Sigurnosni aspekti i metode zaštite informacijskih sustava

Oštrić, David Ivan

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

David Ivan Oštrić

SIGURNOSNI ASPEKTI I MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

ZAVRŠNI RAD

Zagreb, 2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

SIGURNOSNI ASPEKTI I MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

SAFETY AND PROTECTION OF COMMUNICATION INFORMATION SYSTEMS

Mentor: Marko Periša, dipl. ing.

Student: David Ivan Oštrić, 0135223955

Zagreb, 2015.

SIGURNOSNI ASPEKTI I MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

SAŽETAK

Informacijski sustavi omogućuju i pospješuju vođenje i upravljanje bankarskim procesima.
U svome poslovanju, bankarski informacijski sustavi konstantno su izloženi raznim oblicima prijetnji. Uvođenjem sigurnosne politike te njenih pravila i normi pospješuje se stupanj sigurnost. Kako bi se odabrale adekvatne mjere i metode zaštite, analizirane su i objašnjene moguće vrste prijetnji, napadačke metode na bankarske informacijske sustave i razne vrste zlonamjernih programa koji mogu narušiti glavne sigurnosne aspekte i uzrokovati značajne posljedice. Spoznajom mogućih prijetnji, utvrđene su i opisane adekvatne metode zaštite.

KLJUČNE RIJEČI: informacijski sustav; bankarstvo, prijetnje, sigurnost, zaštita

SUMMARY

Information systems are allowing and improving guidance and control of banking processes.
While operating, banking information systems are constantly exposed to various forms of threats. Introducing of safety policy and its regulations and norms, the safety degree is improved. Possible kinds of threats, attacking methods on banking information systems and various kinds of malicious programs which can violate main safety aspects and cause severe consequence had been analyzed to chose adequate measures and method of protection. With investigation of possible threats, adequate measures of protection have been determinated and decribed.

KEYWORDS: information system, banking, threats, safety, protection

SADRŽAJ

1. UVOD

Uz kontinuirani razvoj informacijskih tehnologija, pojavila se potreba za uvođenjem informacijskih sustava unutar raznih poduzeća kako bi se olakšalo vođenje i upravljanje poslovnim procesima. Uz financijski državni sektor koji je među prvima uveo informacijske sustave, podrazumijevaju se i bankarske ustanove koje su naglo pospješile svoje poslovanje nakon uvođenja istih. Uz lako upravljanje i pohranjivanje velike količine informacija i svih ostalih prednosti koje su omogućili bankarski informacijski sustavi, pojavile su se i neželjene posljedice kao što je računalni kriminal i nezakonito otuđenje podataka. Uz ubrzani razvoj bankarskih informacijskih sustava, usporedno su zabilježena brojna povećanja napada na iste te se od samih početaka pojavila nužnost uvođenja raznih načina zaštite i postizanje opće sigurnosti. Sigurnost informacijskih sustava u bankarstvu jedna je od osnovnih komponenti za uspješno upravljanje poslovanjem i ispunjavanjem korisničkih zahtjeva. Uvođenjem raznih normi, mehanizama, sigurnosnih politika te spoznajom i analiziranjem raznih napadačkih alata i programa, stručnjaci za informacijsku sigurnost relativno uspijevaju stvoriti adekvatne načine zaštite. Svrha završnog rada je prikazati i objasniti moguće prijetnje bankarskim informacijskim sustavima i njihovim korisnicima. Cilj završnog rada je na temelju mogućih prijetnji objasniti razne načine zaštite bankarskih informacijskih sustava i njihovih korisnika. Naslov završnog rada je: Sigurnosni aspekti i mjere zaštite informacijskih sustava. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Osnove informacijskog sustava
3. Glavni sigurnosni aspekti u bankarskom informacijskom sustavu
4. Sigurnosna politika
5. Sigurnosne prijetnje bankarskom informacijskom sustavu
6. Metode zaštite bankarskih informacijskih sustava
7. Zaključak

U drugom poglavlju, radi boljeg razumijevanja samog rada opisani su osnovni pojmovi vezani uz informacijske sustave i sigurnost, njihovi glavni elementi i principi sigurnosti informacijskih sustava.

Treće poglavlje obuhvaća glavna tri sigurnosna aspekta svakog informacijskog sustava, te moguće dodatne aspekte. Prikazani i objašnjeni su čimbenici informacijske sigurnosti.

Četvrto poglavlje obuhvaća sigurnosnu politiku i njeno definiranje. Opisan je dokument sigurnosne politike i područja koja sadrži, te primjena i provjera sigurnosne politike.

U petom poglavlju opisane su vrste mogućih prijetnji informacijskim sustavima i metode napada. Nabrojani su i detaljno objašnjeni brojni zlonamjerni programi koji se deklariraju kao potencijalna prijetnja bankarskom informacijskom sustavu.

Šesto poglavlje obuhvaća i opisuje metode zaštite bankarskih informacijskih sustava te se dijeli na tri podcjeline u kojima se opisuju fizičke, programske i organizacijske metode zaštite.

2. OSNOVE INFORMACIJSKOG SUSTAVA

Kako bi se što bolje objasnili sigurnosni aspekti i mjere zaštite informacijskih sustava i bankarskih informacijskih sustava, potrebno je pobliže objasniti neke osnovne pojmove koji su navedeni su sljedećem potpoglavlju.

2.1. Osnovni pojmovi

Kako bi se što bolje objasnili sigurnosni aspekti i mjere zaštite bankarskih informacijskih sustava, te općenito informacijskih sustava, potrebno je pobliže objasniti neke osnovne pojmove, kao što su:

- **Informacija** je podatak koji njegovom primatelju posreduje neku relevantnu novost. Drugim riječima, informacija je skup podataka (najčešće slova, znakova, simbola, zvukova), odnosno podataka koji su nam od prije poznati, koji zajedno opisuju neku drugu stvar [5].

- **Sustav** – općenito se opisuje kao skup određenih elemenata koji su međusobno povezani te tako tvore svrsishodnu cjelinu odnosno sam sustav. Svaki promatrani sustav može se opisati i kao podsustav određenog šireg, odnosno većeg sustava. Kao primjer nekog sustava mogli bi navesti jednu poslovnicu određene banke u nekome gradu, koja je ujedno i podsustav centralne banke koja može biti u nekom drugom gradu. Svaki sustav okružen je svojom okolinom, s kojom je u međudjelovanju.

- **Informacijski sustav** – je dio nekog tehnološkog i/ili organizacijskog stvarnog sustava čija je svrha permanentno opskrbljivanje potrebnim informacijama svih razina njegovog upravljanja i odlučivanja. Informacijski sustav je uvijek podsustav nekog organizacijskog sustava, koji kroz svoje temeljne aktivnosti tj. prikupljanje, obradu, pohranjivanje i distribuiranje informacija, omogućuje upravljanje tim organizacijskim sustavom ili nekim njegovim podsustavom [5].

„*Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike*“ [13].

Svaki informacijski sustav sastoji se osnovnih elemenata, odnosno komponenti koji se međusobno dopunjavaju i izvršavaju svoju danu funkciju te tako omogućuju efikasan rad sustava. Svaki IS sastoji se od šest komponenti kao što je prikazano u [4]:

1. Tehnička komponenta (engl. *Hardware*) – sklopovlje, oprema i uređaji odnosno fizički, materijalni dio informacijskog sustava prvenstveno namijenjen za obradu informacija

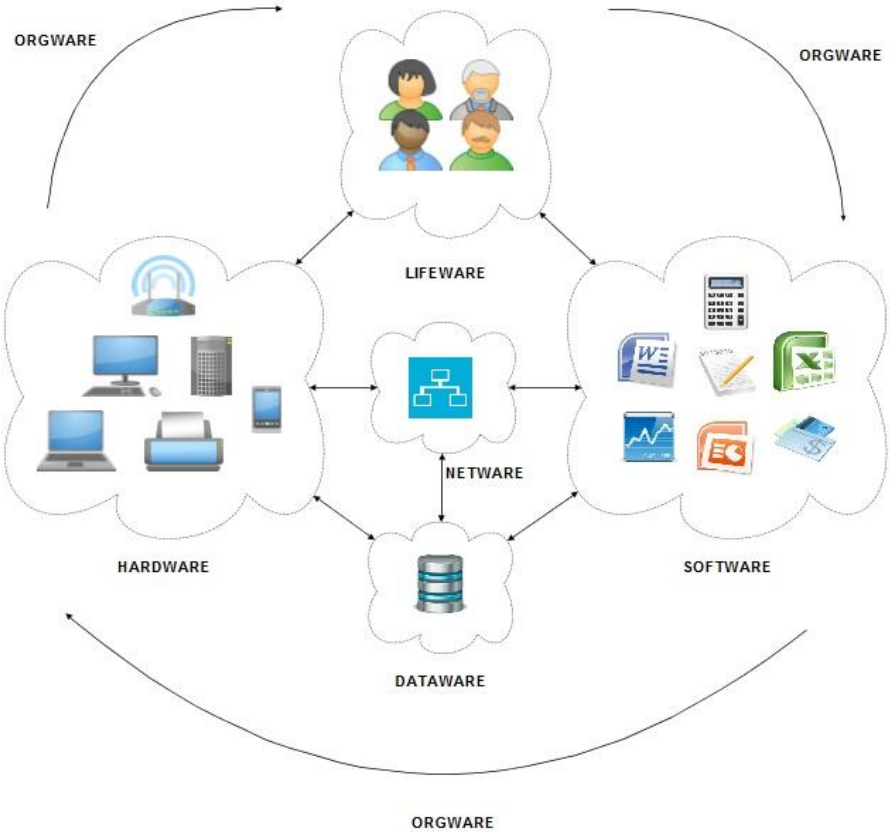
2. Programski komponenta (engl. *Software*) – programska podrška, svi programi i aplikacije koje se od strane korisnika i zaposlenika koriste unutar IS-a, a izvode se na sklopovlju, opremi i uređajima

3. Organizacijska komponenta (engl. *Orgware*) – organizacijski postupci, metode i različiti načini usklađivanja svih elemenata IS-a u funkcionalnu i efikasnu cjelinu.

