi več različnih poslovnih kanalov, preko katerih omogoči svojim komitentom vseh profilov najbolj primeren in udoben način opravljanja bančnih poslov. I-net Bank omogoča naročniku, da komitentom v okviru e-bančništva ponuja storitve z vseh relevantnih področij.

[46] Spletna stran Zrcalo. [URL: http://www.zrcalo.si], 2002.
[47] Povzeto po spletni strani Adacta. [URL: http://www.adacta.si], 2002.

Slika 13: Modularna ponazoritev e-plačilnega prometa



Vir: Spletna stran Adacta, 2002.

Slika 13 prikazuje integriranost posameznih modulov I-net Banke, ki podpirajo funkcionalnost in pokrivajo zahteve komitentov, katerim so namenjeni. Hkrati pa njihova enotna osnova omogoča povezavo z vsemi pogostejšimi bazami podatkov in tehnologijami prenosa podatkov, kar ponuja enostavno in hitro integracijo s preostalimi deli informacijskega sistema v banki[48].

4.4.1.5 Omikron - MULTICASH[49]

Skupina Bank Austria Creditanstalt ima razvejano mednarodno mrežo komercialnih bank v Nemčiji, Češki Republiki, Slovaški, Poljski, Madžarski, Sloveniji, Hrvaški ter od jeseni 1998 tudi v Romuniji in Ukrajini. Mreža poslovalnic BA/CA je povezana v enoten informacijski sistem, ki omogoča opravljanje storitev z imenom EuropaKonto.

EuropaKonto s pomočjo programa MultiCash omogoča opravljanje plačil in upravljanje z računi, odprtimi pri katerikoli podružnici v skupini BA/CA. Sistem MultiCash nemškega podjetja Omikron omogoča elektronsko izvajanje plačilnega prometa za podjetja prek različnih komunikacijskih poti (internet, ISDN, modemska povezava, X.25). Je standardizirana (SWIFT, EDI, Windows) in najbolj razširjena programska oprema za e-bančništvo med podjetji v Evropi. Na strani bančnega komitenta se namesti odjemalski del MultiCash sistema, ki preko običajnih telekomunikacijskih zvez izmenjuje podatke z bančnim MultiCash strežnikom. Posamezna banka lahko zaradi varnosti ali zaradi drugih tehničnih zahtev izbere samo nekatere od možnih komunikacijskih poti.

MultiCash je opremljen s posebnimi moduli za domači in mednarodni plačilni promet. Ti moduli premeščajo jezikovne pregrade in različne standarde. MultiCash je trenutno razpoložljiv v petnajstih jezikih in se lahko uporablja pri poslovanju z vsemi bankami, uporabnicami tega programa. Slovenska različica Multicasha se imenuje E-bank.

[48] Spletna stran Adacta.[URL: http://www.adacta.si/index.asp?lang=SI&content=Resitev&submenu=InetBank], 19.10.2003.
[49] Povzeto po spletni strani BACA. [URL: http://www.baca.si], 2002

Podatki se izmenjujejo na paketni način, kar komitentu omogoča, da lahko pripravi vse načrtovane bančne transakcije vnaprej in se poveže z bančnim strežnikom le takrat, ko je priprava transakcij zaključena. Podjetja lahko program namestijo na dva načina - zgolj na enem računalniku ali na več računalnikih, povezanih v lokalno računalniško omrežje, ki imajo dostop do iste baze podatkov. Tako je možno, da lahko več uporabnikov hkrati pripravlja plačilne naloge ali analizira prispele izpiske plačilnega prometa in stanj na računih.

4.4.2 Primerjava bančnih ponudb na svetovnem spletu

4.4.2.1 Nova Ljubljanska Banka - NLB[50]

Nova Ljubljanska banka je največja banka v in hkrati matična banka v skupini NLB, kjer je vključenih preko 50.000 podjetij in 900.000 individualnih strank. Tržni delež domačih odvisnih bank Skupine NLB je leta 2002 znašal 38 odstotkov celotne aktive slovenskega bančnega sistema. NLB lahko s svojimi absolutnimi primerjalnimi prednostmi v slovenskem prostoru - velikostjo, močjo in mednarodnimi referencami - učinkovito poslovno podpira tudi največja in najbolj dinamična podjetja pri njihovem poslovanju doma in na mednarodnih trgih.

Glavna konkurenčna prednost pred drugimi je v hitrosti in stroških prometa. V tem kontekstu je za gospodarske subjekte izjemno pomembno, da lahko opravijo čim več prometa znotraj enega bančnega sistema, saj ima interni promet številne prednosti pred eksternim. Je objektivno najcenejši, najhitrejši (izvaja se v realnem času), njegov umik pa je do 2 uri daljši od umika za eksterna medbančna plačila prek sistemov žiro kliringa in BPRČ. Vendar pa velikost banke pogosto požene v precejšno togost in okretnost, saj zaradi preobremenjenosti pogosto prihaja do prekinitev povezav in do počasnejšega delovanja sistema.

Ponudba e-bančništva NLB temelji na dveh platformah:

- Proklik NLB in
- Proklik plus NLB.

Proklik NLB je bolj razširjena oblika platforme in je rešitev podjetja Halcom Informatika. Namenjena je 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. 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 e-bančništva prek lastne vstopne točke. Za varno poslovanje prek Proklika NLB je poskrbljeno s šifriranjem in elektronskim podpisovanjem sporočil med uporabnikom in

[50] Povzeto po spletni strani NLB. [URL: http://www.nlb.si], 2002.

banko. Vključeni so vsi varnostni mehanizmi, ki jih podpira in uvaja Halcom v svoji programski različici E-banka.

Proklik plus je nastal v sodelovanju s podjetjem Hermes Softlab. Podjetja opravljajo tolarski in devizni plačilni promet preko svetovnega spleta. Uporabnik potrebuje za svoje delo osebni računalnik, opremljen s čitalcem pametnih kartic in spletnim brskalnikom. Zaradi racionalizacije poslovanja in boljše funkcionalnosti v NLB, so začeli postopoma prenašati poslovanje Proklik plus NLB na elektronsko banko Proklik NLB ter bodo do konca leta 2005 ukinili elektronsko banko Proklik plus NLB.

4.4.2.2 SKB Banka[51]

Leta 1995 je SKB banka prvič predstavila e-bančništvo (5 let po prvi spletni banki v svetu). Nekaj mescev kasneje so začeli uporabljati storitve e-bančništva že prvi uporabniki. Že od samega začetka je za varnost pri prenosu poskrbljeno z 128 bitnim šifriranjem, na protokolu SSL. Sčasoma so dograjevali varnostne komponente, saj je bila zahtevana visoka varnostna politika. Svojo programsko rešitev so zaščitili s sistemom PKI v sodelovanju z družbo ActivCard - tehnologijo pametnih kartic. V letu 2000 se je ponudba razširila na mobilno bančništvo z WAP protokolom. Danes SKB banka v povezavi s SEB sistemom ponuja integriran sistem bančništva v sistem podjetja (Bračun, 2003).

Banka se poskuša prilagoditi vsem oblikam podjetij in jim ponuja 3 programske različice:

1. SKB NET za samostojne podjetnike in manjša podjetja, ki opravijo do 100 nalogov na mesec. Dostopen je s kateregakoli računalnika z dostopom do interneta. Za njegovo uporabo se ne potrebuje posebnih programov, dovolj je sodoben brskalnik s 128-bitnim varnostnim ključem.
2. Poslovni SKB NET za srednja in velika podjetja, ki poslujejo tudi s tujino in opravijo do 1000 nalogov na mesec. Za razliko od SKB NET-a omogoča delo brez stalne povezave z banko.
3. Multi SKB NET za velika in zelo velika podjetja z več kot 1000 transakcij na mesec. Omogoča dostop do večih bank z eno samo pametno kartico in zagotavlja prilagoditev e-bančništva obstoječemu računovodskemu sistemu v podjetju. Multi SKB NET je primeren za podjetja, ki poslujejo s tujimi poslovnimi partnerji, saj je Multi SKB NET vključen v MultiCash sistem, ki povezuje poslovalnice po vsem svetu.

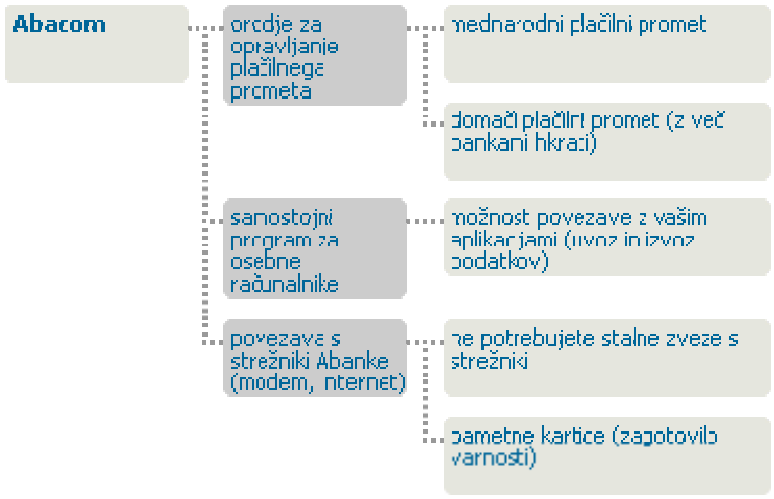
4.4.2.3 Abanka Vipa[52]

Prve produkte e-bančništva je banka ponudila le fizičnim osebam, kasneje pa so jih nadgradili za pravne osebe. Elektronska banka Abacom (glej Slika 14) je samostojni program za osebne

[51] Povzeto po spletni strani SKB banka. [URL: http://www.skb.si], 2002.
[52] Povzeto po spletni strani Abanka Vipa. [URL: http://www.abanka.si], 2002.

računalnike, ki omogoča dostop do strežnika Abanke preko klicne linije (z modemo) ali internetne povezave. Pri tem ne potrebuje stalne zveze s strežnikom v Abanki, temveč se lahko podatki shranjujejo na osebnem računalniku. Varnost zagotavlja pametna kartica, na kateri sta shranjena digitalno potrdilo in zasebni ključ. S pametno kartico se uporabnik prijavi, šifrira in elektronsko podpisuje podatke.

Slika 14: Spletna banka ABACOM



Vir: Spletna stran Abanke.2002.

Banka nudi uporabnikom dve programski različici: enouporabniško ali večuporabniško. Pri slednji lahko program uporablja več uporabnikov hkrati, ki imajo porazdeljene pravice. Pri obeh različicah varnost temelji na uporabi principov asimetrične kriptografije.

Programska različica Abacom omogoča opravljanje domačega plačilnega prometa prek več bank; Abanka, skupina NLB, Bank Austria Creditanstalt, SKB banka, Factor banka in Kartner Sparkasse. Cena programskega paketa znaša 6.000 SIT, zaščitna kartica 12.000 SIT, čitalec USB 8.500 SIT ter mesečna pristojbina za uporaba 1000 SIT oz. 2000 SIT za velika in srednja podjetja. Pri tem pa so še dodatni stroški na namestitev programa, uvajanje ter stroški za intervencijo in pomoč.

4.4.2.4 Nova kreditna banka Maribor - NKBM[53]

Poslovni BANK@NET je virtualna oblika Nove Kreditne Banke za podjetja. Poslanstvo e-bančništva v tej banki je hitro, enostavno, varno in gospodarno poslovanje z banko.

Komitentom sta na voljo dve različni namestitveni aplikaciji za elektronski način poslovanja. Eno je za banko pripravilo podjetje Hermes Softlab, drugo pa Zrcalo. Slednja omogoča e-poslovanje opravljati tudi s službenih poti ali od kod drugod, ne samo iz pisarne. Vendar

[53] Povzeto po spletni strani NKBM. [URL: http://www.nkbm.si], 2002.

uporabniki internetne različice lahko opravljajo le tolarski plačilni promet, medtem ko namestitvena različica Poslovnega Bank@Neta omogoča opravljanje tolarskega in deviznega plačilnega prometa.

