Problem zaštite osobnih podataka u e-bankarstvu

Jokić, Antonio

Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Sveučilišni prijediplomski studij Poslovna Informatika

Antonio Jokić

PROBLEM ZAŠTITE OSOBNIH PODATAKA U E-BANKARSTVU

Završni rad

Osijek, 2024.

Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Sveučilišni prijediplomski studij Poslovna Informatika

Antonio Jokić

PROBLEM ZAŠTITE OSOBNIH PODATAKA U E-BANKARSTVU

Završni rad

Kolegij: Informacijsko-komunikacijska tehnologija (ICT) u bankarstvu

JMBAG: 0010234654
e-mail: ajokic@efos.hr
Mentor: Prof. dr. sc. Nataša Šarlija
Komentor: dr. sc. Adela Has

Osijek, 2024.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
University Undergraduate Study Business informatics

Antonio Jokić

THE PROBLEM OF PERSONAL DATA PROTECTION IN E-BANKING

Final paper

Osijek, 2024.

IZJAVA

O AKADEMSKOJ ČESTITOSTI,

PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je (navesti vrstu rada: završni / diplomski / specijalistički / doktorski) rad isključivo rezultat osobnoga rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.

2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska.

3. Kojom izjavljujem da sam suglasan/suglasna da se trajno pohrani i objavi moj rad u institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).

4. izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan sa dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Antonio Jokić

JMBAG: 0010234654

OIB: 19418495189

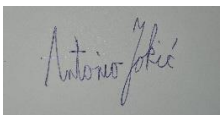
e-mail za kontakt: antonio.jokic2021@gmail.com ili ajokic@efos.hr

Naziv studija: sveučilišni prijediplomski studij Poslovna Informatika

Naslov rada: Problem zaštite osobnih podataka u e-bankarstvu

Mentor/mentorica rada: Prof. dr. sc. Nataša Šarlija

U Osijeku, 2024 godine

Potpis__ 

_

SAŽETAK

U današnje vrijeme sve je važnija zaštita osobnih podataka u e-bankarstvu. Zbog svoje karakteristike sigurnost podataka je jedan od temelja u e-bankarstvu kao temelj za povjerenje korisnika. Uz napredak tehnologija napreduje također i zaštita podataka, sa svakom novom inovacijama i tehnologijom koja se implementira u e-bankarstvu, osigurava se veća sigurnost osobnih podataka. Promjenom tehnologije mijenjaju se i opasnosti. U ovom radu će se istražiti vrste opasnosti koje postoje za osobne podatke, te obveze i uloge banaka i zaposlenika u zaštiti osobnih podataka klijenata. Proces zaštite osobnih podataka mora biti usklađen sa zakonodavnim okvirima, također treba biti kontinuiran i stalno prilagođen novim tehnološkim naprecima i prijetnjama. Cilj ovog istraživanja je prepoznati opasnosti i rizike neodgovornog raspolaganja sa osobnim podacima, te također će ustanoviti i moguće prijetnje. Najčešće prijetnje su hakerski napadi, virusi i crvotočine, nesigurna mreža, slabo ažuriranje softvera, slaba sigurnosna praksa korisnika i zaposlenika, zlouporaba podataka od strane bankarskih institucija. Pri zaštiti osobnih podataka nikada se ne može biti sto posto siguran, ali se može što više minimalizirati rizik o prijetnji i mogućih šteta. U radu će se istražiti također tehnologije koje se koriste za zaštitu osobnih podatka. Također će se usporediti dvije hrvatske banke i vidjeti što poduzimaju pri zaštiti osobnih podataka i njihovoj sigurnosti.

Ključne riječi: E-bankarstvo, zaštita, osobni podaci, tehnologija

Abstract

Nowadays, the protection of personal data in e-banking is becoming increasingly important. Due to its characteristics, data security is one of the foundations of e-banking as a basis for user trust. As technology advances, so does data protection. With each new innovation and technology used in e-banking, the security of personal data is improved. As technology changes, so do the threats. This paper will examine the types of threats to personal data and the obligations and responsibilities of banks and employees in protecting the personal data of their customers. The process of protecting personal data must be in accordance with the legal framework, it should also be continuous and constantly adapted to new technological advances and threats. The aim of this paper is to determine the dangers and risks of irresponsible handling of personal data and to identify possible threats. The most common threats are hacker attacks, viruses and wormholes, insecure networks, insufficient software updates, weak security practices of users and employees, data misuse by banking institutions. The paper also examines the technologies used to protect personal data and compares Croatian banks to determine the level of protection of personal data and its security.

Keywords: E-banking, protection, personal data, technology

Sadržaj

1.Uvod

Zaštita podataka u e-bankarstvu je uvijek bila jedna od glavnih komponenti koje osiguravaju povjerenje klijenata u banku. Bez zaštite podataka u e-bankarstvu nastaju problemi koji su negativne prirode. Banka je odgovorna za osobne podatke svojih klijenata, te treba konstantno biti usklađena sa zakonodavnim okvirima koje treba poštivati i primjenjivati. E-bankarstvo ili online bankarstvo su bankarske usluge koje se omogućavaju klijentima banke da obavljaju svoje financijske transakcije korištenjem elektroničkih kanala poput interneta, telefona i mobilnih uređaja. E-bankarstvo je omogućilo klijentima da ne moraju dolaziti do fizičke poslovnice, što ujedno fizički štiti klijenta od fizičkih ozljeda jer ne mora doći do fizičke poslovnice. Uz napredak tehnologija napreduje također i zaštita podataka, sa svakom novom inovacijama i tehnologijom koja se implementira u e-bankarstvu, osigurava se veća sigurnost osobnih podataka u e-bankarstvu. Kako sve više ljudi koristi e-bankarstvo za upravljanje svojim financijama, pitanja oko sigurnosti osobnih podataka postoji još glasnija i važnija. Implementacijom svake nove tehnologije i inovacije smanjuje se rizik od hakerskim napada i neželjenog oštećenja ili gubitka podataka. Zaštita osobnih podataka postaje sve složenija zbog različitih prijetnji koje mogu ugroziti sigurnost osobnih podataka u e-bankarstvu. Napadi postaju sve sofisticiraniji. Osim zaštite od eksternih čimbenika važno se posvetiti i zaštiti od internih čimbenika poput zaposlenika banke. U slučaju neovlaštenog dijeljenje osobnih podataka klijenata banke, zaposlenici mogu naštetiti ugledu i povjerenju banke. U ovome radu će se navesti načini zaštite osobnih podataka, objasniti obveze i uloge zaposlenika i banke za zaštitu osobnih podataka te objasniti tehnologije koje se koriste pri zaštiti osobnih podataka u e-bankarstvu. Također će se objasniti Opća uredba o zaštiti podataka (GDPR) koja je na snazi u svim državama Europske unije.

2.Teorijska podloga i prethodna istraživanja

E-bankarstvo je u posljednjih par desetljeća doživjelo značaj razvoj i popularnost među korisnicima. Tehnološki napredak je omogućio korisnicima jednostavnije obavljanje niz različitih bankarskih usluga preko Internet i mobilnog bankarstva. Kako napreduje tehnologija tako i banke implementiraju novu tehnologiju i ažuriraju staru kako bi osigurali sigurnost osobnih podataka klijenata banke. Zaštita osobnih podataka je jedan od ključnih faktora kod uspostavljanja povjerenja i sigurnosti korisnika koje banke to shvaćaju ozbiljno. S napretkom tehnologije tako nastaju i nove opasnosti i prijetnje. Osobnim podacima smatra se ime i prezime, adresa stanovanja, datum i mjesto rođenja, OIB, broj telefona, e-mail adresa, IP adresa, primanja i osobna iskaznica ili putovnica. (GDPR Informer, 2023.) Proces zaštite osobnih podataka mora biti usklađen sa zakonodavnim okvirima te mora biti kontinuiran i prilagođen prema novim tehnološkim naprecima i prijetnjama. Najčešće prijetnje su hakerski napadi, virusi i crvotočine, nesigurna mreža, slabo ažuriranje softvera, slaba sigurnosna praksa korisnika i zaposlenika, zlouporaba podataka od strane bankarskih institucija. Te najčešći načini za realiziranje hakiranja prema Široki (2023.) su trojanski program, phising, pharming, lažne web stranice, spoofing, spyware, elektroničke oglasne ploče, internet javne evidencije, trojanski konj i wormhole attack. Veliku ulogu u zaštiti osobnih podataka imaju same banke, zaposlenici banke i korisnici. Vrlo važna je svjesnost zaposlenika i korisnika o mogućim prijetnjama, ako su korisnici i zaposlenici svjesni onda je i lakše educirati ih kako se ponašati u situacijama i kako adekvatno djelovati i prije svega kako izbjegnuti opasnosti. Različite tehnologije se koriste za zaštitu podataka korisnika, najčešće se koriste uređaji za autorizaciju korisnika kao što je TAN tablica, token, display kartica, čitač kartica, USB stick s certifikatom i biometrijski uređaji. Za sigurnost osobnih podataka također se poštuju propis poput opće uredbe o zaštiti osobnih podataka (GDPR). Opća uredba o zaštiti podataka je ujednačena diljem Europske unije što pojednostavljuje i omogućava lakše prilagođavanje banaka propisu. GDPR se isključivo primjenjuje na osobne podatke. Zaštitom osobnih podataka, omogućit će se siguran prijenos i slanje podataka što će uzrokovati sigurnost među klijentima.

