**UNIVERZA V LJUBLJANI**
**FAKULTETA ZA DRUŽBENE VEDE**

**Mojca Berce**

# Varnostni vidiki e-bančništva v Sloveniji

Magistrsko delo

**Ljubljana, 2014**

**UNIVERZA V LJUBLJANI**
**FAKULTETA ZA DRUŽBENE VEDE**

Mojca Berce

**Mentor:** doc. dr. Uroš Svete

# Varnostni vidiki e-bančništva v Sloveniji

Magistrsko delo

**Ljubljana, 2014**

Iz srca se zahvaljujem za pomoč in solidarnost pri izvedbi in oblikovanju zaključnega dela svojega študija mentorju doc. dr. Urošu Svetetu . Brez njegove pomoči mi ne bi uspelo, zato hvala.

Zahvala gre moji družini in prijateljem, ki so me ves čas pisanja bodrili in se menoj veselili vsakega uspeha.

Predvsem gre pa zahvala očetu, ki žal ne bo videl mojega zadnjega dela v akademski sferi.

Univerza v Ljubljani
Fakulteta za družbene vede

*Kardeljeva ploščad 5*
*1000 Ljubljana,*
*Slovenija*
*telefon 01 58 05 122*
*01 58 05 120*

# I Z J A V A  O  A V T O R S T V U
magistrskega dela

Podpisani/-a Mojca Berce, z vpisno številko 21091099, sem avtor/-ica magistrskega dela z naslovom: Varnostni vidiki e-bančništva v Sloveniji.

S svojim podpisom zagotavljam, da:

- je predloženo magistrsko delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal/-a v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah (UL RS, št. 16/07-UPB3, 68/08, 85/10 Skl.US: U-I-191/09-7, Up-916/09-16)), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko magistrskega dela ter soglašam z objavo magistrskega dela v zbirki »Dela FDV«.

V Ljubljani, dne 16.9.2014 Podpis avtorja/-ice: Mojca Berce

**Varnostni vidiki e-bančništva v Sloveniji**

E-bančništvo v Sloveniji se je v zadnjih letih zelo razvilo in pridobilo veliko število uporabnikov. Vendar kljub dobri zaščiti, ki jo banke nudijo svojim uporabnikom e-bančništva, prihaja do različnih zlorab podatkov. V delu predstavljam varnostne vidike in morebitne napade oziroma grožnje s področja informacijske varnosti. S poznavanjem informacijskih groženj in mehanizmov za zaščito pred njimi opredelim pojme, ki so se razvili kot posledica te storitve. Z razvojem informacijsko-komunikacijske tehnologije se je povečal tudi obseg elektronskega poslovanja, skupaj z eno od podkategorij oziroma komponent, tj. e-bančništvom. V prvem delu opisujem teorije, ki so značilne za informacijsko varnost. Poleg teorij so izpostavljeni tudi mehanizmi, ki varujejo pred zlorabami informacijsko-komunikacijske tehnologije. V nadaljevanju je izveden še intervju, prikazani pa so tudi primeri zlorab elektronskega bančništva v Sloveniji. Če povzamem: e-bančništvo bo ostalo razširjeno, komunikacijski in varnostni protokoli pa vedno bolj dodelani. Varnostni sistemi v e-bančništvu bodo napredovali v tej smeri, da bo manj kraj identitet ali gesel. Mogoče je tudi, da bo e-bančništvo sistemsko urejeno in okrepljeno z močnejšim šifriranjem – tako vsaj hekerji ne bodo mogli razbiti kode.

**Ključne besede**: E-bančništvo, zlorabe, varnostni vidiki, informacijska varnost.

**Safety aspects of e-banking in Slovenia**

E-banking in Slovenia has significantly evolved over the years and obtained a large number of users. However, despite the good protection offered by banks offering their customers using e-banking, there are a variety of data abuse. In my thesis, I present the safety aspects and potential attacks or threats to information security. With the knowledge of IT threats and mechanisms to protect against them, identify concepts that have evolved as a result of this service. With the development of information and communication technology has also developed its e-commerce component subcategory of e-banking. The first section describes theories that are specific to information security. In addition, theories are also exposed to mechanisms that protect against abuse of information – communication technology. Following is an interview conducted, with presented examples of misuse of electronic banking in Slovenia. To summarize: e-banking will remain widespread, communication and security protocols are becoming increasingly sophisticated. Security systems in e-banking will be promoted to the extent that there will be less of identity theft or passwords. The possibility also remains that the systematic regulation of e-banking will be reinforced by stronger encryption, at least the “hackers” will not be able to break the code.

**Keywords:** E-banking, abuse, safety aspects, information security.

Kazalo

Kazalo slik:



Kazalo tabel:



Kazalo grafov:

# 1 Uvod

## 1.1 Opredelitev raziskovalnega problema

Komunikacijski sistem je namenjen izključno prenosu podatkov (sporočil) med dvema informacijskima okoljema/subjektoma, pa naj gre za Morsejeve znake prvih telegrafov, zvoke prvih telefonov ali podatkov, kot jih razume klasična z računalništvom podprta informatika, ali pa integracijo poljubne kombinacije naštetih oblik podatkov (Vidmar 2002, 35). Za učinkovito delovanje informacijske varnosti potrebujemo mehanizme, ki nam to varnost zagotavljajo. Informacijska varnost pri e-bančništvu je pomembna zaradi zagotavljanja varnosti prenosa podatkov. Mehanizmi za zagotavljanje informacijske varnosti so zelo raznovrstni. Glavne komponente, ki so najbolj pomembne za zagotovitev informacijske varnosti, so:

- normativni oziroma pravni vidiki: Zakonski in kazenski pregoni kaznivih dejanj (zapisano v kazenskem zakoniku pod členom 221), in sicer pravi člen o napadu na informacijski sistem:

  *221.člen*

  *(1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.*

  *(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.*

  *(3) Poskus dejanja iz prejšnjega odstavka je kazniv.*

  *(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.«*) (KZ-1, 2011);

- kriptografija;
- elektronski podpis/certifikati;
- požarni zid;

- gesla;
- različni tehnični protokoli (SSL, WTSL, SET);
- usposabljanje posameznikov oziroma človeška komponenta, ki prispevka k informacijski varnosti.

Čeprav smo upoštevali vse komponente oziroma mehanizme za zagotavljanje informacijske varnosti, jo lahko še vedno ogrozijo izurjeni napadalci ali pa tehnične napake na opremi, programski kodi itd. Pri tem moramo tudi vedeti, katera so največje grožnje informacijski varnosti, in se zavedati možnosti, da je pri uporabi e-bančništva ogrožena naša varnost. Poznamo več oblik napadov oziroma groženj:

- napadi DDOS
- napadi CSRF
- phishing oziroma ribarjenje
- socialni inženiring
- kriminalna programska oprema (ang. crimeware)
- posnemek (ang. skimming)

S poznavanjem informacijskih groženj in mehanizmov za zaščito pred njimi lahko opredelimo pojme, ki so se razvili kot posledica te storitve. Z razvojem informacijsko-komunikacijske tehnologije se je razvilo tudi elektronsko poslovanje in njegova podkategorija oziroma komponenta e-bančništvo.

Elektronsko poslovanje je poslovanje, ki presega meje ene organizacije in temelji na izmenjavi podatkov med računalniki. Je splošen izraz za elektronski način opravljanja (poslovne) dejavnosti s pomočjo elektronskega sporočanja (Lobe 2003, 3).

> *Elektronsko poslovanje pomeni, da so podjetja s pomočjo računalnikov in informatizacije procesov posodobila del ali celotno poslovanje, kot na primer komunikacijo z dobavitelji in odjemalci, skladiščenje, distribucijo, trženje, prodajo in podobno. Vendar je elektronska trgovina le del elektronskega poslovanja podjetja. Poznamo elektronsko poslovanje med podjetji in posamezniki (elektronska trgovina, elektronsko bančništvo), elektronsko poslovanje med podjetji (trgovanje) in elektronsko poslovanje med posameznikom in državnimi ustanovami (sodelovanje na razpisih, napoved dohodnine ipd.) (Lobe 2003, 3).*

Namen bank pri uvajanju e-bančništva lepo ponazori naslednji citat:
»S pojmom elektronska banka lahko opredelimo način opravljanja bančnih storitev, ki jih lahko kot bančni komitent opravite neposredno s svojega delovnega mesta ali od doma, brez neposredne pomoči bančnega uslužbenca, in to kadarkoli, 24 ur na dan, 365 dni v letu«(Kadivec v Malenšek 2002,9).

Tako so banke začele razvijati e-bančništvo, s katerim je mogoče opravljati transakcije med podjetji prek interneta oziroma lahko fizične in pravne osebe opravljajo bančno poslovanje, ne da bi morale biti fizično prisotne v banki.

V magistrski nalogi želim podati vpogled v informacijsko družbo in informacijsko varnost oziroma vpogled v varnostne vidike e-bančništva v Sloveniji s poudarkom na mehanizmih za zaščito oziroma ogrožanje.

## 1.2 Prikaz dosedanjih raziskovanj opredeljenega raziskovalnega problema

Pri nas se z raziskavami glede uporabe interneta in uporabe e-bančništva ukvarja RIS (Raba interneta v Sloveniji) in tudi druge raziskovalne inštitucije, na primer Valicon in iPROM.

Po pregledu raziskav, ki so dosegljive na internetu, izpostavljam tri raziskave. In sicer:

1. Po RIS-ovi telefonski raziskavi, opravljeni ob koncu leta 2004 in v začetku leta 2005, »je uporaba e-bančništva v Sloveniji še vedno relativno skromna; uporablja ga le okoli petina aktivnih uporabnikov interneta. Zaradi rasti števila uporabnikov interneta absolutno število uporabnikov e-bančništva sicer narašča, v grobem za 20.000–25.000 uporabnikov letno, in je v letu 2004 doseglo 160.000 uporabnikov.« (RIS 2005)

2. Potem sta sledili še raziskavi Valicona in iPROMA v letu 2007, v katerih je sodelovalo 8.046 anketirancev. Raziskava se je poleg področij e-nakupovanja in spletnih dnevnikov osredotočila tudi na uporabo elektronskega bančništva. Spletno banko vsaj nekajkrat letno uporablja približno 17 odstotkov internetnih uporabnikov. »Najpogostejši uporabniki e-bančništva so stari med 30 in 50 let, višje ali visoko izobraženi, zaposleni, imajo otroke in višje dohodke. Izkazalo se je, da sta uporabi interneta in e-bančništva tesno povezani, saj 84 odstotkov vsakodnevnih in 80

odstotkov tedenskih uporabnikov e-banke večkrat dnevno uporablja internet.« (Iprom 2007)

3. Leta 2009 je RIS izvedel še eno raziskavo, ki je vključevala samo e-bančništvo, ta pa kaže, da je v zadnjem desetletju e-bančništvo postalo zelo dobičkonosna spletna storitev. Že v letu 2004 so napovedali, da se bo število uporabnikov povečalo za dvakrat.

> *V štirih letih se je torej število uporabnikov podvojilo z 10 na 21 % v populaciji 10–75 let, kar pomeni 15-odstotno povprečno letno rast. Po zadnjih ocenah RIS-a (2008) je v Sloveniji več kot milijon rednih uporabnikov interneta (v populaciji 10–75 let), od tega jih 312.000 uporablja storitve e-bančništva. O uporabi razmišlja še 230.000 uporabnikov (leta 2004 264.000), od tega jih 87.000 namerava začeti z uporabo v 6 mesecih (leta 2004 113.000). V primerjavi z letom 2004 se je povečalo predvsem število uporabnikov interneta, ki ne uporabljajo e-bančništva in o tem tudi ne razmišljajo (RIS 2004: 336.000, RIS 2008: 535.000).* (RIS 2009)

Podatki so vzeti iz poročila o e-bančništvu iz leta 2009, ki ga je pripravil RIS. (RIS 2009)

## 1.3 Metode raziskovanja

Metode raziskovanja bodo temeljile na raziskovanju sekundarnih virov (raziskave, splet, arhivi). Usmerila se bom tudi na podjetje Halcom, ki skrbi za razvoj in ponudbo storitev e-bančništva ter poskusila pridobiti ključne podatke za nadaljnje raziskovanje (kako je zastavljena varnost v posameznih bankah itd.). V podjetju Halcom nameravam izvesti krajši intervju na temo informacijske varnosti in razvoja aplikacije, ki jo urejajo za uporabo e-bančništva. Podjetje Halcom se ukvarja s programskimi rešitvami za podjetja, ki omogočajo varen prenos denarja in poslovanje. Poleg pridobitve podatkov iz bank (pregled njihovih spletnih strani) in Halcoma (intervju) bom naredila tudi analizo medijskega poročanja. Pregledala bom arhivski material časopisa Delo in svetovni splet, zanimajo pa me članki na temo zlorab in vdorov v informacijsko-komunikacijske sisteme e-bančništva. V raziskavo bom vključila tudi SI-CERT ((Slovenian Computer Emergency Response Team) – center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji), kjer jih bom prosila za statistične podatke o

prijavah zlorab e-bančništva (če sodelovanja z njihove strani ne bo, bom preučila njihova letna poročila, kjer so primeri zapisani).

Glavna raziskovalna hipoteza je:

**E-bančništvo ima vse večje število uporabnikov in s tem večjo izpostavljenost za zlonamerno kodo.**

1. Informacijska varnost e-bančništva v Sloveniji temelji na tehničnih protokolih varnosti.

Poleg teoretične plati informacijske varnosti bom naredila še primerjavo e-bančnih storitev različnih bank (Nova Ljubljanska banka, SKB, Abanka VIPA, Bank Austria – sedaj Unicredit). Tu se bom osredotočila na predstavitev elektronskega bančništva v zgoraj omenjenih bankah in opravila primerjavo e-bančnih drugih bank. Upoštevala bom naslednje kriterije:

- način, na katerega se varuje dostop do osebnega računa (digitalni certifikat, miniračunalnik s kodo, varnostni certifikat, uporaba čitalnika kartic, dvonivojsko geslo (ki onemogoča plačila na račune, ki niso »priljubljeni«))
- katere storitve nudi e-bančništvo (plačevanje položnic, prenos sredstev med računi, pregled prometa, uvoz in izvoz podatkov)
- varovanje (kriptiranje) komunikacijskih kanalov pri uporabi e-bančništva

Namen dela je torej teoretično opisati postopke varovanja storitev e-bančništva in narediti primerjavo ukrepov informacijske varnosti med bankami, torej ugotoviti, v čem se postopki med seboj razlikujejo. Ker pa zaradi strogega varovanja podatkov ne bom mogla dobiti celotnega vpogleda v delovanje varnostnih procesov, bo empirika temeljila na sekundarnih virih – analizi medijev (pregled arhivskih člankov, ki obstajajo na temo zlorab e-bančništva v arhivu Dela in drugih medijih), ter informacijah, ki so dosegljive pri ponudnikih storitev e-bančništva.

## 1.4 Pričakovani rezultati in prispevek magisterija k razvoju znanosti

V Sloveniji je e-bančništvo razširjena storitev za posameznike in podjetja. Pri tem so morali vsi ponudniki zagotoviti uporabnikom primerno informacijsko varnost pri prenosu podatkov in tudi pri obdelavi podatkov. Združenje bank je izdalo priporočilo za uporabo elektronskih tržnih poti v bankah, da bi zagotovili večjo preglednost in razumljivost poslovanja bank pri uporabi sodobnih tržnih poti. (povzeto po Združenje bank, 2014 ) Sicer pa sprejetje in uveljavitev teh priporočil nista zakonsko obvezna. V Republiki Sloveniji sicer to področje ni zadovoljivo zakonsko urejeno, zato je njihova uveljavitev še dodatno priporočljiva. Banka torej lahko sprejme tudi lastne splošne pogoje, ki spreminjajo določila teh priporočil.

Agencija za pošto in elektronske komunikacije, krajše APEK (sedaj preimenovana v AKOS[1]) opravlja svojo vlogo pri vpeljavi e-bančništva pri bankah tako, da je podala navodila oziroma priporočila, kako morajo potekati elektronske komunikacije.

Ker se informacijska tehnologija skozi leta zelo spreminja, je potrebno vedno nadgrajevati sisteme in vzpostavljati ravnovesje med uporabniki in ponudniki.

Pričakovani rezultati:

- e-bančništvo je zelo razširjeno in ugotoviti je potrebno, ali je za varnost storitev ustrezno poskrbljeno s strani zakonodaje in uporabe tehničnih sredstev varovanja storitev;
- zakonska podlaga varovanja podatkov s področja e-bančništva;
- sistemska urejenost e-bančništva oziroma šifriranje podatkov temelji na 256-bitnem kodiranju ali višjem.

Če povzamem: e-bančništvo bo ostalo razširjeno, komunikacijski in varnostni protokoli pa vedno bolj dodelani. Varnostni sistemi v e-bančništvu bodo napredovali v tej smeri, da bo manj kraj identitet ali gesel. Mogoče je tudi, da se bo sistemska urejenost e-bančništva okrepila z močnejšim šifriranjem, tako vsaj hekerji ne bodo mogli razbiti kode.

[1] Agencija za komunikacijska omrežja in storitve Republike Slovenije.

# 2 Teorija informacijske družbe

V različnih knjigah, ki jih beremo na temo informacijske družbe, avtorji pomanjkljivo definirajo informacijsko družbo.

Webster v svoji knjigi Information society theory pri definiciji informacijske družbe najprej izpostavi njene komponente oziroma dimenzije, na katere jo deli, in sicer: tehnologijo, ekonomijo, poklice, prostor in kulturo. V nadaljevanju jih na kratko opredelimo in predstavimo.

Tehnološka dimenzija se je razvila v poznih sedemdesetih letih. Tehnologije so eden od najbolj vidnih indikatorjev novih časov in so zato pogosto sprejete kot priprava na prihod informacijske družbe. V začetek tehnološke informacijske družbe so vključevali kabelsko in satelitsko televizijo, komunikacije na relaciji računalnik–računalnik, osebne računalnike (PC), nove pisarniške tehnologije, predvsem spletne informacijske storitve in urejevalnike besedil, in sorodne objekte (Webster 2006, 10). Z razvojem tehnološke dimenzije se je tudi pohitrila možnost komunikacije in družbeni odnosi so se prilagodili novim razmeram (Blitz v Dimc 2012, 2)

Ekonomska oziroma industrijska informacijska dimenzija ima gospodarsko vrednost informacijskih dejavnosti. Če je človek sposoben, da zapiše povečanje deleža bruto nacionalnega proizvoda (BNP) glede na poslovno informacijo, potem pridemo do točke, ki jo lahko razglasimo kot dosežek informacijske ekonomije. (Jonscher v Webster 2006, 12). Pri uvedbi te komponente se razvoj informacijsko-komunikacijske tehnologije zelo pozna, saj se je v zadnjih desetletjih delovanje celotne družbe toliko spremenilo, da si v bistvu sodobnega življenja in delovanja ne moremo več predstavljati brez spremljajočih prednosti, ki jih prinašajo IKT. (Dimc 2012, 2) Kot pravi Blitz (2004 v Dimc 2012, 3), internet predstavlja »virtualno okno v svet«, kjer lahko v trenutku dostopamo do informacij in celo virtualnih doživetij.

Ob poklicni oziroma razvojni dimenziji je Bell prvo razmišljanje o posledicah informacijske družbe objavil v svoji knjigi » The Coming of Post-Industrial Society[2]«, in sicer naj bi se po poteku tehnološke in ekonomske dimenzije premikali v novo družbeno obdobje, katerega ključna poslovna orientacija temelji na storitvah (Bell v Dimc 2012, 3); po njegovem naj bi

[2] Knjiga je izšla leta 1973 pri založbi v New Yorku.

bila največja pridobitev na področju informacijskih analiz in procesiranju podatkov. Tudi Bell izpostavi v knjigi The Coming of Post-Industrial Society, da so bili računalniki takrat v domeni večjih podjetij ali vladnih agencij. (Dimc 2012, 3)

Prostorska dimenzija informacijske družbe se je skozi čas pokazala v tem, da ključno vlogo igra prenos informacij, in kot je Bell predvidel v svoji knjigi The Coming of Post-Industrial Society je to bistvenega pomena za današnjo družbo in razvoj interneta. Zmanjševanje stopnje tradicionalne industrije in povečanje dejavnosti kot so bančništvo in prodaja na drobno je bilo za Bella kot simptom, ki je usmerjen k znanstveno naravnani družbi, kjer znanje oziroma vedenje predstavlja moč. (Bell v Dimc 2012, 3)

Goddard[3] pa je v prostorskem vidiku našel štiri elemente, ki se povezujejo med seboj in so značilni za prehod v informacijsko družbo, in sicer:

> *Informacije so ključni strateški vir, od katerega je odvisna organizacija svetovne ekonomije*; *računalniška in komunikacijska tehnologija zagotavljata informacijsko infrastrukturo in omogočata upravljanje z informacijami v doslej neznanem razponu; informacije so ključni strateški vir; sektor za trženje informacij naglo narašča,; razvoj informatizacije ekonomije je omogočil in pospešil integracijo nacionalnih in regionalnih ekonomij v globalno ekonomijo*.(Šercar 2000)

Tako pridemo do zadnje dimenzije, kulturne. Kulturno dimenzijo je izpopolnil na podlagi Bellove ideje sociolog Manuel Castells, ki je pravzaprav oblikoval idejo t. i. informacionalizma[4], ki naj bi predstavljala kulturno dimenzijo in naj bi temeljila na zbiranju, obdelavi in interpretacij informacij (povzeto po Dimc 2012, 3). Dimc in Dobovšek v svoji knjigi Kriminaliteta v informacijski družbi (2012, 3) poleg Castellsa omenjata tudi Warscahuerja (1998), ki prav tako razpravlja o spremenljivosti narave časa in prostora v današnjem času, pri čemer izpostavi koncept »kulture realne virtualnosti«. Prvi poizkus

[3] Več o razlikovanjih*: 1) informacije so ključni strateški vir, od katerega je odvisna organizacija svetovne ekonomije; ker je ravnanje z informacijami izjemno pomembno, se informacijski poklici naglo širijo; 2) računalniška in komunikacijska tehnologija zagotavljata informacijsko infrastrukturo in omogočata upravljanje z informacijami v doslej neznanem razponu (online trgovina v realnem času, spremljanje ekonomskega življenja, družbenih in političnih zadev na globalni ravni); 3)sektor za trženje informacij naglo narašča; posledica tega razvoja je radikalna reorganizacija svetovnega finančnega sistema, ki ga razume zelo malo strokovnjakov; tistih, ki ga kontrolirajo, pa je še manj; 4)razvoj informatizacije ekonomije je omogočil in pospešil integracijo nacionalnih in regionalnih ekonomij v globalno ekonomijo; s tem je prišlo tudi do redukcije fizičnega prostora oz. do nastanka prostora brez daljav in brezčasnega časa; temu Giddens pravi 'zgostitev prostora in časa'* ( Šercar 2000, Kritika kritike teorij informacijske družbe)

[4] Informacionalizem naj bi predstavljal novo fazo kapitalizma.

preslikave realnega življenja v virtualnega je znana igra Second life[5]. Nato so se pojavila še socialna omrežja, kot so Myspace, Facebook, Twitter, Linkedin itd. Socialna omrežja prav tako spreminjajo naše delovanje in predvsem povezovanje, hkrati pa vidimo tudi, da se s tem pridobivajo novi načini trženja in raziskovanja trga. To so torej novi način pridobivanja informacij s strani uporabnikov interneta in socialnih omrežij.

Vendar pa pri vsem tem ne smemo pozabiti, da ko sebe izpostavimo na internetu, delimo tudi svoje osebne podatke. Zavedati se moramo tudi, da moramo dati velik poudarek zasebnosti in varovanju teh podatkov. V Sloveniji imamo zelo dobro pravno podlago za varovanje osebnih podatkov.