Za zaščito zasebnosti pri poslovanju s Poslovnim Bank@Netom so v Novi KBM d.d. uporabili varnostni storitvi:

- overjanje - banka preveri komitenta in se prepriča o njegovi avtorizaciji v e-bančništvu,
- šifriranje - zagotavlja zaščito vsebine pred nepooblaščenimi osebami.

Poslovni Bank@Net uporablja za overjanje zahtevnejših storitev t.i. enkratna gesla, ki jih je mogoče uporabiti le enkrat. Vsak uporabnik elektronske banke dobi identifikacijsko kartico (glej Slika 15), ki vsako minuto ustvari novo geslo, znano samo lastniku kartice in elektronski banki. Geslo se pokaže na identifikacijski kartici in od tam ga stranka prepiše v sistem e-bančništva v internetu. Poleg te kartice dobi uporabnik tudi številko PIN, brez nje je identifikacijska kartica neuporabna.

Slika 15: Identifikacijska kartica za generiranje enkratnih gesel

Vir: Spletna stran NKBM, 2002.

4.4.2.5 Banka Koper[54]

Poslovna i-Net Banka zagotavlja varno poslovanje, ki temelji na kombinaciji različnih varnostnih mehanizmov: osebni certifikat, ki je shranjen na čip kartici, certifikat Banke Koper, ki ga je izdal VeriSign - svetovno priznana avtoriteta za izdajanje certifikatov, PIN in poseben PIN za odklepanje.

Do bančnih uslug na internetu je možno vstopati z uporabo spletnih brskalnikov Microsoft Explorer ali Netscape Navigator, ki podpirajo uporabo 128-bitnih SSL ključev. Podjetja, ki imajo nameščene požarne zidove, morajo zagotoviti odprtje le omejenih vrat (PORT 80 - HTTP in FTP prek HTTP in PORT 443 - SSL).

[54] Povzeto po spletni strani Banka Koper. [URL: http://www.banka-koper.si], 2002.

Tarifa za plačilni nalog preko I-net Banke znaša za posebno položnico 70 SIT po nalogu, za interni plačilni nalog na poslovni ali osebni račun 40 SIT po nalogu, za plačilni nalog BPRC, nujni nalog in posebno položnici v znesku 2 mio SIT ali več pa 620 SIT po nalogu. Cene provizij, ki jih banke zaračunavajo na bančnih okencih znašajo bistveno več, saj tarifa za posebno položnico znaša 240 sit po nalogu, plačilni nalog na poslovni račun 210 SIT na nalog ter plačilni nalog BPRČ, nujni nalog ter posebna položnica večjih zneskov 780 SIT po nalogu.

4.4.2.6 Raiffeisen krekova banka[55]

Spletna banka EUREKA, banke Raiffeinsen Krekove banke, omogoča poslovanje s tujino kot tudi opravljanje domačega plačilnega prometa. Varnost je poskrbljena v skladu z Zakonom o elektronskem poslovanju in digitalnim podpisu. Zagotavlja funkcijo zaupnosti podatkov in sporočil s šifriranjem, funkcijo celovitosti podatkov s preprečitvijo kakršne koli nepooblaščenega spreminjanja ali uničenja, funkcijo preverjanja verodostojnosti, ki jo omogoča digitalni podpis, funkcijo nepodvajanja sporočil, ki jo omogočajo s časovno oznako, dodano osnovnemu sporočilo.

V banki funkcije varnost poslovanja zagotavljajo s pomočjo:

1. čitalca kartic in pametne kartice,
2. I-key (USB) – pametnim ključem in
3. privatnim ključem, ki je shranjen na disku.

[55] Povzeto po spletni strani Raiffeisen Krekova banka. [URL: http://www.r-kb.si/eureka.htm], 2005

5 ANALIZA TVEGANJA VARNOSTI E- PLAČILNEGA SISTEMA

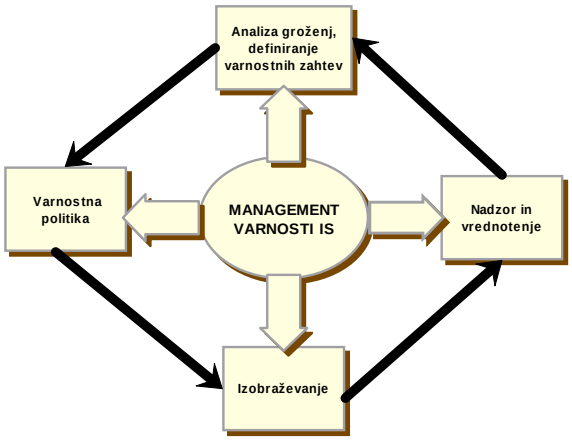
V dosedanji vsebini naloge sem zajela teoretično zasnovo problema varnosti e-poslovanja, predstavila značilnosti e-bančništva in opredelila ključne varnostne komponente. V drugem delu sem s presekom slike bančništva v Sloveniji zajela glavno ponudbo bančnih storitev e-bančništva in uporabniških vmesnikov za e-bančništvo. V zaključku magistrske naloge bom na podlagi vprašalnika o varnosti e-plačilnega sistema analizirala pridobljene podatke z vidika varnosti. Rezultati analize varnosti pri prenosu finančnih informacij med podjetjem in banko mi bodo osnova za določanje ključnih ozkih grl v e-bančništvu med podjetjem in banko ter podlaga za ukrepanje s tehnikam in metodami, ki sem jih opredelila v tretjem poglavju.

5.1 MANAGEMENT VARNOSTI ELEKTRONSKEGA PLAČILNEGA SISTEMA

Mnogi informacijski sistemi se niso izkazali za varne. Varnost, ki jo lahko dosežemo s tehničnimi sredstvi, je omejena, zato jo je potrebno dopolniti še z drugimi vzporednimi postopki. Izbira primerne kontrole zahteva natančno planiranje ter upoštevanje podrobnosti. Za upravljanje varovanja informacij je potrebno predvsem sodelovanje vseh zaposlenih v organizaciji. Prav tako je mogoče zahtevati tudi sodelovanje dobaviteljev, strank in delničarjev kot tudi strokovnih nasvetov izven organizacije. Kontrole za varovanje informacij so veliko cenejše in učinkovitejše, v kolikor so vgrajene v zahtevani specifikaciji ter že na stopnji načrtovanja programov in storitev.

Management varnosti informacijskega sistema igra pri reševanju problematike varnosti v podjetju vidno vlogo, saj z uporabo sodobnih tehnoloških rešitev le-to uspešno obvladuje in načrtuje (glej Slika 16). S pomočjo managementa varnosti informacijskega sistema podjetja izboljšujejo ozaveščenost in povečujejo zavest o pomembnosti podatkovne varnosti ter s tem zmanjšujejo penetracijo ključnih tveganj in omejijo škodo, ki bi jih nevarnosti lahko povzročile.

Slika 16: Vloga managamenta varnosti informacijskega sistema v podjetju



Vir: Internet Security Systems, 2002.

Za varnost informacijskega sistema organizacije je potrebno v prvi vrsti pripraviti strategijo varnostne politike[56], sistematizirati delovno okolje in integrirati varnostno politiko na vse organizacijske dele. To pomeni, da je potrebno določiti varnostno politiko in doseči ustrezno stopnjo zavesti o pomenu varnosti informacijskega sistema pri vseh zaposlenih kot tudi v vseh delih informacijskega sistema. Kot drugo je potrebno poznati dolgoročne in kratkoročne cilje za zagotovitev ustreznega nivoja varnosti v podjetju in ne zgolj reševati trenutno nastale težave.

Za izdelavo varnostne politike in določitev zahtevanih tehnik in mehanizmov varovanja, je v prvi vrsti potrebno »skenirati« objekt varovanja, v našem primeru podjetje, in s pomočjo analize tveganja virov v organizaciji pridobiti informacije in podatke, ki so nujno potrebni za nadaljnje aktivnosti managementa varnosti IS.

5.2 ANALIZA TVEGANJA ELEKTRONSKEGA PLAČILNEGA SISTEMA

Načrtovanje varnosti informacijskega sistema se začne z analizo tveganja. Tehnike ocenjevanja varnostnega tveganja se lahko uporabljajo v celotni organizaciji ali v posameznih oddelkih, lahko pa samo v posameznih informacijskih sistemih ali v specifičnih komponentah sistema ali storitev, kjer je to mogoče, izvedljivo in koristno. V nalogi bom analizirala le sistem e-plačilnega prometa, ki omogoča podjetjem gradnjo višjih oblik poslovnega sodelovanja z banko. Varnostna komponenta je bila in je še vedno ena ključnih dejavnikov pri prehodu s klasičnega bančništva na e-bančništvo preko interneta. Zaradi tega si vsaka banka, ki to storitev ponuja prizadeva, da bi svojo spletno poslovalnico uredila čim bolj varno in učinkovit za dosego želenega cilja.

Analiza tveganja e-plačilnega sistema je temeljni postopek, s katerim sistematično ugotovimo vire plačilnega sistema, jih opredelimo, identificiramo groženje na vire, ocenimo tveganja, ki nastanejo in nadzorujemo celoten potek plačevanja ter uresničujemo zastavljene cilje managementa varnosti e-plačilnega sistema. Analiza je temelj za odkrivanje in odpravljanje varnostnih lukenj pri e-plačevanju in podlaga za izdelavo varnostnih ukrepov. Temeljni koraki analize tveganja so (Turban, 2003, str. 404-405):

1. OCENJEVANJE – organizacija oceni svoja varnostna tveganja z določanjem svojih virov, sistemskih ranljivosti in potencialnih groženj tem ranljivostim.

2. NAČRTOVANJE – cilj te faze je dobili skupek politik, ki definirajo ključne nevarnosti in opredelijo tolerančno mejo dopustnosti ogrožanja. Grožnja je domnevno sprejemljiva, če je strošek varovanja previsok ali pa je tveganje prenizko.

[56] Varnostna politika je množica pravil, ki predpisujejo, kateri viri morajo biti zaščiteni pred katerimi grožnjami in na kakšen način. Pravila predpisujejo, kdo ima dostop do določenih informacij, katere aktivnosti subjektov so dovoljene, katere kriptografske algoritme morajo pri tem uporabljati ipd (Jerman Blažič, 2001, str. 102).

3. IMPLEMENTIRANJE – pri implementaciji se nameščajo različne tehnologije varovanja zoper grožnjam z visoko prioriteto. Izbor določenih tehnologij in mehanizmov temelji na sprejetih smernicah v fazi načrtovanja. Kot prvi korak je potrebno izbrati za vsako grožnjo visoke prioritete svojo generično tehnologijo.

4. NADZOROVANJE – je nenehen proces, ki se uporablja za določanje uspešnosti oz. neuspešnosti posameznih ukrepov, ki potrebujejo spremembe glede na nove tipe groženj, glede uporabe novih tehnologij in glede na to ali obstaja katerikoli nov posel, ki ga je potrebno zavarovati.

Namen analize je pridobiti sliko o stanju varnosti plačilnega sistema. Z analizo lahko že v proaktivni fazi varovanja ugotovimo morebitne ranljivosti računalniškega sistema ter s tem zmanjšamo morebitno škodo ob napadu oz. nastanku nevarnosti. Glede na širino delovanja e-plačilnega prometa, ki se odvija med banko in podjetjem in poteka preko javnega omrežja, je smiselno celotni proces razdeliti na posamezne segmente.

1. varnost informacijskega sistema banke,
2. varnost računalniških in komunikacijskih omrežij in
3. varnost informacijskega sistema podjetja.

Iz vsakega segmenta bomo določili kritične vire sistema, ki jih ocenimo glede na varnostne kriterije; zaupnost (Z), neoporečnost (N) in razpoložljivost (R) informacij. Omenjeni trije kriteriji varnosti, ki jih opredeljujeta tudi mednarodni standard ISO/IEC 17799-2000 in britanski standard BS 7799 (Sokol, 2000, str.3), omogočajo, da se z zagotovitvijo zasebnosti ustavijo neavtorizirani vstopi za branje občutljivih informacij, z neoporečnostjo se poskrbi, da podatki niso bili zbrisani, uničeni ali predrugačeni ter da razpoložljivost računalniškega sistema omogoči razpolaganje s podatki in storitvami ob vsakem trenutku, ko to uporabnik želi (Schneier, 2000, str. 121-122).