4. Ljudska komponenta (engl. *Lifeware*) – ljudski faktor unutar IS-a, odnosno komunikacija stručnih zaposlenika sa krajnjim korisnicima na temelju modela zahtjev – usluga unutar IS-a

5. Mrežna/Prijenosna komponenta (engl. *Netware*) – mrežna odnosno telekomunikacija komponenta sustava koja povezuje dva najbitnija elementa IS-a, hardware i software, te samim time omogućava komunikaciju unutar sustava

6. Podatkovna komponenta (engl. *Dataware*) – obuhvaća sve podatke unutar IS-a. Glavne funkcionalnosti podatkovne komponente su skladištenje podataka unutar baza podataka i njihova distribucija.



Slika 1. *Grafički prikaz pojedinih elemenata informacijskog sustava*

Skladnost i uravnoteženi rad svih šest međusobno povezanih elemenata doprinose optimalnom funkcioniranju sustava i efektivnom ispunjenju radnih zahtjeva što je prvenstveni cilj svakog informacijskog sustava.

2.2. Pojam sigurnosti

Sigurnost je stupanj ili oblik zaštite od različitih nepovoljnih utjecaja i neželjenih događaja bilo da se radi o individualnoj osobi, materijalnim ili nematerijalnim dobrima. Sigurnost također možemo definirati kao kontrolu određene neizvjesnosti u nekom vremenu, odnosno prepoznavanje potencijalnih štetnih događaja i opasnosti te poduzimanje sigurnosnih mjera kako bi se rizik i moguće posljedice smanjile na minimum ili dovele u određene prihvatljive granice. Sigurnost se općenito dijeli na više razina: osobnu, poslovnu, nacionalnu i globalnu. U daljnjim poglavljima, od svih navedenih razina sigurnosti, najviše ćemo se fokusirati na poslovnu tj. korporativnu sigurnost u čijoj je domeni bankarska informacijska sigurnost.

„*Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda*“ [13].

Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te kako bi se osiguralo normalno i nesmetano funkcioniranje samih informacijskog sustava. Sigurnost računarskih sustava najčešće podrazumijeva sigurnost u okviru tehničke arhitekture, računala, mreže i komunikacije, dok sigurnost informacijskih sustava obuhvaća puno šire područje, koje uključuje izgradnju, implementaciju i korištenje informacijskih sustava, što je direktno povezano sa poslovnim procesima i organizacijom tvrtke, osobljem , zakonima i cjelokupnim društvom [12].

Unatoč brojnim izvorima i definicijama informacijske sigurnosti i sigurnosti informacijskih sustava, sa sigurnošću se može reći da niti jedan informacijski sustav nije u potpunosti siguran i zaštićen od raznih napada i prijetnji. Sa tim saznanjem, svaki sustav moguće je opisati terminom „sigurnosno ranjiv sustav“ koji je potrebno svakodnevno nadgledati i održavati ispravnim i funkcionalnim.

2.3. Principi sigurnosti informacijskih sustava

Prema OEDC (**OEDC** - *The Organization for Economic Cooperation and Development*) ustanovljeno je 9 principa sigurnosti IS-a, kao što je prikazano u [1]:

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

Principi organizacije za ekonomsko i korporativno upravljanje odobreni su od strane OECD ministara i predstavljaju temeljno mjerlio za osnivanje sigurnosne politike i upravljanje sustavima. Principe odlikuje njihova neobaveznost, jednoznačnost i mogućnost prilagodbe raznim sustavima. Navedeni principi bitni su za informacijsku sigurnost zbog svoje opće prihvaćenosti, kvalitete te mogućnosti korištenja kod bilo koje vrste razvoja, rada i održavanja informacijskih sustava.

3. GLAVNI SIGURNOSNI ASPEKTI

Glavni sigurnosni aspekti označavaju i definiraju osnovna načela i čimbenike potrebne za uspostavu sigurnosti informacijskog sustava. Razmatraju se i koriste neposredno nakon stvaranja informacijskog sustava i prije uvođenja u operativnu funkciju kako bi testirali i pripremili sustav te ga osigurali od mogućih prijetnji.

3.1. Načela sigurnosti bankarskog informacijskog sustava

Načela ili ciljevi sigurnosti informacijskih sustava sastoje se od tri osnovna načela koja su prikazana na slici 2, te od nekoliko dodatnih načela koja će biti navedena u daljnjem tekstu.

Slika 2. *Prikaz tri osnovna načela informacijske sigurnosti*

Za bankarske informacijske sustave, najbitnija su prva i osnovna 3 načela: povjerljivost, cjelovitost i dostupnost. Navedena načela često se nazivaju i CIA[1] trojstvo.

3.1.1. Povjerljivost

Povjerljivost (engl. *Confidentiality*) je najbitnije načelo svakog bankarskog informacijskog sustava koje se može opisati kao kombinacija tajnosti, autentičnosti i neporecivosti, odnosno kao osobina sustava koja neprestano osigurava zaštitu podataka od svih neautoriziranih korisnika, nepouzdanih entiteta i procesa.

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

Informacije se otkrivaju isključivo poznatim korisnicima koji prođu određene mjere autentikacije i provjere pri pristupu u informacijski sustav [3]. Svako neovlašteno, namjerno ili nenamjerno otkrivanje, objavljivanje ili distribuiranje podataka može dovesti do gubitka povjerljivosti sustava. Gubitak povjerljivosti sustava može dovesti do ozbiljnih povreda bankarskih propisa te za posljedicu imati gubitak povjerenja javnosti i narušavanja reputacije banke. Može doći do neželjenog otkrivanja povjerljivih informacija, ako se s informacijama koje su označene kao povjerljive ne rukuje na adekvatan način. Najčešću prijetnju povjerljivim informacijama čine [10]:

- lažno predstavljanje – korištenje povjerljivih informacija pomoću lozinke drugog korisnika
- neovlaštena aktivnost – korištenje podataka za koje osoba nema ovlasti
- napadači – otkrivanje povjerljivih informacija zbog vlastite koristi ili kako bi te informacije bile javno dostupne na javnoj mreži
- zlonamjerni programi – programi za neovlašten pristup sustavu
- kopiranje podataka na nezaštićene lokacije - povjerljivost se ugrožava tijekom kopiranja podataka na sustave s nedovoljnom razinom zaštite

3.1.2. Integritet

Integritet ili cjelovitost (engl. *Integrity*) je svojstvo podataka i procesa koje osigurava zaštitu od bilo kakve izmjene informacija i sustavnih procesa od strane neautoriziranih korisnika i autoriziranih korisnika koji nenamjerno ili namjerno premašuju svoje ovlasti. Integritet ili cjelovitost je načelo sustava koje osigurava konzistentnost podataka. Podrazumijeva točnost, ispravnost i neizmjenjivost podataka unutar sustava, te njihovu eventualnu izmjenjivost od strane ovlaštenih osoba ili ovlaštenih procesa na prihvatljiv i unaprijed određen način. U bankarskim informacijskim sustavima bitno je potvrditi identitet korisnika nekom vrstom autentikacije, kao što su pametne kartice, jednokratne lozinke, biometrijski čitači i ostalo. Treba obratiti pozornost i tijekom rukovanja podatcima kako bi se spriječile slučajne izmjene u povjerljivim podatcima, a to se postiže osiguravanjem strogo povjerljive okoline koja umanjuje mogućnost namjernih ili nenamjernih izmjena [10]. Gubitak integriteta te korištenje izmijenjenim podacima unutar i izvan sustava može dovesti do raznih prijevara i povrede financijskog stanja korisnika a i samog bankarskog sustava.

3.1.3. Raspoloživost

Raspoloživost ili dostupnost (engl. *Availability*) je svojstvo informacija i procesa koje omogućuje pristup tim informacijama i procesima te njihovu upotrebljivost, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta [2]. Raspoloživost je ključno načelo zaslužno za odgovarajuće vrijeme izvršenja tražene usluge. Glavni cilj ovog načela je što je moguće manji vremenski odziv, tj. trenutno izvršenje tražene usluge, neosjetljivost na moguće greške i probleme, prihvatljiva količina sustavnih resursa, dobro razvijen redundantni sustav u slučaju napada uskraćivanjem usluge ili prirodnih nepogoda. Kako bi informacijski sustav bio dostupan u svakom trenutku obavezan je ispravan rad:

- zaštitnog sustava
- sustava za pohranu i obradu informacija
- komunikacijskih veza putem kojih se pristupa informaciji

Unatoč tomu, dostupnost može biti narušena u slučaju:

- DoS napada (**DoS** - *Denial of Servise attack)*
- gubitka mogućnosti obrade podataka

Gubitak raspoloživosti izuzetno je problematičan za bankarske informacijske sustave jer može dovesti do nemogućnosti izvršavanja bankarskih usluga, odnosno zahtjeva krajnjeg korisnika, i samim time do narušavanja reputacije banke.

Kombinacijom prva tri osnovna načela tvore se dodatna načela kojima se upotpunjuje i dodatno opisuje svrha informacijskog sustava [6]:

- **Neporecivost** (engl. *nonrepudation*) - svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka).
- **Dokazivost** (engl. *traceability*) - svojstvo koje omogućava bilježenje i praćenje određenih aktivnosti
- **Autentičnost** (engl. *autentification*) - svojstvo koje osigurava da je identitet korisnika zaista onaj za koji se tvrdi da jest.
- **Pouzdanost** (engl. *reliability*) - svojstvo očekivanog ponašanja i rezultata

3.2. Čimbenici informacijske sigurnost

Cilj svakog informacijskog sustava je djelotvoran rad, koji je ovisan o učinkovitosti svih njegovih elemenata. Svaki element izložen je određenim mogućim prijetnjama te je bitno definirati čimbenike informacijske sigurnosti kako bi se osigurala adekvatna razina sigurnosti sustava. Među čimbenike informacijske sigurnosti ubrajamo [3]:

Prijetnja (engl. *treath*) - jest ljudska namjera ili čin koji za cilj ima iskorištavanje ranjivosti informacijskog sustava. S obzirom na njihovu mnogobrojnost, najčešće se dijele prema izvoru, što je opširnije opisano u daljnjim poglavljima.

Ranjivost (engl. *vulnerability*) – se definira kao slabost sustava, odnosno mogućnost štetnog djelovanja iskorištavajući propuste pri izradi operacijskih sustava, korisničkih programa, preglednika i drugih.