»Varovanje osebnih podatkov pri nas izvaja informacijski pooblaščenec na podlagi ZVOP-1. Takšna ureditev je v veljavi od 31. decembra 2005, ko se je na podlagi Zakona o informacijskem pooblaščencu ustanovil neodvisen in samostojen državni organ informacijski pooblaščenec« (Informacijski pooblaščenec v Berce 2009, 17).

»Pred tem je v Sloveniji področje nadzora nad varstvom osebnih podatkov opravljal Inšpektorat za varstvo osebnih podatkov. Prva različica ZVOP je bila v Sloveniji sprejeta leta 1990.« (Berce 2009, 17)

Zakon o varovanju osebnih podatkov v prečiščenem besedilu, ki je bil sprejet 2007, v 14. členu govori o zavarovanju občutljivih osebnih podatkov.

*14. člen*

*(1) Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru iz 5. točke 13. člena tega zakona.*

*(2) Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih*

[5] ***Second Life (SL)*** *je virtualni svet, ki ga je razvilo podjetje Linden Lab in je od 23. junija 2003 dostopen preko interneta. Svojim uporabnikom, t.i. prebivalcem, omogoča, da med seboj komunicirajo preko avatarjev. Prebivalci lahko raziskujejo, srečujejo druge prebivalce, se družijo, sodelujejo v posameznih skupinah in dejavnostih, ustvarjajo in delijo virtualne dobrine ter storitve med seboj, kakor tudi potujejo po vsem svetu.(Slovenska wikipedia 2014)*

*metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.* (ZVOP-1, Uradni list št. 94/2007)

V Sloveniji na področju varstva osebnih podatkov poleg ZVOP-1[6] ureja Ustava RS, in sicer v 38. členu:

***38. člen***

***(varstvo osebnih podatkov)***

*Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.*

*Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.*

*Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.* (Ustava RS v Berce 2009, 17)

Morebitne kršitve informacijske zasebnosti sankcionira Kazenski zakonik Republike Slovenije[7] (KZ-1, 2008) z revidiranim zakonom, in sicer: (Berce 2009, 17)

***Zloraba osebnih podatkov***

***143. člen***

*(1) Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.*

*(2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.*

*(3) Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi*

[6] Zakon o varovanju osebnih podatkov. Uradni list.
[7] Kazenski zakonik Republike Slovenije. Uradni list.

*sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.*

*(4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.*

*(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let. (6) Pregon iz tretjega odstavka tega člena se začne na predlog.* (KZ-1, 2008 v Berce 2009, 17)

Neposredno se uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana leta 1994 (Kovačič v Berce 2009, 18).

## 2.1 Razvoj informacijsko-komunikacijske tehnologije

Informacijsko-komunikacijska tehnologija (v nadaljevanju: IKT) opredeljuje številne znanosti, družboslovne in naravoslovne. Kaj torej je IKT? Če povzamem, kar je Svete zapisal v svoji knjigi Varnost v informacijski družbi, je potrebna široka opredelitev IKT-ja. Pravi, da se nanaša na zbiranje, obdelavo in prikaz podatkov, prav tako pa vključuje tudi komunikacijski element, ki omogoča prenos podatkov. Označuje torej prodor moderne elektronske, predvsem računalniške in komunikacijske tehnologije v metode obdelave podatkov.

Zgodovinsko gledano termin IKT sega v 70. leta 20. stoletja, kot piše Bosch (Bosch v Svete 2005, 16). Upoštevati moramo predvsem vidik programske opreme, ki daje napravam uporabno vrednost, in človeški dejavnik, ki programsko in strojno opremo seveda uporablja. Kot pravi Svete, »IKT opredelimo kot sposobnost, znanje, spretnost oziroma tehniko, usmerjeno predvsem za uporabo strojev in naprav, ki omogočajo informacijske dejavnosti in doseganje zaželenih učinkov.«(Svete 2005, 16)

Z razvojem IKT smo v proces posegli tako, da so se podatki in informacije začele digitalizirati. Digitalizacija podatkov je torej omogočila združitev računalnikov, televizije, telekomunikacije in interneta v enotno komunikacijsko okolje, lahko rečemo tudi multimedijsko okolje, in s tem povzročila širjenje IKT tehnologije v skoraj vse družbene sektorje in aktivnosti, od zdravstva do transporta in izobraževanja (Wilson 1998, 20).

Wilson (1998, 21) pravi tudi, da pri analizi varnostnih razsežnosti uporabe IKT lahko ločimo tri vidike, in sicer Wilson (1998, 21–23) piše: IKT kot medij, IKT kot vstavljen dejavnik proizvodnje in IKT kot gonilna sila organizacijskih sprememb.

Naj še opredelimo, kaj mislimo s tem, da se je uveljavila kot medij, dejavnik proizvodnje in kot gonilna sila organizacijska sprememb.

Če pogledamo IKT kot uveljavitev v medijih, je tu mišljeno na vsebino samo. Oddajana in tiskana sporočila ter programi so implicitni kot eksplicitne vrednosti. Pri tem se Wilson sprašuje, ali je bilo sporočilo, ki smo ga poslali, dostavljeno naslovniku, in kako je naslovnik odreagiral nanj, ga prejel. (Svete 2005, 17)

Kot primer naj tu izpostavim različne vsebine na spletnih straneh, ki so lahko za bralca, uporabnika žaljive oziroma lahko vplivajo na etnične in razredne odnose ter lahko povzročijo nestrpnost ali pa v vodijo v konflikte.

Drugi vidik, ki je izpostavljen, je IKT kot vstavljen dejavnik proizvodnje in ta se bistveno razlikuje od prvega vidika. Tu se namreč IKT obravnava podobno kot tradicionalni element proizvodnje, pri katerem odnosi vplivajo na ekonomsko proizvodnjo. IKT tu dobi nov pomen, in sicer, da se nanaša na spremembe virov, do katerih imajo različne skupine ali posamezniki dostop. (povzeto po Wilson v Svete 2005, 17)

Zadnji vidik, ki je bil omenjen, je IKT kot gonilna sila organizacijskih sprememb. V tem sklopu gre za hierarhijo, ki vodi do izravnavanja organizacijskih piramid v javnem in zasebnem kot nevladnem sektorju. (povzeto po Wilson v Svete 2005, 17)

Če pogledamo malce v preteklost, ugotovimo, da je bila prva spletna stran[8] postavljena samo dve desetletji nazaj. (Dimc in etc. 2012, 11) Potem lahko rečemo, da je IKT gonilna sila razvoja tehnologije in da se je v dveh desetletjih resnično uveljavila kot medij, dejavnik proizvodnje in kot gonilna sila organizacijskih sprememb.

[8] Prva spletna stran je bila objavljena 13. 2. 1990 v Evropskem centru za jedrske raziskave (CERN), in sicer jo je objavil fizik in programer Tim Berners Lee. (Dimc in etc, 2012, II)

# 3 INFORMACIJSKA VARNOST

## 3.1 Opredelitev informacijske varnosti

Definicija informacijske varnosti temelji na »varstvu podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, uničenjem ali spremembo.« (Office of Information Technology 2014)

Informacijsko varnost lahko poimenujemo z različnimi imeni, in sicer kot varovanje računalniških sistemov ali pa varovanje informacij. Pri informacijski varnosti gre torej za zaupnost, celovitost in razpoložljivost informacij ne glede na njihovo obliko, ki pa je lahko elektronska, tiskana ali katera druga. (povzeto po Office of Information Technology 2014)

Informacijski sistem tvorijo trije glavni deli: strojna oprema, programska oprema in standardi informacijske varnostne industrije, ki se uporabljajo kot mehanizmi zaščite in preprečitve na treh ravneh: fizičnem, osebnem in organizacijskem. Za informacijsko varnost v podjetjih skrbijo operaterji ali administratorji, ki imajo specifična navodila kako zagotavljati informacijsko varnost znotraj podjetja oziroma ustanove. (povzeto po Office of Information Technology 2014)

Informacijska varnost oziroma vrednost informacij izvira iz treh glavnih lastnosti, ki so tudi njene glavne komponente. In sicer zaupnost, celovitost ter razpoložljivost. V nadaljevanju so opisane.

Zaupnost (Confidentiality): »to so informacije, ki so razumljene kot zaupne že po naravi, morajo biti dostopne, uporabljene ali razkrite osebam, ki imajo pooblastilo za njih, in takrat, ko je to resnično potrebno.« (Hopkins 2006)

Neokrnjenost (Integrity): »v sklopu pojma informacijske varnosti pomeni, da podatki ne smejo biti ustvarjeni, spremenjeni ali uničeni brez pooblastila. Prav tako pomeni, da so podatki shranjeni v enem delu informacijskega sistema, v skladu z drugimi sorodnimi podatki, shranjenimi v drugem delu informacijskega sistema (ali v drugem sistemu).« (Hopkins 2006)

Razpoložljivost (Availability): »informacijsko-računalniški sistem obdela informacije, pri čemer varnostna kontrola skrbi, da so informacije razpoložljive in pravilno delujejo, ko je informacija potrebna.« (Hopkins 2006)

Informacijska varnost je pri nas v Sloveniji tudi zakonodajno opredeljena in določena. Še posebej glede sankcioniranja kršitev, ki izhajajo iz zlorabe tajnih podatkov, in sicer z:

1. Zakonom o tajnih podatkih[9] (Ur.l. RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11),
2. Uredbo o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih[10] (Ur.l. RS, št. 48/07),
3. Uredbo o varovanju tajnih podatkov[11] (Ur.l. RS, št. 74/05, 7/11 in 24/11-popr.),
4. Sklepom o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja[12] (Ur. l. RS, št. 94/06).

**1. ) Zakon o tajnih podatkih**

*39. člen*

*Tajne podatke se mora v organih hraniti na način, ki zagotavlja, da imajo dostop do teh podatkov samo osebe, ki imajo dovoljenje za dostop do tajnih podatkov, in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.*

*Tajni podatki se lahko pošljejo izven prostorov organa samo ob upoštevanju predpisanih varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme oseba, ki ima dovoljenje za dostop do tajnih podatkov in je do teh podatkov upravičena.*

*Postopki in ukrepi varovanja pošiljanja tajnih podatkov izven prostorov organa se predpišejo glede na stopnjo tajnosti teh podatkov.*

*Organi tajnih podatkov ne smejo prenašati ali posredovati po nezaščitenih komunikacijskih sredstvih.*

*Vlada podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov.*(PISRS, 2014)

[9] Zakon o tajnih podatkih. PISRS.
[10] Uredba o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih. Uradni list.
[11] Uredba o varovanju tajnih podatkov. Uradni list.
[12] Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja. PISRS.

**2) Uredba o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih**

*3. člen*

*(pomen izrazov)*

*Posamezni izrazi, uporabljeni v tej uredbi, imajo naslednji pomen:*

*– informacijska varnost zajema določanje in uporabo ukrepov varovanja tajnih podatkov, ki se obravnavajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov;*

*– varnostno dovoljenje za delovanje sistema je pisni sklep, s katerim se dovoljuje obravnavanje tajnih podatkov v sistemu in ki potrjuje izvajanje vseh ukrepov in postopkov za zagotavljanje varnega delovanja sistema;*

*– ključne sestavine sistema so strežniki, usmerjevalniki in delilniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v nešifrirani obliki, oprema za šifrirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij;*

*– varnostni način delovanja sistema nam pove, kako se izvaja nadzor dostopa do sistema. Razlikujemo tri varnostne načine delovanja: neselektiven, selektiven in dvojno selektiven. Razlikujejo se glede na potrebno dovoljenje uporabnikov za dostop do tajnih podatkov in pravico po vedenju;*

*– kritični informacijski varnostni dogodek je vsak dogodek, ki ima ali bi lahko imel za posledico nerazpoložljivost sistema ali njegovih ključnih sestavin, razkritje varovanih podatkov ali izgubo oziroma nezaželeno spremembo podatkov, uničenje ali izgubo opreme in sredstev;*

*– neželeno elektromagnetno sevanje je sevanje, ki se nekontrolirano razširja in omogoča odtekanje tajnih podatkov;*

*– širše varnostno okolje sistema (ŠVO) je celotna okolica objekta, v katerem je nameščen sistem;*

*– ožje varnostno okolje sistema (OVO) je objekt, v katerem je nameščen sistem;*

*– elektronsko varnostno okolje sistema (EVO) je programska in strojna oprema sistema.* (Uradni list RS, št. 48/07)

*14. člen*

*(zaščita tajnih podatkov pri prenosu zunaj varnostnih območij)*

*(1) Prenos tajnih podatkov po komunikacijskih in informacijskih sistemih zunaj varnostnih območij oziroma upravnega območja je dovoljen le v šifrirani obliki.*

*(2) V sistemih se lahko uporabljajo le šifrirne rešitve, ki jih potrdi komisija iz 15. člena te uredbe, kolikor v drugih zakonskih predpisih ni drugače določeno.*

*(3) Izjemoma se lahko v izrednih okoliščinah tajni podatki stopnje tajnosti INTERNO, ZAUPNO in TAJNO prenašajo v nešifrirani obliki. Za vsak tak prenos mora izdati dovoljenje predstojnik organa ali oseba, ki jo je pooblastil. Take izredne okoliščine so:*

*– preteče ali dejanske krize, spopad ali vojne razmere ali*

*– kadar je hitrost dostave bistvenega pomena in pri tem niso na voljo sredstva in metode za šifrirno zaščito ter se ocenjuje, da je možnost zlorabe poslanih tajnih podatkov zelo majhna.*

*(4) Šifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnega oziroma upravnega območja prenašajo skladno s tem členom.*

*(5) Nešifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnih območij oziroma upravnega območja prenašajo skladno z Uredbo o varovanju tajnih podatkov.* (Uradni list RS, št. 48/07)

**3.)Uredba o varovanju tajnih podatkov (Ur.l. RS, št. 74/05, 7/11 in 24/11-popr.):**

*28. člen*

*(uporaba predpisov o poslovanju z dokumentarnim gradivom)*

*(1) Za evidentiranje dokumentov, ki vsebujejo tajne podatke, se uporabljajo določbe te uredbe in predpisov, ki urejajo poslovanje organov javne uprave z dokumentarnim gradivom, ter drugih predpisov, ki urejajo poslovanje z dokumentarnim gradivom.*

*(2) Pri evidentiranju dokumentov, ki vsebujejo tajne podatke, je treba zagotoviti, da se iz posameznih vpisov, ki jih vsebuje evidenca, ne da razbrati vsebine tajnega podatka.*

*(3) Kadar se za evidentiranje ali hrambo dokumentov, ki vsebujejo tajne podatke, uporablja informacijska tehnologija, je pogoj ločene hrambe tovrstnega dokumentarnega gradiva izpolnjen, če se uporablja rešitev, ki je fizično ločena od drugih informacijskih rešitev, ali rešitev, ki temelji na tehnologiji navideznega zasebnega omrežja in uporablja kriptozaščitne postopke in ukrepe, ustrezne stopnji tajnosti obdelovanih tajnih podatkov, ter izpolnjuje druge pogoje, določene v predpisu iz 39. člena te uredbe. Pri uporabi tehnologije navideznega zasebnega omrežja mora biti dostop do tega dela informacijskega sistema dovoljen samo osebam, ki:*

*– imajo dovoljenje ustrezne stopnje tajnosti;*

*– dokumente potrebujejo zaradi opravljanja delovnih nalog in*

*– so se uspešno identificirale z digitalnim potrdilom ter dokazale njegovo izvirnost*.
(Ur.l. RS, št. 74/05, 7/11 in 24/11-popr.):

*39.člen*

*(varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih)*

*(1) Fizične, organizacijske in tehnične ukrepe ter postopke varovanja tajnih podatkov, ki se obdelujejo, prenašajo ali hranijo v komunikacijskih, informacijskih in drugih elektronskih sistemih, ureja poseben predpis.*

*(2) Do uveljavitve predpisa iz prejšnjega odstavka se za označevanje, obdelavo, prenos in hrambo tajnih podatkov v komunikacijskih, informacijskih in drugih elektronskih sistemih uporabljajo uveljavljeni načini posameznih organov in*

*organizacij ob upoštevanju določb 17. člena te uredbe in četrtega odstavka 39. člena zakona.* (Ur.l. RS, št. 74/05, 7/11 in 24/11-popr.)

## 3.2 Mehanizmi za zagotavljanje informacijske varnosti

Mehanizmi za zagotavljanje informacijske varnosti vsebujejo veliko komponent. Poglavitne komponente, ki so najbolj pomembne za zagotovitev informacijske varnosti, so:

- zakonski in kazenski pregoni kaznivih dejanj (zapisano v kazenskem zakoniku pod členom 221, in sicer pravi člen o napadu na informacijski sistem:

  *221. čen*

  *(1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.*

  *(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.*

  *(3) Poskus dejanja iz prejšnjega odstavka je kazniv.*

  *(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.«*) (Uradni list, KZ-1, 2011)

- kriptografija;
- elektronski podpis/certifikati;
- požarni zid;
- gesla;
- različni protokoli (SSL, WTSL, SET);
- usposabljanje posameznikov oziroma človeška komponenta, ki prispevka k informacijski varnosti.

### 3.2.1 Kriptografija

»Informacijsko-komunikacijska tehnologija nam omogoča številne posege v zasebnost, saj je že v zasnovana za celostni družbeni nadzor.« (Kovačič 2006, 90) Vendar imamo prednost, da se nadzoru lahko izognemo. To posebej velja za kriptografijo. Vendar pa se pri izogibanju nadzoru začnemo spopadati z različnimi problemi, saj je v praksi to omejeno z raznimi restriktivni ukrepi in ponekod velja celo za družbeno nezaželeno. Ta princip pa ne velja za tehnologijo, ki je namenjena nadzoru. Tehnologija, ki je namenjena nadzoru, je družbeno zaželena in sprejemljiva. (Kovačič 2006, 90)

#### 3.2.1.1 Zgodovina kriptografije

Kriptografija se je razvila pred približno 4500 let in prihaja iz Egipta. Če bi si v starem Egiptu takrat mislili, da bo kriptografija postala del družbe in razvoja informacijske tehnologije in da so oni prvi začetniki tega velikega odkritja, bi med seboj delovali malce na drugačen način. Kriptografija je bila za njih tekmovanje, igra, ki so si jo izmislili. Za njih je bil to način zabave, saj so pisarji sestavljali besedne igre in tekmovali, kdo bo hitreje razvozlal besedo, ki je napisana ali samo v drugačnem vrstnem redu ali pa ima med seboj tako pomešane črke, da tisti, ki ni imel dovolj izurjenih možganov, uganke ni mogel rešiti. Egipčanom so sledili Mezopotamci, ki so celih 2000 let pozneje na glinene ploščne pisali kriptografska sporočila, kako narediti glineni lonček oziroma lončeno posodo. (Kolak 2010, 15) Naslednji so imeli opravka s kriptografijo Hebrejci. Ti so začeli uporabljati sistematično metodo. Abecedo so razdelili na dva dela in pri tem podpisovali eno na vrh druge v obrnjenem vrstnem redu. Ta postopek naj bi se pojavil nekje okoli 500–600 let pred našim štetjem. Nato je prišlo obdobje razvoja Grkov. Takrat je bil napisan priročnik, ki je vseboval poglavje o skritih pisavah. Začetnik pri Grkih je bil vojaški pisec. V komaj malo več kot desetletju so Špartanci prvi naredili mehanično napravo za pošiljanje sporočil. Ta naprava je bila izdelana iz lesa, v obliki valja, imenovala pa se je »skital«[13]. Na leseni valj so navili papir in nanj napisali sporočilo, ga odvili in poslali po slu naprej do prejemnika. Prejemnik je sporočilo navil nazaj na leseni valj in je sporočilo lahko prebral. Črke so bile zapisane v drugačnem vrstnem redu, uporabljali so metodo transpozicije črk. To je bil tudi prvi primer uporabe kriptografije v vojaške namene, nekako 400 let pred našim štetjem. Drugi pobudnik, ki je kriptografijo začel uporabljati v

[13] To je bila lesena palica, okoli katere se je ovilo pergamentni trak in nanj napisalo sporočilo. (povzeto po Dujella )

vojaške namene in s tem tudi v državno korist (mednarodno komuniciranje), je bil Julij Cezar. Uporabljal je metodo zamenjave črk, ki je po njegovem načrtu potekala tako, da je vsako črko v besedilu zamenjal s črko, ki je bila v abecedi postavljena tri mesta pred njo. (Kolak 2010, 16–20)

Kriptografija se je torej razvijala že dolgo časa pred našim štetjem oziroma pred našim časom. Skozi stoletja, desetletja se je spreminjala. Najbolj znani primer kriptografije se je pojavil med drugo svetovno vojno v Nemčiji, kjer so izumili mehanski stroj Enigma.

#### 3.2.1.2 Razvoj in začetki Enigme

> *Šifrirno napravo imenovano Enigma je leta 1919 patentiral berlinski inženir Arthur Scherbius. Bila je elektro-mehanska naprava, katere šifriranje je temeljilo na polialfabetski zamenjavi črk odprtega teksta. Po različnih modifikacijah ga je v uporabo leta 1926 uvedla nemška mornarica, 1928 pa kopenska vojska in leta 1935 letalstvo. Uporabljali so jo tudi vojaška obveščevalna služba Abwehr, varnostna služba Sicherheitdienst, varnostna policija Sicherheitpolizei, železnice, velika trgovska podjetja in vladni uradi.*(Code breaking in the World War II v Soklič 2002, 28)

Enigma je električna naprava za šifriranje sporočil in je bila zasnovana kakor pisalni stroj. Enigma je bila sestavljena iz 26 tipk, katera je imela vsaka pod seboj še 26 okroglih lučk z istim razporedom črk kot na tipkovnici. Poleg vseh teh tipk in lučk je zadeva vsebovala še tri ali več kolesc skozi katere so črke potovale, da se je sporočilo zakodiralo. Torej, v tem primeru je bilo na vsaki strani(levi in desni) še po 26 izhodov po katerih so črke potovale.

Enigma se je do konca 2.svetovne vojne velikokrat modificirana. K temu je pripomogla odvisnost njene rabe ( katere družbe oziroma državne ustanove so jo uporabljale). (Stripp, 1999)

Naj povem od kod izhaja beseda Enigma. Beseda izhaja iz grške besede aínigma, kar pomeni po naše uganka. Za katero je dobil patent leta 1918, kasneje so Enigmo prevzeli oziroma so ustanovili podjetje, katero je začelo proizvajati te naprave. Proti koncu leta 1920 so začele oborožene sile kazati zanimanje za Enigmo, vendar pa je kasneje izginila iz civilnega trga. To

pomeni, da Enigma ni bila naprodaj za normalnega, civilnega človeka oziroma ni bila družbeno zaželena. (povzeto po Stripp 1999)

Kriptologi oziroma matematiki so se borili skozi to, da sporočilo ki je za kriptirano mora ostati dosegljiv samo tistemu, ki ga želi odkodirati. Enigmo se je dalo odkodirati tudi z najbolj preprostimi strojnimi metodami. Pri Enigmi so se želi držati pravila, ki temelji na znanemu znanstveniku Kerckhoffu in z njim je prišlo tudi to načelo : »Varnost sistema šifriranja ne sme biti odvisna od načina šifriranja. Za tajnost je edina garancija tajnost ključa.«

#### 3.2.1.3 Kaj je kriptografija?

*»*Kriptografija (beseda izvira iz grškega izraza kryptos logos, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil sir Thomas Browne leta 1658 (Kahn 1973, 432)), je veda o tajnosti, šifriranju, zakrivanju vsebine sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza*)«* (Kovačič 2006, 91)

Kriptografijo lahko imenujemo še z drugimi izrazi. Če gre za temeljno sporočilo, ga imenujemo čistopis (ang.: cleartext, plaintext). Če gre za že zašifrirano sporočilo, pa šifropis ali tajnopis (kriptogram, ciphertext).

