BISEC

KONFERENCIJA O BEZBEDNOSTI INFORMACIJA

2014

ZBORNIK RADOVA

Univerzitet Metropolitan, Beograd
18. jun 2014.

www.bisec.rs

Izdavač
UNIVERZITET METROPOLITAN
Tadeuša Košćuška 63, Beograd
info@metropolitan.ac.rs
www.metropolitan.ac.rs

Za izdavača
Prof. dr Dragan Domazet

Urednik
Prof. dr Nedžad Mehić

Zbornik priredila
Katarina Jovanović

Programski Odbor Konferencije
Prof. dr Dragan Domazet
Prof. dr Nedžad Mehić
Doc. dr Miroslava Raspopović
Prof. dr Slobodan Jovanović
Dr Dragan Đurđevi
Dr Aca Aleksić

Organizacioni Odbor Konferencije
Katarina Jovanović
Petar Cvetković
Mladen Radić

Lektura i korektura
Katarina Jovanović
Prof. dr Nedžad Mehić

Prelom i dizajn
Petar Cvetković
Mladen Radić

Štampa:
Copy Print

Tiraž
50

Online verziju zborika možete preuzeti na:
http://bisec.rs/pdf/zbornik-radova-2014.pdf

TEME KONFERENCIJE BISEC 2014

1. BEZBEDNOST KLAUDA, DETEKCIJA UPADA I REŠENJA

2. ULOGA REVIZIJE U PRUŽANJU USLUGA

3. BEZBEDNOST INFORMACIJA I INFORMACINIH SISTEMA

4. FORENZIKA

5. BEZBEDNOST MOBILNIH PLATFORMI, PAMETNIH UREĐAJA I KOMUNIKACIJA

UVODNIČARI

Flying with Digital and Safe Landing
Branislav Vujović

Check Point Security report 2014
Daniel Safar

Atribute Based Identity Infrastructure and new EU regulation regarding Privacy Protection
Avram Adižes

UČESNICI PANEL DISKUSIJE

Revizija/audit – razlike između biznis i IT potreba
Vladimir Petrović

Primjena sigurnih i pravovremenih informacija i informacijskih tehnologija u otkrivanju prijevara u osiguranju
Novica Mihajlović

IT kontrole i revizija informacionih sistema
Stana Jovanović

Prevare i nezakonite radnje u finansijskom sektoru
Gordana Vukelić

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

MODEL BEZBEDNOG E-LEARNING OKRUŽENJA BAZIRANOG NA KLAUD TEHNOLOGIJI

SAFE E-LEARNING ENVIRONMENT MODEL BASED ON CLOUD TECHNOLOGY

FEĐA LEKIĆ
Fakultet informacionih tehnologija, Beograd, fedja.lekic.1761@metropolitan.ac.rs

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

Rezime: *Cilj ovog rada je razvoj i implementaciju modela bezbednog e-learning okruženja baziranog na klaud tehnologiji. Model je razvijen kao podrška računarskim predmetima u oblasti distribuiranih sistema, virtualizacije i klaud kompjutinga na Metropolitan Univerzitetu u Beogradu. Prednosti korišćenja klaud tehnologija i virtualizacije uključuju smanjenje troškova, bolju iskorišćenost hardverskih resursa, stabilno okruženje za rad informacionih sistema. Rad se posebno fokusira na bezbednost klaud kompjutinga i pokušava da odgovi na pitanje da li klaud tehnologija ima propuste u svojoj arhitekturi. U ovom radu će se objasniti principi funkcionisanja klaud tehnologija, prikazati konkretna konfiguraciju klaud sistema i objasniti način implementacije bezbednog IaaS klaud okruženja baziranog na OpenNebula rešenju.*

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

1. UVOD

Zastupljenost klaud tehnologija sve više raste. Pored korišćenja u poslovnim rešenjima, klaud tehnologije su se pokazale korisnim u različitim tehnološkim oblastima, u naučnim istraživanjima, kao osnova, baza za napredne sisteme. Sa osobinama kao što su bolja iskorišćenost hardverskih resursa, lakše upravljanje i proširenje klaud sistema, ne postoji oblast gde se klaud tehnologije ne mogu primeniti.

No, sa rastom primena klaud tehnologija pitanje bezbednosti postaje sve aktuelnije. 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.

Ali pre nego što se počne sa analizom bezbednost, treba odabrati klaud sistem koji će predstavljati osnovu, podlogu informacionog sistema kojeg želimo implementirati. Pored komercijalnih rešenja (Microsoft Azure, HP Cloud, Amazon Elastic Compute Cloud - Amazon EC2, Oracle Cloud, Google Cloud Platform) postoji više besplatnih, open source rešenja (OpenNebula, Open Stack, Eucaliptus i drugi) pomoću kojih se mogu realizovati kvalitetna klaud rešenja. U radu će se koristiti i testirati OpenNebula klaud sistem, o razlozima izbora, kao i opisu samog sistema će biti reči kasnije.

2. KLAUD KOMPJUTING

Principi na kojima se zasniva klaud kompjuting mogu se naći na samom početku razvoja računarskih tehnologija. Pre personalnih računara, dominantan oblik računarstva je bilo terminalno računarstvo [1]. Korisnici su se preko terminala povezivali na glavni kompjuter, koji je svakom korisniku dodeljivao deo procesorskog vremena za izvršavanje zadataka. Ovakav princip rada je bio efikasan način da se iskoristi pun potencijal računara, da ne bude praznog hoda u radu i nepotrebnih troškova.

Sa razvojem tehnologije, kompjuterska snaga raste, smanjuje se cena kompjuterskih komponenti i dolazi do proizvodnje prvih personalnih računara. Mogućnost da se poseduje računar po pristupačnoj ceni, potiskuje terminalno računarstvo kao glavni vid korišćenja računara.

Potreba za što boljim korišćenjem dostupnih resursa, efikasnijim radom i nižom cenom kompjuterskih komponenti, je počela da vraća principe terminalnog računarstva u moderno računarstvo. Pojavljuju se distribuirani sistemi, koji raspoređuju izvršenje zadataka na nekoliko mašina, pri tom dajući privid da se radi o jednom sistemu. Ovim pristupom smanjuje se vreme potrebno za realizaciju zadataka uporedo smanjujući troškove. Razvojem internet tehnologija dolazi do povezivanja mašina koje nisu na istim geografskim lokacijama, ne utičući na opšte performanse sistema koji nad njima funkcioniše [5]. Formira se ideja, da se preko mreže nude hardverski resursi ili servisi ovih mašina. Na ovaj način, krajnji korisnici plaćaju samo hardver ili

softver koji koriste na udaljenim mašinama, jedino je potreban terminal (računar) preko kojeg mogu da pristupe uslugama [8][15]. Ovi sistemi predstavljaju osnov za oblast koju danas zovemo klaud kompjuting.

2.1. KLAUD KOMPJUTING I VIRTUALIZACIJA

Za krajnje korisnike, klaud kompjuting predstavlja način da iznajme hardverske resurse ili servise preko interneta, da svoje podatke pohrane na udaljenim mašinama, da im programi koje koriste uvek budu dostupni i sl. No, sa porastom korisnika klaud servisa, javlja se mogućnost da se uzrokuje preopterećenost servera i onemogući efikasno pružanje usluga. Jedan deo rešenja leži u principu raspoređivanja opterećenja koje su postavili distribuirani sistemi. Drugo rešenje je virtualizacija koja pruža maksimalnu iskorišćenost hardverskih resursa.

Korišćenjem virtualizacije omogućuje se napredna kontrola hardverskih resursa [6]. U okviru operativnog sistema domaćina (*engl. host computer*) kreiraju se virtualne mašine kojima se može dodeliti određeni broj procesora, količina RAM memorije, veličina hard diska. Krajnjim korisnicima se na osnovu njihovih potreba podešavaju virtualne mašine, koje se dalje mogu dopuniti neophodnim softverom.

U zavisnosti od potreba, postoje tri modela korišćenja klaud kompjutinga [1][7]:

1. IaaS (Infrastructure as a Service) model, u kome se nudi korišćenje hardverskih resursa kompjutera, virtualne mašine i operativne sisteme (npr. Amazon EC2, S3)
2. PaaS (Platform as a Service) model, u kome se nudi rešenje za razvoj softvera zasnovanog na klaud tehnologijama (npr. Google App Engine)
3. SaaS (Software as a Service) model, u kom se nude aplikacije na zahtev

Klaud sistem koji smo realizovali u okviru projekta predstavlja implementaciju IaaS modela u vidu privatnog oblaka. Koristeći OpenNebula klaud platformu, kreirali smo virtualne mašine sa Apache web serverima koji pokreću moodle e-learning sistem.

3. OPENNEBULA

OpenNebula je open source rešenje za izgradnju i upravljanje klaud sistema i virtualnih data centara. Osnovana kao istraživački projekat 2005. godine od strane Ignacio M. Llorente i Ruben S. Montero, relativno brzo, 2008. godine, OpenNebula biva puštena u javnost kao open source projekat. Kroz stalno razvijanje i promovisanje, OpenNebula postaje klaud platforma koja se koristi u mnogim velikim kompanijama (BlackBerry, Centos, BBC, Alcatel-Lucent, Nasa, Unity i mnoge druge).

OpenNebula ne predstavlja kompleksan sistem. Zasnovana na već postojećim tehnologijama, pruža kvalitetan način za brzo upoznavanje sa principima rada klaud računarstva i stvaranjem efikasnih klaud sistema. U suštini, ona je skup servisa na Linux operativnom sistemu koji jedinstveno funkcionišu u cilju kreiranja stabilne klaud platforme.

OpenNebula sistem se sastoji iz dva povezana dela:

- Front-end nod: OpenNebula server, centar upravljanja servisima, virtualnim mašinama
- Worker-nod: OpenNebula paket zadužen za pokretanje virtualnih mašina

S ovakvom podelom uloga između mašina (kompjutera) postiže se raspoređenje opterećenosti, garantujući brz odziv sistema, što je izuzetno važan faktor kod korisnika. Front-end služi za upravljanje sistemom dok su worker (radnički) nod-ovi zaduženi za sav težak rad, pri tom ne trošeći resurse na izvršavanje sporednih funkcija. OpenNebula pravi pregled svih radničkih nod-ova i prilikom podizanja novih virtualnih mašina traži onaj sa najmanjom opterećenošću radi pokretanja.

OpenNebula sistemom se upravlja pomoću jednog naloga, oneadmin koji je isti i za front-end nod i za radničke nod-ove i kreira se prilikom instalacije OpenNebula paketa. No, oneadmin nalog nema na svakom kompjuteru odvojeni direktorijum sa podešavanjima, nego se on u stvari deli od front-end nod-a sa svim radničkim nod-ovima. Sva OpenNebula podešavanja, slike virtualnih mašina, daljinske skripte za izvršavanje se dele i ista su za sve mašine. Na ovaj način, ostvaruje se puna kontrola nad sistemom, bez obzira na međusobnu udaljenost hardvera, tj. nod-ova i ostvaruje se transparentnost sistema.

