Projektiranje i zaštita informacijsko - komunikacijskih sustava u bankarskim institucijama

Ćurić, Filip

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Filip Ćurić

PROJEKTIRANJE I ZAŠTITA INFORMACIJSKO – KOMUNIKACIJSKIH SUSTAVA U BANKARSKIM INSTITUCIJAMA

DIPLOMSKI RAD

Zagreb, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 19. travnja 2016.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 3570

Pristupnik: **Filip Ćurić (0135221074)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Projektiranje i zaštita informacijsko - komunikacijskih sustava u bankarskim institucijama**

Opis zadatka:

Prikazati i vrednovati sigurnosne aspekte pri projektiranju i zaštiti informacijsko-komunikacijskih sustava u bankarskim institucijama. Razviti prijedlog primjene novih metoda zaštite.

Zadatak uručen pristupniku: 21. ožujka 2016.

Mentor:

izv. prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

PROJEKTIRANJE I ZAŠTITA INFORMACIJSKO – KOMUNIKACIJSKIH SUSTAVA U BANKARSKIM INSTITUCIJAMA

DESIGN AND PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS IN BANKING INSTITUTIONS

Mentor: izv. prof. dr. sc. Dragan Peraković
Student: Filip Ćurić, 0135221074

Zagreb, ožujak 2017.

PROJEKTIRANJE I ZAŠTITA INFORMACIJSKO - KOMUNIKACIJSKIH SUSTAVA U BANKARSKIM INSTITUCIJAMA

SAŽETAK

U današnje vrijeme ne može se zamisliti niti jedna mala tvrtka/obrt/kompanija bez informacijskog sustava. Informacijski sustavi su okosnica današnjeg poslovanja u mnogim granama, pa tako i u bankarskom sektoru. Omogućuju i pospješuju vođenje i upravljanje bankarskim procesima. Svaka bankarska institucija mora poslovati sukladno načelima propisane od nadležne osobe inače gubi licencu koja joj je potrebna za rad. Kako bi projektanti lakše uskladili i napravili cijeli informacijski sustav bitno je da znaju moguće prijetnje koje mogu biti uzrokovane od strane čovjeka ili prirode te životne navike korisnika banke. U diplomskom radu provedena je i anketa kojom je analizirana percepcija korisnika sigurnosti korištenja bankarskih usluga. One uvelike mogu pomoći budućim projektantima u cilju projektiranja zadovoljavajućeg informacijsko komunikacijskog sustava.

KLJUČNE RIJEČI: informacijski sustav; projektiranje; smjernice; preporuke; sigurnost

DESIGN AND PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS IN BANKING INSTITUTIONS

SUMMARY

At present time small company / craft / company cannot be imagined without information system. Information systems are the backbone of today's business in many sectors including the banking sector. Allow and facilitate the conduct and management of banking processes. Each banking institution must operate in accordance with the principles laid down by the relevant persons or lose the license it needs to operate. To help planners coordinate and make the entire information system, it is important to know the possible threats that can be caused by man or nature and life habits of the user banks. The thesis conducted a survey which analyzed the perception of user security using banking services. They can greatly help future designers in order to design a satisfactory information and communication system.

KEYWORDS: information system; designing; guidelines; recommendations; safety

SADRŽAJ:

1 UVOD

Računalna sigurnost je zahvaljujući sve bržim rastom računalne industrije postala nezaobilazna tema u projektiranju informacijskih sustava. Sigurnost informacijskih sustava vrlo često je zanemarena na globalnoj razini.

Uz sami razvoj informacijskih tehnologija javila se potreba za uvođenjem informacijskih sustava unutar raznih sektora pa tako i bankarskih ustanova. Kako informacijsko komunikacijski (IK) sustav uvelike pomaže u obavljanju svakodnevnih poslova tako donosi i određenu prijetnju.

Svakim danom svjedoči se sve većem broj napada na bankarske informacijske sustave, kako u Hrvatskoj tako i u svijetu. Sigurnost i pravilno projektiranje informacijskih sustava temelj su za uspješno upravljanje poslovanjem te ispunjenje svih korisničkih zahtjeva. Ne postoji potpuno siguran sustav, ali praćenjem i pridržavanjem propisanih normi i standarda moguće je svesti prijetnje na minimum.

Svrha diplomskog rada je prikazati načine i metode pri projektiranju informacijsko komunikacijskih sustava te zaštita istih. Cilj diplomskog rada je na temelju provedene ankete približiti bankama razmišljanja i načine na koji njihovi korisnici koriste njihove usluge te jesu li uopće svjesni opasnosti i na koji način.

Ovaj diplomski rad podijeljen je na devet logičko povezanih cjelina:

1. Uvod;
2. Osnove informacijsko komunikacijskih sustava;
3. Sigurnosni aspekt primjene informacijsko komunikacijskih sustava;
4. Sigurnosna politika;
5. Sigurnosne prijetnje bankarskom informacijsko komunikacijskom sustavu;
6. Definiranje slojeva za unaprjeđenje sigurnosnih aspekata;
7. Preporuke i smjernice pri projektiranju IK sustava u bankarskim institucijama;
8. Istraživanje percepcije sigurnosti primjene IK tehnologija pri korištenju bankarskih usluga u RH;
9. Zaključak.

U uvodnom poglavlju navodi se cilj i svrha diplomskog rada te se prikazuje osnovna struktura rada. Drugo poglavlje diplomskog rada, pod naslovom Osnove informacijsko-komunikacijskih sustava, navodi osnovne definicije. U trećem poglavlju, Sigurnosni aspekt primjene informacijsko-komunikacijskih sustava, navode i objašnjavaju se sigurnosni aspekti, koji nikako ne smiju biti narušeni. Četvrto poglavlje prikazuje važnost sigurnosne politike i proces provedbe u određenim institucijama. U poglavlju Sigurnosne prijetnje bankarskom informacijsko-komunikacijskom sustavu navode se moguće ugroze bankarskih IK sustava. U šestom poglavlju, diplomskog rada, navedeni i objašnjeni su slojevi za unaprjeđenje sigurnosnih aspekata. Sedmo poglavlje, preporuke i smjernice pri projektiranju informacijsko-komunikacijskih sustava u bankarskim institucijama, prikazuje najvažnije smjernice prilikom projektiranja IK sustava u bankarskim institucijama. U pretposljednjem poglavlju prije zaključka, prikazani su rezultati provedene ankete pod naslovom „Istraživanje percepcije sigurnosti primjene IK tehnologija pri korištenju bankarskih usluga u RH“. U zaključku je iznesen osvrt na prethodno napisano kao i mišljenje o rezultatima ankete.

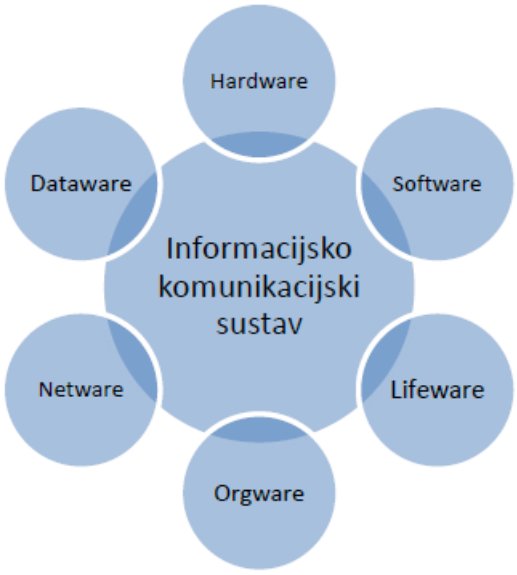
2 OSNOVE INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA

Kako bi se uopće počelo govoriti o informacijskom sustavu, sigurnosnim aspektima te mjerama zaštite o kojima će poglavito biti riječ potrebno je prvo definirati osnovne pojmove.

2.1 Osnovni pojmovi

Informacijski sustav dio je svakog poslovnog sustava, a njegova uloga je konstanta opskrba potrebnim informacijama na svim razinama upravljanja, odlučivanja i svakodnevnog poslovanja. Svako poduzeće ima određenu djelatnost kojom se bavi pa će tako i izgradnja informacijskog sustava za svako poduzeće biti različita [1].

Svaki informacijski sustav sastoji se od šest elemenata (slika 1.)



Slika 1. Grafički prikaz elemenata informacijskog sustava, [2]

Informacijski sustav sastoji se od šest elemenata, odnosno komponenti koje se nadopunjuju i čine jedan kompaktni informacijski sustav. Elementi će biti pojašnjeni u nastavku [2]:

- **Tehnička komponenta (eng. *Hardware*)** predstavlja sklopovski element informacijsko komunikacijskog (IK) sustava, odnosno sve materijalne komponente zadužene za aktivnosti ulaza, obrade, pohrane i izlaza, što između ostalog uključuje i:

  - računala;
  - računalne komponente (procesor, radna memorija, čvrsti disk, itd.);
  - računalnu ulazno - izlaznu opremu (miševi, tipkovnice, monitori, pisači, skeneri, itd.).

- **Programska komponenta (eng. *Software*)** predstavlja nematerijalni element IK sustava u obliku programskih rješenja i operativnih sustava koji se izvršavaju povrh hardverskog elementa.
- **Ljudska komponenta (eng. *Lifeware*)** obuhvaća sve osobe koji su ne određeni način povezane s IK sustavom kao što su projektanti sustava, dizajneri, administratori i krajnji korisnici sustava.

- **Organizacijska komponenta (eng. *Orgware*)** podrazumijeva organizacijske metode, postupke, procedure i procese temeljem kojih se svi elementi IK sustava povezuju u jedinstvenu, svrsishodnu cjelinu.

- **Podatkovna komponenta (eng. *Dataware*)** – element IK sustava koji obuhvaća sve podatke koji se prikupljaju, pohranjuju, obrađuju i razmjenjuju unutar organizacijske strukture IK sustava ili s okolinom.

- **Mrežna / prijenosna komponenta (eng. *Netware*)** predstavlja komunikacijski element IK sustava, a obuhvaća aktivnu i pasivnu mrežnu opremu i komponente čiji je cilj omogućiti komunikaciju između uređaja. *Netware* element obuhvaća sljedeće:

  - računalna mrežna oprema (modemi, mrežne kartice, itd.);
  - usmjerivači (eng. *Router);*

- preklopnici (eng. *Switch*);
- obnavljači (eng. *Repeater*);
- koncentratori (eng. *Hub).*

2.2 Pojam sigurnosti

Sigurnost se može definirati kao proces održavanja prihvatljivog nivoa rizika. To znači da sigurnost nije konačni proizvod ili završno stanje, već proces. Kada je riječ o zaštiti informacijskih sustava i sigurnosti tada postoji nekoliko osnovnih pravila koja i danas važe kao osnovni postulati [3]:

- uz postojanje različitih tehničkih zaštita potrebno je razmotriti i ljudski faktor sa svim svojim slabostima;
- potrebno je naglasiti da apsolutna sigurnost ne postoji;
- sigurnost je proces, skup usluga, proizvoda ili procedura te raznih drugih elemenata i mjera koje se konstantno provode.

Kako bi se omogućilo normalno poslovanje organizacije potrebno je prikladno zaštititi informacije koje se smatraju imovinom svake organizacije. Zahtjev za zaštitom informacija sve je važniji jer u okruženju distribuiranosti poslovne okoline informacije postaju izložene ranjivosti i većem broju prijetnji. Bez obzira u kojem se obliku informacija nalazila vrlo je važno prikladno je zaštititi. Informacije mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektroničkim putem i sl.

Bilo koja od tih oblika informacija u današnje vrijeme predstavlja najvažniji i najskuplji resurs u poslovanju. Upravo tajnost informacija, ispravnost i pravovremeno posjedovanje daju organizaciji moć k napretku.

2.3 Informacijska sigurnost

Informacijska sigurnost je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja. Cilj informacijske sigurnosti svakako je zaštititi informacije od velikog broja prijetnji u svrhu smanjenja poslovnih rizika, osiguranja poslovnog kontinuiteta te u konačnici povećanja broja poslovnih prilika i povrat od investicija. Bitno je naglasiti kako se informacijska sigurnost postiže primjenom raznih kontrola kao što je sigurnosna politika, razni procesi i procedure. Informacijska sigurnost je važna u današnjem poslovanju, upravo zato su informacije, pripadni procesi, sustavi i mreže vrlo važan dio poslovne imovine [3].

Kako bi se osigurao poslovni ugled, zadovoljile zakonske norme i osigurao dotok novca, profitabilnost i ostvarila te zadržala konkurentnost od presudne važnosti može biti: definiranje, implementacija, održavanje i poboljšanje informacijske sigurnosti. Postoje brojne sigurnosne prijetnje s kojim se organizacije suočavaju poput: računalnih prijevara, špijunaža, sabotaža, vandalizma, požara, poplava i slično. Sve prisutnije su štete nanesene organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge. Informacijska sigurnost je od jednake važnosti kako za javna tako i za privatna poduzeća. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Kako bi se pravilno vršilo upravljanje informacijskom sigurnošću zahtjeva potrebno je sudjelovanje svih zaposlenika organizacije, a često je potrebna i pomoć konzultanta izvan granica organizacije.

Prema OECD (OECD - *The Organization for Economic Cooperation and Development*) ustanovljeno je devet principa sigurnosti informacijskog sustava (IS), a oni su [4]:

- **Svijest o informacijskoj sigurnosti** - Važno je biti svjestan potrebe za sigurnošću informacijskih sustava i zaštitnim sigurnosnim mjerama;
- **Odgovornost** - Svi članovi organizacije su odgovorni za sigurnost informacijskih sustava;
- **Odziv** - Svi članovi organizacije trebaju pravovremeno i kooperativno sudjelovati u sprječavanju, detekciji i rješavanju sigurnosnih incidenata;
- **Etika** - Svi članovi organizacije trebaju korektno postupati prema ostalim članovima;
- **Demokracija** - Sigurnost informacijskih sustava treba biti regulirana sa pravilima demokratskog društva;
- **Procjena rizika** - Nužno je provoditi razne procjene rizika kako bi se osigurala adekvatna zaštita;
- **Dizajn i implementacija sigurnosnih mjera** – Sigurnosne kontrole trebaju biti sastavni dio informacijskih sustava u cilj opće sigurnosti sustava;
- **Upravljanje sigurnošću** - Organizacija treba uspostaviti efikasan i jednoznačan pristup upravljanju sigurnošću;
- **Procjenjivanje** - Organizacija treba redovito nadzirati sustav informacijske sigurnosti i izvoditi potrebno modifikacije sigurnosnih politika, mjera, procedura i sl.

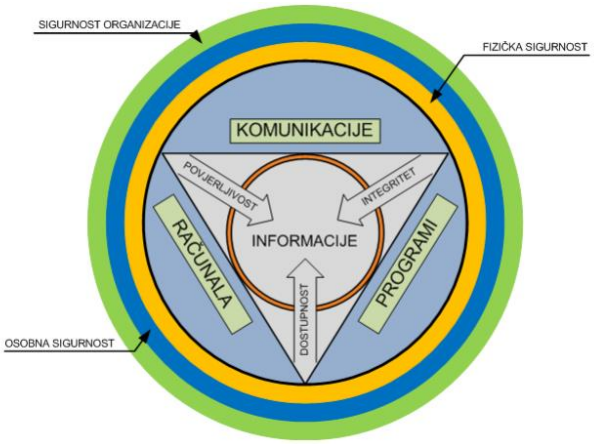
3 SIGURNOSNI ASPEKTI PRIMJENE INFORMACIJSKO – KOMUNIKACIJSKIH SUSTAVA

Sigurnosni aspekti definiraju osnovna načela potrebna za uspostavu sigurnosti informacijskog sustava. Cilj zaštite svakog informacijsko komunikacijskog sustava podrazumijeva očuvanje tri osnovna načela informacijske sigurnosti, povjerljivost (eng. *Confidentiality*), cjelovitost (eng. *Integrity*) i dostupnost (eng. *Availability*). Osnovna načela informacijske sigurnosti obuhvaćena su terminom CIA[1] model.

3.1 Načela sigurnosti informacijskog sustava

Kao što je napisano, načela i ciljevi sigurnosti informacijskih sustava sastoje se od tri osnovna načela. Ta načela su prikazana slikom 2.:

- Povjerljivost (engl. *Confidentiality*);
- Cjelovitost (engl. *Integrity*);
- Dostupnost (engl. *Availability*).



Slika 2. Prikaz načela informacijske sigurnosti, [4]

[1] CIA (eng. *Confidentiality Integrity Aviability)* – kratica koja označava povjerljivost, cjelovitost i dostupnost.

Načela informacijske sigurnosti detaljnije će se razraditi u nastavku diplomskog rada.

3.1.1 Povjerljivost

Povjerljivost (eng. *Confidentiality*) je zaštita podataka koje sadrži sustav od neovlaštenog pristupa. Iako je opće mišljenje da je ovaj tip zaštite od najveće važnosti za državne institucije i vojsku jer svoje planove i mogućnosti moraju čuvati tajno od mogućih neprijatelja, ono također može biti značajno za kompanije koje imaju potrebu zaštititi poslovne planove i informacijske vrijednosti od konkurencije ili kako bi zaštitili podatke od neovlaštenog pristupa.