Kriptografija je starodaven način zagotavljanja zaupnosti. Ko si pošiljatelj in prejemnik delita skrivnost prek kanala, se to imenuje ključ. Enkripcija je postopek, pri katerem se berljiv tekst spremeni v kodiran tekst (cipher text). Če želimo dobiti na drugi strani berljiv tekst, ga moramo dekriptirati. Celoten mehanizem – algoritmi šifriranja in dešifriranja – se imenuje šifra. (povzeto po Si-ca 2014)

Pri simetričnem šifrirnem postopku šifriramo in dešifriramo sporočilo z istim ključem. Pri tem moramo biti pozorni, da so vsi udeleženci, ki imajo dostop do tega sporočila, prisotni in da si geslo oziroma ključ shranijo na varno. Vendar pa uporaba identičnih ključev ni ravno najbolj varna. (Kovačič 2006, 91)

Pri asimetričnih šifrirnih postopkih poznamo dve vrsti ključev: javni in zasebni ključ. Ključ, ki lahko samo šifrira in ne more odšifrirati, se imenuje javni ključ. Dešifrirni ključ pa

imenujemo zasebni ključ. Tu nam ni treba paziti, da pri kodiranju sporočila prejemniku ne pozabimo povedati ključa. En ključ, eno sporočilo. (Kovačič 2006, 92)

Mehanizem uporabe zasebnega in javnega ključa je opisan takole: »Leta 1978 so na Massashusets Institute of Technology (MIT) razvili kodirni algoritem RSA, ki omogoča praktično nezlomljivo kriptografijo, kar pomeni, da so podatki, zaščiteni s to kriptografsko metodo izjemno varni. Metoda RSA namreč deluje tako, da imata tako tisti, ki sporočilo pošilja (pošiljatelj), kot tisti, ki sporočilo sprejema (prejemnik), vsak svoj par ključev. Zasebnega, ki je tajen, in javnega, ki je javno dostopen.« (Povzeto po Kriptografija ali kako se zaščititi pred elektronskim prisluškovanjem, 2014)

Kako poteka kodiranje sporočil? »Ker sta ključa med seboj povezana v posebnem matematičnem razmerju, mora pošiljatelj sporočilo zakodirati s svojim zasebnim in prejemnikovim javnim ključem, tako kodirano sporočilo pa potem pošlje prejemniku. Prejemnik pa to sporočilo nato odkodira s svojim zasebnim in pošiljateljevim javnim ključem.« (Povzeto po Kriptografija ali kako se zaščititi pred elektronskim prisluškovanjem, 2014)

### 3.2.2 Elektronski podpis/certifikati

»Electronic signature« ali po slovensko elektronski podpis, ki ga imenujemo še digitalni podpis, varen elektronski podpis, najboljše opredeljuje Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1), ki pravi, da »je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki (npr. z elektronskim dokumentom), in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.« (Si-ca 2006)

Poleg klasičnega elektronskega podpisa, kot sem omenila zgoraj, poznamo tudi varen elektronski podpis oziroma »advanced electronic signature«. To je elektronski podpis, ki zadošča dodatnim pogojem.

*Po Zakonu o elektronskem poslovanju in elektronskem podpisu*[14] *(ZEPEP-UPB1*[15]*) 2. člen 1. odstavek 4. točka, gre za elektronski podpis, ki izpolnjuje naslednje zahteve:*

- *da je povezan izključno s podpisnikom;*
- *da je iz njega mogoče zanesljivo ugotoviti podpisnika;*
- *da je ustvarjen s sredstvi za varno elektronsko 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;* (Si-ca 2006)

Natančneje poglejmo še, katera dva člena prav specifično vplivata na elektronski podpis na strani zakonodaje:

*14. člen*

*Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.*

*15. člen*

[14] Zakon o elektronskem poslovanju in elektronskem podpisu. PISRS.
[15] UPB1 – pomeni uradno prečiščeno besedilo, kjer so zajete vse spremembe zakona.

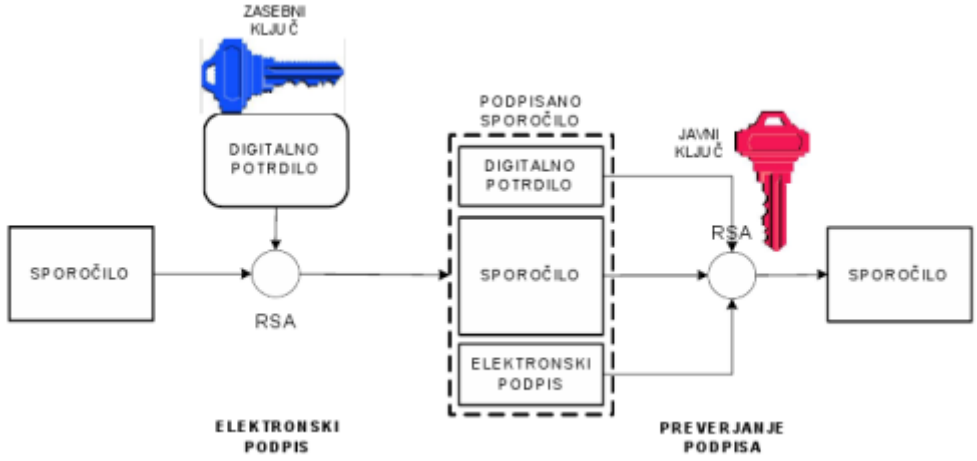
*Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.* (Uradni list RS v PISRS, 2014)

Lahko tudi rečem, da je »ena od osrednjih lastnosti varnega elektronskega podpisa ravno zahteva po neokrnjenosti podatkov v primerjavi z lastnoročnim podpisom podatkov.« (SI-CA 2006)

Na kateri informacijsko-komunikacijski tehnologiji torej temelji elektronski podpis? Elektronski podpis temelji na asimetrični kriptografiji in je v praksi edina tehnična rešitev, ki jo lahko danes uporabimo za varne elektronske podpise. Zagotavlja pristnost podatkov in jih varuje pred spremembami s kriptografskimi metodami, ki sem jih opisala že v poglavju o kriptografiji.

Za boljšo predstavo si oglejmo slikovno in tekstovno predstavitev kriptiranosti sporočila. Imamo izvorno sporočilo, ki ga želimo poslati osebi B. Naše sporočilo je na levi strani in ga podpišemo s svojim kriptiranim (zasebnim) ključem, ki pripada digitalnemu potrdilu. Ko imamo združeni obe komponenti skupaj, torej zasebni ključ in digitalno potrdilo, je naše sporočilo kriptirano, nato pa ga pošljemo prejemniku, torej osebi B. Oseba B s pomočjo javnega ključa, ki ga dobi iz pošiljateljevega digitalnega potrdila, preveri veljavnost podpisa, s čimer potrdi njegovo celovitost. Iz podatkov v digitalnem potrdilu lahko identificira (avtenticira) podpisnika.

**Slika 3.1: Prikaz kriptiranosti elektronskega podpisa**

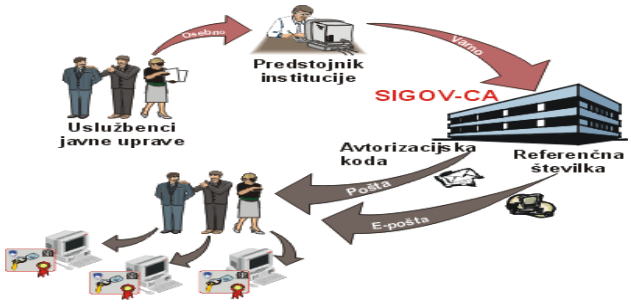



**Vir: Igor Lesjak Crea d.o.o (2014)**

V Sloveniji poznamo različna potrdila:

- SIGOVCA – digitalna potrdila so namenjena identifikaciji v javni upravi,
- »SIGENCA je digitalno potrdilo, ki omogoča dostop do spletnih storitev. Spodaj je prikazan krog, kako deluje digitalno potrdilo oziroma SIGENCA.« (Sigovca v Berce 2009, 24)

**Slika 3.2: Prikaz delovanja SIGENCE**




**vir:SIGOV-CA (2014).**

**Certifikatska agencija POŠTA®CA** je overitelj digitalnih potrdil, ki izdaja:

- kvalificirana digitalna potrdila,
- normalizirana digitalna potrdila in
- varne časovne žige, ki dopolnjujejo elektronsko podpisovanje. (Pošta 2014)

**HALCOM CA** je najstarejši in tudi največji overitelj v Sloveniji, ki za shranjevanje digitalnih potrdil uporablja najvarnejšo tehnologijo pametne kartice. (Halcom 2014)

### 3.2.3 Požarni zid

»Požarni zid ali angl. firewall je verjetno najpogostejši varnostni izdelek s področja omrežne varnosti. Požarni zid morajo imeti nastavljene vse naprave, ki imajo kakršno koli povezavo z internetom.« (Wikipedija 2014)

Požarne zidove delimo na strojne in programske. »Prednost programskih požarnih zidov je običajno v enostavnejši uporabi in ti se uporabljajo predvsem za domačo uporabo. Prednost strojnega požarnega zidu pa je pogosto v hitrosti, saj so običajno strojne rešitve precej hitrejše in tako omogočajo večjo prepustnost.«(Wikipedija 2014) Strojna oprema je primerna za podjetja in ustanove.

Med naprednejše funkcije požarnega zidu spadajo:

- preslikava (zasebnih) omrežnih naslovov (angl. oznaka NAT), ki omogoča skupno rabo internetne povezave,
- demilitarizirana cona (angl. oznaka DMZ), ki omogoča ločen priklop bolj izpostavljenih naprav,
- kontekstno odvisni nadzor dostopa, ki na podlagi protokolov dinamično dovoli dostop do storitev,
- nudijo kriptirane tunelske povezave in tako omogočajo navidezna zasebna omrežja (angl. oznaka VPN) (Cheswick 2014),
- IDS je kratica za sistem zaznavanja vdorov. Je naprava ali aplikacija, ki spremlja dejavnosti omrežja ali sistema glede zlonamernih dejavnosti in pripravlja poročila za upravljanje postaje. (Holland 2004, 4),
- IPS je sistem za preprečevanje vdorov, znan tudi kot sistem za odkrivanje in preprečevanja vdorov (IDPS). Oba sistema sta varnostni naprave omrežja, ki nadzorujeta omrežje in/ali sistemske dejavnosti glede zlonamernih aktivnosti. Glavna funkcija sistemov za preprečevanje vdorov je torej opredeliti zlonamerne aktivnosti. (Holland 2004, 3)

### 3.2.4 Gesla

Geslo je zaščita vašega profila in zasebnih ključev in mora biti dolgo vsaj 8 znakov. Programska oprema vam pri prevzemu posebnega digitalnega potrdila narekuje izbiro gesel, ki omogočajo pomembne mehanizme zaščite za preprečitev napada na osnovi slovarja (iskanje gesel s pomočjo slovarja besed), lahko pa se geslo še bolj zaščiti na naslednji način:

- mešana uporaba velikih in malih črk, števil in posebnih znakov,
- geslo, dolgo vsaj 8 znakov,
- izogibajte se besedam, ki so zapisane v slovarjih. (Sigenca 2014)

Najboljše si je geslo zapomniti. Če si pa si geslo zapišete, ga shranite tako, da boste vedeli zanj samo vi oziroma je najboljše, da ga kriptirate in naredite nevidnega na rezervni kopiji, npr. na USB-ključu. Enako lahko na rezervno kopijo prenesete vsa potrdila.

Zakonodaja, ki ureja varovanje podatkov – in v našem primeru torej gesla in požarni zid –, je standard ISO 17799.

Standard ISO 17799/BS 7799 določa upravljavski sistem za svoje področje – sistem varovanja informacij. ISO 17799 je torej podroben varnostni standard, ki se je razvil iz britanskega standarda za informacijsko varnostno upravljanje (BS 7799). Pokriva deset največjih področji, ki se tičejo varnosti. (B2B Continuty 2014)
Ta področja so:

- poslovno načrtovanje (Business Continuity Planning),
- sistem dostopa (System Access Control),
- sistem za vzdrževanje in razvoj (System Development and Maintenance),
- fizična in okoljska varnost (Physical and Environmental Security),
- skladnost (Compliance),
- osebna varnost (Personnel Security),
- organizacijska varnost (Security Organisation),
- računalniško in mrežno upravljanje (Computer & Network Management),
- razvrstitev in nadzor (Asset Classification and Control),
- varnostna politika (Security Policy).

Vendar zgoraj opisani ISO standard ni več v veljavi, saj nihče več ne preverja in ne revizira po njem. Nadomestil ga je novi standard in sicer ISO IEC 27001:2013.

ISO IEC 27001 je informacijsko varnostni standard z zelo širokim spektrom obsega. Standard vključuje različne informacije v navezavi z podatki, dokumenti, sporočili, komunikacijo, pogovori, prenosi, snemanji oz zabeležbami, risbami in fotografijami. Zajema, torej vse oblike informacij. (Praxiom 2014)

### 3.2.5 Varnostni protokoli

Varnostni protokoli se uporabljajo za varne povezave med strežnikom in odjemalcem (v našem primeru torej z spletnim brskalnikom). Imamo več vrst prenosa podatkov, in sicer SSL, TLS in WLTS.

»**SSL** ali Secure Sockets Layer je kriptografski protokol, ki omogoča varno komunikacijo na medmrežju v naslednjih primerih: pri brskanju po spletu, uporabi e-pošte in instantnega sporočanja.«(Microsoft Technet 2014)

Protkol SSL se uporablja predvsem tam, kjer se pojavlja potreba po prenosu podatkov zaupne narave. Sem sodijo npr. osebni podatki in številke kreditnih kartic. Storitve, pri katerih se to uporablja so različne spletne trgovine, spletno bančništvo (e-bančništvo) in ostale strani, ki vsebujejo vnos osebnih podatkov in njihovo verifikacijo. Slaba lastnost povezave SSL pa je, da ščiti podatke le med pošiljanjem, ne pa tudi, ko prispejo na ciljni računalnik. (povzeto po Microsoft Technet 2014)

»**TLS** ali Transport Layer Security je naslednik SSL-ja. Je kriptografski protokol, ki omogoča varno komunikacijo na medmrežju. Ima enake specifikacije kot SSL, vendar je narejen na varnejši način.« (Microsoft Technet 2014)

Kako torej poteka komunikacija po protokolu SSL ali TLS? Uporabnik prek brskalnika pošlje zahtevo za spletno stran z varovanim prenosom SSL (ali TLS). Ta se na strežniku predstavi z javnim ključem. Proces uporablja šifriranje z javnim ključem in digitalnim potrdilom. Tako se ta zahteva potrdi na strežniku, saj jo strežnik verificira. In ko se strežnik predstavi, se v brskalniku ustvari ključ za enkripcijo s simetričnim ključem, sporočilo zakodira s strežnikovim javnim ključem in ga pošlje. Strežnik prejme ključ in ga dekodira z zasebnim

ključem. Od tu naprej poteka povezava prek veliko hitrejše enkripcije. (povzeto po Microsoft Technet 2014)

**WTLS** ali Wireless Transport Layer Security je v bistvu prirejen TLS, in sicer tako, da podpira izmenjavo paketov na nezanesljivih in počasnih povezavah (WDP ustreza UDP[16] in ne TCP). Potek izmenjave in overitve parametrov ima tako kot pri TLS (prej SSL) skrajšano verzijo, da se za spremembo šifrirnega ključa uporabijo že dogovorjeni parametri in to je seveda zelo pomembno v tem omenjenem okolju (če imamo res zelo počasno povezavo). Tu se uporabljam predvsem skupni šifrirni ključ, ki se imenuje protokol Handshake[17]. (povzeto po Webopedia in Wikipedia 2014)

Protokol **SET** oziroma Secure Electronic Transaction je aplikacijski protokol, ki ureja nakupovanje s kreditnimi karticami prek interneta. (SI-CA 2014) Protokol SET zagotovi uporabniku, »da so trgovci, ki sprejemajo kartice, za to avtorizirani, istočasno pa trgovcu zagotavljajo pravilno identiteto lastnika kartice.« (Ošlak 2005, 40)

### 3.2.6 Usposabljanje posameznikov oziroma človeška komponenta prispevka k informacijski varnosti

V prejšnjih podpoglavjih je bilo veliko napisano o tehnični plati informacijske varnosti, vendar ne smemo pozabiti tudi na človeško komponento, ki veliko prispeva k zagotavljanju informacijske varnosti. Če posamezniki niso podučeni o morebitnih zlorabah/napadih, ki se jim lahko zgodijo, če ne uporabljajo pravilno določenih informacij, so toliko bolj ranljivi za napade, ki bodo opisani v naslednjem poglavju. Drugače pa lahko rečem, da programer kode lahko vedno naredi napako v kodi, ki jo zapiše, ali pa na kateri koli način izpostavi storitev nepravilnemu delovanju. Vendar je ima to tudi pozitivno stran, saj podjetja tako vlagajo v posameznike, jih pošiljajo na razne seminarje, kjer jih seznanjajo z novostmi.

## 3.3 Oblike napadov oziroma ogrožanj informacijske varnosti

Čeprav smo upoštevali vse komponente oziroma mehanizme za zagotavljanje informacijske varnosti, jo lahko izurjeni napadalci še vedno ogrozijo. Pri tem moramo vedeti, katera so

[16] WDP je brezžičen podatkovni protokol, ki definira gibanje podatkov od sprejemnika do pošiljatelja. **UDP** (ang. *User Datagram Protocol*) je nepovezovalni protokol za prenašanje paketov.
[17] To je avtomatiziran proces do pogajanja, ki dinamično nastavi parametre komunikacijskega kanala, vzpostavljen je med dvema entitetama, preden se začne normalna komunikacija prek kanala.

največja ogrožanja informacijske varnosti, in se zavedati možnosti, da je pri uporabi e-bančništva ogrožena naša varnost. Informacijska varnost je lahko ogrožena na več načinov, v primeru e-bančništva pa še toliko bolj izpostavljena. Poznamo več oblik napadov oziroma ogrožanj:

- napadi DDOS,
- napadi CSFR,
- phishing oziroma ribarjenje,
- socialni inženiring,
- kriminalna programska oprema (ang. crimeware),
- posnemek (ang. skimming)
- MITM (ang. Man-in-the-middle attack).

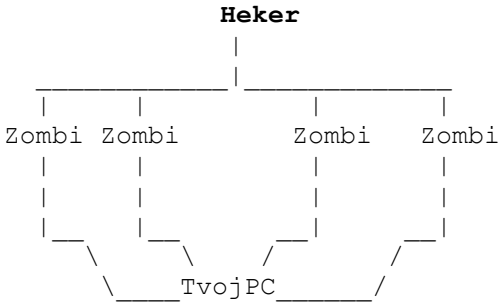
### 3.3.1 Napadi DDOS

Pri napadih DDOS (ang. Distributed Denial of Service) heker običajno nadzoruje večjo količino računalnikov, imenovanih »DoS box« ali »zombi«, ki sledijo njegovim ukazom. Po navadi si je te računalnike pridobil z vdorom ali pa ima legalen dostop do njih. Heker z določenimi ukazi ali pa kar s programom (TFN – Tribe flood Network[18]) sporoči svojim računalnikom DDoS, naj napadejo tarčo z določeno količino podatkov. Pri tem napadu je podatkov bistveno več kot pri DoSu, saj več računalnikov pošlje več podatkov kot eden. (povzeto po Rouse 2014)

Glavna posledica napada DDOS je izpad dostopnosti do sistema, s čimer se prekine veriga osnovnih načel varnosti – zaupnost, okrnjenost, razpoložljivost. To lahko ima za posledico izgubo strank in/ali tudi finančnih izgub za banko. Ob vsem tem pa obstaja še nevarnost vdora v sistem in kraje zaupnih podatkov, kar privede še do dodatnih izgub in stroškov. Posledica napada DDOS na e-bančništvo je onemogočanje dostopa do sistema in se izkoristi za prikrivanje vdora v sistem, ker se sistem več ne beleži dogodkov, postane neodziven ipd. (povzeto po Rouse 2014)

[18] Tribe Flood omrežje ali TFN je niz računalniških programov za vodenje različnih napadov DDoS, kot so poplava ICMP, poplava SYN, poplave UDP in napad Smrkcev. (Ditrrich 1999)

**Slika 3.3: Skica napada DDOS na tarčo**

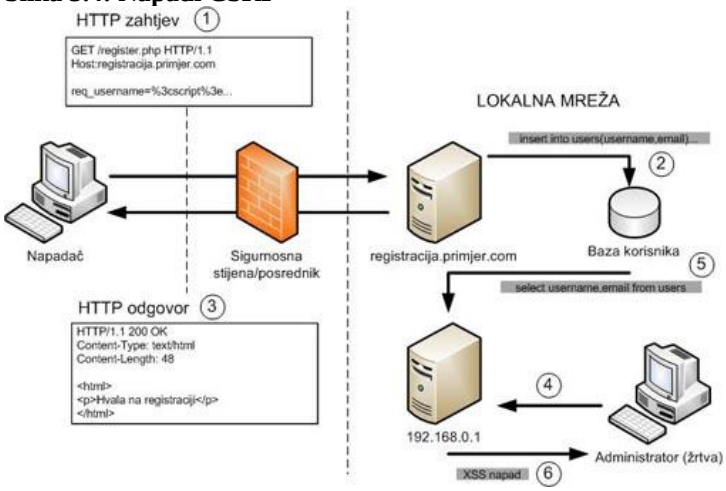



Vir: Wikipedia (2014)

### 3.3.2 Napadi CSRF

Napad CSRF (ang. Cross-Site Request Forgery) je napad, pri katerem napadalec v imenu pooblaščenega uporabnika dostopa do spletne strani. Pri tem izkorišča mesto, ki ne preveri izvora HTTP zahteve, preden jo izvede. Poleg napak na spletni strani je izkoriščen spletni brskalnik, v katerem je uporabnik shranil podatke za dostop do ranljivega spletnega mesta. (Nacionalni Cert + 2014)

**Slika 3.4: Napadi CSRF**




Vir: Zeman (2014)

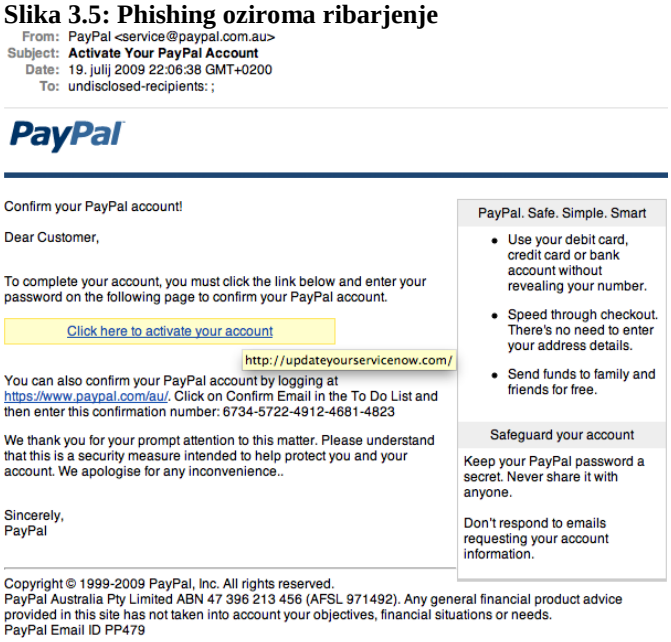
### 3.3.3 Phishing oziroma ribarjenje

Phishing oziroma ribarjenje »je kraja podatkov, ki storilcu omogočijo dostop do spletnih storitev v našem imenu (kraja identitete) in v skrajnem primeru tudi krajo našega denarja. « (Si-cert 2014)

Kako deluje ribarjenje? »V običajnem scenariju nas skuša storilec z elektronskim sporočilom zvabiti na lažno stran banke ali spletne storitve, običajno pod pretvezo, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in »preveriti podatke.« (Si-cert 2014)

Če na tej lažni, tj. phishing strani vpišemo geslo za dostop, se to posreduje storilcu. (povzeto po Si-cert 2014)

**Slika 3.5: Phishing oziroma ribarjenje**




Vir: Anti-virus (2014)

### 3.3.4 Socialni inženiring

Socialni inženiring opredeli Kevin Mitnick, heker in avtor knjige o socialnem inženiringu »Umetnost prevare« (Art of Deception): »Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali pa z manipulacijo. Posledica tega je, da lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologije.«(Informacijski pooblaščenec 2009,5)

**Slika 3.6: Socialni inženiring**


Vir: Informacijski pooblaščenec (2009)

### 3.3.5 Kriminalna programska oprema oziroma crimeware

Kriminalna programska oprema oz. crimeware je zlonamerna programska oprema. To je vsak računalniški program ali skupek programov, namenjenih izrecno za omogočanje nezakonitih aktivnosti na spletu. Sem lahko štejemo veliko raznih vohunskih programov (ugrabitelji brskalnikov, t. i. keyloggerji ipd..). Pogosto se zlonamerna programska oprema lažno predstavlja kot protivirusni program ali zbirka legitimnih programskih orodij z namenom zavajanja uporabnikov. Takšna programska oprema se uporablja predvsem za phishing napade. (povzeto po Panda Security: Crimeware: the silent epidemic 2014)

**Slika 3.7: Prikaz napada s kriminalno programsko opremo**


Vir: Securelist (2014)

### 3.3.6 Posnemek oziroma skimming

Posnemek oz. skimming je kraja podatkov o kreditni kartici. Storilec ukrade številko kreditne kartice s pomočjo klasičnih metod, kot so fotokopiranje potrdil ali z uporabo naprednih

metod, ki vključujejo elektronsko napravo (skimmer) s katero se s kreditne kartice prebere podatke (povzeto Scam watch 2014).