Tehnologije, servisi koje OpenNebula koristi su već dostupni u okviru Linux repozitorijuma (bilo Ubuntu, Debian, RHEL i sl.). Neki od servisa koji se koriste pri distribuciji oneadmin podešavanja i slika virtualnih mašina su:

- SSH–Secure Shell, mrežni protokol za uspostavljanje komunikacije između dva računara
- NFS – Network File System, distribuirani fajl sistem, služi za deljenje fajlova preko mreže
- RPC – Remote Procedure Call, rutina za izvršavanje funkcija na udaljenom računaru

SSH omogućava OpenNebula serveru da uspostavi komunikaciju sa svojim radničkim nod-ovima. Prilikom konektovanja na radnički nod koristi se metoda automatizovane SSH prijave (engl. SSH passwordless login). To se postiže generisanjem SSH javnog i privatnog ključa za oneadmin nalog na front-end nod-u, koje je potrebno preneti na radničke nod-ove. Kako se to postiže? Uz pomoć NFS-a i RPC-a.

Glavni direktorijum gde OpenNebula pohranjuje sva podešavanja, SSH ključeve, slike virtualnih mašina, skripte za kontrolu sistema je /var/lib/one/ . Jednostavnost Open Nebule leži u tome što je potrebno samo distribuirati ovaj direktorijum preko svih mašina u OpenNebula sistemu.

Korišćenjem NFS-a i RPC-a se postiže distribucija direktorijuma i mapiranje njegove lokacije. Kada OpenNebula preko SSH pokuša da prijavi na radnički nod, proverava se javni i privatni SSH ključ za oneadmin korisnika. Pošto je /one/ direktorijum distribuiran od strane front-end nod-a, SSH ključ sa kojim radnički nod upoređuje prosleđene SSH informacije (oneadmin korisničko ime, lozinka) isti za kompjutere, OpenNebula se automatski prijavljuje na sistem i počinje sa izvršavanjem neophodnih skripti.

3.1. OPENNEBULA VIRTUALIZACIJA

OpenNebula ima mogućnost odabira različitih hipervizora, Kernel-based Virtual Machine – KVM, Citrix Xen ili VmWare ESX [2]. Odabir zavisi od potreba sistema koi razvijamo. Za razvoj klaud sistema u ovom radu, koristili smo KVM.

Ceo proces virtualizacije se odvija na radničkim nod-ovima, mašinama čiji je jedini zadatak da ustupe hardverske resurse virtualnim mašinama. Sem servisa za komunikaciju sa OpenNebula front-end nod-om, ove mašine nemaju druga opterećenja.

OpenNebula sadrži slike virtualnih mašina u Datastore. direktorijumu na front-end mašini. Kada se izda komanda za instanciranje virtualne mašine, slika se kopira na radnički nod i pokreće. Kod KVM hipervizora za pokretanje virtualnih mašina su zaduženi paketi libvirt i QEMU. Ukoliko ne naglasimo na kojem radničkom nod-u želimo da pokrenemo virtualnu mašinu, odabir radničkog nod-a se vrši tako da se postigne najviši stepen raspoređenja opterećenosti, odnosno radnički nod sa najmanjom trenutnom potrošnjom hardverskih resursa.

Virtualne mašine dobijaju pristup mreži pomoću bridged interfejsa (mrežno premošćavanje) koji se konfiguriše na radničkim nod-ovima. Ovim interfejsom omogućavamo deljenje fizičkog mrežnog uređaja između više različitih virtualnih mašina, tako da svaka dobije sopstvenu IP adresu odnosno da se na mreži prikaže kao odvojena fizička mašina.

Na radničkim nod-ovima se takođe pokreću i serveri za grafički pristup virtualnim mašinama. OpenNebula ima podršku za VNC i SPICE protokol. U okviru samog OpenNebula interfejsa dovoljno je očitati port virtualne mašine i krenuti sa radom.

3.2. PREDNOSTI OPENNEBULA SISTEMA

Neke od glavnih odlika OpenNebula klaud platforme:

- Fleksibilnost – kvalitetan način podnošenja velikog broja virtualnih mašina
- Otvoreni kod (Open Source) – mogućnost da sistem prilagodimo specijalnim zahtevima
- Jednostavnost – kada se ovlada, OpenNebula je jednostavan sistem za instalaciju i održavanje
- Stabilna – nakon instalacije i konfiguracije OpenNebula je sistem koji se odlikuje stabilnošću

OpenNebula klaud sistem smo odabrali pre svega zbog njene jednostavnosti, brze konfiguracije i kao dobrog primera za učenje osnova klaud računarstva. Pošto koristi već postojeće Linux servise, obilna dokumentacija omogućava da se razume kako svaki servis funkcioniše i koja je njegova uloga u OpenNebula sistemu. Faktor otvorenog koda, doprinosi transparentnosti funkcionalnosti, skoro sve funkcije su napisane u vidu skripti koje su lako razumljive i isto tako lake za modifikaciju.

Instalacija dolazi u dve varijante. Može da se instalira na Centos operativnom sistemu, odvajajući više vremena na konfiguraciju raznih sigurnosnih parametara i stvarajući poslovni klaud sistem ili može da se instalira na Ubuntu sistemu gde instalacija automatizovana i pruža se bolja sredina za eksperimentisanje.

Hardverski zahtevi su veoma važan faktor. OpenNebula pruža mogućnost integracije sa više različitih hipervizora, tako da ako npr. nemamo dovoljno jak procesor za KVM virtualizaciju, možemo da se odlučiti da koristimo XEN i slično.

Podržanost različitih standarda, integracije sa drugim open source servisima, korišćenje i integracija sa komercijalnim klaud sistemima, daje kvalitetan osnov za formiranje bezbednog modela e-learning okruženja zasnovanog na klaud tehnologiji.

3.3. H/S PLATFORMA

U zavisnosti od slučaja korišćenja OpenNebula klaud sistema, hardverski i softverski zahtevi mogu da se razlikuju:

- Na nivou virtualizacije: da li nam potrebna virtualizacija 64-bitnih operativnih sistema?
- Na nivou klaud sistema: da li implementiramo javni, privatni ili hibridni klaud?

Pitanje 64-bitne (hardverske) virtualizacije utiče na izbor procesora, samim tim i na cenu. Iako većina jačih, savremenih PC (Intel i3, i5, i7 ili AMD FX serija) ili serverskih (Intel Xeon ili AMD Opteron) procesora podržava hardversku virtualizaciju (Intel VT ili AMD-V) treba proveriti da li postojeći CPU podržava hardversku virtualizaciju.

Hardverska virtualizacija utiče na izbor hipervizora, tj. da li ćemo odabrati neki hipervizor koji ima mogućnost paravirtualizacije (kao npr. Citrix Xen) ako nemamo mogućnost hardverske virtualizacije ili ako imamo, da koristimo hipervizor koji može da iskoristi pun potencijal hardverske virtualizacije (Kernel-based Virtual Machine – KVM, Citrix Xen, Microsoft Hyper-V).

OpenNebula funkcioniše isključivo na Linux sistemima, izgrađena je tehnologijama koje su implementirane u njima i najčešće se koriste Centos i Ubuntu sistem, ili neki drugi derivati Red Hat Enterprise Linux sistema ili Debian-a. Ovi zahtevi važe za sve klaud sisteme, bilo komercijalna ili besplatna, open-source rešenja.

Za osnovu OpenNebula klaud sistema odabrali smo sledeću postavku:

- Hardver – jedna mašina, ponaša se kao OpenNebula server (front-end mašina) i radnička mašina (worker, služi za pokretanje virtualnih mašina). Hardverske specifikacije uključuju:
  - CPU: Intel i5, 3.2GHz, sa mogućnošću hardverske (64-bitne) virtualizacije
  - RAM: 4GB DDR3
  - HDD: 500GB (efektivnih 468GB)
- Operativni sistem: Linux Lubuntu [8], verzija 13.10, 64-bitni OS – derivat Ubuntu sistema sa lakim okruženjem (LXDE – Light Weight Desktop Enviroment)
- Hipervizor: Kernel-based Virtual Machine (KVM)

Prednost odabrane postavke leži, pre svega, u lakšem upravljanju, modifikovanju i testiranju OpenNebula sistema. Lubuntu sistem nam pruža stabilno okruženje za rad (između ostalog i veliki izbor pomoćnih programa rad) i malu potrošnju sistemskih resursa (stanje mirovanja ~100MB RAM, 0%-1% CPU).

S obzirom na visoku integraciju OpenNebula sistema sa Linux OS, instalacija je direktna i može se izvršiti preko linux paket menadžera (apt za Ubuntu). Instalacija se zasniva na podešavanju glavnog OpenNebula servera a potom radničkih nod-ova.

3.4. INTEGRACIJA E-LEARNING SISTEMA

Razvoj klaud sistema obično podrazumeva integraciju nekog postojećeg informacionog sistema u klaud okruženje. U ovom radu, integrišemo moodle e-learning sistem u OpenNebula klaud sistem.

Moodle je jedan od najpoznatijih e-learning platformi. Zasnovan na php-u nudi veliki broj proširenja (plugin-ova) i podešavanja svakog dela sistema. Sa kvalitetnom integracijom sa Linux sistemima, moodle predstavlja stabilnu platformu za razvoj našeg e-learning okruženja.

Danas se podrazumeva da visokoškolske institucije imaju neki oblik e-learning sistema, radi lakše distribucije materijala, održavanja predavanja, jednostavnije komunikacije između studenata, profesora. Ovakvi sistemi su obično hardverski zahtevni i od njih se očekuje, pored stalnog funkcionisanja, kvalitetan odziv za sve korisnike. Jedno rešenje je da stalno nadograđuju serveri novim i bržim hardverom, ali to iziskuje dosta novčanih sredstava, i ne garantuje bolju funkcionalnost sistema. Drugo rešenje jeste primena klaud tehnologija. Pametno upravljanje hardverskim resursima i deljenjem opterećenja među virtualnim mašinama daje adekvatan odgovor na probleme e-learning sistema [12].

Kreiranje virtualne mašine sa e-learning sistemom ide po istom principu kao da instaliramo na fizički kompjuter. Potrebno je odabrati operativni sistem (mi smo se odlučili za Lubuntu 13.10) i na njega instalirati potrebne pakete.
Instalacija moodle e-learning sistema je prilično direktna na Linux (ubuntu) sistemima. Svodi se na instalaciju Apache2 servera i php5, mysql dodataka za ispravno funkcionisanje sistema. Svi paketi su dostupni preko zvaničnih Ubuntu repozitorijuma.
Kreiranu virtualnu mašinu je potrebno ubaciti u OpenNebula sistem. Prvo se slika pretvara u odgovarajući format (RAW, .img) i potom preko OpenNebula Sunstone web intefejsa ubaciti u sistem.

