Problem sigurnosti u elektroničkom bankarstvu

Krnjić, Katarina

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:639694

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**



Repository / Repozitorij:

REPEFZG - Digital Repository - Faculty of Economcs & Business Zagreb







Sveučilište u Zagrebu
Ekonomski fakultet
Preddiplomski stručni studij

PROBLEM SIGURNOSTI U ELEKTRONIČKOM BANKARSTVU

Završni rad

Katarina Krnjić

Zagreb, rujan 2019.

Sveučilište u Zagrebu

Ekonomski fakultet

Preddiplomski stručni studij

PROBLEM SIGURNOSTI U ELEKTRONIČKOM BANKARSTVU

Završni rad

Student: **Katarina Krnjić,**

Mentor: **Prof. dr. sc. Ivan Strugar**

Zagreb, rujan 2019.

_____
Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____
(vrsta rada)
isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu,_____ _____
(potpis)

SADRŽAJ

1. UVOD 1

1.1. Cilj i svrha rada 1

1.2. Izvori podataka i metode istraživanja 1

1.3. Sadržaj i struktura rada 2

2. RAZVOJ ELEKTRONIČKOG POSLOVANJA 3

2.1. Pojmovno određenje elektroničkog poslovanja 3

2.2. Povijest elektroničkog poslovanja 7

2.3. Modeli elektroničkog poslovanja 9

2.4. Značaj elektroničkog poslovanja 11

3. TEMELJNE ODREDNICE ELEKTRONIČKOG BANKARSTVA 13

3.1. Pojmovno određenje elektroničkog bankarstva 13

3.2. Povijesni razvoj elektroničkog bankarstva 14

3.3. Usluge elektroničkog bankarstva 15

3.3.1. Bankomati 15

3.3.2. Kartično poslovanje 17

3.3.3. EFT/POS 19

3.3.4. Internet bankarstvo 20

3.3.5. Mobilno bankarstvo 21

3.4. Prednosti i nedostaci elektroničkog bankarstva 22

4. RIZICI U SUVREMENOM ELEKTRONIČKOM BANKARSTVU 24

4.1. Pojam i vrste rizika u elektroničkom bankarstvu 24

4.2. Upravljanje rizicima u elektroničkom bankarstvu 26

4.3. Obilježja identifikacije, autentikacije i autorizacije 28

5. SIGURNOST U ELEKTRONIČKOM BANKARSTVU 30

5.1. Načini autorizacije korisnika u elektroničkom bankarstvu 30

5.1.1. Token 30

5.1.2. TAN 31

5.1.3. Smart kartice 32

5.2. Mjere sigurnog korištenja elektroničkog bankarstva od strane banke 34

5.2.1. Zaštita podataka 34

5.2.2. Preventivne mjere 34

5.2.3. Mjere za već nastalu štetu 34

5.3. Mjere sigurnog korištenja elektroničkog bankarstva od strane klijenata 35

5.4. Značaj elektroničkog potpisa u sigurnosti elektroničkog bankarstva 36

5.4.1. Pojam elektroničkog potpisa 37

5.4.2. Povijest digitalnog potpisa 37

5.4.3. Primjena digitalnih potpisa 39

5.4.4. Napadi na digitalni potpis 41

6. ZAKLJUČAK 43

LITERATURA 466

POPIS SLIKA 499

1. UVOD

1.1. Cilj i svrha rada

Banke nisu ostale imune na razvoj informacijskih tehnologija te tako prilagođavaju svoje poslovanje razvoju informacijskih sustava. Jako važno je shvatiti da na današnje poslovanje banaka i financijskih institucija direktno utječe spremnost banke i odgovornih osoba da prihvaćaju nove trendove, odnosno do koje su mjere banke spremne prihvatiti nove trendove. Informacijski sustavi danas imaju veliku ulogu u poslovanju banke i direktno utječu na poslovanje, te se upravo iz navedenih informacijskih sustava razvio novi oblik poslovanja – elektroničko poslovanje.

Cilj ovog rada je prikazati glavne probleme sigurnosti koji se javljaju u suvremenom elektroničkom bankarstvu.

1.2. Izvori podataka i metode istraživanja

Ovaj završni rad je napravljen na temelju prikupljanja i analize sekundarnih izvora podataka. Sekundarni izvori podataka dostupni su znanstvenoj i stručnoj literaturi vezanoj uz elektroničko bankarstvo i sigurnost u navedenom bankarstvu.

Metode koje su korištene prilikom izrade rada su:
1.Metoda indukcije – sustavna primjena induktivnog načina zaključivanja kojim se putem analize pojedinačnih činjenica dolazi do općeg zaključka.
2. Metoda dedukcije – sustavna primjena deduktivnog načina zaključivanja u kojem se iz općeg suda izvode pojedinačni, posebni zaključci u radu.
3. Metoda analize – metoda u kojem se vrši raščlanjivanje složenih pojmova i zaključaka na jednostavnije dijelove i elemente.
4. Metoda sinteze – metoda u kojem se putem znanstvenog istraživanja putem sinteze vrši transformacija jednostavnih sudova u složenije.
5. Metoda generalizacije – metoda u kojoj je misaoni postupak uopćavanja putem kojeg se od posebnog pojma dolazi do općenitijeg.
6. Metoda klasifikacije – podjela općeg pojma na posebne pojmove.
7. Metoda deskripcije – metoda u kojoj se na jednostavan način opisuju činjenice, procesi i predmeti, bez znanstvenog tumačenja i objašnjavanja.

8. Metoda kompilacije – metoda u kojoj se preuzimaju rezultati tuđih opažanja,stavova i spoznaja.

1.3. Sadržaj i struktura rada

Sadržaj i struktura rada koncipirani su u šest poglavlja. Prvo poglavlje govori o cilju i svrsi rada, izvorima podataka te strukturi rada. U drugom poglavlju prikazane su glavne odrednice razvoja elektroničkog poslovanja. Treće poglavlje govori o temeljnim odrednicama elektroničkog poslovanja. U četvrtom poglavlju prikazani su glavni rizici koji se javljaju u suvremenom elektroničkom bankarstvu. U petom poglavlju opisane su odrednice sigurnosti elektroničkog bankarstva. U šestom poglavlju dan je zaključak rada. Sedmo, kao zaključno poglavlje prikazuje bibliografske jedinice koje su korištene prilikom izrade ovog rada.

2. RAZVOJ ELEKTRONIČKOG POSLOVANJA

Pojam elektroničko poslovanje se često miješa sa srodnim pojmom elektronička trgovina, međutim elektroničko poslovanje je širi pojam od elektroničke trgovine jer ne označava samo kupnju i prodaju, već čitav niz poslovnih aktivnosti, odnosno poslovnih procesa između dva ili više poslovnih partnera, i globalno.

„Elektroničko poslovanje se počinje spominjati u gospodarstvu 1995. godine.“[1] Dok je u svijetu, 1999. godine elektronička trgovina bila na svom vrhuncu, u Hrvatskoj je pojam Interneta bio slabo poznat. „Prvi oblici prodaje preko Interneta u Hrvatskoj javljaju se 1996. godine, godinu dana nakon razvoja e-prodavaonica u svijetu.“[2]

2.1. Pojmovno određenje elektroničkog poslovanja

Elektroničko poslovanje je korištenje informatičke infrastrukture u cilju obavljanja poslovnih aktivnosti ili upravljanje poslovnim aktivnostima putem korporacijskih mreža ili Interneta, odnosno virtualno.

„Elektroničko poslovanje suvremeni je oblik organizacije poslovanja, koji podrazumijeva primjenu informatičke, i posebice, internetske tehnologije. Predstavlja najsuvremeniji oblik organizacije poslovanja, kojemu teže sve tvrtke kojima je cilj uspješno poslovanje.“[3]

„Elektroničko poslovanje čini danas najsuvremeniji oblik organizacije poslovanja kojemu teže svi gospodarski subjekti orijentirani aktivnom osvajanju što boljih tržišnih pozicija i intenzivnom ulaganju u razvojne poslove.“[4]

Elektroničko poslovanje određuje je primjena elektroničkih komunikacija i digitalnih podataka koji stvaraju tehnološku platformu za stvaranje trgovinskih veza između organizacija te sa pojedincima. Značajan dio e-poslovanja čini web poslovanje.[5]

[1] Panian, Ž. (2002.): Izazovi elektroničkog poslovanja, Narodne novine d.d., Zagreb, str. 71.
[2] Ružić, D. (2003): E – marketing, Ekonomski fakultet u Osijeku, Osijek, str. 266.
[3]Panian, Ž. (2000.): Elektroničko poslovanje – šansa hrvatskoga gospodarstva u 21. Stoljeću, Ekonomski pregled, 52 (3-4), Zagreb, str. 272.
[4]Panian, Ž., Strugar, I. (2000.): Primjena računala u poslovnoj praksi, Sinergija, Zagreb, str. 121.
[5]Prema: E- poslovanje, http://www.webstrategija.com/ws/05/e-poslovanje, 08.05.2019.

Brojni su razlozi zbog kojih se poduzeća odlučuju na uvrštavanje informacijske i komunikacijske tehnologije u svoje poslovanje. Uvođenjem elektroničkog poslovanja tvrtka teži boljem iskorištavanju raspoloživih poslovnih resursa, posebice onih informacijskih. Ona doprinosi boljoj konkurentnosti poduzeća, smanjuju se troškovi, rad postaje ugodniji, ljudi ne moraju više odrađivati neke zamorne poslove, do izražaja dolazi kreativnost te zadovoljstvo radnika raste. Koncept elektroničkog poslovanja primjenjuje se gotovo svugdje.

„Elektroničko poslovanje donosi brojne prednosti organizacijama, kao i kupcima, te društvu u cjelini. Osim prednosti ima i određenih nedostataka. U nastavku će biti navedene prednosti i nedostaci sa svih aspekata te će biti analizirano kolike su zapravo dobrobiti takvog načina poslovanja u odnosu na njegove nedostatke.“[6]

Prednosti koje organizacije mogu imati od elektroničkog poslovanja su:

- Niski početni troškovi - Elektroničko poslovanje omogućuje globalno poslovanje i osvajanje novih tržišta bez velikih početnih troškova koji su bili potrebni u tradicionalnom poslovanju.“ Organizacije sada imaju pristup tržištu cijelog svijeta, velikom broju kupaca, dobavljačima ili partnerima na globalnoj razini. Primjer je internetska stranica www.airbnb.com“[7] kojoj je primarna djelatnost iznajmljivanje smještajnih kapaciteta turistima, te je veliki konkurent turističkim agencijama. Funkcionira na način da vlasnici sami stavljaju svoje smještajne kapacitete na stranicu kako bi se oglašavali, te kupci direktno komuniciraju sa vlasnicima ukoliko žele iznajmiti određenu smještajnu jedinicu. Ukoliko vlasnik iznajmi svoj apartman, Airbnb mu uzima određeni postotak od prodaje, dok se kupcu cijena poveća za određeni iznos. Obzirom da vlasnici apartmana gotovo sav posao odrađuju sami čime su Airbnb-u uvelike smanjeni troškovi, on ima privilegiju uzimanja manje provizije vlasniku stana kao i kupcu te su cijene smještajnih kapaciteta jeftinije nego kod klasičnih turističkih agencija, pa je Airbnb veliki konkurent klasičnim turističkim agencijama koje zbog svojih troškova nisu u mogućnosti prodavati svoje smještajne kapacitete po takvim cijenama.
- Smanjenje troškova poslovanja - Elektroničko poslovanje smanjuje troškove stvaranja, obrade, prikupljanja, prijenosa i pohrane papirnate dokumentacije.“ Hrvatski Telekom

[6] Spremić, M. (2004.): Menadžment i elektroničko poslovanje, Narodne novine, Zagreb, str. 117.
[7] Airbnb: Smještaj za odmor, domovi, doživljaji i mjesta, https://hr.airbnb.com/, 07.05.2019.

je uveo mogućnost dostave računa putem elektroničke pošte.2[8] Dakle, klasičan papirni račun koji bi se dostavljao poštom, zamijenjen je e-računom. Na taj način je Hrvatski Telekom smanjio svoje troškove poslovanja, kao što su troškovi poštarine primjerice, a smanjena je i potrošnja papira što pridonosi očuvanju prirodnih resursa, dok je korisnicima pojednostavljen način plaćanja računa. Korisnicima je račun dostupan u bilo kojem trenutku gdje god se nalazili, a da im je dostupan Internet, te su ga u mogućnosti platiti istog trenutka, bez čekanja redova u banci. Nakon plaćanja račun ostaje pohranjen u računalu.

- Mogućnost pokretanja diferencirane ili specifične vrste poslovanja - Putem Interneta je danas moguće kupiti gotovo sve, pa nema potrebe za dugotrajnim obilascima trgovina što predstavlja uštedu na vremenu.
- Smanjenje zaliha - Elektroničkim načinom poslovanja moguće je smanjiti zalihe gotovih proizvoda jer se pokušava poslovati prema zahtjevima kupaca koristeći "just in time" metodu. Putem Interneta je puno brže i jeftinije doći do korisničkih potreba i profila, što su informacije kojima započinje poslovni ciklus i na temelju kojeg se planira proizvodnja i ostale poslovne funkcije. Takav način poslovanja omogućuje proizvodnju proizvoda koji su potpuno prilagođeni potrebama i željama kupaca, što je tradicionalnim načinom poslovanja bilo skupo i ekonomski neopravdano.
- Reinženjering poslovanja - Primjena elektroničkog poslovanja znači i reinženjering poslovanja, promjenu temeljnih poslovnih procesa i moguće povećanje učinkovitosti. Time je moguće pojednostaviti procese, unaprijediti kvalitetu, ubrzati poslovanje, povećati produktivnost, smanjiti troškove, povećati fleksibilnost, poboljšati imidž, itd. Kao primjer navest ćemo banke koje su u zadnjih nekoliko godina znatno promijenile način svoj poslovanja primjenjujući informacijske i komunikacijske tehnologije u svoje poslovanje.

Koristi koje kupci mogu imati od elektroničkog poslovanja su:[9]

- 24 – satno radno vrijeme - Elektroničko poslovanje omogućuje kupcima neprekidnu dostupnost potrebnih poslovnih modela, provedbu poslovnih transakcija i dodatnih servisa. Kupac može u bilo koje doba dana kupiti željeni proizvod s određene internetske stranice, kupnja nije ovisna o radnom vremenu.

[8] Što je e-račun?, https://faq.hrvatskitelekom.hr/pages/category.xhtml?question=11537447, 07.05.2019.
[9]Prema: Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str. 49.