Problemima privatnosti, koji u zadnjih par godina privlače sve više interesa, posvećuje se sve više pažnje, kako u državnim institucijama tako i u privatnom sektoru. Ključni aspekt povjerljivosti je identifikacija korisnika i provjera autentičnosti. Identifikacija je proces prijave korisnika na sustav, pri čemu sustav zna da takav korisnik postoji.

Na primjer, korisnik A želi se prijaviti na sustav. Sustav provjeri da li je korisnik A prijavljen na sustav i ako je tada slijedi proces provjere autentičnosti. Provjera autentičnosti je proces kojim sustav želi biti siguran da je korisnik koji se prijavljuje pod imenom A upravo osoba A. Postoji više načina provjere autentičnosti. Najrašireniji je unos lozinke, ali se i sve više razvija tehnika oprema koja jedinstvene ljudske osobine, poput otiska prsta ili mrežnice oka pretvara u digitalne signale. Na primjer, kako bi sustav provjerio da li je korisnik koji se pokušava prijaviti kao osoba A upravo ta osoba, može pri prijavi tražiti od korisnika A određenu lozinku koju zna samo osoba A. Ako korisnik A pošalje upravo tu lozinku, sustav zna da je korisnik upravo osoba A. U suprotnom, korisnik nije osoba A te mu sustav ne dozvoljava korištenje sustava. Povjerljivost može biti narušena na nekoliko načina. Navedene su najčešće prijetnje povjerljivosti [5]:

- hakeri - hakeri su osobe koje koriste sigurnosne slabosti sustava na način da neovlašteno koriste sustav ili ga onesposobe;

- lažno predstavljanje – korištenje povjerljivih informacija pomoću lozinke drugog korisnika;
- neovlaštena aktivnost – korištenje podataka za osoba nema ovlasti;
- zlonamjerni programi – programi za neovlašten pristup sustavu.

3.1.2 Integritet

Očuvanje integriteta podataka znači da korisnik podatke ne može izmijeniti bez odobrenja, tj. da su podaci potpuni i ispravni. Od velike je važnosti zaštititi povjerljive podatke od neovlaštenih izmjena, jer se u velikim sustavima često mogu dogoditi namjerni ili nenamjerni slučajevi narušavanja integriteta podataka [4].

Očuvanjem integriteta podataka osigurava se točnost i ispravnost tih podataka, npr. podataka o građanima, platnim listama, itd. Kako bi se očuvao integritet podataka u velikim sustavima, važno je utvrditi identitet korisnika nekom vrstom autentikacije (npr. jednokratnim lozinkama, pametnim karticama, biometrijskim čitačima, itd.). Također, pri rukovanju podacima potrebno je obratiti oprez kako se ne bi dogodile slučajne izmjene u povjerljivim podacima. Međutim, oprez često nije dovoljan, stoga je potrebno kod rukovanja povjerljivim podacima osigurati strogo povjerljivu okolinu koja umanjuje mogućnost namjernih i nenamjernih izmjena.

3.1.3 Dostupnost

Kako bi informacijski sustav služio svojoj svrsi, sadržane informacije moraju u svakom trenutku biti dostupne. Dostupnost se može definirati kao garancija ovlaštenim korisnicima da će im informacijski sustav biti na raspolaganju kada ga imaju potrebu koristiti. Kako bi informacijski sustav bio dostupan u svakom trenutku podrazumijeva se ispravan rad:

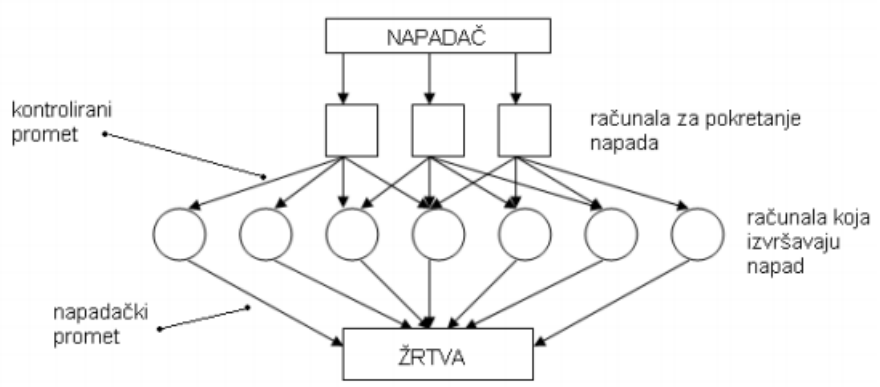
- sustava za pohranu i obradu informacija;
- zaštitnog sustava;

- komunikacijskih veza putem kojih se pristupa informacijama.

Dostupnost informacija najčešće je upitna zbog:

- DoS napada (eng. *Denial of Service attack*);
- gubitka mogućnosti obrade podataka.

DoS[2] napad (slika 3.), tj. napad uskraćivanjem usluge je svaki napad kojem je cilj onemogućiti korištenje poslužitelja ovlaštenim korisnicima. Jedan od načina DoS napada je da napadač pokušava onesposobiti informacijski sustav na način da s velikog broja računala informacijskom sustavu šalje veliki broj zahtjeva, što onemogućava informacijski sustav da radi ispravno i ovlaštenim korisnicima onemogućava pristup podacima.



Slika 3. Primjer DoS napada, [5]

Napadač putem Interneta uspostavlja izravnu vezu s računalima za pokretanje napada i preuzima ovlasti nad njima. Nakon preuzimanja računala za pokretanje napada, napadač uspostavlja izravnu vezu s računalima koja izvršavaju napad i također preuzima ovlasti nad njima.

Napadač putem računala za izvršavanje napada poslužitelju šalje velik broj zahtjeva tj. veliku količinu podataka, koje poslužitelj ne može obraditi u odgovarajućem vremenskom periodu. Pošto poslužitelj ne može obraditi sve zahtjeve

[2] DoS (*eng. Denail of Service*) – koriste se s ciljem sprječavanja legitimnih korisnika u pristupu IK usluga.

i ne može znati koje je od računala napadač zato što velika količina nelegitimnih zahtjeva iskorištava cjelokupni kapacitet obrade podataka koji poslužitelj ima na raspolaganju to je razlog zašto dolazi do odbijanja legitimnih zahtjeva.

Sigurnosne mjere kojima se osigurava dostupnost su [4]:

- fizičke mjere - kojima se uspostavlja provjera pristupa, tj. sprječava se pristup neovlaštenih osoba sklopovlju informacijskog sustava, te drugim sustavima koji kao posljedicu mogu imati nedozvoljenu promjenu u radnom okruženju;
- tehničke mjere - kojima se osigurava ispravnost rada cijelog informacijskog sustava. Primjerice, tehnička mjera je zrcaljenje tvrdih diskova čime se osigurava više kopija istih podataka. Ako se dogodi da se jedan od tvrdih diskova pokvari, drugi, identični će preuzeti njegovo mjesto. Također, tehnička mjera je i stalna provjera ispravnosti rada programa, te izrada sigurnosnih kopija u slučaju prestanka napajanja električnom energijom;
- administrativne mjere - podrazumijevaju uspostavljanje provjere pristupa, provjere izvršavanja procedura i edukaciju korisnika (koja se pokazuje sve važnijom radi ispravnog korištenja informacija dostupnih u sustavu).

3.2 Čimbenici informacijske sigurnosti

Svaki informacijski sustav oslanja se na rad informacijsko komunikacijskog sustava, stoga je bitno postići njegovu optimalnu djelotvornost. Djelotvornost sustava u ovisnosti je o učinkovitosti svih njegovih elemenata. Svaki pristup projektiranju i izgradnji informacijsko komunikacijskom sustavu zasniva se na zadovoljenju funkcionalnosti i ekonomičnosti svakog pojedinog elementa i sustava kao cjeline. Svaki od elemenata posjeduje određene ranjivosti koje mogu biti iskorištene u svrhu narušavanja njegove sigurnosti čime se paralelno narušava i sigurnost informacija koje se pohranjuju [2].

Prijetnja (eng. *Threat*) predstavlja okolnost ili pojavu koja ima potencijal uzrokovati štetu ili gubitak. Prijetnja se sastoji od potencijalne aktivnosti ili pojave koja

može negativno utjecati na osnovna načela informacijske sigurnosti. Prijetnje se ne javljaju samostalno već moraju sadržavati uzroke. Uzorci prijetnje (engl. *Threat agents*) mogu biti predstavljeni ljudskim faktorom ili prirodnom pojavom ili nesretnim događajem.

Ranjivost (eng. *Vulnerability*) je vjerojatnost da prijetnja postane realnost, odnosno slabosti sustava koje mogu biti iskorištene u svrhu uzrokovanja gubitka informacija ili nanošenja štete sustavu. Ranjivosti mogu biti različite, kao i način njihovog iskorištavanja. To je stanje, nedostatak ili slabost u sigurnosnim procedurama, tehničkim kontrolama, fizičkim i drugim kontrolama sustava, dizajnu i implementaciji tih kontrola i procedura koje je moguće iskoristiti. Slučajno ili namjerno iskorištavanje može prouzrokovati operativne i financijske gubitke sustavu.

Imovina (eng. *Asset*) svaki opipljiv i neopipljiv objekt ili karakteristika koja sadrži vrijednost za organizaciju. Primjeri imovine predstavljaju uređaji, postrojenja, patenti, softver, financijski dokumenti, usluge, informacije, ljudski resursi te karakteristike poput reputacije, vještine i znanja. Imovinu organizacije nemoguće je zamijeniti bez značajnih ulaganja resursa (financije, vrijeme, radna snaga ili drugih resursa) [2]. Primjeri elemenata koji predstavljaju imovinu prikazani su tablicom 1.

Tablica 1. Primjeri elemenata koji predstavljaju/ne predstavljaju imovinu organizacije

Naziv objekta	Opis	Primjer	Ključna imovina
Informacija	Podaci prikupljeni, klasificirani, organizirani i pohranjeni u različitim oblicima	Baza podataka klijenata, zaposlenika, proizvodnje, prodaje, marketinga i financija	DA: izrazito kompleksno nadomjestiti
Programski alati	Softver koji služi kao podrška poslovnim procesima organizacije	Prilagođene aplikacije za transakcije narudžbi, generička aplikacija za uređivanje teksta	DA: jedinstvene i prilagođene za organizaciju NE: generičke (*of-the-shelf*)
Operativni sustav	Softver koji pruža temelje za programske alate	Operativni sustav (Windows, Linux, BSD, UNIX)	NE: moguće ga je jednostavno nadomjestiti
Fizički objekti	Računalna oprema, komunikacijska oprema, mediji za pohranu, namještaj, …	Poslužitelji, usmjernici, DVD mediji, napajanja	NE: moguće ih je jednostavno nadomjestiti
Usluge/Servisi	Usluga *outsourcing* računalstva	Glasovna i podatkovna komunikacija	NE: moguće ih je jednostavno nadomjestiti

izvor: [2]

Rizik *(*eng. *Risk)* – vjerojatnost ostvarenja svjesnog, neželjenog događaja. Najčešće se može očitovati u prijenosu raznih povjerljivih informacija. Za važnije informacijske sustave rizik je bitno pravovremeno utvrditi kako bi se njime dalo upravljati te minimizirati ga koliko je moguće.

Utjecaj (eng. *impact)* se odnosi na ostvarenje nepovoljnog događaja. Rezultat je pojave sigurnosnog propusta odnosno iskorištavanje ranjivosti te predstavlja neuspjeh očuvanja povjerljivosti, dostupnosti i integriteta sustava. Prijetnja može biti realizirana putem jednog ili više utjecaja i može postojati i nakon realizacije jer se uzrok prijetnje može realizirati više puta. Poput prijetnje i utjecaj može ostati nepoznat. Takvi utjecaji mogu biti otkriveni nakon određenog vremena ili nikada.

Posljedica (eng. *consequence*) predstavlja rezultat utjecaja, odnosno predstavlja štetu sustava uzrokovanu sigurnosnim incidentom. Šteta se može očitovati u prekidu poslovanja, financijskim gubitcima, gubitkom reputacije, razotkrivanjem privatnih podataka, itd. Postoji mogućnost pojave utjecaja koji ne narušavaju osnovna načela sigurnosti, primjerice virus koji inficira informacijski sustav bez uzrokovanja štete [2].

4 SIGURNOSNA POLITIKA

Učestalost napada na informacijske sustave tvrtki i institucija koji sadrže povjerljive i/ili osjetljive podatke (npr. osobni podaci korisnika, korisnička imena i lozinke, povjerljivi dokumenti, itd.), pokazala je potrebu za propisivanjem pravila kojima će se zaštititi materijalne i intelektualne vrijednosti neke organizacije. Jasno je da napade nije moguće predvidjeti, a ponekad niti spriječiti, ali moguće je poduzeti sve mjere opreza kako bi se šteta koju je napad prouzročio smanjila na najmanju moguću razinu [4].

4.1 Sigurnosna politika

Skup jasno definiranih pravila koja obuhvaćaju sva područja na kojima je moguće izvršiti neku vrstu napada naziva se sigurnosnom politikom.

Sigurnosnom politikom jasno se određuju pravila ponašanja i odgovornosti vezane uz informacijski sustav kako bi se minimizirala šteta nastala namjernim ili nenamjernim djelovanjem. Sigurnosnu politiku predstavlja službena izjava ili plan organizacije koji obuhvaća ciljeve, smjernice i prihvatljive postupke. Ona uključuje sljedeće zahtjeve [6]:

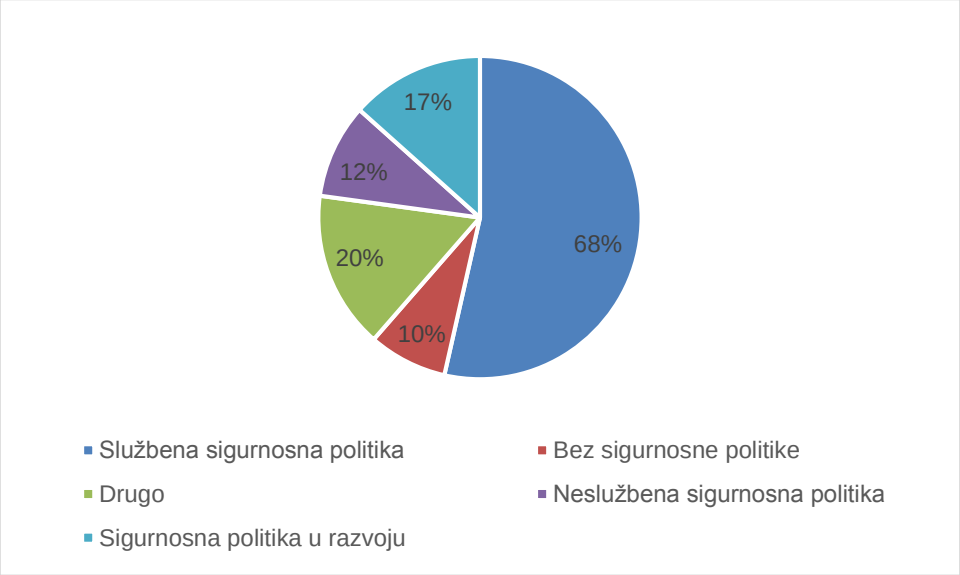
- potrebno je poštovati pravila definirana sigurnosnom politikom;
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija;
- potrebno je usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike;
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima i smjernicama.

Zaštita različitim alatima i tehnologijama u informacijskim sustavima često nije dovoljna kako bi se zaštitili povjerljivi i osjetljivi podaci. Sigurnosti informacijskih sustava pridonosi ispravna uporaba svih dijelova informacijskog sustava i poštivanje pravila propisanih sigurnosnom politikom organizacije. Sigurnosnom politikom

propisuju se dozvoljene i nedozvoljene radnje kako bi se osigurala postojanost računalne opreme,programa i podataka koje informacijski sustav sadrži.

Uspostavom sigurnosne politike korisnicima su nametnuta obvezujuća pravila ponašanja koja ograničavaju slobodu pri pregledavanju povjerljivih informacija, te pravila za ispravno korištenje računalne opreme koja je korisniku dana na korištenje.

Uvođenjem i provođenjem sigurnosne politike tvrtka smanjuje mogućnost gubitka podataka što u velikoj mjeri utječe na učinkovito poslovanje. Međutim, nije u pitanju samo gubitak podataka, već i vremena te novaca. Uništavanjem, kopiranjem ili mijenjanjem povjerljivih podataka, tvrtka može izgubiti poziciju na tržištu. Postotak ustanova sa sigurnosnom politikom prikazan je grafikonom 1.



