Originalni naučni rad

UDK 007:[004.738.5:338.46

DOI 10.7251/SVR1918285M

ZAŠTITA I SIGURNOST INFORMACIJSKIH SUSTAVA

Doc. dr Marijan Mijatović[1]

Nezavisni Univerzitet Banja Luka

Apstrakt: U današnjem vremenu postoje sigurnosne prijetnje i opasnosti zbog razvijanja i korištenja a samim time i održavanja kompletnog informacijskog sustava. Veliku pozornost treba posvetiti zaštiti informacijskih sustava.

Kompletnim razvojem informacijski sustava pojavljuje se sve veća prijetnja i opasnost prema tom sustavu kao i brojnim napadima na poljima informatike. Da bi se spriječile sigurnosne prijetnje i opasnosti mora se posvetiti velika pozornost na sigurnost informacijskih sustava. U ovom radu predstavljene su najpoznatije vrste prijetnji i opasnosti koje se mogu pojaviti u informacijskom sustavu.

Ključne riječi: *sigurnosne prijetnje, klasifikacija napada, zaštita računala, zlonamjerni programi, opasnost*

UVOD

U današnje vrijeme informacijski sustavi se sve više i više razvijaju i postaju složeniji za korištenje, a i njihovo održavanje postaje sve kompleksnije. Upravo zbog takvog ubrzanog rasta i razvoja, javljaju se problemi oko nadzora i same zaštite informacijskih sustava. Kako se ubrzano razvijaju informacijski sustavi, tako i postoji veliki trend u rastu sigurnosnih prijetnji i napada u informatičkoj domeni. Zbog velike složenosti informacijskih sustava koji se danas razvijaju, oni su često izloženi različitim vrstama prijetnji i napada što može izazvati mnoge različite vrste oštećenja, i prouzročiti ogromne štete. Štete se kao takve mogu kretati od malih gubitaka do velikih oštećenja cijelih informacijskih sustava i gubitak mnogih podataka na računalu.

U ovom radu kratko je objašnjena zaštita i sigurnost informacijskih sustava, te što su to napadi i prijetnje na informacijski sustav. Bit će navedene najpoznatije vrste napada i prijetnji, odnosno njihova klasifikacija kao i kratki opis nekih od zlonamjernih programa koji mogu nanijeti i ogromnu štetu našem operacijskom sustavu

ZAŠTITA INFORMACIJSKIH SUSTAVA

Pojam zaštite informacijskih sustava usko je vezan uz pojam sigurnosti informacijskog sustava, no ipak postoji određena razlika. Zaštita

[1] Doc dr na Fakultetu za informatiku Nezavisnog univerziteta Banja Luka

informacijskih sustava može se definirati kao „niz poduzetnih mjera kojim se osigurava željena razina funkcionalnosti operativnog sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji“. S druge strane, sigurnost informacijskog sustava je „niz mjera poduzetih prilikom njegova projektiranja kako bi se ostvarila funkcionalnost sustava u uobičajenim uvjetima djelovanja“. Također, zaštita se odnosi na niz mjera i postupaka koji se poduzimaju kako bi se osiguralo normalno funkcioniranje informacijskog sustava bez narušavanja njegovog integriteta.

Kada se govori o sigurnosti, uzima se u obzir nekoliko činitelja: sigurnost podataka, sigurnost pristupa podacima, sigurnost informacijske tehnologije i sigurnost komunikacija[2]. Prilikom razmatranja sigurnosti, ono što je najbitnije je uzeti u obzir procjenu značaja podatkovnog sadržaja, procjenu djelovanja pretpostavljenih oblika prijetnji, poduzimanje mjera za smanjenje rizika i kontrolu i nadzor nad postojanošću sigurnosti informacijskog sustava.[3]

Ono što je svrha svakog informacijskog sustava je zaštititi sadržaj koji se nalazi na računalu i to: povjerljivost, integritet i dostupnost. Navedeni pojmovi čine tzv. trokut informacijske sigurnosti (eng. CIA – Confidentiality, Integrity, Availability), odnosno model koji se koristi za njenu procjenu u pojedinoj informatičkoj organizaciji. Takav model je je stvoren da bi se mogao osigurati osnovni standard za procjenu i provedbu informacijske sigurnosti bez obzira na temeljni sustav.