Imovina (engl. *asset*) – jest bitan čimbenik informacijske sigurnost jer podrazumijeva sve materijalne i nematerijalne stvari koji imaju određenu vrijednost za određeni informacijski sustav. Dijeli se na:

- Informacijsku (sistemska dokumentacija, korisničke informacije, baze podataka)
- Softversku (aplikacijski softveri i operativni sustavi)
- Fizičku imovinu (računalna oprema, mrežna oprema, komunikacijska oprema, fizički mediji, ostala popratna tehnička oprema)

Rizik (engl. *risk*) – vjerojatnost ostvarenja svjesnog, neželjenog događaja. Najčešće se očituje u prijenosu osjetljivih bankarskih informacija. Za bankarske informacijske sustave rizik je veoma bitno pravovremeno utvrditi, ispravno njime upravljati te ukoliko je moguće, minimizirati ga.

Utjecaj (engl. *effect*) – najčešće korišten kao negativno mjerilo količine štetnog djelovanja na sustav.

Posljedica (engl. *consequence*) – ishod, odnosno stanje nakon neželjenog i štetnog događaja koje se za informacijski sustav najčešće manifestiraju kao dodatni financijski izdatci.

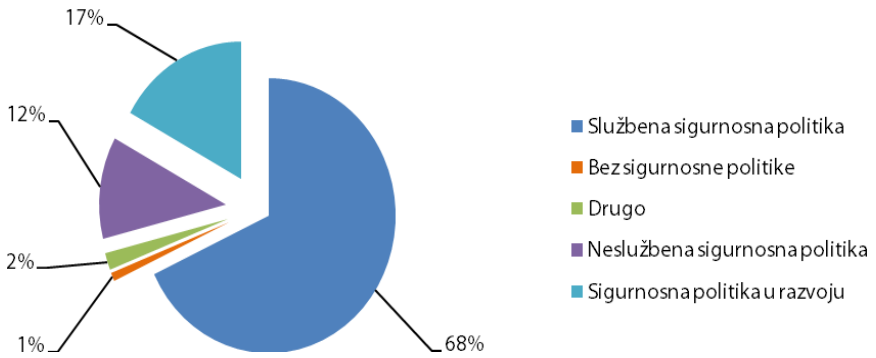
4. SIGURNOSNA POLITIKA

Informacijski sustavi sadrže razne podatke kojima se koriste zaposlenici i razni korisnici. Podaci kojima se koriste zaposlenici i korisnici, najčešće ne trebaju biti javno dostupni, te se kao takvi ne smiju javno objavljivati, mijenjani ili dijeljeni bez odobrenja rukovoditelja te je važno uvesti određena pravila i upute kako bi navedeni uvjeti bili zadovoljeni. Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti [19].

4.1. Sigurnosna politika

Osigurati sigurnost sustava nije moguće samo upotrebom tehnoloških rješenja, te se iz tog razloga uvode dodatne mjere, među kojima je i definiranje sigurnosne politike. Kako bi se zaštitile vrijednosti informacijskog sustava koje uključuju podatke, opremu i programsku podršku, određuju se prihvatljivi i neprihvatljivi načini ponašanja, što predstavlja ujedno i primarnu ulogu sigurnosne politike.

Od iznimne je važnosti da se od strane poslovodstva u pogledu sigurnosti odrazi stav u kojima iskazuju veliku potporu svim subjektima poslovnog sustava kada je riječ o sigurnosti. Od poslovodstva se očekuje iskazivanje podrške i predanosti prema sigurnosti informacija kroz izradu, doradu, naglašavanje i podržavanje politike sigurnosti u cijeloj organizaciji. Na slici 3 prikazana je analiza uvedenosti sigurnosne politike u ustanove koje posjeduju informacijski sustav [10].



Slika 3. *Uvedenost sigurnosne politike u ustanove* [10]

Temeljni okvir za upravljanje sigurnošću informacijskog sustava banke je politika sigurnosti informacijskog sustava. Navedena politika bi trebala održavati opće prihvaćena načela sigurnosti.

Prema politici sigurnosti informacijskog sustava banka propisuje i primjenjuje interne akte koji se odnose na sve aspekte sigurnosti informacijskog sustava. Politika sigurnosti informacijskog sustava sadrži sljedeće:

- Cilj i opseg politike sigurnosti informacijskog sustava
- Načela upravljanja sigurnošću informacijskih resursa
- Opće i posebne odgovornosti koje se odnose na sigurnost informacijskog sustava

Politika sigurnosti informacijskog sustava mora sadržavati principe i načela upravljanja sigurnošću resursa informacijskog sustava, te odgovornosti koje se odnose na sigurnost informacijskog sustava. Banka imenuje osobu odgovornu za praćenje provođenja sigurnosne politike, te donosi i upoznaje korisnike informacijskog sustava s tom politikom. Tako se osigurava adekvatna razina sigurnosti informacijskog sustava, te obuhvaća područja upravljačke, logičke i fizičke zaštite resursa informacijskog sustava u skladu s veličinom i kompleksnosti sustava.

4.2. Dokument sigurnosne politike

Dokument sigurnosne politike treba biti odobren od strane upravitelja, objavljen i poslan svim zaposlenicima i korisnicima kojima je namijenjena. Politika treba odražavati stavove rukovoditelja i definirati koncept upravljanja sigurnosti informacija.

Dokument sigurnosne politike, prema [2] treba sadržavati:

- definiciju informacijske sigurnosti, njezine glavne ciljeve i opseg te važnost sigurnosti kod zajedničkih informacija informacijskog sustava
- izjavu o namjerama uprave, odnosno rukovodstva koje će podupirati ciljeve i principe informacijske sigurnosti u skladu s poslovnom strategijom
- okvir za uvođenje kontrola, kao i strukturu procjene rizika i upravljanja rizikom
- objašnjenje i opis sigurnosne politike, načela, normi i zahtjeve od posebnog interesa koje organizacija treba usvojiti, a to su:

  - suglasnost sa zakonskim, pravnim i ugovornim zahtjevima
  - edukacija o sigurnosti, svijesti o sigurnosti i sigurnosni trening
  - upravljanje kontinuitetom poslovanja
  - posljedice nepridržavanja i narušavanja sigurnosne politike

- definiciju općih i specifičnih odgovornosti u procesu upravljanja sigurnošću, uključujući i prijavu sigurnosnih incidenata
- referentna dokumentacija koja podupire ovu politiku tj.razrađena sigurnosna politika i procedura za specifične informacijske sustave ili sigurnosna pravila prema kojima moraju postupati korisnici

Ispravno i adekvatno definiranim dokumentima, njihovim pridržavanjem, kontinuiranom revizijom i dopunjavanjem osigurava se kvalitetna sigurnosna politika koja je temelj za opću sigurnost informacijskih sustava i njihov ispravan rad.

4.3. Primjena i provjera sigurnosne politike

Sigurnosna politika primjenjuje se tamo gdje je potrebno osigurati tri svojstva informacija koja sadrži određeni sustav, a to su:

- Integritet,
- Povjerljivost,
- Dostupnost.

Isto tako, mehanizmi zaštite i sprječavanja su podijeljeni na tri osnovne razine:

- fizička sigurnost, pod kojom se podrazumijeva sigurnost računalne opreme i podataka, te je ovo i najvažnija razina mehanizma zaštite,
- osobna sigurnost koja predstavlja zaštitu korisnika i povjerljivih informacija o korisniku,
- sigurnost organizacije, koja proizlazi iz prvih dviju razina.

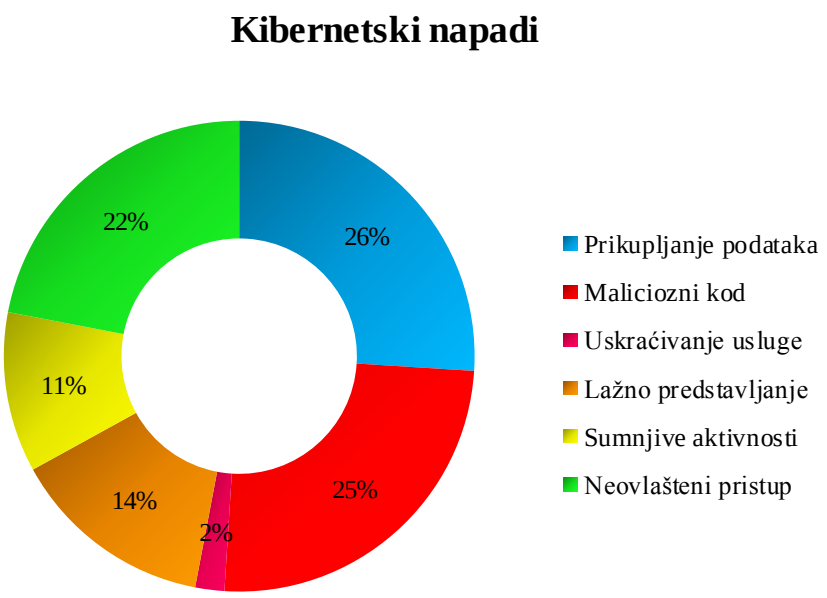
Kako bi se ostvarilo da sigurnosna politika bude jednako učinkovita kao i trenutku kada je osnovana, potrebno je uzeti u obzir promjene koje su se u tom periodu dogodile, te shodno tome prilagoditi pravila i procedure. Tijekom provjere sigurnosti treba uzeti u obzir sljedeće:

- rezultate neovisnih ispitivanja
- izvješća o sigurnosnim incidentima
- promjene vezane uz ranjivosti i prijetnje informacijskim sustavima
- promjene koje mogu pozitivno utjecati na sigurnost informacija
- preporuke stručnih organizacija

U slučaju ako se parametri u okruženju organizacije nisu promijenili, svejedno treba sigurnosnu politiku prilagođavati na godišnjoj bazi jer je moguće da uvedena sigurnosna politika ne odgovara organizaciji u cijelosti. Provjeru sigurnosne politike provodi se jednom godišnje. Ako je u međuvremenu došlo do ugradnje nove opreme ili u slučaju incidenata, potrebno je provjeru češće provoditi [10].