4. BEZBEDNOSNI IZAZOVI OPENNEBULA KLAUD PLATFORME

Klaud tehnologije se obično koriste kao platforma za informacione sisteme koji imaju veliki broj korisnika ili kao datacentri. Zbog velikog obima protoka podataka, naročito privatnih, poverljivih, na faktore bezbednosti, sigurnosti i stabilnosti treba da se posveti izuzetna pažnja tokom dizajniranja klaud sistema [4][11]. Često, hardver klaud sistema je distribuiran na različitim lokacijama (čak i državama, npr kod Google Cloud Platform, Amazon EC2) tako da pored softverskih propusta na bezbednost utiču i spoljni faktori.

OpenNebula kao klaud platforma se pokazala efikasnom i stabilnom, no sada ćemo napraviti osvrt na OpenNebula bezbednosne izazove. Pre svega treba da istaknemo tri faktora koja utiču na bezbednost u OpenNebula sistemu:

- Bezbednosna konfiguracija OpenNebula platforme
- Bezbednost virtualnih mašina
- Bezbednost host računara (front-end i worker nods)

4.1. BEZBEDNOSNA KONFIGURACIJA OPENNEBULA PLATFORME

Tokom konfiguracije OpenNebula platforme mora se najviše obratiti pažnja na podešavanja mreže i pristupnih parametara mašina u okviru sistema [10]. Bilo koji propust otvara mogućnost onesposobljavanja ili preuzimanja kontrole nad celim sistemom.

Kod konfiguracije Sunstone web interfejsa treba odabrati jedan kompjuter, tj. IP adresu i port, sa kojeg ćemo pristupati interfejsu. Kod privatnih klaud sistema jeste jednostavnije podesiti Sunstone tako da je moguće pristupiti interfejsu sa bilo kog kompjutera u mreži, ali kad imamo slučaj da nam se radnički nod-ovi ne nalaze u lokalnom mestu (npr. kada koristimo hardver treće strane) otvaramo mogućnost da interfejsu pristupi zlonamerni korisnik sa bilo koje kompromitovane virtualne mašine ili radničkog noda.

Sunstone Web intefejs je baziran na Ruby on Rails framework-u. Testirali smo mogućnost sql injection napada i utvrdili da je web interfejs solidno zaštićen. Unošenje pristupnih podataka se obrađuje pomoću linux nativne komande find (za pronalaženje korisničkog imena u sqlite bazi) u kombinaciji sa OpenNebula deskripcijom lozinke. Iako se može umetnuti kod tako da se proslede instrukcije find komandi, OpenNebula sistem enkripcije i dekripciije lozinki onemogućava dalje umetanje koda.

Prilikom konfiguracije NFS servera, odnosno deljenja /var/lib/one/ direktorijuma, najbolja praksa je da se za svaki radnički nod u sistemu dodeli unos u exports fajlu umesto da se svim kompjuterima u mreži (i lokalnoj i van nje!) dodeli mogućnost kačenja. Ovde se javlja logistički problem ako se radi sa velikim brojem radničkih nod-ova (slučaj kod velikih poslovnih sistema) gotovo je nemoguće ispisati IP adrese svih nod-ova. Najbolji pristup je da se definiše domen IP adresa koje se dodeljuju radničkim nod-ovima. NFS predstavlja slabu tačku u OpenNebula platformi [1]. Pored mogućnosti da se zavara proveravanje korisničkih privilegija, NFS nije enkriptovani protokol [3].

Potrebno je pojačati SSH kontrolu. Kao svaki sistem, OpenNebula je podložna brute-force napadima. S obzirom da je glavni nalog oneadmin, potrebno je samo naći šifru. Sa alatima kao što su John The Ripper (razbija šifre van mreže) u kombinaciji THC Hydra (na osnovu liste šifri napada metu na mreži) moguće je nakon nekog vremena otkriti i lozinku [9]. Najbolje je ograničiti broj pokušaja prijavljivanja.

Ranije smo pomenuli da oneadmin korisnik ima punu kontrolu nad OpenNebula sistemom i u slučaju da je kompromitovan, npr. ako je došlo do promene lozinke oneadmin naloga, OpenNebula automatski onemogućava korišćenje sistema. Dobra praksa je da se stvori nekoliko administratora koji će pripadati oneadmin grupi korisnika. Oni će, u slučaju da je došlo do onesposobljavanja sistema, moći da imaju kontrolu i da izvršavaju sve funkcije.

4.2. BEZBEDNOST VIRTUALNIH MAŠINA

Virtualne mašine predstavljaju sigurnosni rizik zbog softvera, sistema koji se na njima pokreće [15]. U našem slučaju Moodle e-learning sistem koristi php i Apache2 web server. Ovi programi su podložni napadima preko sql injection ili korišćenjem sigurnosnih rupa u sistemu. Kada napadač ostvari pristup, najmanja šteta je da obori virtualnu mašinu. Problem nastaje kada pristupi lokalnoj mreži i utvrdi gde se nalazi OpenNebula server. Odatle je dovoljno da se iskoriste mane NFS servisa da bi se ušlo u sistem.

Prilikom integracije virtualnih mašina treba voditi računa 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.

4.3. BEZBEDNOST HOST RAČUNARA

Host računare treba konfigurisati tako da im je moguće pristupiti samo sa sigurnih lokacija [11]. Bilo koje otvaranje mreži, otvara mogućnost upada. OpenNebula server ima mogućnost osigurane komunikacije između front-end nod-a sa radničkim nod-ovima i virtualnim mašinama. Svaka veza se može osigurati OpenNebula pristupnim tokenima, koji služe za autentikaciju.

OpenNebula pruža dodatne mogućnosti pri konfiguraciji pristupnih parametara:

1. Autentifikacija klijenata [1]: može se realizovati preko standardne prijave sa korisničkim imenom i šifrom, primenom SSH protokola, LDAP autentifikacije ili x509 standarda
2. Podešavanja pristupa OpenNebula Sunstone Web interfejsu: pored osnovnih korisnika u osnovu OpenNebula sistema moguće je podesiti Sunstone da mu se pristupa preko spoljnog SSL proksija (npr. preko neke web aplikacije)
3. Podešavanja pristupa OpenNebula serverima: OpenNebula sadrži tri servera Sunstone, EC2, OCCI i za svaki je moguće dodatno podesiti pristup

Sa ovim podešavanjima ograničavamo pristup host računarima na nivou OpenNebula sistema. Bilo koje preuzimanje kontrole nad host računarima automatski ugrožava OpenNebula sistem.

5. PONAŠANJE OBEZBEĐENOG OKRUŽENJA

Za ispitivanje faktora bezbednosti pripremili smo dve verzije sistema, jednu u potpunosti konfigurisanu i drugu sa namerno ostavljenim propustima. Analizom koda i funkcionisanja sistema pronašli smo potencijalne bezbednosne ranjivosti. Testiranje smo vršili pomoću profesionalnog alata Metasploit framework koji sadrži bazu podataka iskorišćenja sigurnosnih rupa [14]. Na osnovu ovih testova dobili smo predstavu kako da formiramo bezbedno klaud okruženje.

Primenom Metasploit framework-a smo utvrdili smo 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.

Radi testiranja na test sistemu smo instalirali pakete sa sigurnosnim propustima. Odlučili smo da testiramo primere upada preko paketa za koje je utvrđeno da su kompromitovani: phpMyAdmin-5.2.2.3-all-languages, Samba protokol verzija 2.x - 3.x, Ruby 3.x. Na osnovu rezultata, zaključili smo da novije verzije Linux sistema pojačavaju faktor zaštite i onemogućavaju izvršenje već utvrđenih propusta.

6. SIGURNOSNE RUPE I ZLOUPOTREBE

Postavlja se pitanje koliko je sistem ranjiv ako dođe do upada u sistem. Za ispitivanje ovog problema, koristili smo podrazumevanu konfiguraciju OpenNebula sistema, bez sigurnosnih podešavanja. Formirali smo scenario koji predstavlja spoljni napad i prikazuje slabosti OpenNebula klaud platforme. Napad se sastoji iz nekoliko faza, od

upada u sistem, iskorišćenja propusta u NFS funkcionisanju do samog onesposobljavanja sistema.

Za potrebe ovog scenarija pretpostavljamo da je napadač uspeo da dobije pristup internoj mreži klaud sistema.

Sa ostvarenim pristupom internoj mreži OpenNebula sistema, može da krene sa nizom akcija da pronađe glavni OpenNebula server. Za pretragu mreže najjednostavnije je koristiti široko poznati nmap program [9].

Iz liste pronađenih biramo kompjuter koji nam izgleda najverovatnije kao server. Dalje prelazimo na skeniranje otvorenih portova ciljanog kompjutera. Potrebno je da ciljani kompjuter ima otvoren port 111, što je port za rpc servis, koji je deo NFS servisa.

Ako ciljni kompjuter ima otvoren port 111, treba proveriti da li deli OpenNebula direktorijum /var/lib/one/. U slučaju da deli kreće se sa zloupotrebom NFS servisa.

NFS servis služi za deljenje direktorijuma preko mreže. Koristi servis rpcbind da omogući da deljene direktorijume koriste samo oni korisnici koji imaju odgovarajuće privilegije. Kada se korisnik proverava gleda se njegov jedinstveni ID (UID) u linux sistemu kao i ID grupe (GUID). Nema dodatnih provera.

Zloupotreba se zasniva na tome da kada prvi put preuzme deljeni direktorijum, očitaju se UID i GUID privilegovanog korisnika. Potom kreiramo novog korisnika koji će da imitira pravog. U fajlu /etc/passwd je potrebno izmeni generisane ID-ove sa očitanim i sledeći put kada se preuzme deljeni direktorijum, ulogujemo kao korisnik kog smo napravili za imitiranje i preuzmemo punu kontrolu nad direktorijumom. Kada se dobije pristup direktorijumu, dovoljno je samo da se iščita one_auth fajl u .one direktorijumu.

Sa one admin privilegijama zlonamerni korisnik može da:

- pristupi Sunstone web interfejsu i napravi štetu radničkim nod-ovim, virtualnim mašinama i drugoj virtualnoj infrastrukturi
- Ubaci maliciozan kod u OpenNebula skripte
- Onesposobi u celosti oneadmin nalog i time sistem
- Čita osetljive podatke iz one.db baze podataka

7. ZAKLJUČAK

Rad opisuje razvoj i implementaciju modela bezbednog e-learning okruženja baziranog na klaud tehnologiji. Model je uspešno testiran u realnim uslovima i pokazalo se da klaud tehnologije mogu da pruže stabilnu osnovu za pokretanje i dalji razvoj e-learning sistema. Takođe, pokazalo se da klaud platforme mogu da pruže pristojno okruženje za rad, ostavljajući prostor za detaljnu konfiguraciju bezbednosnog aspekta. Virtualne mašine postižu bolju iskorišćenost hardverskih resursa, dok OpenNebula server vodi računa o opštoj opterećenosti sistema. Dva najvažnija faktora bezbednosti sistema su bezbednost mreže i kontrola pristupnih parametara. Bez obzira na napore da se sistem učini neprobojnim, dovoljan je samo jedan propust da dođe do onesposobljavanja sistema zbog toga, jer upravo princip rada klaud sistema ga čini ranjivim iznutra.