Grafikon 1. Prikaz postotka ustanova koje imaju uvedenu sigurnosnu politiku
izvor: [6]

Osim osnovnih pravila, moguće je definirati i dodatna pravila koje kontrolira sustav [5]:

- **Zaporke generirane od sustava** – zahtjeva od korisnika korištenje slučajno generirane zaporke. Sustav generira zaporku koju je u pravilu nemoguće pogoditi. Budući da je tako generirana zaporka i teško pamtljiva, korisnik je primoran zaporku zapisati što je velika mana ovog pravila;
- **Minimalna duljina zaporke** – općenito su dulje zaporke bolje od kratkih, ne samo što ih je teže pogoditi već i stoga što je potrebno puno više vremena za njihovo probijanje;
- **Vijek trajanja zaporke** – kako bi se otežala mogućnost pogađanja, a ujedno i probijanja lozinke mnogi računalni sustavi zahtijevaju periodičko mijenjanje zaporki korisnika. Korisnik je dužan svako određeno vrijeme promijeniti zaporku, a ako to ne učini, zaporka prestaje vrijediti;
- **Zaključavanje zaporki** – administratori informacijskih sustava mogu koristiti zaključavanje zaporki pojedinih korisnika kako bi se ograničilo pristup sustavu ako korisnik ne može koristiti sustav određeno vrijeme ih nakon radnog vremena;
- **Pametne kartice** – neki sustavi zahtijevaju pristup pametnih kartica i upisa osobnog identifikacijskog broja, prije nego se dozvoli daljnji pristup provjeri zaporke.

4.2 Sigurnosni standardi

Pri uspostavi sigurnosne politike organizacije primjenjuju se određeni standardi vezani uz sigurnost informacijskih sustava. Uspostava sigurnosne politike prema raspoloživim standardima osigurava pridavanje pažnje svim aspektima zaštite nekog informacijskog sustava te dokazuje kvalitetu uspostavljenih mjera sigurnosti. Mjerodavne institucije za izdavanje ovakvih standarda u području zaštite informacijskih sustava su ISO (*International Organization for Standardization*) i IEC (*International Electrotechnical Commission*). Standardi iz ISO/IEC 27000 serije

organizacijama pružaju smjernice za konstruiranje, primjenu i provjeru informacijskih sustava čime se osigurava povjerljivost, integritet i dostupnost informacijskog sadržaja, sustava i procesa unutar organizacije. Za područje sigurnosti informacijskih sustava najčešće se koriste dva standarda [4]:

- ISO/IEC 27001;
- ISO/IEC 27002 (prije 2007. godine poznat kao ISO/IEC 17799:2005). Pri izradi sigurnosne politike preporučuje se upotreba oba standarda.

4.3 Opis procesa uspostave sigurnosne politike

Organizacija može svoju sigurnosnu politiku temeljiti na unaprijed izrađenim standardima, čime se uvelike smanjuju operativni troškovi i vrijeme potrebno za provedbu sigurnosne politike. Također, sigurnosnu politiku organizacije moguće je izraditi samostalno, procjenom mogućih prijetnji informacijskom sustavu, te procjenom i zaštitom slabih točki sustava. Ovaj je proces dakako dugotrajniji i skuplji, ali osigurava način zaštite koji potpuno odgovaraju potrebama organizacije. Iako se na prvi pogled samostalna izrada sigurnosne politike čini kao bolje rješenje, preporučuje se izrada sigurnosne politike organizacije na temelju standarda kako bi se pri uspostavi sigurnosne politike obratila pažnja na sve moguće prijetnje koje mogu ugroziti informacijski sustav. Kao što je u prethodnom poglavlju naznačeno, sigurnosna politika organizacije može se temeljiti na ISO/IEC 27001 standardu. Međutim, potrebno je spomenuti da ISO/IEC 27001 standard opisuje sve što je potrebno napraviti, ali ne i kako je potrebno napraviti. Da bi se odgovorilo na pitanje kako se koristi standard ISO/IEC 27002 (koji daje potrebne smjernice), razrađen je upravo primjer sigurnosne politike na temelju tog standarda. Neki od glavnih postupaka u kreiranju sigurnosne politike su [4]:

- Procjena rizika;
- Sigurnosna politika – Dokument sigurnosne politike;
- Organizacija informacijske sigurnosti;
- Upravljanje imovinom;
- Zaštita od zaposlenika;

- Fizička zaštita i zaštita od okoline;
- Upravljanje komunikacijama i operacijama;
- Provjera pristupa;
- Razvoj i održavanje sustava;
- Upravljanje incidentima u informacijskom sustavu;
- Upravljanje poslovnim kontinuitetom;
- Usklađivanje.

5 SIGURNOSNE PRIJETNJE BANKARSKOM INFORMACIJSKO – KOMUNIKACIJSKOM SUSTAVU

Bankarski sustavi vrlo često su izloženi raznim prijetnjama. Prijetnja može prouzročiti niz neželjenih situacija odnosno šteta koje mogu biti materijalne ili nematerijalne.

5.1 Vrste prijetnji

Svakodnevno su bankarski sustavi izloženi raznim vrstama prijetnji. Istraživanja pokazuju kako je najčešća vrsta prijetnje upravo ljudski faktor te bi se njemu trebala pridonijeti najveća pažnja. Raznim analizama i spoznajama prijetnji moguće je uvelike dobro izraditi i primijeniti načine zaštite od poznatih potencijalnih prijetnji. Ostale vrste prijetnji koje mogu biti namjerne ili nenamjerne prikazane su u tablici 2.

Tablica 2. Vrste prijetnji prema njihovom izvoru

	Pogreška	**Slučajno**	**Namjerno**
Interni	Ljudska	Od strane zaposlenika. Posljedica loših podataka. Uništavanja podataka od strane zaposlenika. Administrativne pogreške.	Od strane zaposlenika. Uništenje podataka od strane zaposlenika. Loše upravljanje podacima.
	Ne ljudska	Problem sa strujom. Programski problemi.	Problemi sa strujom. Programski problemi.
Eksterni	Ljudska	Konkurencija.	Hakeri. DoS napad. Socijalni inženjering.
	Ne ljudska	Vatra. Zemlja. Hladnoća. Voda.	Virusi. Crvi. Trojanci.

izvor: [7]

5.2 Metode napada

Metode napada jedna su od važnijih komponenti u samom opisu nekog informacijskog sustava. U pravilu napadi su inicirani od hakera čije su akcije usmjerene na ugrožavanje sigurnosti informacija. Razlikuju se četiri vrste napada koje će biti kratko i pojašnjene u nastavku.

5.2.1 Metoda napada prekidanjem

Metoda napada prekidanjem (eng. *interruption*), slika 4., predstavlja napada na raspoloživost (eng. *availability*), presijecanjem se prekida tok informacija, onemogućava se pružanje neke usluge ili funkcioniranje nekog sustava [8].

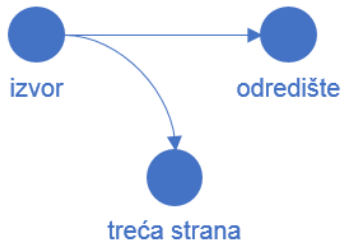
Slika 4. Prekidanje usluge između korisnika
izvor: [9]

Nakon napadačevog pristupa samoj korisničkoj mreži, može učiniti razne štetne kao npr. prikriti neke informacije, slanje nekih nevažećih podataka, opterećenje prometa što bi dovodilo do gašenja računala ili same mreže, blokiranje prometa, itd. [10].

5.2.2 Metoda napada presretanjem

Metoda napada presretanjem (eng. *interception*), slika 5., je metoda koje se događaju posredstvom neke treće strane u komunikaciji. Predstavlja napad na povjerljivost. U praksi može biti provedeno kao prisluškivanje prometa, nadziranje

njegovog intenziteta, uvid u neke osjetljive informacije, snimanje mrežnog prometa itd.

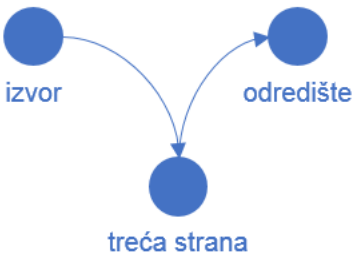


Slika 5. Presretanje od treće strane
izvor: [9]

Ovakve vrste napada posebno je teško izbjeći pri bežičnim komunikacijama, te u komunikaciji koja uključuje višeodredišno (eng. *broadcast*) ili grupno (eng. *multicast*) razašiljanje [11].

5.2.3 Metoda napada izmjenom podataka

Izmjena podataka (eng. *modification*), slika 6., predstavlja napad na integritet. Po svojoj prirodi to je aktivan napad. Ako djeluje na prijenosnom putu može uvelike napraviti štetu po treću stranu, npr. napadač se služi tom metodom napada kako bih izmijenio informacije između pošiljatelja i primatelja poruke.

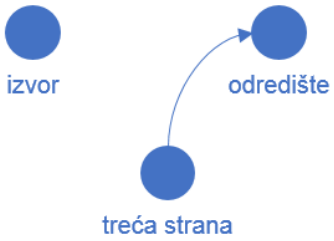


Slika 6. Napad izmjenom podataka
izvor: [9]

Ova vrsta je jedna od najštetnijih metoda napada jer se izmjenjuje sadržaj poruke, koja bi u bankarskom sustavu predstavljala ogroman problem [8].

5.2.4 Metoda napada proizvodnjom podataka

Metoda napada proizvodnjom (eng. *fabrication*), osmišljena je isključivo za krađu i zlonamjerno iskorištavanje korisničkih podataka. Prikazana je slikom 7.

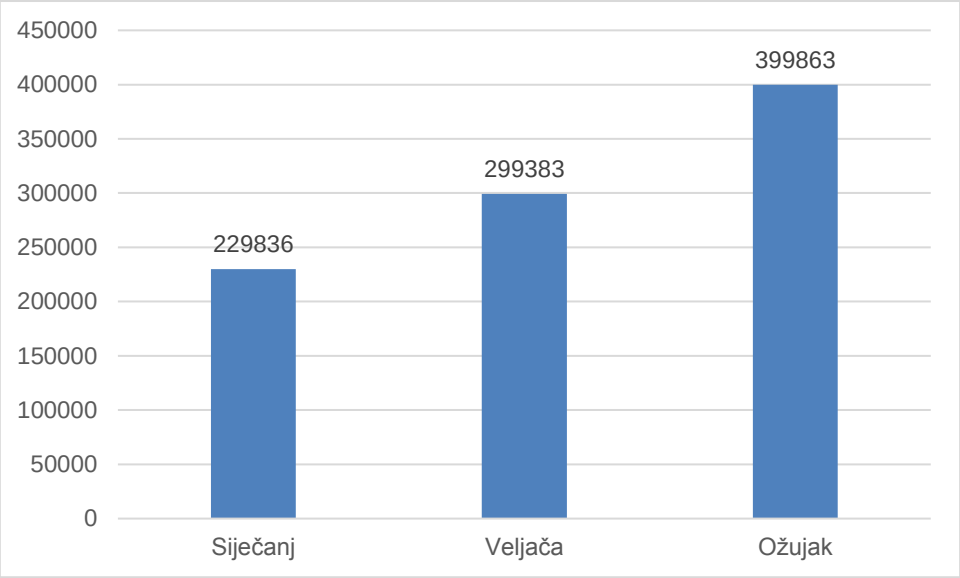


Slika 7. Proizvodnja podataka s ciljem otuđenja podataka
izvor: [9]

Napadač izvodi napad tako što generira lažne podatke, lažni promet ili izdaje neovlaštene komande. Iskorištava slabosti te je u mogućnosti dobiti djelomičnu ili potpunu kontrolu nad sustavom.

5.3 Zloćudni bankarski programi

Zloćudni programi su programi koji napadačima služe kako bi na ilegalan način došli do osjetljivih i važnih korisničkih podataka te ih iskorištavali u neke svoje svrhe. S razvojem tehnologija i mehanizama u posljednjih nekoliko godina bankarski sustavi bilježe sve veći porast napada na informacijske sustave.



Grafikon 2. Prikaz naglog porasta malicioznih programa i prijetnji bankarskim informacijskim sustavima u 2015. godini
izvor: [12]

Na prikazanom grafikonu 2. vidljivo je kako je sve više napada od strane hakera i porast malicioznih programa, kako bi se informacijski sustavi i njihovi korisnici što bolje zaštitili potrebno je znati i detaljno proučiti načine na koje rade. U daljenjem tekstu biti će pojašnjeni neki od najučestalijih malicioznih programa.

5.3.1 Programi za praćenje unosa znakova s tipkovnice (eng. *Keyloggers*)

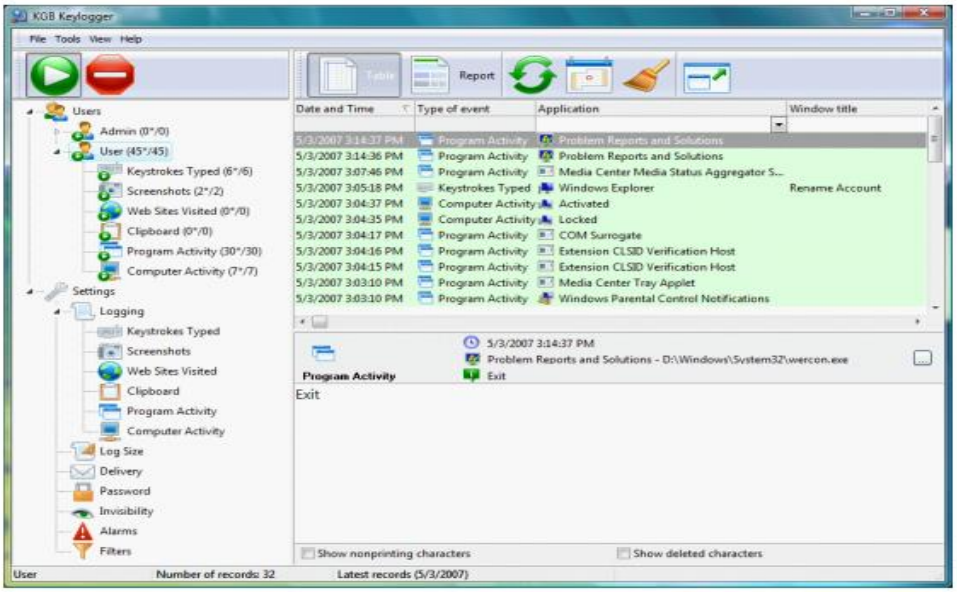
Keyloggeri su špijunski programi koji prate i bilježe svaku tipku koju korisnik pritisne. Dijele se u dvije skupine:

- alati u obliku programskih paketa;
- uređaji koji se ugrađuju u sklopovlje računala.

Programi za praćenje unosa znakova s tipkovnice (primjer na slici 8.) se uključuju u lanac događaja između pritiska tipke na tipkovnici i prikaza znaka na zaslonu računala. To se postiže na više načina [13]:

- postavljanjem video nadzora;

- podmetanjem prislušnog uređaja u tipkovnicu;
- presretanje znakova upotrebom samog računala;
- promjenom upravljačkih programa tipkovnice;
- promjenom programa za obavljanje posebnih funkcija tipkovnice (eng. *filter driver*).



Slika 8. Primjer KGB keylogger programa u izvođenju, [13]

Napadači koriste opisane programe kako bi preuzeli osjetljive informacije kao što su brojevi kreditnih kartica, PIN-ovi (eng. *Personal Identification Number*), korisnički podaci i slično. Programi za praćenje unosa s tipkovnice prikupljaju podatke te ih dostavljaju na posebna računala za spremanje takvih podataka. Jedan od problema ovog programa je da prati isključivo unos znakova s tipkovnice što znači da tu ima ogromna količina informacija koju napadač treba probrati tj. odabrati one najvrjednije PIN, broj kartice i slično a to nije baš jednostavno [13].

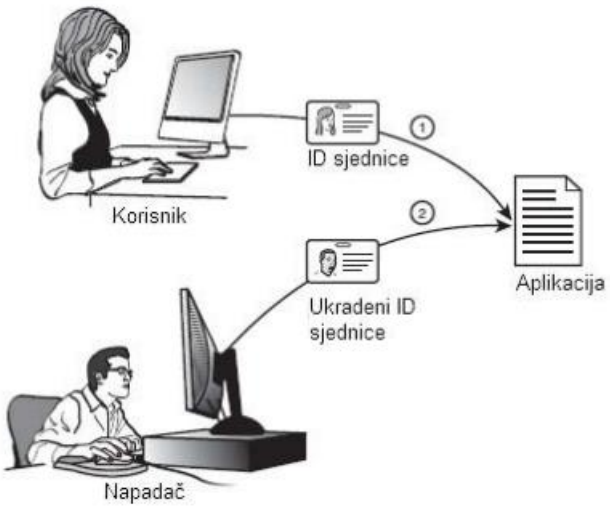
5.3.2 Bankarski trojanski konji

Trojanski konji jedni su od najjednostavnijih i najraširenijih oblika zloćudnih programa. Oni zapravo sadrže neku korisnu funkcionalnost te time privlače korisnika da ih preuzme na svoje računalo i pokrene. Upravo tom akcijom korisnik omogućuje napadaču da pokrene zlonamjerni kod te pristupi određenim podacima na računalu. Jedna od najgorih vrsta su bankarski trojanski konji koji su prvenstveno oblikovani za napada na bankarske sustave, burze dionica i slično.

Jedan od primjera napada na banke je u Švedskoj i Njemačkoj, gdje je trojanski konj *Haxdoor.ki* uzrokovao veliku financijsku štetu. Mnogi bankarski trojanci kradu korisničke podatke, transakcijske brojeve TAN (eng. *Transaction Authentication Number*) ili jednokratne lozinke OTP (eng. *one – time passwords*) i šalju ih poslužiteljima kojima upravljaju napadači [13].