2.1. Opća uredba o zaštiti osobnih podataka

Opća uredba o zaštiti podataka (General Dana Protection Regulation – GDPR) je zakonodavni okvir Europske unije koji je stupio na snagu 25. svibnja 2018. godine i primjenjuje se u svim državama članicama Europske unije. (GDPR Informer, 2023.) Cilj GDPR-a je zaštita osobnih podataka građana Europske unije regulirajući prikupljanje, obradu i pohranu podataka. GDPR je zamijenio prethodnu direktivu o zaštiti podataka iz 1995. godine. Propis je ujednačen u diljem Europske unije što pojednostavljuje i omogućava lakše prilagođavanje tvrtkama propisu. GDPR se isključivo primjenjuje na osobne podatke, dok se ostali podatci koji se ne smatraju osobnim podatcima bit će zaštićeni nacionalnim zakonodavstvom država članica. Podaci koji se smatraju osobnim podatcima se odnose na podatke sa kojima se može sa velikom vjerojatnošću ustanoviti identitet pojedinca. GDPR se ne primjenjuje na anonimizirane podatke. (GDPR Informer, 2023) GDPR uredba se odnosi na sve koji se bave obradom podataka koje potječu iz Europske unije, primjenjuje se na udruge, nevladine organizacije i javnih tijela i također ako se posluje sa rezidentima Europske unije i vrijedi za velike i male tvrtke. Kategorije podataka koje GDPR uredba štiti su: osnovni podaci, podaci s kreditnih kartica, pseudonimizirani podaci, zdravstveni karton, biometrijski podaci, genetski podaci, ip adrese, osobne poruke e-pošte, vjerska i filozofska uvjerenja, etnička pripadnost, ekonomsko stanje, seksualna orijentacija i spolni život, kolačići u pregledniku i članstvo u sindikatu. (GDPR Informer, 2023.) Mjere zaštite podataka su implementirati mjere zaštita podataka, uvesti stroge mjere kontrole pristupa podacima, redovito brisanje osobnih podataka koji više nisu u upotrebi ili relevantni i držati se načela integrirane zaštite privatnosti. Ključna načela obrade su podaci se smiju obrađivati samo na valjanoj zakonskoj osnovi, na pošten i prema ispitaniku transparentan način, obavezno navođenje svih svrha obrade u koje se podaci prikupljaju, prikupljati smijete samo podatke koji su relevantni i potrebni za ispunjavanje svrhe u koju se obrađuju, podaci trebaju biti točni i ažurirani, podatke ne smijete pohranjivati duže od razdoblja potrebnog za ispunjavanje svrhe u koju su prikupljeni, dužni se osobne podatke zaštititi od nezakonite i nedozvoljene obrade, slučajnog gubitka ili uništenja, morate biti u stanju dokazati usklađenost s gore navedenim načelima. Države članice su dužne imenovati agenciju koja će u toj državi biti glavno nadzorno tijelo zaduženo za provedu GDPR uredbe. Glavno tijelo će biti nadležno za komunikaciju sa tvrtkama, što ne znači da se ostala državna nadzorna tijela ne mogu uplesti. Pojedinci dobivaju pravo na više kontrole oko svojih osobnih podataka, te mogu odlučivati jel žele da se njihovi osobni podaci prosljeđuju ili budu u posjedu od neke treće strane, ako više ne žele mogu tražiti brisanje tih osobnih podataka koje se naziva pravo na zaborav. Cilj GDPR-a je povratiti povjerenje korisnika u europske tvrtke. U slučaju ako se tvrtke u ovom slučaju banke ne usklade

sa GDPR uredbom, nadzorna tijela ih mogu kazniti ako se ne pridržavaju propisa. Najčešće kazne su upozorenja, opomene, zabrane obrade i novčane kazne, kazne same po sebi su veće što je povreda zakona veća. (GDPR Informer, 2023.)

Načela obrade osobnih podataka su: načelo zakonitosti, poštenosti i transparentnosti, načelo ograničenja svrhe, načelo smanjenja količine podataka, načelo točnosti podataka, načelo ograničenja pohrane i načelo sigurnosti pohrane.

Prema Musulinu (2023.) potrebno je zakonito, pošteno i transparentno obrađivati podatke ispitanika, po takozvanom načelu zakonitosti, poštenosti i transparentnosti. Načelo zakonitosti podrazumijeva da se obrada podataka može smatrati zakonitom samo uz pristanak ispitanika ili na temelju druge legitimne osnove utvrđene zakonodavstvom države članice. (Musulin, 2023.) Prema Musulinu (2023.) svrha načela transparentnosti je informirati ispitanika da će se obrada podataka koristiti samo u svrhe za koje je privola dana. U privoli moraju biti navedene svrhe obrade i navedene kategorije osobnih podataka koji će se obrađivati.

Prema Musulinu (2023.) načelo ograničenja svrhe nalaže da se prikupljeni podaci koriste isključivo u posebne, izričite i zakonite svrhe te da se ne smiju obrađivati na načine koji nisu u skladu s tim svrhama. Cilj je osigurati specifičnost i jasnoću svrhe obrade, povećavajući transparentnost i pravnu sigurnost. Obrada u nedefinirane ili neograničene svrhe nije zakonita. Jasno je propisano zakonom da se obrada osobnih podataka ne može provoditi ako nije jasno definirana, stoga neograničene i nedefinirane svrhe nisu zakonite. Kroz načelo smanjenja količine podatka, obrada podataka je svedena na primjerene, relevantne i ograničene na one nužne u odnosu na svrhu obrade. Podaci koji se obrađuju prema predmetnom načelu su „primjereni, relevantni i ne previše opsežni u odnosu na svrhu njihova prikupljanja“. (Musulin, 2023.) Kategorije koje su odabrane bi morale biti nužne za postizanje ciljeva postupka obrade podataka. Načelo točnosti podatka nalaže da podaci moraju biti točni i po potrebi ažurirani. Kako bi se osigurala njihova točnost, potrebno je poduzeti potrebne i odgovarajuće mjere. Ako dođe do pogreške pri unosu podataka, podatci se ne smiju brisati već bi se trebala dodati napomena, koja bi jasno ukazala da se radi o naknadnim unosima u odnosu na originalan podatak. Osobni podaci trebaju se čuvati u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno za svrhe radi kojih su prikupljeni, što se naziva načelom ograničenja pohrane. Ovo načelo znači da se osobni podaci moraju izbrisati ili anonimizirati čim više nisu potrebni za svrhu za koju su prikupljeni.

Osim toga, osobni podaci moraju se obrađivati na način koji osigurava njihovu sigurnost prema načelu sigurnosti podataka Musulin (2023.) navodi kako je potrebno provesti odgovarajuće tehničke ili organizacijske mjere prilikom obrade osobnih podataka kako bi se podaci zaštitili od neovlaštenog ili nezakonitog pristupa, upotrebe, izmjene, otkrivanja, uništenja ili oštećenja. Navedena odgovarajuće mjere zaštita također mogla uključivati pseudonimizaciju.

2.2. E-Bankarstvo

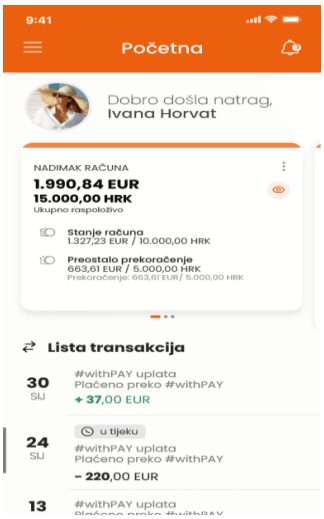
E-bankarstvo ili online bankarstvo su bankarske usluge koje se omogućavaju klijentima banke da obavljaju svoje financijske transakcije korištenjem elektroničkih kanala poput interneta, telefona i mobilnih uređaja. Ovaj oblik bankarstva omogućuje svojim klijentima da obavljaju niz različitih stvari online bez potrebe za odlaskom do fizičke poslovnice. Prema Birovčevci (2021) e-bankarstvo je nastalo kao odgovor financijskih institucija na promjene uvjete potražnje na tržištu, zbog razvoja informacijskih i komunikacijskih tehnologija te pojave računalnih tehnologija i široki spektar proizvoda povezanih s njome. E-bankarstvo se najčešće odvija preko mobilne aplikacije banke ili web stranice banke. Banke preko e-bankarstva omogućuje klijentima da pristupe svome bankovnome računu, pregledavaju stanje računa, plaćaju račune, zahtjeve za kredite, prenose novac, komuniciraju sa bankom i korisničkom potporom, upravljaju svojim sredstvima, pregledavaju izvod, kupovina i plaćanje putem interneta i druge financijske aktivnosti. Klijenti banke koji koriste e-bankarstvo najčešće koriste metodu autentifikacije preko korisničkog imena i lozinke. (Azop, 2023.) Također se može potvrditi identitet preko biometrijskih metoda poput otiska prsta, šarenice oka. Biometrijska metoda autentifikacije identiteta dobiva sve više na popularnosti zbog svoje visoke razine sigurnosti i jednostavnosti. Ostale metode za autentifikaciju identiteta mogu biti: jednokratne lozinke, digitalni potpis i kod za pristup. E-bankarstvo zbog svoje praktičnosti omogućuje svojim korisnicima pristup svome računu bilo kada i bilo gdje jer nije limitirano radom fizičke poslovnice i tako korisnici štede na vremenu od mogućih gužva i na novcu od mogućih troškova za čekove i papirnate izvode. Zbog svojih dobrih karakteristika poput fleksibilnosti, praktičnosti i pristupačnosti u bilo koje vrijeme dana je vrlo atraktivno klijentima. Praktičnost e-bankarstva nema granice zbog svoje lake pristupačnosti, sigurnosti, uštede vremena i mogućnosti upravljanja svojim računom. Prema Rončeviću (2006.) zbog sve većeg broja ljudi koji su informatički pismeni i informatiziranih radnih mjesta, usluge e-bankarstvo postaju sve jeftinije i pristupačnije većem broju klijenata. Kako tehnologija napreduje tako također napreduje i e-bankarstvo, što također sve više osvještava sadašnje i buduće korisnike o korisnosti i praktičnosti e-bankarstva. Sa razvojem tehnologije također ujedno se razvija i opasnost. E-bankarstvo je vrlo sigurno jer radi na svojoj sigurnosti i prati visoko propisane standarde o sigurnosti. Makar je e-bankarstvo vrlo sigurno također nosi sa sobom malu dozu rizika. Prema Ćuriću (2017.) vrlo prisutno e-bankarstvo nije uzrok nastanka novih rizika u poslovanju banaka, nego utječe na promjenu već poznatih rizika koje se treba procijeniti i postaviti adekvatnu sigurnosnu infrastrukturu. Kako bi se smanjili ili izbjegli ti mogući rizici, banke savjetuju da se koriste snažne lozinke, izbjegavaju pristupi bankovnom računu preko javnih mreža i