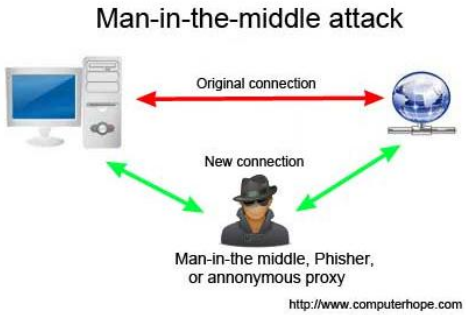
**Slika 3.8: Prikaz delovanja naprave za skimming**


Vir: Sawer (2008)

### 3.3.7 MITM

MITM ali sredinska oseba pri napadu (ang. Man-in-the-middle attack) je napad, kjer uporabnik dobi od pošiljatelja in prejemnika informacije in sniffs kakršne koli informacije, ki so bile poslane. V nekaterih primerih lahko uporabniki pošiljajo nešifrirane podatke, kar pomeni, da man-in-the-middle (MITM) lahko pridobi vse nešifrirane podatke. (Computerhope 2014)

**Slika 3.9: Skica Man-in-the-middle napada na tarči**




**Vir:** Computerhope (2014)

# 4 E- poslovanje

Družboslovci in tehniki pravijo, da se pri elektronskem poslovanju komaj ločljivo prepletajo tehnično-tehnološke in pravno-organizacijske sestavine.(povzeto po Toplišek 1998, 1)

Kakšna je torej definicija elektronskega poslovanja, če zajema vse te komponente?

»Elektronsko poslovanje je poslovanje, ki presega meje ene organizacije in temelji na izmenjavi podatkov med računalniki. Je splošen izraz za elektronski način opravljanja dejavnosti s pomočjo elektronskega sporočanja« (Lobe 2003, 3).

> *Elektronsko poslovanje pomeni, da so podjetja s pomočjo računalnikov in informatizacije procesov posodobila del ali celotno poslovanje, kot na primer komunikacijo z dobavitelji in odjemalci, skladiščenje, distribucijo, trženje, prodajo in podobno. Vendar je elektronska trgovina le del elektronskega poslovanja podjetja. Poznamo elektronsko poslovanje med podjetji in posamezniki (elektronska trgovina, elektronsko bančništvo), elektronsko poslovanje med podjetji (trgovanje) in elektronsko poslovanje med posameznikom in državnimi ustanovami (sodelovanje na razpisih, napoved dohodnine ipd.) (Lobe 2003, 3).*

## 4.1 Opredelitev e-poslovanja

Pojem elektronskega poslovanja izhaja iz angleškega poimenovanja »electronic commerce«. E-poslovanje so sprva uporabljali v trgovini in industriji. Njegova vloga v gospodarstvu pa je obsegala sledeče sestavine (Toplišek 1998, 4):

- »način dela: elektronske izmenjave podatkov,
- vsebine poslovanja: so skoraj neomejene,
- glavne tri skupine udeležencev so: podjetja/podjetniki, državne/javne službe in posamezniki.« (Toplišek 1998, 4)

Tukaj gre za različne vrste interakcije med različnimi subjekti. Tako v literaturi kot v praksi so se izoblikovale tri glavne vrste elektronskega poslovanja (Jerman Blažič 2001, 17):

- podjetje–podjetje (B2B),
- podjetje–potrošnik (B2C),
- javna in državna uprava–podjetja in posamezniki. (Jerman- Blažič 2001, 17)

V novejšem času sta se tem glavnim oblikam pridružili še dve (Mojca Osojnik, Ariana Grčman 2002, 6):

- potrošnik–podjetje (C2B),
- potrošnik–potrošnik (C2C).

## 4.2 Zgodovinsko ozadje e-poslovanja

»E-poslovanje se je začelo z razvojem računalniških omrežij in interneta ter hkrati z združevanjem informacijske in telekomunikacijske tehnologije.« (Jerman - Blažič 2001, 13)

Pri tem so pripomogli tudi standardi za računalniško izmenjavo podatkov. Vse skupaj sega že v leto 1968. Kot pravi Jerman - Blažič v knjigi Elektronsko poslovanje na internetu, »je bila računalniška tehnologija sprava namenjena le računalniškim strokovnjakom in znanstvenikom, vendar je z leti postala veliko bolj uporabna in prijazna, sčasoma pa je postala nepogrešljiva za laike.« (Jerman - Blažič 2001, 13)

Na finančnem trgu se je v sedemdesetih letih spremenil način poslovanja, saj se je takrat pojavil elektronski finančni prenos med bankami prek varnih zasebnih omrežij, imenovan SWIFT.[19]

Že v sedemdesetih letih, predvsem pa v poznih sedemdesetih in zgodnjih osemdesetih se je elektronsko poslovanje razširilo v obliki sistemov za prenos datotek, računalniške izmenjave podatkov in elektronske pošte v okviru podjetji. Že s samo uporabo elektronskih virov so podjetja zmanjšala obseg papirnega dela in povečala avtomatizacijo pisarniškega poslovanja. (povzeto Jerman - Blažič 2001, 14)

Osemdeseta leta so torej minevala v celostnem razvoju računalniške tehnologije, ki se je iz podjetij razširila na veleprodaje in trgovine na drobno, saj so z uvedbo računalniške tehnologije zmanjšali stroške, npr. pri nakupih papirja itd. (Jerman - Blažič 2001, 14)

[19] SWIFT je koda, ki je standardnega formata pri bančnih identifikacijskih oznakah (BIC), in je enoznačna identifikacijska koda za posamezno banko.

»Sredi osemdesetih so se pojavile elektronske konference kot nova oblika družbene interakcije ter prenosa znanja. Hkrati se je povečala tudi dostopnost do informacij in njihova izmenjava.«(Jerman - Blažič 2001, 14)

V poznih osemdesetih in pozneje še v zgodnjih devetdesetih so sistemi za izmenjavo sporočil postali integralni del računalniških sistemov in omrežij. (Jerman - Blažič 2001, 14)

Devetdeseta so z razvojem in razširjenostjo interneta in s pojavom svetovnega spleta prinesla preobrat, ki je elektronsko poslovanje pripeljal do stanja, kakršnega poznamo danes. (povzeto Jerman - Blažič 2001, 14) Uvedene so bile nove tehnologije, aplikacije so bile prilagojene in nadgrajene, da so postale bolj prijazne uporabnikom in enostavnejše za uporabo. Svetovni splet, sedaj znan kot WWW, je pomenil čudežno odkritje, saj si samo z enim klikom na miško prišel do enostavne objave informacij in njihove porazdelitve po internetu. (Jerman - Blažič 2001, 14)

Za vse to je bil potreben samo računalnik, modem in povezava z internetom. Blažič - Jerman zapiše, da mnogo avtorjev ocenjuje, da je elektronsko poslovanje doživelo meteorski vzpon v letu 1996, ko je tehnologija interneta in na njo vezanih aplikacij dozorela. (povzeto po Jerman - Blažič 2001, 16)

## 4.3 Prednosti in slabosti e-poslovanja

### 4.3.1 Prednosti elektronskega poslovanja

Ker smo v prejšnjih dveh podpoglavjih razpravljali o tem, kaj je e-poslovanje in kako je e-poslovanje nastalo, moramo izpostaviti tudi njegove prednosti in slabosti. Vsak sistem ima določene slabosti in tudi pri e- poslovanju ni vse tako, kot bi bilo potrebno.

V našem primeru se oziramo po potrebi e-poslovanja med stranko (posameznikom) in institucijo (banko), ki nam omogoča prenos podatkov oziroma informacij. Katere prednosti ima torej posameznik in katere prednosti ima potem institucija?

*Najpomembnejše prednosti za uporabnike:*

- *različne možnosti dostopa do storitev in informacij,*
- *storitve so prilagojene v večji meri,*
- *uporabniki so vključeni v oblikovanje storitev in njihove izboljšave,*

- *uporabniki so vključeni v proces odločanja,*
- *stroški so nižji,*
- *prihrani se čas za opravljanje storitev in pridobivanje informacij,*
- *storitve so na voljo tudi izven delovnega časa.* (Resnik 2010)

*Najpomembnejše prednosti za podjetja:*

- *kljub začetnim višjim investicijskim stroškom se dolgoročno posluje z nižjimi stroški,*
- *poslovanje je bolj pregledno,*
- *viri so bolje razporejeni,*
- *storitve za uporabnike so hitrejše,*
- *kakovost storitev je višja,*
- *manj je napak in podvajanja dela,*
- *elektronsko komuniciranje prinaša boljšo in modernejšo podobo podjetja pri poslovnih partnerjih in strankah,*
- *višja kvaliteta storitev oz. izdelka.* (Resnik 2010)

### 4.3.2 Slabosti elektronskega poslovanja

Smo v informacijski dobi, ko naj bi vsak posameznik že imel dostop do računalnika (PC) oziroma do drugih naprav, ki so še mnogo prijaznejše za uporabo. Prav tu pa se pokaže tudi največja slabost. Predvsem ne smemo pozabiti in izpostaviti starejših generacij, ki dejansko niso vajene dela z računalnikom in ga v svojem življenju niso skoraj nikoli uporabljale. Poleg zgoraj omenjenih slabosti so še druge, ki so naštete in povzete v spodnjih točkah.

*Omejitve predstavljajo različni dejavniki:*

- *socialne potrebe (npr. osebni stik),*
- *kulturna vprašanja (npr. jezikovne ovire),*
- *ekonomski dejavniki (dostopnost informacijske tehnologije),*
- *dejavniki povezani z učenjem (npr. spoznavanje nove tehnologije, računalniška pismenost, spreminjanje navad ipd.),*
- *fizični dejavniki (npr. telesne nezmožnosti, slepota),*
- *razvitost omrežja za zagotavljanje storitev informacijske tehnologije.* (Resnik 2010)

*Ostale slabosti:*

- *možnost zlorabe informacijske tehnologije,*
- *nezaupanje v novosti,*
- *neosebnost takšne oblike komuniciranja,*
- *napake in zamude, ki se pojavijo ob uvajanju novih tehnologij.* (Resnik 2010)

## 4.4 Pravna ureditev e-poslovanja

Zakon o elektronskem poslovanju in elektronskem podpisu temelji na sodobnih načelih: načelo nediskriminacije elektronske oblike, načelo odprtosti, načelo pogodbene svobode strank, načelo dvojnosti, načeli varstva osebnih podatkov in varstva potrošnikov in načelo mednarodnega priznavanja. (Si-ca 2014)

1. Načelo nediskriminacije v e-poslovanju pomeni, da imata papirna in elektronska oblika smiselno enako težo in da pred sodiščem ali drugimi državnimi organi pri presoji dokazov ne smemo zavreči dokaznega gradiva zgolj zaradi njegove elektronske oblike. (povzeto po Si-ca 2014)
2. Načelo odprtosti, drugače poimenovano tudi kot tehnološka nevtralnost, ni omejeno samo na eno od vrst tehnologije ali pa na trenutno rešitev, temveč ostaja splošno in uporabno za daljše časovno obdobje in nove tehnologije. (povzeto po Si-ca 2014)
3. Vzporedno s tehnološkem razvoj se razvija tudi načelo dvojnosti, »ki dovoljuje uporabo različnih tehnoloških rešitev z različno zanesljivostjo in s tem tudi različnimi pravnimi posledicami uporabe takšnih rešitev.« (povzeto po Si-ca 2014)
4. Načelo pogodbene svobode strank je namenjeno strankam, da se lahko dogovorijo in svoja razmerja uredijo drugače. Tako zakon izrecno določa, »da ne velja za zaprte sisteme, v katerih stranke s pogodbo vnaprej uredijo vse bistvene značilnosti delovanja sistema. Pogodbene stranke tako pri elektronskem poslovanju v zaprtih sistemih niso vezane zgolj na v zakonu predvidene rešitve.« (povzeto po Si-ca 2014)

Pri vsem tem pa ne smemo pozabiti še na to, da e-poslovanje poteka prek različnih tehnologij, v večini primerih prek interneta. Zgolj pri tem pa moramo paziti, da ne zlorabimo informacij oziroma osebnih podatkov potrošnikov v napačne namene.

*Načelo varstva osebnih podatkov sledi najnovejšim pravilom, uveljavljenim v Sloveniji in Evropski uniji, glede varstva osebnih podatkov, ki so v elektronskem svetu še bolj*

*izpostavljeni. Načelo varstva potrošnikov pa varuje povprečnega potrošnika, ki brez veliko tehnološkega znanja v zapletenem elektronskem poslovanju teže uveljavlja svoje pravice, in nalaga ponudnikom storitev posebno skrb za potrošnika.* (Si-ca 2014)

# 5 Bančništvo v Sloveniji

*»Zgodovina dela ljudi modre, poezija duhovite, matematika ostroumne, naravna filozofija globokoumne.« Francis Bacon*

## 5.1 Zgodovina bančništva v Sloveniji

Bančništvo v Sloveniji se je začelo z ustanovitvijo prve inkorporirane domače banke, tj. Ljubljanske kreditne banke (Ljubljana 1900). (Štiblar 2010, 25)Nato je sledila Jadranska banka (Trst 1905) in Illirska banka (Ljubljana 1916). Vse tri banke so bile delniške družbe in univerzalne banke, ki so zagotavljale tako kratkoročne komercialne kredite kot tudi sredstva za dolgoročno korporativno financiranje. (Štiblar 2010, 25)

Obdobje po drugi svetovni vojni bančništvu ni bila naklonjeno, razdelimo pa ga lahko na naslednja podobdobja (Štiblar 2010, 29):

- *obdobje administrativnega sistema (1945–1952),*
- *obdobje prve decentralizacije (1953–1965),*
- *obdobje druge decentralizacije (1966–1971),*
- *obdobje ustavnih amandmajev iz leta 1971 (1972–1976),*
- *obdobje zakona o združenem delu (1977–1983),*
- *obdobje zaostritve gospodarskih in mednarodnih odnosov (1986–1989),*
- *bančna reforma iz leta 1989. (Štiblar 2010, 29)*

Kot Štiblar zapisuje v svoji knjigi Bančništvo kot hrbtenica samostojne Slovenije, je v prvih letih po drugi svetovni vojni nova oblast v Jugoslaviji centralizirala finančno poslovanje v eno

samo centralno banko s sedežem v Beogradu in s podružnicami po celi državi, ki pa so bile samo servisi centralni banki.(povzeto po Zemljič 2011)

Po omilitvi centralizacije so začele predvsem okrog Ljubljanske banke (LB) nastajati močne slovenske poslovne banke. Ljubljanska banka je uspešno podpirala razvoj slovenskega gospodarstva in razvito bančništvo je omogočilo, da je bila Slovenija po standardu pred ostalimi federalnimi enotami.(Štiblar 2010, 28–30) Poleg Beobanke in Jugoslovanske investicijske banke je imela edino Ljubljanska banka podružnice po vsej nekdanji Socialistični federativni republiki Jugoslaviji (SFRJ) in je zelo podpirala zunanjo trgovino, kjer je bila Slovenija posrednik za celotno nekdanjo SFRJ. (povzeto po Zemljič 2011)

Leto 1989 je bilo pomembna prelomnica tudi na bančnem področju. Tega leta je namreč zadnja jugoslovanska vlada pod vodstvom Anteja Markovića začela s korenitimi gospodarskimi reformami. Sprejetih je bilo tudi nekaj pomembnih zakonov, ki so vplivali na delovanje bančnega sektorja:

- Zakon o bankah in drugih finančnih organizacijah (Ur. l. SFRJ, št. 10/89, dne 17. 2. 1989),
- Zakon o sanaciji, stečaju in likvidaciji bank in drugih finančnih organizacij (Ur. l. SFRJ, št. 84/89, dne 22. 12. 1989),
- Zakon o agenciji federacije za zavarovanje depozitov in sanacijo bank (Ur. l. SFRJ, št. 84/89, dne 22. 12. 1989)
- Zakon o zagotavljanju sredstev za ustanovitev in delo Agencije federacije za zavarovanje depozitov in sanacijo bank. (Ur. l. SFRJ, št. 84/89, dne 22. 12. 1989)

Od začetka devetdesetih let so se v slovenskem gospodarstvu zgodile velike spremembe, ki so bile posledica tranzicije iz socialistične samoupravne ureditve v tržno kapitalistično gospodarstvo. Te spremembe so imele velik vpliv predvsem na »stare« banke, ki so bile do takrat v lasti podjetij. Pred osamosvojitvijo oziroma v »viharnih letih« 1989–1991 je na Slovenskem ozemlju nastalo 13 samostojnih domačih bank, prav tako pa so bile ustanovljene tri tuje banke. (povzeto po Zemljič 2014)

Ob osamosvojitvi je bilo v Sloveniji 26 bank, to število pa je do leta 1994, ko je doseglo maksimum, naraslo na 33. Ob koncu leta je število bank začelo padati. Štiblar v monografiji

podrobno opisuje razvoj bančnega sektorja po letih in po različnih kazalnikih. (povzeto po Zemljič 2014)

# 6 E-bančništvo

Namen bank pri uvajanju e-bančništva lepo ponazori naslednji citat: *»S pojmom elektronska banka lahko opredelimo način opravljanja bančnih storitev, ki jih lahko kot bančni komitent opravite neposredno s svojega delovnega mesta ali od doma, brez neposredne pomoči bančnega uslužbenca, in to kadarkoli, 24 ur na dan, 365 dni v letu.«*(Kadivec v Malenšek 2002, 9).

Tako so banke začele razvijati e-bančništvo, s katerimi je mogoče opravljati transakcije med podjetji prek interneta oziroma lahko fizične in pravne osebe opravljajo bančno poslovanje, ne da bi morale biti fizično prisotne v banki.

## 6.1 Opredelitev e-bančništva

Elektronsko bančništvo je krovni izraz za proces, s katerim lahko stranka opravlja bančne transakcije v elektronski obliki brez obiska institucije. Naslednji izrazi se nanašajo na eno ali drugo obliko elektronskega bančništva: bančništvo osebnega računalnika (PC), spletno bančništvo, virtualna bančništva, spletno bančništvo, domače bančništvo, elektronsko bančništvo z oddaljenim dostopom in telefonsko bančništvo. PC-bančništvo in internetno ali spletno bančništvo, so najbolj pogosto uporabljene oznake. Opozoriti pa je treba, da se izrazi, uporabljeni za opis različnih vrst elektronskega bančništva, pogosto uporabljajo izmenično. (povzeto po Richard Insley, Hussam Al-Abed in Trent Fleming, BOL Gurus 2014)

S pojmom elektronske banke oziroma e-bančništva torej opredeljujemo način ponudbe in uporabe bančnih storitev, do katerih ima posameznik, ki ima aktivirano storitev in je komitent banke, pri kateri je izbral storitev e-bančništvo, 24 ur na dan skozi vse leto dostop prek oddaljenega terminala na podlagi telekomunikacijskih vodov. (povzeto po Halcom 2009, 12)

Elektronizacija bančnega poslovanja in informacij sega še v čas pred internetom. Kot sem omenila v prvem odstavku, se za e-bančništvo uporablja tudi termin telefonsko bančništvo.

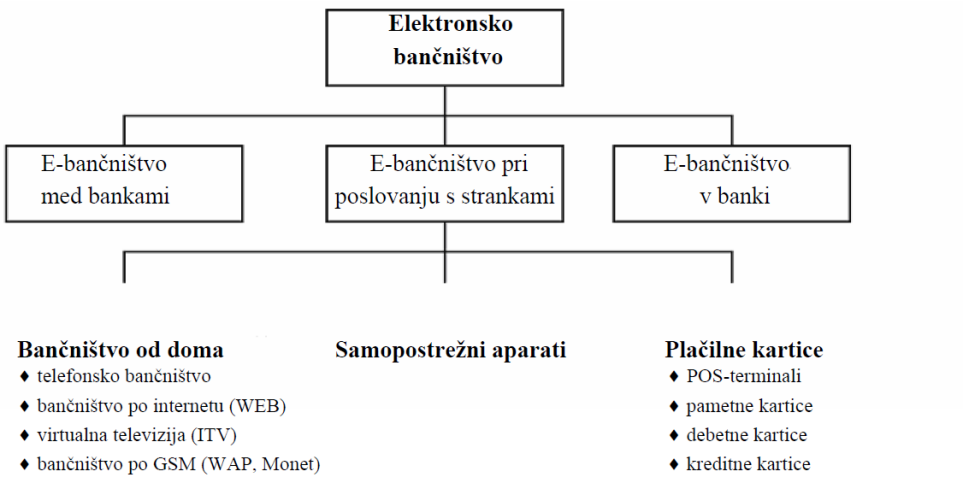
»Telefonske bančne usluge so bile prva oblika elektronskega poslovanja, pozneje pa so nekatere banke razvile lasten programski paket, s katerim je mogoče računalnik priključiti neposredno na bančni sistem« (Sjekloča v Drakulič 2013, 2).

Danes vidimo, da elektronsko bančništvo vedno bolj nadomešča osebno poslovanje z banko. Opazno je tudi, da mlajše generacije – a tudi številni pripadniki srednje generacije – vse več poslujejo z bančnimi karticami in manj z gotovino. Ena od opaznih posledic je, da gotovinsko poslovanje iz dneva v dan izgublja svoj prvotni pomen. Elektronsko bančništvo omogoča optimizacijo distribucije bančnih storitev (Grozdnik in Lindič v Drakulič 2013, 2).

