Primljeno: 26.03.2021.
Odobreno: 16.07.2021.

DOI: 10.5937/bankarstvo2102152B

SISTEMI ZAŠTITE INFORMACIJA U ELEKTRONSKOM BANKARSTVU

Darko Bakić, Samostalni savetnik, Ministarstvo ekonomskog razvoja Crne Gore

Rezime

Imajući u vidu da je implementirano u mrežnom okruženju, elektronsko bankarstvo izloženo je različitim sigurnosnim rizicima. Zbog toga je za bezbedno korišćenje bankarskih usluga u elektronskom obliku potrebno identifikovati potencijalne pretnje kroz analizu mrežne infrastrukture i karakteristika aplikacije, kao i odgovoriti na njih primenom odgovarajućih mera zaštite.

Ključne reči: elektronsko bankarstvo, sistemi zaštite, principi bezbednosti, napadi, mere zaštite, aspekti zaštite, zaštitni zid, kriptozastita

JEL klasifikacija: E42, K24, L86, M15.

Uvod

Elektronsko bankarstvo (e-banking), zajedno sa elektronskom trgovinom, upravljanjem odnosima sa klijentima, planiranjem resursa preduzeća, upravljanjem lancima vrijednosti i poslovnom inteligencijom, predstavlja sastavni dio elektronskog poslovanja (e-business).¹ Elektronsko poslovanje se u najširem smislu definiše kao interni ili eksterni poslovni proces koji se realizuje posredstvom računarske mreže.²

Pod elektronskim bankarstvom podrazumijeva se sveukupnost tehnoloških procedura, koje obezbjeđuju vršenje bankovnih transakcija elektronskim putem.³ Drugačije rečeno, elektronsko bankarstvo je vid bankarstva koji se odvija pomoću elektronskih sistema, čiji je zadatak da vrše transfer novčanih sredstava i prave zapise u vezi sa njima, bez papira, koristeći računarsko komunikacione tehnologije.⁴ Tako, klijenti banaka mogu da koriste usluge elektronskog bankarstva putem interneta, mobilnih uređaja, bankomata i POS terminala.

Kako koncept elektronskog bankarstva korisnicima bankarskih usluga, ali i samim bankama, omogućava da ispunjavaju svoje uobičajene aktivnosti elektronskim putem, to je osnovni preduslov za njegovo normalno funkcionisanje ispravan informacioni sistem banke, funkcionalna infrastruktura mreže i zaštita informacija i transakcija.

¹ Elektronska trgovina (e-trgovina) se definiše kao transakcija preko računarske mreže, koja podrazumijeva prenos vlasništva ili prava za korišćenje roba i usluga, kao na primjer: kupovina knjiga preko interneta, rezervacija hotelske sobe preko interneta, naručivanje i preuzimanje besplatnog softvera preko interneta itd. (B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *Elektronsko poslovanje*, Beograd, 2015, s. 131)

Upravljanje odnosima sa klijentima (Customer Relationship Management – CRM) je dio elektronskog poslovanja koji obuhvata niz metoda, tehnika i oprobanih praksi implementiranih u okviru poslovnog sistema, u cilju unapređenja komunikacije i saradnje sa klijentima, promovisanja proizvoda i usluga i maksimiziranja poslovne dobiti. Riječ je o poslovnoj strategiji čiji rezultati istovremeno optimizuju profitabilnost i prihode, doprinose zadovoljstvu klijenata i ostvarenju lojalnosti, a koja podrazumijeva sve aspekte interakcije kompanije sa klijentima, bez obzira na to da li se radi o prodaji ili uslugama. Želi se ostvariti takva situacija u kojoj će svaki od klijenata imati poseban tretman i ponudu koja mu u datom trenutku najviše odgovara i koja će se odnositi samo na njega. (Isto; V. Simović, *Elektronsko poslovanje-skripta (verzija 2)*, Beograd, 2013, s. 10)

Planiranja resursa preduzeća (Enterprise Resource Planning–ERP) predstavlja softverski paket koji prati sve aspekte poslovanja jedne kompanije. Njega karakteriše efektivno upravljanje procesima u preduzeću, postojanje zajedničke (jedinstvene) baze podataka, kao i mogućnost brzog reagovanja na operativne zahteve. (V. Simović, *n.d.*, s. 11; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *Priručnik za pripremu prijemnog ispita za upis na master studije*, Beograd, 2012, s. 32,33)

Upravljanje lancima vrijednosti (Supply Chain Management–SCM) označava termin koji se koristi da opiše tok materijala, informacija i sredstava kroz lanac nabavke (vrijednosti) od snabdevača preko proizvođača pojedinih komponenti, konačnog spajanja i distribucije (skladišta i maloprodaja) pa do konačnog kupca, pri čemu ovaj proces često sadrži i dodatne usluge koje prate proizvod posle prodaje i povraćaj proizvoda na reciklažu. Lanac vrednosti predstavlja skup poslovnih procesa koji povezuje snabdevače, proizvođače, prodavce na malo, poslovne korisnike, i ostale umešane u stvaranje, prodaju i isporuku robe do krajnjeg kupca. (V. Simović, *n.d.*, s. 11; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 33)

Poslovna inteligencija (Business Intelligence – BI) je proces prikupljanja raspoloživih internih i značajnih eksternih podataka i njihovog pretvaranja u korisne informacije koje pomažu menadžmentu pri donošenju odluka. (M. Milić, *Odlučivanje i poslovna inteligencija*, Banja Luka, 2014, s. 85)

² B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 4.

³ I. A. Reznik, *Elektronnyiye banking*, Orenburg, 2008, s. 7.

⁴ T. Uroš, *Elektronsko bankarstvo*, Beograd, 2014, s. 120.

Svakako da je sa aspekta povjerenja klijenta u pogledu korišćenja sistema elektronskog bankarstva od posebnog značaja da se obezbjedi sigurnost njihovog funkcionisanja, odnosno da se pomoću odgovarajućih sistema zaštite informacija obezbjedi da se sigurnosni rizici kojima je izložena svaka računarska mreža svedu na najmanju moguću mjeru.

Osnovni principi sigurnosti u elektronskom bankarstvu

U osnovne principe sigurnosti na kojima treba da se bazira primjena servisa elektronskog bankarstva ubrajaju se: povjerljivost, integritet, dostupnost, autentičnost, neporecivost, enkripcija i praćenje.⁵

Princip povjerljivosti podrazumijeva nedostupnost informacija neautorizovanim osobama, kao i njihovu zaštićenost od presretanja tokom prenosa.

Poštovanje principa integriteta treba da obezbijedi neizmjenljivost informacija tokom prenosa na mreži.⁶ Drugačije rečeno, princip integriteta podrazumijeva konzistentnost podataka, sprečavajući neovlašćeno generisanje, promjenu i uništenje podataka.⁷

Dostupnost je princip koji autorizovanim korisnicima obezbjeđuje pravovremeni pristup informacijama, tj. riječ je o pristupu informacijama po zahtjevu korisnika.⁸

Princip autentičnosti odnosi se na postojanje mehanizma za izvršavanje autentifikacije korisnika, prije nego što se dozvoli pristup traženim informacijama.

Neporecivost je princip koji podrazumijeva nemogućnost poricanja poruke koju je poslao korisnik, kao i nemogućnost da primalac poruke porekne njeno dobijanje.

Prema principu enkripcije informacije treba da budu enkriptovane i dekriptovane od strane autorizovanog korisnika.

Princip praćenja odnosi se na neophodnost snimanja podataka, kako bi se mogla pratiti dešavanja u sistemu.⁹

Napadi na elektronsko bankarstvo

Elektronsko bankarstvo može biti izloženo različitim vrstama napada kao što su: socijalni inženjering (social engineering), skeniranje portova (port scanners), paket analizator (njuškač paketa-packet sniffers), probijanje lozinke (password cracking), trojanci (trojans), napad uskraćivanjem servisa (denial of service attack), greške na serveru (server bugs), eksploatacije superkorisnika (super user exploits), fišing i dr.¹⁰

⁵ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 225.

⁶ Isto.

⁷ M. Unković, M. Milosavljević, N. Stanišić, *Savremeno berzansko i elektronsko poslovanje*, Beograd, 2010, s. 231

⁸ D. M. Korać, *Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (doktorska disertacija)*, Beograd, 2018, s. 10.

⁹ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 225.

¹⁰ Z.B.Omariba, N.B. Masese, G. Wanyembi, *Security and privacy of electronic banking*, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, s.440; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 226.

