# Sigurnost informacijskih sustava

**Vešligaj, Marko**

**LIBERTAS MEĐUNARODNO SVEUČILIŠTE**

**ZAGREB**

**MARKO VEŠLIGAJ**

# ZAVRŠNI RAD

# SIGURNOST INFORMACIJSKIH SUSTAVA

**Zagreb, rujan 2018.**

**LIBERTAS MEĐUNARODNO SVEUČILIŠTE**

**ZAGREB**

**STRUČNI STUDIJ**

**POSLOVNA EKONOMIJA**

# SIGURNOST INFORMACIJSKIH SUSTAVA

**KANDIDAT: Marko Vešligaj**

**KOLEGIJ: Poslovna informatika**

**MENTOR: mr.sc. Nebojša Stanić**

**Zagreb, rujan 2018**.

*SADRŽAJ*

**1. UVOD ..... 4**

1.1. PROBLEM I PREDMET RADA ..... 4

1.2. CILJ RADA ..... 5

1.3. IZVORI PODATAKA I METODOLOGIJA RADA ..... 5

1.4. STRUKTURA I SADRŽAJ RADA ..... 5

**2. OPĆENITO O INFORMACIJSKIM SUSTAVIMA ..... 7**

2.1. VRSTE INFORMACIJSKIH SUSTAVA ..... 7

**3. OPĆENITO O SIGURNOSTI I INFORMACIJSKA SIGURNOST ..... 9**

3.1. INFORMACIJSKA SIGURNOST ..... 12

4. **HAKIRANJE**……..…….…….**13**

4.1.POVIJESTI HAKIRANJA……..…….…….……13

4.2.NAJPOZNATIJI HAKERSKI NAPADI KOD VODEĆIH DRŽAVA SVIJETA…….……..……14

**5. SIGURNOSNI MEHANIZMI I KONTROLNI POSTUPCI……..……..17**

5.1. DIGITALNI CERTIFIKAT ..... 16

5.2. FIZIČKA ZAŠTITA ..... 18

5.3. KONTROLNI POSTUPCI ..... 21

**5. PRIJETNJE SIGURNOSTI ..... 23**

5.1. IZVORI I OBLICI PRIJETNJI ..... 23

5.2. NAPADI I OBLICI NAPADA ..... 25

**6. INSTITUCIONALNI OKVIRI U REPUBLICI HRVATSKOJ ..... 28**

6.1. UVNS ..... 28

6.2. ZSIS ..... 28

6.3. NCERT ..... 29

6.4. AZOP ..... 30

**7. ZAKLJUČAK ..... 32**

**8. LITERATURA ..... 33**

**POPIS SLIKA ..... 35**

**POPIS GRAFIKONA ..... 36**

# 1. UVOD

U današnje vrijeme sve je više različitih podataka i informacija koje su pojedincima vrlo bitne, pogotovo su bitni podatci koje posjeduje vojska, vlada ili koje drugo državno tijelo, a najvažnija zajednička stavka svih tih podataka jest tajnost i sigurnost tih podataka. Danas je sve više hakera i osoba koje bi vrlo rado došle do tih podataka kako bi ih iskoristili na krivi način te kako bi ugrozili sigurnost države ili pojedinca. Upravo iz tog razloga dostupno je sve više različitih načina zaštite sigurnosti podataka i cjelokupnih sustava među koje spadaju i informacijski sustavi. Ako se dogodi da se naruši povjerljivost informacija u određenom poduzeću, u tom poduzeću može doći do smanjenja dobiti, narušavanja ugleda te mogu se desiti razne negativne radnje vezane uz protok povjerljivih informacija. Mnoga poduzeća danas griješe jer najveću pažnju kada žele zaštititi svoj sustav pridodaju tehničkim mjerama zaštite, dok zanemaruju edukaciju o sigurnosti korisnika sustava koji je bitniji faktor u sigurnosti. Potrebno je dobro educirati korisnika sustava i upoznati korisnika sa tehničkim aspektima zaštite informacijskih sustava. U današnje vrijeme teško je ostvariti potpunu sigurnost bilo kojeg sustava jer se uvijek traži i može pronaći način kako doći do potrebitih informacija. Pravilna sigurnost informacijskih sustava postiže se pravodobnom implementacijom svih mjera zaštite, trebamo kombinirati fizičke, administrativne i tehničke mjere, te moramo dobro educirati vlastite radnike.

Jedan od dobrih primjera za hakiranje, je hakiranje samog Pentagona koji ima jedan od najjačih sustava sigurnosti podataka i sigurnosnih provjera.

U ovom radu detaljno će se obraditi područje sigurnosti te će se obraditi i sigurnost informacijskih sustava, a isto tako će se obraditi prijetnje koje postoje za te informacijske sustave.

Cilj ovog rada je jasno objasniti i prikazati kako se kroz povijest razvijala sigurnost samih informacijskih sustava, prikazati koje su sve vrste sigurnosti informacijskih sustava te koje su prijetnje sigurnosti i tajnosti podataka.

## 1.1. PROBLEM I PREDMET RADA

Problem ovog diplomskog rada jesu nedovoljno razgraničeni pojmovi i teoretska objašnjenja sigurnosti i metoda sigurnosti informacijskog sustava.. Predmet ovog diplomskog rada je

sistematizacija i pojmovno razgraničenje sigurnosti, informacijskih sustava i metoda zaštite informacijskog sustava..

## 1.2. CILJ RADA

Cilj ovog rada je što jasnije definirati metode zaštite i njene ciljeve u svrhu što bolje organizacije informacijskog sustava te u svrhu bolje zaštite i očuvanja tajnosti podataka i očuvanja sigurnosti objekata i sustava.

## 1.3. IZVORI PODATAKA I METODOLOGIJA RADA

Prilikom izrade ovog rada koristit će se izvori podataka u obliku web izvora, priručnika te udžbenika, a metode koje će se koristiti u radu su : meotda deskrpicije, metoda komparacije, metoda sinteze te deduktivna metoda.

## 1.4. STRUKTURA I SADRŽAJ RADA

Rad je podijeljen je u 7 cjelina:

1. Prva cjelina je uvod u kojem je ukratko obrađena tematika ovog završnog rada te je tu naglašen i sami cilj rada.
2. Druga cjelina bavi se općim pojmovima informacijskog sustava te razvojem informacijskog sustava kroz povijest te opisuje i vrste informacijskih sustava koje su i danas u primjeni.
3. Treća cjelina opisuje opću sigurnost te informacijsku sigurnost te je obrađen pojam sigurnosti, koje su vrste sigurnosti te što je informacijska sigurnost.
4. Četvrta cjelina bavi se sigurnosnim mehanizmima i kontrolnim postupcima odnosno objašnjava na koje načine možemo osigurati pojedini sustav te kojim postupcima možemo kontrolirati pristup zaštićenim podacima.
5. Peta cjelina objašnjava prijetnje informacijskom sustavu odnosno koji su to izvori i oblici prijetnji te koji su to izvori i oblici napada na sigurnost informacijskog sustava i u kojoj mjeri su štetni pojedincima.

6. Šesta cjelina ukratko govori o institucionalnim okvirima u Republici Hrvatskoj odnosno o svim institucijama koje se bavi sigurnošću informacijskog sustava, te ova cjelina govori o kontroli podataka, u to spadaju i obrađeni su UVNS, ZSIS,NCERT i AZOP.
7. Sedma cjelina je i sami zaključak rada u kojem je ukratko sintetiziran cijeli rad te je u zaključku iskazano i moje mišljenje o radu kao i o samoj tematici rada.

# 2. OPĆENITO O INFORMACIJSKIM SUSTAVIMA

Za početak potrebno je definirati riječ sustav. Definicija sustava glasi: Sustav je svaki uređeni skup od najmanje dva elementa koji zajedno interakcijom ostvaruju funkciju cjeline[1]. Informacijski sustav dio je svakog poslovnog sustava, a njegova uloga je konstantna 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. Informacijski sustavi prilagođavaju se i razvijaju za realni poslovni sustav, a poslovni procesi realnog sustava temelj su za modeliranje strukture njegovog informacijskog sustava[2]. Strukture informacijskih sustava razlikuju se ovisno o potrebitim informacijama te i o samoj organizaciji poduzeća ili vlasnika samog sustava. Ciljevi informacijskih sustava različiti su za različite radne razine i poslovanja. Najčešća podjela je na tri radne razine: razinu izvođenja (operativnu razinu), razinu upravljanja (taktička razina) i razinu odlučivanja (strateška razina)[3]. Jedna od najčešćih zabluda i pretpostavka o informacijskim sustavima jest ta da su informacijski sustavi vezani isključivo za računala, no to nije istina jer sama riječ informacijski sustav govori da je riječ o informacijama te isto tako riječ sustav nam govori da je to skup informacija koji je organiziran i sortiran po potrebama pojedinca i / ili organizacije ili poduzeća koji se služe upravo tim podacima odnosno informacijama.