5. SIGURNOSNE PRIJETNJE BANKARSKOM INFORMACIJSKOM SUSTAVU

Bankarske povjerljive korisničke informacije i elektronički novac izložen je raznim vrstama prijetnja. Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti financijska šteta [16]. Šteta koja može biti materijalna ili ne materijalna, može nastati kao posljedica ostvarenja kibernetskih[2] napada (prikupljanja podataka, upotrebe malicioznog koda, uskraćivanja usluge, lažnog predstavljanja, neovlaštenog pristupa i slično) kao što je prikazano na slici 4.



Slika 4. *Grafički prikaz kibernetskih napada*, Izvor: [28]

Prijetnje se mogu klasificirati i podijeliti na razne načine, ali najčešća podjela je vrsta prijetnji prema izvoru. Kako bi se što bolje odabrale adekvatne mjere zaštite, potrebno je točno utvrditi prijetnje bankarskom informacijskom sustava kao i način rada potencijalno opasnih zlonamjernih programa te njihov način infiltracije.

[2] Kibernetika – znanost o općim zakonitostima upravljanja informacijama

5.1. Vrste prijetnji

Bankarski informacijski sustavi svakodnevno su izloženi raznim vrstama prijetnji. Prema raznim istraživanjima, ustanovljeno je da je najčešća vrsta prijetnje prema informacijskim sustavima ljudski faktor, odnosno ljudska nenamjerna pogreška (Tablica 1).

Tablica 1. *Vrste mogućih prijetnji prema njihovom izvoru*

Prirodne prijetnje	**Namjerne prijetnje ljudi**	**Nenamjerne prijetnje ljudi**	**Oprema**
meteorološke nepogode, geofizičke nepogode, sezonski fenomeni, astrofizički fenomeni, biološke prijetnje,[8]	gomilanje prometa, neautorizirani pristup, prisluškivanje, otkrivanje podataka, sabotaža, maliciozni programi , namjerno oštećivanje imovine, zlouporaba ovlasti	nedovoljna educiranost, nepravilno rukovanje, nemar i nepažnja, nedisciplina, nenamjerno oštećenje fizičke imovine, nenamjerno brisanje podataka, neadekvatna organizacija	električni kvarovi i neispravnosti, tvorničke greške, prestanak napajanja, ispadi opreme, prekid komunikacije, zračenja

Izvor: [12]

S obzirom na izvor prijetnje, ljudski faktor koji se manifestira kao namjerna ili nenamjerna prijetnja pokazao se kao najučestaliji. Prijetnje uzrokovane kvarom opreme nalaze se na drugom mjestu po učestalosti kao vrsta prijetnji informacijskom sustavu, te prirodne prijetnje na trećem. Spoznajom vrste prijetnje i analizom njena uzorka, moguće je izraditi primjerene metode zaštite te na taj način zaštiti informacijskih sustav od poznatih potencijalnih prijetnji i njihovih posljedica [20].

5.2.Metode napada na informacijski sustav

5.2.1. Metoda napada prekidanjem

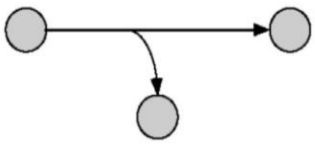
Metode napada prekidanjem (engl. *interruption*) usluge onemogućavaju korisniku normalno i nesmetano korištenje web usluga, a samim time i uslugama internet bankarstva [1]. Nakon što je napadač pridobio pristup korisničkoj mreži, može učiniti sljedeće:

- Prikriti određene sistemske informacije kako se ne bih otkrila napadačeva prisutnost, te mogućnost dodatnih napada
- Slanje nevažećih podataka aplikacijama i mrežnim servisima što uzrokuje njihovu nestabilnost i mogućnost prestanka rada
- Preplavljanje računala ili cijele korisničke mreže s mrežnim prometom što dovodi do gašenja računala ili mreže zbog preopterećenja.
- Blokiranje prometa što rezultira gubitkom pristupa mrežnim resursima

Slika 5. *Prekidanje usluge između dva korisnika*. Izvor: [1]

5.2.2. Metoda napada presretanjem

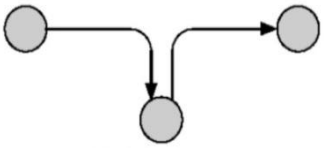
Napadi presretanjem (engl. *interception*) su napadi koji se događaju posredstvom treće osobe u komunikaciji, tako da je treća strana u mogućnosti aktivno pratiti, bilježiti i transparentno kontrolirati komunikaciju (slika 6). Glavna odlika ove vrste napada je mogućnost preusmjeravanja podataka na mrežnim slojevima prijenosa [29]. Napadači koji se koriste presretanjem podataka, ubacuju se u komunikaciju između dvoje ljudi, te preusmjeravaju poruke na svoje računalo i predstavljaju se kao osoba koja je u razgovoru, dok od druge osobe pokušavaju izvući što je moguće više korisnih informacija.



Slika 6. *Presretanje podataka od treće strane*. Izvor: [1]

5.2.3. Metoda napada izmjenom podataka

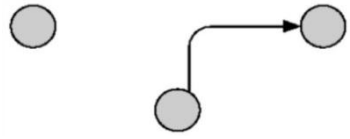
Izmjena podataka (engl. *modification*) je dodatna vrsta napada kojom se napadač služi kako bi izmijenio informacije između pošiljatelja i primatelja poruke. Najčešće neposredno nakon presretanja poruke, napadač bez znanja korisnika izmjenjuje njen sadržaj u svoju korist (slika 7). Ova vrsta napada je izuzetno štetna, pogotovo kad je riječ o raznim novčanim transakcijama putem interneta, kao što su internet bankarstvo, kupovina preko pay pal-a i slično [29].



Slika 7. *Izmjena podataka u komunikaciji između dva korisnika od treće strane*. Izvor: [1]

5.2.4. Metoda napada proizvodnjom podataka

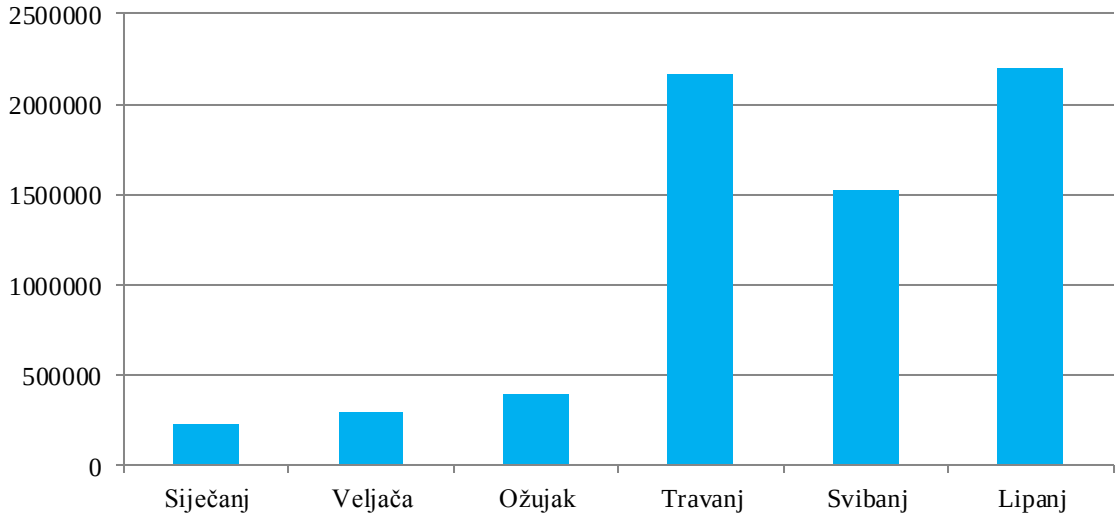
Metoda napada proizvodnjom (engl. *fabrication*) i umetanjem lažnih podataka kao i ostale metode, osmišljena je isključivo za krađu i zlonamjerno iskorištavanje korisničkih podataka. Za razliku od napada presretanjem, napad proizvodnjom podataka orijentiran je isključivo na aplikacijski sloj mreže. Napadač iskorištava slabosti aplikacija i operativnog sustava te je u mogućnosti dobiti djelomičnu ili potpunu kontrolu nad aplikacijama, sistemskim procesima ili mrežom korisnika.



Slika 8. *Proizvodnja lažnih podataka s ciljem krađe podataka*. Izvor: [1]

5.3. Zloćudni bankarski programi

Zloćudni bankarski programi ili jednostavno maliciozni programi je sveukupni naziv za sve zlonamjerne i štetne programske alate kojima se služe razni napadači na bankarske i ostale informacijske sustave kako bi na ilegalan način došli do osjetljivih korisničkih podataka te ih iskorištavali za vlastitu korist. S razvojem tehnologija i sigurnosnih mehanizama u neprekidnom su razvoju i zloćudni bankarski programi te se bilježi i sve veći porast napada na bankarske informacijske sustave (grafikon 1).



Grafikon 1. *Prikaz naglog porasta broja malicioznih programa u bankarskim informacijskim sustavima nakon prvog kvartala 2015.godine*

Izvor: [17]

Kako bi se bankarski informacijski sustavi i njihovi korisnici što je moguće bolje zaštiti od štetnog djelovanja zlonamjernih malicioznih programa, potrebno je detaljno proučiti način rada malicioznih programa, njihove mogućnosti infiltracije u sustav i moguće posljedice. U daljnjem tekstu navedeni su poznati i učestali napadački alati i maliciozni programi.

5.3.1. Programi za praćenje unosa znakova s tipkovnice i bilježenjem stanja na radnoj površini računala

Programi za praćenje znakova (engl. *Keyloggers*) su programi koji imaju mogućnost praćenja i bilježenja svake aktivnosti korisnikovog unošenja znakova s tipkovnice i općenito rada na računalu u cilju krađe brojeva kartica, pinova, korisničkih podataka i sl.. Često se još nazivaju špijunski programi ili jednostavno *Keyloggeri*. Prema načinu implementacije, dijele se u dvije skupine kao što je vidljivo na [7]:

- fizički uređaj koji se ugrađuje u sklopovlje računala
- alati u obliku programskih paketa

Fizički uređaj za praćenje je veoma malih dimenzija, te se umeće u tipkovnicu i spaja na ploču tipkovnice koja se putem kabela spaja s računalom. Uređaj funkcionira tako da bilježi svaki pritisak tipke na tipkovnici i zabilježeni podatak sprema u svoju memoriju. Vrlo rijetko je korišten zbog nepraktičnosti i izuzetnim teškim očitavanjem traženih podataka iz memorije uređaja.