Socijalni inženjering (social engineering) podrazumijeva takvu situaciju u kojoj napadač, predstavljajući se kao sistemski administrator ili predstavnik korisničke službe, navodi korisnika, zloupotrebljavajući njegove socijalne karakteristike (povjerenje, želju da se pomogne drugome, odgovornost itd), na otkrivanje osjetljivih informacija, kako bi pristupio njegovom nalogu.¹¹

Skeniranje portova (port scanners) se koristi od strane napadača da bi se utvrdile ulazne tačke u sistem, radi korišćenja raznih tehnika za krađu informacija. Ova vrsta softvera šalje signale mašini ili ruteru i bilježi poruku kojom mašina odgovara u cilju utvrđivanja tačke ulaska. Glavna svrha skeniranja portova je prikupljanje informacija povezanih sa hardverom i softverom koji pokreće sistem, kako bi se mogao razviti plan napada.¹²

Paket analizator ili njuškač paketa (packet sniffers) koristi se za prikupljanje podataka koji se prenose mrežom, tj. ovaj softver nadgleda vezu između korisnikovog računara i veb servera kako bi prikupio podatke koji se odnose na korisnika, uključujući lozinke i podatke o kreditnoj kartici. Pošto ne manipulišu protokom podataka, već je njihova funkcija hvatanje mrežnog prometa, njuškače paketa je vrlo teško otkriti.

Probijanje lozinke (password cracking) obuhvata različite mogućnosti napada u svrhu dešifrovanja lozinki, među kojima je najpopularniji napad grubom silom. Da bi se na ovaj način pristupilo podacima korisnika skeniraju se hiljade uobičajenih izraza, aktivnosti i imena, koji se potom kombinuju sve dok se ne dobije odgovarajuća kombinacija, odnosno korisnička lozinka. Probijanje lozinke grubom silom uglavnom se primjenjuje kod sistema koji ne zahtjevaju jake lozinke, pa korisnici koriste uobičajena imena i aktivnosti, što olakšava otkrivanje pasvorda, odnosno pristup sistemu. Druge metode probijanja lozinki uključuju upotrebu heš tabela za dešifrovanje datoteka lozinki, koje mogu otkriti celu listu korisničkih imena i lozinki sistema.¹³

Trojanci (trojans) su kompleksne klijent-server aplikacije, koje omogućavaju pristup udaljenim korisničkim računarima u mreži, (do korisnika stižu putem imejla, diskusionih grupa, popularnih čet programa itd.), na način što ih sami korisnici instaliraju na svoj računar, smatrajući da će im biti od koristi.¹⁴ Trojanac, koji se nalazi na računaru korisnika (žrtve) je u stvari server, a klijent je program koji upravlja trojancem i koji se nalazi na računaru osobe koja namjerava da dođe do bitnih informacija na račun žrtve.¹⁵

Napad uskraćivanjem servisa (denial of service attack) predstavlja tip napada koji ima za cilj da spriječi legitimne korisnike da pristupe mrežnim uslugama, što se postiže preopterećenjem mrežnih servisa ili prekomernom konekcijom, usljed čega dolazi do pada konekcije ili servisa. Naime, infrastruktura međusobno spojenih sistema i mreža sastoji se od ograničenih resursa, što je najbitnija činjenica kod napada uskraćivanjem servisa, koji podrazumijevaju slanje velikog broja zahteva ciljanom serveru, kako bi preplavili njegove ograničene resurse i učinile ga neupotrebljivim.¹⁶

¹¹ Isto.

¹² Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.d.*, s.440.

¹³ Isto.

¹⁴ S. Jo, *Zaštita računarskih mreža–analiza antivirusne zaštite (master rad)*, Beograd, 2015, s. 28; M. Milosavljević, V. Mišković, *Elektronska trgovina*, Beograd, 2016, s. 229.

¹⁵ S. Jo, *n.d.*, Beograd, 2015, s. 28–29.

¹⁶ D.V.Vuletić, *Napadi na računarske sisteme*, Vojnotehnički glasnik, br. 1, Beograd, 2012, s. 236.

Greške na serveru (server bugs) se često otkrivaju i blagovremeno ispravljaju. Međutim, sistemski administratori često sporo primenjuju najnovija ažuriranja, što napadaču daje dovoljno vremena da kreira prijetnju.¹⁷

Eksploatacije superkorisnika (super user exploits) omogućavaju napadaču da preuzme kontrolu nad sistemom kao da je administrator. U tom cilju često se koriste skripte¹⁸ za manipulisanje bazom podataka ili napad prekoračenja bafera¹⁹, koji nanosi štetu sistemu slično kao i napad uskraćivanjem servisa.²⁰

Fišing (phishing) predstavlja vrstu napada koja se odnosi na pokušaj krađe ličnih podataka, tako što se žrtva navodi na lažnu veb-stranicu.²¹ U tu svrhu napadači (fišeri) obično koriste falsifikovane imejlove, koje šalju potencijalnim žrtvama u ime određenih organizacija sa kojima one imaju kontakt (npr. banka, osiguravajuća kuća i slično). Tako se, na primjer, mejl šalje korisniku banke u kome se navodi da će mu račun biti ukinut ukoliko ne ažurira lične podatke. U mejlu se daje i link ka lažnom sajtu, koji predstavlja vjernu kopiju originalnog sajta određene ustanove, gdje potencijalna žrtva unosi broj svog računa i lozinku, što kasnije biva zloupotrijebljeno, pre svega u cilju sticanja finansijske koristi napadača.²²

Mjere zaštite računarskih mreža i informacija

Pod zaštitom mreža i informacija podrazumijeva se skup pravila, procedura, algoritama, hardversko-softverskih komponenata, kao i skup organizaciono-tehničkih mjera kojima se štite funkcije mreže pri izvršavanju mrežnih transakcija.

Zaštita informacija obuhvata zaštitu od: neovlašćenog uvida i korišćenja informacija, nekontrolisanog oticanja informacija, slučajnog ili namjernog oštećenja, izmjene ili uništenja.

Zaštita računarskih mreža i informacija realizuje se kroz primjenu različitih mjera kao što su: mjere kadrovske politike; organizaciono-administrativne mjere; tehničke mjere fizičke, elektronske i protivpožarne zaštite; hardversko-softverske mjere; aplikativno programske mjere i mjere kriptozastite.²³

Mjere kadrovske politike su potrebne zbog toga što korisnici usluga mreže predstavljaju nosioce informacija, ali i najveću potencijalnu opasnost po te informacije.

¹⁷ Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.r.*, s. 442.

¹⁸ U računarskom programiranju, skripta je program ili redosled uputstava koji tumači ili izvršava drugi program. (<https://whatistechtarget.com/definition/script>)

¹⁹ Pod prekoračenjem bafera (bafer-blok memorije predviđen za privremeno skladištenje podataka) podrazumijeva se upisivanje sadržaja van granica rezervisane memorije bafera. U stvari to je situacija u kojoj se ukazuje na adresu nekog raspoloživog bafera, ali se koriste lokacije koje ne predstavljaju dio njegove memorije. Prekoračenje bafera može da dovede do neočekivanog toka izvršavanja programa, kao i da omogući razne vrste zloupotreba programa. Ovaj problem je naročito prisutan u programima napisanim na programskom jeziku C. (M. Vujošević-Janičić, *Automatsko otkrivanje prekoračenja bafera u programskom jeziku C (magistarski rad)*, Beograd, 2008, s. 9, 87)

²⁰ Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.r.*, s. 442.

²¹ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 226.

²² D.V.Vuletić, *n.r.*, s. 238

²³ M. Jevtović, *Zaštita računarskih mreža*, Vojnotehnički glasnik br. 5, Beograd, 2005, s. 435.

Organizaciono-administrativnim mjerama se normativno regulišu prava, obaveze i odgovornost korisnika informacionog sistema, uključujući i sankcije prema korisnicima.

U tehničke mjere fizičke, elektronske i protivpožarne zaštite ubrajaju se: fizičko obezbjeđenje, elektronska protivprovalna zaštita i zaštita od nestanka i neadekvatnog napajanja električnom energijom. Ove mjere se primjenjuju radi zaštite: objekata (prostorija u kojima se nalazi računarska i telekomunikaciona oprema), računarske i telekomunikacione opreme i magnetnih i elektronskih nosilaca podataka.²⁴

Hardversko-softverske mjere se koriste radi obezbjeđenja pristupnih tačaka mreži i pojedinim resursima mreže. Ove mjere podrazumijevaju identifikaciju korisnika i utvrđivanje prava i ovlašćenja koja su mu data u pogledu resurse mreže kojima pristupa.²⁵

Aplikativno-programske mere predstavljaju procedure koje se u cilju zaštite ugrađuju u aplikativni softver.

Mere kriptozastite primjenjuju se radi zaštite podataka u memorijskim resursima u računarima i zaštite na prenosnim putevima.²⁶

Različiti aspekti zaštite računarskih mreža i informacija

Različiti aspekti zaštite se veoma često definišu u odnosu na mjesto pozicioniranja mehanizama zaštite u računarskom ili informacionom sistemu ili računarskoj mreži. U tom smislu može se govoriti o zaštiti na nivou aplikacije, zaštiti na nivou operativnog sistema, zaštiti na nivou mrežne infrastrukture, te proceduralnoj i operacionoj zaštiti.²⁷

Zaštita na nivou aplikacije može da obuhvata sljedeće elemente: softversku zaštitu aplikacije, izolovanje kritičnih aplikacija na namenskim hostovima, kao i primenu specifičnih protokola (na primjer, kriptografski zaštićenog SSH protokola umjesto nezaštićenog Telnet protokola).