ažuriraju svoj softver i uređaje. Očekuje se da i korisnici e-bankarstva kontroliraju i provjeravaju svoje transakcije kako bi se lakše utvrdio i otklonio problem. (Azop, 2023.) Kako bi banke omogućile što bolji doživljaj e-bankarstva također nude korisničku podršku i komunikaciju sa bankom preko slanja poruka, postavljanja upita i traženja pomoći putem mobilnih aplikacija i internetskog bankarstva. Upravljanje korisničkim postupcima omogućuje korisnicima da upravljaju svojim preferencijama i postavkama korisničkog računa poput: promjene lozinke, postavljanja obavijesti, ažuriranje osobnih podataka i komunikaciju sa bankom. Glavne podjele e-bankarstva su na internetsko bankarstvo, mobilno bankarstvo, online investiranje, elektronski prijenos novca, online krediti i financiranja. Najzastupljeniji oblici e-bankarstva su internetsko bankarstvo i mobilno bankarstvo zbog svoje jednostavnosti i praktičnosti. Prema Birovčecu (2021.) sve češće se počinje koristiti termin digitalno bankarstvo, jer zbirno opisuje Internet i mobilno bankarstvo, koje je temeljeno na digitalnim tehnologijama. E-bankarstvo je postao standardno u bankarstvom sektoru. U današnje vrijeme sve više se ulaže u nove tehnologije i inovacije kako bi poboljšale iskustvo i sigurnost, sve više se primjenjuje blockchain, umjetna inteligencija i biometrijske metode za autentifikaciju. E-bankarstvo kao svaka stvar ima svoje prednosti i nedostatke. Prednosti e-bankarstva su njegova praktičnost, dostupnost, brzina, ušteda vremena i novca, sigurnost i razne druge usluge. Praktičnost je jedna od glavnih karakteristika i prednosti e-bankarstva. Praktično je zbog obavljanje raznih poslova koje uključuju banku bilo kada i bilo gdje što omogućuje korisnicima neovisnost o fizičkoj poslovnici banke. Praktičnost se nadovezuje na dostupnost jer nema ograničenog radnog vremena i također na brzinu transakcije koja se obavlja u stvarnom vremenu bez čekanja u redu. Zbog svoje brzine korisnik štedi na svome vremenu i bez potrebe za odlaskom do fizičke poslovnice eliminira mogućnost dodatnih troškova poput putovanja i papirnate izvode. Jedna od ključnih prednosti e-bankarstva je sigurnost koja je jedan od glavnih motivatora klijenata. Banke provode visoke mjere sigurnosti koje su propisane zakonom uz pravilno korištenje e-bankarstva i održavanje sigurnosnih mjera, e-bankarstvo može biti vrlo sigurno. Nedostaci e-bankarstvu su sigurnosni rizici, tehnički problemi, tehnička pismenost, nedostatak fizičkog nadzora i nedostatak osobnog kontakta. Iako banke svakodnevno ulažu napore u osiguranje podataka i sigurnosti korisnika i dalje postoje rizici od prijevara i hakiranja jer kako tehnologija napreduje tako se prilagođavaju i hakeri na nove tehnologije. Osim banaka moraju i korisnici biti osviješteni o mogućnosti prijevara i također moraju uložiti svoj doprinos pri očuvanju podataka i sigurnosti. Korisnici doprinose tako da koriste jake lozinke i izbjegava pristupanje računu putem nesigurnih mreža. Tehnički problemi nastaju kada je prekinuta internetska veza, kvarovi u sustavu ili tehničke greške, mogu utjecati na funkcioniranje e-

bankarstva. Informatička pismenost je vrlo važna jer e-bankarstvo zahtjeva određenu razinu informatičkog znanja. Korisnici sa manje iskustva mogu se suočiti sa izazovima pri korištenju i prilagođavanju e-bankarstvu. Nedostatak osobnog kontakta može utjecati negativno na dio korisnika koji su navikli na osobni kontakt. Nedostatak fizičkog nadzora može uzrokovati kod nekih korisnika osjećaj nesigurnosti zbog nepostojanja fizičkog nadzora nad svojim novcem i transakcijama. Uzimajući u obzir prednosti i nedostatke važno je razumjeti vlastite potrebe i na temelju svojih potreba procijeniti što više odgovara.

2.3. Mobilno i internet bankarstvo

Mobilno bankarstvo je vrsta e-bankarstva koja omogućava i pruža svoje usluge klijentima putem mobilnih uređaja poput pametnih telefona i tableta. (Moj bankar, 2023.) Korisnicima je omogućeno upravljanje njihovim računom preko mobilne aplikacije. Korisnici kako bi pristupili svome računu moraju preuzeti mobilnu aplikaciju koju je banka razvila i od banke koje koristi, nakon što se instalira potrebna aplikacija, korisnik se prijavljuje putem svojeg mobilnog uređaja. Mobilno bankarstvo pruža vrlo slične usluge kao Internet bankarstvo a razlika je u tome što je mobilno bankarstvo optimizirano za mobilne platforme. Mobilno bankarstvo omogućuje svojim korisnicima da mogu pogledati svoje stanje računa, platiti račune, otvoriti nove račune, izvršiti prijenos, provjeriti transakcije i također se može pristupiti digitalnim dokumentima i obavijestima putem mobilne aplikacije. Prema Kovačeviću (2017.) ako korisnik želi pristupiti svom računu preko mobilnog bankarstva, potrebna mu internetska veza poput bežične ili mobilne mreže. Za sigurnost putem mobilnog bankarstvo najčešće se koristi biometrijska metoda potvrde poput otiska prsta koji je najčešći i najzastupljeniji, također se koristi prepoznavanje lica i push obavijesti kako bi se poboljšao doživljaj korištenja mobilne aplikacije.

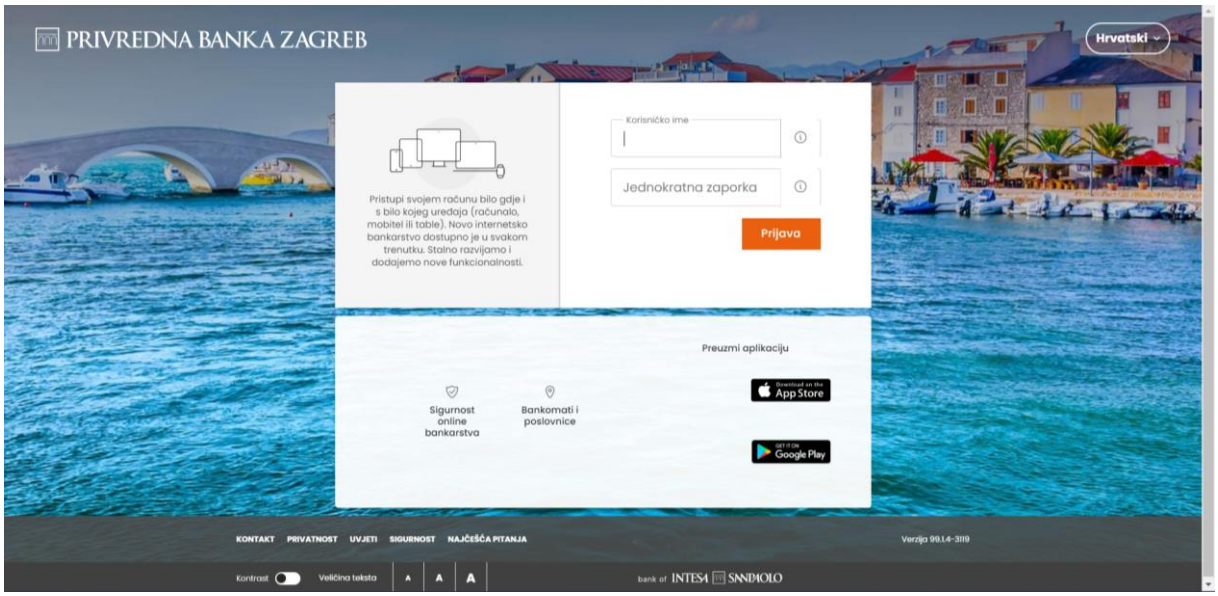


Slika 1. Prikaz ekrana početne stranice nakon prijave u aplikaciju

(Izvor: PBZ, 2023., dostupno na: https://www.pbz.hr/studenti/digitalno-bankarstvo/internet-i-mobilno-bankarstvo.html, preuzeto: 11.07.2023.)

Internet bankarstvo je vrsta e-bankarstva koja pruža i omogućava svoje usluge putem interneta svojim klijentima (Moj bankar, 2023). Korisnici Internet bankarstva pristupaju svojim bankovnim računima preko interneta najčešće preko računala ili prijenosnog računala poput laptopa. Preko web preglednika korisnik pristupa bankarskoj platformi. Kako bi korisnik

pristupio svom računu mora se prijaviti sa valjanim korisničkim imenom i lozinkom. Internet putem bankarstvo omogućuje svojim korisnicima da mogu pogledati svoje stanje računa, platiti račune, otvoriti nove račune, izvršiti prijenos, provjeriti transakcije i također se može pristupiti digitalnim dokumentima i obavijestima. Za sigurnost internet bankarstvo najčešće se koriste dvofaktorske autentifikacije i enkripcije podataka kako bi se osiguralo njihovo slanje i sigurnost. Internet bankarstvo omogućuje brz i praktičan način upravljanja njihovim računom.



Slika 2. Prikaz ekrana pri prijavi preko web preglednika

(Izvor: PBZ, 2023., dostupno na: https://www.pbz.hr/studenti/digitalno-bankarstvo/internet-i-mobilno-bankarstvo.html, preuzeto: 11.07.2023.)