## 2.1. VRSTE INFORMACIJSKIH SUSTAVA

Pod pojmom informacijskog sustava razumijevamo niz elemenata informacijske djelatnosti koji tvore organiziranu cjelinu, sustav. Pod pojmom strukture informacijskog sustava mislimo na unutrašnji raspored tih elemenata, njihov sastav, poredak i odnose u informacijskom sustavu. Struktura informacijskog sustava nastaje povezivanjem informacijskih institucija, organizacija i službi u konkretne informacijske i društvene odnose sa specifičnim ulogama i zadacima u svakom konkretnom informacijskom sustavu.

Ovisno o funkcijama organizacije koju podržavaju, obično razlikujemo sljedeće vrste informacijskih sustava za:

[1] Klasić K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009.
[2] http://www.referenceforbusiness.com/management/Comp-De/Data-Processing-and-DataManagement.html
[3] http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf

• podršku izvođenju obrada

• poslovnu podršku

• podršku izvršavanju operacija

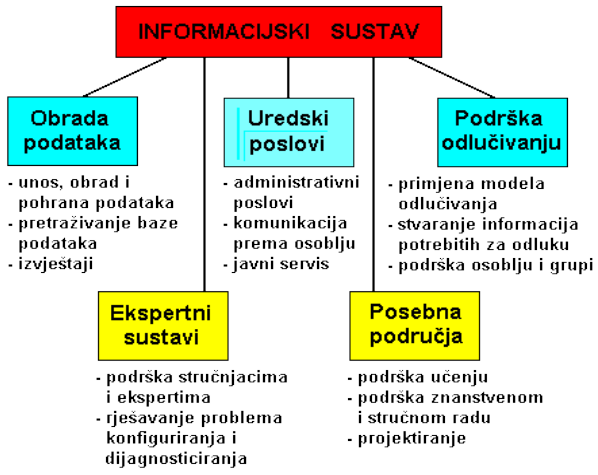
• podršku upravljanju

• podršku odlučivanju

• podršku strateškom planiranju[4]

Svaki sustav organizacija ili osoba može se koristiti zasebno, ali u današnje vrijeme vrste informacijskih sustava se kombiniraju ovisno o potrebama i zadaćama menadžmenta ili drugih pozicija poduzeća. Postoje razne definicije i podjele informacijskih sustava, međutim navedena podjela je detaljnije podijeljena i sadrži više vrsta sustava. Na slijedećoj slici navedena je kratka osnovna podjela informacijskih sustava te koje ciljeve ima određeni podsustav.

Slika 1. Podjela informacijskog sustava na podsustave




Izvor: http://www.informatika.buzdo.com/s870-informatika-u-praksi.htm

Iz prethodno navedene slike ukratko je vidljivo koji sustav je odgovoran za koji dio poslovanja te se iz istog također može zaključiti koji su to sustavi koji određenom poslovanju( misli se na poduzeće) trebaju kako bi isto što učinkovitije funkcioniralo i poslovalo.

[4] M. Tuđman, D. Boras, Z. Dovedan: Uvod u informacijske znanosti

5 http://www.informatika.buzdo.com/s870-informatika-u-praksi.htm

# 3. OPĆENITO O SIGURNOSTI I INFORMACIJSKA SIGURNOST

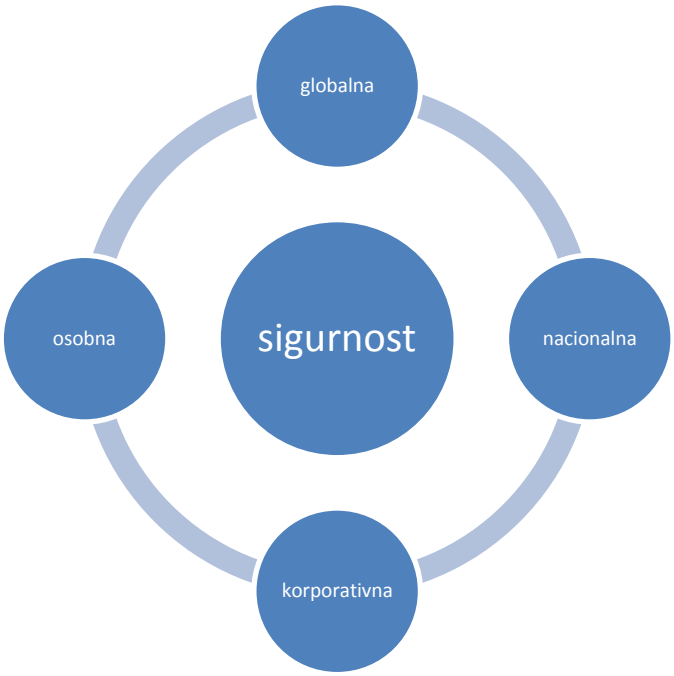
Sigurnost možemo definirati kao potrebu  koja nam daje neku svojevrsnu zaštitu odnosno razinu koja pruža osjećaj zaštite pod kojom smatramo da je rizik najmanji mogući odnosno da smo sigurni. Sigurnost se može javiti u raznim oblicima kao na  primjer osobna sigurnost u smislu tjelohranitelja, sigurnost kao pojam obrane i zaštite, sigurnost kao zaštita od rizika je zapravo pojam koji možemo upotrijebiti kao opis bilo koje vrste sigurnosti.

Sigurnost možemo podijeliti na četiri razine:

1. Osobna ili individualna sigurnost
2. Korporativna odnosno poslovna sigurnost
3. Nacionalna ili javna sigurnost
4. Te globalna odnosno opća sigurnost.

Na sljedećem grafu prikazano je zapravo kako ove četiri razine zapravo stvaraju cjelinu sigurnosti jer su međusobno povezane na način da u konačnici kombiniranjem bilo kojih razina sigurnosti zapravo dobivamo globalnu odnosno opću sigurnost kao rezultat.

Grafikon 1. Prikaz sigurnosti kroz razine koje se kombiniranjem spajaju u istu cjelinu




Izvor: http://www.cps-zg.hr/poslovna-sigurnost/sigurnost-u-poslovanju/

Sigurnost pojedinca možemo definirati kao potrebu pojedinca da se osjeća zaštićeno te da je ta osoba zaštićena od rizika u najvećoj mogućoj mjeri. U današnje vrijeme to se najčešće postiže tjelohraniteljima u smislu osobne zaštite, no isto tako pojedinac osjećaj sigurnosti može imati i zaštitom pojedinih podataka koji su od velikog značaja za njega , neki od tih podataka mogu biti : detalji o pojedinu, podaci, OIB, JMBG, bankovni računi i PIN-ovi, lozinke društvenih mreža i slično.

Korporativna sigurnost odnosi se na zaštitu poslovanja, i možemo ju podijeliti na 3 razine:

1. Tjelesnu i tehničku zaštitu,
2. Informacijsku sigurnost,
3. Sigurnosnu procjenu zaposlenika prilikom zapošljavanja i tijekom rada.

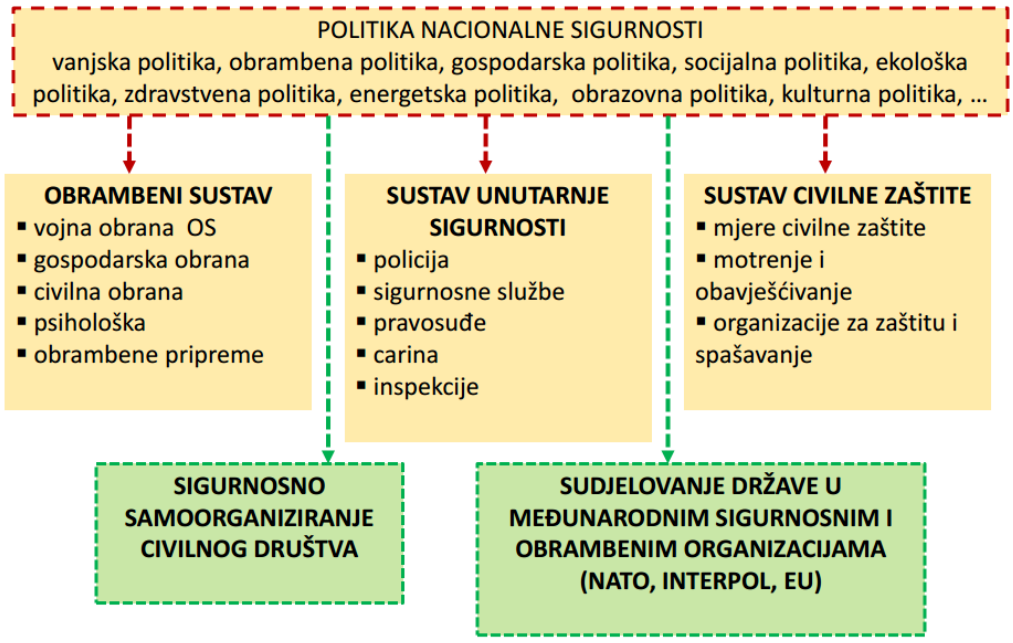
Koristimo li u odgovarajućoj kombinaciji navedene tri mjere sigurnosti, stvaramo tzv. "višeslojnu" sigurnost koja se bazira na prevenciji i detekciji potencijalnih izvora ugrožavanja.[5]

Nacionalna sigurnost je pojam koji se može definirati kao stanje zaštićenosti temeljnih vrijednosti društva i na njima zasnovanih institucija, zaštita vitalnih nacionalnih interesa, integritet državnog područja i njezinih institucija, odnosno najopćenitije kao sigurnost političkog naroda. Pojam "nacionalna sigurnost" mijenja svoj sadržaj i opseg sukladno povijesnim, političkim i geopolitičkim promjenama i okolnostima. Značenje nacionalne sigurnosti ovisi o ideologijskim i svjetonazorskim polazištima. Definirajući nacionalnu sigurnost svako pojedino društvo, jednako kao i svaki teoretičar, izražava svoje vrednote, svoje strahove i nade, a sve to uvjetovano je specifičnom situacijom u kojoj se društvo nalazi.[6]

[5] http://www.cps-zg.hr/poslovna-sigurnost/sigurnost-u-poslovanju/
[6] https://hr.wikipedia.org/wiki/Nacionalna_sigurnost

U sljedećem grafikonu prikazani su temeljni elementi sustava nacionalne sigurnosti jedne suvremene države.