Prav tako bomo v nadaljevanju identificirati grožnje, zoper koga bo organizacija usmerjala svojo varnostno politiko ter opredelili ustrezne varovalne ukrepe.

5.2.1 Varnost informacijskega sistema banke

Informacijski sistem banke je zelo velik in zapleten, ki se je razvijal več desetletij. V sedanjem času predstavlja srce bančnega sistema, zato je pogosta tarča napadalcev. Banke v svoji politiki varovanja informacijskega sistema ločujejo fizični in logični del zaščite. 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 posebno dobro zaščiteni prostori, ki so zaklenjeni, opremljeni z video

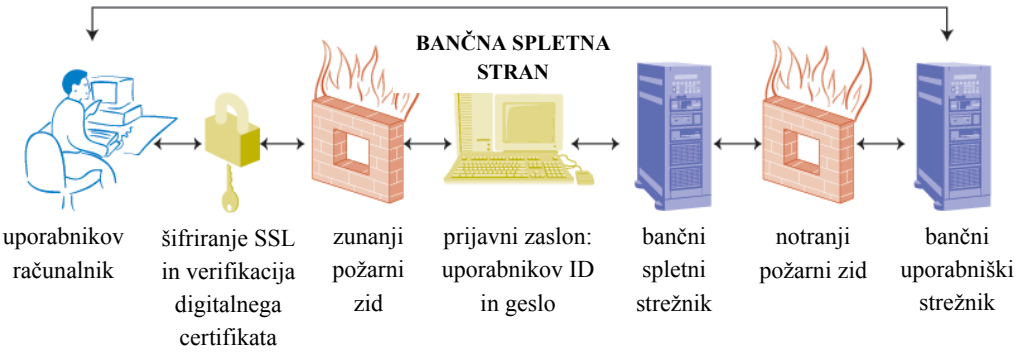
nadzorom ter so varni pred požari in poplavami. Med fizično zaščito spadajo tudi porazdelitev delovnih opravil med zaposlene, tako da nihče ne pride v stik s popolnoma vsemi podatki pri izdaji digitalnih potrdil in drugih občutljivih podatkov za vstop preko e-banke (Gril, 2003, str.9).

Logična zaščita se ukvarja z omejevanjem dostopa do informacijskih sistemov tam, kjer ni fizičnih zaščit ali kot dopolnilo k fizični zaščiti. Pri logični zaščiti pride v veljavo več tehnik in prijemov; od identifikacije in overjanja uporabnikov do šifriranja, elektronskega podpisovanja ter uporabe digitalnih potrdil. Večina logičnih zaščit je vgrajenih v programsko opremo[57] ali se predstavljajo kot samostojne aplikacije. V banki uporabljajo množico programov, ki zagotavljajo nemoteno delo s komitenti kot tudi z drugimi bančnimi poslovalnicami. Poleg operacijskih sistemov ter sistemov za upravljanje z bazami podatkov obstaja veliko število orodij, odjemalskih programov, komercialno dostopnih programskih paketov ter namenskih aplikacij, med katere sodijo tudi programske rešitve za e-bančništvo. Za namenske aplikacije v banki velja, da mora biti vsak uporabnik pooblaščen za delo z njimi. 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 transakcije, je upoštevan tudi princip ločevanja nalog.

Aplikacije so nameščene na računalnikih, ki v bančnem sistemu predstavljajo kompleksno strojno infrastrukturo. Strojno opremo predstavlja glavni računalnik, strežniki, osebni računalniki, kontrolne enote in terminal ter veliko število bankomatov in POS-terminalov. Glede na velikost banke se število strojne opreme temu primerno tudi veča. Ker so banke prisotne na celotnem slovenskem prostoru, je tudi omrežje razvejano po celi Sloveniji. Na centralni lokaciji je razmeroma kompleksen požarni zid, ki ščiti banko pred neželenimi zunanjimi vplivi na omrežje. Vsebuje večkratno filtriranje paketov in preverjanje prometa tako na transportnem nivoju kot tudi na aplikacijskem nivoju (glej sliko 17). 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. Komitentu, ki vstopa v spletno poslovalnico s svojim uporabniškim imenom in geslom, mu sistem dovoli le omejeno gibanje glede njegovih dodeljenih pravic.

[57] Programska oprema, ki povezuje banko s komitenti mora omogočiti tehnike logične zaščite. Podatki pri plačilnih transakcijah morajo biti tajni in jih lahko prebere le tisti, ki so mu namenjeni. Poleg tega pa je potrebno zagotoviti možnost za ugotavljanje verodostojnosti ter avtentičnosti izvora podatkov in na podlagi tega ugotoviti identifikacijo uporabnika. Z ugotovitvijo avtentičnosti podatkov je pošiljatelju tudi odvzeta možnost, da bi se akciji odrekel ali jo zatajil. Tako banka izvaja avtentičnost s pomočjo digitalnega podpisa in zasebnega ključa, s katerim banka identificira vsakega uporabnika, ki vstopa v njihov sistem. Digitalno potrdilo strežniku pove, kdo je, zasebni ključ pa je zato, da mu s posebnimi matematičnimi postopki to tudi dokaže. Vsak uporabnik pa ima določeno vlogo pri upravljanju računa z avtorizacijsko shemo, ki določa pravice in pooblastila vsakega uporabnika.

Slika 17: Proces plačilnega prometa v bančnem informacijskem sistemu



Vir: Turban, 2003, str.119.

5.2.2 Varnost komunikacijskih povezav

Glavna povezava med bančnim in računalniškim sistemom v podjetju je telekomunikacijsko omrežje, ki povezuje različne oddaljene lokacije. S tem ko postajajo računalniški sistemi in omrežja vse bolj odprta in lažje dostopna za uporabnike, narašča tudi možnost zlorab in število vstopnih točk, ki jih je treba zaščititi.

Telekomunikacija med računalniki poteka preko telekomunikacijskih mrež, ki predstavljajo hrbtenico za posredovanje sporočil. Osnovni model je sestavljen iz komunikacijskega prenosnega medija, ki je lahko kabel ali brezžična povezave. Kabelski komunikacijski kanali se razlikuje glede na vrsto kabla[58], ki so povezani v hrbtenico komunikacijskega omrežja, in se razlikujejo glede hitrosti in prepustnosti povezave, ki jo nudi določena tehnologija.

Vsak način prenosa ima svojo arhitekturo in sistem naslavljanja ter protokole. Internet omogoča njihovo povezavo v navideznem enotnem omrežju. Poenotenost omrežja dosežemo z enotnim komunikacijskim protokolom TCP/IP. Glavna naloga osnovnega protokola TCP/IP je, da poskrbi za pravilen prenos paketov. Paketi lahko potujejo po različnih poteh skozi omrežje. Prihajajo lahko v različnem vrstnem redu, kot so bili poslani. Njihove informacije v ovoju omogočajo, da usmerjevalniki pravilno usmerjajo pakete in ugotovijo, katera pot je najboljša in potisnejo pakete iz enega omrežja v drugega. Podatki se na naslovnikovem strežniku uredijo v pravilno zaporedje, ki jih preveri glede pravilnosti prenosa, pristnosti podatkov, avtentičnosti in identificira pošiljatelja. V primeru kakršnihkoli motenj računalnik zavrne dostop preko požarnega zidu.

[58] V praksi srečujemo naslednje kabelske povezave (Gradišar, Resinovič, 1998, str. 314-316): 1. Dvožilni telefonski kabel omogoča do 64 Kbits/s in je najpočasnejši medij. Omogoča prenos na daljšo razdaljo in zaradi izgube signala jih je potrebno ojačevati. Uporablja se za prenos zvoka in manjših količin računalniških podatkov. Slabosti so v nizki hitrosti in v oddajanju elektromagnetnih valovov, ki jih je mogoče zaznati in izvajati skrivno prisluškovanje. 2. Koaksialni kabel omogoča uporabo do 15 km in hitrost do 50 Mbit/s. Namenjen je za gradnjo lokalnih mrež in televizijskih mrež. Glavne lastnosti so majhno elektromagnetno valovanje, majhno sevanja navzven in enostavno širjenje mreže brez motenj tekočega delovanja. 3. Prihodnost je v optičnih kablih, ki vsebujejo tanka vlakna iz čistega stekla in imajo do 100 Mbits/s prenosne hitrosti. Signali se prenašajo s svetlobnimi frekvencami. Primerno za daljše razdalje, saj izgubi le malo svetlobe in je potrebno malo ponavljalnikov. Pomanjkljivost je visoka cena naprav za kodiranje in dekodiranje.

Za varnost skrbijo varnostni protokoli, ki so vključeni že v samo aplikacijo med aplikacijsko in transportno plastjo. Brskalniki imajo integriran del protokola SSL, ki danes predstavlja de facto standard. Omogoča vzpostavitev varne šifrirane povezave med dvema točkama v omrežju, strežnikom in odjemalcem. Danes že vsi najbolj razširjeni brskalniki podpirajo SSL oziroma TLS. Pri vzpostavitvi povezave z banko s pomočjo brskalnika, se običajno najprej vzpostavi nešifrirana povezava. Pri pošiljanju podatkov, se povezava spremeni v šifrirano. V naslovu se protokol spremeni v https, spremeni se številka vrat in na zaslonu se pokaže ikona zaklenjene ključavnice, ki kaže zašifrirano povezavo. Podatke o povezavi in o digitalnem potrdilu strežnika preverimo s klikom na desni gumb miške, kjer se pokažejo podatki o povezavi. Če strežnik nima digitalnega potrdila, ki ga je izdala uveljavljena ustanova, moramo prekiniti povezavo.

Protokol SSL zaščiti zgolj povezavo med dvema točkama. Za zaščito podatkov na strežnikih se je potrebno pred vdori zaščititi z nameščanjem požarnih zidov.

5.2.3 Varnost informacijskega sistema podjetja

Informacijski sistem podjetja je globalen sistem, ki povezuje vse poslovne funkcije in v katerem se informacije ustvarjajo, shranjujejo in pretakajo. Za varnost mora poskrbeti vodstvo podjetja s postavitvijo 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.

V vsej varnostni verigi je pogosto najbolj ranljiv del ravno odnos uporabnikov do e-poslovanja. Organizacije morajo dobro poskrbeti za izobraževanje vseh zaposlenih glede varnosti. Uporabnike morajo motivirati, da posvetijo ustrezno pozornost varnostni politiki, potrebno jim je razložiti pomen varnosti, zakaj so potrebne razne omejitve in kako prepoznati sumljive aktivnosti v postopkih poslovanja. Seznanile naj bi jih s škodljivimi vplivi iz okolja in jih poučile o potrebnem zavarovanju pred njimi. Veliko problemov si lahko prihranijo že z obveščanjem uporabnikov o nevarnostih povezanih z virusi, ki jih lahko dobijo e-pošte ali preko interneta. Organizacije morajo 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. Določiti je potrebno posameznikovo odgovornost pri rokovanju z ranljivimi viri in podatki in določiti pravila za dostop do ranljivih virov in podatkov.

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.

5.3 KORAKI ANALIZE TVEGANJA V E-PLAČILNEM SISTEMU

V nalogi smo pri izvedbi analize ocenili vire in groženje s pomočjo kvalitativne metode[59]. Metoda se mi v proučenem primeru zdi primerna, ker s pomočjo notranjih in zunanjih strokovnjakov opisno ovrednotimo nastalo problematiko. Narava problematike ne omogoča, da bi vse spremenljivke kvantitativno izrazili in merili. Tako sem s pomočjo vprašalnika, ki sem ga prilagodila za posameznega ocenjevalca[60], glede na njihovo vlogo in povezanost z e-plačevanjem, dobila skupno ocene potencialnih virov, groženj in stopenj ogroženosti. Ocena je rezultat videnja različnih subjektov, ki na problematiko gledajo iz različnih perspektiv in posameznemu viru ter grožnji predpisujejo različno težo pomena. Prav tako so pridobljene ugotovitve rezultat skupnega videnja in niso specifično vezane na določeno podjetje.