3. Zaštita osobnih podataka

Zaštita osobnih podataka u e-bankarstvu je niz mjera, zakona i prakse koje su vrlo važne za osiguravanje integriteta i povjerljivosti podataka korisnika. Osobni podatak je svaki podatak koji se odnosi na nekog pojedinca koji se može identificirati na temelju informacija i obilježja koje su specifične za identitet tog pojedinca. Pod osobne podatke se smatraju: ime i prezime, adresa stanovanja, datum i mjesto rođenja, OIB, broj telefona, e-mail adresa, IP adresa, primanja i osobna iskaznica ili putovnica. (GDPR Informer, 2023) Zaštita osobnih podataka je jedan od ključnih faktora kod uspostavljanja povjerenja i sigurnosti korisnika. Sa očuvanjem integriteta podataka, banke rade na tome da uspostave mjere zaštita podataka i da se korisnici osjećaju sigurno i cijenjeno. Proces zaštite osobnih podataka mora biti usklađen sa zakonodavnim okvirima, također treba biti kontinuiran i stalno prilagođen novim tehnološkim naprecima i prijetnjama. Zbog neprestanog razvoja tehnologije i novih tehnoloških otkrića, zaštita stalno zahtjeva nadogradnju i implementaciju novih tehnologija. Najčešće prijetnje za osobne podatke su: neovlašteni pristup podatcima, krađa identiteta, neovlaštena ili zloupotreba distribucije podataka, pokretanje virusa, krađa hardver, softvera ili digitalnog sadržaja. U Europskoj uniji se primjenjuje Opća uredba o zaštiti podataka (GDPR) koja štiti korisnikove podatke pomoću propisanih zakona o prikupljanju, obradi i pohrani osobnih podataka. Za zaštitu osobnih podataka se primjenjuju principi koje banka mora osigurati a neki principi su: povjerljivost podataka, integritet podataka, raspoloživosti podataka, minimalno potrebno prikupljanje podataka, pravo na pristup i ispravak podataka, rok čuvanja i tehničke ili organizacijske mjere. (GDPR Informer, 2023) Također osim principa se moraju primjenjivati i mjere zaštite podataka koje su tehničke, sigurnosne i organizacijske naravi. Mjere koje koriste banke u zaštiti osobnih podataka su: identifikacija, autorizacija, autentifikacija, enkripcija podataka, obrazovanje zaposlenika, obrazovanje korisnika, redovito ažuriranje i sigurnosne zakrpe, antivirusne zaštite, kontrola pristupa podatcima i redovito brisanje osobnih podataka koji više nisu potrebni ili relevantni. Najčešće korišteniji mehanizmi za zaštitu u e-poslovanju su identifikacija, autorizacija i autentifikacija koje se dijele na fizičke i logičke mjere. Identifikacija funkcionira tako da traži od korisnika da se predstavi sustavu sa svojim korisničkim imenom i prezimenom ili identifikacijskim brojem kako bi mogao pristupiti svome korisničkom računu. Autorizacija funkcionira tako da sustav provjerava da li korisnik koji se predstavio ima valjane ovlasti kako bi pristupila sustavu kojem se prijavljuje. Za autorizaciju korisnika u sustavu e-bankarstva koriste se uređaji poput TAN tablice, token, display kartice, čitač kartice, USB stick sa certifikatom i biometrijski uređaji. Autentifikacija je najčešće povezana sa procesom identifikacije jer utvrđuje da li je ta osoba zbilja ta osoba kako se

predstavlja, korisnik potvrđuje najčešće sa lozinkom ili tokenom. Za autentifikaciju osobe se često koristi elektronički potpis ili napredni elektronički potpis. Kako bi se osigurala tajnost podataka pri prijenosu pri različitim računalnim mrežama koristi se kriptografija. Kriptografija je postupak kojim se poruka učini nerazumljivom za osobe koje nisu sudionici razgovora, a kripto analiza bi bio obrnuti postupak pomoću kojeg se pokušava saznati kako su napisane kriptirane poruke sa kojim ključem. U e-poslovanju kriptografija se ne koristi samo za kriptiranje sadržaja nego i za provjeru identiteta u business to customer i buisness to buisness poslovanjima. Svaki kriptološki sustav se sastoji od četiri osnovna elementa kao što su originalna razumljiva poruka, kriptirani tekst koji je nerazumljiva poruka, algoritam kriptiranja to je matematički algoritam sa kojim se originalni razumljivi sadržaj kriptira i ključ koji ima ulogu pomoću kojeg se dekriptira poruka. Dva osnovna kriptografska sustava su simetrični sustavi i asimetrični sustavi, razlikuju se po tome što simetrični sustav je sa tajnim privatnim ključem dok je asimetrični sustav sa privatnim i javnim ključem. Simetrični sustav kriptografije je stariji sustav kriptografije koji koristi isti ključ za dekriptiranje i kriptiranje poruke, primatelj i pošiljatelj poruke se trebaju dogovoriti oko tajnog ključa sa kojeg će koristiti i treba biti poznat samo pošiljatelju i primatelju, ovaj način kriptiranja više nije učinkovit. Asimetričan sustav kriptiranja sa sastoji od privatnog i javnog ključa, privatni ključ ima ulogu da ga zna samo određeni poslužitelj, dok javni ključ se šalje svim sudionicima komunikacije javno i svima je dostupan. Pomoću asimetričnog sustava kriptiranja može provjeriti autentičnost pošiljatelja poruke. Najpopularniji asimetrični sustavi kriptiranja su RSA, PGP, SET i SSL. Jedna od osnovnih prava ispitanika banke, su zahtjevi za ostvarivanje prava poput ispitanika na pristup, brisanje, ispravaka, ograničenje obrade, prenosivost podataka, prigovor. Banka treba imati jasne i transparentno opisane politike privatnosti gdje opisuju prikupljanja, korištenje i čuvanje osobnih podataka korisnika. (HPB, 2023)

3.1. Obveze banke za zaštitu osobnih podataka klijenata

Banke imaju puno zakonskih i etičkih obveza za zaštitu osobnih podataka klijenta kako bi očuvale njihovu cjelovitost i privatnost njihovih informacija. Jedna od glavnih obveza banke je informirati klijente o svrsi prikupljanja podataka i tražiti njihovo odobrene za prikupljanje podataka, osim ako je prikupljanje nužno zbog zakonskih obveza ili izvršenja nekog ugovora. Banke prikupljaju podatke o svojim klijentima kako bi im pružili što bolju i personaliziraniju uslugu. Banke bi trebale prikupljati samo one podatke koji su im nužni za određene usluge jer inače ako bi prikupljale nepotrebne podatke to bi klijent smatrao nepoželjnim. (HPB, 2023) Prikupljanjem viška nebitnih podataka može predstavljati rizik pri sigurnosti, također trebaju obrađivati podatke u skladu sa važećim zakonima. (Azop, 2023) Poštujući načelo minimalizacije banke su obvezne prikupljati samo one osobne podatke koje su im nužni za pružanje njihovih bankarskih usluga. Unutar Europske unije banke se moraju pridržavati Opće uredbe o zaštiti osobnih podataka (GDPR). Banka prema Općoj uredbi o zaštiti osobnih podataka bi trebala štiti osobne podatke klijenta preko kojih se može identificirati klijent a najčešći osobni podatci su ime, prezime, broj osobne iskaznice, podaci sa kreditne kartice, zdravstveni karton, ip adresa, etnička pripadnost, genetski podatci, biometrijski podatci, članstva, seksualnu orijentaciju, spolni život, osobne poruke e-pošte i kolačiće u pregledniku. (GDPR Informer, 2023) Osiguravanje podataka klijenta je vrlo važna za zaštiti osobnih podataka klijenta i jedan od obveza koje banka mora ispuniti. Prema Zekić-Sušac (2013.) da bi postupak obrade podataka bio siguran, banke bi trebale obratiti pažnju na sigurnost i ažurnost mreža te hardverske i softverske opreme. Sa ciljem zaštite osobnih podatka klijenta, banka mora poduzeti odgovarajuće tehničke i sigurnosne mjere kako bi zaštitila podatke od moguće krađe, oštećenja, gubitka i neovlaštenog korištenja. Kako bi se preveniralo postoje sigurnosni protokoli poput enkripcije podataka, osiguravanja sigurnosti mreža, osiguravanje sigurnosti sustava, osiguravanje pristupa samo ovlaštenim osobama, redovito testiranje sigurnosti i obuka zaposlenika o sigurnosnim praksama. Dijeljenje ili razmjena podataka o klijentu je zabranjeno ako klijent nije pristao na to osim u rijetkim slučajevima gdje je zakonom dopušteno ili nužno. (Azop.hr, Agencija za zaštitu osobnih podataka 2023) Banke su obvezne stalno održavati cjelovitost i povjerljivost osobnih podataka klijenta što bi značilo da ne smiju zlorabiti ili mijenjati podatke bez opravdanog razloga. Banke trebale osigurati da su točni osobni podatci i također ažurni i čuvani u skladu sa propisima za ono razdoblje za koje su potrebni. Ukoliko se dogodi neka povreda sigurnosti koja može rezultirati prema neovlaštenom pristupu, gubitku osobnih podataka ili otkrivanju osobnih podataka, onda su banke dužne obavijestiti klijente i nadležna tijela. Obavijest o neovlaštenom pristupu, gubitku ili otkrivanju osobnih podataka bi

trebala biti pravovremeno poslana i sadržavati sve bitne i relevantne podatke o mogućim učincima. (Azop, 2023)

3.2. Uloga zaposlenika banke u zaštiti podataka klijenata

Uloga zaposlenika banke u zaštiti podataka klijenta je vrlo važan faktor osiguravanja privatnosti, sigurnost i cjelovitost podataka. Zaposlenici su jedan od ključnih faktora pri zaštiti podatka klijenta i trebaju biti upoznati sa politikama banke. Zaposlenici bi trebali biti profesionalni pri odrađivanju svojih zadataka i strogo poštovati i pridržavati se pravila i etičkih kodeksa. Profesionalnost bi okarakteriziralo da se ne dijele osobni podatci sa trećim stranama koje nemaju pristup tim informacijama. Povjerljivi podaci mogu biti financijski i osobni podaci, PIN i broj računa. (Azop, 2023) Zaposlenici bi jedino trebali imati pristup takvim podacima ako imaju dozvolu i ako je nužno za izvršavanje nekih poslovnih aktivnosti. Banka bi trebala održavati redovitu obuku o zaštiti podataka i zaposlenici bi je trebali pohađati, takav tip obuke se naziva ongoing obuka jer je stalna i pomaže zaposlenicima pri osvježavanju znanja o propisima, prijetnjama i postupcima. Ongoing obuka pomaže zaposlenicima da budu ažurni pri zaštiti podataka klijenata kako bi mogli prepoznati prijevare i prijetnje te kako bi znali adekvatno reagirati u tim slučajevima. Sa postavljanjem kontrolnog mehanizma banka bi implementirala stroge kontrolne mehanizme koji bi osigurali da samo ovlaštene osobe na određenim razinama imaju pristup na određenim razinama podatcima klijenta, trebaju se postaviti jasni kriteriji. Kako bi se podaci sigurno obradili zaposlenici bi trebali koristiti adekvatne alate za obradu podataka i sigurne postupke. (HNB – Hrvatska narodna banka, 2023)

Kako bi postupak obrade bio siguran treba se koristiti enkripcija, sigurna mreža i softverska aplikacija tijekom cijelog postupka prijenosa podataka, što utječe na smanjenje rizika od curenja podataka ili neovlaštenog pristupa. (Azop, 2023) Zaposlenici bi trebali biti svjesni cijelo vrijeme i biti na oprezu pri nadgledanju aktivnosti sustava, gdje god bi učili neku nepravilnost ili sumnjivu i neobičnu aktivnost trebali bi poduzeti adekvatne postupke pri otkrivanju i rješavanju takvih mogućih prijetnji. Zaposlenici trebaju poznavati propise i biti usklađeni sa zakonom kako nebi nesvjesno postupili protu zakona i tako naštetili banci i klijentu. Također poznavajući zakon lakše se može izbjeći šteta i pogreška. U slučaju pogreške zaposlenik bi trebao biti upoznat sa reagiranjem na incident, kako bi ispravio što prije nepravilnost. Prema Ćuriću (2017.) trebalo bi se najviše pridonijeti pažnje prema ljudskom faktoru jer je najčešća vrsta prijetnje, ljudski faktor može biti namjeran ili nenamjeran.