Slika 2: Elementi nacionalne sigurnosti




Izvor: Pojam sigurnosti u terminologiji međunarodnih odnosa, Mario Nobilo, Zagreb

Na gore navedenoj slici jasno je prikazano kako zapravo nacionalna sigurnost djeluje u praksi te kako je podijeljena na dnevnoj bazi.

Globalnu sigurnost možemo i definirati kao potreba za svjetskim mirom. Globalna sigurnost je prvi cilj UN-a koja se ističe u članku 1. Povelje Ujedinjenih Naroda. U toj povelji su navedeni i definirani pojam mira i sigurnosti te obveze država u postizanju mira i sigurnosti. Bez poštivanja određenih normi koje zapravo predstavljaju minimum u održavanju i postizanju svjetskog mira i sigurnosti, ne bi postojala globalna sigurnost.[7]

[7] Pojam sigurnosti u terminologiji međunarodnih odnosa, Mario Nobilo, Zagreb

## 3.1. INFORMACIJSKA SIGURNOST

Informacijska sigurnost je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja.[8] 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. Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti. Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.[9]

Postoji niz zakona o informacijskoj sigurnosti ali najbitniji su:

1.Zakon o informacijskoj sigurnosti - Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

2.Zakon o elektroničkom potpisu - Ovim se Zakonom uređuje pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa, ako posebnim zakonom nije drukčije određeno

3.Zakon o zaštiti tajnosti podataka - Ovim se Zakonom propisuju pojam, vrste i stupnjevi tajnosti te mjere i postupci za utvrđivanje, uporabu i zaštitu tajnih podataka.

4.Zakon o zaštiti osobnih podataka - Ovim se Zakonom uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj.[10]

[8] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010
[9] Članak 2. Zakona o informacijskoj sigurnosti, NN 79/07
[10] Točka 1,2,3 i 4 preuzete su sa dolje navedene stranice ( skripta o sigurnosti informacijskih sustava- FOI)

# 4. HAKIRANJE PODATAKA

Haker (eng. hacker) je pojam u informatici a označava osobu koja odlično poznaje računala, često se za njih kaže da su kriminalci, ali to su osobe koje imaju znatiželju istraživati granice onoga što je moguće, to često uključuje prepravljanje postojećih hardverskih i softverskih sustava. Hakeri nisu nužno i cyber kriminalci, hakerima se smatraju i stručnjaci koji rade na razvoju sustava čija je svrha poboljšati sigurnost.

Hakerska etika se temelji na razmjeni stručnog znanja te pisanju slobodnog softvera radi lakšeg pristupa informacijama. Etički hakeri se bore protiv virtualnih kriminalaca i otkrivaju pogreške kako bi mogli ukloniti sigurnosne nedostatke sustava.

## 4.1.POVIJEST HAKIRANJA

Hakeri su potekli od Phreakera**.** U povijesti prvo hakiranje je zabilježeno kod vijetnamskog veterana John Draper koji je izveo je jedan od prvih phreakerskih napada davne 1971. godine. Draper je otkrio da pomoću zviždaljke iz Cap'n Crunch zobenih pahuljica koja proizvodi zvuk frekvencije 2.600 Hz može prevariti telefonsku centralu i besplatno telefonirati. Draper je u ovu svrhu napravio i malu spravu zvanu bluebox koja mu je u kombinaciji sa zviždaljkom omogućavala besplatno telefoniranje. Ubrzo nakon Draperovog otkrića, upute kako napraviti bluebox objavio je časopis Esquire i omogućio besplatno telefoniranje svim Amerikancima. Godine 1979**.** Iam Murphy je s još trojicom prijatelja provalio u računalni sustav tvrtke AT&T i promijenio vrijeme na njihovim internim satovima. Zahvaljujući ovome korisnici su skupe telefonske impulse umjesto danju plaćali noću i obrnuto.

Murphy je i prvi čovjek u povijesti koji je uhapšen za računalni zločin
Jedno od poznatijih hakiranje je bio,Vladimir Levin i njegovi sudionici koji su bili odgovorni za pljačku čak 10 milijuna dolara iz banke Citibank oni su upotrijebili računala i hakerske vještine. Godinu dana nakon pljačke koja se dogodila 1994. godine Levin ipak je izručen američkim vlastima i osuđen na tri godine zatvora. Ehudu Tenebaumu pošlo je za rukom provaliti u računala američke vojske i izvući se nekažnjeno. Ovaj izraelski haker poznat pod imenom 'The Anaylist' 1998. godine počešljao je Pentagonova računala i ostavio američki vojne stručnjake.
U sukobu najpoznatijeg hakera današnjice Kevina Mitnicka i stručnjaka za računalnu

sigurnost Shimomure, sve je počelo kada je Mitnick navodno provalio u Shimomourino računalo i objavio broj njegove kreditne kartice. Nakon toga se FBI, koji je već duže vrijeme bezuspješno pokušavao uhvatiti Mitnicka, obratio Shimomuri, koji je ovaj prijedlog objeručke prihvatio. Nadmudrivanje dvaju hakera iz kojeg je Shimomura izašao kao pobjednik, a Mitnick odslužio pet godina zatvorske kazne opisano je u knjizi i filmu 'Takedown'.

Neki hakeri djeluju sami, a neki se organiziraju u grupe. Povijest bilježi nekoliko poznatih hakerskih grupa koje nisu samo provaljivale u velike računalne sustave, već su i međusobno ratovale. U najpoznatije ubraja se Legion of Doom, Masters of Deception i Phone Masters. Neke od velikih zemalja imaju svoje hakerske timove, tako možemo istaknuti kako SAD, Kina, Rusija, Velika Britanija imaju svoje hakerske timove uz pomoć kojeg mogu nanositi štete drugoj državi, tako da uđe u njihov informacijski sustav te otkriju sve njihove skrivene informacije.

## 4.2.NAJPOZNATIJI HAKERSKI NAPADI U VODEĆIM DRŽAVAMA SVIJETA

SAD je u 2015 oj godini postao žrtva hakerskog napada te su im možda ukradeni osobni podaci, i to su ukradeni podaci četiri milijuna federalnih Američkih zaposlenika. Američki dužnosnici vjeruju da je to bio najveći napad na računalnu mrežu vlade SAD-a u povijesti. Napadnuti su računalni sustavi gotovo svake federalne institucije u zemlji. Istražitelji su uvjereni da je krivac za napad Kina, dok Kinezi negiraju napad. Glasnogovornik veleposlanstva Zhu Haiquan je rekao da je Kina poduzela velike napore u sprečavanju cyber-napada te da je praćenje takvih događaja preko granica zemlje vrlo složeno. Vlada SAD-a iskazuje zabrinutost zbog informatičke špijunaže i krađa iz Kine te je zatražila od Pekinga da čini više kako bi se suzbio problem. Kina je optužbe SAD-a odbacila. Kineski su hakeri također 2014 optuženi za provalu u OPM-ovu računalnu mrežu a čini se da su išli za dokumentacijom o desecima tisuća službenika za koje je tražena dozvola za pristup povjerljivim podacima, izvijestio je list New York Times.