5.3.1 Faza ocenjevanja

Namen prve faze ocenjevanja je vrednostno izraziti zahtevano stopnjo tveganja virov, in opredeliti potenciale nevarnosti na vire. Iz vsakega segmenta, ki sem jih opredelila v prejšnjem podpoglavju, identificiramo glavne vire za nadaljnjo analizo. Upoštevamo le ključne vire, ki so pomembni za delovanje e-plačilnega prometa in so med ranljivejši glede na napad groženj (glej Tabela 7).

Tabela 7: Delitev virov za posamezna področja

Področje:	INFOR. SISTEM PODJETJA	KOMUNIKACIJSKO OMREŽJE	INFOR. SISTEM BANKE
Viri:	Delovna postaja	Protokoli modela TCP/IP in SSL	Namenska programska oprema
	Računalniško omrežje - LAN	Komunikacijski kanal	Bančni strežnik, požarni zid
	Informacijski sistem in BP	Usmerjevalniki, mostovi, stikala	Informacijski sistem in BP

Zgoraj našteti viri zajemajo stojno in programsko opremo ter vključuje tudi človeški faktor. Vsak vir izvaja funkcijo pri e-plačilnem sistemu in omogoča da se informacije varno in zanesljivo dostavijo do naslovnika oz. pošiljatelja.

[59] Kvalitativna metoda je kvalitativna ocena tveganja v okolju računalniških operacij, ki so jo razvili predvsem zaradi nezadovoljstva z drugimi metodami (kvantitativnimi in primerjalnimi metodami). Je manj natančna, dolgotrajnejša vendar zanesljivejša kot metoda kvantitativne analize. Kvalitativna metoda se od kvantitativne razlikuje predvsem v tem, da za oceno tveganja ne potrebuje natančnih numeričnih vrednosti, ki so rezultat vrednotenja dobrin in groženj. Vrednotenje dobrin je lahko kvantitativno ali kvalitativno, vse kvantitativne ocene dobrin pretvorimo v kvalitativne, ostale dobrine, ki jih pa nismo uspeli kvantitativno ovrednotiti, pa s pomočjo vprašalnikov vrednotimo kvalitativno. Vse osebje, ki je kakorkoli povezano s prenosom transakcij preko interneta, moramo vključiti v ocenjevanje. Kadri, ki dobro poznajo informacijsko problematiko, naravo poslovanja, procese, konkurente, različne probleme, ki nastopajo ter njihovo reševanje v preteklosti, so vir informacij o tveganjih ter grožnjah sistemu, iz katerih lahko ocenjujemo obliko in obseg preventivne dejavnosti.

[60] Pri ocenjevanju so sodelovali: informatik v podjetju PREVENT d.d., finančna delavka v podjetju PREVENT d.d., programski razvijalec v podjetju Halcom informatika in Hermes Softlab, kriminalistični inšpektor, programer iz IT firme, maneger iz podjetja PALOMA, bančna referentka in samostojni podjetnik.

5.3.1.1 Ocenjevanje zahtevane stopnje varnosti

V prvem koraku ocenimo vire e-plačilnega sistema glede na stopnjo tveganja oz. glede na to, kako organizacije usmerjajo svojo varnostno politiko z opredelitvijo ustreznih varnostnih ukrepov. Vrednotenje je izvedeno s pomočjo opisnih spremenljivk[61], kjer ocena 1 ponazarja nepomemben vpliv, oceno 5 pa ključen vpliv vira pri opravljanju e-plačevanja. V Tabeli 8, Tabeli 9 in Tabeli 10 so združene ocene ocenjevalcev virov glede na zahtevano stopnjo varnosti e-plačevanja .

Tabela 8: Ocena virov IS podjetja glede zahtevane stopnje varnosti

VIR	OPIS	OCENA
Delovna postaja	Strojna in programska oprema z vso pripadajočo opremo za šifriranje in e-podpisovanje ter obnašanje uporabnika	*Z:5 N:4 R:3*
Računalniško omrežje - LAN	Komunikacijska infrastruktura v podjetju s pripadajočimi stikali, strežniki in nameščenimi požarnimi pregradami	*Z:3 N:4 R:4*
Informacijski sistem in BP	Integracija informacijskega sistema s programsko zasnovo in vloga BP ter povezava s finančnim sektorjem	*Z:4 N:4 R:3*

Tabela 9: Ocene virov komunikacijskega omrežja glede zahtevane stopnje varnosti

VIR	OPIS	OCENA
Protokoli modela TCP/IP in SSL	Komunikacijski protokoli za prenos podatkov v javnem omrežju	*Z:3 N:4 R:4*
Komunikacijski kanal	Telekomunikacijsko omrežje in fizična povezava podjetja in banke	*Z:2 N:3 R:5*
Usmerjevalniki, mostovi, stikala	Strojna in programska oprema za usmerjanje paketov v omrežju	*Z:2 N:2 R:4*

Tabela 10: Ocene virov IS banke glede zahtevane stopnje varnosti

VIR	OPIS	OCENA
Namenska programska oprema	Programska podpora za e-poslovanje (bančna spletna aplikacija, brskalnik)	*Z:4 N:4 R:3*
Bančni strežnik, požarni zid	Strojna in programska podpora za dostop do interneta	*Z:4 N:4 R:4*
Informacijski sistem in BP	Integracija informacijskega sistema s programsko zasnovo in vloga baze podatkov	*Z:4 N:4 R:3*

V prvem stolpcu je ime vira, ki predstavlja pomemben del pri e-plačilnemu prometu. V drugem stolpcu je opis vira in v zadnjem je ocena pomembnosti vira. Iz zgoraj opredeljenih ocen ugotavljamo, da je najbolj tvegan vir delovna postaja. Iz tega lahko sklepamo, da je delovna postaja, kjer uporabnik neposredno operira z informacijami in izvaja potrebna opravila, najnevarnejše področje in hkrati tudi najbolj ključnega pomena za pravilnost, brezhibnost in varnost poslovanja s finančnimi podatki v povezavi z banko.

[61] Ocene: 1 – nepomemben, 2 – majhen, 3 – srednji, 4 – pomemben in 5 – ključen.

5.3.1.2 Ocenjevanje potencialnih groženj za vire

Viri računalniškega sistema so izpostavljeni številnim nevarnostim in grožnjam. Nevarnosti izhajajo iz same narave sistema, človeških omejitev kot tudi iz okolja. Varnostne grožnje, ki pretijo virom iz omenjenih okolij, lahko razdelimo v naslednje osrednje kategorije (Gradišar in Resinovič 1998, 429-435):

- Namerne / nenamerne grožnje: Učinki groženj so lahko posledica namernega ali nenamernega delovanja. Nenamerne grožnje so nesreče zaradi napačnega ravnanja človeka, strojne okvare, napake v programu ali v podatku, poškodbe računalniške opreme, neprimerne tehnične značilnosti ali neodgovornosti uporabnikov. Subjekti lahko tako nenamerno povzročijo škodo zaradi napačnih posegov v sistem ali pa namerno iz različnih motivov: škodoželjnosti, koristoljubja, blatenja imena, publicitete ali samopotrjevanja. Tipične namerne grožnje so dejanja računalniškega kriminala, vohunstva, terorizma, vandalizma in kraje.

- Zunanje / notranje grožnje: Storilci dejanj prihajajo iz vrst zaposlenih, ki imajo dostop do varovanih podatkov ali nedovoljeno posestvujejo le-te kot tudi drugi storilci, ki v organizaciji vstopajo od zunaj.

- Pasivne / aktivne grožnje: Glede na način prestrezanja in upravljanja z nedovoljenimi informacijami ločimo aktivne in pasivne grožnje. Pri slednjih podatki ohranijo svojo prvotno obliko, vendar jih s prisluškovanjem komunikacijskim kanalom prestrežejo ali zlorabijo. V drugem primeru storilci podatke predrugačijo, zbrišejo ali kako drugače aktivno vplivajo na prvotno obliko.

V Tabeli 11 so naštete posamezne nevarnosti, ki so zaokrožene v posamezen sklop nevarnosti.

Tabela 11: Potencialne grožnje na vire e-plačilnega prometa

NARAVNE NESREČE	TEHNIČNE OKVARE	NENAMERNE ČLOVEŠKE NAPAKE	NAMERNE ČLOVEŠKE NAPAKE
Potres	Okvara računalnika, diska	Nestrokovnost	Zlonamerna prog. oprema
Poplava	Poškodba strojne opreme	Neodgovornost	Rač. kriminal, vandalizem
Požar	Neprimerna zmogljivost	Nevednost	Prisluškovanje
Plaz zemlje	Prekinitev ali motnja zvez	Malomarnost	Prestrezanje in zloraba
	Neprimerne tehnične značilnosti	Neupošt. varnostne politike	Spreminjanje in uničenje

5.3.2 Faza načrtovanja

V prvem delu smo identificirali ključne vire in nevarnosti e-plačilnega prometa ter vire ocenili glede na zahtevano stopnjo varnosti. Namen druge faze načrtovanja, je dobiti skupno

oceno ogroženosti vira, kjer v ocenjevanje vključimo potencialne grožnje na vire e-plačilnega prometa. Cilj faze je, da določimo tolerančni prag dopustnosti nevarnosti groženj, glede na vsoto vseh ocen, ki določajo stopnjo ranljivosti posameznega vira na grožnje. Ocena ogroženosti vira je za organizacijo prvi pokazatelj, kje je največja verjetnost napada groženj na njihove vire pri e-plačilnem prometu in hkrati se z analizo pokažejo varnostne luknje. To pomeni za organizacijo opozorilni znak za ukrepanje, še preden nastane škoda.

5.3.2.1 Ocenjevanje stopnje ogroženosti vira

Vsak vir a analizi tveganja ocenimo glede na ogroženost na potencialne grožnje. Pri tem smo si postavili vprašanje, kako bi grožnja vplivala na zaupnost informacij, na spremembo informacij in na razpoložljivost delovanja sistema. Ocene so rezultat subjektivnega videnja posameznega ocenjevalca v raziskavi. Rezultat spodaj podanih ocen pomeni povprečje vsot vseh zbranih ocen sodelujočih. V Tabelah 12-17 so podane ocene verjetnosti nastopa potencialnih groženj na vir.

Tabela 12: Ocena stopnje ogroženosti virov IS podjetja

VIR	GROŽNJE	OCENA
Delovna postaja	Kršenje varnostne politike in politike varovanja gesel	*Z:4 N:4 R:3*
Delovna postaja	Tehnične okvare	*Z:4 N:3 R:4*
Delovna postaja	Nenamerne človeške napake	*Z:4 N:3 R:4*
Delovna postaja	Namerne človeške. napake	*Z:4 N:3 R:4*
Računalniško omrežje - LAN	Naravne nesreče	*Z:2 N:3 R:3*
Računalniško omrežje - LAN	Tehnične okvare	*Z:3 N:3 R:3*
Računalniško omrežje - LAN	Nenamerne človeške napake	*Z:3 N:3 R:3*
Računalniško omrežje - LAN	Namerne človeške napake	*Z:4 N:4 R:4*
Informacijski sistem in BP	Naravne nesreče	*Z:2 N:2 R:4*
Informacijski sistem in BP	Tehnične okvare	*Z:2 N:3 R:4*
Informacijski sistem in BP	Nenamerne človeške napake	*Z:4 N:3 R:3*
Informacijski sistem in BP	Namene človeške napake	*Z:4 N:4 R:3*

Najbolj ranljiv vir v podjetju pri prenosu podatkov v banko, je po ocenah ocenjevalcev ponovno delovna postaja. Največja nevarnost preti s strani malomarnosti uporabnikov, slabe varnostne politike in nedorečenih varnostnih zahtev, ki bi jih morali uporabniki dosledno upoštevati. Vzroke za to iščemo v pomanjkanju zanimanja vodstvenih ljudi za varnost podatkov in premalo izobraževanj uporabnikov na področju varnosti IS. Glavne groženje izhajajo iz človeškega faktorja, ki s svojim ravnanjem zavestno ali nezavestno škoduje pri varovanju ranljivih informacij. Kot primer vdora v IS podjetja je eden izmed sodelujočih v raziskavi omenil, da nepooblaščena oseba izvede vdor povsem na legalen način. V podjetju se predstavi pod lažnim imenom firme, ki po navodilo neke organizacije opravlja določen pregled ali nameščanje programov. Na ta način se s svojim računalnikom priklopi na njihov IS in z raznimi programi prestreže želene informacije ali z vnosom podatkov ali programov povzroči škodo. S socialnim inženiringom napadalci pogosto na povsem legalen način

komunicirajo z osebjem iz organizacij in s prijaznim načinom preslepijo osebje, da jim zaupajo podatke, ki jih potem uporabijo v nelegalne namene. Zasledilo smo kar nekaj primerov, ko računalniški kriminal izkorišča naivnost in nevednost ljudi. Potrebno se je zavedati, da varnost ni le stvar informatikov, temveč podjetja kot celota. Ljudje so najšibkejši člen v verigi, zato je potrebno veliko vložiti v notranjo ozaveščenost in izobraževanje zaposlenih ter v njih povečati razumevanje varnostne politike. Statistike kažejo, da večino zlorab zakrivijo zaposleni s pooblastili (48%), zaposleni brez pooblastil (24%) kot tudi bivši zaposleni. Zakaj je tako, je povsem druga zgodba, ki pa pogosto ostane nedotaknjena.