Zaštita na nivou operativnog sistema predstavlja veoma složeno i obimno područje koje se tiče svih slojeva operativnog sistema. Ovaj nivo zaštite obuhvata i vezu na relaciji operativni sistem – aplikacije, kao i odnos prema mrežnoj arhitekturi, tj. vezama prema drugim sistemima. Prema nekim preporukama, minimalna zaštita obuhvata: blokiranje nepotrebnih servisa (finger, ftp, telnet), obezbjeđivanje sveobuhvatne i obavezne kontrole pristupa na nivou korisnika, obezbjeđivanje integriteta softvera koji čini operativni sistem (većina sigurnosnih napada usmjerena je na operativne sisteme bez primijenjenih zakrpa, pa je zato potrebno redovno ažurirati sve elemente sistema najnovijim zakrpama).

²⁴ Isto, s. 435.

²⁵ Identifikacija korisnika može biti fizička (upotrebljavaju se hardverski uređaji) i logička (koriste se softverske metode). Metode fizičke identifikacije zasnovane su na prepoznavanju identifikacionih sredstava koje korisnik poseduje (inteligentne kartice, magnetne i optičke kartice, bedževi, žetoni i slično) i prepoznavanju fizičkih, biometrijskih karakteristika korisnika (otisak prsta, otisak i oblik šake, oblik uha ili glave, osobine glasa, slika mrežnjače oka i drugo) Metode logičkog prepoznavanja zasnovane su na informacijama koje korisnik u procesu identifikacije i autorizacije ovlašćenja daje sistemu. Te informacije moraju biti jednake informacijama kojima sistem raspolaže. (Isto, s. 435, 436)

²⁶ Isto, s. 435

²⁷ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *Sigurnost računarskih mreža*, Beograd, 2006, s. 25.

Zaštita na nivou mrežne infrastrukture obuhvata sljedeće osnovne elemente: primjena mrežnih barijera (firewalls), blokiranje nepotrebnih portova, šifrovanje putanje, izolovanje putanje pomoću rutera i svičeva ili pomoću posebne infrastrukture.

Kada je riječ o proceduralnoj i operacionoj zaštiti imaju se u vidu sljedeći elementi: zaštita primjenom politika i procedura, detekcija napada, proaktivno delovanje u pogledu zaštite ranjivosti sistema, upravljanje konfiguracijom sistema i obrazovanje korisnika.²⁸

Zaštitni zid (fajervol)

Fajervol (eng. firewall) je ključni element u mrežnoj sigurnosti, koji je, radi zaštite privatnih mreža, našao široku primjenu kako u bankama, tako i u drugim organizacijama i institucijama.²⁹

Pod fajervolom se podrazumijeva bezbjedonosni hardverski ili softverski uređaj, koji je najčešće smješten između lokalne mreže i javne mreže (interneta), a čija je namjena da štiti podatke u mreži od neautorizovanih korisnika (blokiranjem i zabranom pristupa u skladu sa pravilima usvojene bezbjedonosne politike).³⁰ Drugačije rečeno, fajervol je filter na relaciji lokalna mreža – internet, koji ispituje sve pakete koji prolaze između privatne mreže i interneta, a u zavisnosti od toga da li paketi zadovoljavaju pravila definisana listama za kontrolu pristupa, fajervol će dozvoliti ili zabraniti protok tog paketa.³¹

Funkcije fajervola

Najčešće funkcije koje obavlja fajervol su: filtriranje paketa, prevođenje mrežnih adresa i proksi servisi.

Filtriranje paketa

Kod filtriranja paketa, zaglavlje paketa (sastoji od izvorišne adrese, odredišne adrese i broja porta) se analizira i upoređuje sa pravilima zaštitnog zida. Shodno tome da li paket zadovoljava pravila, dozvoljava se njegov prolaz ili se vrši njegovo odbacivanje.³²

Proces filtriranja je moguće sprovoditi na osnovu bilo kojeg dijela zaglavlja paketa, pri čemu većina filtera donose odluku na osnovu:

- tipa protokola (na ovaj način moguće je izvršiti diskriminaciju čitavih skupova protokola, kao što su UDP, TCP, ICMP, IGMP)
- IP adrese (prihvatanje ili odbijanje paketa na bazi IP adrese je najjači oblik zaštite koji se može postići prostim filtriranjem paketa)

²⁸ Isto, s. 25, 26.

²⁹ K.Salah-ddine, *Overview Of Firewalls: Types And Policies Managing Windows Embedded Firewall Programmatically*, The International Conference on Engineering & MIS, Monastir, Tunisia, May 2017, s. 1.

³⁰ M. Veinović, A. Jevremović, *Uvod u računarske mreže*, Beograd, 2008, s. 28.

³¹ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, s. 92.

³² Isto, s. 93.

- TCP/UDP porta – na primer, svim računarima se može dozvoliti da pristupe TCP portu 80 (HTTP), dok je pristup TCP portu 22 (ssh) ograničen za računare koji pripadaju određenom opsegu IP adresa.³³

Na bazi definisanih pravila i zaglavlja konkretnog IP paketa, filter paketa može donijeti odluku da prihvati paket, odbaci paket, kao i da odbaci paket i obavesti pošiljaoca da njegov paket nije prihvaćen.³⁴

Prevođenje mrežnih adresa (Network Address Translation-NAT)

NAT predstavlja postupak prevođenja IP adresa računara iz privatne mreže u adresu fajervola, u cilju skrivanja informacija o mrežnim računarima od napadača sa interneta.³⁵ Nakon što je prilikom prolaska paketa kroz zaštitni zid NAT obavio postupak prevođenja adresa, podaci koji se nalaze u tom paketu šalju se mrežnim računarima sa adrese fajervola, pri čemu se koriste tablice prevođenja adresa.³⁶

Postoji nekoliko vrsta prevođenja IP adresa koje omogućavaju da se sakrije identitet računara u lokalnoj mreži. To su: statičko, dinamičko i dinamičko sa preopterećenjem prevođenja IP adresa.

Kod statičkog prevođenja IP adresa blok javnih IP adresa se na osnovu fiksne tablice prevođenja prevodi u blok privatnih IP adresa, tako da jednoj javnoj IP adresi odgovara jedna privatna IP adresa.

Kod dinamičkog prevođenja IP adresa blok javnih IP adresa se dinamički prevodi u blok privatnih IP adresa.³⁷

Dinamičko sa preopterećenjem (port address translation-PAT) prevođenje IP adresa je najčešći način prevođenja IP adresa, koji podrazumijeva da se na osnovu broja porta jedna ili više javnih IP adresa prevodi u veći broj privatnih IP adresa.³⁸

Proksi servisi

S obzirom na činjenicu da analiziraju i eventualno menjaju zaglavlje paketa a ne i njegov sadržaj, filtriranje i NAT ne obezbeđuju potpunu kontrolu podataka koji prolaze kroz fajervol. Tako je moguće da napadač pomoću mrežnog monitora pregleda saobraćaj koji dolazi iz fajervola i na osnovu dobijenih informacija zaključi da zaštitni zid prevodi adrese računara sa unutrašnje mreže.³⁹

³³ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, s. 95.

³⁴ Isto.

³⁵ Isto, s. 98, 99. Posmatrano iz vizure interneta, cijeli saobraćaj iz privatne mreže djeluje kao da dolazi sa jednog računara. (J. Milojković; R. Šoškić, Zaštita mail servera na nivou mrežne infrastrukture, Naučno stručno savetovanje ZITEX, Tara, Srbija, 2006, s. 7. (<https://singipedia.singidunum.ac.rs/izdanje/40097-zastita-mail-servera-na-nivou-mrezne-infrastrukture>))

³⁶ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, s. 98, 99.

³⁷ Isto, s. 99.

³⁸ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, s. 99.

³⁹ Isto, s. 100.

Ova prijetnja sprečava se pomoću proksi aplikativnog sloja, koji omogućava da se potpuno zabrani protok podataka protokola mrežnog sloja i da se dozvoli saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP.

Proksi aplikativnog sloja predstavlja specifičnu klijentsko-serversku kombinaciju za konkretan protokol koji se koristi, pa je, na primer, web proksi kombinacija web servera i web klijenta. Serverski deo proksi protokola prihvata konekcije klijenata unutrašnje mreže, a klijentski deo protokola povezuje se na javni server. Pošto klijentski proksi dio primi podatke od javnog servera, serverska strana proksi aplikacije šalje podatke krajnjem unutrašnjem klijentu.⁴⁰

Kriptozaštita

Kriptografija⁴¹ je deo primenjene matematike koja proučava modele, metode, algoritme, softverska i hardverska sredstva za transformisanje informacija u cilju prikrivanja njihovog sadržaja, kao i sprečavanja njihove modifikacije ili neovlašćene upotrebe.⁴²

Kriptosistem je sistem koji primjenjuje softver, hardver ili softver i hardver u cilju vršenja kriptografske transformacije informacija.⁴³

Kriptoanaliza je odeljak primenjene matematike koji proučava modele, metode, algoritme, softverske i hardverske alate za analizu kriptosistema ili njegovih ulaznih i izlaznih signala s ciljem izdvajanja poverljivih parametara, uključujući i običan tekst.⁴⁴ Znači, kriptoanaliza se, suprotno kriptografiji, bavi otkrivanjem prikrivenog sadržaja transformisanih informacija. Svaki napad na privatnost podataka ustvari predstavlja pokušaj kriptoanalize.⁴⁵

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.⁴⁶

Glavni zadatak kriptografije je da obezbijedi da dvije osobe (pošiljalac i primalac poruke) komuniciraju preko nesigurnog komunikacionog kanala (telefonska linija, računarska mreža itd.) na način da neka treća osoba koja eventualno nadzire komunikacioni kanal ne može razumjeti njihove poruke.⁴⁷

Poruka koju pošiljalac želi da pošalje primaocu naziva se otvoreni tekst (plaintext ili cleartext). Otvoreni tekst se od strane pošiljaoca, pomoću odgovarajućih informacija (ključa za šifrovanje), transformiše u tekst nerazumljiv za treća lica. Takav tekst naziva se šifrat (ciphertext) ili kriptogram, a postupak pomoću kojeg se otvoreni (izvorni) tekst transformiše u kriptogram naziva se kriptovanje ili enkripcija (encryption).⁴⁸

⁴⁰ Isto, s. 100.