## 6.2 Značilnosti e-bančništva

Kaj naj bi nam torej e-bančništvo zagotavljalo? Predvsem to, da je nam omogočeno upravljanje s prilivi in odlivi na daljavo, da nam ni potrebno stati v vrsti v banki in dolge ure čakati za dvig denarja ali plačilo položnice. V raznih nakupovalnih sferah velja rek: »*kupec je car oziroma stranka ima vedno prav*«, enako pa velja tudi za banke. Banke želijo strankam predvsem omogočiti zadovoljstvo in uresničitev njihovih želja ter hkrati znižati stroške poslovanja. Tako pridemo do bistvenih razlogov, ki so bili opisani čisto na začetku tega odstavka.

**Slika 6.1: Shema elektronskega bančništva**




Vir: Miš- Svoljšak (1999)

Storitve, ki nam jih omogoča e-bančništvo, so:

- opravljanje posameznih plačil,
- informacije o stanjih na računih, ki jih komitent odpre pri banki,
- pregled opravljenih transakcij na posameznem računu,
- pregled opravljenih plačil s kreditno kartico,
- prenos sredstev z enega računa na drugega,
- plačilo trajnikov.

## 6.3 Prednosti in slabosti e-bančništva

Kot vsaka storitev ima tudi e-bančništvo svoje prednosti in slabosti. V tem delu se bom osredotočila predvsem na lastnosti, ki gredo v korist komitentom.

Prednosti e-bančništva so:

- enostavno plačevanje položnic,
- pregled prometa na tekočem računu,
- izdelava predlog (plačila, ki jih izvajamo vsak mesec, si lahko shranimo in jih prikličemo pred plačevanjem, ob tem pa moramo samo navesti pravilen sklic in znesek oziroma ju spremeniti),
- plačila lahko zabeležimo vnaprej (prednastavitev plačila določenega računa, npr. v 15. v mesecu),
- omogočeni so interni prenosi med računi iste banke brez plačevanja provizije.

Slabosti e-bančništva so:

- e-banke imajo enak delovni čas kot prave banke (vnosi plačil pozno zvečer ali čez vikend se izvedejo šele naslednji delovni dan),
- ni pisnih potrdil (so plačljiva; mesečni izpiski niso plačljivi, vsa nadaljnja potrdila so),
- ni osebnega stika (če pride do problemov, je potrebno kontaktirati njihovo pomoč ali pa za določene razlage osebno obiskati poslovalnico),
- nimajo vsi dostopa (za dostop je potreben računalnik, internet – tisti, ki tega nimajo, ne morejo dostopati do storitev, pogosto so to starejši ljudje)

- možnost zlorab,
- problem varnosti.

# 7 Pregled e-bančništva v Sloveniji

Leta 2009 je RIS izvedel raziskavo, ki je vključevala samo e-bančništvo; raziskava je pokazala, da je v zadnjem desetletju e-bančništvo postalo zelo dobičkonosna spletna storitev. Že v letu 2004 so napovedali, da se bo število uporabnikov povečalo za dvakrat.

> *V štirih letih se je torej število uporabnikov podvojilo, z 10 % na 21 % v populaciji 10–75 let, kar pomeni povprečno 15-odstotno letno rast. Po zadnjih ocenah RIS-a (2008) je v Sloveniji več kot milijon rednih uporabnikov interneta (v populaciji 10–75 let), od tega jih 312.000 uporablja storitve e-bančništva. O uporabi razmišlja še 230.000 uporabnikov (leta 2004 264.000), od tega jih 87.000 namerava začeti z uporabo v 6 mesecih (leta 2004 113.000). V primerjavi z letom 2004 se je povečalo predvsem število uporabnikov interneta, ki ne uporabljajo e-bančništva in o tem tudi ne razmišljajo (RIS 2004: 336.000, RIS 2008: 535.000).* (RIS 2009)

Podatki so vzeti iz poročila o e-bančništvu iz leta 2009, ki ga je naredil RIS. (RIS 2009)

**Tabela 7.1:Pregled ponudnikov e-bančništva v Sloveniji za fizične in pravne osebe**

| Banka | storitev za fizične osebe | storitev za pravne osebe |
|---|---|---|
| **ABANKA VIPA, d. d.** | Abanet | Abacom |
| **BANKA CELJE, d. d.** | NLB klik | E-banka Banka Celje |
| **BANKA KOPER, d. d.** | I-net Banka | Poslovna I-net Banka |
| **BANKA SPARKASSE, d. d.** | Net.Stik | |
| **DEŽELNA BANKA SLOVENIJE, d. d.** | DBS NET | DBS NET |
| **FACTOR BANKA, d. d.** | ne | ebanka |
| **GORENJSKA BANKA, d. d., KRANJ** | Link | Link + |
| **HYPO ALPE-ADRIA-BANK, d. d.** | HYPOnet | HYPOnet |
| **NOVA KREDITNA BANKA MARIBOR, d. d.** | Bank@Net | Poslovni Bank@Net |
| **NOVA LJUBLJANSKA BANKA, d. d., LJUBLJANA** | Klik NLB | Proklik NLB, Proklik + |
| **POŠTNA BANKA SLOVENIJE, d. d. – bančna** | PBS.net | |
| **PROBANKA, d. d.** | Prosplet | ProspletPlus |
| **RAIFFEISEN BANKA, d. d.** | ne | EKB |
| **SBERBANK BANKA, d. d.** | Sberbank Spletne banke | Sberbank Poslovni Splet |
| **SKB BANKA, d. d., LJUBLJANA** | SKBNet | Pro SKBNet |
| **SLOVENSKA INVESTICIJSKA BANKA, d. d. – v likvidaciji** | ne | SIBnet |
| **SID –SLOVENSKA IZVOZNA IN RAZVOJNA BANKA, d. d., LJUBLJANA** | ne | ne |
| **UNICREDIT BANKA SLOVENIJA, d. d.** | OnlineB@nka | E-Bank |

Vir: Banka Slovenije (2014)

Kot je razvidno iz tabele, so banke lepo razvile storitve e-bančništva in jih razdelile na fizične in pravne osebe.

## 7.1 Primerjava bančnih ponudb na svetovnem spletu v Sloveniji

V tem poglavju bom naredila primerjavo bančnih ponudnikov na svetovnem spletu v Sloveniji. Izbrala sem štiri večje banke, ki ponujajo storitve za fizične in pravne osebe na področju e-bančništva, in sicer Nova Ljubljanska banka, SKB, A banka Vipa in Banka Austria, sedaj imenovana Unicredit banka, ki je sicer v lasti tujcev, vendar ima v Sloveniji velik tržni delež. V tej primerjavi bo razvidno, katera orodja banke uporabljajo za dostop do e-bančništva in njegovo zaščito.

### 7.1.1 Nova Ljubljanska banka

Skupina NLB je največja slovenska bančno-finančna skupina, ki ponuja široko paleto bančnih in drugih finančnih storitev in zagotavlja popolno servisiranje finančnih potreb svojih strank.

Na dan 31. decembra 2012 je Skupina NLB združevala 45 bank in gospodarskih družb. Bančništvo je najpomembnejša dejavnost Skupine NLB, sicer pa skupina ponuja tudi druge finančne storitve, kot so zavarovanje, upravljanje premoženja, najem (lizing), odkup dolgov (faktoring) in oblika financiranja izvoza (forfetiranje), pravijo na spletni strani NLB.

Skupina NLB trenutno deluje v 13 državah, pokriva 14 trgov in obsega:

- 10 bank in 1 podružnico v tujini,
- 7 lizinških družb,
- 9 družb faktoringa in forfetiranja,
- 3 zavarovalnice,
- 1 družbo za upravljanje in
- 16 podjetij, ki opravljajo druge dejavnosti.

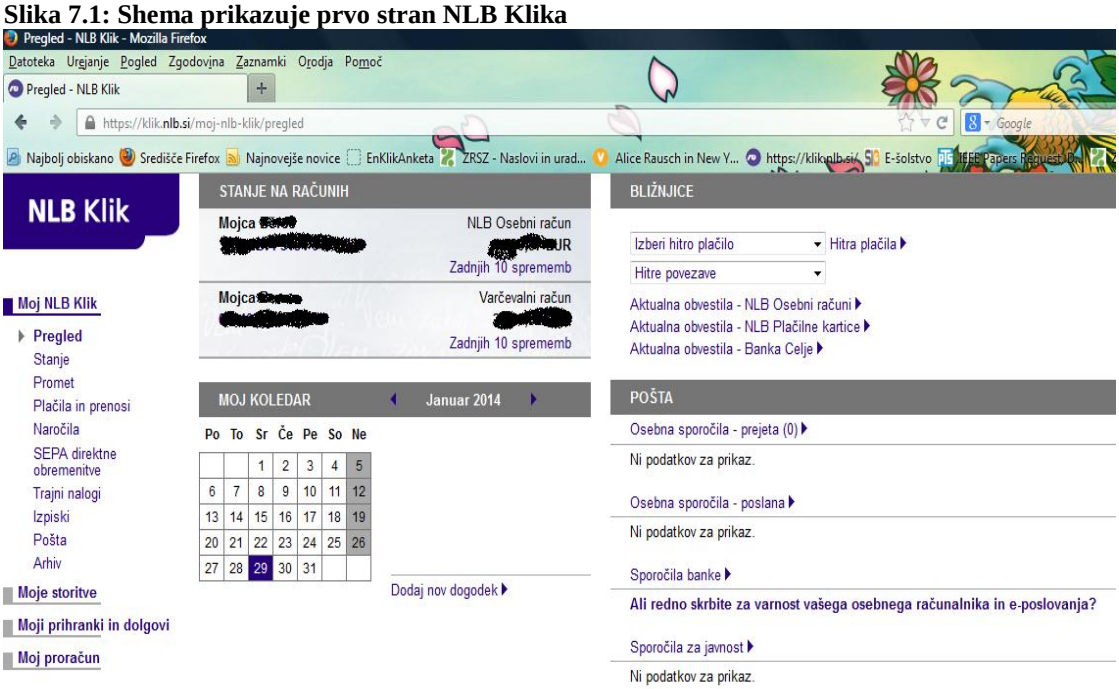
NLB ponuja e-bančništvo za dve platformi, in sicer:

- za fizične osebe : NLB Klik,

- za pravne osebe: Proklik plus NLB.[20]

V nadaljevanju bodo predstavljeni vmesnik in storitve, ki jih NLB ponuja fizičnim osebam za dostop do e-bančništva.

**Slika 7.1: Shema prikazuje prvo stran NLB Klika**




Vir: Lastni vir

Varnostni dostopi do elektronske banke za prebivalstvo pri NLB so:

- dostop prek https,
- kvalificirano digitalno potrdilo AC NLB,
- dvonivojsko geslo,
- osebno sporočilo, za katerega je priporočljivo, da je nastavljeno,
- sporočilo SMS,
- po novem tudi dostop do elektronskega bančništva brez certifikata in prek mobilnega telefona.

Storitve, ki jih ponuja e-bančništvo v NLB Kliku in so zapisane na njihovi spletni strani, so povzete v naslednjih alinejah:

[20] Proklik – uporablja FAT klienta, ki se povezuje na banko (omogoča celo dial-up modemski dostop – kot »varnosti« feature, poleg dostopa preko interneta in zahteva čitalec kartic – ker je privatni certifikat na Smartcartu)

- *vpogled v stanje in promet na lastnem osebnem računu in osebnih računih, za katere ste pooblaščeni,*
- *plačevanje z nalogi UPN doma in v območju SEPA, prenos sredstev med računi in naročilo plačila v tuji valuti,*
- *vpogled v stanje vezanih depozitov, imetniških varčevanj, varčevalnih računov in kreditov,*
- *prejem, plačevanje in naročanje E-računov,*
- *pregled e-izpiskov,*
- *odpiranje, spreminjanje in ukinjanje trajnih nalogov,*
- *sklenitev depozita, pogodbe o varčevanju ali odprtje varčevalnega računa (stalen pregled nad stanjem in drugimi podrobnostmi),*
- *pregled podrobnosti in prometa na imetniških plačilnih karticah,*
- *plačilna kartica NLB – naročanje, sprememba limita,*
- *naročilo vklopa varnostnega SMS-sporočila,*
- *trgovanje z vrednostnimi papirji na Ljubljanski borzi in vpogled v stanje na trgovalnih računih vrednostnih papirjev,*
- *pregled prometa in podrobnosti vzajemnih skladov družbe NLB Skladi,*
- *pregled seznama uporabnikovih zavarovalnih polic življenjske zavarovalnice NLB Vita, d. d., prikaz podrobnosti teh polic in vplačila,*
- *v poglavju Moj proračun urejanje in spremljanje prejemkov in izdatkov,*
- *v poglavju Moji prihranki in dolgovi spremljanje lastnih sredstev in dolgov,*
- *plačevanje nakupov v spletnih trgovinah,*
- *oddaja zahtevka za nakazilo in prevzem gotovine prek sistema Western Union,*
- *naročanje dviga večjih zneskov gotovine,*
- *naročanje na prejem SMS-sporočil o stanju na računih, vstopu v NLB Klik, zapadlosti depozita/varčevanja, zapadlosti limita,*
- *pošiljanje in prejemanje sporočil banke.* (NLB Banka)

### 7.1.2 SKB banka

SKB banka je del skupine Société Générale, ene največjih bančnih skupin v evrskem območju že od leta 1965 naprej.

Njene lastnosti so:

- deležna je podpore pri prenosu sodobnih tehnologij,
- odpiranje novih poslovnih priložnosti in dostopnosti virov financiranja,
- slovenskim strankam nudi raznovrstno paleto visoko konkurenčnih produktov in kakovostnih storitev v okviru mednarodne mreže,
- previdna obravnava tveganj,
- hkrati se osredotoča na učinkovit odziv na pričakovanja strank in tržne spremembe.

SKB ponuja e-bančništvo za dve platformi, in sicer:

- za fizične osebe : SKBNet,
- za pravne osebe: PRO SKBNet.

V nadaljevanju bo predstavljen vmesnik in storitve, ki jih SKB ponuja fizičnim osebam za dostop do e-bančništva.

**Slika 7.2: Slika prikazuje prvo stran SKB net**


Vir: Lastni vir

Varnostni dostopi do elektronske banke za prebivalstvo pri SKB so:

- dostop prek https,
- **identifikacijska kartica** (generira enkratno časovno omejeno varnostno geslo za dostop),
- **posebno geslo** (generirate ga pred prvo uporabo SKB s pomočjo identifikacijske kartice),
- **varnostno geslo** (se generira na enak način kot osebno geslo, prispeva pa k boljši varnosti),

Storitve, ki jih ponuja e-bančništvo v SKBNet in so zapisane na njihovi spletni strani na povezavi Splošni pogoji za uporabo sodobnih bančnih poti za fizične osebe, so povzete v naslednjih alinejah:

- *pregled stanja, prometa, izpiskov in drugih informacij na računih, odprtih pri SKB (osebni, varčevalni, kartični),*
- *cenejša plačila za domače plačilne transakcije kot v bančnih poslovalnicah z možnostjo določitve poznejšega datuma izvedbe plačila,*
- *brezplačni prenosi sredstev med osebnimi računi različnih oseb, odprtimi pri SKB*

*z možnostjo nastavitve datuma v prihodnosti,*

- *brezplačni prenosi sredstev med osebnimi računi in varčevalnimi računi, ki jih ima stranka odprte pri SKB,*
- *prenosi deviznih sredstev na skrbniški in lastni račun pri SKB ali drugi banki v Sloveniji,*
- *odpiranje, pregled in zapiranje trajnih nalogov,*
- *storitev e-račun (prejem e-računov),*
- *pregled transakcij, opravljenih prek SKB NET in SKB TEL (telefonsko bančništvo),*
- *sklepanje vezav ter pregled sklenjenih vezav v evrih in tujih valutah,*
- *oddaja naročil oziroma vlog za:*
  - *odobritev izrednega limita na računu,*
  - *povečanje limita za dvig gotovine na bankomatu,*
  - *napoved dviga večje vsote gotovine,*
  - *odprtje varčevalnega računa,*
  - *MasterCard kartico in VISA kartico,*
  - *spremembo višine limita porabe ali okvirnega kredita na kartičnem računu,*
  - *odobritev hitrega kredita,*
- *menjava valut,*
- *informacije o sklenjenih kreditnih poslih,*
- *varnostne nastavitve:*
  - *nastavitev osebnega seznama prejemnikov,*
  - *nastavitev skupnega dnevnega zneska plačil in najvišjega zneska posameznega plačila,*
- *hitro spreminjaje uporabnikovih kontaktnih podatkov,*
- *varno pošiljanje sporočil v banko. (SKB Banka)*

### 7.1.3 A banka Vipa

Abanka je začela delovati že v letu 1955 kot podružnica Jugoslovanske banke za zunanjo trgovino. Leta 1977, torej po več kot dvajsetih letih poslovanja, se je podružnica preimenovala v Jugobanko – temeljno banko Ljubljane. Decembra 1989 so se na podlagi sklepa zbora banke preoblikovali v Abanko, delniško družbo, in izstopili iz sistema Jugobanke. Že takrat je na ozemlju Slovenije delovalo 26 njihovih poslovnih enot. Kot čisto samostojna banka so resnično začeli delovati leta 1990, in sicer pod imenom Abanka, d. d., Ljubljana. Leta 2002 so se združili še z Banko Vipa, d. d., in se preimenovali v Abanka Vipa, d. d. (Povzeto po Abanka Vipa 2014)

Njihove lastnosti so:

- pomemben člen v mednarodni menjavi,
- usposobljeni so za vse vrste poslov komercialnega bančništva v domačih in mednarodnih plačilih ter drugih finančnih transakcijah,
- povečanje kapitalske moči za razvoj in stabilno poslovanje banke, vključno z možnostjo povezovanja z drugimi bankami,
- okrepitev poslovanja s prebivalstvom ter z malimi in srednjimi podjetji,
- stroškovna in procesna učinkovitost.

Abanka Vipa ponuja e-bančništvo za dve platformi, in sicer:

- za fizične osebe : Abanet,
- za pravne osebe: Abacom.

V nadaljevanju bo predstavljen vmesnik in storitve, ki jih Abanka Vipa ponuja fizičnim osebam za dostop do e-bančništva.

**Slika 7.3: Slika prikazuje prvo stran Abanet**


Vir: Lastni vir

Varnostni dostopi do elektronske banke za prebivalstvo pri A banka Vipa so:

- dostop prek https,
- digitalni certifikat (SIGEN-Ca, Poštarca ali Halcom),
- geslo.

Storitve, ki jih ponuja e-bančništvo v Abanet in so zapisane na njihovi spletni strani so povzete v naslednjih alinejah:

- prihranek časa in denarja,
- preprosto, hitro in učinkovito finančno poslovanje, 24 ur na dan, vse dni v letu,
- izvajanje domačih in čezmejnih plačil ter prenosov sredstev z nižjo bančno provizijo kakor na bančnem okencu,
- možnost oddaje naročila in digitalno sklepanje pogodbe za: kratkoročne in dolgoročne depozite, potrdilo o izvršenem plačilnem nalogu, e-računi, varčevalni račun, pooblastilo za prenos sredstev na varčevalni račun, mobilna storitev Abasms, storitev Oblikuj si kartico! in plačilo v tujino,

- možnost prijave/odjave prejemanja e-računov v spletno banko Abanet pri izbranih izdajateljih računov,
- možnost nakupov v izbranih spletnih trgovinah.

### 7.1.4 Unicredit Banka Slovenije (Bank Austria)

Banka Austria je bila ustanovljena leta 1991, in sicer pod imenom Länder Bank, d. d., Ljubljana[21]. Leta 1992 so se preimenovali v Bank Austria, d. d., Ljubljana. Od leta 1992 je avstrijski Creditanstalt prevzel Novo banko, d. d., Ljubljana in jo poimenoval Creditanstalt – Nova banka, d. d., Ljubljana, ki se je potem leta 1994 spet preimenovala v Banka Creditanstalt, d. d. Leta 2001 je postala glavna banka Austria Creditanstalt, AG, Dunaj, del HVB München in s tem je tudi Bank Austria Creditanstalt, d. d., Ljubljana, postala članica skupine HVB Group. Leta 2005 je HVB München prevzela UniCredit in tudi Bank Austria Creditanstalt, d. d., Ljubljana, je tako postala članica skupine UniCredit. Dokončno ime je Banka Austria, d. d., Ljubljana dobila leta 2007, in sicer se je preimenovala v UniCredit Banka Slovenija, d. d. (povzeto po Unicredit Banka Slovenija o nas, 2014)

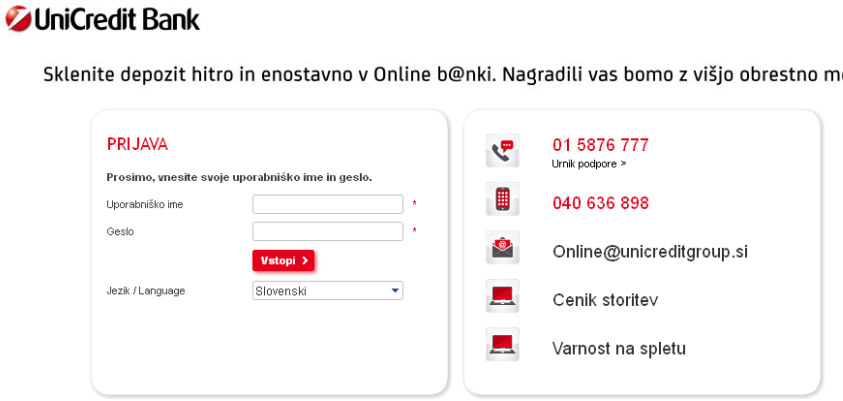
Unicredit Banka Slovenija ponuja e-bančništvo za dve platformi, in sicer:

- za fizične osebe : OnlineB@nka,
- za pravne osebe: E-Bank.

V nadaljevanju bodo predstavljen vmesnik in storitve, ki jih Unicredit Banka Slovenije ponuja fizičnim osebam za dostop do e-bančništva.

[21] Avstrijska Länder Bank in Slovenijales, d. d., Ljubljana sta ustanovila mešano družbo.

**Slika 7.4: Slika prikazuje prvo stran OnlineB@nka**




Vir: UniCredit Bank - OnlineB@nka (2014)

Varnostni dostopi do elektronske banke za prebivalstvo pri A banka Vipa so:

- dostop prek https,
- uporabniško ime,
- geslo,
- žetonček (za mobilno uporabo).

Storitve, ki jih ponuja e-bančništvo v OnlineB@nka in so zapisane na njihovi spletni strani so povzete v naslednjih alinejah:

- *domači – standardni nalog (univerzalni plačilni nalog – UPN), nujni nalogi, odprtje trajnega naloga, sprememba trajnega naloga, izvedba trajnega naloga, izbris trajnega naloga,*
- *direktna obremenitev,*
- *plačilo SEPA, čezmejno plačilo,*
- *mednarodni plačilni promet,*
- *zavrnitev naloga zaradi nezadostnega stanja na računu ali napak v nalogu,*
- *pisno potrdilo o izvršitvi plačilnega naloga,*
- *pristopnina k storitvam elektronskega spletnega in mobilnega bančništva,*
- *mesečni strošek vzdrževanja storitev spletnega in mobilnega bančništva z uporabo sms-žetona,*
- *mesečni strošek vzdrževanja storitev spletnega in mobilnega bančništva z uporabo fizičnega ali m-žetona,*
- *nadomestni žeton za uporabo spletnega bančništva Online banka,*

- *blokada spletne in mobilne banke,*
- *ponovna aktivacija m-žetona v primeru zaklepa zaradi napačnega vnosa gesla PIN,*
- *ponovna aktivacija Mobilne banke GO! v primeru zaklepa osebnega gesla PIN,*
- *M-Online banka (mobilni dostop do Online banke).* (Unicredit Banka)

Kot sklep poglavja si oglejmo še tabelarični povzetek varovanja dostopa do elektronskega bančništva pri zgoraj obravnavanih bankah.