Povjerljivost se odnosi na to da se osigura pristup podacima i informacijama od ovlaštene osobe. Tu spadaju lozinke korisnika i popisi onih koji imaju kontrolu pristupa podacima te se na temelju takvih metoda postiže povjerljivost.

Integritet se odnosi na osiguravanje pouzdanosti i efikasnosti podataka koje se postiže preko raznih šifriranja podataka i algoritama. Pouzdanost omogućuje to da samo ovlaštene osobe mogu imati pristup i mijenjati podatke te da iste se ne mogu promijeniti bez ovlaštenja. Upravo je integritet podataka zadužen za to da sprječava neovlaštenim korisnicima promjenu podataka ili programa. Integritet se može izgubiti u slučaju da neovlaštena osoba napravi bilo kakve izmjene nad podacima ili korigira sadržaj na istom.

Dostupnost kao treći dio trokuta informacijske sigurnosti navodi da su podaci dostupni kada su potrebni. Cilj dostupnosti je osigurati korisnicima informacije kada im trebaju, a u slučaju uskraćivanja podataka, dostupnost informacijskog sustava se može lako izgubiti. Prema svemu navedenome, informacijski sustav je djelotvoran ukoliko zadovoljava sva tri aspekta.[4]

U informacijskim sustavima postoji velika vrsta napada i prijetnji koji se klasificiraju prema različitim kategorijama. Neki od tih napada su iznimno štetni za nas dok postoje oni koji su i bezopasni. Napadi mogu doći

[2] Klasić, 2007

[3] Hutinski, 2013

[4] Techopedia, 2018; Juran, 2014

od različitih izvora, odnosno od korisničke aktivnosti ili hakerskog učinka. Kao što je navedeno ranije, zbog svoje složenosti, informacijski sustavi su sve više i više podložni razno raznim napadima od strane različitih izvora te prijetnjama koji ga mogu ugroziti. Napadi i prijetnje kao takve mogu prouzročiti neželjenu situaciju kroz ranjivost imovine na temelju čega nastaje velika šteta.

Slika 1. CIA trokut zaštite informacijskog sustava

NAPADI I PRIJETNJE

Napad se definira kao akcija koja je usmjerena na ugrožavanje sigurnosti informacija kao i računalnih sustava i mreža. Prijetnje su potencijalni uzroci neželjenog događaja koji može imati za posljedicu određenu štetu za sustav te imovinu ili neku organizaciju.[5] Napadi se kao i prijetnje klasificiraju prema raznim kategorijama te će podjela istih biti navedena u nastavku.

Prijetnje se mogu podijeliti i prema izvoru te se također mogu grupirati prema raznim područjima: kvarovi na opremi, pogreške zaposlenika, fizičke prijetnje, logičku i komunikacijsku infiltraciju. Prijetnje također imaju i svoja obilježja te ona mogu biti unutarnjeg ili vanjskog izvora, imati motiv, učestalost pojavljivanja, razornu moć ili biti prirodnog oblika kao i uzrokovana ljudskim djelovanjem. Jedna od važnih karakteristika prijetnje je to da ona kao takve ne predstavlja rizik kada nema ranjivosti informacijskog sustava koju može iskoristiti. Stoga je kod određivanja neke prijetnje, bitno razmotriti samu vrstu prijetnje, potencijalne ranjivosti informacijskog sustava i postojeće kontrole kojima se sprječava utjecaj prijetnje (Stojaković – Čelustka S., s.a.)