⁴¹ Riječ grčkog porijekla koja se prevodi kao tajni zapis (S. Jo, *n.d.*, s. 18).

⁴² N. A. Gatčenko, A. S. Isaev, A. D. kovlev, *Kriptografičeska za ita informacii*, Sankt-Peterburg, 2012, s. 31.

⁴³ N. A. Gatčenko, A. S. Isaev, A. D. kovlev, *n.d.*, s. 31.

⁴⁴ Isto.

⁴⁵ I. Lacmanović, *Elektronsko bankarstvo*, Beograd, 2010, s. 55.

⁴⁶ N. A. Gatčenko, A. S. Isaev, A. D. kovlev, *n.d.*, s. 31.

⁴⁷ S. Jo, *n.d.*, s. 18.

⁴⁸ Isto; N. A. Gatčenko, A. S. Isaev, A. D. kovlev, *n.d.*, s. 31; D. Lacmanović, B. Markoski, I. Lacmanović, *Zaštita podataka na internetu (Razvoj i testiranje RSA asimetričnog kriptografskog postupka)*, XI međunarodni naučno-stručni Simpozijum INFOTEH-Jahorina, Republika Srpska, 2012 s. 932. (https://www.researchgate.net/publication/323070387_Zastita_podataka_na_Internetu_Razvoj_i_testiranje_RSA_asimetricnog_kriptografskog_postupka)

Nakon kriptovanja, pošiljalac šalje kriptogram preko nekog komunikacionog kanala, pri čemu osoba koja eventualno prisluškuje kanal može saznati sadržaj šifrata, ali mu neće biti jasno šta je zapisano u otvorenom tekstu. Međutim, primalac, budući da mu je poznat ključ kojim je kriptovana (šifrovana) poruka, u stanju je da dešifruje (dekriptuje), odnosno vrati kriptogram u otvoreni tekst, i da ga pročita.⁴⁹

Kriptografski algoritmi ili šifre predstavljaju matematičku funkciju koja se koristi za šifrovanje i dešifrovanje. Razlikuju se ograničeni algoritmi i algoritmi zasnovani na ključu. Kod ograničenih algoritama bezbjednost se zasniva na tajnosti algoritma, dok se kod algoritama zasnovanih na ključu bezbjednost zasniva na ključevima (algoritam je poznat, a ključ se čuva tajnim).⁵⁰

U modernoj kriptografiji koriste se algoritmi zasnovani na ključu zbog njihovih praktičnih prednosti u odnosu na ograničene algoritme. Mogu se podijeliti na simetrične (često se nazivaju i konvencionalnim), asimetrične i hibridne algoritme.⁵¹

Kod simetričnih kriptografskih algoritama isti tajni ključ se koristi i za kriptovanje i za dekriptovanje poruka.⁵² Najpoznatiji simetrični kriptografski algoritama koji se danas koriste su: 3DES, DES-CBC, IDEA, RC5, RC6, AES i drugi.⁵³

Za razliku od kriptovane poruke, koja može da se šalje preko nezaštićenog komunikacionog kanala, s obzirom na to da ne postoji mogućnost da eventualni napadač bez odgovarajućeg ključa pročita izvornu poruku, ključ se, sasvim je jasno, ne smije prenositi nezaštićenim kanalom komunikacije.⁵⁴

Asimetrični kriptografski algoritmi koriste različite ključeve za kriptovanje i dekriptovanje. Za kriptovanje se koristi javni ključ (koji je poznat svima), dok se za dekriptovanje upotrebljava privatni (tajni) ključ, koji je poznat samo primaocu poruke.⁵⁵

Hibridni algoritmi za kriptovanje predstavljaju kombinaciju simetričnih i asimetričnih algoritama. Primjenom hibridnog algoritma izvorni tekst se prvo kriptuje upotrebom ključa (sesijski ključ), a potom se taj ključ zajedno sa kriptovanom porukom pakuje i opet kriptuje pomoću javnog ključa osobe kojoj se šalje poruka. U postupku dekripcije osoba koja je primila poruku prvo dekriptuje istu sa svojim tajnim ključem, pronalazi zapakovani sesijski ključ i koristi ga da bi pročitala izvornu poruku.⁵⁶

Digitalni potpis je način za potvrđivanje autentičnosti i integriteta poruke zasnovan na asimetričnoj kriptografiji.⁵⁷ Digitalan potpis u stvari predstavlja digitalnu verziju svojeručnog potpisa. Kao što svojeručni potpis identifikuje osobu, digitalni potpis identifikuje autora neke poruke, ali i dokazuje da poruka prilikom prenosa komunikacionim kanalom nije izmjenjena.⁵⁸

⁴⁹ S. Jo, *n.d.*, s. 18; I. Lacmanović, *n.d.*, s. 55; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 932.

⁵⁰ S. Jo, *n.d.*, s. 18; I. Lacmanović, *n.d.*, s. 56.

⁵¹ I. Lacmanović, *n.d.*, s. 56; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 932.

⁵² I. Lacmanović, *n.d.*, s. 56.

⁵³ D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 933.

⁵⁴ Isto.

⁵⁵ I. Lacmanović, *n.d.*, s. 56; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 933.

⁵⁶ D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 935.

⁵⁷ M. Veinović, S. Adamović, *Kriptologija I*, Beograd, 2013, s. 18; M. Milić, *Digitalni potpis u elektronskom poslovanju (specijalistički rad)*, Podgorica, 2016, s. 3.

⁵⁸ I. Lacmanović, *n.d.*, s. 58.

Bio on digitalni ili svojeručni, svaki potpis mora da zadovolji pet osnovnih kriterijuma. Pored toga što mora da bude vjerodostojan, potpis treba da obezbjedi identifikaciju, kao i nemogućnost manipulisanja, opovrgavanja i kopiranja.

Ovi kriterijumi mogu se ispuniti pravilnom upotrebom asimetričnih algoritama enkripcije, uz enkripciju poruke privatnim ključem pošiljaoca.

U najvećem broju slučajeva nije potrebno kriptovati cjelokupnu poruku. Dovoljno je samo da se kriptuje digitalni potpis, a poruka da ostane nepromijenjena. Svakako, ukoliko je tajnost poruke kritična, ona može biti zaštićena.⁵⁹

Za kreiranje digitalnih potpisa upotrebljavaju se heš funkcije.⁶⁰ Heš funkcija predstavlja deterministički postupak koji uzima proizvoljan blok podataka i vraća niz bita fiksne dužine, tj. heš vrijednost. Ukoliko dođe do promjene podataka (slučajno ili namjerno) mijenja se i heš vrijednost.⁶¹

Identifikacija pošiljaoca dokazuje se na osnovu same mogućnosti dekriptovanja enkriptovane heš vrijednosti, što se čini na osnovu javnog ključa za koji se zna da pripada pošiljaocu. Prilikom prijema poruke, jednostavnim poređenjem heš vrijednosti na određenom računaru, lako se može utvrditi da li je poruka bila izmijenjena. Na ovaj način se ostvaruje sigurna identifikacija pošiljaoca, uz očuvanje integriteta poruke.⁶²

Postavlja se pitanje kako primalac poruke može biti siguran u to da je vlasnik određenog javnog ključa upravo pošiljalac poruke. Ovaj problem se rješava korišćenjem digitalnih sertifikata.

Digitalni sertifikat se može definisati kao elektronski dokument koji povezuje javni ključ sa imenom vlasnika na povjerljiv i bezbjedan način, koristeći usluge povjerljivog provajdera, poznatog kao sertifikaciono tijelo (Certificatio Authority-CA), koji garantuje ovaj odnos.⁶³

Nakon što mu je aplikant dostavio tražene podatke (javni ključ, informacije o aplikantu) sertifikaciono tijelo, pošto je izvršilo provjeru podataka, izdaje i potpisuje sertifikat svojim privatnim ključem. Time se obezbjeđuje integritet podataka, odnosno integritet izdatog sertifikata, pri čemu se vjerodostojnost potpisa na sertifikatu može provjeriti pomoću javnog ključa izdavaoca sertifikata. Provjerom potpisa na sertifikatu istovremeno se utvrđuje i identitet vlasnika odgovarajućeg javnog ključa.⁶⁴

⁵⁹ Isto.