- Olakšana dostupnost i povećana mogućnost odabira proizvoda - Elektroničko poslovanje nudi kupcima mogućnost odabira prodavača, proizvoda, posrednika. Kupac ima mogućnost pregledati cijene određenog proizvoda na više različitih stranica, i u mjestima koje su udaljena od mjesta stanovanja, te na temelju usporedbe kupiti najpovoljniji proizvod, što bi u slučaju da se radi o tradicionalnom poslovanju bilo otežano i imalo bi dodatne velike troškove.
- Veća informiranost o proizvodima - Elektroničkim načinom poslovanja kupci su mnogo informiraniji, dostupne su im brojne informacije o proizvodima, sugestije, mišljenja ljudi koji su taj proizvod već rabili. Osim toga, elektroničko poslovanje omogućuje brzu isporuku kupljenih dobara (osobito mekih dobara odnosno digitalnih proizvoda). Na nekim stranicama moguće je ispod proizvoda pročitati komentare kupaca na taj proizvod, njihovu ocjenu proizvoda, i pouzdanost prodavača, osim toga na raznim internetskim forumima postoje rasprave o proizvodima.
- Interakcija među sudionicima tržišta - Elektroničko poslovanje omogućuje visoku razinu interakcije među sudionicima tržišta, pa se uz virtualne zajednice često provode i elektroničke dražbe između samih kupaca. Primjer je eBay. Kupci mogu licitirati za željeni proizvod koji je na taj način moguće kupiti ispod cijene.

Nedostaci elektroničkog poslovanja su:[10]

- Sigurnost - Sigurnost poslovanja na Internetu je vrlo ozbiljan problem, s obzirom na to da se svaki dan razvijaju novi virusi, te je potrebno posvetiti pažnju najboljim mjerama zaštite.
- Rizik zlouporabe - Postoji rizik zlouporabe jer podaci koje koriste pojedine tvrtke o svojim korisnicima su konstantno pod rizikom da ne dođu do neželjenih pojedinaca.
- Nepovjerenje – S obzirom da se radi o nečem novom s čime ljudi nisu u potpunosti upoznati te da komuniciraju sa strojevima, često se javlja manjak povjerenja u takav način poslovanja.
- Nedovoljna ili neprimjerena tehnološka infrastruktura – Korištenjem nedovoljne ili neprimjerene tehnološke infrastrukture kao preduvjeta za provedbu elektroničkog poslovanja može se značajno otežati sama izvedba ili čak onemogućiti. Dobra tehnološka infrastruktura omogućava neometan rad.

[10] Prema: Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str. 54.

- Tehnički zahtjevan prijelaz s postojećeg načina poslovanja na elektronički – Prijelaz na elektroničko poslovanje zahtjeva određenu infrastrukturu te je za nju potrebno izvršiti određene prilagodbe da se prijeđe na novi način poslovanja. Takve prilagodbe zahtijevaju dosta resursa.
- Troškovi razvoja elektroničkog načina poslovanja – Takav način poslovanja zahtjeva određene promjene, te opremu i nova znanja koja sa sobom povlače i određene troškove, za čiji povrat će morati proći određeno vrijeme.
- Privatnost, zaštita autorskih prava – u elektroničkom poslovanju mnogi se podaci drže u elektroničkom obliku, te se šalju putem Interneta, zbog toga su podložni zloupotrebi te je potrebno poduzeti određene mjere kako bi se podaci zaštitili.
- Nedostatak stručnog osoblja i znanja – elektroničko poslovanje uvodi mnoge nove tehnologije na svim razinama dosadašnjeg poslovanja, pa je potrebno uložiti u edukaciju osoblja kako bi se nadoknadilo dotadašnje nepoznavanje potrebnih tehnologija.
- Rizik nastanka materijalne štete – jedan od rizika je i nastanak kvarova ili uništenja opreme za provođenje elektroničkog poslovanja uslijed određenih nepogoda, što može proizvesti ogromne troškove i potpuno onemogućiti poslovanje.

Iz prethodno nabrojenih prednosti odnosno nedostataka, vidljivo je da prednosti upotrebe elektronskog poslovanja uvelike prelaze nedostaci. Navedene prednosti govore kako je uvođenje informatičkih tehnologija u poslovanje značajno doprinosi njegovoj kvaliteti te efikasnosti. Unatoč nezanemarivoj brojki nedostataka, uvođenje elektronskog poslovanja poželjno, ali njemu treba pristupiti s oprezom, imajući u vidu nedostatke. Potreban je kontinuiran rad na pronalaženju načina kako ih izbjeći ili smanjiti na najmanju moguću mjeru.

2.2. Povijest elektroničkog poslovanja

Razvoju elektroničkog poslovanja prethodio je nastanak Interneta bez kojeg ne bi mogli govoriti o elektroničkom poslovanju. Internet je nastao u SAD-u, kao projekt pri ministarstvu obrane Sjedinjenih Američkih Država, a u ranim sedamdesetim godinama 20.stoljeća seli se u Europu. U samom početku njime su se koristile uglavnom vladine institucije, da bi u vrlo kratkom vremenu ekspandirao i postao neizostavan u svim segmentima društva. U cijelom svijetu 1992.godine umreženo je više od milijun većih računala.[11]

[11] Prema: Spremić, M. (2004.): Menadžment i elektroničko poslovanje, Narodne novine, Zagreb, str.31.

Primjena Interneta kao infrastrukture poslovanja dovodi do širenja poslovanja izvan granica kompanija, omogućavajući razmjenu informacija, znanja i sadržaja. Udaljenost je prestala biti presudan faktor u poslovanju, a globalno je tržište postalo mjesto za tržišno natjecanje. Elektroničko poslovanje donijelo je povećanje brzine i reakcija tvrtki na globalne promjene.

Sadašnji trendovi ukazuju da se ekonomija sve više seli na Internet, koji više nije samo mreža za povezivanje nego je i poslovno okruženje i osnovni generator novog razvoja. Putem Interneta, djelatnost, proizvod ili usluga kompanije obilaze cijeli svijet. Pored Interneta, razvoj elektroničkog poslovanja danas je uvjetovan i razvojem mobilnih i satelitskih komunikacija, kao i programskih aplikacija koji ga prati i podržava. Menedžmentu je trebao samo trenutak da uvidi sve njegove prednosti u obavljanju gospodarskih odnosno poslovnih aktivnosti. Internet postaje najveće svjetsko tržište, novi prostor na kojem se trguje robom, uslugama, kapitalom, radom i informacijama.

Razvoj elektroničkog poslovanja može se promatrati kroz šest faza:[12]

- U početnoj fazi Internet je bio sredstvo distribucije informacija i sadržaja u obliku kataloga gdje su tvrtke objavljivale informacije o proizvodima i uslugama koje su nudile potrošačima. Te su informacije bile statističke, a jedina komunikacija im je bila putem elektroničke pošte ili često postavljenih pitanja.
- Drugu fazu karakterizira to da razvoj i upravljanje web mjestima preuzimaju informatičari koji Internet i web tehniku koriste za razvoj intraneta – mrežnu povezanost internih korisnika koja omogućuje sigurnu razmjenu informacija i obavljanje radnji vezanih za organizaciju.
- U trećoj fazi korištenje web mjesta postaje znatno lakše i intuitivnije, dodaju se brojne nove usluge u svrhu proširenja odnosa s krajnjim korisnicima kao što su pretraživanje i narudžba proizvoda ili usluga, plaćanje i isporuka. Ovakvo poslovanje prema kupcima znatno ubrzava poslovanje i njegovu učinkovitost a ujedno smanjuje troškove. Rukovodstvo firmi sve se više bavi strategijama unapređenja elektroničke trgovine, kako se postaviti prema tradicionalnom načinu trgovanja, kako privući nove kupce, kako formirati cijene. Težište razvoja nije više samo tehnološki razvoj već su to i suštinske organizacijske promjene.

[12] Prema: Spremić, M. (2004.): Menadžment i elektroničko poslovanje, Narodne novine, Zagreb, str. 33 - 38.

- Mnoge tvrtke koje su ušle u elektroničko poslovanje bez dobro razrađenih modela elektroničkog poslovanja i kupcima nudili obećanja koja nisu mogli izvršiti, izgubili su povjerenje svojih kupaca. Kupci koji nisu dobili proizvod na vrijeme ili su dobili neodgovarajući, ne mogu pratiti status pošiljke ili slično osjećaju se prevareno. Ključni zadaci u četvrtoj fazi su reinženjering poslovnih procesa kako bi se prilagodili novim uvjetima.
- U petoj fazi veliki se značaj pridaje temeljitoj razradi i razvoju novog poslovnog modela u dinamički i poduzetnički. Poslovne transakcije se prate i analiziraju u realnom vremenu što dovodi do brzog i trenutnog odlučivanja. U menadžment se biraju ljudi koji su informacijski pismeni i vladaju novim tehnologijama te imaju znanja iz poslovnog upravljanja.
- Rekonstruiranje poslovanja je provedeno, nova ekonomija je postala uobičajen i jedino moguć način poslovanja, tako da se prefiks e – elektroničko može izostaviti. Konkurencija je velika, potrebna su stalna usavršavanja, poboljšanja i učenja te implementacija inovacija, kako menedžera tako i svakog zaposlenika. Brzina razvoja te prepoznate beneficije e-poslovanja dovode do pojma nove ekonomije - nove ekonomske ere. Neki je još nazivaju i informacijskom erom. Kako god je nazvali, očito je da su time pomaknute granice i pravila tradicionalnih načina poslovanja.

Nemoguće je predvidjeti tok tog brzo rastućeg medija. Potrošači će sve više tražiti web mjesto u zamjenu za fizičkim prostorom. Zbog neograničenog prostora i vremena, kompanije će analizirati i pronalaziti sve novije i novije modele koji će im donijeti maksimalnu dobit. Tvrtke koje nude najpouzdanije, najfunkcionalnije i najbrže usluge, usluge 24 sata na dan, sedam dana u tjednu, imaju najveće izglede za uspjeh.

2.3. Modeli elektroničkog poslovanja

Sudionici poslovnih ili uslužnih transakcija koje se obavljaju elektroničkim putem su poduzeća, tijela državne uprave i administracije, kupci ili klijenti, te građani. „Ovisno o tome tko su sudionici poslovnih transakcija ili pružanja i primanja usluga na koje se primjenjuje neki oblik elektroničkog poslovanja, postoji nekoliko modela, a najznačajniji su:“[13]

[13] Garača, Ž. (2008.): Poslovni informacijski sustavi, Ekonomski fakultet, Split, str. 148. – 152.

- **„Business-to-Business (B2B)/ e – poslovanje među poduzećima**. Ovdje se radi o poslovanju između dva poduzeća. U ovom slučaju primjerice poduzeća kroz međusobno komuniciranje putem Interneta nastoje smanjiti svoje troškove. „[14]
- **„Business-to-Consumer (B2C)/ e - poslovanje s potrošačima**. Ovdje se radi o obavljanju poslovnih transakcija s krajnjim korisnicima, kupcima ili klijentima ovisno o djelatnosti. Uglavnom se odnosi na e- prodaju, odnosno prodaju vlastitih proizvoda, dobara i usluga, ali i na sve druge vrste poslovanja, posebice e–trgovine i e–marketinga. Ovaj model je najrasprostranjeniji u e–poslovanju. Ovaj model poslovanje daje korisnicima mogućnost izvršavanja određenih radnji poput kupovine proizvoda ili plaćanja računa iz udobnosti vlastitog doma. Ujedno ima koristi i za poduzeća koja smanjuju svoje troškove nudeći proizvode ili usluge tim putem.“[15]
- **„Consumer-to-Consumer (C2C)/ e – trgovanje među potrošačima**. Model koji podrazumijeva direktno elektroničko poslovanje među krajnjim korisnicima uz potporu elektroničkih posrednika. Ovdje se najčešće radi o aukcijama, za što je najbolji primjer eBay. Princip funkcioniranja aukcija je jednak klasičnim aukcijama.“[16]
- **„Government-to-Business (G2B)/ e – poslovanje između državnih tijela i poduzeća.** „Model koji obuhvaća infrastrukturu koja omogućava pružanje različitih servisa i provođenje različitih poslovnih transakcija između poslovnih sustava i državnih tijela. Primjer je e-carina koja omogućava razmjenu elektroničkih dokumenata potpisanih elektroničkim potpisom između gospodarstvenika i carine.“[17]
- **„Government-to-Citizen (G2C)/ e – poslovanje između državnih tijela (administracije) i građana**. Model koji predstavlja sve vrste servisa i elektroničkih komunikacija između državnih tijela, odnosno javne uprave i građana. Neki od primjera su mogućnost upisa na fakultet elektroničkim putem. Zatim Hrvatski zavod za zapošljavanje na svojim stranicama objavljuje informacije o slobodnim radnim mjestima, što omogućava traženje posla putem Interneta.“[18]

[14]Ružić, D. (2003): E – marketing, Ekonomski fakultet u Osijeku, Osijek, str. 203.
[15]Business-to-Consumer, https://www.investopedia.com/terms/b/btoc.asp, Will Kenton, 09.05.2019.
[16]What is C2C?, https://www.businessnewsdaily.com/5084-what-is-c2c.html, Andreas Rivera, 09.05.2019.
[17]What is Government-to-Business (G2B), https://www.igi-global.com/dictionary/government-to-business-g2b/12391, 10.05.2019.
[18] G2C (Government to Citizen), https://managementmania.com/en/g2c-government-to-citizen, 10.05.2019.

„Svaki od navedenih sudionika može istovremeno igrati više uloga ili u vremenu mijenjati svoju ulogu u odnosu na druge sudionike.“[19]

2.4. Značaj elektroničkog poslovanja

Broj organizacija koje razumiju važnost elektroničkog poslovanja u stalnom je porastu, pa je za očekivati da će prefiks e- u dalekoj budućnosti biti nepotreban, jer će takvo poslovanje biti jedino prihvatljivo, a to je i vidljivo u šestoj fazi u korištenju usluga elektroničkog poslovanja. Činjenica je da elektroničko poslovanje utječe na svaku poslovnu organizaciju, i nemoguće je sakriti njegov utjecaj na moderno tržište koje je izuzetno podložno promjenama. Radi toga je izgradnja organizacije fleksibilne na promjene, jedan od mogućih aspekata razvoja i implementacije elektroničkog poslovanja u kojemu bi najvažnije karakteristike mogle biti fleksibilnost i skalabilnost. Kako bi se to postiglo potrebno je razvijati poslovne procese u skladu s realnim proizvodnim i operativnim postupcima tvrtke i preslikati ih u elektronički oblik.