Budući rad uključuje proširenje sistema dodavajem host čvorova, poboljšanje performansi i kapaciteta skladišta podataka, dodatne karakteristike kao što je nadgledanje sistema i slično.

LITERATURA

[1] L. Wang and G. v. Laszewski, "Scientific Cloud Computing: Early Definition and Experience," 26 Oktobar 2008. [Online]. Dostupno na : http://cyberaide.googlecode.com/svn/trunk/papers/08-cloud/vonLaszewski-08-cloud.pdf.

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

[3] 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.

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

[5] 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.

[6] 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/8A05CF4FBE8E4E40852574890056B096/$File/rc24590.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] A. Fernandez, D. Peralta, F. Herrera and J.M.Benitez, "An Overview of E-Learning in Cloud Computing," [Online]. Dostupno na: http://sci2s.ugr.es/publications/ficheros/2012-LTEC-Fernandez-E-Learning_CC.pdf.

[13] 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.

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

[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.

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

KLAUD RAČUNARSTVO I ZAŠTITA PODATAKA

CLOUD COMPUTING AND CRYPTO PROTECTION OF INFORMATION

MERIMA UROŠEVIĆ
Vojska Srbije, Vojna akademija, Beograd, merima_15@yahoo.com

MILORAD MARKAGIĆ
Univerzitet odbrane, Vojna akademija, Beograd, milmarkag@yahoo.com

Rezime: *Rad predstavlja kratak pregled klaud računarstva, sa modelima primenjenih metoda korišćenja i osnovnih postulata koji definišu ovu oblast.U jednom delu poseban osvrt dat je na zaštiti podataka i klaud okruženju, metodama zaštite i kriptografiji, kao jednoj od metoda zaštite. Oblast zaštite podataka u kludu nije temeljno definisana i vrlo je malo javno dostupnih rešenja, a kriptografijom u klaudu se u narednom periodu mora temeljnije pozabaviti. U radu su date samo osnovne pretpostavke zaštite i metoda kriptozaštite informacija.*

Ključne reči: *klaud, zaštita, kriptografija*

Abstract: *This paper presents brief overview of cloud computing with models of applied metods of use and basic principles that define this area. Special attention was given to information security and cloud surroundings, methods of protection and cryptography as one of the secutity measures. Information security within the cloud is not clearly defined as there are very few publicly available solutions. In future works problems of cryptography within the cloud must be examined in more detail.Paper contains only basic assumptions about security and crypto protection of information.*

Keywords: *cloud, protection, cryptography*

1. UVOD

Pojavom klaud računarstva (eng. cloud computing) ili računarstva u oblaku, kako se još naziva, menja se naš način razmišljanja o pojmovima "naš sistem" i "naši podaci", jer se oni pojavom klaud računarstva fizički više ne čuvaju na specifičnom, lokalnom skupu računara, već postaju raširenі, odnosno geografski distribuirani resursi. Međutim, u takvoj arhitekturi znatno je teže držati stvari pod sopstvenom kontrolom, tako da među korisnicima postoji određena zabrinutost u pogledu ograničenja i potencijala koje klaud računarstvo nudi. Da bi se bolje sagledala ograničenja i potencijali potrebno je klaud računarstvo sagledati sa nekoliko različitih aspekata, ekonomskih, zakonskih i tehničkih.

Sam termin oblak (eng. cloud) u imenu ove tehnologije potiče od prastarog označavanja Interneta među stručnjacima, u ranom periodu globalne svetske mreže. Tada se prostor i sva njegova svojstva između umreženih računara označavao oblakom, a povezani računari nisu bili „svesni" šta se u njemu nalazi. Odatle naziv Cloud Computing, jer aplikacije postoje na „oblaku" Web servera.
Još uvek ne postoji konsenzus oko toga šta termin klaud računarstvo zapravo znači. Bez obzira na nepostojanje konsenzusa pogledaćemo određene definicije koje će pomoći da se objasni pojam klaud računarstva i šta on predstavlja.

"Klaud računarstvo je model koji omogućava pogodan, na zahtev mrežni pristup računarskim resursima (mreže, serveri, diskovi, aplikacije i servisi) koji se mogu brzo rezervisati ili osloboditi uz minimalan napor ili interakciju sa pružaocem servisa" - U.S. National Institute of Standards and Technolog

"Klaud računarstvo je tip paralelnog i distribuiranog sistema koji se sastoji od skupa međusubno povezanih virtuelnih računara koji se dinamički mogu rezervisati i koji se mogu ponašati kao jedan ili više unificiranih računarskih resursa baziranih na SLA (ugovor šta servisi treba da isporuče i na koji način) između pružaoca servisa i korisnika" - R. Buyya, C.S Yeo, and S.Venugopal.

2. INFRASTRUKTURA PRUŽAOCA USLUGA KLAUD RAČUNARSTVA

Pod pojmom Cloud Computing podrazumeva se korišćenje tj. iznajmljivanje računarskih resursa od specijalizovanih kompanija koje nude te servise (Managed Service Providers). Oni nude široku lepezu servisa koji se naplaćuju na godišnjem ili mesečnom nivou. Suština je u tome da kompanije koje koriste usluge Cloud-a, plaćaju upravo onoliko koliko

računarskih resursa i koriste. Glavna prednost Cloud Computing koncepta je što ne postoji inicijalno ulaganje u informacioni sistem, a to je jedna od glavnih prepreka za razvoj informacionih sistema malih kompanija, jer treba izdvojiti ogromnu količinu novca za njihovu implementaciju.

Cloud Computing predstavlja isporučivanje IT resursa i servera na daljinu, putem Interneta, telefonske ili privatne mreže. Koncept je proizašao iz ideje iznjmljivanja IT resursa (CPU, memorija, storage prostora...) kao usluge koja se plaća na osnovu korišćenja. Cloud Computing karakterišu:

- Velika fleksibilnost,
- Niski troškovi korišćenja,
- Nezavisnost uređaja i lokacije,
- Mogućnost deljenja resursa,
- Pouzdanost,
- Stalabilnost i
- Bezbednost

Na osnovu ugovora o servisima, pružalac klauda skalira računarske resurse da bi odgovorio na potrebe korisnika koje se menjaju vremenom. Ugovor je značajan i za pružaoca klaud servisa jer on nema neograničen broj računarskih resursa tako da će na osnovu ugovora naći skup resursa koje treba rezervisati da bi se odgovorilo na zahteve korisnika i na taj način zadovoljiti odgovarajuće nivoe ugovora. Održavanjem i nadogradnjom računarskih resursa, bez obzira da li se radi o hardverskim ili softverskim, upravlja pružalac klaud servisa.

3. MODELI KLAUD SERVISA

Klaud računarstvo se može klasifikovati u jednu od tri grupe zavisno od servisa koje pružaju. Za opis tipa koristi se obrazac XaaS, koji je uveo Scott Maxwell 2006. godine, gde je X **I**nfrastruktura, **P**latforma ili **S**ervis. Važno je napomenuti da ovi servisi nisu međusobno isključivi nego da svaki od tipova predstavlja osnovu na koju se naslanja drugi tip. Tako Saas se naslanja na PaaS koji se opet naslanja na IaaS.

Infrastruktura u vidu servisa (engl. Infrastructure-as-a-Service, IaaS)

Računarska infrastruktura, kao što su server, skladištenje podataka i umrežavanje ostvaruju se u vidu Cloud Computing-a korišćenjem virtuelizacije. Umesto da kupi servere, softver, prostor u Data centru i mrežnu opremu, korisnik sve pomenute može da koristi u obliku virtuelnih servisa. Ovaj tip usluge obezbeđuje fundamentalne resurse kao što su snaga procesuiranja, prostor za skladištenje, mreža i druge. Klijent ne upravlja potpornom cloud infrastrukturom, ali upravlja operativnim sistemom, ažuriranjem softvera i proizvoljnim aplikacijama koje samostalno instalira.
Benefiti IaaS usluga su: potpuna kontrola i administracija virtuelnih mašina, fleksibilno i efikasno iznajmljivanje resursa, portabilnost, interoperabilnost i drugi. Problemi ovih usluga su: zavisnost od mreže, rizici sigurnosti veb čitača klijenata, ažuriranje sistema, pitanje robusnosti izolacije virtuelnih mašina (obično je u pitanju konfiguracija hipervizora i korišćenje ekstenzija procesora) i dr.

Platforma u vidu servisa (engl. Platform-as-a-Service, PaaS)

PaaS su platforme koje mogu biti korišćene za realizaciju aplikacija obezbeđenih od strane klijenata ili partnera provajdera platforme. Omogućava korišćenje računarskih razvojnih platformi i softverskih sistema u obliku servisa. To znači da nije potrebno preuzimanje i instalacija softvera za projektante, IT menadžere ili krajnje korisnike. Samim tim nestaju troškovi vezani za kupovinu, instalaciju i održavanje softverskih i hardverskih resursa i upravljanje ovim resursima.

Aplikativni programeri mogu da koriste ovaj cloud za razvoj i izvršavanje softvera, bez mogućnosti upravljanja operativnim sistemom, mrežnim parametrima, prostorom za skladištenje, ali uz kontrolu konfiguracije hosting okruženja. Ukratko, PaaS klaud je sličan tradicionalnim računarskim sistemima (platformama) za koje se mogu razvijati aplikacije koje će se izvršavati na njima i koje će koristiti krajnji korisnici usluga. Međutim, za razliku od tradicionalnih sistema, PaaS obezbeđuje jeftinu osnovu za razvoj skalabilnih aplikacija. Neka od problematičnih pitanja u vezi PaaS -a su: rizici sigurnosti veb čitača kod klijenata, zavisnost od mreže, pitanja izolacije nasuprot efikasnosti, kao i manjak portabilnosti između različitih PaaS provajdera.

Softver u vidu servisa (engl. Software-as-a-Service, SaaS)

Predstavlja softver koji je implementiran u obliku hostovanog servisa kome se pristupa putem interneta. Kod ovog modela korišćenja softvera, korisnici na zahtev dobijaju licence za aplikacije koje su im potrebne i koriste ih onoliko koliko su im potrebne.

Ovakav pristup omogućava optimalno korišćenje resursa i smanjenje troškova koji bi nastali kupovinom licenci, instaliranjem i obezbeđivanjem hardverskih resursa neophodnih za njihovo funkcionisanje, ali i troškova koji bi proistekli iz procesa održavanja svih ovih resursa. SaaS je veb servis. Kod ovog modela cloud provajderi obezbeđuju aplikativni softver kojem korisnici pristupaju preko mreže (interneta).Korisnici ne upravljaju potpornom infrastrukturom niti operativnim sistemom na kojem se aplikacije izvršavaju. Ovakav servis je podležan man-in-the-middle napadima na kriptografske protokole implementirane u veb čitaču. Drugi problemi su zavisnost od mreže i pitanja izolacije nasuprot efikasnosti. Postoje tri situacije za koje SaaS nije odgovarajući: Real-time softver, masovni podaci i kritičan softver.