Možemo istaknuti i hakerski napad 2017 godine u svibnju. To je velika hakerska kampanja usmjerena protiv više svjetskih zemalja, u kojoj se informatičke sistem napada takozvanim "ransomware" virusom. Na meti su navodno Sjedinjene Američke Države, Velika Britanija, Rusija, Španjolska, Kina, Italija, Ukrajina, Hrvatska i Nizozemska, a zasad su samo neke to potvrdile. Dosad je otkriveno čak 57.000 napada virusom WannaCry. Iza masovnih hakerskih napada uz traženje otkupa, koji su danas izvedeni na bolnice i kompanije širom Europe, nazire

se navodni cyber virus američke Nacionalne sigurnosne agencije (NSA), tvrdi portal Politico u svom američkom izdanju. Otkupnina iznosi 300 američkih dolara u bitcoinu i raste ako se ne plati do danog roka. Rusko Ministarstvo unutrašnjih poslova potvrdilo je večeras da su se i njihova računala našla na meti hakerskog napada, ali da su na vrijeme primijenjene zaštitne mjere pa je virus blokirao tek manje od jedan posto računala Ministarstva. Britanske bolnice bile su morale da preusmjeravaju pozive upućene Hitnoj pomoći zbog cyber napada izvedenog na cijeloj teritoriji zemlje. Reuters prenosi da je Nacionalna zdravstvena služba (NHS) Velike Britanije rekla da je 16 organizacija iz tog sistema zahvaćeno cyber napadom i da nema informacija da su hakeri uspjeli da pristupe podacima pacijenata. Daily Telegraph je objavio da hakeri traže otkup i da, prema dostupnim informacijama, u bolnicama ne rade telefoni i računala.

Ruska hakerska kampanja je 2018 lako provalila u sigurne mreže u vlasništvu komunalnih poduzeća u SAD-u, i to tako što su prvo prodrli u mreže proizvođača koji su imali povjerenje u elektroenergetske kompanije. Ruski hakeri su stigli su do točke u kojoj su mogli da izbace prekidače i da poremete prijenos struje. Rusija je izjave o napadu negirala i rekla da joj je cilj bila kritična infrastruktura. Homer je za WSJ rekao da su napadači počeli koristeći konvencionalne alate – phishing napade (ciljano slanje e-mailova kako bi došli do povjerljivih informacija) i rupe u sistemu sigurnosti, koji su žrtve omogućile unošenjem lozinki na stranice koji su bili zaraženi – kako bi kompromitirali korporativne mreže dobavljača.

Kada su se našli unutar mreža prodavača oni su se okrenuli prema svom stvarnom fokusu: komunalnim uslugama. Oni su rekli da je to u mnogim slučajevima, relativno lagan proces za uljeze koji su ukrali akreditive od proizvođača i dobili direktan pristup mrežama komunalnih poduzeća. Oni su potom počeli da kradu povjerljive informacije. Hakeri su se upoznali i sa time kako bi objekti trebali da rade, jer napadači moraju da nauče kako da od normalnog naprave nešto što nije normalno. Još nije jasno da li su hakeri koristili svoj pristup kako bi pripremili nešto za budućnost, poput razarajućeg napada na američku električnu mrežu, istaknuli su istražitelji za Wall street Journal.

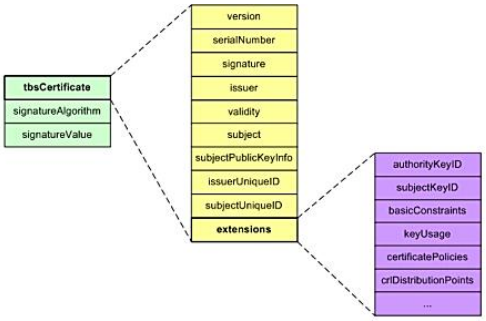
# 5. SIGURNOSNI MEHANIZMI I KONTROLNI POSTUPCI

Sigurnosnim mehanizmima možemo nazvati sve mjere sigurnosti i zaštite koje pojedinac ili poduzeće može poduzeti kako bi zaštitilo svoje vlasništvo bilo materijalno ili intelektualno. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu.[11] Neki od najvažnijih sigurnosnih mehanizama su digitalni certifikat kojim zaštićujemo intelektualno vlasništvo i informacije te dokumente i mehanizmi fizičke zaštite, oba pojma detaljnije su obrađena u nastavku rada.

## 5.1.DIGITALNI CERTIFIKAT

U današnje vrijeme nema osobe koja se nije susrela barem sa jednom vrstom certifikata, najčešći certifikati su ISO certifikati odnosno ISO certifikati koji zapravo određuju propisani standard. Međutim u ovom radu detaljnije su obrađeni digitalni certifikati. Digitalni certifikat je jedan od ključnih elemenata PKI infrastrukture, te je za razumijevanje načina rada digitalnih certifikata potrebno poznavanje osnova PKI infrastrukture a to je tehnologija koja tvori bazu Internet sigurnosti. Možemo reći da su to računalne datoteke koje djeluju kao online propusnice, te omogućuju autentikaciju svojih vlasnika, kao i zaštitu podataka izmijenjenih preko javnih kanala.[12] Na sljedećoj slici grafički je prikazan izgled digitalnog certifikata.

Slika. 3. Grafički prikaz digitalnog certifikata



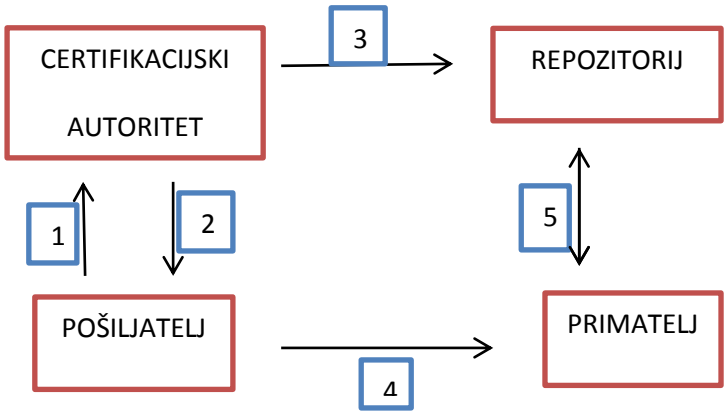

[11] Šehanović, J., Hutinski Ž., Žugaj M., Informatika za ekonomiste, Tiskara Varteks, 2002
[12] http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-135.pdf

Izvor:http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-135.pdf

Svaki digitalni certifikat ima 3 osnovna dijela ( na grafičkom prikazu označeni su zelenom bojom), tbsCertificate označava tko je osoba/poduzeće/korisnik kojem se izdaje digitalni certifikat, tko je izdavač(CA- Certificate Authority) certifikata te period valjanosti certifikata i druge bitne značajke istog. SignatureAlgorithm predstavlja algoritam kojim je certifikator potpisao certifikat ( npr. RSA-MD2, RSA-MD5… ) te zadnje polje odnosno signatureValue sadrži potpis koji je pomoću algoritma enkodiran kao niz bitova odnosno bit string.

Na sljedećem grafikonu prikazan je proces dobivanja certifikata.

Grafikon 2. Prikaz dobivanja certifikata




Izvor:http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-135.pdf

Opis grafikona: Proces započinje kada osoba(pošiljatelj) podnosi molbu za izdavanje elektroničkog certifikata davatelju usluge odnosno certifikacijskom autoritetu ( na grafikonu strelica broj 1) zatim certifikacijski autoritet provjerava identitet osobe te izdaje istoj elektronički certifikati ( strelica pod brojem 2). Sljedeći postupak u procesu odnosi se na davatelja usluge odnosno CA koji objavljuje certifikat u repozitoriju odnosno bazi podataka( strelica br.3), zatim pošiljatelj elektronički potpisuje svoju poruku svojim privatnim ključem odnosno certifikatom i šalje ju primatelju ( strelica br.4), prilikom primitka poruke, primatelj provjerava elektronički potpis javnim ključem pošiljatelja te se u tom trenutku u repozitoriju provjerava status i valjanost certifikata ( strelica broj 5).

U Republici Hrvatskoj FINA izdaje digitalne certifikate , ali je i prvi davatelj usluga certificiranja za javnost i jedini je davatelj certifikata.

## 5.2.FIZIČKA ZAŠTITA

Fizička sigurnost je najosnovniji aspekt zaštite, a obuhvaća kontrolu zaštite prostorija, postrojenja, zgrada i druge imovine. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. Fizička sigurnost se odnosi na sprječavanje oštećenja bilo kojeg dijela nekretnina, postrojenja, ureda, objekata ili zgrada. Fizička sigurnost doprinosi zaštiti ljudi i informacija, iako se na te skupine primjenjuju i druge sofisticirane mjere zaštite. Fizička sigurnost čini dio sveukupne sigurnosti informacijskog sustava kao osnova na kojoj su sve sigurnosne mjere utemeljene.[13]Dakle fizičkom zaštitom možemo smatrati svaki materijalni pojam koji pruža neku sigurnost odnosno koji možemo pravodobno reagirati na prisutnost uljeza bilo da je riječ o običnoj rasvjeti koja se aktivira na senzor kretanja ili da je riječ o sustavima zaključavanja prostorija ili opreme. Najbolja primjena u praksi je takozvani slojeviti pristup odnosno pristup sigurnosti koje seže od unutarnjih do vanjskih granica sustava i suprotno. Na sljedećem prikazu jasnije je objašnjen slojeviti pristup zaštite.