Trenutno je najveći udio primjene elektroničkog poslovanja u domeni elektroničke trgovine, gdje je izazvalo promjenu koncepta poslovanja i utjecaja na sudionike, kojima postupak trgovine, kupnje, prodaje više nije ovisan o vremenu i mjestu, što znači da kupci i korisnici mogu odabrati vrijeme po svojoj volji i obavljati kupovinu koristeći prednosti modernog ekonomsko — tehnološkog okruženja Elektronička trgovina je virtualan svijet kojeg određuju dostupnost, raspoloživost i pouzdanost infrastrukture i tehnologije kao okosnice. Proizvod distribuiran kroz modemi model poslovanja je znatno jeftiniji, nego isti proizvod plasiran kroz tradicionalni model poslovanja.[20]

Osim utjecaja na direktne sudionike tržišta stvara se i domino efekt na podržavajuće sudionike elektroničke trgovine, financijske institucije koje omogućuju prijenos sredstava između partnera u komercijalnom procesu, logističke lance zadužene za prijevoz robe do odredišta, poštanske agencije za usmjeravanje isporuke itd. Također, česta primjena funkcionalnosti e-poslovanja su različiti oblici transakcija kao što je na primjer plaćanje putem Interneta, koje rezultira drastičnim smanjenjem šalterskog poslovanja i značajnim uštedama dugoročno. Za zaključiti je da elektroničko poslovanje već sada svoju primjenjivost u svakom segmentu

[19] Garača, Ž. (2008.): Poslovni informacijski sustavi, Ekonomski fakultet, Split, str.148. – 152.
[20] Prema: Severović, K. (2013.): Upravljanje odnosima s klijentima kao izvor informacija za oblikovanje i poboljšanje usluga, Fakultet organizacije i informatike, Varaždin,str.242.

društvene zajednice, a u najvećoj mjeri pronalazi u B2B (business-to-business) tipu, ako uzmemo u obzir kriterij vrijednost ulaganja, vrijednosti transakcija, i sveukupno sudeći prema globalnoj orijentiranosti na profit.Elektronička trgovina, na primjer, mijenja kanale kojim su kupci i dobavljači tradicionalno trgovali, dobavljačima je pristup tržištu omogućen uz minimalnu infrastrukturu i značajno manje troškove. Novim poduzetnicima je mnogo lakše pokretati poslovne poduhvate, nego u slučaju tradicionalnog poslovnog modela.

Obujam elektroničke prodaje na svjetskoj razini mjeri se u trilijunima dolara. Tvrtka eBay specijalizirana za online prodaju ima godišnji prihod od oko 9.7 milijardi dolara, a na europskom tržištu prihodi od e-trgovine su 2017. godine iznosili ukupno 321.796 milijuna dolara.“ U Hrvatskoj, 14% web trgovaca je 2017. godine imalo prihode veće od tri milijuna kuna (14%).“[21]

[21] Elektroničko poslovanje, https://www.datalab.hr/elektronicko-poslovanje-kako-sto-gdje/, 11.05.2019.

3. TEMELJNE ODREDNICE ELEKTRONIČKOG BANKARSTVA

Banka je organizacija koja bez primjene informacijske i komunikacijske tehnologije ne bi mogla uspješno poslovati ni opstati na tržištu. To je razlog što će ova vrsta elektroničkog poslovanje biti detaljnije objašnjena.

3.1. Pojmovno određenje elektroničkog bankarstva

Elektroničko bankarstvo predstavlja primjenu koncepta elektroničkog poslovanja pri obavljanju svih bankarskih poslova, a ostvaruje se na dvije tehnološke razine, kao samoposlužno i kao internetsko bankarstvo.[22] Samoposlužno bankarstvo odnosi se na one usluge banaka koje dopuštaju korisniku da ih koristi ne ulazeći u prostorije banke, pod to spada primjerice korištenje bankomata, plaćanje karticama. S druge strane internetsko bankarstvo podrazumijeva da se korištenje uslugama banaka odvija putem Interneta, na što se odnose sve usluge koje se mogu koristiti internetskim i mobilnim bankarstvom, primjerice plaćanje računa putem Interneta, provjera stanja na računu, ugovaranje štednje.

Elektroničko bankarstvo omogućuje poslovanje između banaka, između banaka i njihovih komitenata te između komitenata banaka, bez da je korisnik primoran posjetiti poslovnicu banke, te je izostavljena i papirna dokumentacija. Takvom vrstom poslovanja omogućeno je korištenje uslugama banaka putem bankarskog web mjesta što donosi brojne prednosti kao što su ušteda vremena i novca.“ E-bankarstvo danas karakterizira primjena Interneta i web servisa za obavljanje financijskih transakcija. Web mjestu banke korisnici pristupaju koristeći standardne internetske alate.“[23]

Ovisno o tome u kojoj mjeri banke koriste informacijske i komunikacijske tehnologije u poslovanju imamo podjelu na hibridne i virtualne banke. Hibridne – to su banke koje posluju na klasičan način, u svom poslovanju koriste Internet kao dodatni kanal za pružanje usluga klijentima. Poslovnice banaka postoje i u njima se pružaju bankarske usluge, ali je klijentima dana mogućnost da gotovo sve usluge banaka ukoliko žele mogu obavljati putem Interneta ili samoposlužnih uređaja. Takve banke prevladavaju danas. „Virtualne – to su banke koje pružaju bankarske usluge isključivo elektroničkim putem. One ne postoje u fizičkom obliku,

[22] Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str. 17.
[23] Garača, Ž. (2008.): Poslovni informacijski sustavi, Ekonomski fakultet, Split, str. 155.

nemaju nekretnine i imaju mali broj zaposlenih. Takve banke su u manjini, s obzirom da ljudi teže stječu povjerenje u takav način poslovanja.“[24]

3.2. Povijesni razvoj elektroničkog bankarstva

„Postoji određeni put razvoja od klasičnog načina poslovanja banaka do ovog kojeg danas poznajemo i koji koristi moderne tehnologije u svom poslovanju. U nastavku će faze razvoja od uviđanja potrebe za uvođenjem novih tehnologija u poslovanje do izmjene načina poslovanja biti detaljnije objašnjene:“[25]

1.faza – inicijativa,
2. faza – interaktivnost,
3. faza – personalizacija,
4. faza – virtualizacija,
5. faza – pokretljivost.

Prvu fazu karakterizira spoznaja da primjena informacijske tehnologije može doprinijeti kvalitetnijem poslovanju banke. One imaju utjecaj na produktivnost radnika, primjerice smanjuje se količina papirologije koja dovodi do zamora radnika te se on može fokusirati na kreativnije rješavanje problema čime raste njegovo zadovoljstvo pa samim time postaje produktivniji od čega i banka ima koristi. Banka postaje konkurentnija, moguće je ponuditi kvalitetniju uslugu, smanjuju se troškovi banaka, klijenti su zadovoljniji uslugom.

U fazi interaktivnosti mijenja se filozofija poslovanja banaka, dok je prije klijent bio primoran posjetiti poslovnicu banke kako bi obavio određenu transakciju, sada je banci cilj ponuditi klijentu svoje usluge na način da ih on obavlja iz udobnosti vlastitog doma uz uvjet da posjeduje računalo, čime se povećava zadovoljstvo korisnika, a ujedno i banaka smanjenje troškove.

U trećoj fazi kada je već bitan broj klijenata prihvatio novi način pružanja usluga od strane banke dolazi potreba za razvojem načina pružanja usluga kroz Internet bankarstvo kako bi usluga što bolje odgovarala specifičnim potrebama njegovih korisnika te kako bi se smanjio

[24] Ibidem.
[25] Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str. 60 - 61.

otpor korisnika prema takvom obliku pružanja usluge. Tako primjerice imamo Internet bankarstvo za fizičke i pravne osobe.

U četvrtoj fazi se javlja ideja o stvaranju virtualnih banaka, što znači da banke prestaju postojati u fizičkom obliku, te se pojavljuju isključivo na webu. Jedina mogućnost interakcije s bankama je putem Interneta.

Zadnja faza je vezana uz ekspanziju pokretnih (mobilnih) tehnologija i uređaja. Klijentima je omogućeno koristiti usluge banaka i na vlastitim mobilnim uređajima, tako da su im bankarske usluge dostupne u svakom trenutku, gdje god se nalazili.

3.3. Usluge elektroničkog bankarstva

U ovom poglavlju bit će opisane najvažnije i najkorištenije usluge elektroničkog bankarstva. U to se ubrajaju: bankomati, kartično poslovanje, Electronic Fund Transfer at Point Of Sale EFT/POS, Internet bankarstvo i mobilno bankarstvo.

3.3.1. Bankomati

„Bankomat jest elektromehanički uređaj koji omogućuje korisnicima platnih instrumenata podizanje i/ili polaganje gotovog novca, prijenos sredstava, korištenje usluge davanja informacija o stanju na transakcijskom računu i drugih usluga.“[26]

„Prvi bankomat postavljen je 27. lipnja 1967. godine u banci u sjevernom Londonu, a izumiteljem se smatra John Shepherd-Barron**.**No, prvi kojem je palo na pamet uzimati novac sa svog računa pomoću stroja bio je Luther George Simjian, američki izumitelj armenskih korijena, 1939. godine. Njegovom idejom oduševila se banka *Citicorp* i ponudila tu uslugu svojim klijentima.“[27]

„Prvi bankomat u Hrvatskoj 1984., podsjetimo, ugradila je tadašnja Riječka (a današnja Erste banka) u središtu Rijeke.“[28]

[26] Infrastruktura, https://www.hnb.hr/statistika/statisticki-podaci/platne-usluge/infrastruktura, 14.05.2019.
[27] 50. obljetnica bankomata, https://www.24sata.hr/fun/50-obljetnica-bankomata-zanimljivosti-koje-niste-znali-529581, Sanjin Strukić,14.05.2019.
[28] U pet godina udvostručena mreža bankomata, https://lider.media/arhiva/63823/,,Nikola Prskalo, 14.05.2019.

„Elektronički uređaj omogućava klijentu banke korištenje određenih usluga banke poput podizanja gotovine, provjeravanja stanja na računu, uplate gotovine. Osim toga je pogodan i za prodaju nekih elektroničkih usluga, npr. GSM bonova. Aktiviraju se magnetskom ili čip karticom, te unosom osobnog identifikacijskog broja.“[29]

Klijentima se nudi mogućnost korištenja određenih usluga banaka i u vrijeme kada poslovnice banke ne rade. Mogu biti postavljeni na različitim mjestima te nisu vezani uz lokaciju poslovnice banke. Iako je bankomat pogodan za pružanje različitih usluga, bitno je ne preopteretiti ga, tj. da on sačuva svoju osnovnu uslugu koja je isplata gotovine, jer će prevelikim opterećenjem zbunjivati korisnike, stvarat će se redovi, te će oni koji trebaju njegovu osnovnu funkciju čekati poput klijenata za šalterom da dođu na red.

Vrsta uređaja	Obilježje uređaja	na dan 31.03.2019.
	Beskontaktni	
	Kontaktni	5.498
	Beskont. - kontaktni	498
BANKOMAT	Drive-in	9
	S videonadzorom	1.617
	U osigur. prostoru	596
	UKUPNO	5.996

Tablica 1. Broj bankomata u Republici Hrvatskoj

Izvor: https://www.hnb.hr/documents/20182/b6b74739-e1f9-61b8-78a9-c9fbe817ca67

„Zagrebačka banka drži najveći tržišni udio u Hrvatskoj po veličini bankomatske mreže koja broji preko 858 bankomata. Iako je najveći broj bankomata u gradu Zagrebu i Zagrebačkoj županiji, dobra je rasprostranjenost bankomata i u ostalim regijama Hrvatske, odgovaraju. Tako se oko 30 posto ukupnog broja bankomata nalazi u županijama na obali, Istra, Kvarner, Dalmacija, s ciljem zadovoljavanja potreba turista te velikog broja domaćih korisnika koji tijekom godine odmaraju uz obalu.“[30]

Danas u svijetu ima oko 3 milijuna bankomata, a procjenjuje se da će ih do 2020. biti milijun više. Najviše bankomata na milijun stanovnika na području zapadne Europe ima Portugal -

[29] Tomašević Lišanin, M. (1997.): Bankarski marketing, Informator, Zagreb, str 102.
[30] Rasprostranjenost važna kod odabira banke, http://www.poslovni.hr/hrvatska/rasprostranjenost-vazna-kod-odabira-218466, 14.05.2019.

1540. Velika Britanija ih ima 1074, a europski je prosjek 960.“ Najmanji broj bankomata na milijun stanovnika u Europi ima Švedska, tek 333. Zanimljivo, dva bankomata se nalaze na Antarktici, i to u istraživačkom centru McMurdo. U Vatikanu možete dobiti instrukcije na latinskom, dok u indijskim hramovima možete ubaciti svoje donacije u bankomate.“[31]

Bilo bi čudno kada se Ujedinjeni Arapski Emirati ne bi isticali, pa tako u Dubaiju i Abu Dhabiju bankomati raspolažu sa zlatnim polugama i kovanicama.“ Prvi *drive-in* bankomat, odnosno bankomat s kojeg možete podići novac iz vozila, postavljen je u Velikoj Britaniji, u blizini londonske zračne luke Heathrow. Španjolci, pak, na bankomatima nude opciju kupovanja sportskih karata i plaćanja kazni za parkiranje.“[32]

3.3.2. Kartično poslovanje

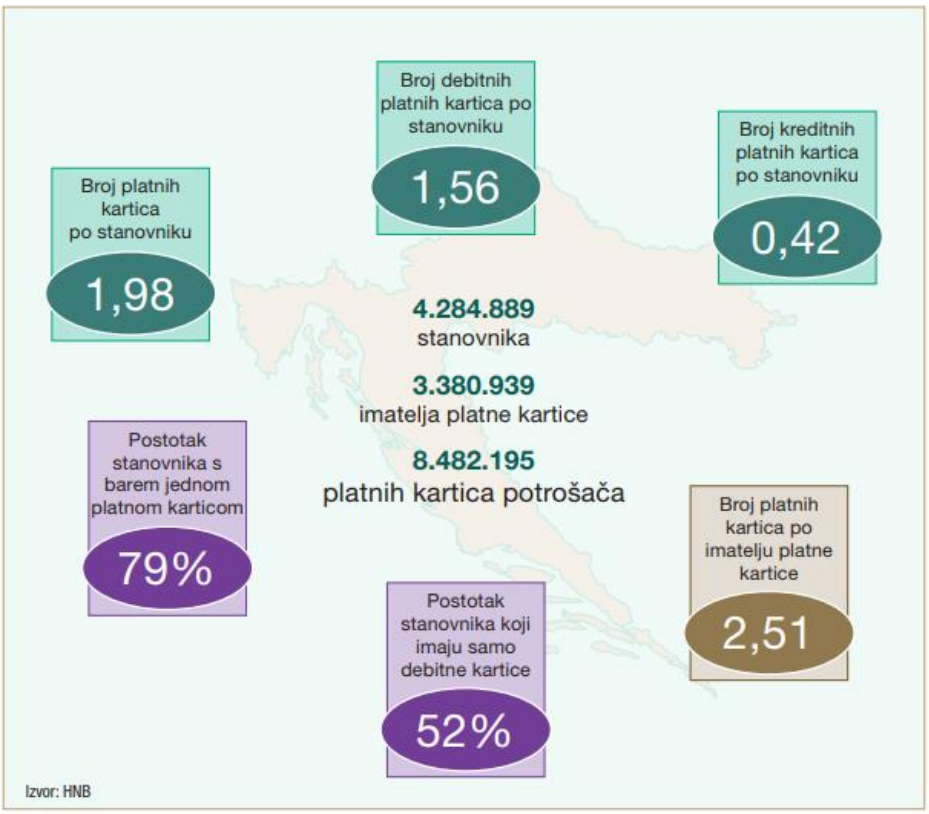
„Plastični novac ili kreditne i debitne kartice nastao je u SAD – u polovicom prošlog stoljeća i za samo nekoliko desetljeća se proširio na cijeli svijet.“[33]

Kartica ili bankovna kartica je plastična kartica sa magnetnom trakom koja sadrži strojno čitljiv identifikacijski broj i izdana je od strane banke ili kartičarske kuće.“ Bankovne kartice koriste za elektronsko poslovanje na POS terminalima- ili Internet te za bankarske transakcije putem bankomata.“[34] Debitna kartica se koristi za bezgotovinska plaćanja koja se pokrivaju onom količinom novca koja se nalazi na računu. Kreditna kartica se koristi za bezgotovinska kreditna plaćanja, što znači da korisnik može platiti kasnije.