3.3. Tehnologije za zaštitu osobnih podataka u e-bankarstvu

U e-bankarstvu postoje različite tehnologije koje se koriste za zaštitu osobnih podataka. Jedni od najzastupljenijih tehnologija za zaštitu podataka su uređaji za autorizaciju korisnika. Najčešći uređaji za autorizaciju korisnika su TAN tablica, token, display kartica, čitač kartica, USB stick s certifikatom i biometrijski uređaji.

TAN tablica je matrica brojeva u kojoj su obilježeni redci sa brojevima a stupci sa slovima. Klijent dobiva TAN tablicu u plastificiranom papiru koja mu koristi pri ulasku u sustav, klijentu prilikom prijave u sustav budu predloženi nasumično odabrani redci i stupci koje klijent mora pogledati na plastificiranom papiru i pravilno onda unijeti. Ukoliko je unos ispravan klijentu je odobren ulaz u sustav. Zbog svoje nesigurnosti ovakav je način napušten jer ako netko prisvoji TAN tablicu od klijenta onda pomoću nje može lako ući u sustav. Prema Hrehoroviću (2023.) TAN tablice se sve više zamjenjuju naprednijim metodama poput SMS kodova, mobilnih aplikacija ili sigurnosnih tokena. Token je fizički uređaj ili program kojeg dobiva autorizirani korisnik za svoju autentifikaciju u sustav, token mu služi za generiranje jednokratne lozinke poput osobnog PIN-a klijenta sa kojim dokazuje da je on taj za kojega se izdaje taj token. Ovaj uređaj ima funkciju ključa za pristup nekom sustavu i vrlo je čest u e-bankarstvu. Prema Hrehoroviću (2023.) koriste se tri vrste tokena a to su hardverski, softverski i mobilni token. Token funkcionira tako da ga nije potrebno spojiti sa računalom, nego je dovoljan neki drugi izvor energije poput baterije. Token na svome zaslonu prikazuje lozinku koja se sastoji od brojeva, klijent bi trebao pri prijavi u sustav unijeti taj broj sa zaslona i također dodatni PIN koji je potpisivanjem ugovora dobio od banke. Noviji tokeni se spajaju preko Bluetooth mreže sa računalom i omogućavaju sigurnije spajanje i zaštitu, jer su token bili podložen napadima zvanim mani n the middle. (HNB, 2023) M-token je programska podrška odnosno aplikacija koja se instalira na mobilni uređaj poput mobilnog telefona ili tableta i koristi se kao zamjena za fizički token. Kako bi se koristio m-token korisnik bi treba imati adekvatnu opremu koja podržava platforme od banke koju koristi i da ima omogućen GPRS pristup internetu s mobilnog uređaja. Instalacija m-tokena teče tako da na mobilni uređaj se inicira sa dostavljanjem SMS poruke koja sadrži poveznicu u obliku linka za preuzimanje aplikacije m-tokena, nakon preuzimanja unosi se PIN broj koji se aktivira jednokratno zaporku koja se kasnije koristi u kombinaciji sa PIN-om za ulaz u sustav. Display kartica služi kao sredstvo za prijavu i autorizaciju transakcija putem elektronskog bankarstva (Erste Banka, 2024). Display kartica je kartica nove generacije koja može funkciju debitne kartice, kreditne kartice i tokena. Korištenjem display kartice eliminira se potreba za korištenjem dodatnog autentifikacijskog tokena. Kartica također sadrži maleni LCD zaslone i osjetljive tipke na dodir. Prednosti display

kartice su što je jednostavna za korištenje, sigurnija od TAN tablice i nepotrebno je nošenje dodatnih tokena za kreiranje jednokratnih lozinki. U Hrvatskoj prva banka koja je uvela display je bila Erste banka. (HNB, 2023) Čitač kartica je identifikacijski uređaj opremljen sa zaslonom i tipkovnicom koji služi za autorizaciju i pristup transakcijama u e-bankarstvu sa pomoću čip kartica, veličine je kartice. Uređaj se spaja preko USB utora, dok se autentifikacija obavlja sa pomoću certifikata koji se instalira na računalo i potvrđuje sa dodatnim PIN brojevima, koriste ga uglavnom poslovni subjekti. Prednosti čitača kartice je što povećava sigurnost upotrebe kartice sa čipom u usporedbi sa karticom sa magnetskom trakom, dok je nedostatak to što je postoji proces instalacije programske podrške i certifikata. U Hrvatskoj prva banka koja je počela koristiti čitale za autorizaciju je Privredna banka Zagreb. USB stick sa certifikatom je uređaj koji radi na sličnom principu poput čitača kartice, prednost njegova je što je manji što ga čini jednostavnijim za nošenje. Koriste ga uglavnom poslovni subjekti. Uređaj se koristi tako da se spoji putem USB utora na računalo nakon toga autentifikacija se obavi tako da se instalira na računalo korisnika i da se koristi dodatni PIN brojevi. (HNB, 2023) Prema Boban i Periš (2015.) najvažniji element u procesu prepoznavanja uzoraka je digitalizacija. Te tvrde kako se suvremena biometrijska identifikacija temelji na prepoznavanju biometrijskih značajki, te uspoređivanje sa pohranjenog uzorkom koji je u podatkovnom obliku unutar baze podataka određenog sustava. Prema Desović (2020.) najučestalija biometrijska tehnologija je tehnologija otiska prsta, dok su ostale biometrijske tehnologije poput čitača dlanova i vena, prepoznavanje glasa i čitači otkucaja srca najmanje korištene biometrijske tehnologije. Biometrijski uređaji za autorizaciju koriste razne biometrijske metode poput fizičkih karakteristika kako bi identificirali identitet korisnika. Biometrijske metode autorizacije dijele se na fizičke metode, metode ponašanja i multimodalne metode. Fizičke metode su otisak prsta, čitanje DNK zapisa, prepoznavanje lica, geometrija šake, skeniranje rožnice oka i provjera vena. Metode ponašanja su dinamika tipkanje, dinamika hoda, prepoznavanje glasa, prepoznavanje rukopisa i prepoznavanje potpisa. Multimodalne metode kombiniraju fizičke metode i metode ponašanja. (GDPR Informer, 2023)

Za osiguranje tajnosti osjetljivih podataka pri prijenosu na različitim računalnim mrežama koristi se kriptografija. Kriptografija je postupak kojim se poruka učini nerazumljivom za osobe koje nisu sudionici razgovora, a kripto analiza bi bio obrnuti postupak pomoću kojeg se pokušava saznati kako su napisane kriptirane poruke sa kojim ključem. Kriptologija je znanost o šifriranju i dešifriranju podataka. Dva osnovna kriptografska sustava su simetrični sustavi i asimetrični sustavi, razlikuju se po tome što simetrični sustav je sa tajnim privatnim ključem

dok je asimetrični sustav sa privatnim i javnim ključem. Kriptološki sustav se sastoji od originalne razumljive poruke, kriptiranog teksta koji je nerazumljiva poruka, algoritam kriptiranja to je matematički algoritam sa kojim se originalni razumljivi sadržaj kriptira i od ključa koji ima ulogu dekriptiranja i kriptiranja poruka. Elektronički potpis je skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani sa ostalim drugim podacima u elektroničkom obliku, koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta. Također se koristi napredni elektronički potpis koji pouzdano jamči identitet potpisnika i koji udovoljava uvjetima da je povezan isključivo s potpisnikom, da je nedvojbeno identificira potpisnika, da nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika, da sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka. Napredan elektronički potpis ima istu pravnu snagu i stoga zamjenjuje vlastoručni potpis ako je izrađen u skladu s odredbama Zakona o e-potpisu. Enkripcija također služi za zaštitu podataka prilikom prijenosa jer je to proces pretvaranja informacije u sigurniji oblik za prijenos i potreban je odgovarajući ključ za dešifriranje podatka. Postoje dvije razine enkripcije a to su 40-bitna enkripcija i 128-bitna enkripcija. Prema Najčešći sigurnosni protokoli koji se koriste za prijenos kriptiranih podataka su Secure Socket layer (SSL) i Standard Security electronic transaction (SET). Kako bi se povećala sigurnost mreže banke često koriste intranet, to jest lokalna ili privatna mreža za neku tvrtku ili instituciju koja funkcionira kao i Internet za prijenos informacija. Intranet se štiti od uljeza sa interneta pomoću firewalla koji je uređaj ili program koji razdvaja fizički intranet od Internet mreže i tako sprječava neželjenih uljeza. Firewall pušta samo željeni promet sa interneta, a funkcionira tako da filtrira ulazne poruke putem namjenskog autorizacijskog poslužitelja i putem ovlaštenih autorizacijskih poslužitelja. Najpopularniji vatrozidi za kućnu upotrebu su Windows firewall, pfSense SG-2100, WatchGuard, Firebox Model T15, Bitdefender BOX, Mikrotik hEX RB750Gr3, Zyxel Next Generation VPN Firewall, CUJO AI Smart Internet Security Firewall. Prema Kovačeviću (2017) najkorišteniji antivirusni programi za zaštitu od virusa i crvotočina su AVG, McAfee Antivirus, Esset NOD32, BitDefender, Fprot i HouseCall. Vise faktorska autentifikacija se služi kombinacijom više faktora za potvrdu identiteta korisnika. Osim što koristi tradicionalne korisnička imena i lozinki, koristi također dodatne faktore poput biometrijski podataka ili jednokratnih sigurnosnih kodova poslanih na mobilni uređaj korisnika. Kako bi se osigurala zaštita podataka od gubitka ili oštećenja, banka redovito stvara sigurnosne kopije tih podatka. Sigurnosne kopije se pohranjuju na udaljenim lokacijama kako bi bile dostupne u slučaju nekih tehničkih kvarova ili prirodnih katastrofa. Sa vremena na

vrijeme banka provodi penetracijsko testiranje kako bi utvrdila slabosti, sve se provodi u stimuliranim uvjetima i nakon toga se radi na poboljšanju i jačanju sustava. Također se koriste sustavi za otkrivanje i sprečavanje napada (IDPS) koji mogu preko analize mrežne aktivnosti i prometa podataka prepoznati sumnjiva obrasce i tako automatski reagirati i poduzeti mjere zaštita poput blokiranja prometa i upozoravanje. Sustav za otkrivanje upada (IDS) je također sigurnosni sustav koji nadzire mrežni promet i tako dekretira sumnjive ili zlonamjerne aktivnosti. Sustav za otkrivanje upada omogućava sigurnosnim timovima brzu reakciju pri sprečavanju napada prije nego što se prouzroči šteta.