5.3.3 Otimanje sjednica

Trojanski konji osim što se mogu koristiti za krađu korisničkih i autentifikacijskih podataka, mogu se još koristiti i za otimanje autentificiranih sjednica. Ako trojanski konj preuzme administratorske podatke, čak ni višeslojni autentifikacijski sustav neće pružiti zaštitu od upotrebe autentificirane sjednice za pokretanje ili izmjenu transakcija [13]. Primjer je prikazan na slici 9.



Slika 9. Otimanje sjednice, [13]

Prilikom izvođenja napada otimanjem sjednica, zlućudni program može promijeniti sadržaj transakcija. Na primjer, korisnik unosi nalog za prijenos 200 kuna na tekući račun određene osobe. Ako napadač otme sjednicu, on može promijeniti iznos od 200 kuna u 1000 kuna i umjesto te osobe koja treba primiti nova upiše svoje podatke o svome računu ili računu kojim upravlja.

5.3.4 Pharming

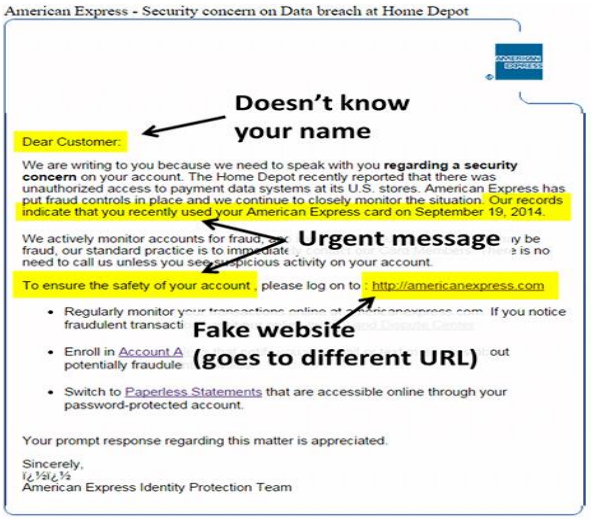
Neki bankarski trojanci preusmjeruju korisnika prilikom prijave na Internet bankarstvo na lažnu web stranicu. Ova metoda napada naziva se pharming. Napadač oblikuje stranicu tako da ona oponaša web stranicu banke. Takva stranica također može služiti za napad s čovjekom u sredini, mijenjajući sadržaj prometa koji se prenosi između bankarske stranice i korisnikovog web preglednika. Postoji puno različitih tehnika pharming napada. Na primjer, trojanski konj može dodati nazive web stranica banke u datoteku s IP adresama koje upućuju na zlonamjernu stranicu [13].

Dobar primjer takvog trojanca je *Ohost.je.* Još jedna tipična metoda je presretanje funkcija iz biblioteke „*wininwt.dll*“ u procesu web preglednika Internet Explorer. Također, neke inačice trojanca *Haxdoor* imaju ovu opciju. Mnogi web preglednici imaju opciju upozoravanja korisnika da web stranica koju posjećuju nema

valjani certifikat. Bankarski trojanski konj koji izvodi pharming napade upotrebom funkcija „wininet.dll“ u pregledniku može zaobići ili potisnuti dijaloške prozore o upozorenjima. Također, trojanski konj koji može mijenjati datoteke na korisničkom računalu, može i instalirati vlastiti certifikat te tako spriječiti pojavu upozorenja [13].

5.3.5 Phishing

Phishing (slika 10.) je vrsta napada koja putem elektroničke pošte upotrebom lažnih poruka s ciljem prevare i navođenjem korisnika na dolazak na lažne web stranice i otkrivanje osjetljivih podataka (broj kartica, imena, lozinke, PIN-ovi i slično).



Slika 10. Primjer phishing napada, [14]

U bankarskom sustavu, uz običan phishing pojavljuje se i „*spear phishing*“. Spear phishing je poseban oblik phishinga u kojem napadač isključivo cilja na zaposlenike unutar pojedinih financijski usmjerenih organizacija i bankarskih poslovnica [14]. U početku procesa *spear phishinga*, napadač prvo prikuplja opće i kontaktne informacije određene banke, kao što su: logo i slogan banke, imena i prezimena izvršnih zaposlenika, adresa banke i slično. Nakon dovoljno prikupljenih informacija napadač kreira email koji šalje pojedinim zaposlenicima, te se najčešće

predstavlja kao mrežni administrator unutar istog bankarskog sustava, odnosno kao njihov kolega [14].

6 DEFINIRANJE SLOJEVA ZA UNAPRIJEĐENJE SIGURNOSNIH ASPEKATA

Računalne mreže čine jedne od važnijih dijelova svakog informacijskog sustava. Za svaku veću organizaciju potrebno je izraditi sigurnosni model. To je model po kojem mora funkcionirati mreža jer je ona prvi kontakt sa informacijama pojedine organizacije. Sigurnosni model mreže računala prikazan je (slikom 11.)

Mrežna sigurnost sastoji se od postavljanja sigurnosnih mjera i politika, koje donosi uprava organizacije. Sigurnost se tiče svih ljudi u organizaciji. Ključ izgradnje sigurne mreže je definiranje značenja sigurnosti za svaku organizaciju. Organizacija sigurnosti po slojevima dobar je način osiguravanja optimalne zaštite mrežnog sustava [15].

Slika 11. Sigurnosni model mreže računala
izvor: [15]

Ukoliko napadač uspješno zlouporabi računalnu mrežu, uz pomoć sigurnosnog modela lakše je pronaći i popraviti problem. Kod analize napada obično se pregledava mreža računala po ISO/OSI slojevima odozdo prema gore. Na isti je način osmišljen i sigurnosni model mreže računala. Posljedice napada analiziraju se od nižih prema višim slojevima. Kada se ustanovi koji je sloj zatajio, odmah se zna da

su i svi slojevi ispod njega zatajili. Nakon toga će stručnjak brzo moći utvrditi koja su sve računala zahvaćena napadom i osigurati ih od ponovnih napada [15].

6.1 Fizički sloj

Fizički sloj definira fizičku sigurnost koja se primjenjuje za sprečavanje neovlaštenog pristupa napadača. U bilo kojem scenariju napada, ako je fizički sloj napadnut, vatrozid neće pomoći u sprječavanju napada. Ako zataji fizički sloj, napadač može neovlašteno pristupiti podacima. Fizička sigurnost uključuje projektiranje sigurnosti ustanove, postavljanje uređaja za kontrolu pristupa, alarma i kamera. Fizički sloj najlakše se osigurava jer ne zahtijeva napredne tehničke koncepte [16].

6.2 VLAN sloj

VLAN (eng. *Virtual Local Area Network*) sloj bavi se stvaranjem i održavanjem virtualnih lokalnih mreža. Osnovni razlog primjene je grupiranje zajedničkih računala iz sigurnosnih razloga. Jedan od primjera je stavljanje jednog odijela na jednu VLAN mrežu, a drugog odijela na drugu VLAN mrežu. Kako odjeli ne razmjenjuju iste podatke poželjno bi bilo da je svaki odjel na zasebnoj VLAN mreži.

Prvi korak u primjeni VLAN mreže je određivanje javnih i privatnih mreža. Bilo koji uređaj kojim se pristupa izvan Intraneta treba biti u javnoj VLAN mreži. Na primjer web poslužitelji, vanjski FTP i DNS poslužitelji. Idući je korak postavljanje uređaja u privatni VLAN koji se može podijeliti na unutarnji korisnički VLAN i unutarnji poslužiteljski VLAN. Posljednji korak u primjeni je podjela unutarnjih korisničkih i poslužiteljskih VLAN mreža po odjelima i grupiranje podataka respektivno [16].

VLAN je ključan sloj za sigurnosni model računalne mreže jer mreža koja nije podijeljena sadrži neorganizirane skupine poslužitelja i uređaja. VLAN mreže su odličan način za pronalaženje ugroženog računala.

Pregledom povećanog prometa koji dolazi s pojedine VLAN mreže, administrator mrežne sigurnosti može smanjiti opseg te lakše identificirati koje je računalo napadnuto [16].

6.3 ACL sloj

ACL (eng. *Access Control List)* sloj definira stvaranje i održavanje popisa koji definiraju kontrolu pristupa. Liste se postavljaju na usmjerivače (eng. *router*) i vatrozide (eng. *firewall*). Postavljene su kako bi se dozvolilo ili zabranilo pristup među računalima na različitim mrežama. To je neophodno u području mrežne sigurnosti.

Kvalitetnom definicijom popisa kontrole pristupa, administrator može spriječiti mnoge napade prije nego što ih napadač i pokuša izvesti. Prilikom postavljanja listi kontrole pristupa u obzir treba uzeti neke od parametara, kao što su povratni promet ili svakodnevni promet. Ukoliko se liste ne naprave kvalitetno, ACL može dozvoliti neovlašteni promet i/ili zabraniti ovlašteni promet [16].

Kod stvaranja listi kontrole pristupa treba jednako razmatrati dolazni kao i odlazni promet. Većina se administratora koncentrira na stvaranje listi kontrole pristupa koje zabranjuju pristup mreži tvrtke s Interneta. Prilikom stvaranja listi kontrole potrebno je usredotočiti se na takve tipove listi koje su primjenjive jednako za odlazni i dolazni promet. Administrator mora znati kojim vratima treba omogućiti pristup izvan Intraneta, kao i u Intranet [16].

6.4 Programski sloj

Programski sloj usredotočen je na programske pakete, njihovo ažuriranje, primjenu zakrpa i ispravljenih inačica u svrhu smanjivanja njihove ranjivosti.

Administratori mrežne sigurnosti moraju biti upoznati s programima koji se nalaze na računalima u mreži i održavati ih u smislu primjene novih i ispravljenih inačica. Također trebaju znati točno što koja zakrpa čini kada se instalira te znati ukloniti neželjene programe [16].

6.5 Korisnički sloj

Korisnički sloj odnosi se na edukaciju zaposlenika i način prijenosa znanja korisnicima o sigurnosti računalnih mreža. Korisnici moraju razumjeti osnovne koncepte mrežne sigurnosti. Također trebaju naučiti koje aplikacije ne smiju pokretati ili instalirati na svojim sustavima. Osim toga, korisnici trebaju imati pojam o tome kako se ponaša njihovo računalo kada radi normalno i kako se ponaša kada to nije slučaj.

Osnovni način primjene korisničke sigurnosti je obrazovanje korisnika o aplikacijama. Korisnik mora znati koje aplikacije treba izbjegavati, kako se njihovo računalo ponaša kada radi normalno i kada to nije slučaj. Na primjer, korisnike treba upozoriti na opasnosti korištenja P2P (eng. *Point to point*) aplikacija gdje datoteke koju preuzimaju mogu sadržavati virus, trojanski konj ili neki drugi program koji može biti poguban za računalo. Od iznimne je važnosti naučiti korisnike kako funkcionira njihov sustav jer ako to znaju, moći će i sami otkriti problem [16].

Ako je korisnički sloj ugrožen, ugrožen i korisnički račun. Napadač uspješnom zlouporabom ranjivosti može preuzeti korisnički račun i tako prouzročiti veliku štetu sustavu. Krađom korisničkog računa, napadač može, ovisno o ovlastima računa, mijenjati, kopirati ili brisati podatke pohranjene ne samo na jednom računalu već i na cijelom sustavu. Korisnički sloj se nalazi iznad administrativnog zbog toga što ako je ugrožen administrativni sloj, ugrožena je i sigurnost korisničkog sloja.

Većina će napadača prvo napasti korisnički sloj jer obični korisnici imaju manje znanja o sustavu, pa će se takvi napadi teže spriječiti [16].

6.6 Administrativni sloj

Administrativni sloj obuhvaća administratora sigurnosti mreže i svih korisnika koji upravljaju mrežom. Sličan je korisničkom sloju, ali podaci kojima se rukuje su na višoj sigurnosnoj razini. Kao i korisnike u korisničkom sloju, administratore mreže računala također treba obrazovati i educirati. Moraju potpuno razumjeti i poznavati sustav kako bi mogli što ranije otkriti probleme.

Ako napadač ugrozi sigurnost administrativnog sloja, može uspješnom zlouporabom ranjivosti preuzeti administrativni korisnički račun. To može imati pogubne posljedice za podatke u sustavu jer će ih napadač moći mijenjati, kopirati i brisati. Osim toga, moći će instalirati i pokretati programe po volji. Posebno je opasno što će moći stvoriti teško vidljive ranjivosti i na nižim slojevima, koje kasnije može uspješno koristiti a da ne bude otkriven.

Administrativni sloj se nalazi prije sloja odjela za sigurnost IT-a. Ako je sedmi sloj (sloj odjela za sigurnost informacijske tehnologije) kompromitiran ujedno je kompromitiran i administrativni sloj [16].

6.7 Sloj odjela za sigurnost IT-a

Sloj u koji su uključeni su svi profesionalci iz područja mrežne sigurnosti, mrežni arhitekti i specijalisti za programsku podršku. To su ljudi koji omogućuju i održavaju rad računalne mreže. Svi članovi ovog sloja imaju administrativne korisničke račune za cijeli sustav, što znači da imaju pristup bilo kojem uređaju i servisu na mreži.

Na primjer, korisnik s takvim ovlastima ima mogućnost čitanja, pisanja i promjene strukture baze podataka, a administrator i korisnici samo ovlasti čitanja, pisanja i promjene sadržaja baze podataka [16].

Najvažnije, ako napadač izvede uspješan napad na sedmi sloj, imat će potpuni pristup svim uređajima u mreži. Dakle moći će upravljati usmjerivačima, vatrozidima, posrednim računalima te VPN mrežom. Spomenuti napad je vrlo poguban jer napadač može potpuno paralizirati i onemogućiti mrežu. Posljedice predstavljaju velike financijske gubitke za tvrtku jer gube potpuno povjerenje klijenata. [16].

7 PREPORUKE, SMJERNICE I MJERE PRI PROJEKTIRANJU I UPRAVLJANJU INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA U BANKAMA S CILJEM SMANJENJA OPERATIVNOG RIZIKA

Projektiranje i izgradnja informacijsko komunikacijskih sustava vrlo je zahtjevan i složen posao. Podrazumijeva analize, oblikovanja, razvoj i implementaciju sustava. Informacijski sustav (IS) predstavlja skup resursa – podataka, metoda, organizacije, tehničkih sredstava za pružanje informacija tako da ih prikuplja, obrađuje i komunicira istim informacijama koje su prijeko potrebne za donošenje odluka i bolje funkcioniranje sustava. Prilikom planiranja IS-a pitanja na koje je, najčešće, potrebno dati odgovor su [17]:

- Čime će se organizacija baviti?
- Koji su problemi, zadaće i ciljevi poslovnog sustava?
- Koja je željena uloga IS-a u postizanju postavljenih ciljeva?
- Koji su raspoloživi resursi?

U svakoj banci jedno do osnovnih načela u poslovanju su načela likvidnosti i solventnosti. Kako bi osigurale poslovanje na razini sa spomenutim načelima, banke su dužne stalno i kontinuirano provoditi mjerenja, procjene i upravljanja koje uključuju rizik od neadekvatnog upravljanja informacijskim tehnologijama. Kao što je i ranije već spomenuto, informacijska tehnologija danas je prisutna u gotovo svim aspektima bankarskog poslovanja. Prema tome potrebno je posvetiti punu pažnju prilikom upravljanja informacijskim sustavima, kako bi se osiguralo pouzdano i sigurno poslovanje [18].

Upravljanje sigurnošću informacijskog sustava predstavlja sveobuhvatan, detaljan proces identificiranja potreba te postizanja zadovoljavajuće razine sigurnosti informacijskog sustava. Upravljanju treba pristupiti ozbiljno zato što bez informacijskog sustava banke ne bi mogle funkcionirati [18].

U nastavku slijedi detaljniji opis smjernica i mjera koje je potrebno ispuniti u cilju zadovoljenja svih korisničkih, ali i vlastitih potreba te smanjenja operativnog rizika [17].

7.1 Organizacija i upravljanje informacijskim sustavom

Funkcioniranje IS-a ovisi o podršci uprave. Uprava banke odgovorna je za organizaciju, strateško odlučivanje, dodjelu resursa i donošenje pravila te procedura u kontekstu upravljanja IS-a [17].

Uprava banke trebala bi odrediti člana uprave koji će nadzirati kontrolu procesa upravljanja. Također uspostaviti organizacijsku strukturu, odgovarajuće funkcije i odbore za upravljanje rizikom. Uprava banke dužna je između ostalog donijeti strategiju IS-a u skladu sa strategijom banke, donijeti interne akte te definirati kriterije i načine izvješćivanja uprave o mogućim pojedinostima. Zatim imenovanje voditelja organizacijske jedinice (strateška pitanja, funkcionalnost, djelotvornost IS-a), voditelja sigurnosti IS-a u cjelini i odbor za upravljanje [18].