**Tabela 7.2: Povzetek opisanih varnostnih dostopov**

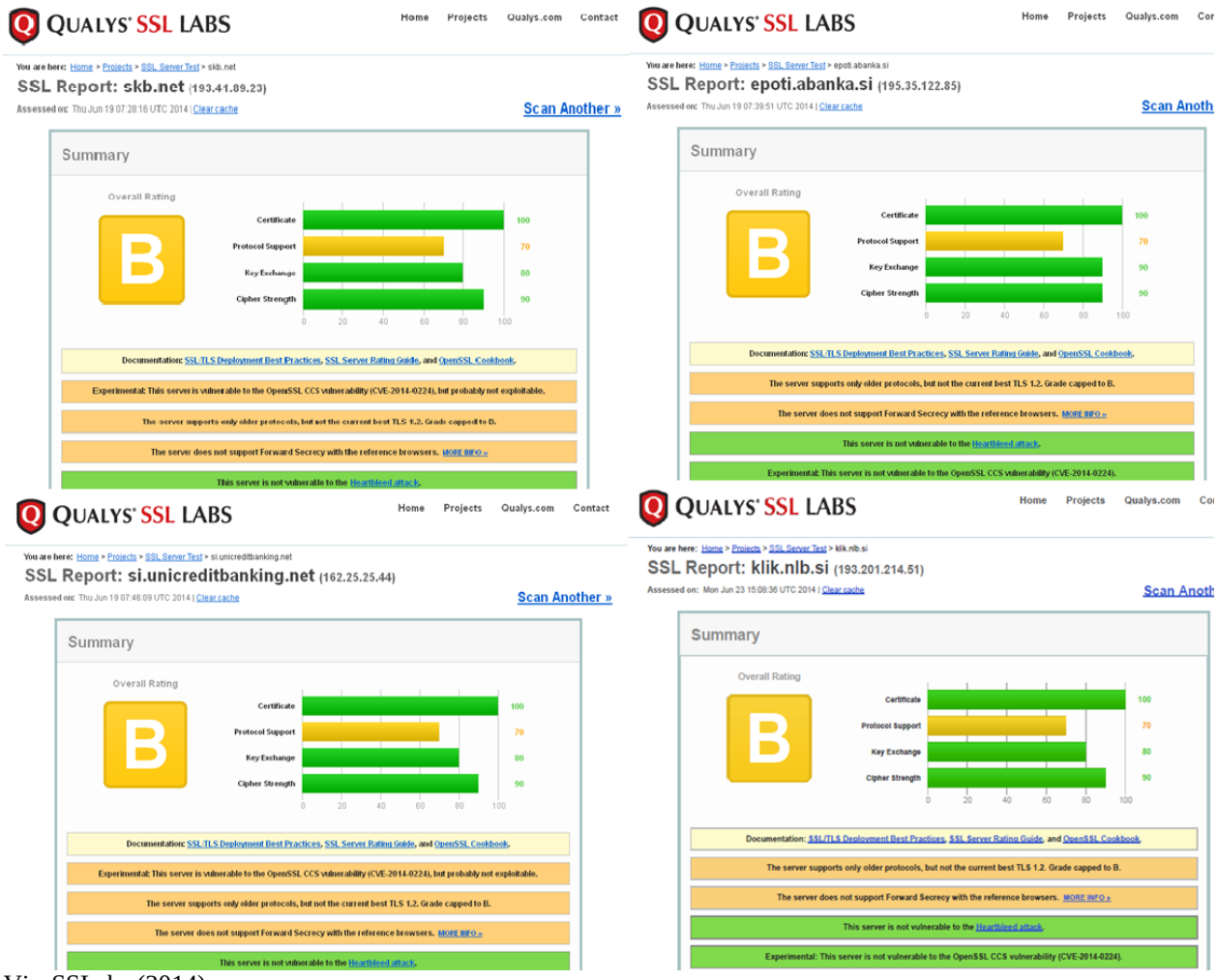
| Varnostni dostop / Banka | Spletna stran | Certifikat oziroma dostop | Uporabniško ime | geslo | drugo |
|---|---|---|---|---|---|
| NLB | https | certifikat | da | da | osebno sporočilo |
| SKB | https | identifikacijska kartica | da | da | -posebno geslo,<br>-varnostno geslo |
| Unicredit bank (Banka Austria) | https | certifikat | da | da | žetonček (za mobilno uporabo) |
| A banka Vipa | https | certifikat | da | da | / |

VIR: Lastni vir

Vse banke imajo v brskalnikih dostop prek povezave https, kar pomeni zaščiten dostop do strani. Tri od preučevanih bank uporabljajo za avtentikacijo certifikate, le ena uporablja identifikacijsko kartico. Pri vseh preučevanih bankah je potrebno vpisati uporabniško ime in geslo. Poleg tega imajo vzpostavljene še dodatne lastne varnostne sisteme, da je fizična stranka še dodatno zavarovana pred zlorabo podatkov pri vstopanju v elektronsko bančništvo.

Kako varni so torej dostopi do elektronskega bančništva? Testiranje za banke, ki sem jih v magistrskem delu preučevala, je bilo opravljeno prek strani sslabs.

**Slika 7.5: Prikaz testiranja preko SSLLabs za vse štiri banke**




Vir: SSLabs (2014)

Pregled varnosti vseh štirih obravnavanih bank je pokazal, da so vse podprte s certifikati (100 %) in vse imajo t. i. protocol support pri 70 %, kar pomeni, da uporabljajo protokol TLS 1.0., ne pa tudi TLS 1.1 in TLS 1.2., ter starejši kriptografski SSL 3[22], razen Unicredit bank, ki uporablja tudi še SSL 2[23].

Strežniki so pri vseh bankah nastavljeni tako, da ne omogočajo t. i. ponovnega pogajanja za vzpostavitev seje SSL s strani odjemalca (t. i. *client-initiated session renegotiation*).

[22] »/.../ tega je celo priporočljivo izključiti,« pravi Matej Kovačič v svoji objavi na spletnem dnevniku Pravokator. *(Pravokator 2014)*

[23] Vendar z opombo, da je protokol podprt, a pri cenejših verzijah je onesposobljen. *(Pravokator 2014)*

Ravno tako strežniki niso nastavljeni, da bi onemogočali napade BEAST (*Browser Exploit Against SSL/TLS*).[24]

Ko gre za povišano stopnjo zaupnosti, ki jo v angleščini poimenujejo poimenovanje *perfect forward security* oz. *perfect forward secrecy*[25], Abanka in NLB na strežnikih te funkcije nimata nastavljene. Banki SKB in Unicredit imata podporo za to funkcijo samo v določenih brskalnikih, sta pa ranljivi za napade MITM (OpenSSL CCS vuln. (CVE-2014-0224) )

Vsa spletišča so bila s strani SSL Labs označena z oceno B, kar pomeni, da imajo 2048-bitni ključ RSA, zaradi česar se samodejno uvrstijo pod oceno B (pri čemer je A je najvišja ocena). Glede na te rezultate lahko rečemo, da je varnost bank zanesljiva, ne moremo pa trditi, da so varne pred zlorabami. Ko gre za ranljivost Heartbleed (tj. Ranljivost programske knjižnice OpenSSL CCS), je samo pri Abanki potrjeno, da je odpravljena, pri ostalih treh bankah pa ranljivost obstaja, vendar naj ne bi bilo nevarosti za zlorabe. Glede na to, da je odsotnost *Heartbleed* ranljivosti ena redkih ter OpenSSL CCS vuln.,vendar je za zadnje napisano, samo pri Abanki ter potrjeno, da ni ranljiv, pri ostalih pa je zapisano, da je vendar, tega se ne izkorišča.

[24] Matej Kovačič v zapisu na spletnem dnevniku o napadu BEAST pravi: »/.../ *napad sta leta 2011 prikazala varnostna raziskovalca Thai Duong in Juliano Rizzoplet, napadalcu pa omogoča izvedbo kriptoanalize (dešifriranja šifriranih podatkov) ter posledično rekonstrukcijo sejnega kriptografskega ključa. S tem podatkom nato lahko napadalec npr. ukrade spletni piškotek žrtve ter izvede krajo identitete itd.« (*Pravokator 2014)

[25] »*Gre za varnostno nastavitev, ki omogoča samodejno spreminjanje šifrirnih ključev vsako novo spletno sejo oz. na določeno časovno obdobje. Če napadalec uspe razbiti enega izmed šifrirnih ključev, bo lahko dešifriral le spletni promet, ki je bil šifriran v dani seji, za vse ostale seje pa bo moral izvesti ponoven (navadno zamuden) napad. S pomočjo tega mehanizma upravljavec spletnega strežnika poskrbi, da je škoda ob morebitnem uspešnem napadu čim manjša,«* je zapisal Matej Kovačič. *(Pravokator 2014)*

# 8 Intervju s podjetjem Halcomom ( Denis Tomaševič)

»*Vdorov v elektronske banke ni, so zlorabe.« (Denis Tomaševič)*

Intervju je potekal v Ljubljani, na sedežu Halcoma, dne 21. februarja 2014, od pol petih popoldan do šestih zvečer.

Podjetje Halcom je bilo ustanovljeno leta 1992. Vrsto let so razvijali svoje storitve in prišli so do rešitev, ki so na področju elektronskega bančništva, svetovanja in ponujanja drugih storitev ugodne tako za pravne kot fizične osebe.

Intervju sem izvedla z Denisom Tomaševičem, vodjo IT-sektorja pri Halcomu. Tu dela že od leta 2008. Začel je kot vodja IT-oddelka oziroma področja informacijsko-komunikacijske tehnologije. Sedaj dela kot direktor informatike (CIO) in vodja urada za informacijsko varnost (CISO). Po izobrazbi je univerzitetni diplomirani elektrotehnik.

Intervju z njimi je bil narejen zaradi njihove ponudbe, saj ponujajo rešitve za podjetja in posameznike na področju elektronskega bančništva. V ponudbi Halcoma so programske rešitve za elektronsko banko in elektronsko plačevanje, natančneje: certifikat Halcom CA, elektronsko računalništvo v oblaku (imajo več kot 10 let izkušenj z delovanjem elektronske banke v oblaku. E-banko v oblaku imajo lahko banke na njihovih strežnikih.

Četudi je v računalniškem smislu rešitev enaka, so cilji različni: treba je vedeti, kaj si posamezni uporabnik želi. Sedaj v ospredje postavljajo mobilno banko in mobilno plačevanje, poleg svojih certifikatov in računalništva v oblaku. Mobilna banka in mobilno plačevanje imata čisto drugačen scenarij. Pri mobilni banki upravljaš vse tako kot v elektronski banki, mobilno plačevanje pa pokriva sistem *Moneta*.

Najuspešnejši produkt je seveda elektronsko poslovanje, in sicer je izpostavljena pametna kartica. Pametna kartica je eden od najbolj izpopolnjenih varnostnih mehanizmov, saj ključa ni mogoče odtujiti od kartice – če pa že to uspe, je treba poznati tudi kodo PIN. Prav tako so uspešni na področju mobilnega bančništva, veliko je uporabnikov njihovih certifikatov Halcom CA.

Njihovo varovanje podatkov in izvajanje storitev je usklajeno z načelom in standardi kakovosti **ISO 9001** od 2003 in **ISO 27001** od leta 2010 (varovanje informacij).

G. Tomaševič tudi pravi, da do zlorab pri njih ne prihaja, saj so sodobni hekerji bolj usmerjeni na uporabnike kot pa na banke. Vendar pa so že imeli par poizkusov vdorov, a o tem ne sme razpravljati, ker primeri še niso zaključeni na sodišču.

Za varnost podatkov je torej pri podjetju Halcom poskrbljeno. Zaupa jim več kot 75 bank, od tega jih večina uporablja storitev e-bančništvo v oblaku. Predvsem je bilo izpostavljeno, da je to prednost za majhne banke, saj pri njih pridobijo celotno infrastrukturo, kar se večini pozna pri stroških. Banke so lastniki podatkov in ti podatki so varovani.

# 9 Primeri zlorab v e-bančništvu

## 9.1 SKB banka - phishing napad na komitente SKB banke

21. 8. 2012: Nekateri slovenski uporabniki so prek elektronske pošte prejeli lažno obvestilo SKB banke, ki jih skuša prepričati, naj se prijavijo v sistem elektronskega bančništva zaradi »preverjanja podatkov«. (SI-CERT 2014)

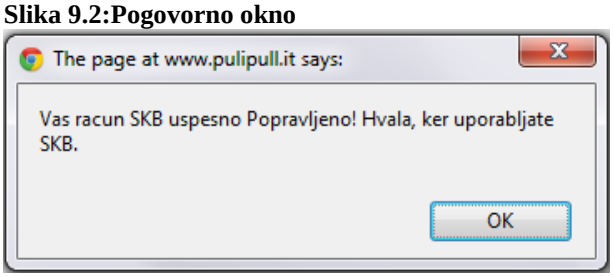
**Slika 9.1:Phising napad na komitente SKB Banke**


Vir: SI-CERT (2014)

Uporabnike na ponujeni povezavi pričaka kopija spletnega mesta banke, ki je namenjena kraji uporabniškega imena in gesla. SKB banka je bila o varnostnem incidentu obveščena in je že sprejela ukrepe za zmanjšanje tveganja svojih komitentov. (povzeto po SI-CERT 2014)

Ob prijavi na lažnem spletnem mestu se je uporabniku prikazalo naslednje pogovorno okno:

**Slika 9.2:Pogovorno okno**




Vir: SI-CERT (2014)

## 9.2 Bančni trojanec, ki krade avtentifikacijske podatke za Klik NLB

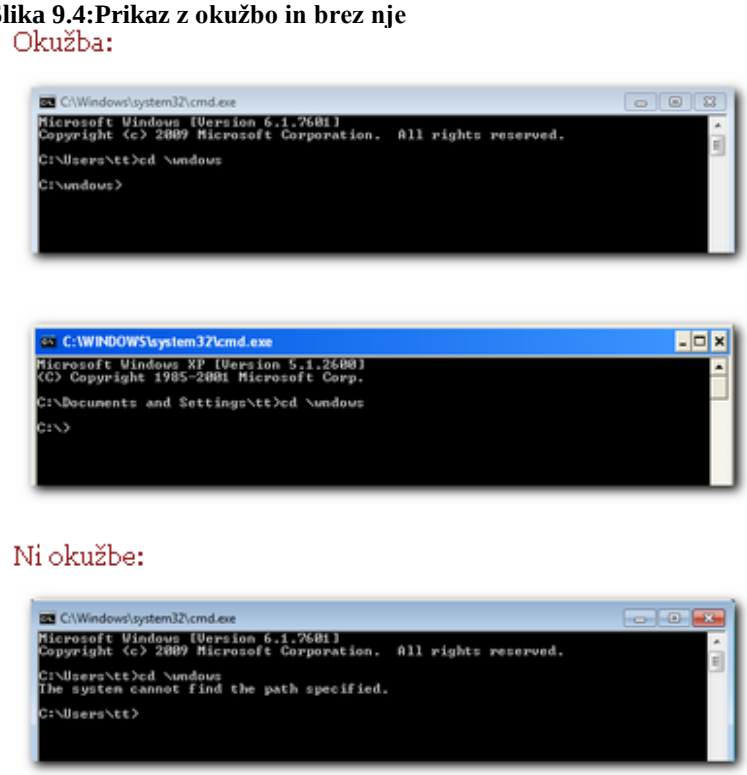
14. 12. 2012: Na SI-CERT so identificirali in analizirali zlonameren program, različico bančnega trojanca Spyeye, ki se po okužbi skrije v sistemu, in ko se uporabnik prijavi v spletno banko Klik NLB, napadalcu pošlje zajete avtentikacijske podatke in digitalni certifikat, od uporabnika pa zahteva tudi vpis celotnega dodatnega gesla. Po njihovih podatkih ni šlo za množično okužbo, ampak zgolj za posamezne primere. (povzeto po SI-CERT 2012-16, 2014)

**Slika 9.3:Bančni trojanec**


Vir: SI-CERT (2014)

Po okužbi se je zlonamerni program skopiral v mapo *c:wndows* in ustvaril zagonski ključ v registru. V določenih sistemih okužbo skrije s t. i. rootkit tehnologijo, tako da niti zagonski ključ niti mapa *c:wndows* z običajnimi orodji nista vidna. Zlonamerno kodo injicira v legitimna procesa explorer.exe in svchost.exe, s čimer še dodatno skrije svojo prisotnost. Odkrijemo jo tako, da preko ukazne vrstice (*START → cmd.exe*) vpišemo ukaz *cd wndows*. (povzeto po SI-CERT 2012-16, 2014)

**Slika 9.4:Prikaz z okužbo in brez nje**




Vir: SI-CERT (2014)

V primeru okužbe vpisani ukaz, ne bo vrnil napake.

## 9.3 Banka Celje in specializirani računalniški bančni virus SpyEye – ZEUS

V septembru 2012 so na območju Slovenije zabeležili porast vdorov v informacijske sisteme uporabnikov spletnega bančništva. Ugotovili so, da so bili vsi računalniki oškodovancev okuženi s specializiranim računalniškim bančnim virusom SpyEye. Šlo je za prenovljeno in posodobljeno verzijo Zeusa, ki je bil v Sloveniji že prisoten, in sicer v letu 2009 do prve polovice leta 2010. In kako storilci dostopajo z Zeusom do oškodovančevega računalnika? Storilci prek elektronske pošte ali katerega drugega komunikacijskega sredstva okužijo oškodovančevo računalnik in mu potem poskušajo odtujiti denar prek spletnega bančništva z uporabo digitalnega certifikata in gesla. (Banka Celje 2014)

## 9.4 Unicredit Bank – kraja denarja prek spleta oziroma kako je mogoče izkoristiti luknjo v spletnem bančništvu (primer Izraelca in Ukrajinca)

20. novembra 2007 je policija prijela prebivalca Izraela, ki si je pri nas odprl dva tekoča računa in je ob pomoči neznanih sodelavcev izkoristil slabo zaščitene računalnike uporabnikov elektronskega bančništva in uspešno praznil njihove račune. Pridobil naj bi okoli 9.000 evrov, od tega pa naj bi si delež prenakazal v domovino.

Mesec dni pred dogodkom z Izraelcem, kot je pisalo v časopisu Dnevnik, je podoben podvig naredil Ukrajinec. Na svoj bančni račun, ki ga je odprl v Sloveniji, si je nakazal zavidljivih 26.000 evrov, denar pa je pozneje pošiljal svojim pajdašem v Rusijo. (povzeto po Dnevnik 2014)

## 9.5 Zlorabe elektronskega bančništva – potek preiskave v praksi (Bojan Ostanek, SKP Ljubljana) [26]

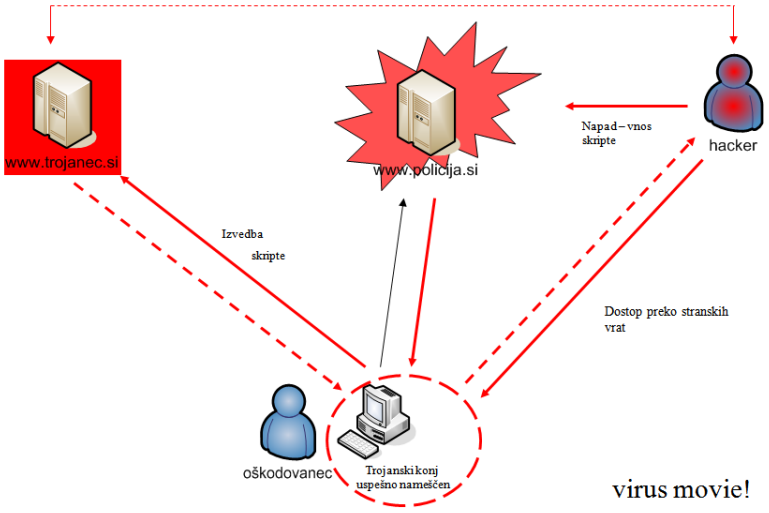
Opis podane prijave:

> *»Dne 26. 08. 2006 A. B. na PP Ljubljana prijavi, da mu je nekdo iz bančnega računa odtujil 700.000,00 SIT. Gotovina je bila ukradena iz njegovega e-bančnega računa tako, da je bila znotraj e-banke preko načina WU Money transfer nakazana osebi C. D. v BIH. Oškodovani A. B. zagotavlja, da prenakazila ni opravil sam, saj tega dne sploh ni uporabljal osebnega računalnika, preko katerega dostopa do svojega e-bančnega računa /.../«*

Tu ni šlo za osamljen primer, saj je bila v obdobju 10 dni odtujena gotovina z e-bančnih računov še 9 oškodovancev v skupni vrednosti takratnih 11 mio SIT. Denar je storilec kradel s pomočjo trojanskega konja, ki ga je podtaknil na računalnike oškodovancev. Odtujeni denar ki je bil prenesen na račun s. p.-ja, »hackerja« oz. vdiralca pa so na koncu identificirali pri dvigu gotovine.

[26] Več o primeru je zavedeno v literaturi in sicer pod Ostanek Bojan.

**Slika 9.5:Slikovni prikaz, kako je storilec odtujeval denar**




Vir: Ostanek (2014)

## 9.6 Primeri zlorab, ki so bili že kazensko preganjani

- **Višje sodišče v Ljubljani (kazenski oddelek) 2. april 2008**

Zločin: Uporaba ponarejene magnetne kartice s skopiranim magnetnim zapisom prave bančne kartice na bančnem avtomatu pomeni vdor v zaprt prostor, to je v varnostni sistem bančnih avtomatov.

Obtoženci: D. L. B., M. P. in F. C. G. spoznalo za krive nadaljevanega kaznivega dejanja velike tatvine po 1. točki 1. odst. 212. člena KZ v zvezi s 25. členom KZ.

Oškodovali: pri opravljenih hišnih preiskavah v skupnem znesku 15.960,00 EUR. (povzeto po VSL0023138)

- **Vrhovno sodišče (kazenski oddelek) 31. januar 2008**

Zločin: Če obsojenec (s sostorilci) vdre v tuje bančne račune v sistemu on-line bančništva in prenese sredstva na svoj račun ter kasneje dvigne ta sredstva, izpolni vse zakonske znake kaznivega dejanja velike tatvine po 1. točki prvega odstavka 212.člena KZ.

Obtoženci: obsojenega Š.F. spoznalo za krivega nadaljevanega kaznivega dejanja velike tatvine.