⁶⁰ Isto.

⁶¹ Podaci koji se kodiraju često se nazivaju porukom, a heš vrijednost se naziva sažetak ili otisak poruke. Idealna heš funkcija ima četiri glavne osobine: heš vrijednost se lako izračunava za bilo koju poruku; za zadatu heš vrijednost nije moguće pronaći originalnu poruku; sadržaj poruke je nemoguće promijeniti, a da se ne promijeni njena heš vrijednost; nije moguće pronaći dvije poruke koje imaju istu heš vrijednost. (M. Milić, *n.r.*, s. 8.)

⁶² I. Lacmanović, *n.d.*, s. 59.

⁶³ M. Milosavljević, G. Grubor, *Osnovi bezbjednosti i zaštite informacionih sistema*, Beograd, 2006, s. 179.

⁶⁴ M. Veinović, S. Adamović, *n.d.*, s. 142, 143; I. Lacmanović, *n.d.*, s. 61.

Zaključak

S obzirom na činjenicu da se servisi elektronskog bankarstva ostvaruju u mrežnom okruženju, oni podliježu istim sigurnosnim rizicima kao i ostali tipovi veb-aplikacija. Da bi se osigurala sigurnost ovih servisa od raznih napada (socijalni inženjering, skeniranje portova, probijanje lozinke, trojanci, fišing i dr) neophodno je obezbjediti strogu kontrolu svih komponenti sistema i zaštitu na nivoima mreže, operativnog sistema, aplikacije i korisnika, te proceduralnu i operacionu zaštitu. To se postiže primjenom različitih mjera zaštite računarskih mreža i informacija kao što su: mjere kadrovske politike; organizaciono-administrativne mjere; tehničke mjere fizičke, elektronske i protivpožarne zaštite; hardver-sko-softverske mjere; aplikativno programske mjere i mjere kriptozastite. Pri tome se, svakako, treba pridržavati osnovnih principa sigurnosti na kojima se temelji primjena elektronskog bankarstva, u koje spadaju: povjerljivost, integritet, dostupnost, autentičnost, neporecivost, enkripcija i praćenje.

Posmatrano sa aspekta bankarskog elektronskog poslovanja, obezbjeđenje adekvatne zaštite informacija, uz kvalitet servisa koje banka nudi svojim klijentima, sigurno da je od suštinskog značaja prilikom opredjeljivanja klijenata za korišćenja usluge određene banke, pošto oni, sasvim je jasno, ne žele da budu predmet hakerskih napada, koji im u konačnom ishodu uglavnom nanose štetu finansijske prirode. Stoga banke, ukoliko žele da zadrže postojeće i privuku nove klijente, posebnu pažnju moraju da obrate na trendove razvoja sistemima zaštite informacija i njihovu blagovremenu primjenu.

Literatura

1. Veinović, M., Adamović, S., *Kriptologija I*, Beograd, 2013.
2. Veinović, M., Jevremović A., *Uvod u računarske mreže*, Beograd, 2008.
3. Vujošević-Janičić, M., *Automatsko otkrivanje prekoračenja bafera u programskom jeziku C (magistarski rad)*, Beograd, 2008.
4. Vuletić, D.V., „Napadi na računarske sisteme”, *Vojnotehnički glasnik*, br. 1, Beograd, 2012, 235–249.
5. Gatčenko, N. A., Isaev, A. S., kkkovlev A. D., *Kriptografičeska zaštita informacij*, Sankt-Peterburg, 2012.
6. Jevtović M., „Zaštita računarskih mreža”, *Vojnotehnički glasnik* br. 5, Beograd, 2005, 430–441.
7. Jo, S., *Zaštita računarskih mreža–analiza antivirusne zaštite (master rad)*, Beograd, 2015.
8. Korać D. M., *Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (doktorska disertacija)*, Beograd, 2018.
9. Lacmanović, I., *Elektronsko bankarstvo*, Beograd, 2010.

10. Lacmanović, D., Markoski B., Lacmanović I., „Zaštita podataka na internetu (Razvoj i testiranje RSA asimetričnog kriptografskog postupka)“ XI međunarodni naučno-stručni Simpozijum INFOTEH-Jahorina, Republika Srpska, 2012, 931–936. (https://www.researchgate.net/publication/323070387_Zastita_podataka_na_Internetu_Razvoj_i_testiranje_RSA_asimetricnog_kriptografskog_postupka)
11. Milić, M., *Digitalni potpis u elektronskom poslovanju (specijalistički rad)*, Podgorica, 2016.
12. Milić, M., *Odlučivanje i poslovna inteligencija*, Banja Luka, 2014.
13. Milojković, J.; Šoškić, R., Zaštita mail servera na nivou mrežne infrastructure, Naučno stručno savetovanje ZITEX, Tara, Srbija, 2006. (<https://singipedia.singidunum.ac.rs/izdanje/40097-zastita-mail-servera-na-nivou-mrezne-infrastrukture>)
14. Milosavljević, M., Grubor, G., *Osnovi bezbjednosti i zaštite informacionih sistema*, Beograd, 2006.
15. Milosavljević, M., Mišković, V., *Elektronska trgovina*, Beograd, 2016.
16. Omariba, Z.B., Masese, N.B., Wanyembi, G., „Security and privacy of electronic banking“, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, 432–446.
17. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M., *Sigurnost računarskih mreža*, Beograd, 2006.
18. Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., Labus, A., *Elektronsko poslovanje*, Beograd, 2015.
19. Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., Labus, A., *Priručnik za pripremu prijemnog ispita za upis na master studije*
20. Reznik, I. A., *Elektronный banking*, Orenburg, 2008.
21. Salah-ddine, K., *Overview Of Firewalls: „Types And Policies Managing Windows Embedded Firewall Programmatically“*, The International Conference on Engineering & MIS, Monastir, Tunisia, May 2017.
22. Simović, V., *Elektronsko poslovanje-skripta (verzija 2)*, Beograd, 2013.
23. Unković, M., Milosavljević, M., Stanišić, N., *Savremeno berzansko i elektronsko poslovanje*, Beograd, 2010.
24. Uroš, T., *Elektronsko bankarstvo*, Beograd, 2014.
25. <https://whatistechtarget.com/definition/script>

Received: 26.03.2021
Accepted: 16.07.2021

DOI: 10.5937/bankarstvo2102152B

INFORMATION PROTECTION SYSTEMS IN E-BANKING

Darko Bakić, Independent Advisor, Ministry of Economic Development
of Montenegro

Summary:

Because it is implemented in a network environment, electronic banking is subject to various security risks. Therefore, in order to safely use banking services electronically, it is necessary to identify potential threats through the analysis of network infrastructure and application characteristics, as well as to respond to them by applying appropriate protection measures.

Keywords: electronic banking; protection systems; safety principles; attacks; protection measures; aspects of protection; firewall; cryptosecurity

JEL classification: E42, K24, L86, M15

Introduction

Electronic banking (e-banking), together with e-commerce, customer relationship management, enterprise resource planning, value chain management and business intelligence, is an integral part of e-business.¹ Electronic business is defined in the broadest sense as an internal or external business process that is realised through a computer network.²

Electronic banking means the totality of technological procedures, which ensure the electronic execution of banking transactions.³ In other words, electronic banking is a type of banking that takes place using electronic systems, whose task is to transfer funds and make records related to them, without paper, using computer communication technologies.⁴ Thus, bank clients can use electronic banking services via the Internet, mobile devices, ATMs and POS terminals.

As the concept of electronic banking enables the users of banking services, but also banks themselves, to fulfil their usual activities electronically, the basic precondition for its normal functioning is a correct bank information system, functional network infrastructure and protection of information and transactions.

¹ E-commerce is defined as a transaction via a computer network, which involves the transfer of ownership or rights to use goods and services, such as: buying books online, booking a hotel room online, ordering and downloading free software online, etc. (B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *Electronic Business*, Belgrade, 2015, p. 131)

Customer Relationship Management (CRM) is a part of e-business that includes a number of methods, techniques and proven practices implemented within the business system, in order to improve communication and cooperation with customers, promote products and services and maximize business profits. It is a business strategy whose results simultaneously optimize profitability and revenue, contribute to customer satisfaction and loyalty, and which include all aspects of the company's interaction with customers, regardless of whether it is sales or services. The goal is to create a situation in which each of the clients will have special treatment and offers that suits them best at a given moment and that will apply only to them. (Ibid.; V. Simović, *Electronic Business-Script*) (version 2), Belgrade, 2013, p. 10)

Enterprise Resource Planning (ERP) is a software package that monitors all aspects of a company's business. It is characterized by effective management of processes in the company, the existence of a common (unique) database, as well as the ability to respond quickly to operational requirements. (V. Simović, nd, p. 11; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *Manual for the preparation of the entrance exam for enrolment in master studies*, Belgrade, 2012, p. 32.33)

Supply Chain Management (SCM) is a term used to describe the flow of materials, information and resources through the supply chain (value) from the supplier through the manufacturer of individual components, final connection and distribution (warehousing and retail) to the final customer, whereby this process often includes additional services that accompany the product after the sale and return of the product for recycling. A value chain is a set of business processes that connects suppliers, manufacturers, retailers, business users, and others involved in creating, selling, and delivering goods to the end customer. (V. Simović, n.d., p. 11; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, n.d., p. 33)

Business Intelligence (BI) is the process of gathering available internal and significant external data and converting it into useful information that helps management in decision-making. (M. Milić, *Decision Making and Business Intelligence*, Banja Luka, 2014, p. 85)

² B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, n.d., p. 4.