Najčešći oblici prijetnji sigurnosti informacijskog sustava prema izvoru su namjerne i nenamjerne prijetnje ljudi, prirodne nepogode i od strane same opreme. Što se tiče namjernih postupaka ljudi, tu spadaju krađa, razni neautorizirani pristupi, virusi i maliciozni programi, namjerni oblici uništenja, ratno razaranje i slično. Nenamjerne prijetnje obuhvaćaju radnje za koje čovjek nije svjestan, a to su većinom nepažnja prilikom korištenja kao i nemar te neznanje. Prirodne nepogode obuhvaćaju ono na što čovjek

[5] Vukelić, 2016

kao takav ne može utjecati, a mogu uzrokovati velike štete informacijskim sustavima. To su požari, potresi, poplave, oluje i slično. Kvar na opremi, tehničke pogreške, prestanak napajanja, zračenja i prekidi komunikacije spadaju pod kategoriju opreme kao prijetnje informacijskim sustavima.

Prema provedenim istraživanjima, više od 50 % problema u informacijskim sustavima su nastali na temelju ljudske pogreške. Da bi se spriječili takvi propusti i zaštitio informacijski sustav neke organizacije, potrebno je provesti odgovarajuće mjere. Neke od tih mogu biti između ostalog i educiranje zaposlenika. Time se može zaustaviti uništenje integriteta i same sigurnosti pojedinih informacijskih sustava. Također, da bi se spriječili kvarovi računalne opreme, što je također jedan od većih uzroka prijetnji, korisno je da ona bude smještena u sigurnosne posebne prostorije te je važno da bude zaštićena od neovlaštenih upada. U takvim prostorijama je potrebno održavati dobru temperaturu i vlagu. Ostalu vrstu napada koji dolaze izvana, sprječavaju se na način da se kontrolira promet koji dolazi s interneta te jednako tako i sprječavanjem instaliranja raznih programa i kriptiranje važnih podataka. Uz to, za maksimalnu sigurnost sustava, potrebno je obratiti pažnju na fizičku sigurnost, sigurnosne mjere za osoblje, sigurnost komunikacija i operacijsku sigurnost.[6]

KLASIFIKACIJA I METODE NAPADA NA INFORMACIJSKI SUSTAV

Kao što je navedeno ranije, napad je u osnovi akcija ili neka radnja koja je usmjerena na ugrožavanje sigurnosti informacija i samog informacijskog sustava i računalnih mreža. Najčešći motivi napada su ostvarenje štete ili samodokazivanja napadača. Jednako kao i prijetnje, i napadi se dijele prema raznim kategorijama: prema cilju kojeg nastoje ostvariti, oblicima, izvoru te metode napada. Uz to, postoje mnoge razne podjele napada te će u nastavku biti navedene neke od njih.

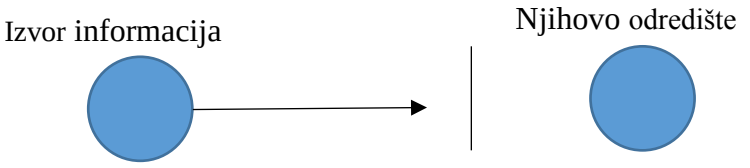
Napadi prema cilju kojeg žele ostvariti mogu biti: napad pristupa, napad modifikacije, napad uskraćivanjem usluge. Napad pristupa se odnosi na to da napadač želi zadobiti pristup određenim resursima i informacijama za koje nije ovlašten te je to njegov cilj. Napad u kojem napadač želi izmijeniti podatke za koje također nema pristup te nije ovlašten spada u drugu vrstu napada, modifikaciju. Treća kategorija prema podjeli na temelju cilja je napad uskraćivanjem usluge gdje napadač želi prekinuti rad kompletnog informacijskog sustava.