Banka s korisnikom ugovara maksimalni iznos koji može potrošiti kreditnom karticom. Svrha ovog uvođenja bila je povećanje djelotvornosti banke u pružanju kreditnih i depozitnih usluga, povećavajući broj mjesta na kojima je moguće dobiti te usluge.[35] Osim prednosti koje korištenje kartice donosi korisniku kao što je odgoda plaćanja, te jednostavnost kupovine,

[31] 50. obljetnica bankomata, https://www.24sata.hr/fun/50-obljetnica-bankomata-zanimljivosti-koje-niste-znali-529581, Sanjin Strukić,14.05.2019.
[32] Ibidem.
[33] Rončević, A (2006.): Nove usluge bankarskog sektora:razvitak samoposlužnog bankarstva u Hrvatskoj, Ekonomski pregled, 11, Zagreb, str. 756.
[34] Kartice, http://www.moj-bankar.hr/Kazalo/K/Kartice, 15.05.2019.
[35] Prema: Bašić, R. (2006.): Primjena tehnoloških inovacija i elektroničkog plaćanja u hrvatskom bankarstvu, Ekonomski fakultet, Rijeka, str. 125.

neke od neugodnosti korištenja karticama su kvarovi na uređajima koji omogućavaju plaćanje karticama.[36]



Slika 1. Zastupljenost platnih kartica potrošača u RH na dan 31. prosinca 2017.

Izvor: https://www.hnb.hr/documents/20182/2504205/h-pkkt_2017.pdf/1fb88d57-d0d8-41c8-b3b7-2bf9df5a29b9

„Na dan 31. prosinca 2017. ukupan broj imatelja platnih kartica potrošača koji imaju debitnu karticu iznosio je 3.365.680, odnosno 79% stanovništva RH ima barem jednu debitnu karticu. Nadalje, broj imatelja koji imaju samo debitnu karticu na dan 31. prosinca 2017. iznosio je 2.233.941, odnosno 52% stanovništva RH ima samo debitnu karticu, tj. ne posjeduje kreditnu karticu. Ukupan broj imatelja platnih kartica potrošača koji imaju kreditnu platnu karticu jest 1.146.998 ili 27% stanovništva RH.“[37]

[36]Prema: Severović, K. (2013.): Upravljanje odnosima s klijentima kao izvor informacija za oblikovanje i poboljšanje usluga, Fakultet organizacije i informatike, Varaždin, str. 250.
[37]Platne kartice i kartične transakcije, https://www.hnb.hr/documents/20182/2504205/h-pkkt_2017.pdf/1fb88d57-d0d8-41c8-b3b7-2bf9df5a29b9, 18.05.2019.

Najčešće korišten platni instrument u Republici Hrvatskoj je platna kartica i upravo je na tržištu platnih kartica i kartičnih plaćanja zabilježen stalan rast i razvoj. Jedanaest godina je broj nacionalnih kartičnih platnih transakcija porastao za 100%, i to s 203,68 milijuna koliko ih je izvršeno u 2006. godini na 407,39 milijuna koliko ih je izvršeno u 2017. godini.“ Nadalje, u istom razdoblju vrijednost nacionalnih kartičnih platnih transakcija porasla je za 64%, i to s 85.331,34 milijuna kuna na 140.198,53 milijuna kuna. S obzirom na rast kartičnih plaćanja i sve brojnije alternativne metode plaćanja, budućnost gotovog novca postala je aktualna tema. Prema statističkim podacima 86,1% broja fiskaliziranih računa u RH odnosi se na plaćanje gotovinom, dok se na plaćanja karticama odnosi 12,5%. Kada se gleda vrijednost fiskaliziranih računa, 56,1% vrijednosti odnosi se na plaćanje gotovim novcem, a 37,2% vrijednosti na plaćanja karticama.“[38]

3.3.3. EFT/POS

„EFTPOS uređaj (engl. Electronic funds transfer at point of sale) elektronički je uređaj koji omogućuje imateljima platnih kartica iniciranje kartičnih platnih transakcija na prodajnom mjestu.“[39]

EFTPOS uređaji se mogu podijeliti na kontaktne i beskontaktno-kontaktne. „Kontaktni EFTPOS uređaji podržavaju prihvat platnih kartica koje sadržavaju zapise temeljene samo na čipu i/ili magnetnoj traci. Beskontaktno-kontaktni EFTPOS uređaji podržavaju prihvat platnih kartica koje, osim zapisa temeljenog na magnetnoj traci i/ili čipu, sadržavaju i zapise temeljene na beskontaktnoj tehnologiji (blizinsko čitanje kartice, NFC i slično).“[40]

EFTPOS uređaj za isplatu i uplatu je uređaj koji imateljima platnih kartica omogućuje iniciranje samo platnih transakcija podizanja i/ili polaganja gotovog novca platnom karticom. Taj uređaj je najčešće smješten u prostorijama treće osobe koja na osnovi ugovora radi u ime i za račun pružatelja platnih usluga (npr. Financijska agencija, Hrvatska pošta i sl.).“ Na dan 31. prosinca 2017. ukupno je evidentirano 905 EFTPOS uređaja za isplatu i uplatu, dok ih je na dan 31. prosinca 2016. ukupno evidentirano 936. Smanjenje broja EFTPOS uređaja za

[38]Platne kartice i kartične transakcije, https://www.hnb.hr/documents/20182/2504205/h-pkkt_2017.pdf/1fb88d57-d0d8-41c8-b3b7-2bf9df5a29b9, 18.05.2019.
[39] Ibidem.
[40] Ibidem.

isplatu i uplatu tehnološko je unapređivanje dijela uređaja na kojima je osim uplata i isplata omogućena kupnja robe i usluga te su ti uređaji svrstani u EFTPOS uređaje."[41]

3.3.4. Internet bankarstvo

Banka je financijska institucija koja se bavi novcem, te stoga treba efikasnu tehnologiju obrade podataka. Praćenje novca banke obavlja se preko raznih vrsta računa (tekući računi, žiro računi, računi oročitelja, kreditni računi...) čiji se podaci nalaze pohranjeni u bazi podataka informacijskog sustava. Osim toga cilj banaka je prikupiti što više podataka o klijentu kako bi mu mogli ponuditi uslugu namijenjenu njegovim potrebama. Na temelju prikupljenih podataka banka je u mogućnosti ponuditi klijentima određene pogodnosti (npr. studenti imaju niže cijene korištenja usluga banaka, ili mu ponuditi štednju koja će odgovarati njegovim mogućnostima i željama) čime doprinosi zadovoljstvu klijenata. Poslovanje banke odvija se kroz brojne financijske transakcije, koje su ujedno i transakcije informacijskog sustava. To pokazuje važnost sustava za obradu transakcija čija je uloga da evidentira svaku transakciju i aktualizira stanja na računima, za što je potreban dobar te računalom podržan informacijski sustav. Klijent banke može svoje transakcije obavljati putem internetskog bankarstva, time znatno pojeftinjujući cijenu transakcije. Klasična transakcija obavljena na šalteru poslovnice je najskuplja, internetska transakcija obavljena tzv. internetskim bankarstvom je jeftinija od šalterske. Razlog tome je što internetsku transakciju obavlja sam klijent na svom računalu pa banka ne troši niti svoje ljude niti svoju tehniku. Banka stimulira transakcije obavljene putem Interneta smanjenjem naknada za tako obavljene transakcije kako bi se što više ljudi odlučilo na obavljanje transakcija tim putem jer one donose banci veći prihod obzirom na gore navedeni razlog.[42]

Internet bankarstvo je bankovni informatički servis namijenjen svim pravnim ili fizičkim osobama koje imaju otvoren račun bilo koje vrste u banci (osim stare tradicionalne štedne knjižice) kako bi mogle u bilo koje vrijeme imati uvid i kontrolu nad svojim financijama, također služi za bezgotovinsko plaćanje bez bankovnog posrednika, odnosno front office-a banke. Takva se osoba (fizička ili pravna) naziva korisnikom. Korisnik prethodno korištenju Internet bankarstva mora zatražiti zahtjev za korištenje Internet bankarstva i mora pristati na opće uvjete korištenja usluge Internet bankarstva. Korisniku nije potreban specijalan software i podaci sa servisa se ne spremaju na korisnikov hard disc. „Pristup banci i računu je moguć s

[41] Ibidem.
[42] Prema: Panian, Ž. i sur. (2010.): Poslovni informacijski sustavi, Element, Zagreb, str. 133 – 135.

bilo kojeg mjesta u svijetu 365 dana u godini, 24 sata dnevno. Banka brine o održavanju servisa, odnosno cijele mreže. Takvu vrstu usluge banke najčešće naplaćuju kroz naknadu za vođenje računa.“[43]

„Kada je riječ o korisnicima Internet bankarstva u Republici Hrvatskoj u 2017. godini, struktura je sljedeća:

- 1.241.414 korisnika internetskog bankarstva
- 183.262 korisnika internetskog bankarstva – poslovni subjekti.“[44]

Internet nudi bankama velike mogućnosti zarade iako se još uvijek globalna mreža uglavnom koristi u promotivne svrhe. Internet bankarstvo je najjeftiniji oblik bankarskih usluga, dostupan 24 sata dnevno, praktično bez prostorne ograničenosti. Glavni ograničavajući faktori, koji uvjetuju pristanak klijenta na ovu vrstu tehnologije, su sigurnost i privatnost. Sa tehničke točke gledišta, ovaj problem su neke banke već riješile, ali ostaje činjenica da je ponašanje klijenata vođeno prije potrošačkom percepcijom nego tehničkim činjenicama. Neprihvaćanje da se bankarske transakcije obavljaju preko Interneta postoji prije svega iz straha da ključne financijske informacije budu otkrivene. Jasno su vidljive razlike između Internet bankarstva i on-line bankarstva. Osnovna razlika je u ugradnji specijalnih softverskih programa, koji ograničavaju korisnika na obavljanje usluga isključivo s računalom u koji je ugrađen odgovarajući software. Razlike su i u stupnju sigurnosti pri obavljanju transakcija, zatim u novcu potrebnom za kupovinu i ugradnju programa i vremenu potrebnom za obuku korisnika. Spomenuti razlozi jasno ukazuju da je Internet bankarstvo praktičniji, ekonomičniji i sigurniji način obavljanja bankarskog poslovanja direktno iz kuće.

3.3.5. Mobilno bankarstvo

Mobilno bankarstvo je način obavljanja bankarskih aktivnosti pomoću mobitela. Tu nije potreban token za potvrdu transakcija, nego je softverski token ugrađen u samu aplikaciju. Gotovo sve ono što omogućava Internet bankarstvo, omogućava i mobilno, s tim da mobilno bankarstvo ima dodatnu prednost što je pristup mobitelom puno jednostavniji i brži. Prema mnogim istraživanjima bankarstvo putem mobitela je jedno od najbržih rastućih tržišta na svijetu.

[43] Poslovanje budućnosti, http://manager-magazine.com/content/view/21/1, 15.05.2019.
[44] Statistika platnog prometa u Republici Hrvatskoj, https://www.hnb.hr/documents/20182/2569921/hp26092018-brosura-platni-promet-press-release-2018.pdf/18a2d0e8-3499-4fb9-a266-27de3f21e6a1, 15.05.2019.

Mobilno bankarstvo pruža mogućnost obavljanja financijskih transakcija u pokretu, s bilo kojeg mjesta pokrivenog mobilnim signalom i u bilo koje vrijeme. Za rad s aplikacijom mobilnog bankarstva potrebno je imati pristup Internetu te dovoljno raspoložive memorije za pohranu aplikacije na mobilnom uređaju. Tijekom korištenja usluge šalje se minimalna količina podataka te se trošak internetskog prometa naplaćuje prema količini prenesenih podataka i ne ovisi o duljini trajanja konekcije. Aplikacije za mobilno bankarstvo bi trebale imati instaliran visoko sigurnosni softver koji će uz zaštitu osigurati i jednostavnost rada. Uz to, pristup aplikaciji ne bi trebao biti moguć bez unosa PIN-a koji je poznat samo korisniku, a novije generacije mobilnih uređaja imaju i opciju pristupa otiskom prsta (Touch ID). Isto tako, u slučaju 3 puta pogrešnog uzastopnog unosa PIN-a, kao i u slučaju pet minuta neaktivnosti, preporučljivo je da se aplikacija zaključa iz sigurnosnih razloga i da zahtjeva novu prijavu.

Neke od usluga mobilnog bankarstva koje koristi najveći broj korisnika su: korištenje mtokena, kupnja bonova za mobitel, kupnja na prodajnim mjestima uz upotrebu mobitela, lociranje poslovnica i bankomata u blizini, obraćanje Banci putem poruka (upiti, potrebe, …), plaćanje računa, plaćanje računa skeniranjem uplatnice kamerom mobitela, pregled stanja i prometa po računima te prijenos novca na vlastite račune.