Tabela 13: Ocena stopnje ogroženosti komunikacijskega omrežja

VIR	GROŽNJE	OCENA
Protokoli modela TCP/IP	Naravne nesreče	*Z:2 N:3 R:3*
Protokoli modela TCP/IP	Tehnične okvare	*Z:4 N:4 R:4*
Protokoli modela TCP/IP	Nenamerne človeške napake	*Z:3 N:3 R:4*
Protokoli modela TCP/IP	Namerne človeške napake	*Z:4 N:4 R:4*
Komunikacijski kanal	Naravne nesreče	*Z:3 N:2 R:3*
Komunikacijski kanal	Tehnične okvare	*Z:3 N:2 R:3*
Komunikacijski kanal	Nenamerne človeške napake	*Z:3 N:3 R:4*
Komunikacijski kanal	Namerne človeške grožnje	*Z:4 N:3 R:4*
Usmerjevalniki, mostovi	Naravne nesreče	*Z:2 N:2 R:4*
Usmerjevalniki, mostovi	Tehnične okvare	*Z:2 N:2 R:4*
Usmerjevalniki, mostovi	Nenamerne človeške napake	*Z:3 N:3 R:4*
Usmerjevalniki, mostovi	Namerne človeške napake	*Z:3 N:3 R:4*

Komunikacijsko okolje predstavlja največjo spremembo med klasičnim in elektronskim načinom poslovanja. Javno omrežje je virtualno področje, ki za marsikoga ostaja nerazumljivo področje in zbuja dvom o popolnosti in varnosti. Iz podanih ocen lahko sklepamo, da so poglavitne grožnje komunikacijskemu omrežju namerna človeška dejanja, ki s posegi v komunikacijo prisluškujejo, prestrezajo in zlorabljajo podatke. Najvišje ocene so podane za kriterij razpoložljivosti. Iz tega lahko sklepamo, da je komunikacijsko omrežje z vidika izvajanje nalog e-plačevanja najpomembnejša pri zagotavljanju brezhibnosti prenosa. Cilj prenosa je dosežen, ko paketi dospejo nepoškodovani in pravočasno od naslovnika do banke. Danes se z uporabo sodobnih načinov telekomunikacijskih povezav zmanjšuje možnost prestrezanja informacij s prisluškovanjem. Kljub temu pa možnosti za moteno delovanje e-bančništva obstajajo. Kot ena najpogostejših motenj so prekinitve in počasnost komunikacijskih povezav, ki niso zmožne v normalnem času izvesti želene transakcije komitentov. Te motnje so se v zadnjem letu bistveno zmanjšale, saj so sisteme dogradili in odpravili pomanjkljivosti, ki so se pojavljale na samem začetku.

Tabela 14: Ocene stopnje ogroženosti virov bančnega IS

VIR	GROŽNJA	OCENA
Namenska programska oprema	Naravne nesreče	*Z:3 N:3 R:3*
Namenska programska oprema	Tehnične okvare	*Z:4 N:4 R:4*
Namenska programska oprema	Namerne človeške napake	*Z:4 N:4 R:3*
Namenska programska oprema	Napadi na šifrirni sistem, vdori v program	*Z:4 N:3 R:3*
Informacijski sistem in BP	Naravne nesreče	*Z:3 N:4 R:4*
Informacijski sistem in BP	Tehnične okvare	*Z:3 N:4 R:4*
Informacijski sistem in BP	Nenamerne človeške napake	*Z:3 N:3 R:3*
Informacijski sistem in BP	Namerne človeške napake	*Z:4 N:4 R:5*
Bančni strežnik, požarni zid	Naravne nesreče	*Z:3 N:4 R:4*
Bančni strežnik, požarni zid	Tehnične okvare	*Z:3 N:4 R:4*
Bančni strežnik, požarni zid	Nenamerne človeške napake	*Z:4 N:3 R:4*
Bančni strežnik, požarni zid	Namerne človeške grožnje	*Z:5 N:5 R:4*

Bančno okolje je specifično okolje in ga je težko primerjati z okoljem podjetja. Na strani bank je zadevo veliko bolj varovana, vendar zaradi obsežnosti obdelav podatkov in velike stopnje varovanja lahko že nepomemben vdor povzroči velik preplah pri komitentih in drugih uporabnikih njihovega sistema, ki si pomen vdora interpretirajo kot nezanesljiv način poslovanja z njihovimi prihranki. Iz zgornje tabele izhaja, da so podane največje ocene glede verjetnosti namernih vdorov v sistem. Po mojem mnenju je glavni razlog za visoko oceno ocenjevalcev, količina zaupnih podatkov in stopnja njihovega varovanja. Podatke je potrebno varovati pred nepooblaščenimi osebami kot tudi ščititi del informacij pred pooblaščenimi osebami, da ne bi banka imela popolnega nadzora nad tajnimi informacijami (javni ključ, gesla, itd.) določenega komitenta. Visoko oceno je dobila tudi namenska programska oprema, ki v verigi e-plačilnega prometa predstavlja most med banko in komitentom. Pri tem pa bi še dodala, da se komitenti niti ne zavedajo, da je pogost vzrok za zlorabo njihovega bančnega računa prav njihova nepazljivost pri povezovanju z bančnim strežnikom in neupoštevanje sprotnega ažuriranja digitalnega potrdila in preverjanje le-tega.

5.3.2.2 Skupna ocena ogroženosti

Če združimo obe oceni (oceno stopnje zahtevane varnosti in oceno ogroženosti vira), dobimo skupno oceno tveganja, ki nam pove, kako je posamezen vir ranljiv pri delovanju e-plačevanja. V spodnji Tabeli 14 je skupna ocena ogroženosti za področje IS podjetja. V zadnjem stolpcu je skupna ocena tveganja posameznega vira, ki je seštevek vseh treh kriterijev (zaupnost, neoporečnost, razpoložljivost).

S sodelujočimi pri ocenjevanju smo postavili mejo med bolj in manj občutljivimi viri področij. Vse vire, ki imajo skupno vsoto tveganja več kot 22 smo kategorizirali kot ranljivejše vire visoke prioritete in so povzeti v Tabeli 17.

Tabela 15: Skupna ocena ogroženosti IS podjetja

VIR	OPIS	OCENA	VSOTA
Delovna postaja - računalnik	Varnostna politika	**Z:9 N:8 R:6**	**23**
Delovna postaja - računalnik	Tehnične okvare	**Z:9 N:7 R:7**	**23**
Delovna postaja - računalnik	Nenamerne človeške napake	**Z:9 N:7 R:7**	**23**
Delovna postaja - računalnik	Namerne človeške napake	**Z:9 N:7 R:7**	**23**
Računalniško omrežje - LAN	Naravne nesreče	**Z:5 N:7 R:7**	**19**
Računalniško omrežje - LAN	Tehnične okvare	**Z:6 N:7 R:7**	**20**
Računalniško omrežje - LAN	Nenamerne človeške napake	**Z:6 N:7 R:7**	**20**
Računalniško omrežje - LAN	Namerne človeške napake	**Z:7 N:8 R:8**	**23**
Informacijski sistem in BP	Naravne nesreče	**Z:6 N:6 R:7**	**19**
Informacijski sistem in BP	Tehnične okvare	**Z:6 N:7 R:7**	**20**
Informacijski sistem in BP	Nenamerne človeške napake	**Z:8 N:7 R:6**	**21**
Informacijski sistem in BP	Namerne človeške napake	**Z:8 N:8 R:6**	**22**

Tabela 16: Skupna ocena ogroženosti komunikacijskega omrežja

VIR	OPIS	OCENA	VSOTA
Protokoli modela TCP/IP	Naravne nesreče	**Z:5 N:7 R:7**	**19**
Protokoli modela TCP/IP	Tehnične okvare	**Z:7 N:8 R:8**	**23**
Protokoli modela TCP/IP	Nenamerne človeške napake	**Z:6 N:7 R:8**	**21**
Protokoli modela TCP/IP	Namerne človeške napake	**Z:7 N:8 R:8**	**23**
Komunikacijski kanal	Naravne nesreče	**Z:5 N:5 R:8**	**18**
Komunikacijski kanal	Tehnične okvare	**Z:5 N:5 R:8**	**18**
Komunikacijski kanal	Nenamerne človeške napake	**Z:5 N:6 R:9**	**20**
Komunikacijski kanal	Namerne človeške napake	**Z:6 N:6 R:9**	**21**
Usmerjevalniki, mostovi	Naravne nesreče	**Z:4 N:4 R:8**	**16**
Usmerjevalniki, mostovi	Tehnične okvare	**Z:4 N:4 R:8**	**16**
Usmerjevalniki, mostovi	Nenamerne človeške napake	**Z:5 N:5 R:8**	**18**
Usmerjevalniki, mostovi	Namerne človeške napake	**Z:5 N:5 R:8**	**18**

Tabela 17: Skupna ocena ogroženosti IS banke

VIR	OPIS	OCENA	VSOTA
Namenska programska oprema	Naravne nesreče	**Z:7 N:7 R:6**	**20**
Namenska programska oprema	Tehnične okvare	**Z:8 N:8 R:7**	**23**
Namenska programska oprema	Napadi na šifrirni sistem	**Z:8 N:7 R:6**	**21**
Namenska programska oprema	Namerne človeške napake	**Z:8 N:8 R:6**	**22**
Informacijski sistem in BP	Naravne nesreče	**Z:7 N:8 R:8**	**23**
Informacijski sistem in BP	Tehnične okvare	**Z:7 N:8 R:8**	**23**
Informacijski sistem in BP	Nenamerne človeške napake	**Z:7 N:7 R:7**	**21**
Informacijski sistem in BP	Namerne človeške napake	**Z:8 N:8 R:9**	**25**
Bančni strežnik, požarni zid	Naravne nesreče	**Z:7 N:8 R:7**	**24**
Bančni strežnik, požarni zid	Tehnične okvare	**Z:7 N:8 R:7**	**24**
Bančni strežnik, požarni zid	Nenamerne človeške napake	**Z:8 N:7 R:7**	**22**
Bančni strežnik, požarni zid	Namerne človeške napake	**Z:9 N:9 R:7**	**25**

Iz zgornjih tabel lahko razberemo, da je med najbolj ranljivimi viri e-plačilnega sistema po

ocenah ocenjevalcev delovna postaja, IS in BP v banki kot tudi bančni strežnik. Iz pridobljenih rezultatov lahko ugotavljamo, da so bile podane dokaj visoke ocene, kar potrjujejo visoke zahteve po varnosti v e-poslovanju. Že v poglavju o varnosti sem opozorila, da so algoritemski sistemi že zelo dovršeni in izpopolnjeni, ter da se storilci raje poslužujejo lažjih načinov dostopov in čakajo na napake uporabnikov in drugih v verigi e-plačilnega sistema. Delovna postaja je prvi člen v verigi, kjer se vnašajo vhodni podatki in kjer se opravi največji operativni fizični del e-transakcije. Vloga finančnih administratorjev je na prvi pogled nepomembna, vendar ob podrobnejšem pregledu njihovih pooblastil za izvajanje nalog, zaznamo pomembno vlogo, ki ni zanemarljiva. Pri tem pa ne smemo prezreti dejstva, da vloga finančne administratorke v podjetju pri vključitvi v izobraževanje o informacijskemu sistemu in varnosti računalniškega sistema vse prej kot dobra.