Današnji *keyloggeri* u gotovo svim slučajevima su softverskog oblika (slika 9), odnosno u obliku programskih paketa koji su lako dostupni i moguće ih je besplatno preuzeti na raznim P2P[3] stranicama i forumima. Programski *keylogger* je sveobuhvatniji od fizičkog uređaja za praćenje unosa znakova s tipkovnice jer pri instalaciji ima mogućnost samokonfiguriranja unutar operacijskog sustava. Svoju svrhu postiže presretanjem podataka o svakom pojedinom unosu znaka s tipkovnice te je sprema u određeni, sakriveni dio memorije na računalu. *Keylogger* je programski proces koji radi u pozadini, te ga je moguće konfigurirati tako da je u potpunosti nevidljiv korisniku.

[3] P2P - (eng. *Peer to peer*) vrsta računalne mreže koja se temelji na jednakosti svih korisnika

Slika 9. *Prikaz korisničkog sučelja Award keylogger-a* [18]

Dodatne funkcionalnosti programskog Keyloggera su:

- „prtsc – *PrintScreen*“ opcija – fotografiranje, odnosno dohvaćanje trenutnog stanja radne površine računala i spremanje u obliku slike (*jpg, png file*) koje je moguće podesiti s vremenskom odgodom i tajmerom.
- „s&s – *Save and Send*“ – spremanje podataka na računalo korisnika i prikriveno slanje putem lokalne mreže i/ili javne mreže napadaču na udaljeno računalo (eng. *dropzone*)

Keyloggeri su relativno kompleksni špijunski programi kojima je najveći nedostatak bilježenje dosta velike količine podataka u kojoj je za napadača teško odrediti koji su podaci korisni a koji nisu. Iz tog razloga, *keyloggeri* se najčešće koriste u kombinaciji s drugim programima koji omogućavaju filtriranje podataka. Neki od najpoznatiji *keyloggera* koji se besplatno mogu preuzeti na raznim stranicama i web servisima su: *Ardamax*, *Award*, *Elite*, *Ghost*, *KGB*, *Steel*, *The best keylogger* i drugi.

5.3.2. Bankarski trojanski konj

Trojanski konj (engl. *Trojan horse*) je maliciozni program, odnosno prikriveni dio koda u određenom računalnom programu, namijenjen prikupljanju korisničkih podataka. Iz očitih razloga, svoj naziv dobio je po konceptu trojanskog konja iz grčke mitologije. Dok se u današnje vrijeme često koristi naziv „Trojan" ili „Trojanac".

Trojanski konj kao dio programskog koda, najčešće se izrađuje od strane zlonamjernih računalnih programera, tj. takozvanih „hakera", te se pri izradi umeće u program najčešće zabavnog sadržaja koji je zanimljiv osobnim korisnicima računala. Korisnik s određenih web stranica preuzima instalacijski paket, te ga kroz proces instalacije raspakirava na svoje računalo. Prvi prvom pokretanju izvršne datoteke korisnik nesvjesno pokreče i zlonamjerni dio programa, odnosno trojanskog konja, te tako omogućuje napadaču pristup određenim podacima sa svoga računala. Napadač uz pomoć trojanskog konja je u mogućnosti prikupljati korisničke podatke poput brojeva kreditnih kartica, raznih lozinki za pristup određenim web servisima i dr., pristupiti sistemskim datotekama i izmjenjivati ih, te u krajnjim slučajem čak i u potpunosti preuzeti kontrolu nad korisničkim računalom.

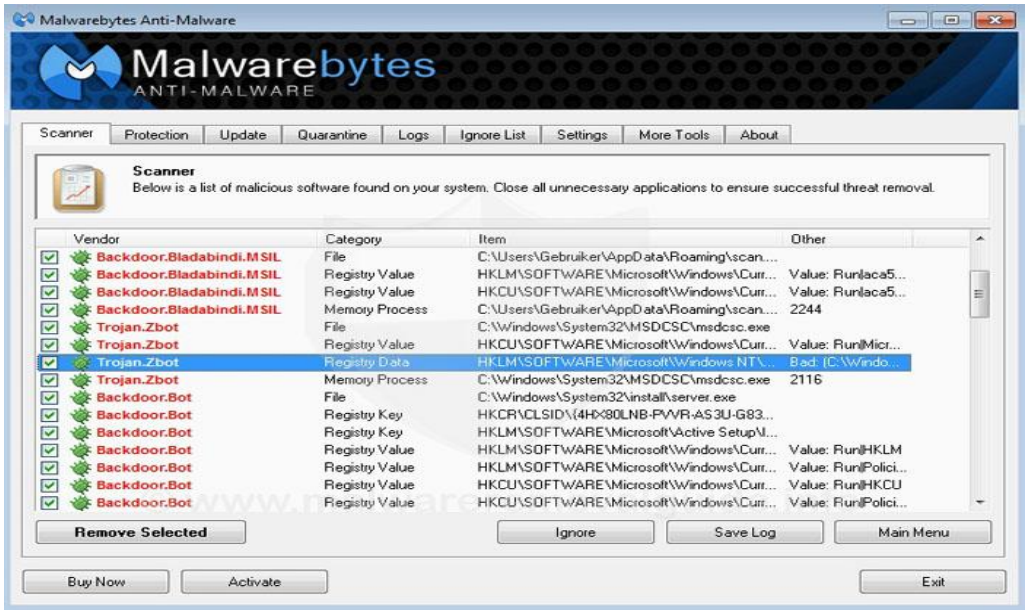
Na sličnom konceptu funkcioniraju i bankarski trojanci, koji su deklarirani kao najopasnija vrsta trojanskog konja zbog njihove specijaliziranost za krađu za podataka koji se koriste za bankarske transakcije putem interneta. Kao takvi, posjeduju napredne tehnike za izbjegavanje njihove detekcije od strane antivirusnih alata. Unatoč tomu, s adekvatnim alatima i dalje ih je moguće detektirati (slika 10). Glavna razlika između jednostavnih trojanskih konja i bankarskih je u lokaciji infiltracije.

Bankarski trojanci se najčešće integriraju u korisnički web preglednik putem naizgled korisnih ekstenzija tj. dodataka za web preglednik. Takav postupak integriranja trojanaca naziva se HTML[4] (engl. *Hyper-Text Markup Language*) injekcija. „*HTML injekcija je ubacivanje HTML koda u odgovor web poslužitelja kako bi se izmijenio sadržaj web stranice koju korisnik učitava*" [7].

[4] HTML – programski jezik za uređivanje i oblikovanje izgleda web stranica

Takav postupak omogućava napadaču izmjenu web stranice određene banke u realnom vremenu, prikrivanjem starih i dodavanjem novih dijaloških polja kojima se korisnika traži da upiše osjetljive podatke poput brojeva kreditnih kartica, korisničkih PIN-ova[5], OTP[6] lozinki, TAN[7] brojeva, brojeva osiguranja, e-mail-ova i slično.

Trojanski konj aktivira se čim korisnik pristupi web adresi banke, te nakon unosa osjetljivih podataka javlja korisniku da je pogrešno unio određene pristupne podatke, dok u međuvremenu iste, ukradene podatke šalje napadaču [9]. Zbog velike količine korisničkih podataka koja se prikuplja bankarskim trojanskim konjima, najčešće se uz njih koriste i dodatni maliciozni alati poput keyloggera i različitih programa za filtriranje URL[8] adresa koje korisnik koristi za pristup internet bankarstvu kako bi napadaču olakšali pronalaženje točno traženih podataka potrebnih za krađu i slanje žrtvinog novca na druge bankovne račune [7].



Slika 10. *Detekcija trojanskog konja „Zeus" uz pomoć antivirusnog programa* [26]

Bankarski trojanski konji najčešće su programirani u programskom jeziku *Visual Basic*, te ih je moguće kupiti i preuzeti na crnom tržištu odnosno „podzemlju" interneta. Neki od najpoznatijih bankarskih trojanskih konja su: *Haxdoor*, *Sinowal*, *Bancos*, *Limbo*, *Zeus* i drugi.

[5] PIN (eng. *Personal identification Number*) – osobni identifikacijski broj
[6] OTP (eng. *One Time Password*) – jednokratne lozinke
[7] TAN (eng. *Transaction Authentication Number*) – autentikacijski broj transakcije
[8] URL (eng. *Uniform Resource Locator*) – usklađeni lokator resursa

5.3.3. Otimanje sjednice

Otimanje sjednice (engl. *Session hijacking*) podrazumijeva napad otimanja tekuće sesije slanja novca putem internet bankarstva. Prilikom svakog korisničkog pristupa internet bankarstvu, korisnikovo računalo postaje bankovni terminal jer omogućuje prihvat i slanje novca. Otimanje sjednice, tj. tekuće sesije je također jedna od mogućih funkcionalnosti trojanskog konja, do koje dolazi kada trojanski konj preuzme administratorske podatke određene bankarske web stranice, te time dobiva mogućnost preuzimanja, izmjene i preusmjeravanja transakcija. Napadač dobiva pristup poslanom ispunjenom virmanu, odnosno posebnom nalogu za prijenos novca putem internet bankarstva od strane korisnika prije nego li stigne do centralnog bankarskog sustava odakle se šalje naredba za izvršavanje transakcije. Na taj način, napadač je u mogućnosti izmijeniti iznos transakcije, broj računa na koji se šalje novac ili u potpunosti izraditi novi nalog za prijenos novca [7].

5.3.4. Preuzimanje kontrole nad podacima u predlošcima

Preuzimanje kontrole nad podacima u predlošcima (engl. *Form grabbing*) trenutno je jedna od najraširenijih i najaktualnijih zlonamjernih metoda za prikupljanje korisničkih podataka. Preuzimanje podataka iz predložaka tijekom godina se pokazalo se kao veoma efektivna tehnika za krađu korisničkih podataka prilikom korištenja usluga poput internet bankarstva. Odlikuje se po tome što zaobilazi sigurnosne mehanizme web preglednika te se korisnički podaci izvlače iz predložaka web stranica, tako da je poprilično jednostavno odrediti koje su informacije korisne, poput korisničkih imena i lozinki. Osnovna ideja je presretanje korisničkih podataka koji se upisuju u predloške pri pristupu određenim web stranicama i servisima prije nego su oni poslani sa korisničkog računala prema udaljenom poslužitelju [31].