3.4. Prednosti i nedostaci elektroničkog bankarstva[45]

Prednosti elektroničkog bankarstva su:

- Smanjenje troškova - jedna od najvećih prednosti su smanjeni troškove, za razliku od tradicionalnih načina plaćanja računa, korištenjem elektroničkog bankarstva znatno se reduciraju troškovi kako za banku tako i za korisnike elektroničkog bankarstva. Primarni razlog zašto se troškovi smanjuju je taj što prilikom takvih transakcija banka dobiva uštedu na tome što se smanjuje broj zaposlenih, te klijent za to koristi svoju opremu.

- Jednostavnost - vrlo je jednostavan za korištenje što ga čini dostupnim velikom broju korisnika, potrebna su najosnovnija informatička znanja za njegovo korištenje.

[45] Prema: Rončević, A., Nove usluge bankarskog sektora: elektronski pregled 2006., str.765.

- Udobnost - najugodniji je način izvršavanja neugodnih radnji poput plaćanja računa, bilo koju transakciju je moguće izvršiti u doba koje osobi najviše odgovara iz udobnosti vlastitog doma.

- Faktor vremena - Tu je i ušteda vremena vrlo značajna jer nema dugačkih i zamornih čekanja u redovima. Tako da je vrijeme koje bi se nekad utrošilo na beskrajno čekanje moguće korisnije utrošiti. U ovom slučaju je banka otvorena 24 sata dnevno, nema ograničenja što se tiče radnog vremena.

Nedostaci elektroničkog poslovanja banaka:[46]

- Rizici koje donosi korištenje Interneta - postoje opasnosti od virusa, krađe podataka, zloupotrebe.
- Otpor prema korištenju elektroničkog bankarstva - zbog nepovjerenja prema modernim tehnologijama. Ovdje se uglavnom radi o ljudima starije dobi i onima koji nisu informatički pismeni.

[46] Prema: Ibidem.

4. RIZICI U SUVREMENOM ELEKTRONIČKOM BANKARSTVU

Rizici u elektroničkom bankarstvu gledaju se s aspekta sigurnosti informacijskog sustava koji je potreban za pružanje bankarskih usluga putem platformi za Internet bankarstvo. Sigurnosni sustav je složen i čvrsto hijerarhijski složen. Hijerarhiju čini šest osnovnih slojeva sustava[47]:

1. sigurnosna politika i procedure,
2. mjere fizičkog osiguranja sustava,
3. mjere identifikacije i autentifikacije korisnika,
4. mjere autorizacije korisnika,
5. mjere osiguranja integriteta podataka,
6. mjere revizije sustava.

4.1. Pojam i vrste rizika u elektroničkom bankarstvu

Bankovne organizacije već godinama pružaju usluge elektroničkog bankarstva svojim klijentima i poduzećima. Elektronički transferi sredstava, uključujući mala plaćanja i sustave za upravljanje gotovinom poduzeća, kao i javno dostupni automatizirani uređaji za podizanje gotovine i upravljanje računima stanovništva raširena su pojava u svijetu. Međutim, sve veće prihvaćanje Interneta u svijetu kao distribucijskog kanala za bankarske proizvode i usluge osigurava bankama nove mogućnosti, kao i poboljšanje usluga za klijente.

Grupa za elektroničko bankarstvo je utvrdila da osnovne karakteristike e-bankarstva (i općenito e-trgovanja) postavljaju nekoliko izazova pred upravljanje rizikom:[48]

- Brzina promjena povezanih s tehnološkim inovacijama i inovacijama usluga klijentima u e-bankarstvu je bez presedana. Nekad su nove bankovne aplikacije uvođene tijekom relativno dugoga vremenskog razdoblja te tek nakon što su detaljno testirane. Danas se banke susreću s pritiscima konkurencije za razvoj novih poslovnih aplikacija u vrlo kratkom vremenu – često prođe tek nekoliko mjeseci od ideje do proizvodnje. Zbog konkurencije se pojačava izazov za upravljanje u smislu da je teško osigurati provođenje adekvatne strateške procjene, analize rizika i preispitivanja sigurnosti prije uvođenja aplikacija e-bankarstva.
- Transakcijske web-stranice e-bankarstva i povezane poslovne aplikacije za stanovništvo i poduzeća obično se integriraju što je više moguće s postojećim

[47] Prema: Panian, Ž. i sur. (2010.): Poslovni informacijski sustavi, Element, Zagreb, str.138.
[48] Prema: Načela upravljanja rizikom u elektroničkom bankarstvu, http://old.hnb.hr/supervizija/papiri-bazelske-komisije/h-upravljanje-rizikom-u-elektronickom-bankarstvu.pdf, 17.05.2019.

računalnim sustavima kako bi se obrada elektroničkih transakcija (engl. straight-through processing, STP)bila što izravnija. Takva izravna automatizirana obrada smanjuje mogućnost ljudske pogreške i prijevare karakteristične za ručnu obradu, no međutim povećava ovisnost o zdravoj organizaciji i strukturi sustava, kao i o interoperabilnosti sustava i operativnoj skalarnosti.

- E-bankarstvo povećava ovisnost banaka o informacijskoj tehnologiji, tako da povećava tehničku složenost mnogih operativnih i sigurnosnih pitanja i dalje razvijajući trend prema većoj suradnji, povezanosti i eksternalizaciji uz pomoć trećih strana, od kojih su mnoge neregulirane. Takav razvoj dovodi do stvaranja novih poslovnih modela koji uključuju i banke i nebankarske subjekte, poput pružatelja internetskih usluga, telekomunikacijskih kompanija i drugih poduzeća koja se bave tehnologijom.
- Internet je svima dostupan i globalan po svojoj prirodi. To je otvorena mreža, kojoj nepoznate strane imaju pristup omogućen s bilo kojeg mjesta u svijetu rutiranjem poruka preko nepoznatih lokacija i pomoću bežičnih uređaja koji se brzo razvijaju. To uvelike povećava važnost sigurnosnih kontrola, tehnika provjere identiteta klijenata, zaštite podataka, postupaka ostavljanja pisanoga revizijskog traga te standarda zaštite privatnosti klijenta.

Kada se radi o elektroničkom bankarstvu i poslovanju preko Interneta pojavljuju se rizici i može doći do narušavanja sigurnosti. Internet poslovanje se uglavnom odvija putem internetske mreže. Internet je javni medij, komunikacija na njemu je otvorena i nema formalnih mehanizama kontrole. Rizici kod korištenja elektroničkog bankarstva obično se odnose na pokušaje prevare od strane trećih lica ili različitim pogreškama u obradi informacija. Razina sigurnosti za obavljanje transakcija putem elektroničkog bankarstva utječe i na sustav Internet bankarstva kojim se banka služi. U elektroničkom poslovanju banke se koriste različitim algoritmima za siguran protok podataka. Banke koje posluju na području Republike Hrvatske se koriste SSL algoritam (eng. Secure Socket Layer).

Načini na koje se može ugroziti sigurnost poslovanja su[49]:

- Krađa hardvera digitalnog sadržaja ili softvera,

[49] Prema: Panian, Ž. i sur. (2013.): Elektroničko poslovanje druge generacije, Ekonomski fakultet u Zagrebu, Zagreb, str.82.

- Intenzivnim napadima na ranjiva područja (pretrpavanje poslužitelja nebitnim zahtjevima koje izaziva pad sustava),
- Pokretanje virusa ili malicioznih programa kojima se napada software ili hardware,
- Neovlašteno pristupanje (skrivanje IP adresa, probijanje lozinki).

Zbog gore navedenih načina ugrožavanja sustava postoje određeni mehanizmi i tehnike zaštite kako bi se spriječili bilo kakvi pokušaji napada na sustav.

4.2. Upravljanje rizicima u elektroničkom bankarstvu

Postoje dva osnovna područja na kojima bi banke trebale štiti podatke[50]:

1. Mreža - napadi na komunikacijsku mrežu banke najčešće su u obliku upada haker-a i krađe podataka pri njihovom prijenosu mrežom. Mjere prevencije su koristiti jake sustave enkripcije onih podataka koji se prenose putem mreže
2. Hardverska i softverska oprema - napadi na hardver i softver banke mogu biti s ciljem onemogućavanja njihovog funkcioniranja (tzv. Denial of Service – DoS napadi) ili s ciljem logiranja kao uljez koji će neovlašteno obaviti neku transakciju ili postaviti virus kako bi se urušio sustav. Mjera prevencije za ove napade su vatrozidi (eng. Firewalls) na točkama gdje se oprema banke spaja s mrežom.

Rizici narušavanja sigurnosti su veliki, ali postoje metode zaštite koje banke primjenjuju da se ti rizici smanje što je više moguće. Potrebno je napraviti strategiju upravljanja sigurnošću, dokument u kojem tvrtka, u ovom slučaju banka, detaljno razrađuje postupke za očuvanje sigurnosti Cilj strategije je omogućiti neometano i sigurno odvijanje svih dijelova poslovanja.

Prilikom razradnje strategije potrebno je pripaziti na nekoliko detalja:

1. Potrebno je isplanirati sigurnosne sustave za svaki dio poslovanja, svi dijelovi poslovanja su važni,

2. Stalno ulagati u nove sigurnosne sustave, što uključuje financijska ulaganja u sustave i stručno usavršavati osoblje zaduženo za održavanje sustava.

Zbog gore navedenih načina ugrožavanja sustava postoje određeni mehanizmi i tehnike zaštite kako bi se spriječili bilo kakvi pokušaji napada na sustav.

[50] Prema: Šverko, I., (2007.): Upravljanje nekreditnim rizicima u hrvatskim financijskim institucijama, Hrvatski institut za bankarstvo i osiguranje, Zagreb, str.42.

„Mehanizmi i tehnike zaštite u elektroničkom bankarstvu su: [51]

- Identifikacija, autentikacija i autorizacija,
- Zaštita intraneta od pristupa neovlaštenih korisnika,
- Mjere antivirusne zaštite,
- Zaštita tajnosti podataka i poruka,
- Zaštita privatnosti korisnika.“

Prilikom zaštite tajnosti podatak koji se prenose računalnim mrežama koriste se metode šifriranja (kriptografija, kriptoanaliza). Kriptografija je postupak kojim se originalna poruka napravi nerazumljiva osobama koje nisu sudionici komunikacije, a zatim se kriptoanalizom radi obrnuti postupak, odnosno primalac poruke uz pomoć pronalaženja tajnog ključa enkriptirane poruke vidi njezin sadržaj, tj. originalnu poruku.

„Šverko dijeli sustav upravljanja rizicima na četiri osnovne faze koje su dijelovi cjelokupnog procesa kao sustavnog rješenja. Sustav se osniva na sljedećim fazama:

- identifikacija rizika,
- kvantifikacija rizika,
- upravljanje rizicima,
- kontrola i izvješćivanje o rizicima.“[52]

Prva faza identifikacije rizika je osnovna faza i temelj za sve ostale faze ciklusa. Osnovni cilj je identificirati sve rizike koji utječu na poslovanje te ih jasno prepoznati i kategorizirati po vrstama rizika jer svi rizici su nositelji potencijalne opasnosti za poslovanje banke.

Druga faza, faza kvantifikacije rizika je najteže provediva faza zbog problematike kvantificiranja većine rizika. Kvantifikacija rizičnosti prikazuje se prema visi štete i vjerojatnosti nastanka štete. Najveći problem je što se rizik ne prepoznaje dok se ne dogodi materijalni gubitak uzrokovan tim rizikom. Mnogi stručnjaci pokušavaju razviti savršen model kvantifikacije rizika te koriste matematičke i statističke formule za mjerenje rizika.

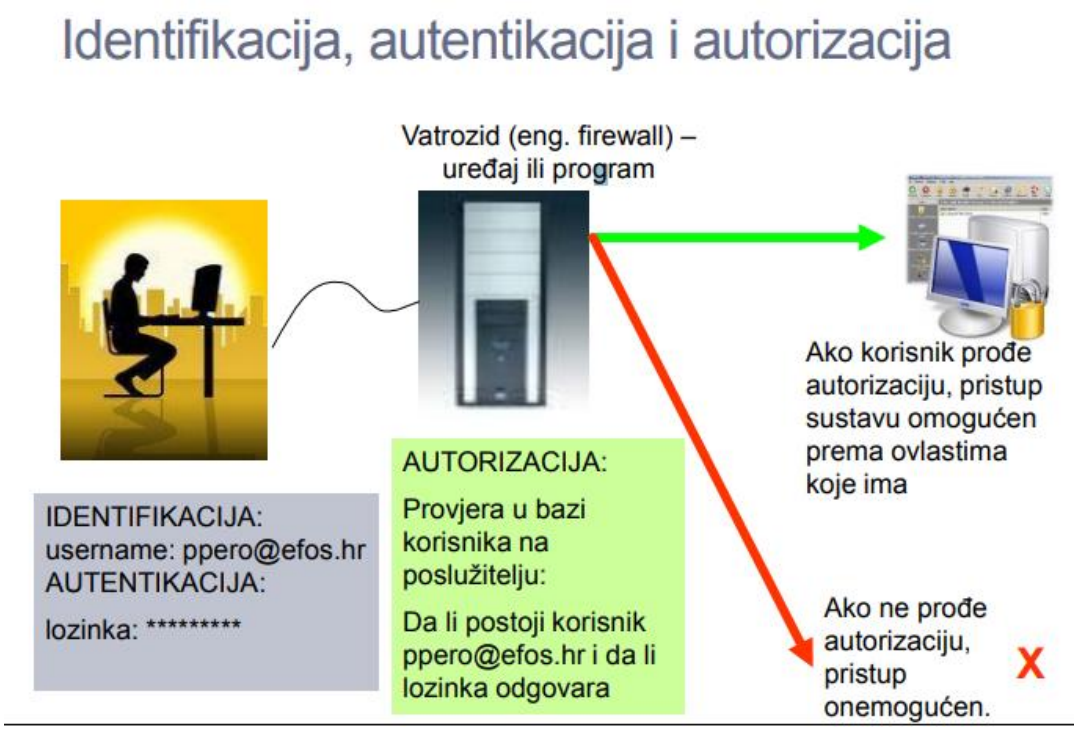
[51] Sigurnost informacijskog sustava e-bankarstva, http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf, 16.05.2019.
[52] Šverko, I., (2007.): Upravljanje nekreditnim rizicima u hrvatskim financijskim institucijama, Hrvatski institut za bankarstvo i osiguranje, Zagreb, str. 43.