Visoke ocene so bile podane tudi pri virih banke, kjer med skrb vzbujajočimi prištevajo skoraj vse podane vire. Veliko težo k takšni oceni prav gotovo prispeva dejstvo, da operirajo z občutljivimi podatki kot tudi z ogromno količino informacij. Pri tem bi opozorila, da se informacijski sistem v finančnih institucijah brez dvoma razlikuje od informacijskega sistema podjetja. Potreben je večji poudarek na zaščiti informacijskih sistemov, saj komitenti za varnost svojega denarja zahtevajo visoko stopnjo varnosti, zaupnosti in tajnosti poslovanja. Bistvo bančnega informacijskega sistema je delovanje notranjega informacijskega sistema banke. Na bančni strani mora sistem e-bančništva delovati neprestano in stabilno, poskrbljeno mora biti za varnost dostopa do bank in ustrezno avtorizacijo dokumentov. Pri tem bi opozorila na kar nekaj storjenih kaznivih dejanj, ki jih storijo storilci s pomočjo bančnih uslužbencev, kateri pridobljene zaupne informacije odnašajo iz bančnega sistema. Žal ti podatki pogosto ostanejo skriti pred javnostjo, saj se tako izognejo izgubi ugleda in posrednim posledicami izgube komitentov in zaupanja.

5.3.3 Faza implementiranja

Pri ocenjevanju virov so se pokazala ozka grla varnosti e-plačilnega sistema. V Tabeli 18 so izluščeni vsi prioritetni viri, ki imajo skupno vsoto ocene tveganja več kot 22. Ti kritični viri e-plačilnega prometa, po mnenju ocenjevalcev, predstavljajo podjetjem in bankam največjo potencialno nevarnost za zlorabo ali uporabo v nezakonite namene. Za izboljšanje varnostne slike in odpravo pomanjkljivosti, ki smo jih dobili z rezultati analizi, je potrebno v podjetjih in bankah uvesti razne dodatne ukrepe za preprečitev morebitnih napadov.

Tabela 18: Najbolj ranljivi viri pri e-plačilnem sistemu

VIR	OPIS	VSOTA
INFOR. SISTEM PODJETJA		
Delovna postaja - računalnik	Varnostna politika	**23**
Delovna postaja - računalnik	Tehnične okvare	**23**
Delovna postaja - računalnik	Nenamerne človeške napake	**23**
Delovna postaja - računalnik	Namerne človeške napake	**23**
Računalniško omrežje - LAN	Namerne človeške napake	**23**
KOMUNIKACIJSKO OMREŽJE		
Protokoli modela TCP/IP	Tehnične okvare	**23**
Protokoli modela TCP/IP	Namerne človeške napake	**23**
INFOR. SISTEM BANKE		
Namenska programska oprema	Tehnične okvare	**23**
Informacijski sistem in BP	Naravne nesreče	**23**
Informacijski sistem in BP	Tehnične okvare	**23**
Informacijski sistem in BP	Namerne človeške napake	**25**
Bančni strežnik, požarni zid	Naravne nesreče	**24**
Bančni strežnik, požarni zid	Tehnične okvare	**24**
Bančni strežnik, požarni zid	Namerne človeške napake	**25**

Forchtova v knjigi Computer security management navaja splošne smernice zmanjšanja števila nesreč in računalniškega kriminala, ki bi jih morali uvesti v organizacijah kot tudi stalno spremljati njihovo zadovoljivost. Te so:

- vzdrževanje fizične varnosti,
- nadzor dostopa do računalnikov in mrež,
- nadzor obdelave podatkov,
- spremljanje delovanja sistema,
- priprava na nesrečo, itd.

To so le grobi ukrepi, ki se jih posamezna podjetja lotevajo na različne načine. Iz njih je mogoče izpeljati vrsto konkretnih ukrepov, ki so specifični za vsako organizacijo. Nekaj načinov ukrepanja, sem zajela v spodnjih alinejah.

INFORMACIJSKI SISTEM PODJETJA

- Pravilo »čiste mize«; pospravljati papirje in skrbno varovati pametne kartice kot tudi številko PIN in druga gesla. Poskrbeti je treba za osnovno pravilo "čiste" mize, kar pomeni, da uporabniki po končanem delu ne smejo puščati dokumentov s podatki na mizi in da morajo zaklepati predale in omare, kjer hranijo zaupne podatke. Dokumente, ki se ne potrebujejo več je treba uničiti s sežiganjem ali razrezanjem, oziroma jih zanesljivo zbrisati.
- Omejiti pravice dostopa do računalnikov kot tudi do podatkov na njih ter zagotoviti nadzor nad prihajajočimi in odhajajočimi podatki iz drugih omrežij in medijev.
- Ažurno nameščanje novih antivirusnih programov.
- Veliko skrb je potrebno posvetiti ustreznemu hranjenju pametnih kartic in gesel, ki so

potrebna za logiranje v bančni sistem za e-plačevanje.
- Informiranje in opozarjanje uporabnikov ter vzpostavitev dodatnih kontrol.
- Fizično ločiti računalnik od drugih in ne dovoliti, da prihajajo nepooblaščene osebe v stik s tem računalnikom.
- 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.
- Izobraževanje administratorjev, nadzor nad njihovim delom, občasna preverjanja namestitev in izvajanje notranje kontrole.
- Paketna obdelava podatkov z enkratno vključitvijo v bančni sistem.

KOMUNIKACIJSKO OMREŽJE
- Preprečiti prisluškovanje in prestrezanje z uporabo močnih šifrirnih sistemov. Potrebno je tudi sprotno ažurirati in uporabljati močnejše ključe.
- Uporaba optičnih kablov, kjer ni mogoče prestrezanja magnetnih signalov.
- Nadzor nad delom sistemskih analitikov, ki nastavljajo pravice uporabnikom in zasledujejo varnostni politiki.
- Uporaba najsodobnejših požarnih pregrad.

INFORMACIJSKI SISTEM BANKE
- Naložba v rezervni računalniški center bi preprečila izpade ob naravnih nesrečah.
- Namestitev zmogljivejših strežnika, ki bi bili kos močnejšemu prometu.
- Dobro testiranje programskih aplikacij, preskušanje vseh možnih kombinacij, da se odkrijejo morebitne luknje – nadzor kakovosti programske opreme.
- Protivirusni programi, požarni zid in stroga disciplina uporabe e-pošte zmanjšuje verjetnost zlonamernih računalniških programov.
- Posodabljanje starejših baz podatkov, ki še niso vsebovale toliko varnostnih zahtev, kot jih imajo današnje.
- Različni nivoji pravic dostopa in dosledno izvajanje notranje kontrole.

Pri konkretni uporabi varnostnih mehanizmov se zastavi vprašanje, katere mehanizme je treba implementirati in koliko. Odgovor je nekako takšen: toliko, da bo ravno prav! Da, ravno prav, če so informacije premalo varovane in zaščitene, se lahko ob varnostnem incidentu zgodi nezaželeno, dostikrat povezano z negativnimi posledicami pri poslovanju: izguba dobrega imena, finančna izguba, ogrožanje poslovanja in drugo. Če pa smo uporabili preveč varnostnih mehanizmov, se kaj hitro izkaže, da smo informacije sicer zaščitili, vendar smo njihovo uporabo, dostopnost zelo otežili, če ne celo onemogočili, ter za to porabili ogromno sredstev, časa in energije. Dejstvo je, da popolnega varovanja informacij ni in ga tudi ne bo, ker ni smiselno!

5.3.4 Faza nadzorovanja

Zadnja faza – faza nadziranja je ena najpomembnejših faz, saj lahko s preventivo preprečimo marsikatero škodo, ki bi jo povzročile morebitne grožnje. Podjetja kot tudi banke se morajo zavedati, da z naraščanjem števila sodobne informacijske opreme v praktično vseh družbenih dejavnostih kaže na povečanje e-poslovanja in s tem posredno teži k povečanju števila in vrednosti poslovnih transakcij preko interneta. Pomembno je, da razumejo potrebo, ki neposredno vpliva na povečanje potrebe po varnem, cenenem, hitrem in zanesljivem plačevanju preko interneta. To pa ni mogoče, če se ne prenese v praktično uporabo in se upoštevajo ta spoznanja pri uvajanju kot tudi opravljanju prenosa transakcij.

Po določilih varnostnih zahtev v organizaciji in izbiri primernih varnostnih mehanizmov sledi določitev pripadajoče varnostne kontrole, ki udejanja varnostne mehanizme. Od izbire varnostnih kontrol je odvisno, kako bomo informacijam in sistemom zagotavljali zaupnost, popolnost in razpoložljivost. Med splošne varnostne kontrole vključujemo (Forcht, 1998, str. 419-420):

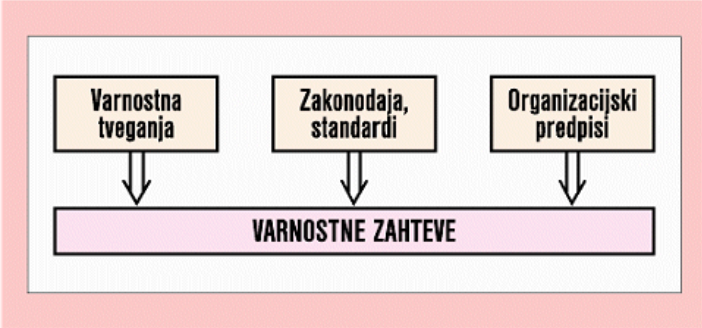
- organizacijske in administrativne kontrole, ki zagotavljajo učinkovito ločevanje funkcij in omejitev pri dostopu do podatkov, dopolnjenih s testiranjem učinkovitosti zaščitnih varnostnih procedur,
- avtentičnost uporabnikov, dopolnjena z dodatnimi procedurami verifikacije, namenjenim dokazovanju legitimnosti uporabnika,
- fizične varnostne ukrepe, namenjene zagotavljanju kontinuitete procesnih servisov v primeru naravnih in človeških katastrof in za nadzor nad dostopom ter
- določila komunikacijskih protokolov, ki so posebej vključeni za zagotavljanje varovanja podatkov.

Mnenja drugih strokovnjakov so, da bi naj spisek kontrol vseboval še notranjo kontrolo, administrativno in fizično kontrolo, usposobljenost in strokovnost kadra, integriteto podatkov, integriteto programske opreme, komunikacijske kontrole, stroškovne kontrole, interaktivne kontrole, itd. V primeru nastale nevarnosti je nadzorni organ tisti, ki ukrepa prvi in ki mora zaščititi druge vire, ki niso napadeni, in preprečiti morebitno nadaljnje širjenje nevarnosti. Dolžen je obvestiti odgovorne ljudi, ki so zadolženi za odpravljanje težav na posameznih virih kot tudi druge ljudi in organizacije, ki imajo kakršno koli povezavo z virom in se jih povzročena nevšečnost dotika posredno. Naloga nadzornega organa je tudi vodenje reševalne akcije oz. procedure odprave nevarnosti ter informiranje nadrejenih o stanju škode (Forcht, 1998, str. 428 -429). Žal pa se v realnosti vse pogosto zanemarja zadnja faza in se odgovorni začno zavedati o kontroli in nadzorstvu takrat, ko je že prepozno. Pristop faze nadzorovanja ni le aktivno naravnan, ampak bi moral biti proaktivno usmerjen in preprečevati nastajanje škode.

5.4 INTERPRETACIJA RAZISKAVE IN REZULTATOV

Informacijska varnost ima pri sodobnem poslovanju, kjer je vse več poslovnih postopkov podprtih z informacijsko tehnologijo, čedalje večjo vlogo. Le z ustrezno opredelitvijo varnostnih tveganj in zaščito pred njihovimi učinki, se je namreč mogoče izogniti škodi, ki lahko nastane zaradi ne dovolj zavarovanih ključnih informacij v podjetju. Zato je izredno pomembno, da podjetje opredeli varnostna tveganja in se pred njihovimi nezaželenimi učinki ustrezno zaščiti in zavaruje z izbiro ustreznih kontrol. Pri tem more upoštevati tudi zakonodajo, standarde in druge notranje predpise (glej slika 18).