³ I. A. Reznik, *Elektronnyiĭ banking*, Orenburg, 2008, p. 7.

⁴ T. Uroš, *Elektronsko bankarstvo*, Belgrade, 2014, p. 120.

Certainly, from the aspect of the client's trust in terms of using electronic banking systems, it is of special importance to ensure the security of their functioning, i.e., to use appropriate information protection systems to ensure that the security risks to each computer network are minimised.

Basic Principles of Security in Electronic Banking

The basic security principles on which electronic banking services applications should be based include: confidentiality, integrity, availability, authenticity, undeniability, encryption and monitoring.⁵

The principle of confidentiality implies the unavailability of information to unauthorised persons, as well as their protection from interception during transmission.

Respect for the principle of integrity should ensure the invariability of information during online transmission.⁶ In other words, the principle of integrity implies data consistency, preventing unauthorised generating, modification, and destruction of data.⁷

Accessibility is a principle that provides authorised users with timely access to information, i.e., it refers to the access to information at the request of the user.⁸

The principle of authenticity refers to the existence of a mechanism for performing user authentication before allowing access to the requested information.

Non-denial is a principle that implies the impossibility of denying the message sent by the user, as well as the impossibility for the recipient of the message to deny having received it.

According to the principle of encryption, information should be encrypted and decrypted by an authorised user.

The principle of monitoring refers to the need to record data, in order to be able to monitor events in the system.⁹

Attacks on Electronic Banking

Electronic banking can be exposed to different types of attacks such as: social engineering, port scanners, packet sniffers, password cracking, trojans, denial-of-service attacks, server bugs, super user exploits, phishing, etc.¹⁰

⁵ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 225.

⁶ Isto.

⁷ M. Unković, M. Milosavljević, N. Stanišić, *Savremeno berzansko i elektronsko poslovanje*, Belgrade, 2010, p. 231

⁸ D. M. Korać, *Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (PhD thesis)*, Belgrade, 2018, p. 10.

⁹ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, s. 225.

¹⁰ Z.B.Omariba, N.B. Masese, G. Wanyambi, *Security and privacy of electronic banking*, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, p.440; B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, p. 226.

Social engineering involves a situation in which an attacker, posing as a system administrator or customer service representative, tricks a user, abusing their social characteristics (trust, desire to help others, resilience, etc.), to reveal sensitive information in order to access their account.¹¹

Port scanners are used by attackers to identify entry points into the system, using a variety of information theft techniques. This type of software sends signals to a machine or router and records a message by which the machine responds in order to determine the point of entry. The main purpose of port scanning is to gather information related to the hardware and software that runs the system, so that an attack plan can be developed.¹²

Packet analysers or packet sniffers are used to collect data transmitted over the network, i.e., this software monitors the connection between the user's computer and the web server to collect user-related data, including passwords and credit card information. Since they do not manipulate the flow of data, and their function is to capture network traffic, packet sniffers are very difficult to detect.

Password cracking includes various attack options for the purpose of decrypting passwords, the most popular among which is brute force attack. In order to access user data in this way, thousands of common expressions, activities and names are scanned, which are then combined until the appropriate combination, i.e., the user password, is obtained. Violent password cracking is mainly used on systems that do not require strong passwords, so users use common names and activities, which makes it easier to detect the password, i.e., access the system. Other methods of cracking passwords include the use of hash tables to decrypt password files, which can reveal a full list of system usernames and passwords.¹³

Trojans are complex client-server applications, which allow access to remote user computers in the network (they reach users via email, newsgroups, popular chat programs, etc.), in the way that users install them on their computer, believing that they will be of use to them. The Trojan, which is located on the user's (victim's) computer, is actually a server, and the client is a program that manages the Trojan and which is located on the computer of the person who intends to access important information on the victim's account.¹⁴

A denial-of-service attack is a type of attack that aims to prevent legitimate users from accessing network services, which is achieved by overloading network services or over-connection, resulting in a connection or service drop. Namely, the infrastructure of interconnected systems and networks consists of limited resources, which is the most important fact in denial-of-service attacks, which involve sending a large number of requests to the target server, to overwhelm its limited resources and make it unusable.¹⁵

Server bugs are often detected and corrected in a timely manner. However, system administrators are often slow to apply the latest updates, giving the attacker enough time to create a threat.¹⁶

¹¹ Ibid.

¹² Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.d.*, s.440.

¹³ Ibid.

¹⁴ S. Jo, *n.d.*, Belgrade, 2015, p. 28–29.

¹⁵ D.V.Vuletić, *Napadi na računarske sisteme*, Vojnotehnički glasnik, br. 1, Belgrade, 2012, p. 236.

¹⁶ Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.r.*, p. 442.

Super user exploits allow an attacker to take control of the system as if they were an administrator. For this purpose, scripts are often used¹⁷ to manipulate the database or a buffer overrun attack¹⁸, which damages the system much like a denial-of-service attack.¹⁹

Phishing is a type of attack that involves attempting to steal personal information by tricking the victim into entering a fake website.²⁰ For this purpose, attackers (fishermen) usually use forged emails, which they send to potential victims on behalf of certain organisations with which they have contact (e.g., bank, insurance company, etc.). For example, an email is sent to a bank user stating that their account will be terminated if they do not update their personal information. The e-mail also provides a link to a fake website, which is a true copy of the original website of a certain institution, where the potential victim enters their account number and password, which is later misused, primarily in order to obtain financial benefits for the attacker.²¹

Measures to Protect Computer Networks and Information

Network and information protection refers to a set of rules, procedures, algorithms, hardware and software components, as well as a set of organisational and technical measures that protect network functions when performing network transactions.

Information protection includes protection against: unauthorised access to and use of information, uncontrolled leakage of information, accidental or intentional damage, alteration or destruction.

The protection of computer networks and information is realised through the application of various measures such as: personnel policy measures; organisational-administrative measures; technical measures for physical, electronic and fire protection; hardware and software measures; application program measures and cryptosecurity measures.²²

Personnel policy measures are needed because the users of network services are the information carriers, but also the greatest potential danger for that information.

Organisational-administrative measures normatively regulate the rights, obligations, and responsibilities of information system users, including sanctions against users.

¹⁷ In computer programming, a script is a program or sequence of instructions that is interpreted or executed by another program. (<https://whatistechtarget.com/definition/script>)

¹⁸ Exceeding the buffer (buffer block of memory intended for temporary data storage) means writing content outside the boundaries of the reserved buffer memory. In fact, it is a situation in which the address of an available buffer is indicated, but locations that are not part of its memory are used. Exceeding the buffer can lead to an unexpected flow of program execution, as well as allow various types of program abuse. This problem is especially present in programs written in the programming language C. (M. Vujošević-Janičić, *Automatsko otkrivanje prekoračenja bafera u programskom jeziku C (magisterial thesis)*, Belgrade, 2008, s. 9, 87)

¹⁹ Z.B.Omariba, N.B. Masese, G. Wanyembi, *n.r.*, p. 442.

²⁰ B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, *n.d.*, p. 226.

²¹ D.V.Vuletić, *n.r.*, p. 238

²² M. Jevtović, *Zaštita računarskih mreža*, Vojnotehnički glasnik br. 5, Belgrade, 2005, p. 435.

Technical measures for physical, electronic and fire protection include: physical security, electronic burglary protection and protection against disappearance and inadequate power supply. These measures are applied for the protection of: facilities (premises where computer and telecommunication equipment is located), computer and telecommunication equipment and magnetic and electronic data carriers.²³

Hardware-software measures are used to provide access points to the network and individual network resources. These measures include identifying the user and determining the rights and authorities given to them in relation to the network resources which they access.²⁴

Application-program measures are procedures that are built into the application software in order to protect it.

Cryptoprotection measures are applied to protect data stored in memory resources in computers and for protection on transmission paths.²⁵

Various Aspects of Computer Network and Information Protection

Different aspects of protection are very often defined in relation to the place of positioning of protection mechanisms in a computer or information system or computer network. In this sense, we can talk about protection at the application level, protection at the operating system level, protection at the network infrastructure level, and procedural and operational protection.²⁶

Application-level security can include the following elements: software application protection, isolation of critical applications on dedicated hosts, as well as the application of specific protocols (for example, cryptographically protected SSH protocol instead of unprotected Telnet protocol). Operating system-level protection is a very complex and extensive area that affects all layers of the operating system. This level of protection includes the connection between the operating system and the application, as well as the relationship to the network architecture, i.e., connections to other systems. According to some recommendations, minimal protection encompasses: blocking unnecessary services (finger, ftp, telnet), providing comprehensive and mandatory access control at the user level, ensuring the integrity of the software that makes up the operating system (most security attacks are aimed at operating systems without patches, so it is necessary to regularly update all system elements to the latest patches).