Treća faza, upravljanje rizicima obuhvaća propise, akte, limite i strategije, te upravljanje aktivom i pasivom. Procesi upravljanja rizicima dijele se na vertikalne i horizontalne. Vertikalni prethode horizontalnima koji su puno složeniji. Vertikalni procesi su zapravo postavljanje limita po organizacijskim jedinicama vertikalno po organizacijskoj strukturi, dok su horizontalni procesi postavljanje limita za određene transakcije, svakodnevno donošenje rizičnih odluka te kontrola unutar organizacijske jedinice.

U četvrtoj fazi, izvješćivanje i kontrola rizika bitno je da to nezavisna funkcija kojoj je zadatak apsolutno objektivno prikazati procijenjenu izloženost banke rizicima. Također je iznimno bitno primjenjivati propise i jedinstvene standarde izvješćivanja i iskazivanja pojedinih rizičnih pozicija. Rezultat te funkcije su različita izvješća i informacije namijenjene različitim razinama upravljanja.

4.3. Obilježja identifikacije, autentikacije i autorizacije

U nastavku će biti prikazani proces identifikacije, autentikacije i autorizacije.



Slika 2. Proces identifikacije, autentikacije i autorizacije
Izvor: http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf

„Identifikacija je postupak prilikom kojeg se od korisnika traži upisivanje imena i prezimena, identifikacijskog broja ili korisničkog imena koje je dobio od banke.“[53]

„Autentikacija je postupak povezan s identifikacijom, a dokazuje da li je osoba koja se pokušava ulogirati na stranicu zaista ta osoba za koju se predstavlja, za autentifikaciju se koriste tri najčešća načina:

- Nešto što korisnik zna (npr. lozinka, PIN ili slično),
- Nešto što korisnik ima (npr. pametna kartica, stick, TAN tablica i sl.),
- Nešto što korisnik jest (biometrija – otisak prsta, rožnica oka, rukopis i sl.).“[54]

Autorizacija je postupak provjere sustava u kojoj se provjerava je li osoba koja se predstavila sustavu ima ovlasti pristupanja samom sustavu (provjera s unaprijed pohranjenim podacima unutar sustava).[55]

[53] Sigurnost informacijskog sustava e-bankarstva, http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf, 16.05.2019.
[54]Sigurnost informacijskog sustava e-bankarstva, http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf, 16.05.2019.
[55]Prema: Ibidem.

5. SIGURNOST U ELEKTRONIČKOM BANKARSTVU

Otvaranjem svojeg računa u banci, klijent dobiva na korištenje uređaj koji je potreban za autorizaciju (provjeru). Autorizacija predstavlja prvi važni korak prije korištenja bilo kakve usluge internetskog bankarstva ili obavljanja transakcije. Važan je zbog toga što banka pouzdano mora znati tko je korisnik, dok s druge strane korisnik isto tako mora biti siguran da nitko drugi umjesto njega ne može raspolagati njegovim sredstvima i poslovati u njegovo ime. Ovisno o tome jeste li pravna ili privatna osoba postoji nekoliko načina autorizacije. Za privatne su korisnike to najčešće tokeni ili TAN-ovi, dok pravne osobe u pravilu koriste smart-kartice. Ovisno o banci i tehnološkoj pozadini, klijentima se nudi jedna od spomenutih načina autorizacije. Ukoliko se to pokaže kao najoptimalnije rješenje, banke klijentima ponekad nude i izbor između dvije različite metode.

5.1. Načini autorizacije korisnika u elektroničkom bankarstvu

U nastavku će biti prikazani načini autorizacije korisnika u elektroničkom bankarstvu.

5.1.1. Token

„Token je samostalni, osobnom lozinkom zaštićeni uređaj vrlo sličan džepnom kalkulatoru koji se daje klijentu na privremeno korištenje. Namijenjen je digitalnom potpisivanju financijskih transakcija i identifikaciji korisnika prilikom prijave u sustav bankarstva. Kako bi se onemogućilo njegovo neovlašteno korištenje, token je zaštićen PIN-om duljine 4 znamenke.“[56] Fizički unos PIN-a (eng. Personal Identification Number) koji je nužan za uspješnu autorizaciju tokena, omogućen je pomoću numeričkih tipaka. Nakon autorizacije, token generira jednokratni tajni broj koji se zajedno sa serijskim brojem tokena mora unijeti u aplikaciju. Serijski je broj svakog tokena je jedinstven i sadrži dio kriptografskog ključa koji omogućuje generiranje dinamičkog koda za pristup mreži. „Za vrijeme svakog novog korištenja usluge token vam generira novi jednokratni tajni broj koji se zatim koristi za identifikaciju prilikom ulaska na korisnikove račune.“[57]

[56] Token, http://www.poslovniforum.hr/info/internet_bankarstvo.asp, 19.05.2019.
[57] Načini autorizacije, https://sites.google.com/site/internetbankarstvo2013/home/nacini-autorizacije, 19.05.2019.

„Ovakav način autorizacije koji se sastoji od dva faktora (serijskog broja tokena i niza jednokratnih brojeva koje token generira) omogućava računalu u banci da automatski identificira klijenta te mu omogući pristup svim njegovim računima.“ [58]



Slika 3. Token OTP Banke
Izvor: https://elementa.otpbanka.hr/gradjani/upute/token.htm

Ukoliko klijent unese neispravan PIN nekoliko puta za redom, na primjer tri puta, utoliko će se token automatski zaključati i za njegovo otključavanje je jedino ovlašten administrator. Za korištenje tokena nije potrebna nikakva posebna vještina ili dodatno informatičko znanje.

5.1.2. TAN

Autorizacija putem TAN-ova uobičajeno podrazumijeva list papira s pedesetak ili stotinjak nizova znamenaka koje klijent zaprima od banke. Kada klijent iskoristi sve nizove s liste, banka mu poštom šalje novu listu. Pojedine banke izdaju karticu s određenim brojem TAN-ova koje tada korisnik kružno koristi pri čemu nema potrebe za zaprimanjem novih TAN-ova. TAN-ovi izgledaju poput telefonskih brojeva te je time smanjena opasnost zloupotrebe u slučaju krađe ili provale. Velika prednost ove metode autorizacije je što ne zahtjeva nošenje uređaja za obavljanje bankarskih transakcija. „Korisnik može sa sobom uvijek imati nekoliko

[58] E-banking i sigurnos tehničkih rješenja za transakcije, https://www.slideshare.net/dina1302/ebanking-i-sigurnost-tehnickih-rjesenja-za-internet-transakcije, 20.05.2019.

TAN-ova u slučaju potrebe za obavljanjem neke transakcije. S druge strane veliki nedostatak TAN-ova čini teška administracija. Naime, banka mora čuvati u svojoj bazi popis TAN-ova za svakog klijenta, kako potrošenih, tako i tek dodijeljenih.“[59]



Slika 4. TAN tablica

Izvor:

https://t4.ftcdn.net/jpg/00/52/21/35/500_F_52213547_m6BMr79jfEJT73rknAODDASCIXctu1eX.jpg

S administracijskog gledišta banaka, token je dosta jednostavniji za korištenje. Jednom kad banka preda token korisniku, ona se do daljnjeg ne mora brinuti oko njegove autorizacije niti spremati toliku količinu podataka u bazu kao kod TAN-a.

5.1.3. Smart kartice

Smart ili pametna kartica predstavlja noviju inovaciju koja nudi veliki broj mogućih primjena uključujući funkcije pretplate, elektronsku gotovinu, identifikaciju vlasnika gotovine ,itd. „To je plastična kartica koja po svom izgledu podsjeća na običnu kreditnu ili debitnu karticu, uz napomenu da posjeduje jedan detalj koji ju bitno razlikuje od drugih kartica. U njoj se može nalaziti:

- mikroprocesor i memorijski čip,

[59] E-banking, http://www.mathos.unios.hr/~mjankov1/dokumenti/E-banking.pptx, 20.05.2019.

- samo memorijski čip s neprogramabilnom logikom.“[60]

Kartica se temelji na PKI (Public Key Infrastructure) tehnologiji koja se zasniva na asimetričnoj kriptografiji, odnosno na paru tajnih i javnih ključeva za šifriranje podataka. Svaki korisnik ima svoj javni ključ i svoj tajni ključ. Samo je javni ključ korisnika dan drugima na uvid. Korisnik podatke koje želi nekome poslati šifrira svojim tajnim ključem. Kada bi takvi podatke poslali, pročitati bi ih mogao svatko tko posjeduje javni ključ pošiljatelja. „Iz tog razloga pošiljatelj šifrira podatke još jedanput, ovaj put javnim ključem primatelja podataka. Na taj su način podaci dostupni samo primatelju. Naime, primatelj ih mora dešifrirati najprije pošiljateljevim javnim ključem, a zatim i svojim tajnim ključem. Svi su ti ključevi u digitalnom obliku pohranjeni na smart-kartici.“[61]



Slika 5. Token i smart kartica

Izvor: https://upload.wikimedia.org/wikipedia/commons/thumb/6/6c/Internet_Banking-01_%28xndr%29.JPG/800px-Internet_Banking-01_%28xndr%29.JPG

„Najčešće primjene smart-kartica su:

- kreditne kartice,
- elektroničke kartice,
- za Internet bankarstvo,

[60] Sigurnost bankarstva, https://www.scribd.com/document/399855475/Sigurnost-e-Bankarstva, 20.05.2019.
[61] Bankarstvo, http://4u2c-marketing-marinacuric.blogspot.com/2013/08/internet-bankarstvo-kako-ga-iskoristiti.html, 20.05.2019.

- kod kodiranih satelitskih programa,
- kao identifikacije u vladinim institucijama,
- kod bežične komunikacije,
- kod računalnih sigurnosnih sustava,
- kod mobilnih uređaja na karticu.“[62]

5.2. Mjere sigurnog korištenja elektroničkog bankarstva od strane banke[63]

Banke u Hrvatskoj koriste najsuvremenije i najsigurnije sigurnosne tehnologije, a to su PKI pametne kartice ili tehnologija jednokratnih zaporki. Tome u prilog ide činjenica da otkad se u Hrvatskoj koristi Internet bankarstvo nije zabilježen nijedan slučaj zlouporabe. U Hrvatskoj se krađe/napadi na klijente danas uglavnom svode na fizičke napade kao što je skimming kartica i slično. Aplikacije Internet bankarstva koje nude naše banke zaštićene su tzv. dvofaktorskom autentikacijom, korištenjem koje je za pristup potrebno imati određeni predmet (npr.token, smart karticu) i PIN.

5.2.1. Zaštita podataka

Prilikom zaštite tajnosti podatak koji se prenose računalnim mrežama koriste se metode šifriranja (kriptografija, kriptoanaliza). Kriptografija je postupak kojim se originalna poruka napravi nerazumljiva osobama koje nisu sudionici komunikacije, a zatim se kriptoanalizom radi obrnuti postupak, odnosno primalac poruke uz pomoć pronalaženja tajnog ključa enkriptirane poruke vidi njezin sadržaj, tj. originalnu poruku.

5.2.2. Preventivne mjere

Mjere preventivne zaštite – korisniku se preporučuje izbjegavanje upotrebe sumnjivih programa, otvaranje poruka nepoznatog podrijetla, redovito spremanje sigurnosnih kopija svojih datoteka i programa i upotreba antivirusnih programa za detektiranje virusa.

5.2.3. Mjere za već nastalu štetu

Mjere za već nastalu štetu – pokušati spasiti podatke i programe poslovanja, koristiti antiviruse za čišćenje virusa (ako je potrebno obrisati zaražene datoteke i njihov sadržaj). Najkorišteniji antivirusni programi koji mogu obaviti gore navedene zadaće su AVG, McAfee

[62] E-banking, http://www.mathos.unios.hr/~mjankov1/dokumenti/E-banking.pptx, 20.05.2019.
[63] Prema: Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str.90.

Antivirus, Esset NOD32, BitDefender, F-prot, HouseCall. Ako dođe do zaraze virusom postoji mogućnost nekontroliranog slanja mail poruka (eng. spam), šalje se veliki broj poruka velikom broju korisnika u jako malom vremenskom razdoblju. Korisnik nije ni svjestan operacija koje se dešavaju jer virus sam obavlja slanje spam poruka. Kako bi se spriječilo slanje spam poruka korisnik bi treba koristiti anti spam programe kao što su AddAware, StopZilla, Panda Titanium Antivirus + Antismap i dr.

5.3. Mjere sigurnog korištenja elektroničkog bankarstva od strane klijenata[64]

S ciljem sigurnosti korištenja računala i usluge elektroničkog bankarstva, preporuka je biti oprezan kod otvaranja e-mail poruka od nepoznatih korisnika, pa čak i od prijatelja ako se u mail poruci traži otvaranje neke Internet veze (linka) ili ako poruka sadrži privitak koji ne očekujete od navedenog prijatelja. Uvijek je potrebno pažljivo pročitati poruku i razmisliti je li ta poruka očekivana i logična u nekom trenutku, jer napadači iskorištavaju osnovne situacije kad su ljudi neoprezni, tj. znatiželju, suosjećanje, strah ili stres.

Za sigurnost računala, preporuka je koristiti najnovije operativne sustave, redovno instalirati sigurnosne nadogradnje za operativne sustave i sve aplikacije koje se koriste na računalu, imati uvijek uključenu aktualnu antivirusnu zaštitu, vatrozid (firewall) te koristiti računalo sa minimalnim ovlastima, tj. kao običan korisnik a ne korisnik sa administrativnim pravima. Za prijavu na računalo i za sve servise na Internetu, obavezno je koristiti lozinke minimalne duljine 12 znakova ili više, te ne koristiti identičnu lozinku na svim mjestima.

„Nažalost, napredak tehnologije omogućio je i kriminalcima da zloupotrijebe nove elektroničke usluge na razne načine:

- zaraze računalo spywareom i ukradu identitet,
- zatrpaju računalo skočnim prozorima i zaraze virusima,
- šalju spam i lažne e-poruke,
- nagovore da otvorite privitak iz lažne e-poruke
- nagovore da posjetite lažne stranice i otkrijete im svoje osobne podatke i / ili
- pristupe vašoj bežičnoj mreži.“[65]

[64] Prema: Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb, str.91.

[65] Preporuke za sigurnost korisnika bankarstva, https://ibank.sabank.hr/doc/Preporuke_sigurnost_korisnika_internet_bankarstva.pdf, 21.05.2019.