Oškodovali: »Vzetje tuje premične stvari z namenom protipravne prilastitve z *vdor*om v tuje bančne račune v sistemu on-line bančništva tako, da je v času od 6.9. do 18.9.2006 eden od neugotovljenih storilcev na neugotovljen način vdrl na on-line bančni račun različnih oškodovancev in z njihovega računa vzel ter prenesel na račun obsojenca v izreku navedene denarne zneske, nato pa je obsojenec po predhodnem obvestilu o prenosu denarja na njegov račun denarne zneske bodisi dvignil bodisi jih poskušal dvigniti, pri tem pa sebi in neznanim

sostorilcem pridobil za 7.990.000 SIT protipravne premoženjske koristi.« (povzeto po VS24074)

- **Vrhovno sodišče (kazenski oddelek) 21. februar 2008**

Zločin: Jemanje tuje premične stvari (denarja) iz bančnega avtomata z uporabo ponarejene bančne kartice in varnostne kode z namenom protipravne prilastitve pomeni uresničevanje zakonskih znakov kaznivega dejanja velike tatvine.
Obtoženci: E.G. in T.B. spoznana za kriva storitve desetih kaznivih dejanj velike tatvine
Oškodovali: Sta s ponarejenimi bančnimi karticami in pravo varnostno kodo PIN premagala oziroma poskušala premagati varnostni sistem bančnih avtomatov NLB, d. d., Ljubljana, in iz njih dvigovala oziroma poskušala dvigniti denar. Kolikšno vsoto sta si prisvojila, ni zapisano. (povzeto po VS24134)

- **Vrhovno sodišče (kazenski oddelek) 27. marec 2008**

Zločin: Zloraba računalniškega sistema z nepooblaščeno uporabo magnetnega zapisa ter varnostnih kod predstavlja vdor v računalniški sistem *banke* oziroma premagovanje večjih ovir, ki stojijo storilcu na poti do denarja v bančnem avtomatu.
Obtoženci: D.Z. in J.B. spoznana kriva za storitve nadaljevanega kaznivega dejanja velike tatvine v sostorilstvu.
Oškodovali: Osumljenca sta morala plačati premoženjskopravni zahtevek oškodovani banki, in sicer E. B. v višini 75.000,00 SIT, za preostanek pa je sodišče oškodovano banko napotilo na pravdo. (povzeto po VS2004244)

- **Vrhovno sodišče (kazenski oddelek) 31. maj 2005**

Zločin: »Pri tatvini denarja iz bančnega avtomata zloraba računalniškega sistema z nepooblaščeno uporabo magnetnega zapisa ter varnostne kode (PIN) v nekem smislu res prestavlja tudi *vdor* v računalniški sistem banke; v kontekstu obravnavanega kaznivega dejanja pa pomeni zgolj način izvršitve kaznivega dejanja oziroma premagovanje ovire, ki stoji storilcu na poti do denarja v avtomatu.«
Obsojeni: R. M.
Oškodovali: Ni zapisano, kolikšna vsota je bila prisvojena. (povzeto po VS23372)

# 10 Zaključek

V magistrskem delu sem skozi teorijo in prakso preučevala varnostne vidike e-bančništva v Sloveniji. Hipoteze, ki sem si jih zastavila na začetku, so:

**E-bančništvo ima iz leta v leto vse večje število uporabnikov in s tem večjo izpostavljenost za zlonamerno kodo.**

1. Informacijska varnost e-bančništva v Sloveniji temelji na tehničnih protokolih varnosti.

Osredotočam se na hipoteze, ki sem jih preverjala skozi teorijo in z intervjujem. Elektronsko bančništvo uporablja vse več ljudi v Sloveniji. Kot je povedal tudi g. Tomaševič, banke obveščajo svoje uporabnike prek elektronske pošte znotraj e-bančništva o tem, kako morajo uporabljati njihovo storitev (da poskrbijo za svojo varnost) in tudi prirejajo razne delavnice na temo uporabe e-bančništva (predvsem za starejše, ki niso ravno vešči uporabe računalnika in svetovnega spleta).

Potrditev glavne hipoteze je nakazana že v poglavju prej, in sicer pri vdorih v e-bančništvo. Sistematično je prikazana tudi v spodnjih tabelah in grafih. Spodnje tabele in grafi prikazujejo problematiko računalniške kriminalitete, kakor jo je zabeležila Slovenska policija oziroma je do njih prišla prijava. Glede na to, da so podatki združeni od leta 2001 do 2013, v njih niso zajete samo zlorabe v e-bančništvu, temveč še vdori v druge račune raznih podjetji. Natančne statistike, koliko je bilo posameznih zlorab v e-bančništvu, ni mogoče dobiti.

Problematika računalniške kriminalitete je v tem, da večina žrtev ne prijavi zlorabe sistemov, saj lahko zaradi tega podjetje izgubi tržno vrednost, ugled in zaupanje strank. Dostikrat pa se zadeva preprosto pomete pod preprogo, saj je postopek prijave zapleten in vsa nadaljnja dejanja žrtvam slabo znana ali neznana; prijava zahteva poseg tretje osebe v sistem, ki vsebuje zaupne podatke. Tako je enostavneje, da sistemski tehnik ali administrator strežnika preprosto odpravi škodo, programerji pa popravijo oziroma odpravijo varnostno luknjo.

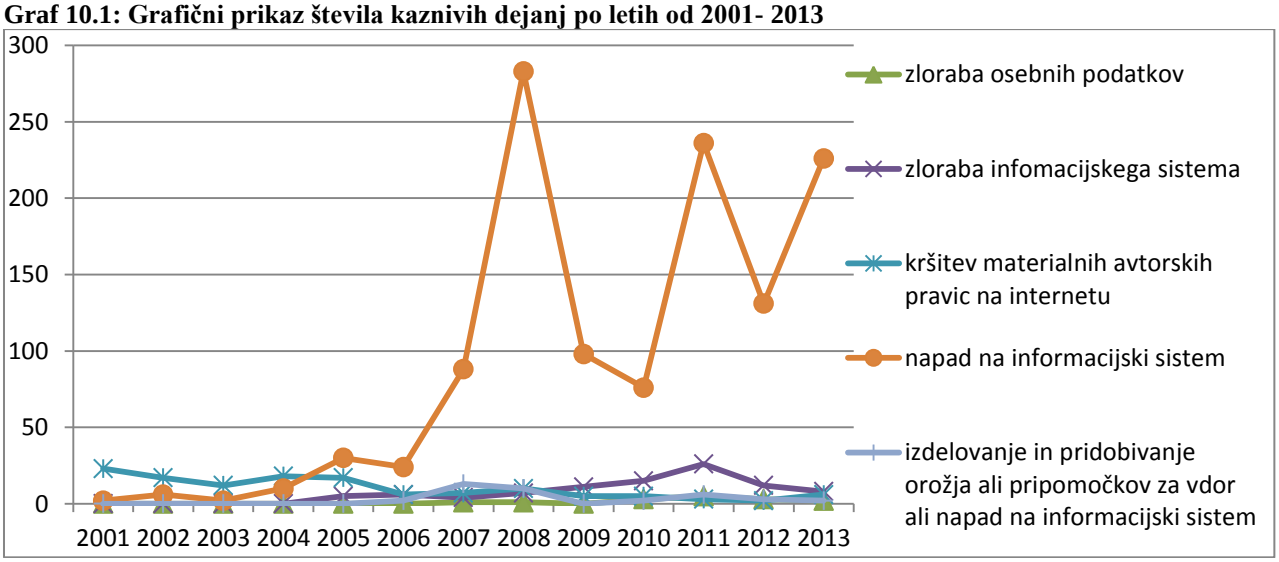
V nadaljevanju so za področje računalniške kriminalitete prikazani združeni podatki Policije na podlagi letnih poročil za obdobje 2001–2013. Zajeta so vsa podjetja, ne samo banke.

**Tabela 10.1:Prikaz števila kaznivih dejanj po letih od 2001- 2013**

| Kazniva dejanja računalniške kriminalitete | število kaznivih dejanj | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
| zloraba osebnih podatkov | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 3 | 5 | 3 | 2 |
| zloraba infomacijskega sistema | 0 | 0 | 0 | 0 | 5 | 6 | 4 | 7 | 11 | 15 | 26 | 12 | 8 |
| kršitev materialnih avtorskih pravic na internetu | 23 | 17 | 12 | 18 | 17 | 6 | 7 | 10 | 5 | 5 | 3 | 2 | 6 |
| napad na informacijski sistem | 2 | 6 | 2 | 10 | 30 | 24 | 88 | 283 | 98 | 76 | 236 | 131 | 226 |
| izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem | 0 | 0 | 0 | 0 | 0 | 2 | 13 | 10 | 0 | 2 | 6 | 3 | 2 |

Vir: Letna poročila Policije od let 2001-2013

**Graf 10.1: Grafični prikaz števila kaznivih dejanj po letih od 2001- 2013**




Vir: Letna poročila Policije od let 2001-2013

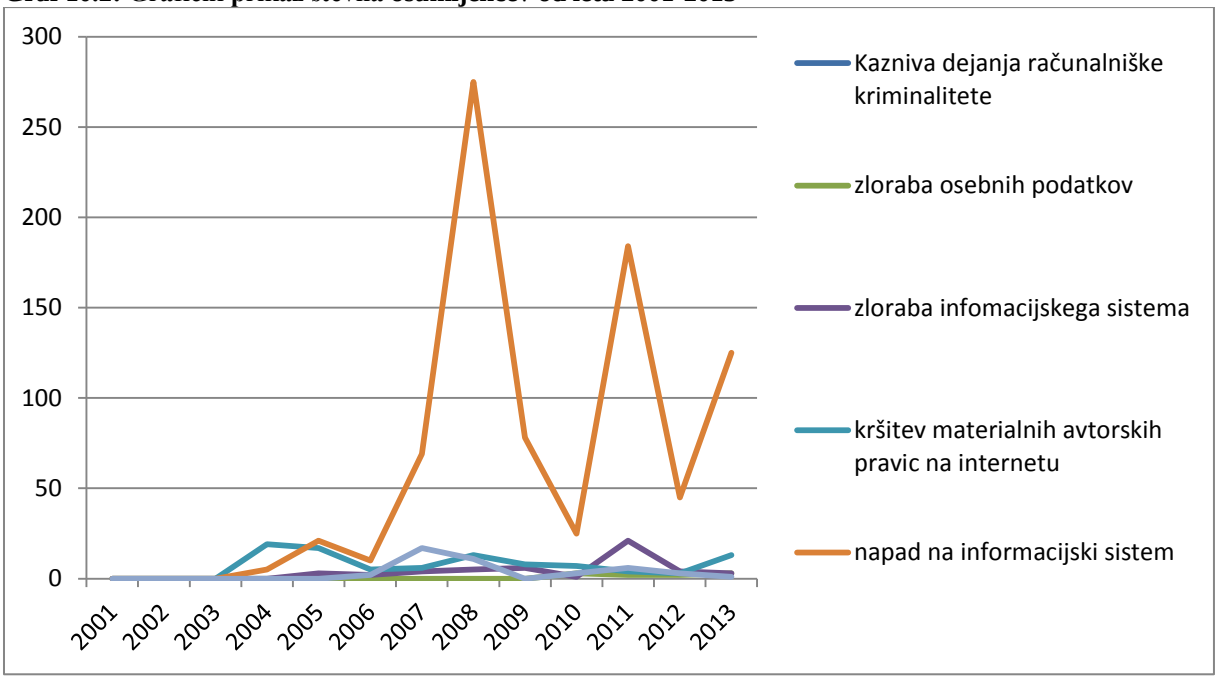
Zgornja tabela (10.1.) in spodnji graf (10.1.) prikazujeta, koliko kaznivih dejanj se je zgodilo od leta 2001 do leta 2013. Največ jih je bilo na področju napada na informacijski sistem. Hipoteza se glasi: »**E-bančništvo ima iz leta v leto vse večje število uporabnikov in s tem večjo izpostavljenost za zlonamerno kodo,«** in vidno je, da se je število kaznivih dejanj iz leta v leto spreminjalo, in sicer je prihajalo do zelo velikega variiranja med leti. Se je pa v primerjavi z letom 2012 (131) v letu 2013 (226) stopnja napadov na informacijski sistem dvignila za 172 %. In, kot je prikazano v raziskavi RIS, je bilo leta 2008 312.000 uporabnikov e-bančništva. Po zadnjih podatkih spletne strani SURS in opravljeni analizi Eurostat se je število uporabnikov e-bančništva v primerjavi z letom 2011 zmanjšalo, in sicer ga je »leta 2011 uporabljalo 39,7 %, leta 2012 pa 35,9 %.« (RIS 2013)

**Tabela 10.2:Prikaz števila osumljencev od leta 2001-2013**

| | število osumljencev | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kazniva dejanja računalniške kriminalitete | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
| zloraba osebnih podatkov | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 3 |
| zloraba infomacijskega sistema | 0 | 0 | 0 | 0 | 3 | 2 | 4 | 5 | 6 | 1 | 21 | 4 | 3 |
| kršitev materialnih avtorskih pravic na internetu | 0 | 0 | 0 | 19 | 17 | 5 | 6 | 13 | 8 | 7 | 4 | 3 | 13 |
| napad na informacijski sistem | 0 | 0 | 0 | 5 | 21 | 10 | 69 | 275 | 78 | 25 | 184 | 45 | 125 |
| izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem | 0 | 0 | 0 | 0 | 0 | 2 | 17 | 11 | 0 | 3 | 6 | 3 | 1 |

Vir: Letna poročila Policije od let 2001-2013

**Graf 10.2: Grafični prikaz števila osumljencev od leta 2001-2013**




Vir: Letna poročila Policije od let 2001-2013

Tabela 4 in grafični prikaz (10.2.) prikazujeta, koliko osumljencev je bilo vsako leto pridržanih ali zaradi napada na informacijski sistem (125) ali drugih kaznivih dejanj, ki so jih storili na področju računalniške kriminalitete.

Tehnični protokoli za zagotavljanje informacijske varnosti e-bančništva temeljijo predvsem na standardih ISO in zakonodaji države, v kateri se izvaja storitev e-bančništva.

Obe hipotezi, ki sta bili zastavljeni, sta bili potrjeni v teoriji in praksi.

Tudi po primerih zlorab bančnih sistemov vidimo, da je nekaj takih dogodkov bilo. Čeprav v

vednost lahko rečem, da vsi primeri tudi ne pridejo v javnost, kajti potem je že lahko ogrožen tudi ugled banke (še posebej, če se je pri njih že zgodilo več zlorab). Gre predvsem za zlorabe kot so skimming ali phishing. Vdora oziroma zlorabe direktnega bančnega sistema kot primera nisem nikjer pridobila (predvidevam, da zaradi varovanja podatkov).

Kako se torej zavarovati v prihodnosti? Še vedno je tu tudi vprašanje, kaj torej narediti, da nam hekerji ne bodo mogli odtujiti denarja prek bankomata ali osebnega računalnika? Nadvse priporočljivo je upoštevanje varnostnih navodil, ki nam jih posreduje banka. Na vsakem bankomatu je potrebno vedno pregledati vse prednje odprtine, kjer bi lahko bila nameščena naprava, ki bi iz magnetnega zapisa prebrala naše podatke pri vnosu kode PIN.

Kaj nas čaka v prihodnost in kako preprečiti še več zlorab? Tako, da se naredi še močnejše sisteme mehanizmov varovanja e-bančništva. Zakonsko je potrebno natančno definirati, da poseg v tujo lastnino in njena nedovoljena pridobitev ne bosta več obravnavana samo kot večja tatvina, ampak bo to mogoče obravnavati tudi kot krajo identitete posameznika, kateremu je bil odtujen denar. Predvsem pa je potrebno zagotoviti, da bo laže dokazljivo na sodiščih, da so storilci res storilci in da se na koncu ne bo storilca oprostilo ali pa mu izreklo samo pogojno kazen, ker mu zločina ne morejo 100-odstotno dokazati. Pri obravnavi takih dejanj so organi doslej čisto pozabili na oškodovanca, ki ima pri tem večje težave. Oškodovanec mora v primeru zlorabe že takoj posredovati prijavo, priložiti vse izpise in dokaze, da tega denarja ni izkoristil oziroma se ni želel okoristiti na račun banke. Oškodovanec je tisti, ki na koncu (vsaj v primeru, ki mi ga je opisala oškodovanka, a ga zaradi varovanja podatkov ne smem podrobneje opisati) sicer lahko dobi povrnjeno škodo, vendar šele po dolgotrajnem postopku.

Varnostni sistemi e-bančništva v Sloveniji so sedaj na točki, ko potrebujejo nadgradnjo, več testiranj, več varnostnih ukrepov, boljše sisteme in mlajši kader, ki bo bolje predvideval, kaj vse se lahko v prihodnosti zgodi. Potrebno je preučiti mlajše generacije, česa vsega so zmožni sedaj in česa vsega bodo zmožni v prihodnosti.

# 11 LITERATURA:


1. A banka Vipa. *A banet.* Dostopno prek: http://www.abanka.si/e-poti/spletna-banka-abanet. (1. marec 2014)
2. Agencija za pošto in elektronske komunikacije Republike Slovenije. 2006. *Smernice za zagotavljanje varnosti omrežij.* Dostopno prek: www.apek.si/sl/datoteke/File/koncni%20uporabniki/smernice_za_zagotavljanje_varnosti_omrezi.pdf (5.januar 2014).

3. Angleška Wikipedia: *Wireless Transport Layer Security*. Dostopno prek: http://en.wikipedia.org/wiki/Wireless_Transport_Layer_Security (23. marec 2014)
4. Anti-virus: *Spletno ribarjenje ali Phishing*, 2014 http://www.anti-virus.si/spletno-ribarjenje-ali-phishing/ (23. marec 2014)
5. Arora, Anu. *1997. Electronic banking and the law*. [S. l.] : IBC business publishing.
6. B2B Continuity. 2002. *ISO 17799 & BS 7799 Compliance.* Dostopno prek **:** http://www.b2bcontinuity.com/ISO17799BS7799.html (3. maj 2014)
7. Banka Celje: *Banka Celje in specializirani računalniški bančni virus SpyEye – ZEUS* - Dostopno prek: http://www.banka-celje.si/osebne-finance/trzne-poti/elektronsko-bancnistvo (14.marec 2014)
8. Berce, Mojca. 2009. *Informacijska zasebnost na internetu in v E-upravi.* Diplomsko delo.Dostopno prek: http://dk.fdv.uni-lj.si/diplomska_dela_1/pdfs/mb11_berce-mojca.pdf (14.marec 2014)
9. Cheswick, William R. in Steven M. Bellovin. *Firewalls and Internet Security:Repelling the Wily Hacker ( first edition)*. Dostopno prek: http://www.wilyhacker.com/1e/
10. Computerhope : *Man-in-the-middle attack* . Dostopno prek : http://www.computerhope.com/jargon/m/mitma.htm (14.marec 2014)
11. Dimc, Maja in etc. 2012. *Kriminaliteta v informacijski družbi.* Ljubljana : Fakulteta za varnostne vede.
12. Dittrich, David. *1999. The Tribe Flood Network"distributed denial of service attack tool.* University of Washington. Dostopno prek: http://staff.washington.edu/dittrich/misc/tfn.analysis (14.marec 2014)

13. Dnevnik: 20.11.2007 . *Prek spleta kradel denar: Izraelec je izkoristil luknjo v*

*spletnem bančništvu*. Dostopno prek: http://www.dnevnik.si/kronika/281724 ( 25. marec 2014)

14. Dujella, Andrej. *Klasična kriptografija.* Dostopno prek: http://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (23. marec2014)
15. Evropska centralna banka. 2013. *Priporočila za varnost spletnih plačil.* Dostopno prek: http://www.bsi.si/library/includes/datoteka.asp?datotekaid=5194&ei=5u8zvnq3jpfzap_pgrak&usg=afqjcnffgae3jrlj03kv5aqgogaqcqysga&sig2=zxoyxltm3eklp8xwiym-hq&bvm=bv.75558745,d.d2s&cad=rja/ (23. marec 2014)
16. Holland, Ted. 2004. *Understanding IPS and IDS: USing IPS and IDS together for Defense in Depth.* Dostopno prek: http://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381 (23. marec 2014)
17. Hopkins, Charles. 2006. *Basic Elements of Information Security, Ezilon infobase December*. Dostopno prek: http://www.ezilon.com/articles/articles/3528/1/Basic-Elements-of-Information-Security (1.april 2014)
18. Informacijski pooblaščenec. 2009. *Socialni inženiring in kako se pred njim ubraniti?* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf (14.marec 2014)
19. Insley Richard, Hussam Al-Abed inTrent Fleming, BOL Gurus. What is the definition of "e-banking"?. Dostopno prek: http://www.bankersonline.com/technology/gurus_tech081803d.html (13. Marec 2014)
20. Iprom. 2007. *E-bančništvo uporabljajo predvsem zaposleni, višje izobraženi, z družinami in višjimi prihodki.* Dostopno prek: http://www.iprom.si/press.html?id=128 (13. Marec 2014)
21. Jerman - Blažič, Borka in etc. 2001. *Elektronsko poslovanje na internetu*. 1. natis. Ljubljana : GV založba.
22. Kolak, Anja. 2006. *Pomen in vloga kriptografije in kriptoanalize na področju zagotavljanja nacionalne varnosti.* Diplomsko delo. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Kolak-Anja.PDF (14.marec 2014)
23. Kovačič, Matej. *Zasebnost v Informacijski družbi*. Teorija in praksa, Let. 37, št. 6 (nov./dec. 2000), str. 1019–1034, strokovni članek. Dostopno prek: http://www.ris.org/index.php?fl=2&lact=1&bid=231&menu=0 (7. marec 2014)
24. --- 2014. Pravokator. *Heartbleed ranljivost in varnost slovenske državne uprave*.