23 Ibid, p. 435.

24 User identification can be physical (hardware devices are used) and logical (software methods are used).

Physical identification methods are based on recognizing the user's identification means (smart cards, magnetic and optical cards, badges, tokens, etc.) and recognizing the user's physical, biometric characteristics, fingerprint, fingerprint and hand shape, ear or head shape, voice characteristics, retinal image and more)

Logical recognition methods are based on the information that the user gives to the system in the process of identification and authorization of authorizations. This information must be identical to the information available to the system. (Ibid, p. 435, 436)

25 Ibid, p. 435

26 D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *Sigurnost računarskih mreža*, Belgrade, 2006, p. 25.

Network infrastructure protection includes the following basic elements: applying network barriers (firewalls), blocking unnecessary ports, encrypting paths, isolating paths using routers and switches, or using special infrastructure.

When it comes to procedural and operational protection, the following elements are taken into account: protection by applying policies and procedures, attack detection, proactive action in terms of protecting system vulnerabilities, managing system configuration and user education.²⁷

Firewall

The firewall is a key element in network security, which, has found wide application both in banks and in other organisations and institutions for the protection of private networks.²⁸

A firewall is a security hardware or software device, usually located between a local network and a public network (Internet), whose purpose is to protect data on the network from unauthorised users (blocking and denying access in accordance with the rules of the adopted security policy).²⁹ In other words, a firewall is a filter on the local area network - the Internet, which examines all packets passing between the private network and the Internet, and depending on whether the packets meet the rules defined by access control lists, the firewall will allow or deny the packet.³⁰

Firewall Functions

The most common functions performed by firewall are: packet filtering, network address translation and proxy services.

Packet Filtering

When packet filtering, the packet header (consisting of the source address, destination address, and port number) is analysed and compared to the firewall rules. Depending on whether the package meets the rules, its passage is either allowed, or rejected.³¹

The filtering process can be performed based on any part of the packet header, with most filters making a decision based on:

- protocol type (in this way it is possible to discriminate against entire sets of protocols, such as UDP, TCP, ICMP, IGMP)

²⁷ Ibid, p. 25, 26.

²⁸ K.Salah-ddine, *Overview Of Firewalls: Types And Policies Managing Windows Embedded Firewall Programmatically*, The International Conference on Engineering & MIS, Monastir, Tunisia, May 2017, p. 1.

²⁹ M. Veinović, A. Jevremović, *Uvod u računarske mreže*, Belgrade, 2008, p. 28.

³⁰ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, p. 92.

³¹ Ibid, p. 93.

- IP addresses (accepting or rejecting packets based on IP address is the strongest form of protection that can be achieved by simply filtering packets)
- TCP/UDP ports - for example, all computers can be allowed to access TCP port 80 (HTTP), while access to TCP port 22 (ssh) is restricted to computers belonging to a certain range of IP addresses.³²

Based on the defined rules and headers of a specific IP packet, the packet filter can make a decision to accept the packet, reject the packet, as well as to reject the packet and inform the sender that its packet has not been accepted.³³

Network Address Translation - NAT

NAT is the process of translating computer IP addresses from a private network to a firewall address, in order to hide information about network computers from attackers from the Internet.³⁴ After the address translation process has been performed during the passage of the packet through the NAT firewall, the data contained in that packet is sent to the network computers from the firewall address, using the address translation tables.³⁵

There are several types of IP address translation that allow you to hide the identity of your computer on the local network. These are: static, dynamic, and dynamic overload translation of IP addresses.

In static IP address translation, a block of public IP addresses is translated into a block of private IP addresses based on a fixed translation table, so that one public IP address corresponds to one private IP address.

In dynamic IP address translation, a block of public IP addresses is dynamically translated into a block of private IP addresses.³⁶

Dynamic overload translation (PAT) of IP addresses is the most common way of translating IP addresses, which means that based on the port number, one or more public IP addresses are translated into a larger number of private IP addresses.³⁷

Proxy Services

Due to the fact that they analyse and possibly change the packet header and not its contents, filtering and NAT do not provide complete control of the data passing through the firewall. Thus, it is possible for an attacker to use a network monitor to view traffic coming from the firewall and, based on the

³² D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, p. 95.

³³ Ibid.

³⁴ Ibid, p. 98, 99.

Viewed from the perspective of the Internet, all traffic from a private network acts as if it came from a single computer. (J. Milojković; R. Šoškić, *Zaštita mail servera na nivou mrežne infrastructure*, Naučno stručno savetovanje ZITEX, Tara, Serbia, 2006, p. 7. (<https://singipedia.singidunum.ac.rs/izdanje/40097-zastita-mail-servera-na-nivou-mrezne-infrastrukture>))

³⁵ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, p. 98, 99.

³⁶ Ibid, p. 99.

³⁷ D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *n.d.*, s. 99.

information obtained, conclude that the firewall is translating computer addresses from the internal network.³⁸

This threat is prevented by the proxy application layer, which allows to completely prohibit the flow of network layer protocol data and to allow traffic only to higher layer protocols, such as HTTP, FTP and SMTP.

An application layer proxy is a specific client-server combination for a particular protocol used, so it is, for example, a web proxy combination of a web server and a web client. The server portion of the proxy protocol accepts internal network client connections, and the client portion of the protocol connects to the public server. Since the client proxy part receives data from the public server, the server side of the proxy application sends the data to the end internal client.³⁹

Cryptosecurity

Cryptography⁴⁰ is a part of applied mathematics that studies models, methods, algorithms, software and hardware means of transforming information in order to conceal their content, as well as to prevent their modification or unauthorised use.⁴¹

A cryptosystem is a system that applies software, hardware, or software and hardware to perform cryptographic information transformation.⁴²

Cryptanalysis is a section of applied mathematics that studies models, methods, algorithms, software and hardware tools for analysing a cryptosystem or its input and output signals in order to extract confidential parameters, including plain text.⁴³ Thus, cryptanalysis, in contrast to cryptography, deals with the detection of the hidden content of transformed information. Any attack on data privacy is actually an attempt at cryptanalysis.⁴⁴

Cryptology is a science that combines cryptography and cryptanalysis.⁴⁵

The main task of cryptography is to ensure that two people (sender and receiver of a message) communicate through an insecure communication channel (telephone line, computer network, etc.) in such a way that a third person who is possibly monitoring the communication channel cannot understand their messages.⁴⁶

The message that the sender wants to send to the recipient is called plaintext or cleartext. The plaintext is transformed by the sender, with the help of appropriate information (encryption key), into text

³⁸ Ibid, p. 100.

³⁹ Ibid, p. 100.

⁴⁰ A word of Greek origin that translates as a secret record (S. Jo, *n.d.*, p. 18).

⁴¹ N. A. Gatčenko, A. S. Isaev, A. D. Яkovlev, *Kriptografičeskaja zaučita informacii*, Sankt-Peterburg, 2012, p. 31.

⁴² N. A. Gatčenko, A. S. Isaev, A. D. Яkovlev, *n.d.*, p. 31.

⁴³ Ibid.

⁴⁴ I. Lacmanović, *Elektronsko bankarstvo*, Belgrade, 2010, p. 55.

⁴⁵ N. A. Gatčenko, A. S. Isaev, A. D. Яkovlev, *n.d.*, p. 31.

⁴⁶ S. Jo, *n.d.*, p. 18.

incomprehensible to third parties. Such text is called a ciphertext or cryptogram, and the process by which open (original) text is transformed into a cryptogram is called encryption.⁴⁷

After encryption, the sender sends a cryptogram via a communication channel, whereby the person who is possibly eavesdropping on the channel can find out the content of the cipher, but it will not be clear to them what is written in the open text. However, the recipient, since they know the key with which the message is encrypted, is able to decrypt the message, i.e., return the cryptogram to the plaintext form, and read it.⁴⁸

Cryptographic algorithms or ciphers are a mathematical function used to encrypt and decrypt. There are limited algorithms and key-based algorithms. In limited algorithms, security is based on the secrecy of the algorithm, while in key-based algorithms, security is based on keys (the algorithm is known, and the key is kept secret).⁴⁹

Modern cryptography uses key-based algorithms because of their practical advantages over limited algorithms. They can be divided into symmetric (often referred to as conventional), asymmetric, and hybrid algorithms.⁵⁰

In symmetric cryptographic algorithms, the same secret key is used to encrypt and decrypt messages.⁵¹ The most well-known symmetric cryptographic algorithms used today are: 3DES, DES-CBC, IDEA, RC5, RC6, AES and others.⁵²

Unlike an encrypted message, which can be sent over an unsecured communication channel, since there is no possibility for a potential attacker to read the original message without an appropriate key, the key must not be transmitted through an unsecured communication channel.⁵³

Asymmetric cryptographic algorithms use different keys for encryption and decryption. An encryption uses a public key (known to everyone), while a decryption uses a private (secret) key, which is known only to the recipient of the message.⁵⁴

Hybrid encryption algorithms are a combination of symmetric and asymmetric algorithms. Using a hybrid algorithm, the source text is first encrypted using a key (session key), and then that key is packed together with the encrypted message and re-encrypted using the public key of the person to whom the message is sent. In the decryption process, the person who received the message first decrypts it with their secret key, finds the packed session key and uses it to read the original message.⁵⁵

⁴⁷ Ibid; N. A. Gatčenko, A. S. Isaev, A. D. Яkovlev, *n.d.*, s. 31; D. Lacmanović, B. Markoski, I. Lacmanović, *Zaštita podataka na internetu (Razvoj i testiranje RSA asimetričnog kriptografskog postupka)*, XI međunarodni naučno-stručni Simpozijum INFOTEH-Jahorina, Republika Srpska, 2012 s. 932. (https://www.researchgate.net/publication/323070387_Zastita_podataka_na_Internetu_Razvoj_i_testiranje_RSA_asimetrichnog_kriptografskog_postupka)

⁴⁸ S. Jo, *n.d.*, p. 18; I. Lacmanović, *n.d.*, p. 55; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, p. 932.