7.2 Razvoj i održavanje informacijskog sustava

Jedna od glavnih komponenti kod održavanja informacijskog sustava je upravljanje imovinom. Ono obuhvaća: detektiranje, evidentiranje, raspolaganje, praćenje, planiranje, obnavljanje, zaštitu. Banka treba definirati procese upravljanja promjenama hardverskih, softverskih i drugih komponenti informacijskog sustava banke te praćenja svih promjena [18].

Još jedna bitna stavka je uspostava procesa upravljanja konfiguracijama hardverskih i softverskih komponenti, koji podrazumijeva razne postupke, analize, definiranja, testiranja i praćenja svih osjetljivih podataka komponenti informacijskog sustava. Nadalje, potrebno je definirati postupke izrade, pohrane, održavanja i čuvanja dokumentacije koja se odnosi na informacijski sustav banke te korisnicima zabraniti pristup istoj.

Stalna i kontinuirana naobrazba svih korisnika informacijskog sustava je primarna i neophodna, zato što omogućuje obavljanje zadataka i smanjuje mogućnost pojave neželjenog događaja. Osim navedenog, naobrazba služi korisničkom praćenju promjene trendova u informacijskim sustavima i okolini [18].

7.3 Upravljanje promjenama u informacijskom sustavu

Brzi napredak tehnologije, kao i česte izmjene poslovnih zahtjeva uzrokuju potrebu za promjenom komponenti informacijskog sustava. Osnovni zadatak upravljanja promjenama je osigurati da promjene ne naruše sigurnost i funkcionalnost informacijskog sustava [18].

Promjene u IS-u neizbježan su dio procesa razvoja i održavanja. Kako ne bi došlo do štetnih utjecaja ili kako bi se smanjili rizici preporučljivo je osigurati [17]:

- Odgovorne osobe za upravljanje IT koje su upoznate s planiranim promjenama i potencijalnim rizicima;
- Planirane promjene odobrene samo od strane odgovorne osobe za upravljanje IT prije same njene provedbe;
- Da su korisnici upoznati s promjenama ako utječu na neku od provedbi korisničkih zadataka, primjerice kad se radi o promjenama u poslovnim aplikacijama itd.
- Vođenje evidencije o samim promjenama u IS, što podrazumijeva opise promjena, imena predlagatelja, imena odobravatelja, procijenjene rizike, status odobrenja, testiranja itd.

7.4 Izdvajanje procesa informacijskog sustava

Izdvajanje procesa IS organizacije podrazumijeva uključivanje drugih osoba u obavljanje poslova vezanih uz IS. Neki od takvih poslova mogu biti održavanje

komponenti IT, razvoj aplikacija, neki vid obrade podataka, pružanje usluga uporabe tehničke i sigurnosne infrastrukture itd.

Kako bi se smanjile štete nastale zbog rizika vezane uz vanjske pružatelje usluga preporučuje se [17]:

- Procijeniti rizike izdvajanja procesa – provesti analizu u cilju dobivanja odgovora na koje poslovne procese i resurse utječe izdvajanje, kako bi prekid utjecao na poslovanje, na koji način će se nadzirati pružanje usluge, na koji način osigurati neprekinutost poslovanja itd.
- Procijeniti primjerenost pružatelja usluga – provesti i dokumentirati analizu s ciljem dobivanja odgovora na perspektivu pružatelja u stabilnosti poslovanja, posjedanju referenci, iskustva, znanja itd.
- Definirati i sklopiti ugovor primjeren usluzi – ugovor bi trebao sadržavati najmanje: detaljan opis predmeta ugovora, obveze čuvanja podataka, novčanu vrijednost ugovora, uvjete jednostranog raskida ugovora, trajanje ugovora te način rješavanja sporova.

Usluge *cloud computinga*[3] od velikog su značaja. Prednosti korištenja „*Cloud Computing*“ usluga mogu se manifestirati u vidu ušteda kod nabave informatičke opreme, zapošljavanja stručnih kadrova, troškova održavanja, jednostavnijeg načina rješavanja pitanja planova oporavka nakon katastrofe i drugih.

Upravo zbog takvih osobina uporaba *cloud computinga* nosi sa sobom i neke rizike. Kako bi se smanjili rizici preporučljivo je primjenjivati mjere i postupke kao što je prethodno i napisano u poglavlju uz još primjenu sljedećeg. Bitno je steći uvjerenje da će pružatelj obavljati uslugu u skladu s propisima, poglavito u kontekstu zaštite podataka te steći uvjerenje u primjerenost podržavajuće infrastrukture.

[3] *Cloud Computing* je koncept podjele programskog okruženja koji koristi internet kao platformu, te

.

7.5 Planiranje kontinuiteta poslovanja

Vjerojatnost da prijetnje, usprkos svim primijenjenim zaštitnim mjerama i postupcima, ostvare štetne učinke ili otežaju normalno poslovanje uvijek postoji. Planiranje kontinuiteta u najvećoj mjeri treba osigurati kontinuitet poslovanja što znači kraći oporavak ako dođe do neželjenih situacija. Osiguravanje kontinuiteta postiže se poduzimanjem raznih mjera radi prevencije neželjenih događaja, ograničavanja njihovog učinka i oporavka u slučaju prekida [18].

Zbog velike ovisnosti banke o informacijskoj tehnologiji, prilikom planiranja kontinuiteta banka bi trebala posvetiti posebnu pozornost osiguranju resursa potrebnih za odvijanje vitalnih procesa. Nadalje, banka bi trebala usvojiti plan kontiuniteta poslovanja, plan oporavka i uspostaviti proces upravljanja incidentima. U slučaju težih incidenata obavijestiti i Hrvatsku narodnu banku o incidentu, uzrocima te načinu rješavanja. Također periodično izrađivati i pohranjivati kopije kako bi se osigurala usklađenost navedenih postupaka sa zahtjevima iz plana kontinuiteta te svakih najmanje 18 mjeseci testirati plan poslovanja, oporavka i odgovora na incidente [18].

7.6 Fizička sigurnost

Fizička sigurnost obuhvaća mjere, postupke i kontrole koje se provode u cilju zaštite resursa informacijskog sustava od neovlaštenog pristupa. Nepostojanjem primjerenih mjera i postupaka fizičke sigurnosti, povećan je rizik od otuđenja i oštećenja informatičke opreme [18].

Kako bi se rizici smanjili preporučuje se: smjestiti značajnu informatičku opremu u posebne prostorije (poslužitelji, mediji za pohranu podataka, aktivna mrežna oprema), strogo ograničiti pravo pristupa u takvim prostorijama, osigurati stalni video nadzor vanjskih suradnika, od strane ovlaštenih osoba, prilikom ulaska u te prostorije. Također, može se uvesti vođenje evidencije osoba koje pristupaju tim prostorijama i primjena nekih dodatnih mjera za kontrolu pristupa (video nadzor, protuprovalni alarm, protuprovalna vrata i sl.)

Okolišna sigurnost podrazumijeva primjenu mjera i postupaka u cilju zaštite resursa IS od djelovanja prirodnih pojava poput vatre, vode, pojave vlage i slično. Djelovanje prirodnih pojava može biti pogubno po resurse IS i učiniti ih trajno nedostupnima ili neupotrebljivima, zato je potrebno učiniti sljedeće[17]:

- Ograničiti izloženost značajne informatičke opreme;
- Osigurati primjerenu zaštitu od požara za sve prostorije a naročito sa značajnom informatičkom opremom (redovito održavani i atestirani protupožarni sustavi);
- Osigurati temperaturu prostorije u kojoj je smještena informatička oprema (klimatizacija);
- Osigurati senzore vlage, sustave za detekciju prodora vode itd.

7.7 Logičke kontrole pristupa

Logičke kontrole pristupa pripadaju skupu sigurnosnih mjera implementiranih na softverskoj razini informatičke opreme, poput operativnih sustava računala i mrežne opreme, baza podataka te aplikacija. Neprimjerene logičke kontrole pristupa mogu izložiti subjekte različitim prijetnjama putem kojih je moguće ostvariti neovlašteni pristup IS-u (hakerski napadi, maliciozni kod, zlonamjerno djelovanje zaposlenika i dr.) [17].

Kako bi se umanjili rizici potrebno je osigurati postojanje primjerenih logičkih kontrola pristupa (operativnim sustavima računala i mrežne opreme, sustavnih i poslovnih aplikacija i servisa te drugim softverskim resursima putem kojih je omogućen pristup osjetljivim podacima) i osigurati logičke kontrole pristupa informatičko opremi, koja je privremeno bez nadzora (zaključavanje korisničkog sučelja).

Dodjela, izmjena i ukidanje korisničkih računa sastavni je dio većine sustava za logičku kontrolu pristupa. Dodjelom računa korisniku se omogućuje pristup jednom sustavu, primjerice operativnom sustavu računala ili poslovnoj aplikaciji, dok se dodjelom prava pristupa ovlaštenim korisnicima omogućuje pristup pojedinačnim

resursima unutar tog sustava, primjerice samo određenom skupu podataka unutar aplikacije.

Neprimjereno upravljanje korisničkim računima može ugroziti mjere kontrole pristupa stoga je potrebno [19]:

- Dodjelu, izmjenu i ukidanje korisničkih računa i prava pristupa provoditi na temelju dokumentiranih poslova i minimalnih potrebnih prava za obavljanje radnih zadataka;
- Provoditi periodičku provjeru usklađenosti dodijeljenih korisničkih računa;
- Svakom korisniku dodijeliti poseban korisnički račun (izbjegavati grupna korištenja).

Lozinke u IS predstavljaju mehanizam potvrde korisničkog identiteta. Neprimjereno upravljanje lozinkama znatno umanjuje učinkovitost mjera logičke kontrole pristupa, stoga se preporučuje [19].

- Identificirati i primijeniti minimalne standarde svojstava lozinki za pristup pojedinim resursima (dužina, rok trajanja, složenost);
- Čuvati tajnost lozinke;
- Osigurati da su u sustavima pohranjene u nečitljivom obliku;
- Lozinke pamtiti, nikad ih ne zapisivati na papir ili u elektroničke datoteke;
- Pri definiranju lozinki izbjegavati korištenje riječi iz rječnika, osobne podatke ili druge fraze.

7.8 Sigurnost računalnih mreža

Računalne mreže su najbitniji čimbenik komunikacije u bankama. Služe za povezivanje računala i uređaja. U većini slučajeva lokalnim mrežama se vrši najveći dio prijenosa osjetljivih poslovnih podataka, pa je njima potrebno pružiti i najveću pozornost u kontekstu zaštite i sigurnosti.

Kako bi se umanjili rizici od neprimjerene zaštite potrebno je [17]:

- Ograničiti pristup konfiguracijskim sučeljima mrežnih uređaja (preklopnici, usmjerivači);
- Zaštititi računala i poslužiteljske servise kojima je omogućen pristup putem javnih mreža;
- Računala i poslužiteljske servise kojima je omogućen pristup putem javnih mreža izdvojiti u mrežni segment odvojen od lokalne računalne mreže (poslužitelj internetskih stranica);
- Zaštititi prijenos osjetljivih podataka putem javnih mreža (kriptografska zaštita putem SSL/TLS[4] komunikacijskog protokola);
- Napredna zaštita bežičnih mreža (WPA2[5] protokol).

Udaljeni pristup podrazumijeva pristup lokalnoj mreži i korištenje IS subjekta smještene izvan njegovih poslovnih prostora. U svrhu sigurne zaštite od trećih osoba preporučuje se primjereno zaštititi podatke u prijenosu (SSL/IPSEC protokol) i osigurati izradu operativnih te sustavnih zapisa o aktivnostima korisnika.

7.9 Upravljanje incidentima te operativnim i sustavnim zapisima

Operativni i sistemski zapisi omogućuju uvid u aktivnosti resursa informacijskog sustava (operativni sustav, vatrozid, sustav za otkrivanje neovlaštenog pristupa, aplikacijskih sustava). U kombinaciji s odgovarajućim aktima, procedurama i alatima operativni zapisi omogućuju otkrivanje od neovlaštenog pristupa, identifikaciju problema itd [18].

Incidenti se definiraju kao nepredviđeni događaji i situacije koje mogu narušiti funkcionalnost i sigurnost IS.

[4] SSL/TLS (eng. *Transport Layer Security, Secure Sockets Layer*) su kriptografski protokoli koji omogućuju sigurnu komunikaciju putem Interneta za stvari kao Internet bankarstvo.
[5] WPA2 (eng. *Wi-Fi Protected Access*) je algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža

Neke od mjera su [17]:

- Omogućiti korisnicima IS pravovremenu prijavu incidenta;
- Odrediti obveze i odgovornosti u zaprimanju, daljnjoj eskalaciji i rješavanju incidenata;
- Rješavati uočene incidente i primjenjivati mjere u prevenciji pojave incidenata u budućnosti;
- Vođenje evidencije o prijavljenim incidentima (ime osobe koja je prijavila, opis incidenta, ime osobe koja je preuzela rješavanje incidenta sl.).

Operativni i sustavni zapisi komponenti IT, primjerice aplikacija i operativnih sustava računala, generiraju se u svrhu bilježenja informacija o aktivnostima i događajima vezanima uz njih. Ključnu ulogu imaju u rekonstrukciji događaja vezanih uz komponente IT te u utvrđivanju odgovornosti korisnika IS. U cilju primjerenog upravljanja operativnim i sustavnim zapisima potrebno je [17]:

- Osigurati generiranje operativnih i sustavnih zapisa u svim važnim komponentama IT (korisničko ime osobe koja je provela aktivnost, opis aktivnosti, naziv komponente IT te vrijeme);
- Zaštititi zapise važnih komponenti IT od neovlaštenog pristupa;
- Izrađivati pričuvne kopije zapisa.

7.10 E – bankarstvo

E-bankarstvo uključuje sustave koji klijentima pružaju bankarske proizvode i usluge. Stalne inovacije, širenje telekomunikacijskih kanala, Interneta i sve veća konkurencija omogućili su razvoj postojećih novih proizvoda i usluga. Kako samo e-bankarstvo koje je danas tako jako prisutno nije uzrok nastanka novih rizika u poslovanju banaka, vidljivo je kako utječe na promjenu karakteristika već poznatih rizika (strateškog, operativnog, pravnog rizika).

Sve navedeno povećava potrebu da se i prije uvođenja nove e-bankarske usluge provede procjena rizika. Ubrzanim napretkom tehnologije posebno su povećani rizici povezani s e-bankarstvom. Kako bi se ti rizici smanjili potrebno je

uspostaviti sigurnosnu infrastrukturu koja će djelotvorno štititi resurse, primijeniti sigurne i učinkovite autentifikacijske metode, zaštititi informacije od neovlaštenog otkrivanja, mijenjanja, brisanja te osigurati adekvatnu potvrdu. Te na kraju osigurati adekvatnu potvrdu svog identiteta, osigurati postojanje operativnih i sustavnih zapisa za sve transakcije te stalno upozoravati korisnike s mogućim rizicima [18].

8 ISTRAŽIVANJE PERCEPCIJE SIGURNOSTI PRIMJENE IK TEHNOLOGIJA PRI KORIŠTENJU BANKARSKIH USLUGA U RH

U okviru istraživanja percepcije sigurnosti i pomoći budućim projektantima u lakšoj izradi zadovoljavajućeg IK sustava, izrađen je anketni upitnik. Osim navedenog, upitnik je izrađen za potrebe analize ispitanikovih korištenja pojedinih usluga, ali i ispitivanje percepcije korisničke sigurnosti. Kako projektiranje novog IK sustava podrazumijeva razne analize, oblikovanja, skupove podataka u cilju boljeg funkcionairanja sustava i zadovoljenja korisničkih potreba, provedena anketa bi pomogla u jednom od segmenata.

Anketni odgovori bi budućim projektantima pomogli na način da lakše pristupe određenoj populaciji u vidu ponude usluga, korištenju usluga, vizualnom identitetu usluga itd.

U vidu zaštite, odgovori bi budućim projektantima pomogli tako da lakše pojedinoj populaciji približi svjesnost od mogućih prijetnji i napada te zaštita od istih. Također bi dali odgovor koliko često bi trebalo ići u smjeru edukacije korisnika da znaju identificirati problem ako do njega i dođe, te ga i riješe.

Anketa može pomoći smjernicama i preporukama kod lakših i bezbolnijih načina potvrde identiteta, autorizacije, dodjeli korisničkih računa, sigurnosti mreža itd.

Anketni upitnik izrađen je uz pomoć aplikacije *LimeSurvey*.

Anketa o percepciji sigurnosti primjene IK tehnologija pri korištenju bankarskih usluga provedena je anketiranjem na terenu i putem studentske stranice Fakulteta prometnih znanosti, e-student. U anketi su sudjelovala 203 ispitanika.