Slika 18: Temelji varnostnih zahtev



Vir: Standardi posredovanja sporočil med bankami in njihovimi komitenti, 2004.

Na podlagi teoretičnih izsledkov, ki sem jih razvila skozi vsebino magistrskega dela, sem v tem drugem delu, poskusila le-te s pomočjo raziskave prenesti v praktično uporabo. Z izvedbo analize tveganja e-plačilnega sistema, sem prišla do rezultata, ki opredeljuje varnostno tveganje e-plačilnega prometa med banko in podjetjem. Uporabila sem metodo zbiranja podatkov na podlagi anketnega vprašalnika, s katerim sem od ocenjevalcev pridobila ocene o varnosti e-plačilnega prometa. V raziskavi so sodelovale osebe z različnimi poklici (informatik, računalniški programer, finančna administratorka, bančna administratorka, manager, kriminalistični inšpektor, samostojni podjetnik in razvijalec programske opreme) in iz različnih panog (proizvodno podjetje, banka, IT firma, samostojni podjetnik, policija). Njihovo poznavanje tega področja je različno, zato sem morala pri nekaterih težo vprašalnika glede na njihovo delo in poznavanje omenjene tematike rahlo prilagoditi. Tako zbrane podatke sem v nadaljevanju s pomočjo korakov analize tveganja e-plačilnega prometa obdelala. Korake analize sem povzela po Turbanu. Glede na proučevano problematiko raziskave, sem analizo tveganja zaradi lažje interpretacije rezultatov prilagodila mojemu primeru.

Analiza temelji na ocenjevanju virov e-plačilnega prometa in ocenjevanju verjetnosti napada groženj na le-te. Tehnika vrednotenja podatkov temelji na kvalitativnem ocenjevanju. Ocene ocenjevalcev sem združila v povprečno skupno oceno, ki predstavlja končni rezultat moje raziskave o varnosti e-plačilnega sistema. Zbrane ocene sem tabelarično predstavila. Glede na

doseženo skupno oceno sem izmed vseh ocen izluščila prioritetne vire ter jih tabelarično prikazala. Nadalje sem za vsak segment posebej, predlagala možne dodatne ukrepe, ki bi poleg osnovnih mehanizmov varovanja, preprečile morebitne napade na najbolj občutljive prioritetne vire računalniškega sistema pri izvajanju nalog e-plačilnega prometa.

Rezultat analize potrjuje teoretična izhodišča o pomanjkljivi varnosti e-plačilnega sistema. Ocenjevalci so podali dokaj pesimistične ocene, saj niso noben vir ocenili kot popolnoma varen. To sem tudi v nalogi poudarila, da ne moremo zagotoviti popolne varnost, ampak le optimalne. Informacijska tehnologija je živa stvar, ki se nenehno spreminja in v njej igrajo pomembno vlogo tudi »nepridipravi«.

6 SKLEP

Ob koncu naloge lahko zaključim, da sem dosegla v uvodu zastavljene cilje in prišla do želenega rezultata, ki kaže, da varnost ne more biti nikoli zadostna, lahko pa je optimalna za določeno aktivnost. V magistrskem delu sem predstavila problem varnosti pri e-plačilnem sistemu v podjetjih. Z reformo plačilnega prometa so podjetja prenesle račune iz APP na poslovne banke ter v večini začela uporabljati internet za prenosni medij finančnih transakcij z banko. S tem se je začela močno širiti uporaba e-bančništva in pojavili so se prvi dvomi glede varnosti e-poslovanja.

E-poslovanje med podjetji ni novo, saj so že v 60-tih letih v elektronski obliki pošiljali in sprejemali naročila, fakture in ostalo dokumentacijo. Od tu tudi izhaja definicija e-poslovanja kot izmenjava poslovnih informacij preko omrežja s pomočjo računalniške izmenjave podatkov. V zadnjem desetletju smo priča velikim in pomembnim spremembam v poslovanju podjetij, ki so nastale kot posledica razvoja nove informacijsko komunikacijske tehnologije – razvoja interneta. Internet je v e-poslovanje vnesel veliko svežine in razvili so se številni različni načini uporabe. Najbolj so se uveljavile oblike digitalne komunikacije preko e-pošte, uporaba spletnih strani kot tudi uporaba najrazličnejših multimedijskih storitev.

E-poslovanje igra pomembno vlogo v različnih poslovnih funkcijah v podjetjih. Finančni oddelek se srečuje z ožjim delom e-poslovanja, ki temelji na prenosih finančnih podatkov v sodelovanju z bankami in drugimi zunanjimi subjekti. E-bančništvo obsega vso bančno poslovanje, ki temelji na informacijski tehnologiji in deluje neodvisno od fizičnih poslovalnic. Med pravnimi osebami se je dobro uveljavila oblika posredovanje finančnih podatkov preko interneta, ki zamenjuje dosedanji način fizičnega prenosa virmanov v APP ali pošiljanje preko e-pošte.

Banke so se z e-bančništvom srečale že v 70. letih, ko so bile povezane preko sistema SWIFT. Uspešnost bank je bila vse bolj odvisna od učinkovite uporabe informacijske tehnologije, ki zmanjšuje stroške tradicionalnega poslovanja, povečuje konkurenčnost in krepi tržni delež. Hitrejša dinamika razvoja bančnega trga je povečala razlike v razvitosti bank, saj postaja ključni dejavnik uspešnosti bank hitrost in prožnost pri odzivanju na konkurenco. Koristi pridobljene z e-bančništvom se kažejo na daljši rok. Pri tem se moremo zavedati, da ne moremo samo pobirati sadežev, ampak je potrebno za to tudi nekaj investirati, vzdrževati in spremljati nove trende na trgu.

Z vse večjim številom računalnikov in manjših omrežij, povezanih v internet, je zaupnost podatkov postala vse bolj občutljiva in dostopna množici potencialnih storilcev iz vsega sveta. Tako se srečujemo z nevarnostjo, da nam lahko nekdo ukrade denar z vnosom lažnih podatkov, s spremembo programa, zlorabi oz. uniči informacije ali pa namenoma uniči ugled podjetja z namernim prikazom ranljivosti njegovega računalniškega omrežja. Med

najpogostejšimi nevarnostmi štejemo kraje, vandalizem in sabotaže. Nevarnost tako prihaja s strani zunanjih napadalcev kot tudi s strani notranjih oseb, ki lahko iz malomarnosti oz. nevednosti povzročijo veliko škodo podjetju kot tudi posamezniku.

Med osnovne tehnike za zagotavljanje informacijske varnosti se prištevajo;

- storitve overjanja (po navadi s kombinacijo nečesa, kar legitimen uporabnik ima, in nečesa, kar ve, kar preprečuje dostop do informacij neavtoriziranim osebam),
- storitve razpoložljivosti (upravičenim uporabnikom se ne prepreči dostopa do sporočila),
- storitve zaupnosti (zagotavljanje tajnosti sporočil),
- storitve celovitosti (neokrnjenost podatkov, še posebno z zagotavljanjem nespremenljivosti sporočil na poti od oddajnika do prejemnika) in
- storitve preprečevanja tajenja avtorstva podatkov.

Vse te lastnosti lahko zagotovimo le z uporabo ustreznih tehnologij, metod in rešitev, ki jih z ustrezno kombinacijo povežemo v celoto tako, da je varnost komunikacije prek interneta največja. Med najbolj uporabljenimi metodami uvrščamo: šifriranje, požarni zid, digitalno podpisovanje, varnostni protokoli in ustrezna varnostna kultura organizacije. Z izbiro ustreznih tehnologij, metod in rešitev ter z ustrezno kombinacijo le-teh, lahko zagotovimo optimalno informacijsko varnost. Priporočljiva je uporaba infrastrukture za overjanje javnih ključev (PKI), ki neločljivo povezuje javni ključ z uporabnikom, ki ima pri sebi odgovarjajoči zasebni ključ. Temelj PKI je digitalno potrdilo, ki ga izdaja zaupanje vredna organizacija, ki pooseblja zaupanje in ji uporabniki znotraj PKI zaupajo. Infrastruktura PKI zadošča strogim merilom varnosti, ki so potrebna pri varnem e-plačevanju.

Varnostni mehanizmi se iz leta v leto izpopolnjujejo, dopolnjujejo in spreminjajo. Prav tako se je bančništvo v kratki zgodovini samostojne Slovenije kar nekajkrat spremenilo, kar je posledica ekonomskega sistema bivše Jugoslavije. V starem sistemu je APP pri opravljanju storitev plačilnega prometa imela monopolni položaj, ločeno sta se izvajala tolarski in devizni plačilni promet, ki je predstavljal problem centralni banki pri nadzoru likvidnosti. Leta 1999 se je začela reforma plačilnega sistema, kjer so poslovne banke dobile ključno vlogo pri izvajanju plačilnega prometa in s tem možnost, da z uporabo e-bančništva pridobijo čim več novih komitentov. Sistem plačilnega prometa je doživel strukturne spremembe in postal tržno naravnan, kar je povsem primerljiv s sistemi v drugih evropskih državah. Slovenija je leta 2000 sprejela Zakon o elektronskem poslovanju in elektronskem podpisu in Uredbo o pogojih za elektronsko poslovanje, ki urejata zakonsko področje in določata splošna pravila za delovanje skupnega trga na področju informacijske družbe z vsemi vrstami transakcij med uporabniki. Slovenija je zakonsko prilagojena evropskim smernicam. Najpomembnejša zakonska podlaga je Direktiva o elektronskem poslovanju, ki zagotavlja enoten režim in pravila o e-poslovanju za države članice, ne glede na državno mejo v EU. Z osnovnimi temelji zakonodaje, ki so povzeti po evropski zakonodaji, je Slovenija še dodatno prispevala k

skupnemu, enotnemu trgu, kjer se brišejo meje in kjer poslovanje poteka po enotnih pravilih.

Zakonska določila za e-poslovanja vključujejo tudi področje e-bančništva. Danes uvrščamo e-bančništvo med najpomembnejšo dejavnost, s katero banka navezuje stik s svojimi komitenti. Ta nov način poslovanja pomeni za uporabnike nižjo ceno plačilnega prometa, bančnim referentom pa nudi več časa za stranke, katerim lažje posvetijo več časa za svetovanje. Banka je z možnostjo uporabe e-bančništva odprla vrata vsem komitentom, ki lahko z uporabo interneta do banke pristopajo kadarkoli in kjerkoli.

Sodobni življenjski ritem in tehnološki razmah izredno vplivata na razvoj bančnega poslovanja. Nenehna dostopnost raznolikih, prilagodljivih in cenovno konkurenčnih bančnih storitev z uporabo številnih tržnih poti, postaja temelj današnjega bančništva. Število uporabnikov raste iz dneva v dan. Podjetja lahko glede na njihove potrebe in zahteve izberejo med modemskim ali direktnim internetnim dostopom do bančnih storitev. Poglavitni ponudniki spletnih bančnih platform v Sloveniji so: Halcom Informatika, Zrcalo, Hermes Softlab in Adacta.

Podjetje se z banko povezuje preko interneta z uporabo programske aplikacije, ki ju funkcionalno povezuje uporabniški vmesnik. Z vključitvijo lokalnega omrežja v internet, postane informacijski sistem dostopen množici potencialnih vlomilcev iz vsega sveta. Z pomočjo managementa informacijskega sistema, podjetja izboljšujejo ozaveščenost in povečujejo zavest o pomembnosti podatkovne varnosti pri zaposlenih ter s tem zmanjšujejo nastajanje ključnih tveganj.