⁴⁹ S. Jo, *n.d.*, p. 18; I. Lacmanović, *n.d.*, p. 56.

⁵⁰ I. Lacmanović, *n.d.*, p. 56; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, p. 932.

⁵¹ I. Lacmanović, *n.d.*, p. 56.

⁵² D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, p. 933.

⁵³ Ibid.

⁵⁴ I. Lacmanović, *n.d.*, p. 56; D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, p. 933.

⁵⁵ D. Lacmanović, B. Markoski, I. Lacmanović, *n.r.*, s. 935.

A digital signature is a way to verify the authenticity and integrity of a message based on asymmetric cryptography.⁵⁶ A digital signature is actually a digital version of a handwritten signature. Just as a handwritten signature identifies a person, a digital signature identifies the author of a message, but also proves that the message has not been altered during transmission through the communication channel.⁵⁷

Whether digital or personal, each signature must meet five basic criteria. In addition to being authentic, the signature should provide identification as well as the impossibility of manipulation, refutation and copying.

These criteria can be met by the correct use of asymmetric encryption algorithms, with encryption of the message with the sender's private key.

In most cases, it is not necessary to encrypt the entire message. All you have to do is encrypt the digital signature and keep the message unchanged. Certainly, if the confidentiality of a message is critical, it can be protected.⁵⁸

Hash functions are used to create digital signatures.⁵⁹ A hash function is a deterministic procedure that takes an arbitrary block of data and returns it through bits of fixed length, i.e., hash value. If there is a change in the data (accidentally or intentionally), the hash value also changes.⁶⁰

The sender's identification is proven on the basis of the very possibility of decrypting the encrypted hash value, which is done on the basis of the public key that is known to belong to the sender. When receiving a message, by simply comparing the hash values on a particular computer, it is easy to determine whether the message has been altered. In this way, a secure identification of the sender is achieved, while preserving the integrity of the message.⁶¹

The question arises as to how the recipient of a message can be sure that the owner of a particular public key is really the sender of the message. This problem is solved by using digital certificates.

A digital certificate can be defined as an electronic document that associates a public key with the owner's name in a confidential and secure manner, using the services of a trusted provider, known as a Certification Authority (CA), that guarantees this relationship.⁶²

After the applicant has submitted the requested data (public key, information about the applicant), the certification body, after verifying the data, issues and signs the certificate with its private key. This ensures the integrity of the data, i.e., the integrity of the issued certificate, whereby the authenticity of the signature on the certificate can be verified using the public key of the issuer of the certificate.

⁵⁶ M. Veinović, S. Adamović, *Kriptologija I*, Belgrade, 2013, p. 18; M. Milić, *Digitalni potpis u elektronskom poslovanju (specijalistički rad)*, Podgorica, 2016, p. 3.

⁵⁷ I. Lacmanović, *n.d.*, p. 58.

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ The data that is encoded is often called a message, and the hash value is called a summary or imprint of the message. The ideal hash function has four main features: the hash value is easily calculated for any message; it is not possible to find the original message for the given hash value; the content of the message cannot be changed without changing its hash value; it is not possible to find two messages that have the same hash value. (M. Milić, *n.r.*, s. 8.)

⁶¹ I. Lacmanović, *n.d.*, p. 59.

⁶² M. Milosavljević, G. Grubor, *Osnovi bezbjednosti i zaštite informacionih sistema*, Belgrade, 2006, p. 179.

By verifying the signature on the certificate, the identity of the owner of the corresponding public key is also determined.⁶³

Conclusion

Due to the fact that e-banking services are provided in a network environment, they are subject to the same security risks as other types of web applications. In order to ensure the security of these services from various attacks (social engineering, port scanning, password cracking, Trojans, phishing, etc.) it is necessary to provide strict control of all system components and protection at the network, operating system, applications and users, and procedural and operational protection. This is achieved by applying various measures to protect computer networks and information, such as: personnel policy measures; organisational-administrative measures; technical measures for physical, electronic and fire protection; hardware and software measures; application software measures and crypto security measures. In doing so, the basic principles of security on which the application of electronic banking is based should be adhered to, which include: confidentiality, integrity, availability, authenticity, non-repudiation, encryption and monitoring.

Observed from the aspect of e-banking, providing adequate information protection, along with the quality of services that the bank offers to its clients, is certainly essential when clients decide whether to use the services of a particular bank, as they clearly do not want to be hacked, which would ultimately and mainly financially harm them. Therefore, banks, if they want to keep existing and attracting new customers, must pay special attention to the development trends of information protection systems and their timely implementation.

References

1. Veinović, M., Adamović, S., *Kriptologija I*, Belgrade, 2013.
2. Veinović, M., Jevremović A., *Uvod u računarske mreže*, Belgrade, 2008.
3. Vujošević-Janičić, M., *Automatsko otkrivanje prekoračenja bafera u programskom jeziku C (magistarski rad)*, Belgrade, 2008.
4. Vuletić, D.V., „Napadi na računarske sisteme”, *Vojnotehnički glasnik*, br. 1, Belgrade, 2012, 235–249.
5. Gatčenko, N. A., Isaev, A. S., Яkkovlev A. D., *Kriptografičeskaja zaščita informacii*, Sankt-Peterburg, 2012.
6. Jevtović M., „Zaštita računarskih mreža”, *Vojnotehnički glasnik* br. 5, Belgrade, 2005, 430–441.
7. Jo, S., *Zaštita računarskih mreža–analiza antivirusne zaštite (master rad)*, Belgrade, 2015.

⁶³ M. Veinović, S. Adamović, *n.d.*, p. 142, 143; I. Lacmanović, *n.d.*, p. 61.

8. Korać D. M., *Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (doktorska disertacija)*, Belgrade, 2018.
9. Lacmanović, I., *Elektronsko bankarstvo*, Belgrade, 2010.
10. Lacmanović, D., Markoski B., Lacmanović I., „Zaštita podataka na internetu (Razvoj i testiranje RSA asimetričnog kriptografskog postupka)“XI međunarodni naučno-stručni Simpozijum INFOTEH-Jahorina, Republika Srpska, 2012, 931–936. (https://www.researchgate.net/publication/323070387_Zastita_podataka_na_Internetu_Razvoj_i_testiranje_RSA_asimetrichnog_kriptografskog_postupka)
11. Milić, M., *Digitalni potpis u elektronskom poslovanju (specijalistički rad)*, Podgorica, 2016.
12. Milić, M., *Odlučivanje i poslovna inteligencija*, Banja Luka, 2014.
13. Milojković, J.; Šoškić, R., Zaštita mail servera na nivou mrežne infrastructure, Naučno stručno savetovanje ZITEX, Tara, Srbija, 2006. (<https://singipedia.singidunum.ac.rs/izdanje/40097-zastita-mail-servera-na-nivou-mrezne-infrastrukture>)
14. Milosavljević, M., Grubor, G., *Osnovi bezbjednosti i zaštite informacionih sistema*, Belgrade, 2006.
15. Milosavljević, M., Mišković, V., *Elektronska trgovina*, Belgrade, 2016.
16. Omariba, Z.B., Masese, N.B., Wanyembi, G., „Security and privacy of electronic banking“, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, 432–446.
17. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M., *Sigurnost računarskih mreža*, Belgrade, 2006.
18. Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., Labus, A., *Elektronsko poslovanje*, Belgrade, 2015.
19. Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., Labus, A., *Priručnik za pripremu prijemnog ispita za upis na master studije*
20. Reznik, I. A., *Elektronnyi banking*, Orenburg, 2008.
21. Salah-ddine, K., *Overview Of Firewalls: „Types And Policies Managing Windows Embedded Firewall Programmatically“*, The International Conference on Engineering & MIS, Monastir, Tunisia, May 2017.
22. Simović, V., *Elektronsko poslovanje-skripta (verzija 2)*, Belgrade, 2013.
23. Unković, M., Milosavljević, M., Stanišić, N., *Savremeno berzansko i elektronsko poslovanje*, Belgrade, 2010.
24. Uroš, T., *Elektronsko bankarstvo*, Belgrade, 2014.
25. <https://whatis.techtarget.com/definition/script>