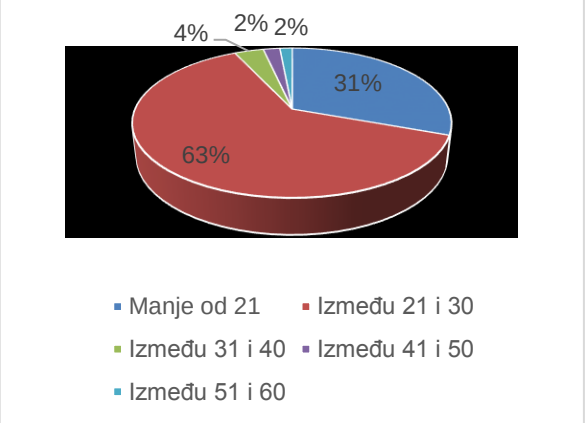
Anketni upitnik sastavljen je od 29 pitanja, koja su logički podijeljena u četiri dijela. Prvi dio anketnog upitnika sastoji se od pitanja koja se odnose na demografske karakteristike ispitanika: dob, spol, obrazovanje i djelatni status. U drugom dijelu upitnika ispitanici su pitani o učestalosti korištenja pojedinih usluga, npr. NFC plaćanja. U trećem i četvrtom dijelu anketnog upitnika, ispitanici su

odgovarali na pitanja vezana za korištenje mobilnog terminalnog uređaja i osobnog računala, kao sredstva za korištenje bankarskih usluga.

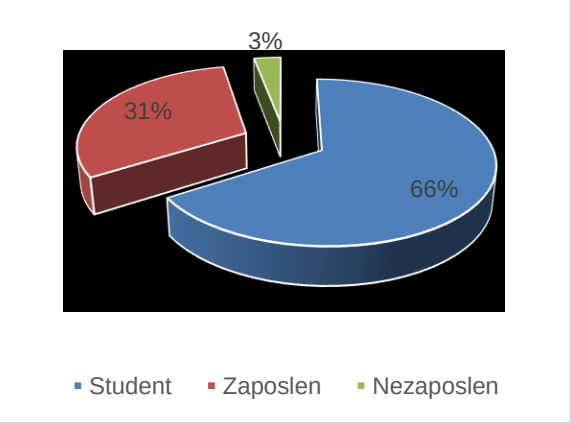
8.1 Analiza strukture korisnika

Najviše ispitanika činila je studentska populacija, odnosno ispitanici u starosti od 21. do 30. godine života, što je vidljivo iz grafikona 3a.

Najčešći odgovori dobiveni su od studentske populacije odnosno dobne skupine od 21 do 30 godina kao što je i vidljivo na grafikonima 3a i 3b.



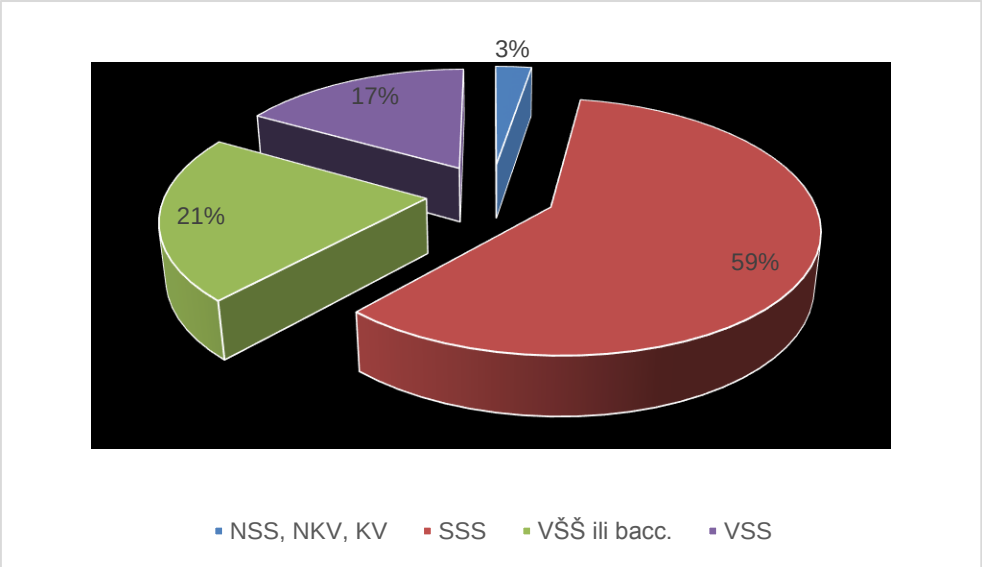
(a) Starosna dob ispitanika



(b) Djelatni status ispitanika

Grafikon 3. Starosna dob i djelatni status ispitanika

Prema završenoj stručnoj spremi, najviše ispitanika čine ispitanici koji imaju srednju stručnu spremu. To je i logično, s obzirom na to kako je većina ispitanika bila studentska populacija. Navedeno je prikazano grafikonom 4.

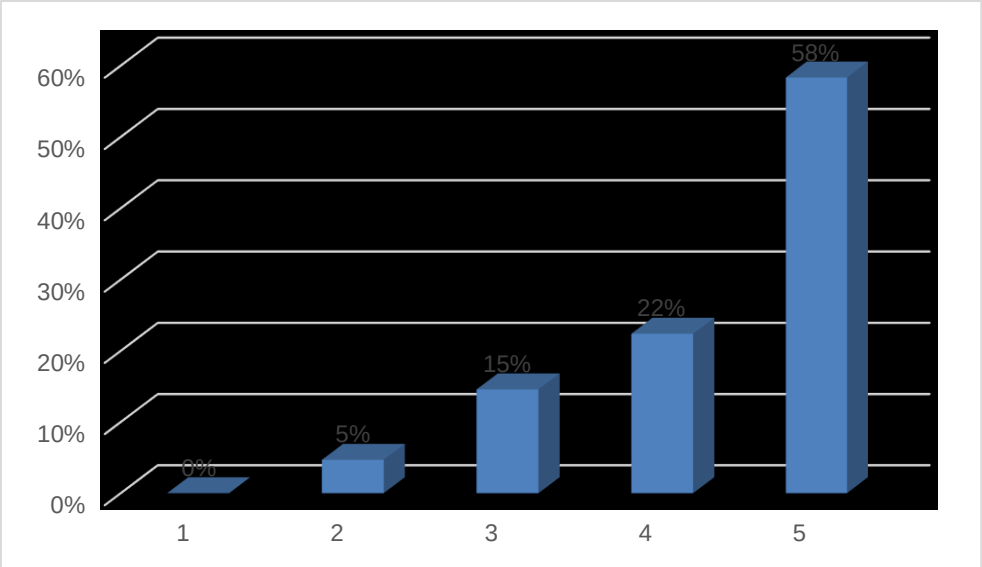


Grafikon 4. Stručna sprema ispitanika

8.2 Rezultati analize korištenja bankarskih usluga

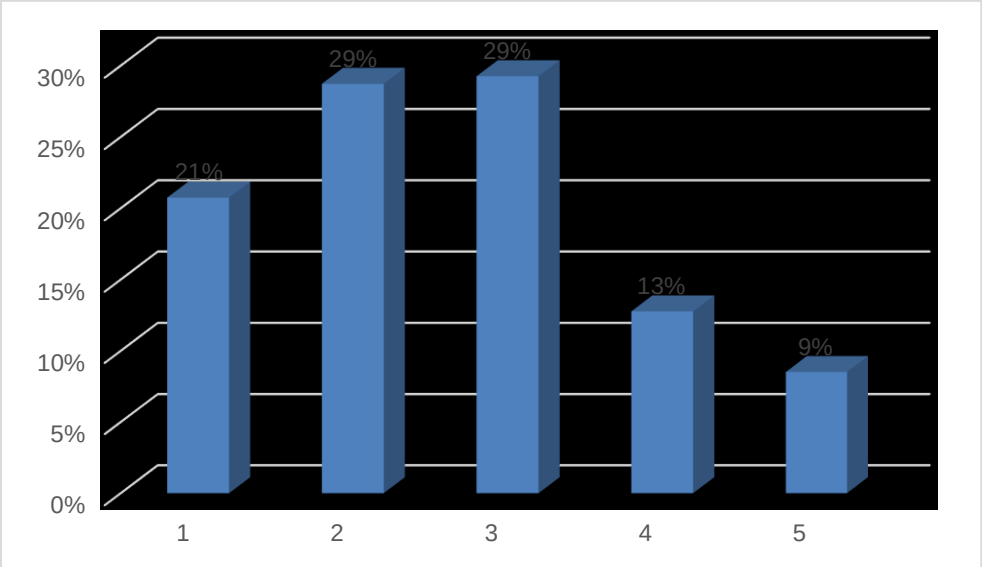
Korisnici imaju različite načine i običaje kod plaćanja, tako je na sljedećim grafikonima vidljivo koliko često i kako ispitanici koriste neke od najpoznatijih usluga. Na grafikonu 5. vidljivo je kako su korisnici još uvijek najodaniji plaćanju gotovinom i to više puta na svakodnevnoj bazi. Na grafikonima brojke predstavljaju:

- 1 – ne koristi se uopće
- 2 – koristi se jednom tjedno
- 3 – koristi se par puta tjedno
- 4 – koristi se barem jednom svakodnevno
- 5 – koristi se nekoliko puta svakodnevno



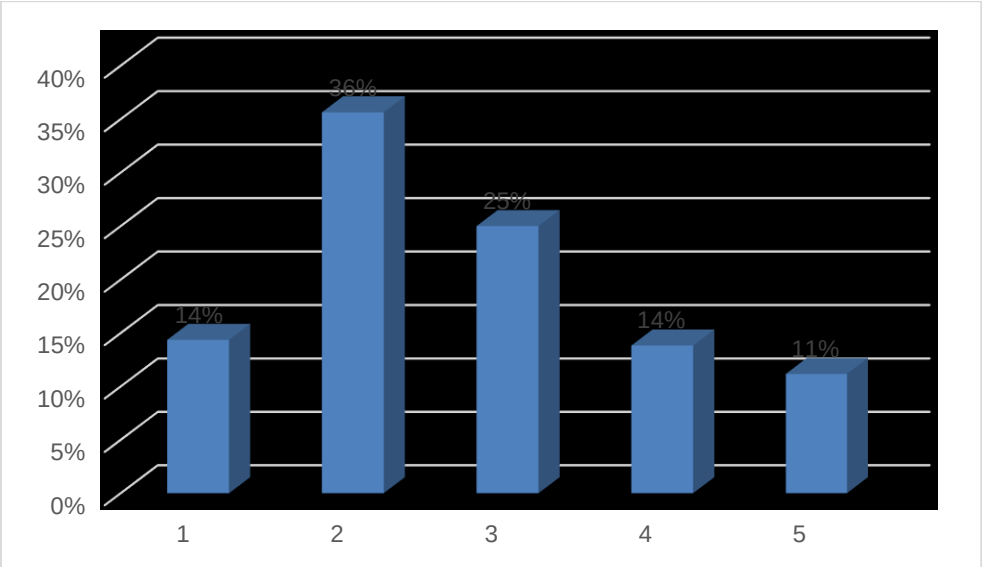
Grafikon 5. Učestalost plaćanja gotovinom

Iz grafikona 6. vidljivo je kako raste trend plaćanja kreditnim karticama. Vidljivo je kako najviše ispitanika koriste kartice za plaćanje barem par puta tjedno, ako ne i više, odnosno jednom svakodnevno ili par puta svakodnevno.



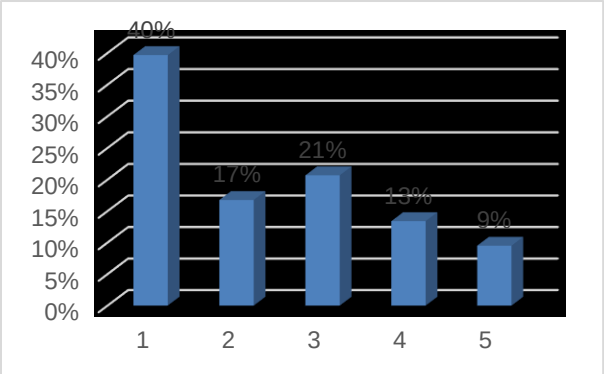
Grafikon 6. Plaćanje kreditnim karticama

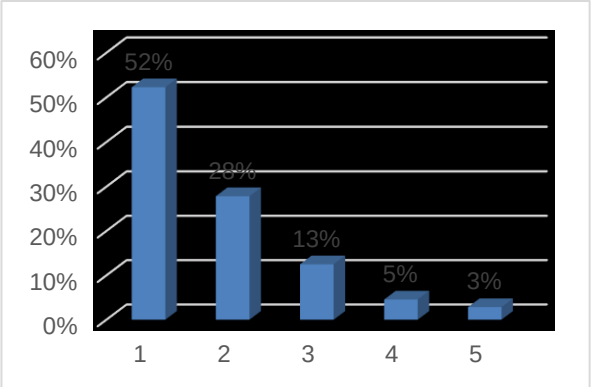
Podizanje gotovine s bankomata je na očekivanoj razini, odnosno bar jednom tjedno (grafikon 7.). Sam taj proces banke bi htjele svesti na minimum, jer svako punjenje bankomata gotovinom za njih predstavlja trošak.



Grafikon 7. Podizanje gotovine s bankomata

Što se tiče korištenja m-bankarstva i e-bankarstva vidljivo je kako ispitanici još uvijek nemaju naviku korištenja m-bankarstva (grafikon 8a.) i e-bankarstva (grafikon 8b.). Tako se dolazi do rezultata kako od ukupnog broja anketiranih osoba čak 40% ne koristi m-bankarstvo. Kod e-bankarstva vidljivo je kako čak 50% ispitanika ne koristi tu uslugu odnosno samo mali broj koji i koriste bar jednom tjedno.

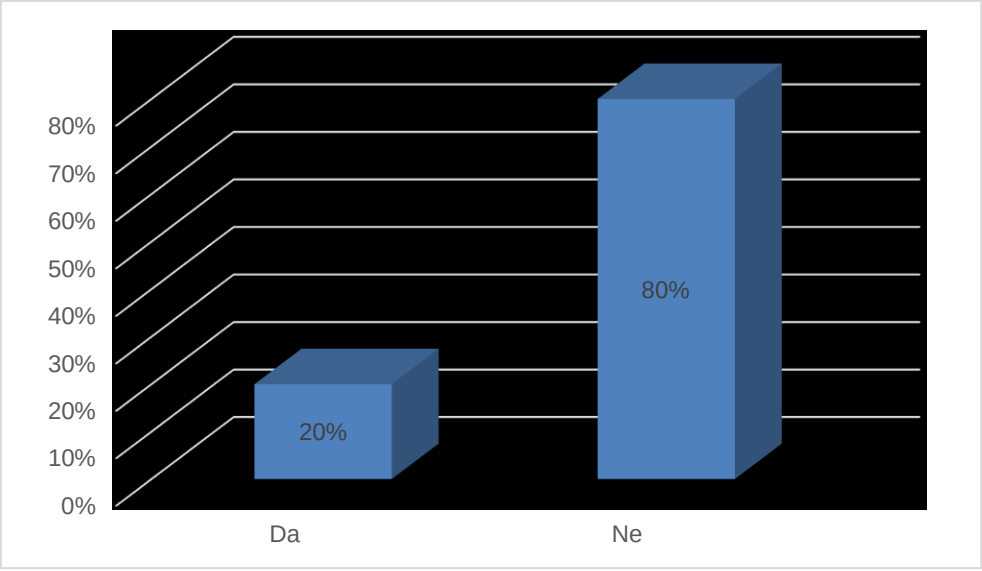




(a) Korištenje m-bankarstva **(b)** Korištenje e-bankarstva

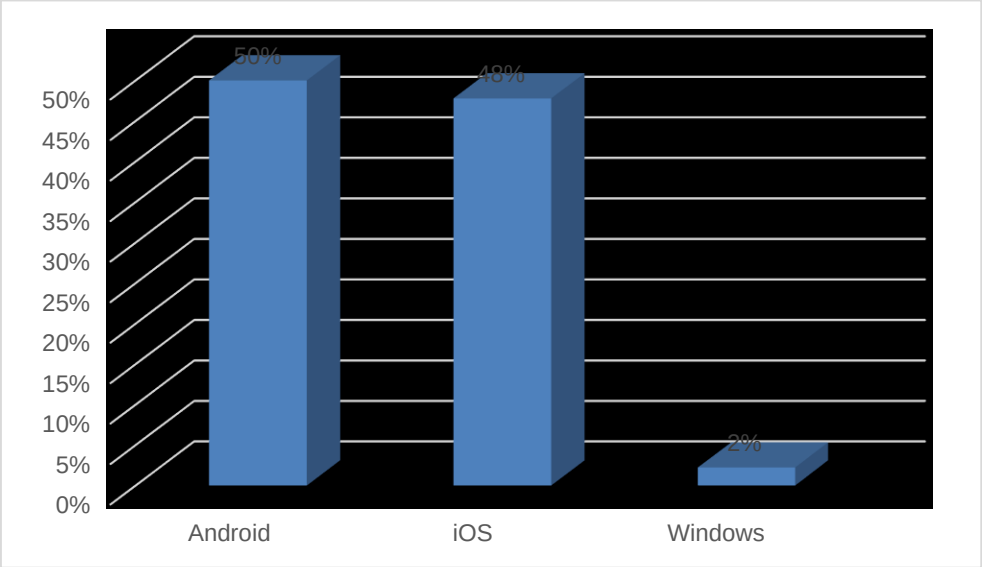
Grafikon 8. Zastupljenost korištenja usluga m-bankarstva i e-bankarstva

Kod korištenja mogućnosti bezkontaktnog plaćanja (NFC kartice) vidljivo je, i očekivano, kako 20% ispitanika koristi tu uslugu koju. Mogućnost plaćanja NFC karticama, također nije u ponudi nekih banka. Tako mali postotak korištenja vjerojatno proizlazi i iz toga što je većina korisnika svjesna rizika gubitka kartice i posljedica koje bih se mogle dogoditi po osobu koja je izgubila svoju karticu. Broj ispitanika koji koriste NFC karticu prikazan je grafikonom 9.