Javni i privatni klaud

Klaud sistemi se mogu podeliti i na osnovu modela rasporeda infrastrukture klaud servisa.Možemo govoriti o Public, Private, Community i Hybrid klaud sistemima. Različiti modeli razlikuju se po arhitekturi, lokaciji i potrebama korisnika.Pomenimo samo neke od njih: Public klaud, Private klaud, Community klaud, Hybrid klaud i td.

4. SIGURNOST PODATAKA I POVERLJIVOST

Distribuirana priroda klaud računarstva znači da se ogroman broj podataka prenosi preko mreže povećavajući sigurnosne rizike. Poverljivost podataka mora biti obezbeđena bez obzira da li se radi o čuvanju podataka u klaudu ili prenosu podataka od do klauda. Dok se enkripcija može koristiti kod prenosa podataka, ona nije adekvatna za procesiranje podataka na klaudu. Podaci moraju biti enkriptovani u nekom mometu u okviru klauda da bi bili obrađeni jer određene operacije nije moguće izvršiti na kriptovanih podacima ili bi njihovo izvršavanje zahtevalo previše vremena.

Geografska lokacija podataka je značajna u određenim slučajevima. Znanje o tome gde se fizički nalaze podaci je veoma važno za sigurnost podataka jer mogu postojati značajne razlike u zakonskoj regulativi različitih zemalja. Korisnici klaud računarstva moraju razmotriti i ovaj aspekt razmatranjem zakonske regulative u zemljama u kojima će koristiti klaud.

Korisnik javnog klauda može zahtevati brisanje njegovih podataka ili kompletno brisanje podataka sa klauda. S obzirom da se ovo jedino može uraditi brisanjem pa upisivanjem proizvoljnih podataka ili formatiranjem diskova na serverskim računarima može se ispostaviti da u klaud okruženju pružaoca klaud usluga ovo nije moguće. Ovo ostavlja mogućnost napadačima da mogu doći do podataka koji su ostali na diskovima. Takođe, postoji i manja verovatnoća da je moguće doći do podataka preko kojih su prepisani drugi podaci.

Kriptografija u klaud okruženju

Najsigurniji vid zaštite podataka u klaud okuženju jeste interna enkripcija istih, pre skladištenja. Međutim ovaj vid zaštite nije moguće realizovati na svakoj platformi i kod svakog operatera. Osnovni problem za korišćenje interne enkripcije predstavlja rad sa podacima u otvorenom obliku korišćenjem resursa pružaoca usluga, kada je aplikacija korisnika dostupna na mreži, kao i postupak kriptovanja gde slučajno ili namerno treća strana može doći do ključa korisnika.

Pokušaji da se preko infastrukture javnih ključeva vrši enkripcija podataka nisu dali rezultate jer pružaoci usluga, pravdajući se nedostatkom ljudskih, vremenskih I tehničkih resursa izbegavaju ponuđena rešenja.

Programi za enkripciju operativnih sistema su ranjivi i prostim metodama dekripcije u veoma kratkom roku dolazi se do podataka u otvorenom obliku.

Ukoliko korisnik nema sopstvenih resursa za skladištenje poverljivih podataka, preporuka je da se na posebnom računaru izvrši kriptovanje istih, te da se kao takvi smeste u klaud u vidu zaštićenog fajla.

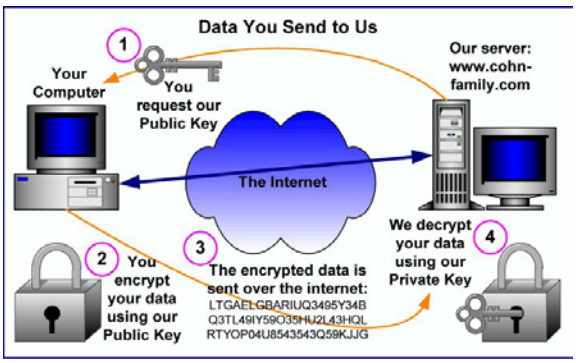
U zavisnosti od primenjenog algoritma, a pre svega kriptografskog ključa sigurnost podataka može biti garantovana trajno ili za određeni vremenski period.

Imajući u vidu da postoje i zlonamerni korisnici klauda, te da je na svakoj mreži prisutan veliki broj napadača, preporuka je da se kriptovanje podataka vrši ključem za jednokratnu upotrebu i da se svaka poruka kriptuje kao samostalna celina.

Iako je metodama dekripcije moguće uz ogromno angažovanje resursa probiti šifrovanu poruku, pitanje je interesa napadača i koristi koju može izvući, da li će se odlučiti na grubi napad kriptovanih podataka. Uglavnom se nakon saznanja da se radi o praktično ili apsolutno sigurnom sistemu enkripcije, napadač odustaje od probijanja i traži pogodniju žrtvu.

Kao osnovnu tehniku enkripcije podataka, Cloud Computing koristi RSA algoritam za asimetričnu kriptografiju , prvenstveno namenjenu šifrovanju podataka, ali se danas koristi i u sistemima elektronskog potpisa. RSA algoritam danas predstavlja industrijski standard u oblasti asimetične kriptografije i zaštite podataka, tako da je široko primenjen u mnogim sigurnosnim protokolima i sistemima elektronskog poslovanja. Tvorci ovog algoritma su Ronald Rivest, Leonard Ejdlman i Adi Šamir, gde RSA predstavlja akronim njihovih prezimena. Algoritam je patentiran od strane MIT-a 1983. godine u SAD, pod šifrom U.S. Patent 4,405,829.

U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi. Sigurnost RSA zasniva se na složenosti faktorizacije velikih brojeva. Smatra se da je određivanje originalne poruke na osnovu šifrata i ključa za šifrovanje ekvivalentno faktorizaciji proizvoda dva velika prosta broja. Prosti brojevi koji se koriste u ovom algoritmu uglavnom sadrže nekoliko stotina cifara i zbog toga se ovde javljaju više problema praktične prirode. Da bi se pomnožili toliko veliki brojevi, moraju se koristiti posebni algoritmi za množenje. Sem toga, lako se da primetiti da je za takve operacije potrebno više vremena, pa su tako ovi algoritmi šifrovanja mnogo sporiji u odnosu na simetrične algoritme. DES algoritam šifrovanja je oko 100 do 1000 puta brži u odnosu na RSA algoritam. Sem ovoga algoritmi za faktorizaciju brojeva postaju svakim danom sve bolji, kao i neumoljiv razvoj kompjutera učinili su da danas 512-bitni RSA algoritam ne bude dovoljan za bezbedno šifrovanje poruka, za 1024-bitne algoritme pretpostavlja se da će biti bezbedni barem još 15- tak godina.



Slika 1: Princip RSA algorima

Oporavak i backup

Pružaoci klaud usluga trebalo bi da imaju plan backup-a u slučaju da dođe to neke katastrofe ili otkaza na sistemu. Ovo je moguće postići replikacijom, kopiranjem podataka, na različite lokacije. Ako dođe do otkaza sistema ili katastrofe na jednoj lokaciji koristiće se podaci sa druge lokacije. Ovo je veoma važno i ovaj plan mora biti spomenut u ugovoru između klijenta i pružaoca klaud usluga.

5. ZAKLJUČAK

Krajnji korisnici klaud sistema nemaju znanja o tome gde se računari koji izvršavaju njihove aplikacije fizički nalaze. Oni verovatno ne znaju ni broj fizičkih računara na kojima se njihove aplikacije izvršavaju. Ono što korisnici uvek očekuju su iste perfomanse sistema za isti isnos koji plaćaju pružaocu klaud usluga. Međutim, ovo u praksi ne mora uvek biti slučaj jer perfomanse zavise od raznih faktora, na većinu kojih krajnji korisnici nemaju uticaj. U stvari, ovo je jedan od glavnih problema koje korisnici razmatraju kod prelaska na klaud rešenja.

Ekonomičnost klaud sistema zasniva se na povećanju nivoa iskorišćenosti infrastrukture, ali nije jasno da li će jedan korisnik uticati na perfomanse korisnika druge aplikacije. Na osnovu navedenog latentnost prema lokacijama gde se nalaze serveri može varirati zavisno od perioda vremena u kome se koristi sistem (da li sistem koristi više ili manje korisnika u određeno vreme), lokacijie na kojoj se nalaze serveri i komunikacionih linkova. Pružaoci usluga mere perfomanse sistema u svom okruženju, a ne u okruženju korisnika, korisnici klaud sistema treba da imaju to na umu kod potpisivanja ugovora.
Kriptovanje podataka vršiti kada je to moguće, a oak su podaci u otvorenom obliku, isti ne bi trebalo da sadrže poverljive informacije.

LITERATURA

[1] IBM Corporation (International Business Machines Corporation) 2010. http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf
[2] IBM Corporation (International Business Machines Corporation) 2010. http://linux1.beausanders.com/whitepapers/Benefits_of_Cloud_Computing.pdf
[3] IBM Corporation (International Business Machines Corporation) 2010. ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/ciw03062usen/CIW03062USEN.PDF
[4] Klaud racunarstvo - Varduna http://www.varduna.rs/sh/blog/8-technology/42-klaud-racunarstvo.html
[5] 10.a Предавање 294.99 KB www.viser.edu.rs/download.php?id=14425
[6] 10.b Предавање 294.99 KB www.viser.edu.rs/download.php?id=14425

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

PRANJE NOVCA: PLASTIČNI I VIRTUELNI NOVAC

MONEY LAUNDERING: PLASTIC AND VIRTUAL MONEY

DRAGAN ĐURĐEVIĆ
Akademija za nacionalnu bezbednost, BIA, Republika Srbija, djurdjevic@bia.gov.rs

---

Rezime: *Ovaj rad predstavlja aspekte bezbednosti informacionih tehnologija (IT) u sferi interakcije uloge "plastičnog i virtuelnog novca u funkciji suzbijanja pranja novca. Gigantska ekspanzija IT, internet, e_poslovanje, sve jeftiniji i efikasniji informatički resursi (takozvana demokratizacija IT) otvara nova polja i mogućnosti neslućenog privrednog rasta, u čijoj je osnovi elektronski novac i platni promet. Nove mogućnosti kreiraju i nove bezbednosne propuste, breše i rizike. Rast prekograničnog prometa legalnih, ali paraleleno i nelegalnih sadržaja, koji su delimično kontrolisani, ali svakako ne i u potpunosti. Pranje novca u delu korišćenja plastičnog i virtuelnog novca dobija nove dimenzije, zbog čega je potrebno sa aspekta nacionalne, regionalne i globalne bezbednosti pristupiti strateški suzbijanju i preventivnom bezbednosnom delovanju, kao bitnom elementu politike nacionalne bezbednosti Srbije. Rad elaborira savremeni model i sistem suprotstavljanju pranja novca. Analiziraju se faze pranje novca, standardna metodologije IFAC-a, vritualna šeme valutnih transakcija. Prezentira se pregled situacije sa Bitcoin-om, efekti i prve javne reakcije i stavovi regulatornih vlasti i bezbednosnih agencija. Ukazuje se na negativne fiskalne implikacije nastanka novih šema pranja novca korišćenjem plastičnog i elektronskog novca. Perspektive rešenja se sagledavaju u školovanju specifičnih kategorija stručnjaka u oblasti regulative, revizije i bezbednosti IT.*