Tehnika preuzimanja korisničkih podataka iz predložaka koristi dvije osnovne metode kako bi ostvarila svoj cilj, odnosno kako bi na nezakonit način preuzela osjetljive korisničke podatke:

1. Metoda presretanja podataka uz pomoć „*sniffer*“[9] alata za hvatanje podataka unutar mreže. Nedostatak ove metode jest ograničenost njena djelovanja samo na nekriptirane komunikacije.

2. Druga metoda koristi „*hooking*“[10] tj. prispajanje koje se izvršava u suradnji s već postojećim malicioznim programom na računalu korisnika, tako da se maliciozni program prispaja na preglednički DLL[11] (eng. *Dinamic Link Libraries*) u cilju preuzimanja podataka iz predloška prije nego su oni budu poslani na udaljeni poslužitelj. Ako je ova metoda izvedena ispravno, korisnički podaci mogu biti ukradeni i prije nego budu kriptirani te je napadač u mogućnosti izmijeniti i urediti izgled web stranice koje korisnik posjećuje i izvršiti ilegalne operacije predstavljajući se kao korisnik. Budući da maliciozni program ostaje na žrtvinom računalu i nema izravnu interakciju s mrežnim prometom, ova vrsta napada je efektivna čak i ako se provode ozbiljniji oblici zaštite podataka poput dvostruke autentikacije prilikom prijave na npr. stranice internet bankarstva. Ovu metodu otuđenja korisničkih podataka moguće je ostvariti uz pomoć raznih „*hooking*“ alata i malicioznih programa a najčešće je korištena kao prividno koristan dodatak web pregledniku.

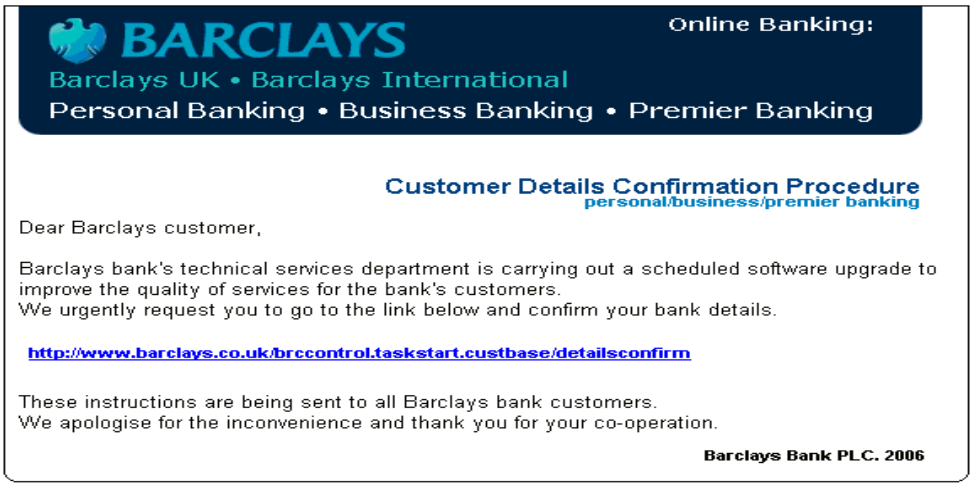
[9] Sniffer alati – alati za praćenje mrežnog prometa
[10] Hooking alati – programski kod koji ima mogućnost nadovezivanja na DLL web preglednika
[11] DLL – biblioteke dinamičkog linka dio su Windows operativnog sustava koje pomažu u pokretanju i izvršavanju aplikacija

5.3.5. Phishing

Phishing je vrsta napada putem elektroničke pošte upotrebom lažnih poruka s ciljem prevare i navođenjem korisnika na dolazak na lažne web stranice i na otkrivanje vlastitih osobnih podataka. Sam naziv odlazi od engleske riječi „*fishing*“ što znači „pecanje“ kojom se metaforički opisuje postupak kojim napadači mame korisnike elektroničke pošte kako bi dobrovoljno otkrili osobne podatke [21]. Od osobnih podataka, napadači najčešće putem lažnog email-a traže korisnička imena, razne lozinke, brojeve kreditnih kartica, PIN brojeve, brojeve osiguranja i slično.

U bankarskom informacijskom 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 [22]. 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.

Sadržaj email-a, kao što je prikazano na slici 11, najčešće pokušava navesti zaposlenike da putem vlastitog korisničkog imena i lozinke potvrde valjanost njihovog poslovnog računa tako da preko poveznice pristupe lažnoj web stranici banke.



Slika 11. *E-mail poruka sa lažnim predstavljanjem banke* [30]

Ako samo jedan zaposlenik bude prevaren, napadač se uz pomoć dobivenih podataka može predstavljati kao prevareni zaposlenik i preko socijalnog inženjeringa u mogućnosti je doći do drugih osjetljivih podataka.

Za razliku od običnog *phishinga,* email poruke *spear phishinga* se uvijek pojavljuju kao poruke koje dolaze od povjerljivog izvora, što otežava detekciju mogućnosti prevare. Uspjeh *spear phishinga* ovisi od tri glavne komponente:

- Izvor poruke uvijek se mora prikazivati kao pouzdan izvor
- Podaci unutar poruke uvijek moraju biti potkrijepljeni stvarnim informacijama
- Zahtjev od korisnika mora biti logički utemeljen i realan [21]

Prema „*Kaspersky Lab study*“ izvješću iz 2014.-te godine na temelju prikupljenih podataka, zaključeno je kako je trećina od svih phishing napada upravo usmjerena na financijske organizacije, na što se najveći odnosi upravo na bankarske informacijske sustave i njihove korisnike.

5.3.6. Pharming

Pharming je napad sličan phishingu napadu kod koje se korisnika preusmjerava s legitimne web stranice na lažnu koja je pod kontrolom napadača. Za razliku od *phishinga, pharming* se ne oslanja na elektroničku poštu, već na trojanske konje koji se infiltriraju u korisnikov sustav ili web preglednik. Sam napad počinje se odvijati prilikom korisnikovog pristupa i prijave na internet bankarstvo nakon čega se ga pri učitavanju prave web stranice automatski preusmjerava na lažnu web stranicu banke gotovo identičnog izgleda ali drugačije URL adrese. Neoprezan korisnik popunjava dijaloške okvire svojim pristupnim podacima te nakon toga s lažne web stranice dobiva poruku da je pogrešno unio svoje podatke i ponovno ga se preusmjerava na originalnu stranicu banke kako ne bi posumnjao da se radi o prevari i krađi podataka. Na taj način napadaču omogućava nesmetan pristup svojim bankovnim računima. *Pharming* napadi su dosta kompleksniji i teže izvedivi od phishing napada se te rjeđe koriste. Unatoč tomu, uspješni *pharming* napadi uzrokuju znatno veće posljedice te kako bi ih se spriječilo, poželjno je poduzeti adekvatne mjere zaštite [7].

5.3.7. Distribuirani napadi uskraćivanjem usluge

Distribuirani napad uskraćivanjem usluge (engl. *Distributed Denial of Service*) je tehnika napada koja izravno utječe i narušava dostupnost informacijskog sustava, tj. treće načelo informacijskog sustava. Svaki računalni i informacijski sustav posjeduje svoja ograničenja, koja se umanjuju korištenjem redundancije u više segmenata. Unatoč redundanciji i dalje postoje određena ograničenja koja elemente informacijskog sustava i dalje čine ranjivima na napade uskraćivanjem usluge.

Koncept DDoS napada je da više sustava nadvladava jednog. Drugim riječima, DDoS napad nastaje aktivnim umreženjem više zaraženih računala određenim malicioznim kodom. Takav skup računala naziva se botnet, koji se koristi kao sredstvo za napad tehnikom slanja prekomjernih legitimnih zahtjeva prema ciljanom sustavu ili prema web poslužitelju što dovodi do prekida, odnosno uskraćivanja usluge [25].

Ovakva vrsta napada koja izričito utječe na načelo dostupnosti informacija, izuzetno je opasna za bankarske informacijske sustave jer dovodi do općeg nepovjerenja i nezadovoljstva korisnika bankarskim uslugama što također može rezultirati velikim financijskim gubitcima i u najgorim slučajevima gubitkom korisnika.

6. METODE ZAŠTITE U BANKARSKOM INFORMACIJSKOM SUSTAVU

Kako bi se postigla maksimalna sigurnost bankarskog informacijskog sustava potrebno je obratiti pažnju na [10]:

- fizičke metode zaštite,
- programske metode zaštite i zaštite podataka
- organizacijske metode zaštite

6.1. Fizičke metode zaštite

Fizička sigurnost bankarskog informacijskog sustava jedna je od ključnih komponenti cjelokupne zaštite informacijskog sustava. Fizičku sigurnost podrazumijeva tri osnovna aspekta kako bi se osigurala adekvatna zaštita, a to su:

- zaštita informacijske opreme i uređaja
- zaštita okoline
- kontrola fizičkog pristupa

6.1.1. Fizička zaštita informacijske opreme i uređaja

Fizička zaštita informacijske opreme i uređaja objedinjuje sigurnosne metode zaštite za svaki pojedini uređaj i cjelokupnu informacijsku opremu unutar informacijskog sustava. Prvenstveno se odnosi na zaštitu „*server*“, odnosno poslužiteljskih računala koja su najbitnija za sve informacijske sustave pa tako i bankarski informacijski sustav jer sadrže i upravljaju svim informacijama unutar sustava. Poslužiteljska računala najčešće se fizički odvajaju od svih ostalih uređaja i iz njihove neposredne blizine te se pohranjuju u posebne prostorije i posebna, najčešće fiksirana metalna kućišta (Slika 12), koja je moguće zaključati kako bi bili izvan dosega neovlaštenih radnika i drugih korisnika bankarskih ustanova.