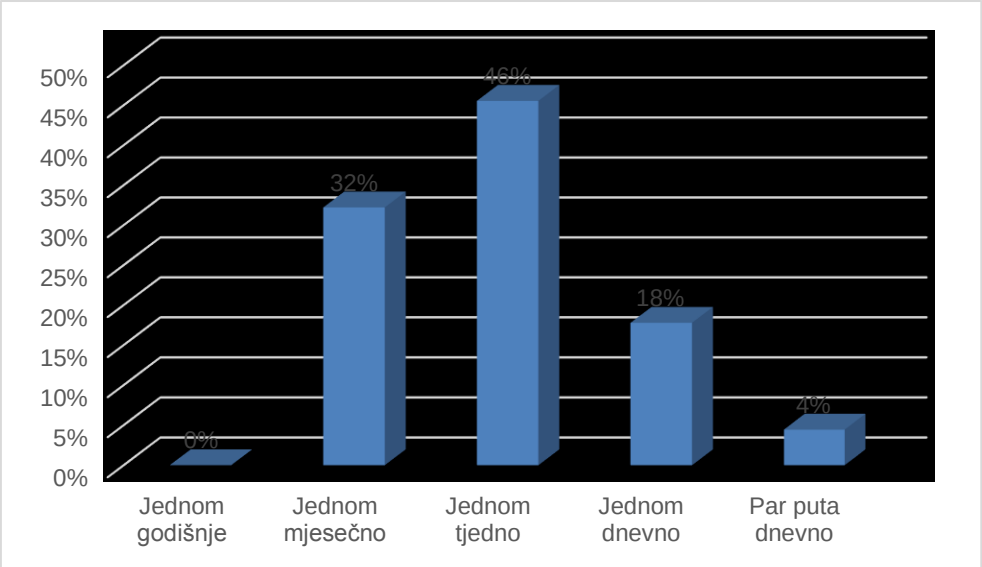
Grafikon 9. Broj korisnika koji koriste NFC karticu kao sredstvo plaćanja

Kako je i prethodno prikazano, dio ispitanika koristi mobilni terminalni uređaj za pristup bankarskim uslugama. Najčešći operacijski sustavi i dalje su iOS i Android, zbog zastupljenosti navedenih operacijskih sustava, a ne zbog pitanja sigurnosti. Raspodjela operacijskih sustava prikazana je grafikonom 10.



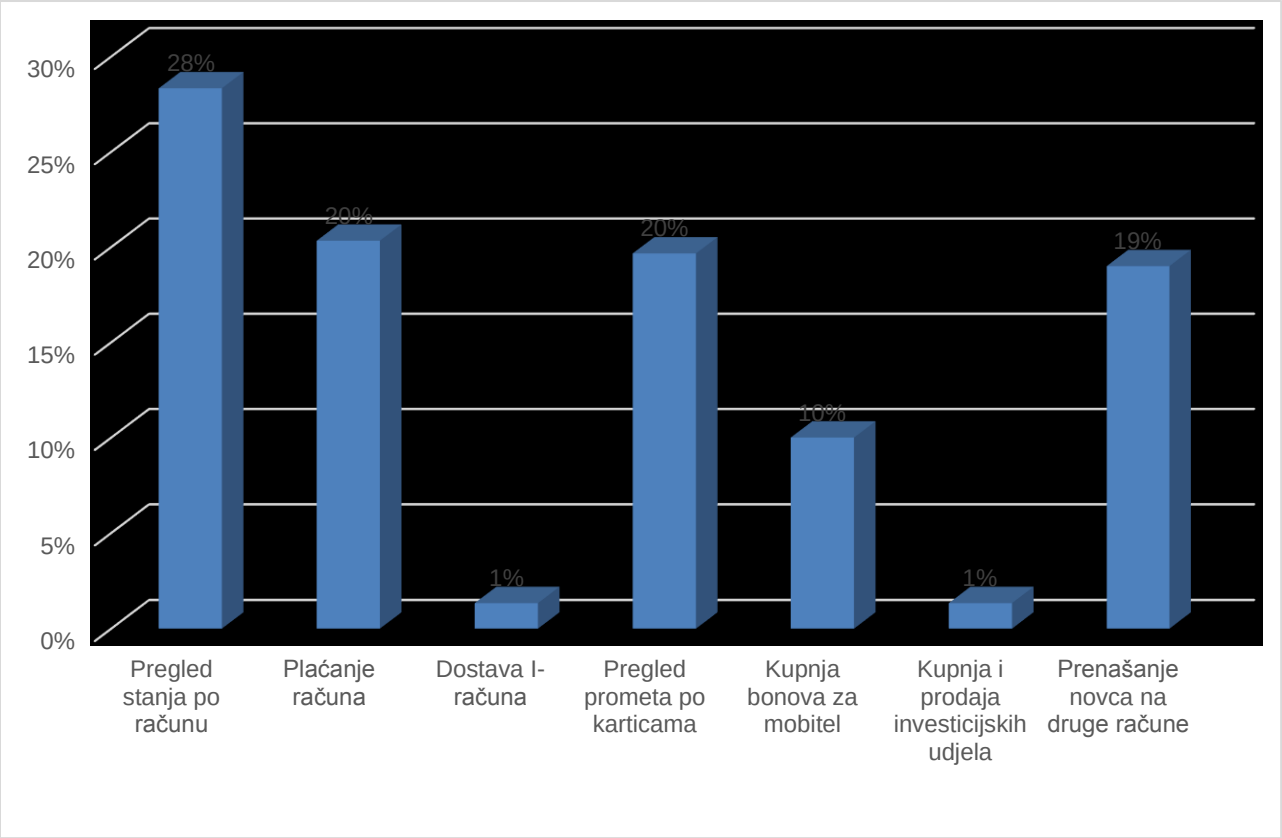
Grafikon 10. Operacijski sustav na mobitelu

Na pitanju o učestalosti korištenja mobilnog terminalnog uređaja, polovica ispitanika koristi navedeni jednom tjedno, a trećina jednom mjesečno. Navedeno je prikazano grafikonom 11.



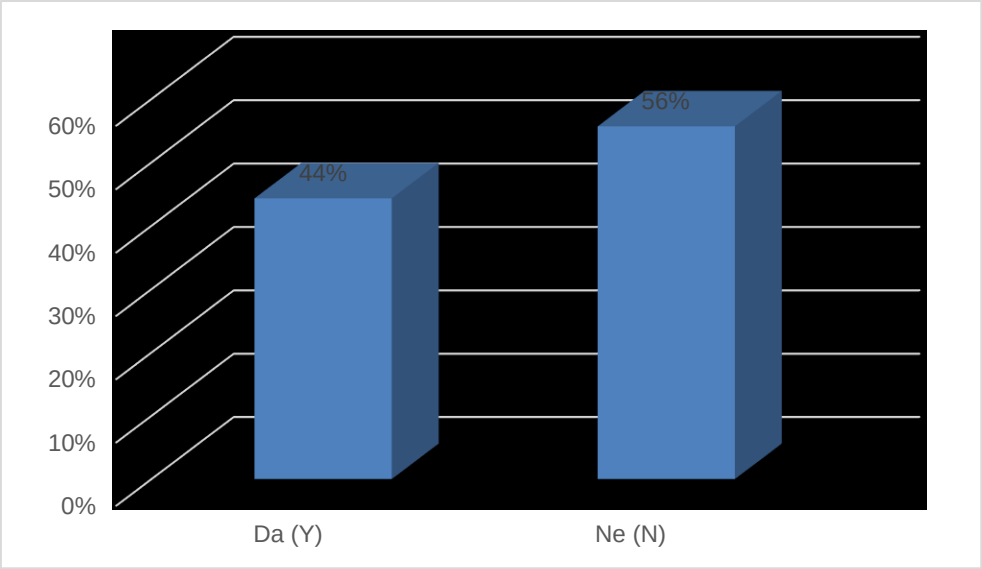
Grafikon 11. Učestalost korištenja mobilnih terminalnih uređaja za bankarske usluge

Najveći broj ispitanika (njih 28%; grafikon 12.) koristi m-bankarstvo za pregled stanja računa, plaćanje računa i promet. Mali broj ispitanika koristi m-bankarstvo za dostavu i-računa i kupnju bonova.



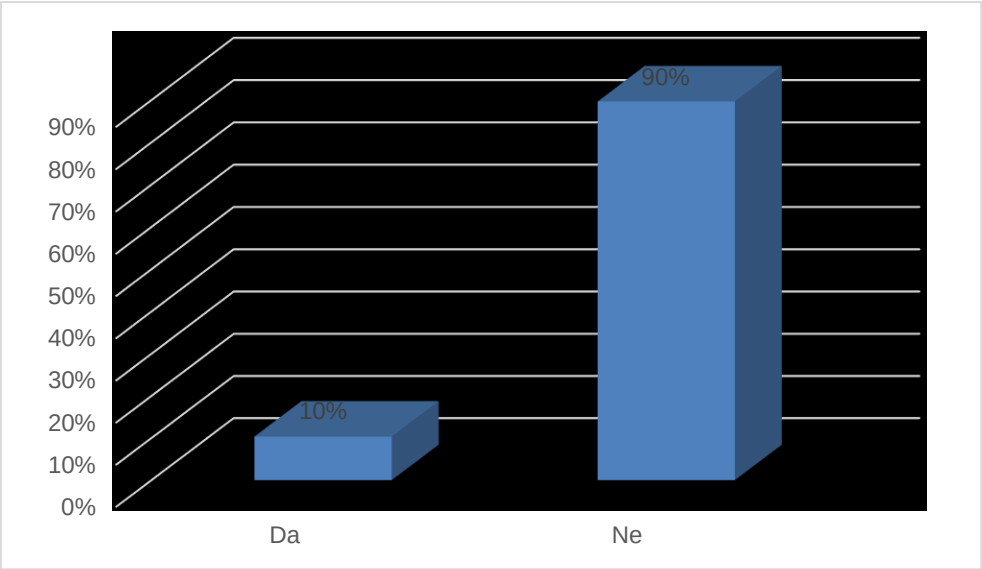
Grafikon 12. Korištenje m-Bankarstva za određene usluge

Više od polovice ispitanika ne spaja se na nepoznate Wi-Fi mreže te su svjesni opasnosti, dok njih 44% još uvijek ne smatra da postoji neka mogućnost opasnosti po mobilni uređaj, ukoliko se normalno spajaju na nepoznate Wi-Fi mreže. Otprilike isti broj ispitanika smatra kako postoji ista opasnost od nekog oblika napada, ako je mobilni uređaj spojen na moblinu (3G/4G) mrežu.



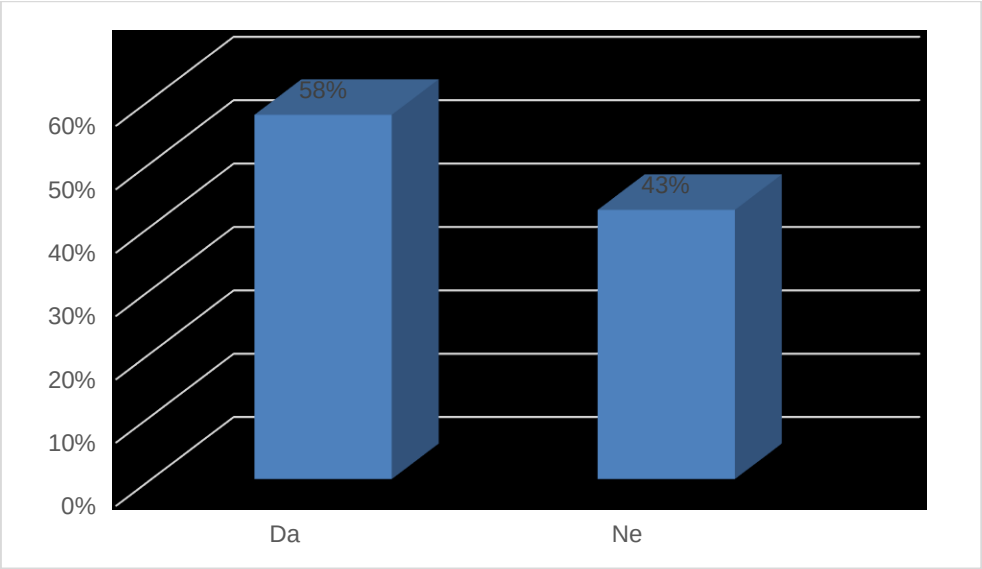
Grafikon 13. Spajanje mobilnim terminalnim uređajem na nepoznate WiFi mreže

Čak 90% ispitanika ne koristi neku od aplikacija za suzbijanje zlonamjernih softvera, te pola ispitanika nisu upoznati s nekim od najzastupljenijih napada, a ostali koji jesu za najopasnije napade naveli su: *malware*, gubitak uređaja, gubitak podataka i *phishing*.



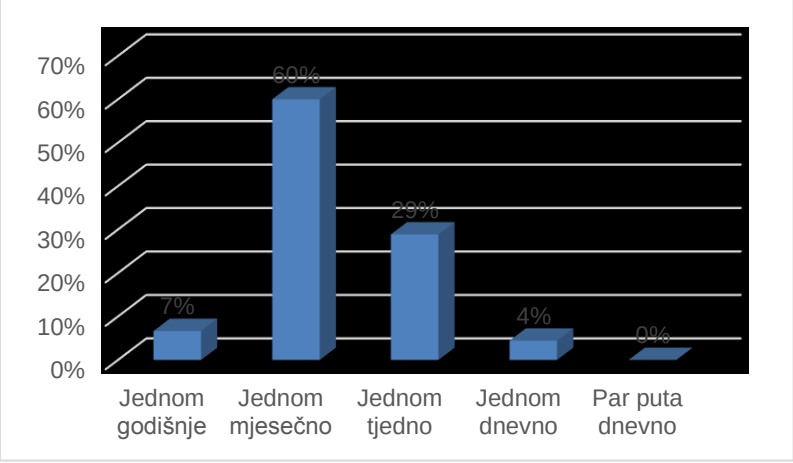
Grafikon 14. Zlonamjerni softver na mobilnom terminalnom uređaju

S grafikona 15. vidljivo je kako među ispitanima samo 58% njih koristi računalo za pristup nekim bankarskim uslugama, dok svi imaju Windows operacijski sustav (100%).



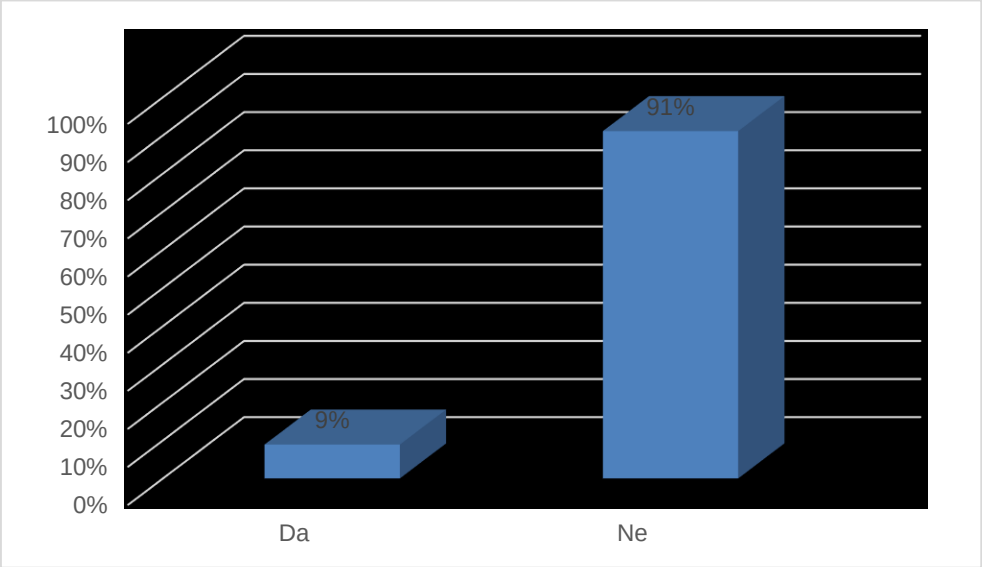
Grafikon 15. Korištenje e-Bankarstva

Nadalje je vidljivo iz grafikona 16., kako učestalost korištenja bankarskih usluga preko računala nije veća od jednom mjesečno, što znači kako gotovo 60% ispitanika samo jednom mjesečno koristi te usluge, a njih 29% jednom tjedno.