Ključne reči: *Informaciona bezbednost, pranje novca, virtuelna valuta, bitkoin,*

Abstract: *This paper is presenting the security aspect of information technology (IT) in the sphere of interactive role of the "plastic and virtual money" in a role of anti-money laundering. Gigantic expansion of IT, Internet, E-commerce, even cheaper and more efficient information resources (so called the "IT democratization") is opening up new fields and possibilities for unforeseen economic growth, based on the electronic money and money transfers. New solutions and possibilities are creating new securities shortfalls, breaches and risks. Volume of cross-border legal transactions is increasing, and parallel with it increases the volume of illegal transactions, which have being partially controlled, but certainly not fully comprehensive. Money laundering in the area of plastic and virtual money is gaining new dimension. This is the reason why it is necessary from the aspects of national, regional and global security to start-up strategically anti-money laundering and preventive hard security measures and activities, as an important segment of the Serbian national security policy. The paper is closely elaborating the contemporary model and the system of anti-money laundering. It has being analysed the phases of money laundering, IFAC standard methodology, virtual schemes of money laundering. It is presented the situation regarding Bitcoin, effects and first public reaction and position of the regulatory authority and security agencies. It is pointed out on the negative fiscal implications of the creation of new money laundering schemes of using the plastic and electronic money. Perspective solutions are envisaged in the education of the specific categories of professional in the field of regulation, audit and IT security.*

Keywords: *Information security, money laundering, virtual money, bitcoin,*

1. UVOD

Izražena nestabilnost savremenog sveta u ekonomskom, političkom i društvenom pogledu, uz unipolarni svetski poredak koji je potisnuo blokovske tradicionalne podele i hladni rat ali ga nije eliminisao, donela je nove izazove. Jedan od svakako najvećih izazova je pranje novca. Ogroman napredak u razvoju informacionih tehnologija, internet, e_poslovanje, relativno jeftini informatički resursi (lakoća nabavke i korišćenja personalnog računara od strane pojedinca, zakup i usluge internet provajdinga), kao i ostvarivanje dugogodišnjeg sna "kupovina iz fotelje" [1] preko mreže, uz posedovanje platne kartice za plaćanje elektronskim novcem, stvorili su i preduslove da se u glavama pojedinaca stvori ideja za zloupotrebu istih. Visoka pokrivenost računarskim mrežama na globalnom nivou i rasprostranjenost informacionih tehnologija, bez obzira na materijalni status pojedinaca, organizacija i/ili država, stvara jaku infrastrukturu za prekogranični promet znanja, usluga i novca za pravna i fizička lica. Povoljni tehnički preduslovi za vršenje kiber kriminala i kiber pranja novca predstavljaju potencijalnu pretnju [2]. Prethodno definisano okruženje kao jednu od bitnih determinanti ima i ekspanziju zloupotrebe informacionih tehnologija do neslućenih granica. Zbog toga, ali svakako ne samo zato, pranje novca prerasta od usko nacionalnog i eventualno regionalnog u primarni problem regionalne i globalne bezbednosti koji će biti u fokusu svetske politike tokom prvih dekada 21. veka.

Savremeni tokovi platnog prometa, monetarne politike, elektronskog transfera novca, novi načini trgovine i plaćanja usluga nametnuli su upotrebu kreditnih i debitnih kartica takozvanog "plastičnog novca", kao jedinu pravu i priznatu alternativu tradicionalnim novčanim apoenima. Na vežbama iz tipologija jedna od zemalja članica FATF-a je, još davne 2003. godine podnela materijal o studiji, koja je sprovedena da utvrdi kako kreditne i debitne kartice mogu biti korišćene za pranje novca [3].

Suprotstavljanje pranju novca predstavlja skup mera, radnji, aktivnosti i postupaka koje preduzimaju nadležni organi u cilju ostvarivanja funkcije države u domenu suzbijanja mehanizama pranja novca, odnosno zaštite njenih vitalnih nacionalnih vrednosti. Zaštita ne predstavlja bilo kakvu posebnu organizaciju koja bi izvršavala zadatke iz oblasti javne i državne bezbednosti, već naprotiv, delatnošću nadležnih državnih i društvenih organa ostvaruje se funkcija integralne zaštite nacionalnih interesa od negativnih efekata pranja novca.

Sistem suprotstavljanja pranju novca predstavlja jedan od najnovijih podsistema u okviru integralnog sistema bezbednosti (javne i nacionalne) i obuhvata niz radnji i mera u sklopu organizacije fizičke i tehničke zaštite i bezbednosne zaštite (aktivne i pasivne), radi sprečavanja raznih kriminalnih i drugih oblika ugrožavanja nacionalne bezbednosti u sferi pranja novca i borbi protiv terorizma na nacionalnom, regionalnom i međunarodnom planu, sa ciljem otkrivanja njihovih učinilaca, kao i efikasnije zaštite države od mehanizama pranja novca i terorizma što je od centralnog značaja za bezbednost zemlje, nacionalne privrede i građana.

2. FAZE PRANJA NOVCA

Prema radnoj definiciji IFAC-a, [4] oni koji se bave pranjem novca zapravo se bave prikrivanjem svojih aktivnosti i prihoda, što dodatno otežava procenu, jer njihove transakcije nisu obelodanjene u okviru službenih nacionalnih finansijskih statistika, niti ih mogu evidentirati i o njima izveštavati nacionalni obračunski sistemi. Ovo je problem koji je uočio i MMF za koji nema još pravog i adekvatnog odgovora. Aktivnosti i metode pranja novca postale su mnogo kompleksnije, "kreativnije" i uz to i dovitljivije, a "operacije-transakcije" se uobičajeno sastoje od tri segmentirane aktivnosti: a) plasman, b) raslojavanje i c) integracija.

Oni koji se bave pranjem novca veoma vode računa o nacionalnim zakonima, regulativama, strukturi vlasti, trendovima i strategijama i tehnikama kriminalističkih službi, kako bi njihovi prihodi ostali sakriveni, njihove metode tajne, a njihovi identiteti i profesionalni izvori anonimni.

Elektronska trgovina hartijama od vrednosti, drugim robama i uslugama i elektronski platni promet, omogućavaju servisiranje znatno većeg obima veoma složenih transakcija, ali je istovremeno sve teže analitički pratiti, a još teže ući u prirodu svake pojedinačne transakcije i to samo onih koje prolaze kroz legalne kanale. Elektronska trgovina hartijama od vrednosti (e-trgovina) uopšte otvara nove mogućnosti ali kreira i nove probleme [3]. U transakcijama elektronske trgovine hartijama od vrednosti revizori, brokeri, berze i klijenti su u SAD obavezni da izveštavaju o svim transakcijama, počev od čuvanja originalnih računovodstvenih evidencija, u čemu u mnogome pomažu IT sistemi i visoko sofisticirana IT revizija. [5]

Detaljnom analizom studije, koja je zasnovana na pregledu značajnih obelodanjenih sumnjivih aktivnosti i identifikaciji određenog broja karakteristika sumnjivih aktivnosti povezanih sa ovom vrstom kartica definisani su sledeći indikatori:

- Struktuirana plaćanja u gotovom za neizmirene iznose kredita, odnosno salda na kreditnim karticama – (kreditna salda su bila najrasprostranjeniji oblik aktivnosti koji je detektovan, često sa relativno velikim sumama kao plaćanjem).
- Pokušaj "treće strane" da plati u gotovom u ime vlasnika kartica.
- Zloupotrebe kreditnih kartica, (korišćenje izgubljenih ili ukradenih kartica od strane trećih lica).
- Korišćenje avansa u gotovom sa računa kreditne kartice, da bi se kupili čekovi na donosioca,
- Korišćenje avansa u gotovom sa računa kreditne kartice, da se elektronski prebace fondovi na inostrane destinacije
- Ulaganja avansnih depozita na štedne ili tekuće račune.

Prethodno navedene karakteristike predstavljaju samo deo obelodanjenih aktivnosti, koje mogu biti označene kao samostalni čin, ali isto tako mogu biti deo šire šeme aktivnosti povezane sa različitim finansijskim kriminalima, kao i pranja novca i terorističkog finansiranja. Kako se radi o lokalizovanom segmentu, moguće kriminalne i finansijske aktivnosti, neophodno ga je posmatrati sa različitih aspekata.

3. VIRTUELNE ŠEME

Izdavanjem dokumenta „Virtual currency schemes" [6], oktobra 2012 godine ECB je dala detaljno obrazloženje fenomena nazvanog Virtuelne šeme. Ova pojava je nastala ubrzanim razvojem interneta i inicirala razvoj i primenu virtuelnih valuta. U početnom stadijumu razvoja virtuelnih valuta, primena je bila ograničena na zatvorene grupe i mahom se odnosila na igrice, kladionice i sl. Eksperti evropske centralne banke, brzo su uočili moguće opasnosti i potencijale masovnog korišćenja ovog resursa. Detaljnom analizom uočenih aktivnosti od strane kreatora virtuelnih valuta uočene su tri kategorije šema:

- I potpuno zatvorene šeme, korišćene u onlajn igrama;
- II virtuelne šeme koje imaju jednosmerni tok (obično prema unutra), za pravi novac kupuje se „virtuelna valuta" koja se koristi za virtuelna dobra i usluge na internetu, izuzetno za realna dobra i usluge;

- III virtuelne šeme koje imaju dvosmerno kretanje novca, mogu se menjati u/iz realne valute, i koriste se kako za kupovinu virtuelnih, tako i realnih dobara i usluga.

Bitno obeležje pobrojanih šema je nepostojanje posrednika na relaciji kupac - prodavac. Nedostatak regulatornog i zakonskog okvira, omogućava privatnom, nefinansijskom subjektu, da u njenom kreiranju, razmeni i korišćenju izmiče monitoringu i reviziji. Analitičkim pristupom sagledavanju razlika između virtuelnih šema i e-novca, uočava se sledeće: rizik e-novca vezan je samo za zloupotrebe informacionih sistema, dok kod virtuelne šeme, pored rizika od zloupotrebe informacionih tehnologija, postoji kreditni i rizik likvidnosti, kao apsolutno nepredvidive kategorije.