3.4.Problemi i prijetnje u zaštiti osobnih podataka

Zaštita i sigurnost osobnih podataka su vrlo važne u kontekstu e-bankarstva. Iako banke stalno poduzimaju nove mjere i implementiraju nove tehnologije, i dalje postoje prijetnje za sigurnost osobnih podataka. Najčešće prijetnje su hakerski napadi, virusi i crvotočine, nesigurna mreža, slabo ažuriranje softvera, slaba sigurnosna praksa korisnika i zaposlenika, zlouporaba podataka od strane bankarskih institucija. Hakerski napadi su jedni od najvećih rizika koji pokušavaju neovlašteno pristupiti osobnim podatcima korisnika banke, hakerski napad može rezultirati krađom identiteta i financijskom prijevarom. Prema Široki (2023.) najčešća podjela programa za hakiranje je na viruse, crve, trojance, adware i spyware. Virusi su računalni programi koji se ubacuju u uobičajene korisničke programe koje zatim mijenjaju, namjera virusa je prouzročiti štetu. Virusi mogu oštetiti datoteke, obrisati datoteke i njihov sadržaj, oštetiti programe i prouzročiti teškoće u radu. Crvi su neovisni samostalni programi koji se reproduciraju u umreženim računalima i tako šire štetu, crvi su opasniji od virusa jer se teže kontroliraju. Nesigurna mreža omogućuje hakerima pristup podacima, zato se preporučuje korištenje sigurnih mreža. Saba sigurnosna praksa je se pojavljuje kod korisnika jer nisu dovoljno svjesni opasnosti, nastaje zbog slabo postavljenih lozinka i slabog mijenjanja lozinka što omogućuje jednostavniji pristup hakeru do njihovih računa. Slabo i nedovoljno ažuriranje sustava može otvoriti vrata hakeru tako da pronađe sigurnosne propuste u starijim verzijama, dok u novijim verzijama je to ispravljeno. Nedovoljna enkripcija podataka može prouzročiti da podaci nisu pravilno šifrirani prilikom pohrane podataka ili prijenosa podataka, što može omogućiti hakerima pristup podacima. Zloupotreba podataka od same bankarske institucije može nastati pri zlouporabi ili neovlaštenom dijeljenju podataka, stoga je vrlo važno da banke imaju uređene politike o privatnosti.

5. Metodologija istraživanja

Cilj i predmet ovog rada je istražiti o problemu zaštite osobnih podataka u e-bankarstvu. U izradi ovoga rada korištena je znanstvena i stručna literatura iz područja e-bankarstva, Internet bankarstva, mobilnog bankarstva te zaštite osobnih podataka. Osim toga, korištene su web stranice banaka kao i službene stranice Europske unije koje se odnose na reguliranje zaštite osobnih podataka. U radu je detaljno opisana zaštita osobnih podataka, opća uredba o zaštiti osobnih podataka, tehnologija za zaštitu podataka, obveze banaka i uloge zaposlenika pri zaštiti osobnih podataka, moguće prijetnje i problemi pri zaštiti podataka. U svrhu usporedbe, kao primjeri su korištene dvije hrvatske banke a to su Privredna banka Zagreb (PBZ) i Hrvatska poštanska banka (HPB).

6. Opis istraživanja i rezultati

Problem zaštite osobnih podataka u e-bankarstvu je stalan u svijetu bankarstva. Kako bi se što više minimalizirala opasnost krađe ili zloupotrebe osobnih podataka postoje razne pravne regulative koje štite klijente banaka. U ovome radu će se istražiti kako se brinu banke o zaštiti osobnih podataka klijenata, usredotočiti će se na banke u Hrvatskoj kao što su Privredna banka Zagreb (PBZ) i Hrvatska poštanska banka (HPB). Usporedit će se što nude navedene banke i što implementiraju i kako postupaju da bi zaštitili osobne podatke svoj klijenata.

Rezultati istraživanja će obuhvatiti analizu dviju banaka. Promatrat će se koja banka omogućava više zaštite podataka te koliko su transparente i javno dostupne informacije o aktivnostima banaka i njihovom ulaganju napora pri zaštiti osobnih podataka svojih klijenata. Usporedit će se kako banke prikupljaju osobne podatke, obrađuju osobne podatke, prijenose podatke, rokovi čuvanja podataka, privole za korištenja osobnih podataka i koja prava imaju klijenti. Kako istraživanje o zaštiti podatka u e-bankarstvu, istraživati će se kako banke štite podatke osobnih podataka u e-poslovanju preko mobilnog bankarstva i Internet bankarstva. U novije vrijeme ima sve više tehnologija i inovacija koje štite osobne podatke u e-bankarstvu, što i dalje ne isključuje i ne garantira cjelokupnu zaštitu osobnih podataka klijenata u e-bankarstvu. Obje banke se pozivaju i pridržavaju Opće uredbe o zaštiti osobnih podataka (GDPR), uredba 28. siječnja 2018. godine u svim članicama Europske unije, GDPR uredba nije jedina zaštiti klijenata u e-bankarstvu, već postoje ostali zakoni koje određuje država. Obje banke nude osnovne zaštite osobnih podataka i pružaju podjednake informacije klijentima na temu zaštite podataka. Kako je sigurnost jedan od temelja u e-bankarstvu tako je i povjerenje klijenta u banke, a njihovo povjerenje se zasniva na percipiranoj sigurnosti koja pruža njihova banka. Obje banke rade na informiranosti svojih klijenata i zaposlenika o zaštiti osobnih podataka kako bi digli svijest i sa time minimalizirali opasnost u e-bankarstvu.

6.1. Zaštita osobnih podataka u HPB banci

Kako bi korisnici mogli biti informirani i u bilo koje vrijeme pogledati svoja prava ili se informirati o zaštiti podataka u e-bankarstvu, Hrvatska poštanska banka je omogućila svojim klijentima ili zainteresiranim osobama javno dostupne i transparente informacije o tome kako i na koje načine štite osobne podatke svojih klijenata. HPB štiti osobne podatke sukladno sa Općom uredbom o zaštiti podataka, te imaju politiku o zaštiti, prikupljanju i obradi osobnih podataka. Banci je u cilju uspostaviti što bolju politiku i proces zaštite i upravljanja osobnim podacima klijenata, zaposlenika, poslovnih partnera i drugih osoba čiji se osobni podaci obrađuju. Hrvatska poštanska banka želi da se klijenti osjećaju sigurno te da su njihova iskustva na najvišoj razini. Na sažet, transparentan i razumljiv način Hrvatska poštanska banka pruža informacije o obradi osobnih podataka koje su propisane sa Općom uredbom za zaštitu osobnih podatka sa člancima 13 i 14, u slučaju dodatnih pitanja banka omogućuje da se klijenti informiraju preko mail adrese. (HPB, 2023) Pojam obrada podataka podrazumijeva njegovo spremanje, organiziranje, snimanje, uvid i prijenos osobnih podataka u banci, odnosno kod trećih osoba s kojima je Banka u ugovornom poslovnom odnosu, za vrijeme trajanja poslovnog odnosa kao i nakon prestanka trajanja poslovnog odnosa s klijentom, te tijekom razdoblja u kojem je banka dužna čuvati pojedinu dokumentaciju. Hrvatska poštanska banka je uredila web stranicu vizualno kako bi korisnicima bila jednostavnija za koristiti, zbog čestih upita postavljenja su najčešća pitanja koja imaju, te razvrstana prema korisnicima, trećim stranama, kandidatima za zaposlenje, HPB invest i HPB nekretnine. Hrvatska poštanska banka transparentno informira o prikupljanju osobnih podataka, obradi osobnih podataka, pravima klijenata, privolama za korištenje osobnih podataka, dodatnim podacima, ustupanju i prijenosu podataka, rokovima čuvanja podataka i kontakt podacima. Banka može ustupiti podatke klijenata sukladno važećim zakonskim propisima određenim institucijama npr. HNB-u, HANFA-i, Agenciji za zaštitu osobnih podataka, poreznim tijelima (HPB, 2023). (HPB – Zaštita osobnih podataka, 2023) Banka osobne podatke prikuplja i obrađuje s ciljem ugovaranja usluge i uspostavljanja ugovornog odnosa te ispunjenja ugovorene obveze. Količina podataka koju banke moraju prikupiti ovisi o zatraženoj usluzi ili proizvodu. Osim podataka koji su potrebni za ugovaranje usluge, također su potrebni i neki podaci za koje postoji zakonska obveza prikupljanja. Banka u svrhu sprječavanja zloupotreba i iz sigurnosnih razloga prilikom korištenja izravnih kanala banke prikuplja i obrađuje podatke o IP adresi uređaja s kojega se pristupa izravnom kanalu te podatke o uređaju.

Pri obradi potaka, sve podatke koje je banka obradila i doznala dok je pružala uslugu su zaštićeni sa zakonom o tajni podataka. Hrvatska poštanska banka neće pristupiti obrađivanju

podataka klijenata ako nema nikakve potrebe, se smatra ako obrada nema nikakvih temelja prema zakonskoj, ugovornoj ili legitimnoj osnovi, te ako nije nužno pri realizaciji obrade ili korisnik nije dao privolu za obradu podataka. Osobe koje obrađuju osobne podatke klijenata su voditelj obrade, zajednički voditelj i izvršitelj. Voditelj obrade obrađuje podatke u kojima ugovara vlastite proizvode i usluge i također određuje samostalno svrhu obrade u suradnji sa drugim pravnim subjektom, dok zajednički voditelj obrađuje podatke pri svrsi kreiranja i ponude zajedničkih proizvoda, a izvršitelj radi po nalogu drugog subjekta obrađuje osobne podatke i ne određuje svrhu obrade. Sa automatskom obradom se obrađuje izračun prešutnog dopuštenog prekoračenja to se ponavlja periodički jer je to dio poslovanja banke. Korisnik u skladu sa Općom uredbom o zaštiti osobnih podataka ima pravo prigovora na automatsku i ručnu obradu. (HPB, 2023) Osobni podatci klijenata su zaštićeni sa Općom uredbom o zaštiti osobnih podataka te klijenti imaju pravo zatražiti ispravak netočnih osobnih podataka, zatražiti brisanje podataka koji nisu nužni, opozivati privolu temeljem koje se obrađuju osobni podaci, uložiti prigovor na postupak obrade ili na prenosivost podataka, zatražiti prijenos podataka drugom voditelju obrade. Klijent banke može uputiti pisanim putem poštom ili e-mailom ako želi realizirati neka od navedenih prava. (HPB, 2023) Hrvatska privredna banka osobne podatke čuva sukladno sa zakonskim propisima te može i duže čuvati ako ima pravovaljani interes kao na primjer rješavanje potencijalnih pritužbi ili sporova. Rokovi čuvanja podataka su utvrđeni sa posebnim internim aktom.