Slika 12. *Primjer fizičke zaštite poslužiteljskih računala* [27]

Fizička zaštite informacijske opreme također se odnosi na opremu i uređaje kojima se služe zaposlenici unutar određenog bankarskog sustava. Pod opremu i uređaje podrazumijevamo sve elektroničke uređaje koji izvršavaju određenu funkciju kako bi osigurali uredno poslovanje bankarskih sustava a kojima se služe zaposlenici, poput: računala za poslovanje, POS[12] uređaja za ispis potvrda i računa, digitalni potpisnici, VOiP[13] telefoni, uređaji i predmeti za transfer novca unutar poslovnica te ostali uredski uređaji [8].

Obavezna je edukacija zaposlenika i korisnika o pravilnom načinu korištenja opreme i uređaja kako bi se osigurala dugotrajnost i ispravan rad istih. Dodatno, uređaje poput stolnih i prijenosnih računala, moguće je zaštiti posebnim zaštitnim kablovima s lokotom ili lozinkom, dok se ostali uređaji najčešće pohranjuju u posebne zaštićene odjeljke unutar svakog pojedinog ureda.

[12] POS (engl. *Point Of Sale*) je uređaj koji omogućuje plaćanje robe i usluga
[13] VoIP – (engl. *Voice over Internet Protocol*) je oznaka za tehnologiju koja omogućava prijenos govora preko javne mreže.

6.1.2. Fizička zaštita okoline informacijskog sustava

Fizička zaštita okoline informacijskog sustava objedinjuje sve mjere i metode potrebne za zaštitu od utjecaja nepovoljnih vanjskih čimbenika na informacijski sustav. Kod zaštite okoline informacijskog sustava prvenstveno se misli na okolinu računalno pohranjenih osjetljivih podataka, tj. poslužiteljskih računala. Kao što je ranije rečeno, poželjno je da budu pohranjena unutar metalnih kućišta kojima je ograničen pristup, koja su toplinski regulirana i ujedno vodootporna te zaštićena od bilo kakvih vanjskih fizičkih utjecaja. Sam pristup prostorijama u kojima se čuvaju poslužiteljska računala trebao bi kao i bankarski centralni sef, biti zaštićen posebnim ulaznim vratima koja je moguće otvoriti jedino posebnim ključem ili digitalnom lozinkom, biti posebno nadgledan putem videonadzora, zaštićen raznim alarmnim sustavima te po mogućnosti osobno zaštićen od strane ljudskog faktora, tj. zaštitarom [8].

6.1.3. Kontrola fizičkog pristupa

Kontrola fizičkog pristupa obuhvaća svako ograničavanje pristupa određenim prostorima i računalnim resursima unutar bankarskog sustava. Pristup se ograničava najčešće prostorijama u kojima se nalazi računalna i informatička oprema u kojoj su pohranjeni povjerljivi bankarski informacijski resursi. Ovisno o razini moguće prijetnje i vrijednosti uređaja i informacija, formira se adekvatna kontrola pristupa uz pomoć raznih elemenata (Slika 13) za postizanje fizičke sigurnosti, poput:

- posebnih magnetskih kartica za određene zaposlenike koje omogućuju pristup samo određenim prostorijama unutar banke
- Nadzornih infracrvenih kamera
- Alarmni sustava u slučaju neovlaštenog pristupa

Slika 13. *Elementi za postizanje kontrole fizičkog pristupa*

6.2. Programske metode zaštite

Programske metode zaštite su za bankarske informacijske sustave najbitniji aspekt zaštite te kako bi osigurale što viši nivo zaštite, uvode se na više razina:

6.2.1. Zaštita na razini operacijskog sustava

Zaštita na razini operacijskog sustava je osnovni stupanj zaštite koji se dijeli na administratore operacijskog sustava i na njegove korisnike, odnosno zaposlenike unutar bankarskog informacijskog sustava. Administratori određenog operacijskog sustava određuju ostalim zaposlenicima koji se koriste operacijskim sustavom korisničko ime i pripadajuću lozinku pri pristupu sustavu. Uz navedeno, administratori također određuju ovlasti pojedinog ili više zaposlenika, odnosno ograničavaju njihovo korištenje operacijskim sustavom u cilju opće sigurnosti cjelokupnog informacijskog sustava.

6.2.2. Zaštita na razini korisničke programske podrške

Zaštita na razini korisničke podrške podrazumijeva ograničenja tijekom korištenja aplikacijama i podacima unutar operacijskog sustava te je također regulirana od strane mrežnog administratora. Ograničenja se dijele na tri razine te se najčešće provode lozinkom za pristup ili jednostavno zabranom pristupa određenim dijelovima operacijskog sustava.

1. razina – najniža razina koja korisnicima dozvoljava samo čitanje određenih podataka iz baze podataka
2. razina – srednja razina koja korisnicima omogućava izmjenu pojedinih podataka i eventualni unos novih podataka
3. razina – najviša razina kojoj samo rijetki zaposlenici mogu pristupiti te koja im uz dozvole s prve dvije razine dozvoljava i prividno brisanje podataka iz operacijskog sustava, ali ne i iz baze podataka

6.2.3. Kriptografija u bankarskom sustavu

Kriptografija i njene metode su najbitnije sredstvo programske zaštite osjetljivih i povjerljivih podataka u bankarskim i općenito financijskim informacijskim sustavima. Kriptografske metode omogućavaju efikasnu zaštitu osjetljivih podataka te imaju za cilj maksimizirati tajnost, a samim time i provjerljivost podataka što je ključno načelo svakog informacijskog sustava. Osnovni dijelovi svake kriptografske metode čine kriptografski algoritam koji transformira podatke i kriptografski ključ s kojim se podaci obrnuto transformiraju, odnosno vraćaju u prvobitno stanje kako bi bili vidljivi samo osobi kojoj su upućeni. (načelo povjerljivosti, 3.1.1. povjerljivost, str. 8).

Kriptografija ima osnovnu podjelu na simetričnu i asimetričnu:

- Simetrična kriptografija je vrsta kriptografije kod koje postoji samo jedna vrsta transformacije podataka koja se obrnuto transformira sa samo jednim ključem, te joj je glavni nedostatak što obje osobe u komunikaciji moraju imati isti ključ. Simetrična kriptografija se deklarira kao slabija vrsta zaštite i rijetko je u upotrebi.
- Asimetrična kriptografija je vrsta kriptografije kod koje se koriste javni i tajni ključ. Javnim ključem se poruka s podacima transformira i kao takva vidljiva je svim sudionicima u komunikaciji, dok je tajni ključ samo kod jednog primatelja te je samo on u mogućnosti obrnuto transformirati poruku i pristupiti podacima.

Kriptografija i njene metode u bankarskim informacijskim sustavima koriste se za općenito enkripciju podataka, elektroničko potpisivanje, očuvanje integriteta i povjerljivosti te za utvrđivanje autentičnosti korisnika [15].

6.2.4. Dvokoračna autentikacija

Dvokoračna autentikacija predstavlja novi, unaprijeđeni način obične autentikacije korisnika. Za razliku od obične jednostavne autentikacije koja zahtijeva samo korisničko ime i pripadajuću lozinku, dvokoračna autentikacija sadrži dvostruku lozinku od koje je jedna korisnička a druga najčešće grafička. Grafička lozinka generirana je od strane autentifikatora, odnosno ponuditelja usluge te zahtijeva od korisnika da slova, brojeve i znakove sa grafičkog prikaza prepiše u poseban predložak kako bi se potvrdila njegova autentičnost i njegovo trenutno prisustvo pri pristupu sustavu [7].

6.2.5. Zaštita od malicioznih programa

Kao što je ranije bilo rečeno, maliciozni kod je bilo koji oblik programskog koda koji djeluje zlonamjerno i opasno, neovisno da li riječ o djelovanju na informacijski, softverski ili hardverski resurs. Kako bi se osigurala adekvatna zaštita za bankarske informacijske sustave, potrebno je uvesti određene sigurnosne procedure, mehanizme i alate.

Najučinkovitija zaštita sustava od zlonamjernih programa uspostavlja se prikladnim antivirusnim alatima. Antivirusni alati su korisnički programi koji sadrže digitalne potpise gotovo svih mogućih oblika virusa, crva, trojanskih konja i sličnih zlonamjernih programa. Posjeduju mogućnost skeniranja računala, detekcije malicioznih programa i mogućnost njihova izoliranja iz sustava ili potpunog brisanja. Također bitna funkcija je automatsko obnavljanje, odnosno ažuriranja baze podataka o potencijalnim novim prijetnjama.

Vatrozid (engl. *Firewall*) je temeljni i osnovni element za povećanje sigurnosti bilo kojeg informacijskog sustava čija izvedba može biti hardverska ili softverska. Vatrozid se postavlja kao virtualna granica između lokalne mreže i javne mreže, tj. Interneta koja je dizajnirana kako bi zaštitila povjerljive podatke unutar informacijskog sustava, te blokirala i preusmjerila sav neželjen promet koji dolazi s javne mreže prema lokalnoj. Vatrozid funkcionira na principu filtriranja mrežnog prometa prema unaprijed određenim pravilima i to na svim slojevima prijenosa podataka [24].

6.2.6. Zaštita podataka sa sigurnosnim kopijama

Zaštita podataka uz razne obrambene mehanizme od napadača također podrazumijeva izradu sigurnosnih kopija (engl. *backup*). Sigurnosne kopije su skup podataka i informacija koji se pohranjuju na zasebne memorijske lokacije, poslužitelje i fizičke medije za pohranu podataka kako bi se u slučaju hardverskih kvarova, programskih pogrešaka, zlonamjernih djelovanja i napada ostali zaštićeni te bili u mogućnosti ponovno se vratiti u sustav nakon njegova oporavka. Prema [23], ovisno o potrebni, vrijednosti informacija i mogućem riziku, postoji nekoliko metoda izrade sigurnosnih kopija:

- Potpuna sigurnosna kopija (engl. *Full backup*) – sveobuhvatna i najsigurnija kopija, koja podrazumijeva kopiranje i pohranu svi sustavnih datoteka i podataka. U potpunosti je neovisna o ranije napravljenim sigurnosnim kopijama te iziskuje veliki vremenski period pri svojoj izradi
- Diferencijalna sigurnosna kopija (engl. *Differential backup*) – kopija samo određenih podataka koji su dodani ili izmijenjeni od izrade zadnje potpune sigurnosne kopije.
- Inkrementalna sigurnosna kopija (engl. *Incremental backup*) – podrazumijeva izradu sigurnosne kopije svih datoteka i podataka koji su dodani ili izmijenjeni od zadnje potpune, diferencijalne ili inkrementalne sigurnosne kopije. Inkrementalnu metodu odlikuju brzina izrade sigurnosne kopije i jednostavan povrat spremljenih podataka

Svaka bankarska institucija obavezna je kroz određene vremenske intervale izrađivati sigurnosne kopije i uspostaviti proces upravljanja pohranjenim podacima. Proces upravljanja podrazumijeva postupke izrade, pohrane i testiranja sigurnosnih kopija kako bi se osigurala dostupnost podataka čak i u slučaju raznih napada i gubitka podataka unutar bankarskog informacijskog sustava [16].