„Mjere koje je potrebno provoditi kako bi se osigurala sigurnost prilikom korištenja elektroničkog bankarstva su:

- Redovito ažurirati sigurnosna rješenja i preuzimati potrebne zakrpe,
- Instalirati antivirusne programe,
- Ažurirati preglednike,
- Koristiti osobni vatrozid,
- Koristiti anti – spyware program,
- Zaustaviti neželjenu poštu,
- Čuvati lozinku na sigurnom mjestu,
- Ne koristiti opciju AutoComplete u pregledniku,
- Zaštititi računalo lozinkom,
- Ne pristupati računalu kao administrator,
- Zaštititi bežične mreže.“[66]

5.4. Značaj elektroničkog potpisa u sigurnosti elektroničkog bankarstva[67]

Ovjeravanje dokumenata vlastoručnim potpisom vuče korijene od samih početaka ljudske pismenosti. Potpisi se danas nalaze na najrazličitijim dokumentima, a potpisom se smatra ne samo vlastoručni potpis, već i bilo koji drugi znak na dokumentu načinjen s ciljem ovjeravanja dokumenta. Razvojem i širenjem računala i računalnih mreža, postalo je jasno da je potreban novi način ovjeravanja.

Digitalni ili napredni elektronički potpis (eng. digital signature) je jedna od najpoznatijih implementacija elektroničkog potpisa, zasnovan je na asimetričnoj kriptografiji i algoritmima sažimanja, te predstavlja prvi stupanj u identifikaciji. Digitalni potpis osigurava autentičnost (identitet pošiljatelja utvrđuje se dešifriranjem sažetka poruke), integritet elektroničke informacije (provjerom sažetka poruke utvrđuje se da li je poruka mijenjana), te neporecivost (pošiljatelj ne može poreći sudjelovanje u transakciji, jer jedino on ima pristup do svog privatnog ključa kojim je potpisao poruku). Jedino što digitalni potpis ne osigurava je tajnost.

[66] Ibidem.
[67] Prema: Siladi, D. (2006.): Pogled u digitalizaciju tinte, Mreža br. 5, Bug d.o.o, Zagreb, str.62.

5.4.1. Pojam elektroničkog potpisa

U današnje doba informatizacije digitalni potpis je zamijenio tradicionalni potpis na digitalnim dokumentima. Kako bi vjerodostojno zamijenio klasični potpis, mora onemogućiti njegovo krivotvorenje i osigurati autentičnost potpisa i. „Digitalni potpis je niz znakova u digitalnoj formi (obično dužine 1024 bita) dobiven primjenom asimetrične kriptografije. Upotreba digitalnog potpisa podrazumijeva provođenje postupka izrade potpisa i postupka provjere odnosno verifikacije potpisa.[68]

„Digitalni potpis - digitalni kod koji služi za zaštitu poruka koje se elektronički prenose putem javne mreže. Svrha digitalnog potpisa:

- omogućiti identifikaciju pošiljaoca,
- osigurati autentičnost sadržaja poruke.“[69]

Elektronički potpis podrazumijeva skup podataka u elektroničkom obliku pomoću kojih se vrši identifikacija potpisnika i provjera vjerodostojnosti potpisanog elektroničkog dokumenta. Elektronički potpis je niz znakova u elektroničkom obliku. Kreiran računalom i ima istu pravnu snagu kao i vlastoručni potpis.

Svojstva digitalnog potpisa su:

- digitalni potpis je autentičan, što znači da ga može napraviti samo posjednik privatnog ključa,
- digitalni potpis je moguće provjeriti uporabom javnog ključa potpisnika,
- digitalni potpis izražava autorstvo ili slaganje sa sadržajem dokumenta, a pošto je funkcija dokumenta slijedi da je neodvojiv od sadržaja,
- digitalni potpis se ne može poreći.

5.4.2. Povijest digitalnog potpisa

„Prva primjena digitalnog potpisa bila je za vrijeme hladnog rada, kada su radi zaštite podataka SAD i SSSR dopustili međusobno postavljanje seizmometara kako bi nadzirali nuklearne testove. Informacije je bilo potrebno zaštiti od izmjena sa suprotne strane, kao i

[68] Digitalni potpis, https://bib.irb.hr/datoteka/481946.Zovkic-Vrbanec_-_Digitalni_potpis.pdf, 21.05.2019.
[69] Elektronički (napredni) potpis (digitalni potpis), https://elf.foi.hr/pluginfile.php/27999/mod_resource/content/1/3_EComm_sec.pdf, 21.05.2019.

omogućiti uvid u informacije kako bi se suprotna strana uvjerila da se šalju samo dogovoreni podaci.
Mehanizam koji se pri tome koristio bio je digitalni potpis.“[70] Danas je digitalni potpis prešao u drugu dimenziju, ali bit je ostala i dalje ista, a odnosi se na autentičnost i integritet bitnih informacija.

„Digitalni potpis predstavlja podskupinu elektroničkih potpisa koji koriste različite kriptografske metode, zbog toga je njegov razvoj usko vezan uz povijest kriptografije s javnim ključem (eng. public key cryptography), a koja započinje 1874. godine opisom jednosmjernih enkripcijskih funkcija u knjizi „The Principles of Science: A Treatise on Logic and Scientific Method“ autora William Stanley Jevonsa.“[71]

Ranih 1970-ih godina James H. Ellis, Malcolm Williamson i Clifford Cocks osmišljavaju prve algoritme temeljene na asimetričnom ključu. Whitfield Diffie i Martin Hellman 1976. godine objavljuju prvu praktično upotrebljivu metodu razmjene ključeva, koja je kasnije postaje poznata pod nazivom Diffie-Hellman razmjena ključeva i predstavlja poseban slučaj RSA algoritma. RSA algoritam je dobio naziv po početnim slovima prezimena svojih autora Ron Rivest, Adi Shamir i Leonard Adleman, a prvi je puta javno opisan 1977. godine i prvi je algoritam prikladan za potpisivanje i enkripciju podataka, te se smatra sigurnim, pod pretpostavkom korištenja dovoljno dugih ključeva i ažurnih implementacija.[72]

Neal Koblitz i Victor S. Miller 1985. godine su predložili korištenje eliptičkih krivulja nad konačnim poljima u kriptografskim algoritmima s javnim ključam. Na temelju ovakve enkripcije razvijen je ECDSA (eng. Elliptic Curve DSA) algoritam, varijanta DSA (eng. Digital Signature Algorithm) algoritma, koji pomoću manjeg ključa i s približno jednakim vremenom izvođenja daje sigurniji digitalni potpis jednake veličine.[73]

„Standardizacija DS algoritama u Sjedinjenim Američkim Državama započinje sredinom 1990-ih godina, a 1994. godine National Institute of Standards and Technology izdaje standard s oznakom FIPS PUB 186 (eng. Federal Information Processing Standards

[70] Siladi, D. (2006.): Pogled u ditalizaciju tinte, Mreža br. 5, Bug d.o.o .Zagreb, str. 64.
[71] Digitalni potpis, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf, 22.05.2019.
[72]Prema: Ibidem.
[73] Prema: Ibidem.

Publications). Godinu dana kasnije American National Standards Institute izdaje ANSI X9.30 standard. Standardizacija na području Europe započinje krajem 1990.-ih i početkom 2000.-ih godina, na razini Europske Unije i pojedinih zemalja.“[74]

5.4.3. Primjena digitalnih potpisa

U nekoliko zemalja digitalni potpis ima sličan status onomu tradicionalnog pisanog potpisa. To znači da digitalno potpisani dokument potpisnika pravno obvezuje, u skladu s uvjetima navedenim u spomenutom dokumentu. Zbog toga se preporučuje korištenje različitih parova ključeva za potpisivanje i za enkripciju.“ Korištenjem para ključeva namijenjenih enkripciji, korisnik može sudjelovati u kriptiranoj komunikaciji (npr. pregovorima o kupnji nekretnine), ali ne potpisuje svaku poruku pravno važećim potpisom. Jednom kada zainteresirane strane postignu dogovor, ugovor se digitalno potpisuje i tek tada su potpisnici pravno vezani potpisanim dokumentom. Tako potpisani ugovor moguće je zatim, zbog dodatne zaštite, slati kriptiranog.“[75]

DS algoritmi i protokoli ne pružaju informaciju o tome kada je dokument potpisan. Potpisnik može, ali i ne mora, uključiti vremensku oznaku (eng. time stamp) unutar digitalnog potpisa ili u samom dokumentu može postojati datum i vrijeme potpisivanja. Ovakvo označavanje vremena omogućuje navođenje netočnog, npr. ranijeg datuma ili vremena potpisivanja. Korištenjem sigurnih vremenskih oznaka (eng. trusted time stamp) se sprečava ovakva zloupotreba digitalnog potpisa. Sigurne vremenske oznake mora osigurati pouzdana treća strana, tzv. TSA (eng. TimeStamping Authority), koja time potvrđuje postojanje određenih podataka prije nekog vremena. Ranjivosti takvog korištenja vremenskih oznaka je moguće umanjiti umetanjem više oznaka različitih TSA organizacija u potpis. Jedna od osnovnih prednosti korištenja digitalnih potpisa, uz osiguravanje autentičnosti i integriteta dokumenta, je onemogućavanje nepriznavanja dokumenta od strane potpisnika (eng. nonrepudiation). Ako sporna poruka nije potpisana, njezin ju navodni pošiljatelj uvijek može zanijekati tvrdeći kako ju je netko drugi napisao i poslao. Takvo što se ne može dogoditi s potpisanim porukama osim u slučaju otkrivanja korisnikovog privatnog ključa, kojeg zbog toga treba čuvati u strogoj tajnosti. [76]

[74] Ibidem.
[75] CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb, str. 9.
[76] Prema: Ibidem.

„Spremanje privatnog ključa na tzv. pametnoj kartici (eng. smart card) jedan je od načina osiguravanja njegove tajnosti. Alternativa je čuvanje privatnog ključa na osobnom računalu korisnika, ali takav pristup ima dva ozbiljna nedostatka:

- korisnik može potpisivati dokumente samo na spomenutom računalu i
- tajnost privatnog ključa ovisi o sigurnosti računala na kojemu je pohranjen.“[77]

Karticu je potrebno povezati na računalo i proslijediti joj hash vrijednost poruke, ugrađeni procesor zatim iz pohranjenog privatnog ključa i primljenog otiska poruke proračunava potpis koji se potom šalje računalu. Na taj način privatni ključ nikada ne napušta karticu. Većinu kartica potrebno je prije upotrebe aktivirati osobnim identifikacijskim brojem (eng. Personal Identification Number – PIN), a građene su tako da onemogućavaju, ili barem otežavaju, neovlašten pristup pohranjenim podacima.

Slijepi potpis (eng. blind signature) je oblik digitalnog potpisa kod kojega je sadržaj poruke skriven (eng. blinded) od potpisnika. Takvim potpisom moguće je provjeriti vjerodostojnost originalne otkrivene (eng. unblinded) poruke isto kao što se to čini običnim digitalnim potpisom. Ovakvi potpisi najčešće se koriste u primjenama gdje je jedna strana autor poruke, a neka druga strana njezin potpisnik, npr. u kriptografskim sustavima za glasovanje ili kod sigurnih elektroničkih platežnih sustava. Druga moguća primjena slijepih potpisa je sprječavanje potpisnika da poveže potpisanu skrivenu poruku s kasnije otkrivenom porukom tijekom njezinog eventualnog ocjenjivanja (eng. unlinkability). Slijepi potpisi se koriste u primjenama kod kojih je nužna anonimnost pojedinih sudionika. Slijepo potpisivanje je moguće implementirati pomoću raznih DS algoritama s javnim ključem, npr. RSA ili DSA algoritmom. „Poruka se prije potpisivanja skriva, najčešće kombiniranjem s nasumično odabranim ključem (eng. blinding factor) i zatim ju se potpisuje nekim od uobičajenih DS algoritama. Vjerodostojnost potpisane skrivene poruke, zajedno s ključem korištenim za njeno skrivanje, moguće je utvrditi pomoću potpisnikovog javnog ključa.“[78]

Različite sadržaje web stranica je moguće potpisati XML digitalnim potpisom koji je reguliran W3C XML Signature standardom krovne međunarodne standardizacijske organizacije na području web tehnologija World Wide Web Consortium.“ XML potpisom moguće je potpisati sljedeće tipove podataka:

[77] Ibidem.
[78] CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb, str. 9 – 10.

- XML elemente, skupove XML čvorova (eng. nodes) i njihov sadržaj,
- vanjske URI oznake,
- vanjske binarne datoteke i
- binarne podatke ugrađene u XML dokument u obliku znakovnih nizova kodiranih na bazi 64.“[79]

Na pojedinoj web stranici je moguće potpisati bilo koji njezin programski dostupan element (dijelove HTML i XML programskog koda te skrivena i vidljiva polja formulara, kao i njihove sadržaje), datoteke prisutne na klijentskom računalu mrežne resurse koji su dostupni izravno s klijentskog računala ili posredno preko poslužitelja. „Postoje tri tipa XML potpisa:

- omotani (eng. enveloped) – potpis je ugrađen u podatke koje potpisuje,
- omotavajući (eng. enveloping) – potpisani podaci su ugrađeni u XML potpis i
- odvojeni (eng. detached) – XML potpis i potpisani podaci su razdvojeni.“[80]

5.4.4. Napadi na digitalni potpis

Sigurnost kriptiranih dokumenata ovisi o tome koji se algoritam koristi za kriptiranje, te duljini kriptografskih ključeva. Kriptoanaliza je znanstvena disciplina koja proučava metode otkrivanja otvorenog teksta uz poznavanje ključa, te bez poznavanja ključa, a cilj je pronalaženje ranjivosti u kriptografskim shemama kako bi se otkrili tajni ključevi za dekriptiranje informacija. Osnovna pretpostavka kriptoanalize je da kriptoanalitičar zna koji se kriptosustav koristi.

Osnovne vrste napada mogu se klasificirati u sljedeće kategorije:[81]

- samo kriptirani tekst (eng. cyphertext-only) - napadač ima pristup samo skupini kriptiranih tekstova i cilj mu je da otkrije izvorni tekst što većeg broja poruka ili da otkrije ključ kojim su poruke šifrirane.
- poznati otvoreni tekst (eng. known-plaintext) – napadač ima skupinu kriptiranih tekstova za koje poznaje odgovarajući nekriptirani tekst. Cilj napada je otkrivanje ključa ili algoritma za dešifriranje poruka koje su šifrirane tim ključem.

[79] CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb, str. 9 – 10.
[80] Ibidem.
[81] Prema: Dujella, A., Maretić M. (2007.): Kriptografija, Element, Zagreb, str. 4.

- izabrani otvoreni tekst (eng. chosen-plaintext) – napadač ima privremeni pristup alatu za šifriranje tako da može dobiti kriptirani tekst odabranog otvorenog teksta. Ova vrsta napada je jača od napada na poznat otvoreni tekst.
- izabrani kriptirani tekst (eng. chosen-cyphertext) – poput prethodnog, osim što napadač ima pristup alatu za dešifriranje, tako da može dobiti otvoreni tekst. Ova vrsta napada je tipična za kriptosustav s javnim ključem.
- potkupljivanje, ucjena, krađa i slične aktivnosti (eng. rubber-hose) – ova vrsta napada iako ne spada u matematičke oblike kriptoanalize, vrlo je efikasna te često se primjenjuje.