6.2. Zaštita osobnih podataka u PBZ banci

Da bi korisnici mogli biti informirani i u bilo koje vrijeme pogledati svoja prava ili se informirati o zaštiti podataka u e-bankarstvu. Privredna banka Zagreb je omogućila svojim klijentima ili zainteresiranim osobama javno dostupne i transparente informacije o tome kako i na koje načine štite osobne podatke svojih klijenata. PBZ štiti osobne podatke sukladno sa Općom uredbom o zaštiti podataka, te imaju politiku o zaštiti, prikupljanju i obradi osobnih podataka. (PBZ, 2023) Banci je u cilju uspostaviti što bolju politiku i proces zaštite i upravljanja osobnim podacima klijenata, zaposlenika, poslovnih partnera i drugih osoba čiji se osobni podaci obrađuju. Privredna banka Zagreb želi da se klijenti osjećaju sigurno te da su njihova iskustva na najvišoj razini. Na sažet, transparentan i razumljiv način Privredna banka Zagreb pruža informacije o obradi osobnih podataka koje su propisane sa Općom uredbom za zaštitu osobnih podatka sa člancima 13 i 14, u slučaju dodatnih pitanja banka omogućuje da se klijenti informiraju preko mail adrese. Pojam obrada podataka podrazumijeva njegovo spremanje, organiziranje, snimanje, uvid i prijenos osobnih podataka u banci, odnosno kod trećih osoba s kojima je Banka u ugovornom poslovnom odnosu, za vrijeme trajanja poslovnog odnosa kao i nakon prestanka trajanja poslovnog odnosa s klijentom, te tijekom razdoblja u kojem je banka dužna čuvati pojedinu dokumentaciju. Privredna banka Zagreb je uredila web stranicu simplistički što više moguće sa osnovnim informacija poput informacije o podacima o voditelju obrade, kontakt podaci službenika za zaštitu podataka, kategorije osobnih podataka, svrhe i pravne osnove obrade, koje kategorije osobnih podataka prikupljamo, u koje svrhe obrađujemo vaše podatke i na temelju koje pravne osnove, kategorije primatelja vaših osobnih podataka, prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, razdoblje čuvanja osobnih podataka, prava ispitanika, obrada posebnih kategorija osobnih podataka i zajednički voditelji obrade. (PBZ, 2023) Banka osobne podatke prikuplja i obrađuje s ciljem ugovaranja usluge i uspostavljanja ugovornog odnosa te ispunjenja ugovorene obveze. Količina podataka koju banke moraju prikupiti ovisi o zatraženoj usluzi ili proizvodu. Osim podataka koji su potrebni za ugovaranje usluge, također su potrebni i neki podaci za koje postoji zakonska obveza prikupljanja. Banka u svrhu sprječavanja zloupotreba i iz sigurnosnih razloga prilikom korištenja izravnih kanala banke prikuplja i obrađuje podatke o IP adresi uređaja s kojega se pristupa izravnom kanalu te podatke o uređaju. Pri obradi potaka, sve podatke koje je banka obradila i doznala dok je pružala uslugu su zaštićeni sa zakonom o tajni podataka. Privredna banka Zagreb neće pristupiti obrađivanju podataka klijenata ako nema nikakve potrebe, smatra ako obrada nema nikakvih temelja prema zakonskoj, ugovornoj ili legitimnoj osnovi, te ako

nije nužno pri realizaciji obrade ili korisnik nije dao privolu za obradu podataka. Obrada posebnih kategorija osobnih podataka potreban je izričit pristanak korisnika sa privolom koja bi dopustila obradu posebnih kategorija osobnih podataka. Osobe koje obrađuju osobne podatke klijenata su voditelj obrade, zajednički voditelj i izvršitelj. Voditelj obrade obrađuje podatke u kojima ugovara vlastite proizvode i usluge i također određuje samostalno svrhu obrade u suradnji sa drugim pravnim subjektom, dok zajednički voditelj obrađuje podatke pri svrsi kreiranja i ponude zajedničkih proizvoda, a izvršitelj radi po nalogu drugog subjekta obrađuje osobne podatke i ne određuje svrhu obrade. Sa automatskom obradom se obrađuje izračun prešutnog dopuštenog prekoračenja to se ponavlja periodički jer je to dio poslovanja banke. Korisnik u skladu sa Općom uredbom o zaštiti osobnih podataka ima pravo prigovora na automatsku i ručnu obradu. (Obrada osobnih podataka – PBZ, 2023) Osobni podatci klijenata su zaštićeni sa Općom uredbom o zaštiti osobnih podataka te klijenti imaju pravo na pristup podacima, pravo na ispravak, pravo na brisanje, pravo na ograničenje obrade, pravo na prijenos podataka, pravo na prigovor, automatizirano pojedinačno donošenje odluka uključujući profiliranje, pravo na pritužbu i pravo podnošenja prigovora nadležnom tijelu za zaštitu podataka. Klijent banke može uputiti pisanim putem poštom ili e-mailom ako želi realizirati neka od navedenih prava. Ukoliko klijent napravi upit e-mailom najkasnije unutar mjesec dana će dobiti odgovor putem e-maila. (PBZ, 2023) Privredna banka Zagreb osobne podatke čuva sukladno sa zakonskim propisima te može i duže čuvati ako ima pravovaljani interes kao na primjer rješavanje potencijalnih pritužbi ili sporova. Rokovi čuvanja podataka su utvrđeni sa posebnim internim aktom. Minimalno se 10 godina od prestanka poslovnih odnosa čuvaju podaci.

6.3. Usporedba zaštite podataka u PBZ i HPB banci

Kako bi korisnici Privredne banke Zagreb i Hrvatske poštanske banke mogli biti informirani i u bilo koje vrijeme pogledati svoja prava ili se informirati o zaštiti podataka u e-bankarstvu. Obje banke su omogućile svojim klijentima ili zainteresiranim osobama javno dostupne transparente informacije o tome kako i na koje načine štite osobne podatke svojih klijenata. Hrvatska poštanska banka i Privredna banka Zagreb štiti osobne podatke sukladno sa Općom uredbom o zaštiti podataka, te imaju politiku o zaštiti, prikupljanju i obradi osobnih podataka. Bankama je u cilju uspostaviti što bolju politiku i proces zaštite i upravljanja osobnim podacima klijenata, zaposlenika, poslovnih partnera i drugih osoba čiji se osobni podaci obrađuju. Objema banka je u interesu da se njihovi klijenti osjećaju sigurno te da su njihova iskustva na najvišoj razini. Na sažet, transparentan i razumljiv način Privredna banka Zagreb i Hrvatska poštanska banka pružaju svojim klijentima informacije o obradi osobnih podataka koje su propisane sa Općom uredbom za zaštitu osobnih podatka sa člancima 13 i 14, u slučaju dodatnih pitanja banke su omogućile da se klijenti informiraju preko mail adrese ili fizičkim pismom . (HPB ,2023) Pojam obrada podataka podrazumijeva njegovo snimanje, spremanje, organiziranje, uvid i prijenos osobnih podataka u banci, odnosno kod trećih osoba s kojima je Banka u ugovornom poslovnom odnosu, za vrijeme trajanja poslovnog odnosa kao i nakon prestanka trajanja poslovnog odnosa s klijentom, te tijekom razdoblja u kojem je banka dužna čuvati pojedinu dokumentaciju. Privredna banka Zagreb i Hrvatska poštanska banka su obje uredila web stranicu na svoj način, Privredna banka Zagreb je uredila simplistički što više moguće sa osnovnim informacija o podaci i voditelju obrade, kontakt podaci službenika za zaštitu podataka, kategorije osobnih podataka, svrhe i pravne osnove obrade, koje kategorije osobnih podataka prikupljamo, u koje svrhe obrađujemo vaše podatke i na temelju koje pravne osnove, kategorije primatelja vaših osobnih podataka, prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, razdoblje čuvanja osobnih podataka, prava ispitanika, obrada posebnih kategorija osobnih podataka i zajednički voditelji obrade. (Obrada osobnih podataka – PBZ, 2023) Dok je Hrvatska poštanska banka je uredila web stranicu više vizualno kako bi korisnicima bila jednostavnija za koristiti, zbog čestih upita postavljenja su najčešća pitanja koja imaju, te razvrstana prema korisnicima, trećim stranama, kandidatima za zaposlenje, HPB invest i HPB nekretnine. Na kraju krajeva obje banke su gotovo identične.

7. Rasprava

U radu je istražena zaštita osobnih podataka u e-bankarstvu. Postoji niz tehnologija i zakona koje štite osobne podatke. Uspoređene su dvije banke a to su PBZ i HPB, obje banke imaju vrlo slične informativne stranice i njihova zaštita podataka je identična, jer poštuju propisane propise. Za kršenje uredba o zaštiti osobnih podataka postoje kazne. Ujedno sa vremenom kako prolazi e-bankarstvo raste i razvija, nastaje također sve veća i veća zabrinutost oko sigurnosti i zaštite osobnih podataka klijenata. Stoga se više u centar pažnje stavlja sigurnost i zaštita podataka kako bi se osigurao kontinuitet implementiranja i razvijanja novih korisnih tehnologija koje bi štitile osobne podatke klijenata u e-bankarstvu. Pod osobne podatke koji mogu biti kompromitirani spadaju ime i prezime, adresa stanovanja, datum i mjesto rođenja, OIB, broj telefona, e-mail adresa, IP adresa, primanja i osobna iskaznica ili putovnica. Načela obrade osobnih podataka su: načelo zakonitosti, poštenosti i transparentnosti, načelo ograničenja svrhe, načelo smanjenja količine podataka, načelo točnosti podataka, načelo ograničenja pohrane i načelo sigurnosti pohrane. Jedna od najčešće zlouporabe osobnih podataka su neovlašteni pristup podatcima, krađa identiteta, neovlaštena ili zloupotreba distribucije podataka, pokretanje virusa, krađa hardver, softvera ili digitalnog sadržaja. Kao što postoji puno tehnologija za zaštitu osobnih podataka također postoji i puno prijetnji za osobne podatke. Jedne od vodećih prijetnji su hakerski napadi, virusi i crvotočine, nesigurna mreža, slabo ažuriranje softvera, slaba sigurnosna praksa korisnika i zaposlenika, zlouporaba podataka od strane bankarskih institucija. U e-bankarstvu postoje različite tehnologije koje se koriste za zaštitu osobnih podataka. Jedni od najzastupljenijih tehnologija za zaštitu podataka su uređaji za autorizaciju korisnika. Najčešći uređaji za autorizaciju korisnika su TAN tablica, token, display kartica, čitač kartica, USB stick s certifikatom i biometrijski uređaji. Za zaštitu podataka važna je također i dobra pravna podloga kao što je Opća uredba o zaštiti osobnih podataka koja se koristi u svim zemljama članicama Europske unije. Zaposlenici su jedan od ključnih faktora pri zaštiti podatka klijenta i trebaju biti upoznati sa politikama banke. Također su važne i banke jer imaju puno zakonskih i etičkih obveza kako bi zaštitili osobne podatke svojih klijenta te kako bi očuvale njihovu cjelovitost i privatnost njihovih informacija. Jedna od glavnih obveza banke je informirati klijente o svrsi prikupljanja podataka i tražiti njihovo odobrene za prikupljanje podataka, osim ako je prikupljanje nužno zbog zakonskih obveza ili izvršenja nekog ugovora. Svaka banka se pridržava Opće uredbe o zaštiti osobnih podataka stoga su gotovo identične, jedino razlike nastaju u unutarnjim politikama banke koje banke same smišljaju