6.3. Organizacijske mjere zaštite

Organizacijske mjere podrazumijevaju osiguranje ažurnosti, točnosti i pravilnosti obavljanja poslova, kao i sprječavanje neovlaštene izmjene dokumentacije i podataka te neovlaštenog korištenja informatičke opreme i mreže.

Organizacijskim mjerama zaštite određuje se:

- Organizacija prostora
- Odgovorna osoba za provedbu sigurnosti
- Kretanje unutar bankarske ustanove
- Distribucija novca
- Program edukacije zaposlenika

Pravilnom organizacijom radnog prostora zaposlenika, prostorom za usluživanje korisnika, posebnih prostorija za pohranu i distribucija novca postiže se prostorno-organizacijska mjera zaštite. Nakon adekvatne organizacije prostora, određuje se i imenuje osoba, ili ako je potrebno više osoba za provedbu organizacijskih mjera unutar bankarske ustanove. Organizacijske mjere također podrazumijevaju definiranje i upravljanje kontrolom kretanja zaposlenika na radnome mjestu i korisnika unutar bankarske ustanove, u cilju zaštite informacijskih resursa. Propisuju se posebna pravila i upute za zaposlenike koji obavljaju financijske transakcije i upravljaju isplatama i uplatama novca. Najbitniji dio organizacijskih mjera zaštite odnosi se na edukaciju zaposlenika o upravljanju novcem, korištenjem računalnih i informacijskih sustava, tehničke opreme i raznih uređaja potrebnih za uspješno izvršavanje radnih zadataka. Edukacija se također odnosi i na korisnike bankarskih usluga, koji se od strane bankarske ustanove na razne načine pokušavaju informirati o raznim mogućim prijetnjama i načinima zaštite [14].

Svaki bankarski informacijski sustav koji korisnicima omogućuje svoje usluge putem interneta, poput internet bankarstva, obvezan je na određeni način svoje korisnike redovito obavijestiti o mogućim propustima i napadačima, te izdavati brošure i naputke s mjerama sigurnosti koje korisnici mogu sami ostvariti u cilju opće sigurnosti i poslovanja.

7. ZAKLJUČAK

Informacijski sustavi integrirani su u potpunosti u bankarske ustanove i procese. Bankarski informacijski sustavi temelje se na povjerljivosti, cjelovitosti i dostupnosti što se deklarira kao tri osnovna načela koja konstantno moraju biti ispunjena i nikada ne smiju biti povrijeđena. Uz mnogobrojne prednosti i usluge koje omogućavaju moderni bankarski informacijski sustavi, od strane zlonamjernih napadača stvorene su razne metode napada na takvu vrstu sustava, u cilju otuđenja korisničkih identiteta, povjerljivih podataka, te velikih financijskih svota koje se svakodnevno prenose raznim transakcijama diljem svijeta.

Analizom raznih vrsta napada i mnogobrojnih napadačkih alata i programa, poput trojanskih konja, programa za praćenje unosa znakova s tipkovnice i sličnih, moguće je uvidjeti dosadašnje sigurnosne propuste na mnogim tehničkim i programskim razinama te tako odabrati i primijeniti odgovarajuće mjere zaštite. Mjere i metode zaštite koncipirane su na razne načine, ali ih je moguće i jednostavno podijeliti na fizičke, programske i organizacijske. Uvođenjem pravilne sigurnosne politike, provedbom i pridržavanjem propisanih mjera i metoda zaštite, te kontinuiranom edukacijom zaposlenika i korisnika bankarskih usluga, bankarski informacijski sustavi mogu postići zadovoljavajući stupanj opće sigurnosti i zaštite.

LITERATURA

1. B.,Vukelić: Sigurnost informacijskih sustava, nastavni materijal, Sigurnost informacijskih sustava, Veleučilište u Rijeci, Rijeka
2. D., Kovačević: Sigurnosna politika, diplomski rad, Fakultet elektrotehnike i računarstva, Zagreb, 2008.
3. D., Peraković, I.Cvitić: Sigurnost i zaštita informacijsko komunikacijskog sustava – skripta, Sigurnost i zaštita informacijsko komunikacijskog sustava, Fakultet prometnih znanosti, Zagreb, 2015.
4. D., Peraković, M., Periša, I., Forenbacher: Elementi informacijskog sustava, Informacijski sustavi mrežnih operatera, Fakultet prometnih znanosti, Zagreb, 2013.
5. D., Peraković, M., Periša, I.,Forenbacher: Teoretske osnove informacijskih sustava, Informacijski sustavi mrežnih operatera, Fakultet prometnih znanosti, Zagreb, 2013.
6. Guverner Hrvatske narodne banke: Odluka o primjerenom upravljanju informacijskim sustavom, Narodne novine, Zagreb, 2010.
7. Hrvatska akademska i istraživačka mreža: Bankarski zloćudni programi, Nacionalni CERT u suradnji s LSS, Zagreb, 2010.
8. Hrvatska akademska i istraživačka mreža: Fizička zaštita informacijskih sustava, Nacionalni CERT u suradnji s LSS, Zagreb, 2010.
9. Hrvatska akademska i istraživačka mreža: Limbo malware, Nacionalni CERT u suradnji s LSS, Zagreb, 2008.
10. Hrvatska akademska i istraživačka mreža: Sigurnosna politika, Nacionalni CERT u suradnji s LSS, Zagreb, 2009.
11. I.,Marijanović: Upravljanje sigurnošću informacija, diplomski rad, Fakultet elektrotehnike i računarstva, Zagreb, 2006.
12. N., Hadljina: Zaštita i sigurnost informacijskih sustava, Nastavni materijal, Zavod za primijenjeno računarstvo, Fakultet elektrotehnike i računarstva, Zagreb, srpanj 2009.
13. Republika Hrvatska: Zakon o informacijskoj sigurnosti (NN 79/07), Hrvatski sabor, Zagreb, 2007.
14. Republika Hrvatska: Zakon o zaštiti novčarskih institucija, Hrvatski sabor, Zagreb, 2015.

15. Sigurnost informacijskih sustava zloporaba informacijskih tehnologija, Nastavni materijal, Primjena računarstva, Studij brodostrojarstvo, Sveučilište u Zadru, Zadar, 2012.
16. Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, Hrvatska narodna banka, Zagreb, 2006.

17. http:// securelist.com (12.08.2015)
18. http://award-keylogger-for-mac.soft112.com/ (13.08.2015)
19. http://os2.zemris.fer.hr/ISMS/2008_kovacevic/sigurnosnaPolitika.html (10.08.2015)
20. http://os2.zemris.fer.hr/ISMS/2008_kovacevic/sigurnostIS.html (10.08.2015)
21. http://os2.zemris.fer.hr/ns/2008_ruzman/ (16.08.2015)
22. http://searchsecurity.techtarget.com/definition/spear-phishing (16.08.2015)
23. http://sistemac.srce.unizg.hr/index.php?id=35&no_cache=1&tx_ttnews%5Btt_news%5D=805 (25.08.2015)
24. http://web.zpr.fer.hr/ergonomija/2005/feric/index.html (24.08.2015)
25. http://www.cis.hr/WikiIS/doku.php?id=dos_attacks (18.08.2015)
26. http://www.malwareremovalguides.info/trojan-zbot/ (12.08.2015)
27. http://www.myloc.de/images/colocation/server_cage.png (25.08.2015)
28. https://securityintelligence.com/cyber-security-challenges-how-do-retailers-protect-the-bottom-line/#.VcxXnPkVjIU (12.08.2015)
29. https://technet.microsoft.com/en-us/library/cc959354.aspx (11.08.2015)
30. https://www.tcd.ie/ITSecurity/guidelines/phishing2.php (16.08.2015)
31. https://www.virusbtn.com/virusbulletin/archive/2011/11/vb201111-form-grabbing (14.08.2015)

POPIS SLIKA I TABLICA

POPIS KRATICA

Kratica	Puni naziv
IS	(engl. *Information System*) informacijski sustav
ISMS	(engl. *Information Security Management System*) sustav upravljanja informacijskom sigurnošću
CIA	(engl. *Confidentiality Integrity Aviability*) povjerljivost cjelovitost dostupnost
OEDC	(engl. *The Organization for Economic Cooperation and Development*) organizacija za ekonomsku suradnju i razvoj
CSII	(engl. *Cyber Security Intelligence Index*) indeks kibernetske zaštitne inteligencije
PRTSC	(engl. *PrintScreen*) zabilježavanje zaslona
JPG	(engl. *Joint Photographic Group*) udruženje fotografskih grupa
PNG	(engl. *Portable Network Graphics*) mrežno prenosive grafike
S&S	(engl. *Save and Send*) spremi i pošalji
HTML	(engl. *Hyper Text Markup Language*) jezik za označavanje hiperteksta
PIN	(engl. *Personal Identification Number*) osobni identifikacijski broj
TAN	(engl.*Transaction Authentication Number*) broj autentičnosti transakcije
URL	(engl. *Uniform Resource Locator*) usklađeni lokator resursa
DLL	(engl. *Dinamic Link Libraries*) biblioteke dinamičke veze
DoS	(engl. *Denial of Service*) uskraćivanje usluge
DDoS	(engl. *Distributed Denial of Service)* distribuirano uskraćivanje usluge
POS	(engl. *Point Of Sale*) mjesto prodaje
VoIP	(engl. *Voice over Internet Protocol*) prijenos govora preko internet protokola