Slika 4. Prikaz slojevite fizičke zaštite


Izvor:NCERT-PUBDOC-2010-06-304

[13] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf

Slika nam govori kako je važno osigurati svaki aspekt poduzeća, od zelenih površina, parkirališta do cesta i prilaza poduzeću te i samo okolno područje objekta bilo da je riječ o zaštiti pomoću kamera ili rasvjete ili da je riječ o unajmljivanju zaštitara koji "patroliraju" područjima oko objekta te na taj način mogu pravodobno reagirati u slučaju potrebe. Vrlo je važna zaštita i unutarnjeg sloja poduzeća odnosno svih pristupa samom poduzeću kao što su ulazi i izlazi , prostorije te do materijalnih vrijednosti objekata kao što su ormarići, oprema, sefovi i slično. Najupotrebljiviji načini odnosno elementi fizičke zaštite su :

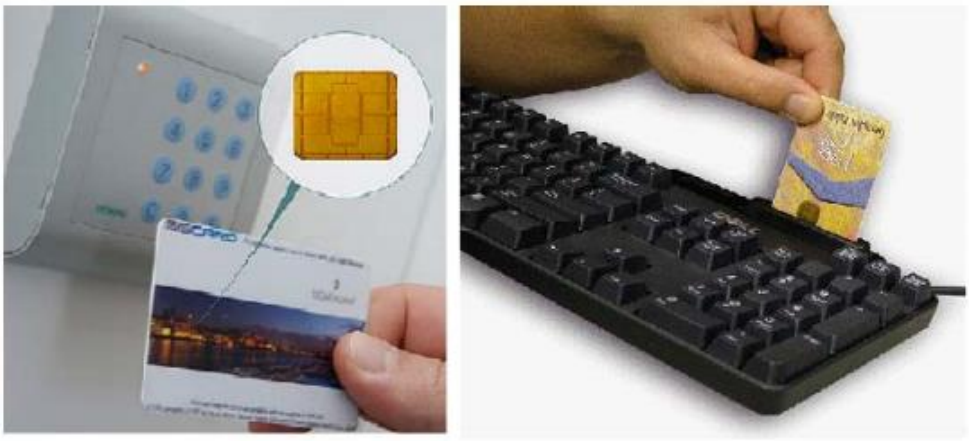
- Alarmni sustavi
- Rasvjeta
- Zaštitari
- Nadzorne kamere
- Uređaji za kontrolu pristupa
- Sustavi za zaključavanje prostorija
- Sustavi za zaključavanje opreme
- Te sustavi za praćenje i otkrivanje lokacije

Alarmni sustavi danas su izuzetno popularni i manje-više svako poduzeće posjeduje neku vrstu alarmnog sustava. Postoji nekoliko vrsta alarmnih sustava no u praksi se najčešće upotrebljavaju alarmi protiv provale koji su dizajnirani za upozoravanje u slučaju provale, često se koriste u obliku tihih alarma za obavještavanje policije bez uzbunjivanja provalnika te vremenski alarmi koji pokreću aktiviranje alarma u trenutku koji je definirao korisnik, zaposlenik, vlasnik ili treća osoba. [14] Neki od laboratoriji koriste i alarme za sigurnost koji obavještavaju o nadolazećoj prirodnoj nepogodi ili čak i u slučaju radijacije. Rasvjeta kao što je i ranije navedeno, najčešće se koristi u obliku rasvjete koja stalno radi dakle tokom cijele noći osvjetljava određene prostore ili se koristi oblik rasvjete koji se aktivira na senzor pokreta što u nekim poduzećima može biti povezano sa alarmom koji se automatski aktivira ukoliko se aktivira i rasvjeta. Zaštitari su najčešće osobe koje su unajmljene ili unajmimo poduzeće čija je svrha osiguranje okoline poduzeća, ali i samog poduzeća kao objekta. Ovisno o zahtjevu poduzeća te sklopljenom ugovoru , zaštitari mogu kontrolirati i spriječiti neku kriminalnu radnju ili mogu biti na samom ulazu u poduzeće u svrsi kontrolora koji kontroliraju osobe koje ulaze i/ili napuštaju objekt ili okolinu poduzeća. Nadzorne kamere služe za nadzor ili cjelokupnog objekta ili određenih prostorija odnosno sustava, najčešće u

[14] NCERT-PUBDOC-2010-06-304

praksi rade cijeli dan odnosno punih 24 sata svih 7 dana u tjednu. Neka poduzeća imaju pristup kamerama i putem određenih online linkova kojim zapravo u bilo kojem trenutku imaju nadzor nad objektom ili prostorijama te se sve snimke najčešće pohranjuju na određeni disk ili CD, DVD diskove, no u današnje vrijeme to je sve rjeđi slučaj. Uređaji za kontrolu pristupa najčešće se koriste u obliku kartica koje sadrže podatke o osobi odnosno korisniku iste. Na sljedećoj slici prikazan je izgled pametne kartice.

Slika. 5 Prikaz kartice za identifikacije



Izvor: NCERT-PUBDOC-2010-06-304

Sustavi za praćenje i otkrivanje lokacije imaju ulogu detektirati krađu te otkriti položaj ukradenog uređaja ili druge opreme. Vrlo su korisni u slučajevima gubitka neke od važnih komponenata, uređaja za pohranu podataka i sl. Pri krađi prijenosnih računala, organizaciji se nanosi materijalna šteta puno veća od same vrijednosti uređaja. Razlog tomu je što oni često sadrže razne važne podatke o poslovanju, zaposlenicima, kupcima, partnerima, proizvodima i dr.[15] Neki od programa koji se koriste su : "LoJack" (omogućuje otkrivanje lokacije ukradenih prijenosnih računala njegovim praćenjem preko Internet mreže) , "Locate Laptop"( provodi kontinuirano praćenje lokacije prijenosnih računala dok je spojeno na Internet) i „GadgetTrak“( ovaj program svoj rad zasniva na iskorištavanju ugrađenih kamera i spajanju na Internet).

[15] NCERT-PUBDOC-2010-06-304

## 5.3.KONTROLNI POSTUPCI

Jedan od najvažnijih kontrolnih postupaka je autentifikacija odnosno utvrđivanje pristupa korisniku temeljem identifikacije pristupnika. Neki od mehanizama autentifikacije su : autentifikacija zasnovana na statičkim odnosno dinamičkim lozinkama, biometrijska autentifikacija, autentifikacija pomoću hardverskih uređaja, autentifikacija zasnovana na javnim i privatnim ključevima. Autentifikacija zasnovana na statičkim lozinkama jedan je od najpopularnijih oblika autentifikacije. Korisnik koristi određenu identifikacijsku oznaku (e-mail ili korisničko ime) te pripadajuću lozinku kako bi se predstavio sustavu koji zatim provjerava odnosno uspoređuje lozinku sa ranije memoriranom lozinkom, ako se potvrdi podudarnost lozinki, korisniku se dozvoljava pristup, u suprotnom korisnika se obavještava da lozinka nije odgovarajuća te ju tada korisnik može ponovno unijeti. Autentifikacija zasnovana na dinamičkim lozinkama provodi se putem hardverskim uređaja odnosno tokena, ono što token radi  jest to da generira novu lozinku za svaki novi pristup koji korisnik zahtjeva odnosno korisnik prilikom svake autentifikacije unosi novu lozinku te pripadajući serijski broj tokena. Na sljedećoj slici prikazan je jedan oblik token uređaja.

Slika 6. Token uređaj


Izvor: http://security.foi.hr/wiki/index.php/Mobilno_bankarstvo

Biometrijska autentifikacija zasniva se na upotrebi biometrijskih karakteristika pojedinca odnosno kroz na primjer digitalni sken otiska prsta, očne rožnice ili DNK pojedinca(jako rijetko u praksi) koji se unaprijed memorira u sustav i kada korisnik zatraži pristup, njegove karakteristike u tom trenutku se uspoređuju sa memoriranim karakteristikama te se ili dopušta pristup. Problem može nastati prilikom otiska prsta jer ako je osoba npr. porezala jagodicu ili vrh prsta koji koristi prilikom autentifikacije, sustav će najvjerojatnije odbiti pristup korisniku jer se obilježja neće podudarati, no u tom slučaju postoje i takozvana rezerva obilježja kao što su: prepoznavanje glasa, dinamika tipkanja, prepoznavanje rukopisa ili potpisa, prepoznavanje lica ili šarenice i slično.

Svaka tvrtka trebala bi provoditi što više kontrolnih postupaka, od kojih su sljedeći najvažniji:

- Kontrola povjerljivosti
- Kontrola pristupa
- Kontrola integriteta
- Kontrola raspoloživosti
- Kontrola nemogućnosti poricanja

Kontrola povjerljivosti odnosi se na zaštitu podataka odnosno na kriptiranje podataka tako da se tijekom njihovog prijenosa štitit neovlašten uvid u iste radi sprječavanja moguće zloporabe. Kontrole pristupa su ranije gore obrađene i one se ukratko odnose na autentifikaciju korisnika koji traži pristup sustavu. Kontrola integriteta štiti podatke/programe ili procese od bilo kojih namjernih ili nenamjernih promjena koje nisu dopuštene, sami integritet označava potpunost i točnost informacija odnosno označava da su informacije koje korisnik dobiva originalne te da nisu mijenjane ni u koju svrhu, najpopularniji mehanizam zaštite integriteta su antivirusni sustavi. Kontrola nemogućnosti poricanja postiže se digitalnim potpisom ili potpisivanjem suglasnosti, ali i zakonom, ono što se osigurava na taj način jest to da korisnici ne mogu poricati aktivnosti koje su poduzeli na sustavu.