Metode napada na informacijski sustav su sljedeće: metoda napada prekidanjem ili presijecanjem, metoda napada presretanjem, izmjena ili promjena sadržaja i proizvodnja ili izmišljanje poruka.

Metoda napada prekidanjem usluge između dva korisnika je vrsta aktivnog napada gdje napadač sprječava isporuku informacija do krajnjeg korisnika. Nakon ostvarenja pristupa korisničko mreži, napadač je u

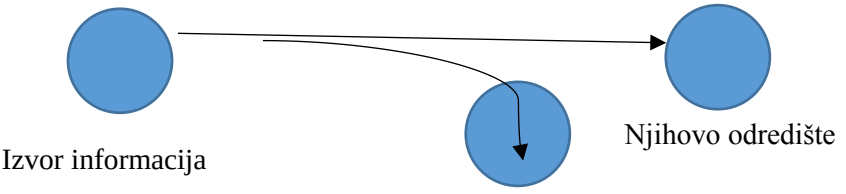
[66] Kovačević, 2008

mogućnosti prikriti određene informacije kako bi se otkrila njegova prisutnost, zatim može slati nevažeće podatke programima ili aplikacijama kojima može da uzrokuje nestabilnost i prestanak rada istih. Uz to, ono što također može učiniti je opterećenost računala ili računalne mreže što može blokirati promet čime se dovodi do gubitka pristupa mrežnim resursima. Takvim napadom se narušava svojstvo dostupnosti informacije iz spomenutog trokuta sigurnosti informacijskog sustava.



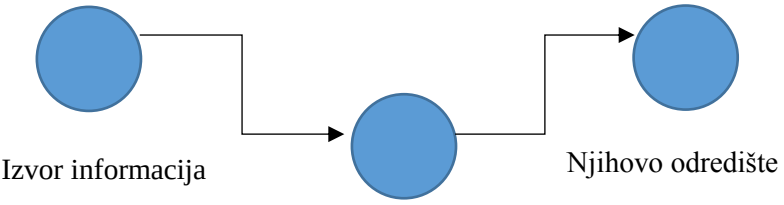
Slika 2. Metoda napada prekidanjem

Sljedeća metoda je metoda napada presretanjem koja se odnosi na napade s posredstvom neke treće osobe. Ona može pratiti i kontrolirati komunikaciju. Napadači koji koriste navedenu metodu se koriste presretanjem podataka na način da se ubacuju u komunikaciju između dva krajnja korisnika i preusmjeravaju poruke. Na taj se način ugrožava tajnost podataka. Karakteristika takvog napada je to što informacija dolazi do krajnjeg korisnika, no on ne zna da nju je netko drugi također preuzeo.



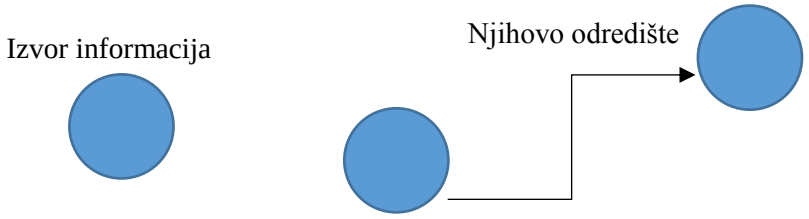
Slika 2. Metoda napada presretanjem

Treća metoda napada je izmjena informacija. Karakteristika takvog napada je to što napadač izmjenjuje informacije i poruke koje putuju od korisnika do korisnika. Izmjenjuje poruke bez znanja korisnika i to najčešće u svoju korist. Kod takve metode, napadač najprije prekida komunikacijski kanal te mijenja sadržaj poruke i prosljeđuje nju do primatelja. Uz to, lažno se predstavlja kao pošiljatelj. Navedeni napad može biti štetan naročito kod transakcija putem interneta. Ovakva vrsta napada je napad na integritet.