U daljem tekstu pomenutog dokumenta zapaža se ozbiljna zabrinutost eksperata na budući uticaj ovih šema na ekonomiju i reputaciju centralne banke, ukazujući na sledeće, da one u ovom trenutku:

- ne nose rizik na cenovnu stabilnost, sve dok je ukupan obim virtuelnog novca relativno mali;
- ne mogu uticati na finansijsku stabilnost, sve dok je njihov upliv u realnu ekonomiju zanemariv, i ne postoji šira mreža prihvatilaca;
- budući da nisu monitorisane i kontrolisane, svaki učesnik u šemi to radi na sopstveni rizik;
- mogu predstavljati izazov za državne organe, jer zbog svoje prirode lako mogu postati instrument za pranje novca i finansiranje kriminalnih aktivnosti;
- mogu imati negativan uticaj na reputaciju centralne banke, budući da je njihov rast nepredvidiv, i ekspanzija takve valute može stvoriti utisak da centralna banka ne radi svoj posao;
- nisu podložne reviziji, nameću obavezu centralnoj banci da se priprema za iznalaženje rešenja u smislu kontrole i nadzora kretanja ove valute.

Pojava virtuelnih moneta je od strane šire društvene zajednice tretirana kao jedna od tehničkih inovacija, sa predznakom rizično, nepouzdano, verovatno kratkotrajno, međutim moramo naglasiti da je isti put prošao i plastični - kartični novac, kasnije prihvaćen i uvučen u regulatorni okvir. Jedan od argumenata koji je, u prvo vreme, privukao zaluđenike za tehnologiju, internet i investitore avanturiste je taj, što ove monete ne kontrolišu centralne banke koje, opet, kontrolišu vlade. Svetskim moćnicima ne odgovara korišćenje paralelnih, virtuelnih valuta, jer one omogućavaju zaobilaženje globalnih pravila. Iza virtuelnih moneta ne stoje centralne banke, njihovu vrednost utvrđuje mnoštvo računara a poseduju i prirodnu zaštitu od inflacije i prevare. Virtuelne monete su zaštićene od inflacije matematičkom funkcijom koja onemogućava da njihova količina naraste iznad unapred određene granice. [7].

U poplavi virtuelnih valuta koja je poslednjih pet godina uzela maha, (Bitcoin, Litecoin, Peercoin, Dogecoin, Namecoin, Blackcoin, Darkcoin ...) značajno mesto i primat u međunarodnim okvirima zauzeo je Bitcoin (BtC), valuta sa virtuelnom šemom bazirana na „pear to pear“ mreži. [8]

Bitcoin (BtC) virtuelna valuta, se pojavila 2009. godine i najverovatnije je delo japanskih programera mada se na internet forumima ovo delo pripisuje Satoši Nakamotu. Sistem je baziran na BitTorrent protokolu za deljenje fajlova preko interneta. Jedan bitkoin u svom izvornom obliku predstavlja niz digitalnih potpisa. Imalac ove valute poseduje par ključeva, javni i tajni, koji su smešteni lokalno, računaru vlasnika, formirajući virtuelni novčanik. Gubitkom ovih ključeva došlo bi do gubitka „novca“. Kako se emitovanje ovog novca zasniva na veoma komplikovanim kripto algoritmima i ne zavisi od drugih valuta, odluka vlada i centralnih banaka, teoretski, može se reći da je zaštićen od monetarnog udara i finansijskih instrumenata koji bi mogli uticati na njegovu vrednost. Vrlo je značajno naglasiti, u prilog stabilnosti ove valute, algoritamska procena da je maksimalan mogući broj bitkoina u opticaju ograničen na 21 milion, što ograničava nekontrolisanu emisiju. Najjednostavniji način za posedovanje ove valute je putem prodaje ili pružanjem usluge elektronskim putem, odnosno naplatom u pomenutoj valuti. Drugi, daleko teži i nepovoljniji način, je da se uključite u jedan složen proces putem interneta u operaciju koja se zove „rudarenje“. Kako se radi o veoma specifičnoj računarskoj operaciji koja „zadaje“ vašem procesoru zadatke rešavanja teških matematičkih problema, koji su u svakoj narednoj iteraciji sve složeniji, te iziskuju sve više brzine i procesorske snage, čijim rešavanjem se kreira Bitkoin novčić. Potrebno je naglasiti da su zadatci sve složeniji i teži, odnosno nameću potrebu za snažnijim procesorima - računarima, tako da se "rudari", snalaze formirajući računarske klastere i primenjuju druge tehnike kako bi dobili na snazi i brzini opreme.

4. SITUACIJA U SVETU

Da pojava bitkoina nije naivna igra, govori i njegova pojava na berzama, u početku sramežljivo a kasnije sve agresivnije, kako u primeni tako i u vrednosti. Pored toga, redovno raste spisak preduzeća koja prihvataju ovu valutu za plaćanje roba i usluga. Prihvatanje ove valute kao sredstva plaćanja ukazuje na rešenost velikih svetskih kompanija da je u potpunosti podrže i prihvate:

- Microsoft je na sajtu Bing.com uveo opciju konverzije 50 svetskih valuta u popularnu virtuelnu valutu bitkoin, kao i konverziju bitkoina u tih 50 valuta. Konverzija je moguća samo za korisnike iz SAD-a, Velike Britanije, Australije i Indije. Kompanija Coinbase je svojim servisima omogućila Microsoftu praćenje vrednosti valute koja se menja i više puta dnevno. Coinbase nudi različite usluge u oblasti kupovine, prodaje, kao i skladištenje bitkoina. [9]

- Agencija za nekretnine Forsit Rial Istejt, sa sedištem u Sidneju, od 26. aprila ove godine prihvata virtuelnu monetu bitkoin kao sredstvo plaćanja za svoje usluge. Ovo je prva australijska agencija koja se odlučila na ovakav potez. Agencija pruža mogućnost plaćenja nekretnine preko platforme za plaćanje bitkoinom KoinDžar (CoinJar) koja konvertuje virtuelnu monetu u dolare uz nadok-

nadu od 0,5 odsto na ukupan iznos transakcije. Cilj ovakve odluke australijske agencije je privlačanje investitora, pre svega kineskih, jer se na ovaj način izbegavaju bankarski troškovi koji su veoma visoki ako se radi transakcijama između banaka između stranih zemalja. [10]

- Kompanija Xapo (Kalifornija) predstavila je bitkoin debitnu karticu koja bi trebalo da funkcioniše poput klasičnih bitkoin kartica. Plaćanje se odvija na način da nakon obavljene transakcije Xapo skida određeni iznos bitkoina sa korisnikovog novčanika i prodaje na Bitstampu, trenutno najvećem servisu za razmenu bitkoin valute. Kartice će biti dostupne u dve verzije: virtuelnoj koja je besplatna i fizička koja košta 15 dolara. Xapova kartica za sada neće raditi ni na jednom bankomatu, ali se očekuje da će se to uskoro promeniti. Kompanija Cryptex ranije je predstavila svoju verziju kartica koja radi na većini američkih bankomata, ali korisnicima se naplaćuje posebna naknada svaki put kada se bitkoini pretvaraju u američke dolare. [11]

- Kipar, nikozijski univerzitet će omogućiti budućim studentima plaćanje školarine u bitkoinima. [12]
- U Hong Kongu je otvorena prva prodavnica bitkoina, tako da je moguće kupiti virtuelnu valutu, a da se ne bude onlajn.

5. STAVOVI

Američka fiskalna administracija je saopštila da bitkoin ne smatra monetom, već sredstvom plaćanja koje može biti oporezovano: "Virtuelne monete mogu se koristiti za kupovinu robe i usluga ili biti upotrebljene kao investicije (...) ali one nemaju zakonsku vrednost", navela je američka poreska agencija IRS. Najpoznatija digitalna valuta će tako biti tretirana kao "sredstvo", a zarada dobijena korišćenjem bitkoina biće oporezovana, navodi se u dokumentu IRS o fiskalnom statusu bitkoina u SAD. Američka agencija navela je i da će i plate u bitkoinima po uplaćivanju iznosa biti oporezovane, kao i druge uplate. Početkom marta i vlada Japana odredila je da bitkoin nije valuta, već "roba", ali da neke transakcije tim sredstvom treba da se oporezuju. Globalno tržište bitkoina procenjuje se na oko sedam milijardi dolara. [13]

Nakon niza skandala koji su vezani za dogadjaje oko digitalne valute, a koja je u protekle dve godine stekla veliku popularnost.Američka Regulatorna agencija za finansijska tržišta (FINRA Financial Industry Regulatory Authority) izdala je sledeće upozorenje: "Kupovina i korišćenje digitalne valute poput bitkoina sa sobom nosi rizik, dok spekulativno trgovanje bitkoinom nosi još veći rizik. Platforme koje kupuju i prodaju bitkoine mogu biti hakovane, a neke od njih su već doživele krah. Osim toga, moguće je i da digitalni novčanici takođe budu hakovani, zbog čega potrošači mogu, a neki već jesu izgubili novac". Agencija je ukazala i na moguće korišćenje bitkoina u kriminalnim radnjama poput pranja novca. [14]

Nurijel Rubini ekonomista, je mišljenja da bitkoin nema budućnost kao valuta, ali smatra da je stvorena veštački i funkcioniše po principima piramidalne prevare. U izjavi za mrežu CNBC, pomenuti stručnjak, smatra da je to novi kanal za kriminalne aktivnosti, posebno ako se ima u vidu rizik od hakera, smatrajući da bi se bitkoin po svemu mogao smatrati investicijom visokog rizika, dok bitkoin entuzijasti kažu da je to zato što mnogi virtuelnu valutu i dalje vide kao robu.Po mišljenju Erik Votsona, očekuje se svetla budućnost, ne samo bitkoina, već i drugih virtuelnih valuta, kad, potrošači budu počeli da otkrivaju praktične prednosti privatnih transakcija, raširenost valute će se kretati s malim rastom, dok će se biznisi prilično sporo privikavaju na bitkoin, a onda će u jednom trenutku, u relativno bliskoj budućnosti, nastati bum, posle čega će ljudi masovno početi da ga koriste, istakao je on. [15] Povodom sve učestalijeg korišćenja bitkoina, ruske vlasti su objavile saopštenje u kom navode da se bitkoin često koristi za pranje novca i finansiranje terorističkih organizacija, da se smatra ilegalnom paralelnom valutom. Državni tužilac je saopštio da se prema Ustavu Rusije rublja smatra jedinom važećom valutom i da se korištenje bitkoina kao druge valute od strane ruskih državljanja i kompanija smatra nedopustivim. Korištenjem bitkoina pojedinci i organizacije mogu lako biti uvučeni u ilegalne aktivnosti i zbog toga državno tužilaštvo će u saradnji sa centralnom bankom pooštriti zakonske regulative koje se bavi problematikom korištenja virtuelnih i paralelnih valuta. Pored toga, regulatorni organi smatraju operacije virtuelnim valutama potencijalno sumnjivim, čiji mogući cilj je finansiranje terorizma ili pranje novca. Bitkoin je najuspešnija i verovatno najkontroverzija šema virtuelne valute. Ona se koristi u mnogim zemljama i konkuriše zvaničnim valutama, među kojima i evru i dolaru. [16]