# 6. PRIJETNJE SIGURNOSTI

Prijetnjom sigurnosti možemo nazvati bilo koji oblik koji može izazvati rušenje zaštite. U iste ubrajamo i napade i sve njegove oblike. Mogu biti prirodne vrste u obliku nepogoda, namjerne ili nenamjerne prijetnje sigurnosti.

## 6.1.IZVORI I OBLICI PRIJETNJI

Ranjivost (engl. vulnerability) – stanje, nedostatak ili slabost u sigurnosnim procedurama, tehničkim kontrolama, fizičkim ili drugim kontrolama sustava, dizajnu i implementaciji tih kontrola i procedura koja se može iskoristiti, slučajno ili namjerno aktivirati i eksploatirati, što može rezultirati povredom sigurnosti i/ili sigurnosne politike, koja prouzrokuje operativne i financijske gubitke za organizaciju. Prijetnja (engl. threat) - mogućnost izvora prijetnje da iskoristi neku ranjivost slučajnim ili namjernim aktiviranjem i eksploatacijom.[16]Prirodne prijetnje jedne su od najprisutnijih opasnosti za fizičku sigurnost na koje čovjek ne može utjecati. Ipak, postoje određene mjere kojima je moguće smanjiti njihov štetan učinak na sigurnost informacijskog sustava.

U skupinu prirodnih prijetnji spadaju

- Meteorološke nepogode – uključuju sve atmosferske nepogode poput raznih padalina (kiša, snijeg), vjetra, oluje, jako visokih i niskih temperatura i sl. Neke od posljedica ovih nepogoda na informacijski sustav su gubitak ili degradacija komunikacija te uništenje uređaja i informacija.

- Geofizičke nepogode – podrazumijevaju potrese i vulkanske aktivnosti, a mogu izazvati niz drugih nepogoda poput požara, poplava, ispuštanja plina ili otrovnih kemikalija, prekida napajanja i sl. Kao osnovni učinci ovih prijetnji javljaju se mogućnosti uništenja ili oštećenja uređaja što može rezultirati gubitkom podataka, prekidom rada sustava i velikim materijalnim gubicima.

[16] Hadjina, N., Zaštita informacijskih sustava. Zagreb: FER, 2009.

• Sezonski fenomeni – uključuju nepogode vezane uz neko razdoblje poput vremenskih ekstrema, šumskih požara ili uragana, a mogu dovesti do gubitka ili degradacije mrežnih komunikacija te uništenja uređaja.

• Astrofizički fenomeni – podrazumijevaju sunčane fenomene i meteore koji mogu uzrokovati gubitak ili degradaciju satelitskih veza.

• Biološke prijetnje – razne bolesti koje mogu uzrokovati smanjenje broja sposobne radne[17] .

Postoje i ljudske prijetnje, a najčešći oblik ljudske prijetnje su zaposlenici tvrtke.

Neki od oblika ljudske prijetnje, prema NCERT-u su :

• Neposlušnost – jedna od prijetnji ove skupine javlja se uslijed neposlušnosti zaposlenika što može dovesti do prosvjeda ili štrajka. Posljedice takve situacije mogu biti oštećenje imovine ili uređaja te ozljeđivanje samih zaposlenika.

• Otkrivanje osjetljivih podataka – zaposlenici također mogu nanijeti druge oblike šteta poput otkrivanja osjetljivih podataka zbog nepravilnog rukovanja ili nerazumijevanja/nepostojanja sigurnosne politike.

• Sabotaža – svaka organizacija trebala bi uvesti i zaštitu od sabotaže ili namjernog narušavanja rada sustava i ispravnosti uređaja.

• Nenamjerno oštećenje imovine – nepravilno rukovanje može dovesti do oštećenja uređaja ili drugih dijelova imovine. Kako bi se to spriječilo, zaposlenike treba pravilno educirati i upozoriti na posljedice nepravilnog korištenja.

• Zlouporaba ovlasti – zaposlenicima treba jasno definirati uloge te objasniti prava i posljedice njihovog nepridržavanja. Zlouporaba ovlasti može se odraziti u obliku prekomjernog korištenja imovine organizacije ili njenog iznošenja izvan prostora za koji je namijenjena.

• Neovlašten pristup podacima ili imovini – zaposlenicima treba pravilno definirati prava pristupa kako ne bi došli do povjerljivih podataka. Ukoliko zaposlenici rade s nekim povjerljivim podacima ili dijelovima sustava potrebno je napraviti ugovore o povjerenju.

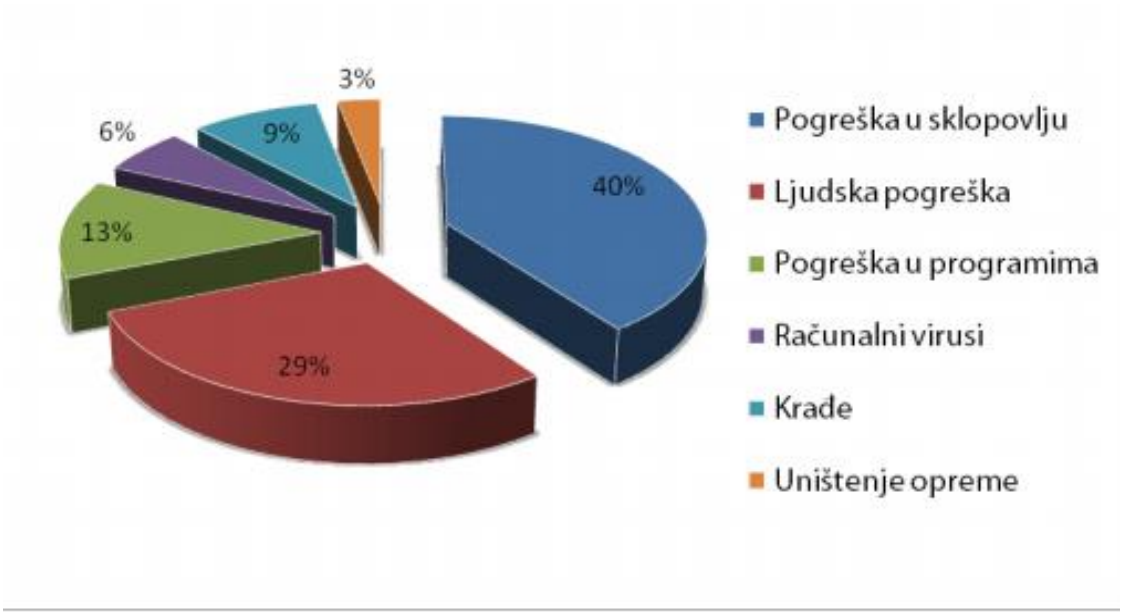
[17] NCERT-PUBDOC-2010-06-304

• Krađa – zaposlenici koji imaju pristup imovini organizacije mogu prisvojiti neke dijelove ili uređaje[18]

Ostali oblici i izvori prijetnje također mogu biti : eksplozija, prašina, poplava, gubitak napajanja..

Na sljedećoj slici prikazan je graf koji objašnjava uzroke gubitka podataka.

Grafikon 3. Uzroci gubitka podataka ( izvor: Graziadio Business Report




Izvor: NCERT-PUBDOC-2010-06-304

Kao što je vidljivo iz grafikona jedan od najčešćih uzroka je ljudska pogreška, bilo da je namjerna ili nenamjerna , i dalje drži visoki postotak u razlogu gubitka podataka.