8. Zaključak

Zaštita podataka predstavlja temelje bankarstva, banka ne može dobro poslovati ako ne može štiti imovinu svojih klijenata. Sa zaštitom osobnih podataka osigurava se stabilno poslovanje banke te povjerenje klijenata u banku. Kako vrijeme teče tako se i tehnologija razvija, sa vremenom nastaju i nove inovacije koje se mogu implementirati pri zaštiti osobnih podataka u e-bankarstvu. Zaštita osobnih podataka nije briga samo banke već i zaposlenika banke i klijenata banke. Važno je dignuti svijest klijenata o rizicima koji mogu oštetiti, uništiti i zloupotrijebiti podatke. Pod osobne podatke se spadaju ime i prezime, adresa stanovanja, datum i mjesto rođenja, OIB, broj telefona, e-mail adresa, IP adresa, primanja i osobna iskaznica ili putovnica. Sigurnost i zaštita osobnih podataka u e-bankarstvu ne može biti sto postotna, nego se jedino može težiti minimalizaciji. Sukladno sa razvojem zaštite, sigurnosnih mjera i zakonodavnih propisa također napreduju prijetnje koje ugrožavaju integritet osobnih podataka u e-bankarstvu. Prvi korak pri zaštiti osobnih podataka je preventiva, kako bi se spriječilo trebalo bi se educirati o rizicima i prijetnjama koje se mogu pojaviti u e-bankarstvu, banke informiraju svoje korisnike na web sjedištima. Na web sjedištima korisnici usluga banaka mogu se informirati o svojim pravima i mogućnostima poput informacije o podacima o voditelju obrade, kontakt podaci službenika za zaštitu podataka, kategorije osobnih podataka, svrhe i pravne osnove obrade, koje kategorije osobnih podataka prikupljamo, u koje svrhe obrađujemo vaše podatke i na temelju koje pravne osnove, kategorije primatelja vaših osobnih podataka, prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, razdoblje čuvanja osobnih podataka, prava ispitanika, obrada posebnih kategorija osobnih podataka i zajednički voditelji obrade. Uz sustavnu zaštitu također su važne i pravne regulative koje štite podatke klijenata, unutar Europske unije na snazi je Opća regulativa o zaštiti osobnih podataka koja isključivo štiti osobne podatke. U e-bankarstvu postoje različite tehnologije koje se koriste za zaštitu osobnih podataka, a jedne od najzastupljenijih tehnologija za zaštitu podataka su uređaji za autorizaciju korisnika. Najčešći uređaji za autorizaciju korisnika su TAN tablica, token, display kartica, čitač kartica, USB stick s certifikatom i biometrijski uređaji. Osim uređaja također se koriste mjere kao što kriptografija, enkripcija, autentifikacija, identifikacija te snažne lozinke, višefaktorske autentifikacije i precizna autorizacija. Važna je suradnja banaka sa nadzornim tijelima i stručnjacima za sigurnost. U konačnici sigurnost osobnih podataka klijenata štiti korisnike i gradi povjerenje u e-bankarstvo. Stalno razvijanje i implementiranje zaštite rezultirat će povjerenju i integritetu podataka klijenata.

Literatura

1. Birovčec, F. (2021) Utjecaj digitalnih tehnologija na poslovanje banaka. Dostupno na: https://repozitorij.efzg.unizg.hr/islandora/object/efzg%3A6845/datastream/PDF/view [Datum pristupanja: 24.06.2024.]

2. Boban, M. i Perišić, M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Dostupno na: https://hrcak.srce.hr/file/209925 [Datum pristupanja: 24.06.2024.]

3. Ćurić, F. Projektiranje i zaštita informacijsko – komunikacijskih sustava u bankarskim institucijama, Zagreb: Sveučilište u Zagrebu, Fakultet Prometnih znanosti. Dostupno na: https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A803/datastream/PDF/view [Datum pristupanja: 23.06.2024.]

4. Desović, A. Inovacije u biometriji, Rijeka: Veleučilište u Rijeci. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:125:380395 [Datum pristupanja: 23.06.2024.]

5. Hrehorović. I. Kanali e-bankarstva i hardvreske komponete u bakarstvu, Osijek: Sveučilište u Osijeku, Ekonomski fakultet. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:145:545007 [Datum pristupanja: 23.06.2024.]

6. Kovačević, D. Primjena informatičke tehnologije u bankarstvu, Osijek: Sveučilište u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:200:528933 [Datum pristupanja: 23.06.2024.]

7. Mladin, P. Odgovornost za zaštitu osobnih podataka, Zagreb: Sveučilište u Zagrebu, Pravni fakultet. Dostupno na: https://www.pravo.unizg.hr/_download/repository/Odgovornost_za_zastitu_osobnih_podataka_u_bankarstvu%5B1%5D.pdf [Datum pristupa: 06. 06. 2023.]

8. Plavi ured, Dominik Musulin (2023), GDPR – načela obrade osobnih podataka. Dostupno na: https://plaviured.hr/vodici/gdpr-nacela-obrade-osobnih-podataka/ . [Datum pristupa: 10.09.2023.]

9. Rončević, A. (2006) Nove usluge bankarskog sektora: Razvitak samposlužnoga bankarstva u Hrvatskoj. Dostupno na: https://hrcak.srce.hr/file/12965 [Datum pristupa: 23. 07. 2024.]

10. Široki, K. Najpoznatiji hakerski napad i online sigurnost, Rijeka: Sveučilište u Rijeci, Fakultet za menadžment u turizmu i ugostiteljstvu Opatija. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:191:037245 [Datum pristupa: 23. 07. 2024.]

11. Zekić Sušac, M. (2013) Sigurnost informacijskog sustava e-bankarstva. Dostupno na: http://www.efos.unios.hr/ict-u-bankarstvu/wp content/uploads/sites/241/2013/04/pogl8_Sigurnost.pdf [Datum pristupa: 24. 06. 2023.]

Internetski izvori:

1. Azop.hr, Agencija za zaštitu osobnih podataka. Dostupno na: https://azop.hr/ [Datum pristupanja: 10.09.2023.]

2. Europa.eu, Zaštita podataka u EU-u – European Commison. Dostupno na: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_hr [Datum pristupanja: 07.09.2023.]

3. EDPB – European Dana Protection Bord. Dostupno na: https://edpb.europa.eu/edpb_en [Datum pristupanja: 01.06.2023.]

4. Erste banka – Što je display kartica? Dostupno na: https://www.erstebank.hr/hr/pomoc/help-center/poslovni-klijenti/on-line-bankarstvo/netbanking/sto-je-display-kartica [Datum pristupanja: 23.06.2024.]

5. GDPR Informer. Dostupno na: https://gdprinformer.com/hr/vodic-kroz-gdpr [Datum pristupanja: 09.09.2023.]

6. Gdpr-info.eu General Dana Protection Regulation (GDPR) – Official Legal Text. Dostupno na: https://gdprinfo.eu/hr [Datum pristupanja: 21.08.2023.]

7. Gov.hr - e-Građanin - Zaštita osobnih podataka. Dostupno na https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868 [Datum pristupanja: 09.07.2023.]

8. HNB – Zaštita osobnih podataka u Hrvatskoj narodnoj banci. Dostupno na: https://www.hnb.hr/zastita-osobnih-podataka [Datum pristupanja: 09.09.2023.]

9. HPB – Zaštita osobnih podataka. Dostupno na: https://www.hpb.hr/hr/zastita-osobnih-podataka/2970 [Datum pristupanja: 10.09.2023.]

10. HUB - Zaštita osobnih podataka - Hrvatska udruga banaka. Dostupno na: https://www.hub.hr/hr/zastita-osobnih-podataka-u-bankama [Datum pristupanja: 09.09.2023.]

11. IUS-INFO – Opća uredba o zaštiti osobnih podataka (GDPR). Dostupno na: https://www.iusinfo.hr/document?sopi=DDHR20181007N112 [Datum pristupanja: 08.09.2023.]

12. Microsoft Learn - Opća uredba o zaštiti podataka (GDPR). Dostupno na: https://learn.microsoft.com/hr-hr/legal/gdpr [Datum pristupanja: 25.06.2023.]

13. Mpgi.gov.hr, Zaštita podataka. Dostupno na: https://mpgi.gov.hr/zastita-podataka/8631 [Datum pristupanja: 05.08.2023.]

14.PBZ - Obrada osobnih podataka, Dostupno na: https://www.pbz.hr/gradjani/obrada-osobnih-podataka.html [Datum pristupanja: 10.09.2023.]

15. Rdd.gov.hr, Opća uredba o zaštiti podataka. Dostupno na: https://rdd.gov.hr/opca-uredba-o-zastiti-podataka-203/203 [Datum pristupanja: 05.08.2023.]

16. Szp.hr Zaštita osobnih podataka – Središnji portal za potrošače. Dostupno na: https://www.szp.hr/sve-potrosacke-teme-na-jednom-mjestu/zastita-osobnih-podataka/75 [Datum pristupa: 06. 06. 2023.]

Popis slika