Dostopno prek: https://pravokator.si/index.php/2014/04/11/heartbleed-ranljivost-in-varnost-slovenske-drzavne-uprave/ (1. junij 2014)

25. ---. *Kriptografija*. Članek. Dostopno prek : http://www.ris.org/si/ris99/teksti/kript.html (14.marec 2014)
26. ----*PGPfone ali kako se zaščititi pred telefonskim prisluškovanjem*. Dostopno prek: http://www.ljudmila.org/matej/pgp/pgpfone.html (30. marec 2014)
27. --- 2006. *Nadzor in zasebnost v informacijski družbi*. Znanstvena knjižnica, Fakulteta za družbene vede, Ljubljana 2006
28. Kozic, Tina, Katja Prevodnik, Vasja Vehovar in Luka Kogovšek. 2009. *E-bančništvo 2009*. Dostopno prek: http://www.ris.org/2008/10/RIS_porocila/Ebancnistvo_2009/? (10. april 2014).
29. Lesjak Igor. *Varen elektronski podpis kot temelj elektronskega poslovanja*. Dostopno prek: http://www.ltfe.org/objave/varen-elektronski-podpis-kot-temelj-elektronskega-poslovanja/ (21.januar 2014)
30. Lobe, Jaka. 2003. *Razvoj elektronskih plačilnih sredstev - stanje v Sloveniji*. Diplomsko delo. Dostopno prek: www.cek.ef.uni-lj.si/u_diplome/lobe647.pdf (1. februar 2014)
31. Malenšek, Blaž. 2007. *Elektronsko bančništvo* . Diplomsko delo. Univerza v Ljubljani: Ekonomska fakulteta. Dostopno prek: www.cek.ef.uni-lj.si/u_diplome/malensek473.pdf (30.april 2014)
32. Microsoft TechNet. *TLS/SSL technical references*. Dostopno prek: http://technet.microsoft.com/en-us/library/cc783349%28v=ws.10%29.aspx#w2k3tr_schan_how_hkrr (23.februar 2014)
33. Ministrstvo za javno upravo. *Uporaba kriptografije v internetu*. Dostopno prek: http://www.ca.gov.si/kripto/enigma.htm (dostop dne 30.april 2014)
34. Ministrstvo za notranje zadeve. Policija. 2001-2013. *Letna poročila o delu policije.* Dostopno prek: http://www.policija.si/index.php/statistika (15. Junij 2014)
35. Miš- Svojšak I. 1999. E-črka, ki spreminja svet. *Bančnik 4: 4-7.*
36. Mitnick, Kevin David. 2002. *The art of deception : controlling the human element of security.* Indianapolis, Ind. : Wiley, cop. Dostopno prek: http://fr.thehackademy.net/madchat/esprit/textes/The_Art_of_Deception.pdf (30.april 2014)
37. Nacionalni cert +. *CSRF napadi*. Dostopno prek: http://www.cert.hr/node/15454 (30.april 2014)

38. Nova Ljubljanska banka. *Klik*. Dostopno prek: http://www.nlb.si/klik (1. marec 2014)
39. Office of Information Technology. *Definition of Information Security*. Dostopno prek: http://oit.unlv.edu/network-and-security/definition-information-security (30. marec 2014)
40. Organizacija Ljudmila. *Kriptografija ali kako se zaščititi pred elektronskim prisluškovanjem* . Dostopno prek: http://www.ljudmila.org/matej/pgp/crypto.html (dostop dne (30. marec 2014)
41. Ostanek, Bojan, SKP Ljubljana: *Zlorabe elektronskega bančništva - potek preiskave v praksi*. Dostopno prek: http://videolectures.net/site/normal_dl/tag=48935/kkdf09_ostanek_zeb_01.ppt (14.marec 2014)
42. Panda Security. *Crimeware: the silent epidemic*. Dostopno prek: http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/ (30.april 2014)
43. PISRS. 2006. *Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1).* Dostopno prek: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4161 (15.april 2014)
44. --- 2006.*Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja*. Dostopno prek: http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE6520 (15.april 2014)
45. --- 2006-2011. *Zakon o tajnih podatkih (ZTP).* Dostopno prek: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133(15.april 2014)
46. Pivec, Franci. 2004. *Informacijska družba*. Subkulturni azil Maribor.
47. Praxiom Research Group. 2013-2014. *ISO IEC 27001:2013 (Translated into plain English).* Dostopno prek: http://www.praxiom.com/iso-27001.htm (10. junij 2014).
48. Rouse, Margaret. 2013. *Distributed denial-of-service attack (DDoS)*. Dostopno prek: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (14.marec 2014)
49. Sawer Patrick. *The Telegraph 'Card-skimming' gang targets train stations*. Dostopno prek: http://www.telegraph.co.uk/news/uknews/1581820/Card-skimming-gang-targets-train-stations.html (30.april 2014)
50. Scam watch. *Card skimming.* Dostopno prek:

http://www.scamwatch.gov.au/content/index.phtml/tag/CardSkimming(30.april 2014)

51. Securelist. *Crimeware: A new round of confrontation begins*. Dostopno prek: https://www.securelist.com/en/analysis/204792115/Crimeware_A_new_round_of_confrontation_begins (30. marec 2014)
52. Si-cert : *Phishing*. Dostopno prek: https://www.cert.si/si/varnostne-groznje/phishing/ (30. marec 2014)
53. --- 2012. *Bančni trojanec, ki krade avtentikacijske podatke za Klik NLB* - https://www.cert.si/si-cert-2012-16-bancni-trojanec-ki-krade-avtentikacijske-podatke-za-klik-nlb/
54. ---- 2012. SKB banka. *Phishing napad na komitente SKB banke*. Dostopno prek: https://www.cert.si/si-cert-2012-09-phishing-napad-na-komitente-skb-banke/ (30. marec 2014)
55. SI-CA. 2006. *Uporaba kriptografije v internetu – Digitalni podpis*. Dostopno prek: http://www.si-ca.si/kripto/kr-podp.htm (14.marec 2014)
56. SKB. *O SKB banki*. Dostopno prek: https://www.skb.net/Default.aspx (1. marec 2014)
57. Sodba I Ips 374/2007 - *VS2004244*. 2008. Dostopno prek: http://sodnapraksa.si/?q=vdor%20banke*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=22284 (3. maj 2014)
58. Sodba I Ips 381/2007 - VS24134. 2008. Dostopno prek: http://sodnapraksa.si/?q=vdor%20banke*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=26915 (3. maj 2014)
59. Sodba I Ips 461/2007 - *VS24074*. 2008. Dostopno prek: http://sodnapraksa.si/?q=vdor%20banke*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=26855 (3. maj 2014)
60. Sodba I Ips 98/2004 - *VS23372*. 2005. Dostopno prek: http://sodnapraksa.si/?q=vdor%20banke*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=26155 (3. maj

2014)

61. Soklič, Jure. 2002. *Vloga kriptografije v času II. svetovne vojne*. Diplomsko delo, Fakuleteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Soklic-Jure.PDF (3. maj 2014)
62. SSLab test. *SSL Server Test.* Dostopno prek: https://www.ssllabs.com/ssltest/ (13. Marec 2014)
63. --- 2014. *Server test za A banko*. Dostopno prek: https://www.ssllabs.com/ssltest/analyze.html?d=epoti.abanka.si (1. junij 2014)
64. --- 2014. *Server test za SKB*. Dostopno prek: https://www.ssllabs.com/ssltest/analyze.html?d=skb.net (1. junij 2014)
65. ---2014. *Server test za Unicredit Bank*. Dostopno prek: https://www.ssllabs.com/ssltest/analyze.html?d=si.unicreditbanking.net (1. junij 2014)
66. ---2014. *Server test za NLB*. Dostopno prek: https://www.ssllabs.com/ssltest/analyze.html?d=klik.nlb.si (1. junij 2014)
67. Stripp Alan: *How the Enigma Works*. Dostopno prek: http://www.pbs.org/wgbh/nova/military/how-enigma-works.html 2014 (3. maj 2014)
68. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
69. Šercar M. Tvrtko. 2000. *Gradivo za uvod v kritiko informacijske družbe*, COBISS Obv. 2000, 5(1), 1-18. Dostopno prek: http://home.izum.si/cobiss/cobiss_obvestila/2000_1/Html/clanek_01.html (10. maj 2014)
70. --- 2007. *Kritika kritike teorij informacijske družbe.* Institut informacijskih znanosti, Maribor. Dostopno prek: http://home.izum.si/cobiss/cobiss_obvestila/2001_2/Html/clanek_02.html (3.januar2014).
71. Štiblar, Franjo. 2010. *Bančništvo kot hrbtenica samostojne Slovenije*. Ljubljana : Založba ZRC, ZRC SAZU
72. *The swift codes*. Dostopno prek: http://www.theswiftcodes.com/slovenia/ (1. junij 2014)
73. Tomaševič, Denis. 2014. *Intervju z avtorjem*. (21.februar 2014)
74. Toplišek, Janez. 1998. *Elektronsko poslovanje*. Ljubljana : Atlantis
75. Unicredit Bank. *Spletna stran Unicredit Bank*. Dostopno prek:

http://www.unicreditbank.si/sl/Prebivalstvo/Elektronsko_bancnistvo/Online_banka (13. Marec 2014)

76. Uradni list. 2005. *Uredba o varovanju tajnih podatkov.* Dostopno prek: https://www.uradni-list.si/1/content?id=57489 (15.april 2014)
77. --- 2007. *Zakon o varovanju osebnih podatkov*. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlurid=20074690 (15.april 2014)
78. --- 2007. *Uredba o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih.* Dostopno prek: http://www.uradni-list.si/1/content?id=80528 (15.april 2014)
79. --- 2008. Kazenski zakonik Republike Slovenije (KZ-1). Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlurid=20082296 (15.april 2014)
80. Verbič, Miroslav. *Zaščita*. Dostopno prek: http://www2.arnes.si/~ssdmverb/pgp_si.htm (7.marec 2013)
81. Vehovar, Vasja in Luka Kronegger. 2005. *E- bančništvo*. RIS. Dostopno prek: http://www.ris.org//uploadi/editor/1237817193E-bancnistvo.pdf (10. februar 2014).
82. Vidmar, Tone. 2002. *Informacijsko-komunikacijski sistemi*. Založba Pasadena.
83. Wikipedia. Požarni zid. 2014. Dostopno prek: http://sl.wikipedia.org/wiki/Po%C5%BEarni_zid (7.marec 2013)
84. VSL sodba III Kp 6/2008 - *VSL0023138*. 2008. Dostopno prek: http://sodnapraksa.si/?q=vdor%20banke*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=43152 (3. maj 2014)
85. Webopedia: *WTLS* . Dostopno prek: http://www.webopedia.com/TERM/W/WTLS.html (23. marec 2014)
86. Webster, Frank. 2006. *Information society theory. Third edition. Lanchester University.* Dostopno prek: http://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf (15. januar 2014)
87. Wikipedia. 2007. *Cryptography.* Dostopno prek: http://en.wikipedia.org/wiki/Cryptography (7.marec 2007)
88. ---. *Second Life*. Dostopno prek: http://en.wikipedia.org/wiki/Second_Life (15.marec 2014)
89. Wilson III, E.J. 1998. *Globalization, Information, Technology and Conflict in the Second and Third Worlds.* ROCKEFELLER BROTHERS FUND, INC. Dostopno

prek:
http://www.rbf.org/sites/default/files/Globalization%2C_Information_Technology%2C_and_Conflict.pdf (23. marec2014)

90. Združenje bank: *Priporočila za uporabo elektronskih tržnih poti v bankah.* 2006. Dostopno prek:
https://www.sparkasse.si/filelib/zahtevki/net.stik/priporoila_za_uporabo_elektronskih_trnih_poti.pdf (3. maj 2014)
91. Zeman, Matija: *Sigurnost Web aplikacija zasnovanih na AJAX tehnologiji*,. Dostopno prek: http://os2.zemris.fer.hr/ostalo/2007_zeman/ (23. Marec2014)
92. Zemljič, Igor. 2011. *Franjo Štiblar: Bančništvo kot hrbtenica samostojne Slovenije*. Dostopno prek: http://knjiznicainz.blogspot.com/2011/02/franjo-stiblar-bancnistvo-kot-hrbtenica.html (23. marec2014)

# 12 PRILOGE

PRILOGA A: Intervju in prepis pogovora

Podjetje Halcom se ukvarja s programskimi rešitvami za podjetja, ki omogočajo varen prenos denarja in poslovanje.

1) Koliko časa ste že v podjetju Halcom in kaj ste po izobrazbi ter kakšna je vaša delovna pozicija v podjetju Halcom?

*V podjetju Halcom sem že od leta 2008. Prva pozicija, ki sem jo imel, je bila vodja IT-oddelka oziroma šef informacijsko-komunikacijske tehnologije. Sedaj pa mi je dodeljena vloga direktorja informatike (CIO) in delam kot vodja urada za informacijsko varnost (CISO). Sem univerzitetni diplomirani elektrotehnik.*

2) Katere produkte in storitve ponujate bančnemu trgu?

*Ponujamo programske rešitve za elektronsko banko in elektronsko plačevanje. Ločimo med temi pojmi in je pomembno za njih. Stališča uporabnika so drugačna ... rešitev je enaka, cilj je drugačen oz. je pomembno, kaj si posamezni uporabnik želi. Pri elektronski banki želimo določene storitve plačevati ... mobilna banka in mobilno plačevanje je čisto drugačen scenarij. Pri mobilni banki upravljaš vse tako kot v elektronski banki, za plačevanje pa je sistem Moneta. Mobilni telefon ima torej že vgrajene višjo zaščito in tudi mobilni telefon začnemo hitreje pogrešati in s tem tudi poskrbimo za večjo varnost.*
*Storitve: certifikat Halcom CA, elektronsko računalništvo v oblaku (imamo več kot 10 let izkušenj pri delovanju elektronske banke v oblaku). Elektronske banke lahko delujejo na naših strežnikih. Podpiramo prek 75 bank in od tega jih večina uporablja to storitev. Za majhne banke je to prednost, saj pridobijo pri nas celotno infrastrukturo, kar se pri večini pozna pri stroških. Banke so lastniki podatkov in se ti podatki varujejo.*

3) Izdelanih je že kar nekaj aplikacij za poslovanje pri e-bančništvu. Katere so najuspešnejše aplikacije in storitve podjetja Halcom?

*Varna avtentikacija – dvostopenjska varnost. Predvsem je izpostavljena pametna kartica, saj ključa ne moreš odtujiti od kartice. Če ti pa že to uspe, pa moraš poznati PIN. Naj izpostavim tudi biometrične metode, vendar pri npr. biometrični podpis ne deluje najbolj varen, saj*

*obstaja veliko metod in vsaka metoda ima svoje izjeme. Če ti uporabljaš prstni odtis in ne poskrbiš dovolj za zaščito, lahko nekdo drug pride do prstnega odtisa. Biometrične metode so problematične in se jih v elektronskem bančništvu ne uporablja.*

4) Vaše področje dela so varnostni vidiki aplikacij in storitev. Katere varnostne postopke, metode in tehnologije uporabljate za zaščito podatkov strank in uporabnikov?

*Zakonodaja je samo pravni vidik, tu je še tehnološki vidik. Potem pa obstajajo še drugi vidiki. Pri pravnem vidiku gre zgolj zato, da uporabniki želijo od banke iztržiti škodo. Primer: bančna kartica, ki jo nekomu daš in jo nekdo izkoristi, ali pa nekdo izkoristi tvojo pametno kartico, vendar brez čitalnika vsega tega ne more.*

5) Katere standarde uporabljate (ISO ipd.) kot smernice pri uvajanju postopkov in ukrepov za varovanje informacij? Jih lahko v splošnem opišete?

*Standardi ISO so eno, debelina zidu, ki je opisana v zakonih, je drugo. V informacijski dobi se stvari spreminjajo vsako leto in tudi obstajajo različni pravilniki, vendar nobena stvar ne govori, kako zaščiti infrastrukturo. Vendar imaš pa delovne akte, ki govorijo, kako zaščititi, vendar ne moreš vsega uskladiti med seboj. Zato prihaja do vsakoletnih večkratnih sprememb. Standardi ISO so plačljivi. Naj bi bili neodvisni od posamezne industrije (kaj in ne kako). Imajo več dokumentov (številka 1 – presoja, če podjetje zadostuje pogojem, in veliko prilog, ki govorijo, kako ... vsaka številka pomeni neko stvar), standard je fleksibilen.*
*Delujemo po standardih kakovosti **ISO 9001** od 2003 in **ISO 27001** od 2010 (varovanje informacij).*

6) Halcom CA izdaja digitalne certifikate za pravne in fizične osebe. Kakšne so razlike med certifikati za pravne in fizične osebe?

*Razlika med certifikati za pravne in fizične osebe je predvsem v lastništvu certifikata, ki se izda na ime in priimek, vendar, ko gre za pravno osebo, je lastnik podjetje. TU gre torej za bistveno razliko med pravno in fizično osebo (podjetje lahko kadar koli prekliče, lahko tudi na osebnega da omejitev, vendar je potem večja možnost in problem osebnega preklica).*

- *digitalno potrdilo na pametni kartici ali ključu USB ENA ZA VSE,*
- *obnova digitalnega potrdila,*
- *strežniška potrdila.*

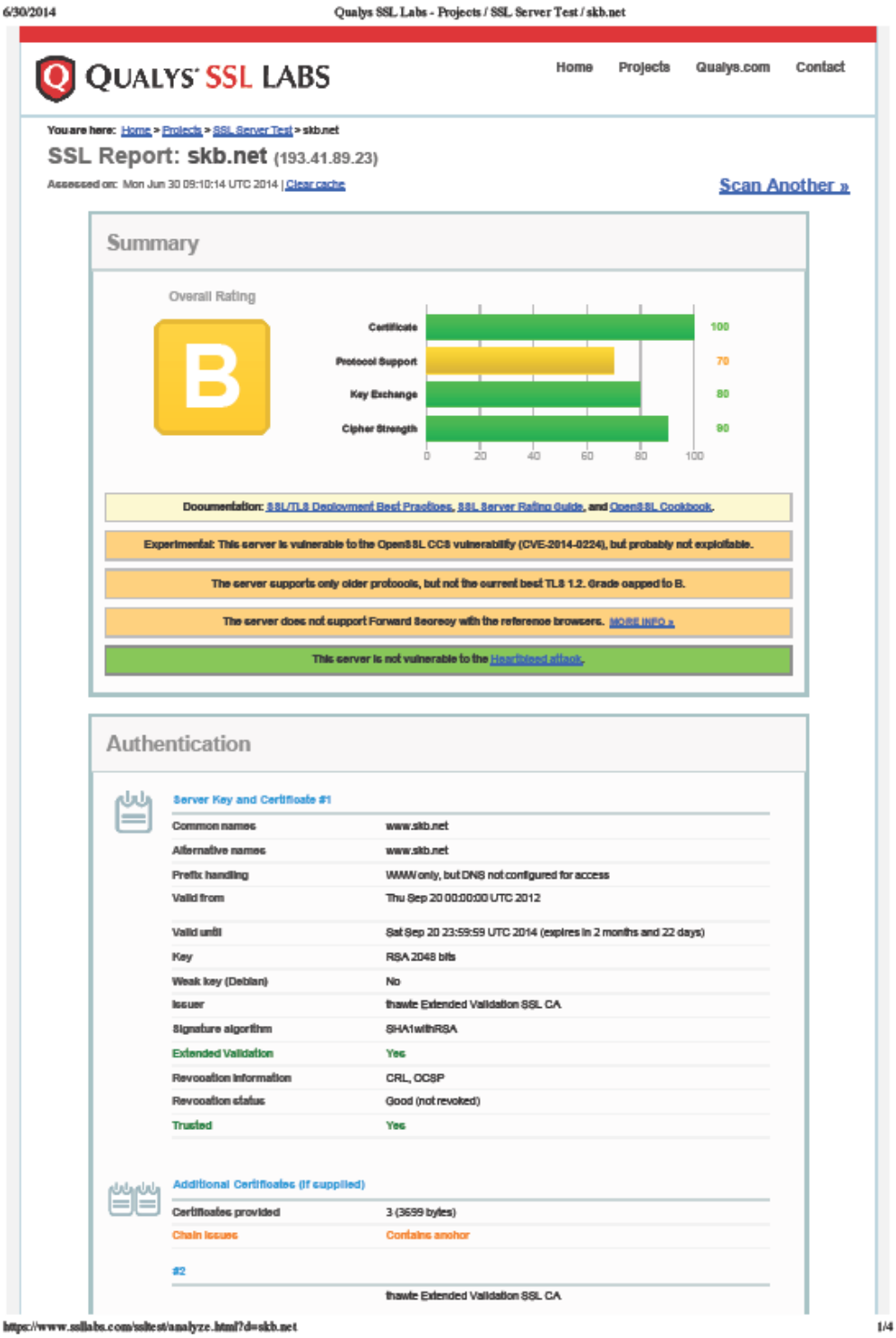
7) Ste v svoji karieri že doživeli kakšen hekerski napad na e-bančni sistem ali aplikacijo? Če da, bi prosila za opis, kateri napad in kakšne so bile posledice?

*Vdorov v elektronske banke ni, so zlorabe računov. Primerov vdorov praktično ni, so zlorabe, ki so usmerjene bolj v uporabnike. Kot primer: če bi nekdo znal ponatisniti ček, tak kot je, in ne vzeti tvojega, kjer gre za zlorabo. Različni načini kako se hekerji dokopljejo do podatkov, to pa je vdor. Inštalacija trojanca je zloraba in ne vdor. Nekaj let nazaj so se dogajali vdori, saj so se pojavljale sistemske napake. Sedaj se je pa stvar spremenila, saj je vse na strani uporabnika in kako nekdo prelisiči posameznike, uporabnike.*

*Tisto, kar se je včasih reklo napad, je sedaj predrugačeno. Tistih, ki želijo ugotoviti, kaj je vse odprto na spletu, je veliko. Večina napadov je usmerjenih na uporabnike in ne na banko. Primer Googla, kjer so bili točno usmerjeni napad na njih, z bombardiranjem vsega. Opozarjam: če bi uporabniki brali obvestila banke itd. do napadov oziroma zlorab ne bi prihajalo.*

*Primerov, ki so v kazenskem postopku in še niso zaključeni, se zaradi varovanja podatkov ne sme povedati, dokler ni proces zaključen. O takih primerih napadov oziroma zlorab ne smem pripovedovati.*

PRILOGA B: Izpis iz spletne strani https://www.ssllabs.com/ssltest/



QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > epoti.abanka.si

# SSL Report: epoti.abanka.si (195.35.122.85)

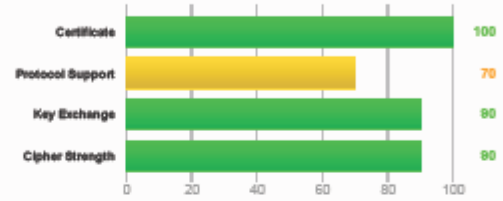
Assessed on: Mon Jun 30 09:10:40 UTC 2014 | Clear cache

Scan Another »

## Summary

Overall Rating

B




Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

## Authentication

### Server Key and Certificate #1

| | |
|---|---|
| Common names | mpoti.abanka.si |
| Alternative names | mpoti.abanka.si epoti.abanka.si |
| Prefix handling | Not required for subdomains |
| Valid from | Mon Mar 18 00:00:00 UTC 2013 |
| Valid until | Mon Mar 23 12:00:00 UTC 2015 (expires in 8 months and 26 days) |
| Key | RSA 2048 bits |
| Weak key (Debian) | No |
| Issuer | DigiCert High Assurance EV CA-1 |
| Signature algorithm | SHA1withRSA |
| Extended Validation | Yes |
| Revocation information | CRL, OCSP |
| Revocation status | Good (not revoked) |
| Trusted | Yes |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 2 (3636 bytes) |
| Chain issues | None |

#2

DigiCert High Assurance EV CA-1

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > si.unicreditbanking.net

# SSL Report: si.unicreditbanking.net (162.25.25.44)

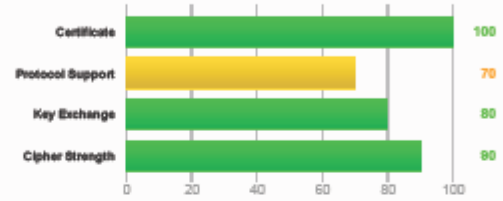
Assessed on: Mon Jun 30 09:10:37 UTC 2014 | Clear cache

Scan Another »

## Summary

Overall Rating

B




Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

Experimental: This server is vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224), but probably not exploitable.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

## Authentication

### Server Key and Certificate #1

| | |
|---|---|
| Common names | si.unicreditbanking.net |
| Alternative names | si.unicreditbanking.net |
| Prefix handling | Not required for subdomains |
| Valid from | Fri Dec 13 15:40:30 UTC 2013 |
| Valid until | Sat Dec 13 15:40:30 UTC 2014 (expires in 5 months and 16 days) |
| Key | RSA 2048 bits |
| Weak key (Debian) | No |
| Issuer | UniCredit Subordinate External |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Revocation information | CRL |
| Revocation status | Good (not revoked) |
| Trusted | Yes |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 3 (3018 bytes) |
| Chain issues | Contains anchor |

#2

| | |
|---|---|
| | UniCredit Subordinate External |

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > klik.nlb.si

# SSL Report: klik.nlb.si (193.201.214.51)

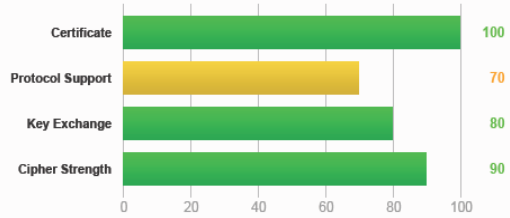
Assessed on: Mon Jun 23 15:08:36 UTC 2014 | Clear cache

Scan Another »

## Summary

Overall Rating

B




Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

## Authentication

### Server Key and Certificate #1

| | |
|---|---|
| Common names | klik.nlb.si |
| Alternative names | klik.nlb.si |
| Prefix handling | Not required for subdomains |
| Valid from | Thu Jun 19 08:11:42 UTC 2014 |
| Valid until | Sun May 06 22:10:50 UTC 2018 (expires in 3 years and 10 months) |
| Key | RSA 2048 bits |
| Weak key (Debian) | No |
| Issuer | Entrust Certification Authority - L1C |
| Signature algorithm | SHA1withRSA |
| Extended Validation | No |
| Revocation information | CRL, OCSP |
| Revocation status | Good (not revoked) |
| Trusted | Yes |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 2 (2556 bytes) |
| Chain issues | None |