## 6.2.NAPADI I OBLICI NAPADA

Kada govorimo o napadima, u ovom slučaju ne mislimo na fizičke napade, tu mislimo na napade na informacijske sustave. Postoje četiri vrste napada a to su:

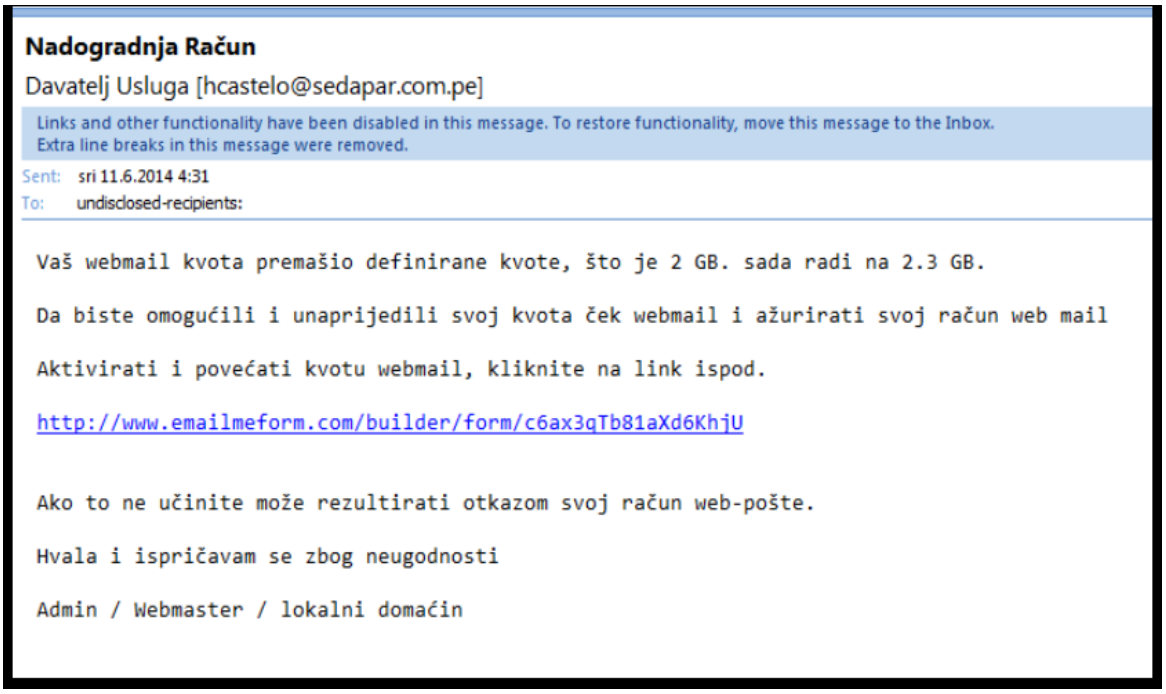
- Prisluškivanje
- Prekid

[18] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf

- Promjena sadržaja
- Izmišljanje poruka

Prisluškivanje odnosno napad na tajnost daje napadaču uvid u tajnost odnosno uvid u osjetljive informacije, ovaj oblik napada se jako teško otkriva jer ne utječe na funkciju sustava, a smatra se da je to najčešće pripremna faza za neki drugi oblik napada jer se ovim napadom mogu prikupiti sve potrebne informacije za jači odnosno teži napad. Ovakav napad na raspoloživost onemogućuje pružanje neke usluge odnosno blokira normalan rad sustava. Promjena sadržaja najčešće se karakterizira kao napad na integritet, a glavna karakteristika ovog napada jest da jedan period ostaje neprimijećen u potpunosti, također i izmišljanje poruka je jedan od napada na integritet jer prilikom napada napadač generira lažne podatke u svrhu prikupljanja tajnih podataka. Jedan od primjera za tu vrstu napada je tzv. Phishing odnosno "pecanje" povjerljivih podataka. Na sljedećoj slici prikazan je jedan od oblika Phishinga na koji ljudi često nasjedaju jer ne primjećuju jednu glavnu stvar, a to je da takve vrste napada najčešće nisu pravopisno niti gramatički točno napisane.

Slika 7: Primjer Phishing napada




Izvor: FTHM, SIS T1 predavanje

Napade također možemo podijeliti na

- AKTIVNE

- PASIVNE

Aktivnim napadom napadač može utjecati na ponašanje i funkcioniranje sustava ili na sami sadržaj informacija (npr. napad na integritet). Dok pasivnim napadom napadač tj. uljez ne djeluje na informacije te je na taj način ugrožena jedino tajnost informacija ( prisluškivanje)

U današnje vrijeme najčešći oblici napada su :

- Virusi
- Crvi
- Logičke bombe
- Trojanski konji
- Botnet programi
- Adware
- Dialeri
- Spam
- Hijackeri
- Hoax

Virusi su oblik napada koji za svoju egzistenciju i širenje koriste druge programe ili datoteke. Prema definiciji dr. Fredericka Cohena[19] virus je program koji može inficirati druge programe, modificirajući ih tako da uključe novu kopiju njega samoga, po potrebi također modificiranu. Glavna karakteristika virusa je to što koriste potpuno legitimne funkcije u legitimnim programima i to je jedan od glavnih razloga zašto ih se teže otkriva. Jedan od prvih virusa je Jeruzalem, a najpoznatiji hrvatski virus je BOBO. Crvi su samostalni programi koji svoje funkcionalne kopije šire na druga računala najčešće putem računalne mreže. Logičke bombe su najčešće dijelovi trojanskih konja, one predstavljaju funkciju odnosno skup funkcija koje se aktiviraju kada su ispunjeni određeni uvjeti (npr. Određeno vrijeme na određeni datum). Trojanski konji su maliciozni programi koji nemaju mogućnost repliciranja te se ne smatraju niti virusima niti crvima, ovaj oblik virusa najčešće se koristi za krađu podataka. Hoax virusi zapravo se i ne smatraju virusima, oni su najčešće u obliku e-maila neistinitog sadržaja čiji je glavni cilj daljnje prosljeđivanje e-mailova, najbolji primjer u praksi su e-mailovi sa takozvanim lancima sreće.

[19] Definicija je objavljena u jednom od njegovih prvih radova o virusima u njegovoj disertaciji

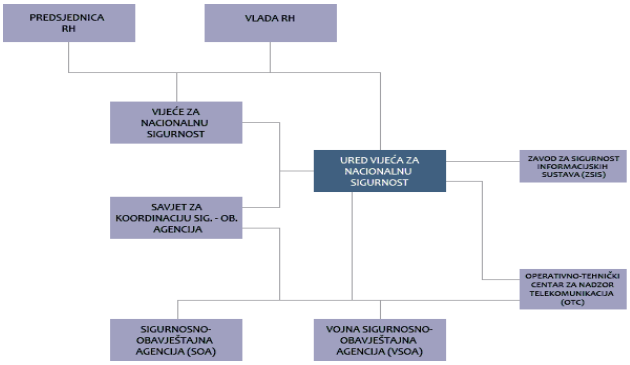
# 7. INSTITUCIONALNI OKVIRI U REPUBLICI HRVATSKOJ

U ovom poglavlju govori se o institucijama koje se bave poslovima zaštite i sigurnosti informacijskih sustava u Republici Hrvatskoj. Osim zakonodavnog okvira koji u svojem opsegu ima zakone o informacijskoj sigurnosti, postoje i zakon o tajnosti podataka, zakon o zaštiti osobnih podataka itd… U RH postoje i institucije koje se bave uređivanjem i u nekoj mjeri i provođenjem samih zakona. Najbitnije institucije u RH su : UVNS, ZSIS, NCERT i AZOP.

## 7.1.UVNS

UVNS odnosno Ured vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost. Ovo vijeće koordinira i usklađuje donošenje i primjernu mjera odnosno standarda informacijske sigurnosti u RH. Putem ovog ureda, predsjednik vlade i sami predsjednik (trenutno predsjednica u Republici Hrvatskoj) države mogu imati nadzor nad sigurnosno-obavještajnim agencijama. Na sljedećoj slici prikazan je shematski prikaz uloge UVNS-a u sigurnosno- obavještajnom sustavu RH.

Slika 8.- Prikaz uloge UVNS-a u sustavu RH



[20]

Izvor: http://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

## 7.2.ZSIS

[20] http://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

ZSIS odnosno Zavod za sigurnost informacijskih sustava središnje je državno tijelo koje se bavi tehničkim poslovima informacijske sigurnosti državnih tijela. U njihovoj nadležnosti je upravljanje kripto materijalima koji se koriste u razmjeni klasificiranih podataka između državnih tijela RH i drugih država odnosno organizacija , te je njihova dužnost i prevencija odnosno otklanjanje problema vezanih uz sigurnost računalnih mreža u državnim institucijama. Osim poslova prevencije i odgovora na računalne ugroze informacijskih sustava, zavod za sigurnost informacijskih sustava zadužen je za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima i njihovo trajno usklađivanje s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.[21]

### 7.3.NCERT

NCERT odnosno Nacionalni CERT ( Croatian national computer emergency response team) je nacionalno središte za računalnu sigurnost. Nacionalni CERT u okviru svog djelovanja provodi proaktivne i reakativne mjere. Proaktivnim mjerama djeluje prije Incidenta i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprečavanja ili ublažavanja mogućih šteta. Informacije o pro aktivnim mjerama se javno objavljuju.[22]

Proaktivne mjere podrazumijevaju[23]:

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti u svrhu priprema za sprečavanje šteta
- kontinuirano praćenje računalno-sigurnosnih tehnologija te se sva nova saznanja prikupljaju i diseminiraju
- javno objavljivanje novih informacija u svrhu edukacije najšire javnosti i unapređenju svijesti o značaju računalne sigurnosti
- provođenje detaljne edukativne obuke za specifične grupe korisnika

[21] https://www.zsis.hr/default.aspx?id=13
[22] http://www.cert.hr/onama
[23] http://www.cert.hr/onama

Reaktivnim mjerama djeluje se na Incidente u Republici Hrvatskoj te druge događaje koji mogu ugroziti računalnu sigurnost javnih informacijskih sustava u Republici Hrvatskoj.