Slika 3. Metoda napada izmjenom

Četvrta metoda napada je napad proizvodnjom podataka i umetanjem lažnih informacijama. Takav napad je osmišljen za krađu i zlonamjerno iskorištavanje informacija. Kod takvog napada, napadač je usmjeren na slabosti i ranjivosti aplikacije i operacijskog sustava gdje može dobiti kontrolu nad procesima i samim aplikacijama. Kontrola može biti djelomična ili potpuna te je ovakva vrsta napada također napad na integritet informacijskog sustava.



Slika 4. Metoda napada proizvodnjom[7]

Slična podjela navedenoj je prema narušavaju sigurnosti i prijenosa informacija te se prema tome napadi svrstavaju u šest kategorija: prisluškivanje, prekidanje, lažno predstavljanje, izmišljanje poruka, promjena sadržaja poruka i poricanje.[8]

Uz navedene podjele, postoje dva oblika napada: (pasivni i aktivni). Pasivni napad je onaj gdje napadač ne djeluje aktivno na informacije te je time ugrožena samo tajnost podataka. Neke do metoda ovakvog napada su prisluškivanje ili otkrivanje sadržaja informacija. S druge strane, aktivni napad je onaj gdje napad kao takav može utjecati na funkcioniranje sustava ili na sam sadržaj poruke i informacija. Promjena sadržaja, metoda prekidanja i izmišljanje poruka spadaju u ovakav oblik napada.[9]

Neki od primjera napada su: DOS napad, krađa prijenosnog računala, neovlašteni pristup, virusi, financijske prijevare, zloupotreba bežičnih mreža, Bot programi, DNS napadi, krađa lozinki, sabotaža, proboj u sustav, telekomunikacijska prijevara, zloupotreba raznih programa i slično.

Zlonamjerni i štetni programi

Kada se govori o pojmu napada informacijskog sustava, većina ljudi to shvaća kao zlonamjerne programe, odnosno viruse ili crve. Takve programske i sistemske prijetnje su najčešće stoga će biti opisane u nastavku ovog rada.

Zlonamjerni ili zloćudni programi, tj. softveri (engl. malware) su posebno dizajnirani programi čiji je cilj oštećenje računala i informacijskog sustava bez znanja vlasnika, tj. takvi programi imaju zlonamjerne namjere. Općenito im je cilj krađa privatnih podataka ili otvaranje pristupa računalu bez korisničkog odobrenja. Uz krađu podataka, zlonamjerni programi šire

[7] Vukelić, 2016

[8] Oštrić D., 2015

[9] Pavlaković, 2008

različite neželjene poruke, uništavaju određenu imovinu te su sastavni dio računalnog kriminala.

Postoje različiti čimbenici koji mogu učiniti računalo ugroženim i ranjivim za potencijalne zlonamjerne programe, a najvažniji od njih su nedostaci u izradi operacijskog sustava. Nedostatak kod istog je to što se gotovo svim korisnicima daju potpuna prava pristupa za korištenje sustavom te se na taj način najčešće preuzimaju virusi. Najbolja zaštita za sprječavanje djelovanja zlonamjernih programa, odnosno njihovo preuzimanje je oprez kod korištenja računala te neotvaranje privitka u elektroničkim poštama. Jednako tako potrebno je svjesno koristiti Internet i ne otvarati sumnjive web stranica te izbjegavati instaliranje programa za koje korisnik nije siguran da je program u redu. Također, svako računalo mora posjedovati instalirani antivirusni program te ga redovito ažurirati i održavati (Norton.com, 2018).

Postoje razne vrste zlonamjernih programa, a najpoznatiji su računalni virusi i crvi. Tu se ubrajaju još i spyware, adware, spam, trojanski konj, rootkit, bootnet, keylogger i drugi. U nastavku će biti opisani neki od njih.