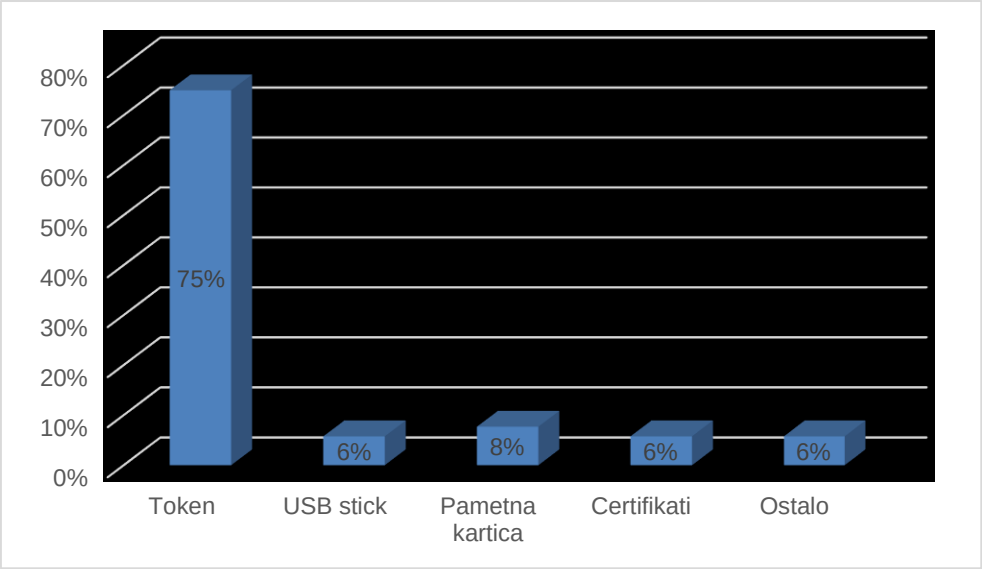
Grafikon 16. Korištenje računala za bankarske usluge

Zadovoljava činjenica kako preko 90% ispitanika se ne spaja računalom na nepoznate Wi-Fi mreže (grafikon 17.), iako ih je samo pola svjesno opasnosti spajanja na nepoznate Wi-Fi mreže. Također samo polovica ispitanika koristi neke od aplikacija za suzbijanje zlonamjernih softvera na računalu.



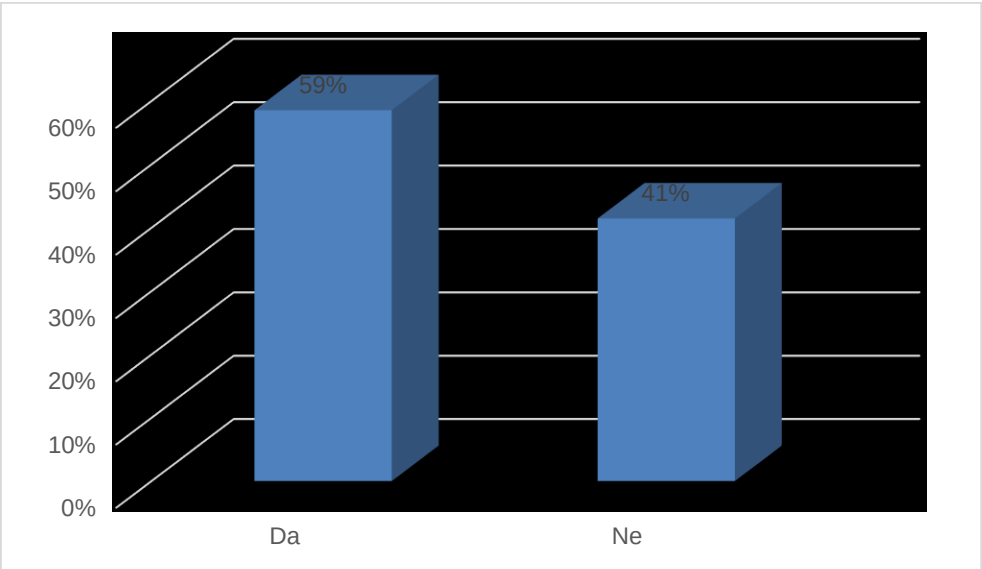
Grafikon 17. Spajanje na nepoznate Wi-Fi mreže s osobnim računalom

Najčešći način autentifikacije za povezivanje na e-bankarstvo je Token (grafikon 18.), koji prevladava u odnosu na ostale načine. Banke redovito angažiraju neovisne konzultante i revizore kako bi provjerili i potvrdili sigurnost sustava. Provjerava se: arhitektura, konfiguracija i sigurnosne postavke mrežne opreme, servera i aplikacija. Također, banke na razne načine štite svoje klijente od automatske odjave ako se ne koristi određeni broj minuta do upozorenja korisnika o mogućim novim prijetnjama.



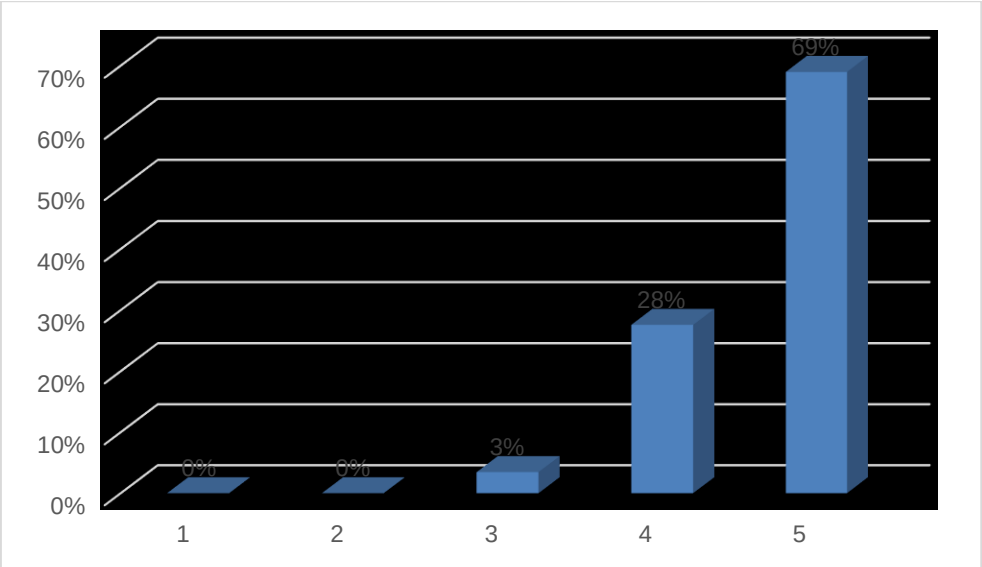
Grafikon 18. Načini autentifikacije za e-bankarstvo

Više od polovice ispitanika je upoznato sa najčešćim vrstama napada za računala (grafikon 19.), a kao najzastupljenije i najopasnije navode: *malware*, *phishing*, *keylogger*.



Grafikon 19. Upoznatost ispitanika s mogućnostima napada

Na samom kraju ankete više od pola ispitanika tvrdi kako koristi *PayPal* za plaćanje te ga smatra vrlo sigurnim sredstvom za plaćanje. Na grafikonu 20. brojke prikazuju percepciju sigurnost od 1 do 5.



Grafikon 20. Ocjena sigurnosti *PayPal* sustava za plaćanje

9 ZAKLJUČAK

Bankarski informacijski sustavi temelje se na povjerljivosti, cjelovitosti i dostupnosti, što se deklarira kao tri osnovna načela koja konstantno moraju biti ispunjena i nikada povrijeđena.

Kroz ovaj rad prikazana su: glavna načela sigurnosti, sigurnosni aspekti, sigurnosna politika te preporuke i smjernice u cilju postizanja zavidne razine sigurnosti u bankarskom sektoru.

U diplomskom radu napravljen je i anketni upitnik u svrhu prikaza percepcije sigurnosti korištenja bankarskih usluga i pomoći budućim projektantima u lakšoj izradi zadovoljavajućeg IK sustava. Glavni cilj ankete je prikazati određenu populaciju korisnika, njihove životne navike, običaje plaćanja, korištenja usluga te njihovu percepciju sigurnosti korištenja.

Anketni upitnik proveden je u svrhu pomoći i lakšeg pristupa pri projektiranju pojedinih dijelova informacijsko komunikacijskih sustava. Kako za banku svaki dodatni napor predstavlja nepotrebni trošak i vrijeme, od iznimne je važnosti znati kako i na koji način razmišlja određena populacija te kako pristupiti projektiranju informacijsko komunikacijskih sustava i predstavljanju istih.

Provedenom anketom o istraživanju percepcije sigurnosti primjene IK tehnologija pri korištenju bankarskih usluga u RH obuhvaćene su 203 osobe, od kojih je navjeći broj njih od 21 do 30 godine starosti (63%).

Iz dobivenih rezultata ankete vidljivo je kako raste trend plaćanja kreditnim karticama, što je zadovoljavajuće za banke, pošto svako podizanje gotovine s bankomata predstavlja nepotrebni trošak.

Daljnjom analizom rezultata korištenja m-bankarstva i e-bankarstva dolazi se do podatka kako 40% anketiranih ne koristi m-bankarstvo te polovica ispitanih neki oblik e-bankarstva. Ta brojka možda proizlazi jednostavno iz navika korisnika ili straha od napada putem interneta.

Korisnici m-bankarstva najviše pristupaju usluzi jednom tjedno, velika većina koristi uslugu za pregled stanja računa, plaćanje i promet, a mali broj njih za usluge

dostavu i-računa i kupnju bonova. Polovica ispitanih se ne spaja na nepoznate Wi-Fi mreže te ih je isto toliko upoznato sa najučestalijim napadima, od kojih za najopasnije navode malware, gubitak uređaja, gubitak podataka itd. Većina tih napada može se spriječiti upotrebom nekom od aplikacija za suzbijanje zlonamjernih softvera gdje čak 90% ispitanika nema instalirano ništa od navedenog.

Korisnici e-bankarstva u velikoj većini koriste uslugu najviše jednom mjesečno. Također zadovoljava činjenica kako se 90% korisnika ne spaja računalom na nepoznate Wi-Fi mreže te što ih polovica koristi neke od aplikacija za suzbijanje softvera na računalu što je puno veći postotak nego kod m-bankarstva.

Provedenim analizama dobivenih podataka pretpostavka je kako su korisnici još uvijek nepovjerljivi u sustav bankarskog poslovanja putem Interneta ili jednostavno potaknuti životnim navikama u vidu slabijeg korištenja bankarskih usluga. Činjenica je kako taj podatak koči daljnji rast broj korisnika elektroničkih bankarskih usluga. Konkretne preporuke i smjernice u vidu dobivanja novih korisnika kao i zadržavanje starih trebale bi ići u pravcu češćih anketa, stalnog osluškivanja stalnih i budućih korisnika te stalna edukacija kako korisnika tako i zaposlenika banaka.

Rastom broja korisnika pametnih telefona, razvoj budućih usluga ići će sve više u smjeru mobilnog poslovanja putem Interneta. Mlađe generacije odrastaju uz Internet te će zasigurno biti puno lakše doći do njih kao i prezentirati im buduće usluge kao i sve prijetnje koje su uvijek prisutne.

LITERATURA

[1] Juran, A.: *Sigurnost i zaštita informacijskih sustava*, diplomski rad, Pomorski fakultet, Rijeka, 2014.

[2] Peraković, D., Cvitić, I.: *Sigurnost i zaštita informacijsko komunikacijskog sustava*, skripta iz kolegija Sigurnost i zaštita informacijsko komunikacijskog sustava, Fakultet prometnih znanosti, Zagreb, 2015.

[3] Vukelić, B.: *Sigurnost informacijskih sustava*, nastavni materijal iz kolegija Sigurnost informacijskih sustava, Veleučilište u Rijeci, Rijeka

[4] Hrvatska akademska i istraživačka mreža: *Sigurnosna politika*, Nacionalni CERT u suradnji s LSS, Zagreb, 2009.

[5] Kovačević, D.: *Sigurnosna politika*, diplomski rad, Fakultet elektrotehnike i računarstva, Zagreb, 2008.

[6] *CSI/FBI Computer Crime and Security Survey*, URL: http://www.issa-sac.org/docs/FBI2004.pdf (pristupljeno: srpanj 2016.)

[7] URL: http://www.arraydev.com/commerce/JIBC/2012-08/AaronFrenchv02.pdf (pristupljeno: travanj 2016.)

[8] Vrabac, A. i dr.: *Vrste zaštite računarskih sistema i podataka*, seminarski rad, Fakultet za saobraćaj i komunikacije, Sarajevo, 2010.

[9] URL: http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustava_0.pdf (pristupljeno: rujan 2016.)

[10] *Common Types of Network Attacks*, URL: https://technet.microsoft.com/en-us/library/cc959354.aspx (pristupljeno: svibanj 2016.)

[11] Gledec, G., Mikuc, M., Kos, M.: *Sigurnost u privatnim komunikacijskim mrežama*, Fakultet elektrotehnike i računarstva, Zagreb, 2008.

[12] *IT threat evolution in Q1 2015*, URL: https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/ (pristupljeno: lipanj 2016.

[13] Hrvatska akademska i istraživačka mreža: *Bankarski zlćudni programi*, Nacionalni CERT u suradnji s LSS, Zagreb, 2009.

[14] *Email Spam Alert – American Express / Home Depot Breach Phishing Scam*, URL: https://www.spamstopshere.com/blog/spam-news/email-spam-alert-american-express-home-depot-breach-phishing-scam (pristupljeno: lipanj 2016.)

[15] Hrvatska akademska i istraživačka mreža: *Sigurnosni model mreže računala*, Nacionalni CERT u suradnji s LSS, Zagreb, 2009.

[16] *SANS Institute, Network Security Model*, URL:https://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843 (pristupljeno: siječanj 2017.)

[17] *Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora*, URL: http://www.hanfa.hr/getfile/41744/7Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf (pristupljeno: rujan 2016.)

[18] *Smjernice za upravljanje informacijskim sustavom u cilju smjanjenja operativnog rizika,* URL: http://old.hnb.hr/supervizija/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf (pristupljeno: veljača 2017.)

[19] Kramarić, D., *Smjernice za primjereno upravljanje rizicima informacijskih sustava nadzora*, URL: http://icti.svijetosiguranja.hr/UserFiles/file/icti/ICTI%202015/Prezentacije/01.%20Drazen%20Kramaric.pdf (pristupljeno: veljača 2017.)

POPIS ILUSTRACIJA

Popis slika

Popis tablica

Popis grafikona

POPIS KRATICA

Kratica	Puni naziv
CIA	(eng. *Confidentiality Integrity Aviability)* kratica koja označava povjerljivost, cjelovitost i dostupnost
CPU	(eng. *Central Processing Unit*) središnja procesorska jedinica
DNS	(eng. Domain Name System) je raspoređeni sustav imenivanja računala, servise ili bilo koje sredstvo na Internetu
DoS	(eng. *Denial of Service Attack*) napad uskraćivanjem usluge
FTP	(eng. File Transfer Protocol) je standardni mrežni protokol koji se koristi za premještanje datoteka s jednog hosta na drugi putem mreže temeljene naTCP-u, kao što je Internet.
IDS	(eng. Intrusion Detection System) je sustav prevencije od mrežnih napada
IEC	(eng. *International Electrotechnical Commission*) Međunarodna elektronička komisija
IPS	(eng. *Intrusion Prevention System*) je sustav prevencije od mrežnih napada
IS	(eng. *Information System*) Informacijski sustav
ISO	(eng. *International Organization for Standardization*) Internacionalna Organizacija za standardizaciju
IT	(eng. *Information Tehnology*) je razvoj, istraživanje, provedba, dizajn i upravljanje informatičkim sustavima
OTP	(eng. *one – time passwords*) su jednokratne lozinke
PIN	(eng. *Personal Identification Number*) osobni identifikacijski broj
RAM	(eng. *Random Access Memory*) je oblik primarne računalne memorije
SSL/TLS	(eng. *Transport Layer Security, Secure Sockets Layer*) su kriptografski protokoli koji omogućuju sigurnu komunikaciju putem Interneta za stvari kao Internet bankarstvo
TAN	(eng. *Transaction Authentication Number*) transakcijski broj
VLAN	(eng. *Virtual Local Area Network*) bavi se stvaranjem i održavanjem vitrualnih lokalnih
VPN	(eng. *Virtual Private Network*) Virtualna privatna mreža

WPA2 (eng. *Wi-Fi Protected Access*) je algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža

METAPODACI

Naslov rada: Projektiranje i zaštita informacijsko - komunikacijskih sustava u bankarskim institucijama

Student: Filip Ćurić

Mentor: izv. prof. dr. sc. Dragan Peraković

Naslov na drugom jeziku (engleski): Design and Protection of Information and Communication Systems in Banking Institutions

Povjerenstvo za obranu:

- prof. dr. sc. Zvonko Kavran, predsjednik
- izv. prof. dr. sc. Dragan Peraković, mentor
- Ivan Cvitić, mag. ing. traff., član
- doc. dr. sc. Marko Periša, zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: diplomski

Studij: Promet (npr. Promet, ITS i logistika, Aeronautika)

Datum obrane diplomskog rada: 7.3.2017.

Napomena: pod datum obrane diplomskog rada navodi se prvi definirani datum roka obrane.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Projektiranje i zaštita informacijsko - komunikacijskih sustava u bankarskim institucijama**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 16.2.2017.

(potpis)