V nalogi sem s koraki analize tveganja varnosti e-plačilnega prometa, identificira ključne vire pri delovanju e-plačilnega prometa in ključne nevarnosti, ki ogrožajo nemoten prenos finančnih transakcij. S pomočjo zunanjih sodelavcev iz različnih področji dela, sem ovrednotila vire glede na zahtevano stopnjo varnosti in ogroženosti glede na predhodno določene potencialne nevarnosti in grožnje. Vsak vir je bil ocenjen glede na kriterije zaupnosti, neoporečnosti in razpoložljivosti. Skupna vsota vseh ocen za posamezni vir je dala skupno oceno ogroženosti vira. Končni rezultat, ki pomeni skupno oceno vseh sodelujočih pri raziskavi, je postregel z ugotovitvami, da je najobčutljivejši del v podjetju delovna miza, kjer finančna administratorka operira s podatki in sproži prenos pošiljanja podatkov po omrežju do banke.

V zaključku sem podala nekaj možnih ukrepov, ki preprečujejo nastanek neljubih dogodkov in povečujejo zavest uporabnikov o pomenu varnosti e-poslovanja. Varnost je le tolikšna, kot je varen najšibkejši člen znotraj opazovanega sistema. Zato je nujno, da se prijemi za preprečevanje nastajanje nevarnosti uporabljajo skupaj in ne ločeno za vsako obliko grožnje. Nič ne pomaga najsodobnejša tehnološka zaščita, če v organizaciji ni prisotne ustrezne varnostne politike, ki se ustrezno in dosledno izvaja. S povečanjem zavesti o varnosti med zaposlenimi, lahko preprečimo napade s t.i. socialnim inženiringom, kjer napadalec pride do

potrebnega gesla le s klicem na tehnično pomoč podjetja ali s krajšim sprehodom po pisarnah v času malice oz. s prijaznim nastopom do uporabnika, do uporabnih podatkov za izvedbo svojega nelegalnega dejanja. To pomeni, da postavitev varnostne pregrade še ne zadošča za miren spanec, ampak zahteva nenehno izpopolnjevanje in nadzor nad sistemom e-poslovanja ter gojiti zavest o varnostni politiki na vseh ravneh organizacije.

7 LITERATURA

1. Bračun Franc: SEB security story – SKB Banka. The bank of tomorrow. [URL:http://www.hermes-softlab.com], 17.10.2993.
2. Cheswick William, Steven M. Bellovin: Firewalls and Internet Security. New York : Adison-Wesley publishing company, 1994. 51 str.
3. Collin, Barry: What happens if your partner turns against you?. Computer Security Institute, 1998. [URL: http://www.gocsi.com/extranet.htm], 15.04.2000.
4. Forcht A. Karen: Computer security management. Cambridge : International Thomson publishing company, 1998. 486 str.
5. Gradišar Miro, Resinovič Gortan: Informatika v organizaciji. Kranja : Moderna organizacija, 1998. 472 str.
6. Gril Matej: Varnost in tehnološka zaščita informacijskega sistema v banki. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2003. 90 str.
7. Grenko Barbara: Razvojni trendi v evropskem bančništvu (1). Bančni vestnik, Ljubljana, 2000a, 6, str. 36-41.
8. Grenko Barbara: Razvojni trendi v evropskem bančništvu (2). Bančni vestnik, Ljubljana, 2000b, 7-8, str. 65-69.
9. Internet Security Systems. Creating, Implementing and Managing the Information Security Lifecycle. 2002, TruSecure Corporation Security Solutions. [URL: http://www.iss.net/customer_care/resource_center/whitepapers/], 2002.
10. Jerman Blažič Borka, et al.: Elektronsko poslovanje na internetu. Ljubljana : Gospodarski vestnik, 2001. 206 str.
11. Kalakota Ravi, Whinston Andrew: Electronic Commerce. A Manager's guide. B.k. : Addison-Wesley Longman, 1997. XVI, 431 str.
12. Kranjc Simon: Varnostni vidiki sodobnih informacijskih sistemov. Diplomska naloga. Maribor : Ekonomska poslovna fakulteta, 2001. 75 str.
13. Kuščar Samo: O varnosti in odgovornosti. Monitor, Ljubljana, Infomedij, št. 11, nov. 2002, str.8.
14. Lamberger Igor: Gospodarski kriminal. Gradivo za kriminalistični tečaj. Ljubljana : MNZ, GPU, Uprava kriminalistične policije, April, 2004, str. 108.
15. Lenstra Arjana, Verhaul Erica: Selecting Criptographi Key Sizes. 27.10.1999. [URL http://security.ece.orst.edu/koc/ece575/papers/cryptosizes.pdf], 20.12.2004.
16. Marinšek Primož, Cepec Miro: Prenova plačilnega sistema. Zaslon. [URL:http://www.zaslon.si/bancniasistent/izobrazevanje/placilni_promet/prenova_placilnega_sistema.html], 10.09.2002.
17. Milenkovič Vladoša: Ureditev v EU. Glas gospodarstva, Ljubljana, 2001, april, str. 96-98.
18. Miš Svoljšak Irena: Osnove trženja finančnih storitev. Maribor : Združenje bank Slovenije, 1997. 23. str.
19. NA - Network Associates. An Introduction to Cryptography. Santa Clara : Network Associates Inc. 1999.

20. Oman Saša: On-line bančništvo v svetu in Sloveniji. Bančni vestnik, Ljubljana, 51, 2002, 6, str.17-21.
21. Pavliha Marko: Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. Ljubljana : GV Založba, 2002. 222 str.
22. Pečenko Nikolaj: Virus. PC&Mediji. Ljubljana : Infomediji, 02/VIII, februar 2002, str. 60-69.
23. Pernovšek Tomaž: Varna izmenjava e-sporočil na osnovi podpisa XLM v podjetniškem poslovanju. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2004, 102 str.
24. Perše Zoran: Varstvo in zaščita osebnih podatkov pri elektronskem poslovanju. Gospodarski vestnik, Pravna praksa, Ljubljana, 11, 2000, str.11.
25. Pinterič Mojca: Pametne kartice izpodrivajo gotovino. Gospodarski vestnik, Ljubljana, 1995, str.5-29.
26. Power Richard: How NOT to build a firewall. Computer Security Institute, 1998. [URL: http://www.spirit.com/CSI/Papers/hownot.htm], 24 april, 2000.
27. Prodnik Pepevnik Vesna: Marketinški vidik uvajanja elektronskega poslovanja v slovenska podjetja. Ministrstvo za informacijsko družbo. [URL: www.merkur.si], 10.02.2004.
28. Puciher Andreja: Priložnosti in težave elektronskega poslovanja med organizacijami v Sloveniji. Uporabna informatika, Ljubljana, 7, 1999, 4, str. 7-13.
29. Robinson Peter: Understanding Digital Certificates and Secure Sockets Layer (SSL). Entrust, Inc., 2001. [URL: http://www.entrust.com/resourcenter/whitepapers.htm], 01.02.2003.
30. Schneier Bruce: Secrets & Lies. Digital Security in a Networked World. NY : Wiley Computer Published, 2000, 412 str.
31. Šega Polona: Trendi v svetovnem bančništvu in vplivi na slovenski bančni prostor. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2001. 89 str.
32. Sjekloča Marko: Elektronsko bančništvo. Bančni vestnik, Ljubljana, 1999, 1-2, str. 31-33.
33. Škedelj Franc: Informacijska podpora prenovi plačilnega prometa. Zalon. [URL: http://www.zaslon.si], maj 2002.
34. Škrlec Ivan: E-poslovanje in uporaba formata XML. Finance, Ljubljana, 2002, 6.maj, str. 18.
35. Sokol S. Marc, Curry A. David: Security Architecture and Incident Management for E-business. Internet Security Service, 17.05.2000. [URL: http://iss.com], 17.10.2003.
36. Toplišek Janez: Elektronsko poslovanje. Ljubljana : Založba Atlantis, 1998. 336 str.
37. Turban Efraim, et al.: Electronic Commerce. A Managerial Perspective. New York : Prentice-Hall, 2003. 512 str.
38. Valher Anita: Zaključek reforme plačilnega prometa. Kapital, Maribor, 11, 2002, 287, str. 26-28.
39. Young-Seock, Cha: E-Commerce Security Technologies. Network Security Library, 2000. [URL: http://secinf.net/info/fw/ecom/], 05.01.2003.
40. Wright Michael, Patel Mukul: Kako stvari delujejo. Ljubljana : Mladinska knjiga, Svet knjige, 2002. str. 287.

8 VIRI

1. Banka Slovenije: Seznam poslovnih bank. [URL: http://www.bsi.si/html/povezave/seznam_bank.html], 26.08.2004.
2. Bratož David: Elektronsko bančništvo za pravne osebe. Seminarska naloga pri predmetu Sodobne telekomunikacijske storitve in tehnike. Novo mesto, 2002, 28 str.
3. E-bančništvo. Povzetek. RIS 2002. [URL:http://www.ris.org/publikacije/najnovejsa/e_bancnistvo2k2.html], 28.04.2003.
4. Introduction to network security. SupportNet Online. [URL: http://supportnet.merit.edu/m-intsec], 12.06.2002.
5. Kazenski zakonik. Uradni list RS, št. 70-1/1994, 11.11.1994.
6. Kazenski zakonik, Popravki kazenskega zakonika, KZ-A popravki. Uradni list RS, št. 23-1035/999, 08.04.1999.
7. Osnovni pojmi in nekaj primerov. Simetrični algoritmi. [URL: http://www.sigov.si/tecaj/seminar.html], 30.08.2002.
8. Osnove tehnologije elektronskega poslovanja in elektronskega podpisa. [URL: http://www.gov.si/cvi/slo/index_slo.htm], 20.06.2002.
9. Plačilni sistemi: Nekaj informacij o reformi plačilnih sistemov v Sloveniji. [URL: http://www.bsi.si/html/ps/nekaj_info.html], 21.06.2002.
10. Pošiljanje plačilnih nalogov po elektronski pošti. Združenja bank Slovenije. [URL: http://www.zbs.giz.si], 10.09.2002.
11. Sistem elektronskega bančništva (SEB). Zaslon. [URL: http://www.zaslon.si/elba/seb.html]. 20.06.2002.
12. Spletna stran Abanka Vipa. [URL: http://www.abanka.si], 2002.
13. Spletna stran Adacta. [URL: http://www.adacta.si], 2002.
14. Spletna stran Adacta. [URL:http://www.adacta.si/index.asp?lang=SI&content=resitve& submenu =InetBank], 19.10.2003.
15. Spletna stran BACA. [URL: http://www.baca.si], 2002.
16. Spletna stran Banka Koper. [URL: http://www.banka-koper.si], 2002.
17. Spletna stran Banke Slovenije. [URL: http://www.bs.si], 2004.
18. Spletna stran EuroPKI. [URL: http//www.europki.com], 29.01.2003.
19. Spletna stran Halcom. [URL: http://www.halcom.si], 2002.
20. Spletna stran Nova Kreditna Banka Maribor. [URL: httm://www.nkbm.si], 2002.
21. Spletna stran Nova Ljubljanska Banka. [URL: http://www.nlb.si], 2002.
22. Spletna stran NUA. [URL: http://www.nua.com], 01.01.2003.
23. Spletna stran Raba interneta v Sloveniji. [URL: http://www.ris.org], 20.07.2002.
24. Spletna stran Raiffeisen Krekova banka. [URL: http://www.r-kb.si/eureka.htm], 02.02.2005
25. Spletna stran Security Firs Network Bank. [URL: http://www.sfnb.com], 01.01.2003.
26. Spletna stran SKB Banka. [URL: http://www.skb.si], 2002.
27. Spletna stran Zaslon. [URL: http://www.zaslon.si], 2002.

28. Spletna stran Zrcalo. [URL: http://www.zrcalo.si], 2002
29. SSL. [URL: http://www.sigov.si/tecaj/kripto/kr-ssl.htm], 26.06.2002.
30. Standardi posredovanja sporočil med bankami in njihovimi komitenti. [URL: pdf:stand_spl /mapa novo], 22.08.2004.
31. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Uradni list RS, št. 77/2000, št. 2/2001.
32. Vicomsoft: Firewall White Paper.
    [URL: http://www.firewall_software.com/firewall_white_paper.html], 01.01.2003.
33. Zakon o elektronskem poslovanju in elektronskem podpisu. Uradni list RS, št.57/2000.
34. Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu. Uradni list RS, št. 25/2004.
35. Zapiski predavanj – Komunikacijska tehnologija, 2001.