Računalni virus je vrsta zlonamjernog softvera koji se širi umetanjem, tj. infekcijom programa i postaje dio njega. Virus se širi s jednog računala na drugo te na taj način zlonamjerno djeluje na sva računala. Može štetno djelovati na podatke i softvere te može djelovati i uskraćivanjem usluge prema korisniku. Virus kao takav može postojati na sustavu, ali ne mora biti aktiviran te se može širiti dok ga korisnik ne pokrene ili ne otvori datoteku koja ga sadržava. Neki virusi mogu prebrisati druge programe, a šire se kada se softver ili datoteka na koji je povezan prenose s jednog računala na drugo pomoću računalne mreže, dijeljenja datoteka ili zaraženih privitaka unutar elektroničke pošte.

Računalni crv je sličan računalnom virusu međutim oni su samostalni softver i ne zahtijevaju programe domaćina niti ljudsku radnju prilikom pokretanja. Za širenje, računalni crvi iskorištavaju ranjivost unutar cijelog ciljanog sustava ili koriste neku vrstu socijalnog inženjeringa kako bi se pokrenuli i izvršili zlonamjernu radnju. Računalni crv ulazi u sustav kroz njegovu ranjivost.

Spyware se odnosi na programe koji nenamjerno prate aktivnosti na računalnom sustavu i prijavljuju te podatke drugim korisnicima bez pristanka vlasnika podataka. Spyware je instaliran na osobnom računalu te prikuplјuje podatke o korisnicima tog računala i njegovim samim karakteristikama te prati navike korisnika da bi ih slao nekom drugom. Uz to može preuzeti druge zlonamjerne programe i instalirati ih na računalo bez znanja korisnika.

Trojanski konj je jedan od vrste zlonamjernih programa, a predstavlja štetan dio softvera, koji nakon aktivacije, prouzrokuje štetu na većem broju datoteka kod zaraženog računala. Može uzrokovati nasumično otvaranje prozora ili promjenu radne površine na računalu kao i oštećenje datoteka korisnika, krađu podataka ili aktiviranje i širenje drugih zlonamjernih programa, poput virusa. Uz to, trojanski konj je poznati po tome što otvara neovlašteni pristup drugim zlonamjernim napadačima. Trojanski konj se ne

širi zarazom drugih datoteka niti se sam replicira, već putem interakcije korisnika preko privitaka unutar elektroničke pošte kao i pokretanjem preuzetih datoteka sa interneta.

Rootkit je tajni računalni program osmišljen kako bi osigurano kontinuirani pristup računalu dok aktivno skriva svoju prisutnost. Općenito je povezan s drugim zlonamjernim programima poput računalnih virusa, crve i trojanskim konjima. Rootkit omogućava izvršavanje naredbi i ima kontrolu nad računalom bez da vlasnih računala ima znanje o tim radnjama[10].

Zaštita informacijskog sustava od napada i prijetnji

S obzirom na veliku količinu prisutnih zlonamjernih programa kao i napada i prijetnji, računalo je potrebno zaštititi. Kao što je spomenuto ranije, preporučljiva je instalacija antivirusnoga programa. Od ostalih vrsta zaštite postoje i antispyware zaštita za spyware zlonamjerne programe. Uz to postavljanje vatrozida (engl. firewall) koji služi za blokiranje sumnjivih poruka te upozorava na to da li se korisnik želi spojiti na neku određenu stranicu na internetu ili preuzeti određeni sadržaj. Osim toga, dobro je znati da se ne preuzimaju datoteke za koje nitko ne garantira da su korisne i ne zaražene te da se poduzimaju mjere antivirusne provjere sadržaja istih. Također svaku datoteku prilikom preuzimanja valja testirati na viruse dok se datoteke unutar elektroničke pošte nepoznatog izvora ne preuzimaju[11].