Reaktivne mjere podrazumijevaju[24]:

- na osnovu prikupljenih saznanja izrađuju se i distribuiraju sigurnosna upozorenja, javno ili ciljano
- Nacionalni CERT prikuplja, obrađuje i priprema sigurnosne preporuke o slabostima u informacijskim sustavima te ih javno distribuira i arhivira u svom informacijskom sustavu
- koordinacija rješavanja značajnijih Incidenata u koje je uključena barem jedna strana iz Republike Hrvatske

### 7.4.AZOP

AZOP to jest Agencija za zaštitu osobnih podataka za glavne ciljeve uzima učinkovito djelovanje na ispunjavanje svih prava i obaveza iz područja zaštite osobnih podataka koje se Republici Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe, tu spada i povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka vezano za primjenu propisa koji su obuhvaćeni zakonskim okvirom zaštite osobnih podataka u Republici Hrvatskoj uz odgovarajuću primjenu mjera informacijske sigurnosti.[25] Nadležnost Agencije je obavljanje nadzora nad obradom osobnih podataka sukladno Zakonu o zaštiti osobnih podataka. Agencija u okviru javnih ovlasti:

• nadzire provođenje zaštite osobnih podataka,

• ukazuje na uočene zloupotrebe prikupljanja osobnih podataka,

• rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom,

• vodi središnji registar,

[24] http://www.cert.hr/onama
[25] http://azop.hr/djelatnost-agencije/detaljnije/o-agenciji

• prati primjenu organizacijskih i tehničkih mjera za zaštitu osobnih podataka i predlaže poboljšanje tih mjera,

• o povredi prava na zaštitu osobnih podataka Agencija odlučuje Rješenjem,

• Agencija može predložiti pokretanje postupka kaznene ili prekršajne odgovornosti pred nadležnim tijelom,

• daje prijedloge i preporuke za unapređenje zaštite osobnih podataka,

• daje savjete u svezi s uspostavom novih zbirki osobnih podataka,

• nadzire iznošenje osobnih podatak iz Republike Hrvatske,

• prati uređenje zaštite osobnih podataka u drugim zemljama i surađuje s tijelima nadležnim za nadzor nad zaštitom osobnih podataka u drugim zemljama,

• obavlja i druge poslove određene Zakonom[26].

[26] http://azop.hr/djelatnost-agencije

# 8. ZAKLJUČAK

U ovom diplomskom radu možemo zaključiti da je uvijek potrebno ulagati u sigurnost informacijskog sustava, ulaganje u sigurnost informacijskog sustava je jedna od najvažnijih komponenata za svako poduzeće ili samog pojedinca. Ulaganjem u sigurnost smanjuje se rizik od opasnosti i smanjuje se rizik od prijetnji od napada na našu informacijsku sigurnost koje su svuda oko nas.

Informacijska sigurnost je disciplina kojoj je cilj osigurati zaštitu svih informacija i osigurati zaštitu pojedinih informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja. Neki od najvažnijih sigurnosnih mehanizama za informacijski sustav su: digitalni certifikat kojim zaštićujemo intelektualno vlasništvo i informacije i fizička zaštita a tu spada kontrola zaštite prostorija, zgrada i druge imovine, te su tu se uz pomoć mjera zaštite sprječava neovlašten pristup ili uništenje dobara. Jedan od najvažnijih kontrolnih postupaka je autentifikacija odnosno utvrđivanje pristupa korisniku temeljem identifikacije samog pristupnika. Prijetnjom sigurnosti nazivamo bilo koji oblik koji može izazvati rušenje zaštite, prijetnje mogu biti prirodne vrste u obliku nepogoda, namjerne ili nenamjerne prijetnje sigurnosti. Napadi mogu biti aktivni ili pasivni. U današnje vrijeme najčešći oblici napada su : virusi, crvi, trojanski konji, spam, hoax..

Danas u svijetu postoje hakeri, to su ljudi koji odlično poznaju računala, često se za njih kaže da su kriminalci, ali nisu svi hakeri kriminalci postoje i hakeri koji rade na razvoju sustava čija je svrha poboljšati sigurnost informacijskih sustava.

U RH postoje institucije koje se bave zaštitom i sigurnošću informacijskog sustava a to su : UVNS, ZSIS, NCERT i AZOP.

Temelj svakog uspješnog poslovanja je imati uspješne i lojalne zaposlenike. Nekada su virusi bili puno popularniji i uništavali su informacijski sustav, ali tih virusa imamo i danas ali s obzirom na sve vrste dostupnih antivirusnih sustava i sistema, mnogo brže i lakše se detektiraju i rješavaju. Jedna zanimljiva činjenica koju sam zaključio je da ako na bilo koji od današnjih Microsoft Windows operacijskih sustava ne instalirate niti jedan antivirusni program, ako imate samo sustav prosječna brzina zaraze vašeg informacijskog sustava ako surfate svaki dan internetom će biti 16 sekundi. Na osnovu ove činjenice možemo zaključiti

kako su antivirusni sustavi zapravo neophodni za svakog pojedinca koji posjeduje informacijski sustav.

# 9. LITERATURA

**KNJIGE:**


1. Antoliš, K.,et al, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010
2. Hadjina, N., Zaštita informacijskih sustava. Zagreb: FER, 2009.
3. Klasić, K., Klarin, K., Informacijski sustavi: načela i praksa. Zagreb : Intus informatika, 2009
4. Šehanović, J., Hutinski, Ž., Žugaj, M., Informatika za ekonomiste, Tiskara Varteks, 2002
5. Tuđman M., D. Boras, Z. Dovedan, Uvod u informacijske znanosti, Zagreb: FF, Zavod za informacijske studije, 2004.


**ČLANCI**


1. Članak 2. Zakona o informacijskoj sigurnosti, NN 79/07


**WEB IZVORI:**


1.http://www.referenceforbusiness.com/management/Comp-De/Data-Processing-and-DataManagement.html ( 01.04.2016.)

2.http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf ( 01.04.2016.)

3. http://www.informatika.buzdo.com/s870-informatika-u-praksi.htm ( 01.04.2016.)

4. http://www.cps-zg.hr/poslovna-sigurnost/sigurnost-u-poslovanju/ (03.04.2016)
5. https://hr.wikipedia.org/wiki/Nacionalna_sigurnost (03.04.2016)
6. http://web.efzg.hr/dok/MAR/avuletic/01_Pojam%20sigurnosti.pdf (03.04.2016)
7. https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjxtt-JiJnMAhXjFZoKHb9zCe0QFggZMAA&url=http%3A%2F%2Ffoiskripte.com%2Fwp-content%2Fuploads%2F2014%2F11%2Fsigurnost_informacijskih_sustava-

skripta.doc&usg=AFQjCNGFXXydyM8bPrkb3EauU4q1rVtRpw&sig2=95FQRD8KrxpTz0B-sAFmsA&bvm=bv.119745492,d.bGs (03.04.2016)

8. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-135.pdf (07.04.2016.)
9. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (07.04.2016.)

10.http://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh (07.04.2016.)

11.https://www.zsis.hr/default.aspx?id=13 (16.04.2016.)

12.http://www.cert.hr/onama (18.04.2016)

13.http://azop.hr/djelatnost-agencije/detaljnije/o-agenciji (19.04.2016.)

14.http://azop.hr/djelatnost-agencije (19.04.2016.)

15.http://hr.n1info.com/a53701/Svijet/Svijet/Najveci-hakerski-napad-na-SAD-u-povijesti.html (19.09.2018.)

16. http://balkans.aljazeera.net/vijesti/u-toku-globalni-hakerski-napad(19.09.2018)

17.https://www.radiosarajevo.ba/vijesti/svijet/americke-kompanije-na-meti-ruskih-hakera/307486(19.09.2018)

18. http://security.foi.hr/wiki/index.php/Mobilno_bankarstvo(26.09.2018)

**OSTALI IZVORI**

1) NCERT-PUBDOC-2010-06-304
2) Graziadio Business Report
3) FTHM, SIS T1 predavanje

## *POPIS SLIKA*

Slika 1. Podjela informacijskog sustava na podsustave…….…….4

Slika 2: Elementi nacionalne sigurnosti…….8

Slika 3. Grafički prikaz digitalnog certifikata…….……..10

Slika 4. Prikaz slojevite fizičke zaštite…….....……12

Slika 5. Prikaz kartice za identifikacije…….…….....…..14

Slika 6. Token uređaj……..…..15

Slika 7. Primjer Phishing napada…….….20

Slika 8. Prikaz uloge UVNS-a u sustavu RH…….……..22

## *POPIS GRAFIKONA*

Grafikon 1. Prikaz sigurnosti kroz razine koje se kombiniranjem spajaju u istu cjelinu……..…6

Grafikon 2. Prikaz dobivanja certifikata……11

Grafikon 3. Uzroci gubitka podataka ( izvor: Graziadio Business Report)……19