„Dvije osnovne skupine napada na digitalni potpis su :

- napadi uz poznavanje ključa – napadaču je dostupan samo potpisnikov javni ključ,
- napadi uz pristup porukama – napadač ima pristup potpisanim porukama.“[82]

Napadi uz pristup porukama mogu se podijeliti prema načinu na koji su poruke dostupne napadaču odabrane:

- Napad na poznate poruke – napadač ima pristup skupu m1, …, mt potpisanih poruka koje nije on odabrao.
- Napad na generički odabrane poruke – napadač prije nego što pokuša lažirati potpis odabire skup poruka i daje ih korisniku na potpis. Prilikom odabira poruka napadač nema uvid u niti jedan vjerodostojan potpis te se ovo smatra neadaptivnim napadom. Izbor poruka ne ovisi o korisnikovom javnom ključu pa se napad naziva generičkim – jednak skup poruka koristi se za napade na potpise svih korisnika.
- Usmjereni napad na odabrane poruke – napadač odabire poruke na temelju korisnikovog javnog ključa, ali bez uvida u vjerodostojan potpis. Ovo se također smatra neadaptivnim napadom, ali nije generički, jer je usmjeren na pojedinog korisnika.
- Adaptivan napad na odabrane poruke – napadač korisniku na potpis daje poruke odabrane na temelju korisnikova javnog ključa i prethodno pribavljenih potpisa.[83]

[82] CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb, str. 11.
[83] Prema: CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb, str. 11 - 12.

6. ZAKLJUČAK

Cilj ovoga rada je bio prikazati sve evidentne probleme sigurnosti s kojima se banke, a i korisnici elektroničkog bankarstva susreću. Razvoj informatičke tehnologije doveo je do velikih promjena u poslovanju. Poduzeća su uočila dobrobiti koje im pruža tehnologija te su je počeli uvrštavati u svoje poslovanje kako bi ga unaprijedili. Sve tvrtke koje žele imati što uspješnije poslovanje koriste se elektroničkim poslovanjem jer im ono omogućuje bolje iskorištavanje poslovnih resursa, a naročito informacijskih. Tržište se proširilo na cijeli svijet, pa je i konkurencija postala veća, te je potrebno sve više truda i ulaganja u svoje poslovanje i nove tehnologije kako bi se opstalo na tržištu i uspješno poslovalo.

Informatička tehnologija imala je veliki utjecaj i na poslovanje banaka. Bankama se olakšalo poslovanje, smanjili troškovi, povećalo se bankarsko tržište, te su se promijenile usluge koje banke pružaju. Banke danas osim putem klasičnih kanala svoje poslovanje ostvaruju putem bankomata, telefona, SMS – a, Interneta te mobilnih telefona. Gotovo sve usluge banaka dostupne su i putem Interneta te je posjećivanje banaka gotovo nepotrebno, smanjili su se redovi u bankama, troškovi banaka, sve usluge banaka su dostupne 24 sata dnevno te je i korištenje usluga banaka postalo ugodnije klijentima banaka.

Ono što predstavlja problem u ovom vidu poslovanja je sigurnost, međutim banke u Hrvatskoj koriste najsuvremenije sigurnosne sustave te je mogućnost negativnih iskustava svedena na minimum i uglavnom je povezana sa neznanjem korisnika. Određen broj ljudi još uvijek zbog neznanja ili nepovjerenja ne koristi usluge banaka, međutim banke sustavno rade na tome da približe korisnicima svoje usluge, te se svake godine broj korisnika elektroničkog bankarstva povećava. Bez uvođenja informacijske i komunikacijske tehnologije u poslovanje banke ne mogu opstati na tržištu, niti biti konkurentne, potrebno je ponuditi kvalitetnu uslugu, te sigurnosne sustave kako bi korisnici imali povjerenje u usluge banaka i bile zadovoljne uslugom.

Elektroničko bankarstvo omogućuje korisnicima korištenje bankarskih usluga bez dolazaka u poslovnicu banke. Mnogim ljudima to značajno olakšava život jer ne moraju trošiti vrijeme i novac na dolazak u banku, nego to mogu obaviti elektroničkim putem. Međutim, prije korištenja bilo kakve usluge Internet bankarstva ili obavljanja transakcije, potrebno se je autorizirati. Autorizacija je važna jer banka pouzdano mora znati tko je korisnik, dok korisnik

isto tako mora biti siguran da nitko drugi umjesto njega ne može koristiti njegova sredstva i poslovati u njegovo ime. Postoji nekoliko načina autorizacije, ovisno o tome jeste li pravna ili privatna osoba. Privatni korisnici najčešće koriste TAN-ove, dok pravne osobe u pravilu koriste smart-kartice. Upravo kako bi se Internet korisnicima omogućio što sigurniji način autorizacije, banke konstantno moraju izmjenjivati i tražiti što više specifične i jedinstvene načine identifikacije.

Svjedoci smo brojnih hakerskih napada, a također i krađe na bankomatima, te korištenja neovlaštenih kreditnih kartica. Banke u Hrvatskoj koriste najsuvremenije i najsigurnije sigurnosne tehnologije, kao što su PKI pametne kartice ili tehnologija jednokratnih zaporki. Napadi se u Hrvatskoj najčešće svode na fizičke napade kao što je skimming kartica. Povjerljivi se sadržaji moraju zaštititi od neautoriziranih osoba tako da se šifriraju. Pošiljatelj šifrira sadržaj poruke prije njena slanja, a primatelj je dešifrira po primitku. Svaka verzija sigurnosnog sustava zahtjeva neki način kodiranja. Enkripcija se omogućava preko matematičkih funkcija, takozvanih hash funkcija. Na brz i lak način se kodira neka ulazna riječ te se prvobitna informacija ne može saznati bez ključa.

Registracijom na Internet , identificiramo se svojom IP adresom. Preko vatrozida se može doći do sustava informacija koje dolaze direktno od klijenta. Elektroničkim potpisom se ustanovljuje autentičnost potpisanog dokumenta. Kako bi se zaštitila klijentska strana Internet bankarstva potrebno je redovito ažuriranje softvera, korištenje pouzdanog antivirusa i anti-malware softvera, te ne upisivati bankovne podatke kada ste spojeni na javnu Wi-Fi mrežu. Mjere za već nastalu štetu su da pokušamo spasiti podatke i programe poslovanja, te da ako je potrebno obrišemo zaražene datoteke i njihov sadržaj.

Prilikom otvaranja e-mail poruka od nepoznatih korisnika ili čak od prijatelja, ako se u poruci traži otvaranje neke Internet stranice moramo biti oprezni. Potrebno je pažljivo pročitati poruku i razmisliti je li ta poruka očekivana u tom trenutku, jer napadači vrebaju svaku priliku kako bi se domogli podataka. Digitalni potpis ima značajnu ulogu pri sigurnosti u elektroničkom poslovanju jer osigurava autentičnost, integritet elektroničke informacije i neporecivost. Digitalni potpis ima slične ovlasti kao i tradicionalni potpis. On potpisnika obvezuje, u skladu sa svim navedenim uvjetima u spomenutom dokumentu.

U budućnosti će banke morati donijeti značajne strategije elektroničkog bankarstva i sigurnosti kao dio poslovne strategije banke, svakako će biti potrebno procijeniti rizike koji su povezani sa elektroničkim bankarstvom te je potrebno osigurati djelotvoran sustav nadzora i praćenja elektroničkog bankarstva. Osim navedenog, banke će morati primjenjivati sigurne i učinkovite autentifikacijske metode o potvrdi identiteta i ovlasti osoba, procesa i sustava. Fokus će se morati staviti i na zaštitu informacija od neovlaštenog otkrivanja, mijenjanja ili brisanja za vrijeme unosa, obrade i prijenosa preko telekomunikacijskih mreža, kao i kod pohrane i čuvanja informacija na sustavima banke i klijenata.

LITERATURA

1. 50. obljetnica bankomata, https://www.24sata.hr/fun/50-obljetnica-bankomata-zanimljivosti-koje-niste-znali-529581, 14.05.2019.
2. Bankarstvo, http://4u2c-marketing-marinacuric.blogspot.com/2013/08/internet-bankarstvo-kako-ga-iskoristiti.html, 20.05.2019.
3. Bašić, R. (2006.): Primjena tehnoloških inovacija i elektroničkog plaćanja u hrvatskom bankarstvu, Ekonomski fakultet, Rijeka
4. Business-to-Consumer, https://www.investopedia.com/terms/b/btoc.asp, 09.05.2019.
5. CARNet (2007.): Digitalni potpis, Hrvatska akademska i istraživačka mreža, Zagreb
6. Digitalni potpis, https://bib.irb.hr/datoteka/481946.Zovkic-Vrbanec_-_Digitalni_potpis.pdf, 21.05.2019.
7. Digitalni potpis, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf, 22.05.2019.
8. Dujella, A., Maretić M. (2007.): Kriptografija, Element, Zagreb
9. E- poslovanje, http://www.webstrategija.com/ws/05/e-poslovanje, 08.05.2019.
10. E-banking i sigurnost tehničkih rješenja za transakcije, https://www.slideshare.net/dina1302/ebanking-i-sigurnost-tehnickih-rjesenja-za-internet-transakcije, 20.05.2019.
11. E-banking, http://www.mathos.unios.hr/~mjankov1/dokumenti/E-banking.pptx, 20.05.2019.
12. E-banking, http://www.mathos.unios.hr/~mjankov1/dokumenti/E-banking.pptx, 20.05.2019.
13. Elektronički (napredni) potpis (digitalni potpis), https://elf.foi.hr/pluginfile.php/27999/mod_resource/content/1/3_EComm_sec.pdf, 21.05.2019.
14. Elektroničko poslovanje, https://www.datalab.hr/elektronicko-poslovanje-kako-sto-gdje/, 11.05.2019.
15. Garača, Ž. (2008.): Poslovni informacijski sustavi, Ekonomski fakultet, Split, str. 148. – 152.
16. Infrastruktura, https://www.hnb.hr/statistika/statisticki-podaci/platne-usluge/infrastruktura, 14.05.2019.
17. Kartice, http://www.moj-bankar.hr/Kazalo/K/Kartice, 15.05.2019.

18. Načela upravljanja rizikom u elektroničkom bankarstvu, http://old.hnb.hr/supervizija/papiri-bazelske-komisije/h-upravljanje-rizikom-u-elektronickom-bankarstvu.pdf, 17.05.2019.
19. Načini autorizacije, https://sites.google.com/site/internetbankarstvo2013/home/nacini-autorizacije, 19.05.2019.
20. Panian, Ž. (2000.): Elektroničko poslovanje – šansa hrvatskoga gospodarstva u 21. Stoljeću, Ekonomski pregled, 52 (3-4), Zagreb
21. Panian, Ž. (2002.): Izazovi elektroničkog poslovanja, Narodne novine d.d., Zagreb
22. Panian, Ž. (2013): Elektroničko poslovanje druge generacije, Ekonomski fakultetu Zagrebu, Zagreb
23. Panian, Ž. i sur. (2010.): Poslovni informacijski sustavi, Element, Zagreb
24. Panian, Ž., Strugar, I. (2000.): Primjena računala u poslovnoj praksi, Sinergija, Zagreb
25. Platne kartice i kartične transakcije, https://www.hnb.hr/documents/20182/2504205/h-pkkt_2017.pdf/1fb88d57-d0d8-41c8-b3b7-2bf9df5a29b9, 18.05.2019.
26. Poslovanje budućnosti, http://manager-magazine.com/content/view/21/1, 15.05.2019.
27. Preporuke za sigurnost korisnika bankarstva, https://ibank.sabank.hr/doc/Preporuke_sigurnost_korisnika_internet_bankarstva.pdf, 21.05.2019.
28. Rasprostranjenost važna kod odabira banke, http://www.poslovni.hr/hrvatska/rasprostranjenost-vazna-kod-odabira-218466, 14.05.2019.
29. Rončević, A (2006.): Nove usluge bankarskog sektora:razvitak samoposlužnog bankarstva u Hrvatskoj, Ekonomski pregled, 11, Zagreb
30. Ružić, D. (2003): E – marketing, Ekonomski fakultet u Osijeku, Osijek
31. Severović, K. (2013.): Upravljanje odnosima s klijentima kao izvor informacija za oblikovanje i poboljšanje usluga, Fakultet organizacije i informatike, Varaždin
32. Sigurnost bankarstva, https://www.scribd.com/document/399855475/Sigurnost-e-Bankarstva, 20.05.2019.
33. Sigurnost informacijskog sustava e-bankarstva, http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf, 16.05.2019.
34. Sigurnost informacijskog sustava e-bankarstva, http://www.efos.unios.hr/ict-u-bankarstvu/wp-content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf, 16.05.2019.
35. Siladi, D. (2006.): Pogled u digitalizaciju tinte, Mreža br. 5, Bug d.o.o, Zagreb
36. Spremić, M. (2004.): Menadžment i elektroničko poslovanje, Narodne novine, Zagreb

37. Statistika platnog prometa u Republici Hrvatskoj, https://www.hnb.hr/documents/20182/2569921/hp26092018-brosura-platni-promet-press-release-2018.pdf/18a2d0e8-3499-4fb9-a266-27de3f21e6a1, 15.05.2019.
38. Što je e-račun?, https://faq.hrvatskitelekom.hr/pages/category.xhtml?question=11537447, 07.05.2019.
39. Šverko, I., (2007.): Upravljanje nekreditnim rizicima u hrvatskim financijskim institucijama, Hrvatski institut za bankarstvo i osiguranje, Zagreb
40. Token, http://www.poslovniforum.hr/info/internet_bankarstvo.asp, 19.05.2019.
41. Tomašević Lišanin, M. (1997.): Bankarski marketing, Informator, Zagreb
42. U pet godina udvostručena mreža bankomata, https://lider.media/arhiva/63823/, 14.05.2019.
43. What is C2C?, https://www.businessnewsdaily.com/5084-what-is-c2c.html,09.05.2019.
44. What is Government-to-Business (G2B), https://www.igi-global.com/dictionary/government-to-business-g2b/12391, 10.05.2019.

POPIS SLIKA

Slika 1. Zastupljenost platnih kartica potrošača u RH na dan 31. prosinca 2017. ..... *18*

Slika 2. Proces identifikacije, autentikacije i autorizacije *28*

Slika 3. Token OTP Banke *31*

Slika 4. TAN tablica *32*

Slika 5. Token i smart kartica *33*