ZAKLJUČAK

Današnji su informacijski sustavi zbog svoje složenosti podložni brojnim ranjivostima koje utječu na mogućnost napada i prijetnji. Takvi napadi mogu da uzrokuju velike i male štete svakog informacijskog sustava što dovodi do gubitka ili krađe podataka. Da bi se informacijski sustav zaštitio on mora zadovoljavati tri definirana aspekta: povjerljivost podataka i informacija od strane ovlaštene osobe, zatim integritet koji osigurava pouzdanost informacija i podataka te dostupnost tih podataka kada su potrebni. U informatičkom, tj. računalnom svijetu danas postoji vrlo mnogo vrsta napada i prijetnji na informacijski sustav.

Napad je akcija ili radnja čiji je cilj ugroziti sigurnost informacija te njihov sadržaj, sustava i mreža. Prijetnje su s druge strane uzroci neželjenog sadržaja koji radi štetu, a mogu biti ljudskog karaktera (namjerne i nenamjerne), kvarovi na računalnoj opremi te prirodne nepogode. Što se tiče napada, najpoznatije metode su metoda presijecanja, prekidanja, izmjene podataka i proizvodnja podataka. Pod pojmom napada, većinom se smatraju zlonamjerni programi čiji je cilj oštećenje računala i sustava bez znanja vlasnika. Najpoznatiji zlonamjerni programi su računalni virusi i crvi te trojanski konj i spyware. Od takvih programa se korisnik se možei mora na adekvatan način zaštititi instalacijom antivirusnoga programa i opreznim korištenjem računala i interneta.

[10] Cisco.com, 2018

[11] Bug.hr, 2010

INFORMATION SYSTEMS SECUIRITY AND PROTECTION

Marijan Mijatović PhD

Abstract: At present, there are security threats and dangers to develop and use and therefore to maintain a complete information system. Great care should be taken to protect the information systems.

With the complete development of the information system there is an increasing threat and danger to that system as well as numerous attacks on IT fields. In order to prevent security threats and dangers, great attention must be paid to the security of information systems. This thesis presents the most common types of threats and dangers that may occur in the information system.

Key words: *security threats, attack classification, computer protection, malware, danger*

LITERATURA

1 Cisco.com, (2018).: What is the difference: Viruses, Worms, Trojans and Boots?, www.cisco.com, dostupno https://www.cisco.com/c/en/us/about/security-center/virus-differences.html 10.1.2018.
2. Hutinski Ž., (2013): Sigurnost informacijskog sustava, skripta FOI, Varaždin, dostupno na https://www.scribd.com/document/71149222/17094401-Sigurnost-informacijskih-sustava, 8.1.2018.
3. Juran A., (2014): Sigurnost informacijskih sustava, diplomski rad, Pomorski fakultet u Rijeci, Rijeka, dostupno na http://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/290-2014.pdf 9.1.2018.
4. Klasić K., (2007): Zaštita informacijskih sustava u poslovnoj praksi. stručni rad, Zagreb, dostupno na https://hrcak.srce.hr/11861, 8.1.2018.
5. Kovačević D., (2008): Sigurnosna politika, diplomski zadatak, Fakultet elektrotehnike i računarstva, Zagreb, dostupno http://sigurnost.zemris.fer.hr/ISMS/2008_kovacevic/docs/SigurnosnaPolitika.pdf 10.1.2018.
6. Norton.com, (2018).: What is malware and how can we prevent it, www.us.norton.com, dostupno na: https://us.norton.com/internetsecurity-malware.html 8.1.2018.
7. Oštrić D., (2015): Sigurnosni aspekti i mjere zaštite informacijskih sustava, završni rad, Fakultet prometnih znanosti, Zagreb, dostupno https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A111/datastream/PDF/view 10.1.2018.
8. Pavlaković N., (2008).: Sustavi za otkrivanje napada, diplomski rad, Fakultet prometnih znanosti, Zagreb, dostupno http://sigurnost.zemris.fer.hr/ns/2008_pavkovic/Sustavi_za_otkrivanje_napada.html#_Toc213593969 , 10.1.2018.