6. SRBIJA

Bitkoin u Srbiji, polako ali uspešno ulazi u naše živote, idemo u korak sa svetom, čak postoji i „menjačnica“ gde se digitalna valuta može zameniti za dolare ili evre. Plaćanje u Srbiji bitkoinom je moguće u dve ustanove, uz ogradu da kako ne postoji pravni okvir niti regulativa ostaje i otvoreno pitanje da li neko čini prekršaj ili krivično delo, mada poštujući trenutno važeću zakonsku regulativu jedino zvanično sredstvo plaćanja u Srbiji je dinar. Kako je neophodno pred zakonom ostati čist, osnivači e-gimnazije koja je jedna od dve ustanove, koje su omogućili plaćanje bitkoinom, druga je restoran Apetit, morali su pribeći "okolo - naokolo" rešenju. Cena školovanja u e-gimnaziji iznosi četiti bitkoina, projektovani paritet je zasnovan na ekvivalentu od 2000 eura, iako je virtuelna valuta sklona velikim dnevnim oscilacijama kursa. Novi vid plaćanja će svakako biti zanimljiv onima koji imaju bitkoine, tako što će iz svog virtuelnog novčanika, valutu prebaciti u novčanik e-gimnazije, da bi se zatim na nekoj od berzi bitkoina, Bitstamp ili MtGox na internetu, konvertovale u evre ili dr. Tako dobijene devize će se potom uplatiti na račun u banci u Srbiji, a zatim isti konvertovati u dinare i platiti školarinu, "rezervno" rešenje je dodela stipendije učeniku koji je izvršio uplatu bitkoina i na taj način izbeći zakonske prepreke. Restoran Apetit, je morao da pribegne inovativnom rešenju kako bi mogli ostati

u zakonskim okvirima, kako bi gostima izdali fiskalni račun. Vlasnici restorana su angažovali softversku kuću koja je razradila novi način plaćanja, restoran je koristio sopstveni novac, stavljao ga u kasu ili plaćao svojom karticom, a gost je prethodno izmireni račun platio bitkoinima. Pošto se promet slaže, restoran gostu izdaje fiskalni račun. Pre toga, restoran gostu prinese tablet računar sa aplikacijom u koju se unese iznos računa u dinarima i automatski obračuna njegova vrednost u bitcoinima prema trenutnoj vrednosti na Bitstamp berzi. Mušterija onda svojim mobilnim telefonom skenira poseban kod sa tablet računara i traženi iznos se automatski skida sa njegovog virtuelnog novčanika i prebacuje u novčanik restorana. Restoran kasnije sebi prebacuje novac preko pomenutih bitkoin berzi. Zakonom o platnom prometu utvrđeno da se poslovi platnog prometa obavljaju u dinarima, a Zakonom o deviznom poslovanju da se plaćanje, naplaćivanje i prenos između rezidenata i između rezidenata i nerezidenata vrši u dinarima osim u slučajevima predviđenim tim zakonom. Legalno, otvorenu menjačnicu za promet digitalnim valutama - bitkoinom u Srbiji za sada nema niko iako se u postupku za dobijanje dozvole nalazi jedno lice. [17]

7. ZAKLJUČAK

Veliki broj zemlja i njihove poreske vlasti bore se s problemom regulative novonastalog virtuelnog tržišta, dok neke sa visokom dozom realnosti vide upotrebu bitkoina kao mogućnost za izbegavanje poreza, pranje novca, finansiranje terorizma, i mogućnosti da je samo mašta ograničenje za valutu, koja u sekundi može preći sa jednog, na drugi kraj sveta, bez kontrole treće strane i monitoringa. Rusija je proglasila transakcije bitkoinima nelegalnim, a Kina je zabranila svojim bankama da prihvataju trgovanje u toj virtuelnoj valuti a ima poziva da to isto uradi SAD. Singapur je uveo porez na trgovinu bitkoinima, a bitkoine registruje kao robu. Preporuka ECB je detaljno praćenje mogućeg rizika na cenovnu, finansijsku stabilnost i platni sistem,kroz praćenje interakcija bitkoina i realnog sveta. Ono što se sa sigurnošću može ustanoviti bitkoin je ušao u tokove realnih ekonomija, i da se ovim fenomenom danas bave ekonomisti, pravnici, IT stručnnjaci, hakeri, centralne banke, bezbednosne službe.

Američki senator Tom Karper izrazio je mogući strah za platni promet u informatičkim saobraćaju: *"Mnoge valute bi mogle biti sredstvo za pranje novca, preprodavanje droga ili pak iskorišćavanje dece iz celog sveta, a lista može biti i duža. Bitkoin budi maštu jedinih, strahove drugih dok ostale čini samo zbunjenima"*. [18]

I na kraju, pored svih do sada pobrojanih argumenata, sa namerom da se ukaže na nove načine pranja novca, bez obzira sa kakvim pobudama se pranje izvodi, može se izvesti zaključak, da je ovaj proces u usponu i da su sve oblasti i sfere života potencijalno ugrožene, jer sofisticirani mehanizmi, finansijski instrumenti i prednosti savremenog života otvaraju neslućene mogućnosti ka razvoju novih virtuelnih kriminalnih aktivnosti, kojima treba stati na put. [19] Pred eksperte za ovu oblast se postavljaju sve teži i ozbiljniji zadaci, koje je moguće rešiti jedino uključenjem u međunarodne tokove, praćenjem najnovijih saznanja o mehanizmima prevencije, detekcije, suzbijanja i represije počinilaca. Na osnovu svega izloženog nameće se potreba za povećanom kontrolom društvenih i državnih činilaca nad pojavama virtuelnih platnih šema, pranjem novca i zloupotrebe informacionih tehnologija. Rešenje je u školovanju specifičnih kategorija stručnjaka u oblasti pravne regulative i bezbednosti informacionih tehnologija. [20]

LITERATURA

[1] FATF, Report: *Money Laundering Using New Payment Methods*,FATF/OECD, Paris, October 2010.

[2] Đurđević D. Ž., Pranje novca i zloupotreba informacionih tehnologija, Zbornik radova (CD-ROM), savetovanje: *Zloupotrebe informacionih tehnologija ZITEH 2004*, Tara, 01.-03. jun 2004.

[3] Đurđević, D. Ž., *Doktorat, Suprotstavljanje pranju novca u funkciji borbe protiv terorizma*, Univerzitet u Beogradu, Fakultet bezbednosti, Beograd, 2006.

[4] IFAC, International Federation of Accountants: *Anti–Money Laundering,* 2nd Edition IFAC. p. 4., 2004.

[5] Ljutić, B. Ž., Polić, S., *Revizija informacione tehnologije,* Narodna banka Jugoslavije: Zavod Za obračun i plaćanje. COBISS.SR-ID 86853644, Beograd, 2002.

[6] ECB, *Virtual Currency Schemes*, Frankfurt, October 2012.

[7] http://www.b92.net/biz/vesti/srbija.php?yyyy=2013&mm=12&dd=03&nav_id=784939 (04.04.2014.)

[8] http://bitinfocharts.com/ (10.05.2014.)

[9] http://www.bing.com/blogs/site_blogs/b/search/archive/2014/02/10/coinbit.aspx (15.02.2014)

[10] http://www.blic.rs/Vesti/Svet/454123/Moguca-kupovina-nekretnina-u-Australiji-u-bitkoinima (01.04.2014.)

[11] https://xapo.com/in/campaign/debit/ (28.04.2014.)

[12] www.itnetwork.rs/Alternativa-bitkoinu-lajtkoin-article-12503.htm (22.12.2013.)

[13] http://money.cnn.com/2014/03/31/technology/irs-bitcoin/ (27.03.2014.)

[14] http://www.finra.org/investors/protectyourself/investoralerts/fraudsandscams/p456458 (09.05.2014.)

[15] www.cnbc.com/id/101479123 (11.05.2014.)

[16] http://rt.com/business/bitcoin-russia-use-ban-942/ (15.03.2014.)

[17] http://www.danas.rs/danasrs/ekonomija/bitkoin_uspesno_obilazi_zakon.4.html?news_id=273194 (12.05.2014.)

[18] www.cnbc.com/id/101316945 (08.05.2014.)

[19] Petrović R. S., *Kompjuterski kriminal*, Vojnoizdavački zavod, III izdanje, Beograd, 2004.

[20] Đurđević D. Ž. (2013) Primena informacione tehnologije u suzbijanju pranja novca, Zbornik radova (CD-ROM), ISBN 978-86-89251-01-2, konferencija: Informaciona bezbednost 2013, Beograd, 05. jun 2013.

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

ULOGA INTERNE REVIZIJE U PRUŽANJU USLUGA UVERAVANJA BEZBEDNOSTI PODATAKA I ZAŠTITE PRIVATNOSTI U KORPORATIVNOM SEKTORU SRBIJE

THE ROLE OF INTERNAL AUDIT IN ASSURANCE SERVICES ON DATA SECURITY AND PROTECION OF DATA PRIVACY IN THE SERBIAN CORPORATE SECTOR

BRANKO LJUTIĆ
Fakultet za ekonomiju i inženjerski menadžment, Novi Sad, bljutic@sbb.rs

DRAGAN SOLEŠA
Fakultet za ekonomiju i inženjerski menadžment, Novi Sad, dragan.solesa@fimek.edu.rs

ZORAN ĐORĐEVIĆ
Ministarstvo odbrane republike Srbije, Beograd, zoran.enzo@gmail.com

---

Rezime: *Funkcije interne revizije u firmi dobija novu ulogu koja obuhvata pružanje usluga uveravanja o stepenu bezbednosti informacija i zaštite privatnosti. Time se funkcije interne revizije i bezbednosti korporativnih informacija spajaju na sinergetskoj osnovi. Osoblje interne revizije koje je odgovorno za bezbednost IT bavi se zaštitom informatičkih resursa firme. Procenjuje procedure i tehnologije, mehanizme zaštite, pruža sugestija za unapređenje i inoviranje. U pristupu se sagledava interakcija revizije i bezbednosti IT, menadžment informacija, uz definisanje interne revizije kao prve i poslednje linije bezbednosti IT. Rad se zalaže za pristup u kome se interna revizija i bezbednost IT integrišu kao nezavisne poslovne funkcije koje dejstvuju sinergetski.*

Ključne reči: *Interna revizija, bezbednost, korporativnih informacija, preduzeća, Srbija*

Abstract: *Role of internal audit in a firm is gaining a new ground embracing the assurance services on the level of security of information and on the protection of the data privacy. By that the role of internal audit and the security of corporate information are amalgamating on a synergy base. The internal audit department staff responsible for IT security is in charge of protection of the information resources of the firm. The staff is assessing the procedures and technology, mechanisms of protection and data security, offering improvement suggestions and innovation hints. In the introductory part it has being observed the interaction between the audit and IT security, information management, while at the same time it has being defined the internal audit as a first and last line of defence of the IT security. The paper is in favour of an approach in which the internal audit function and IT security are integrated as independent function of the business organization which are acting complementary in a synergy.*

Keywords: *Internal audit, security, corporate information, firms, Serbia*

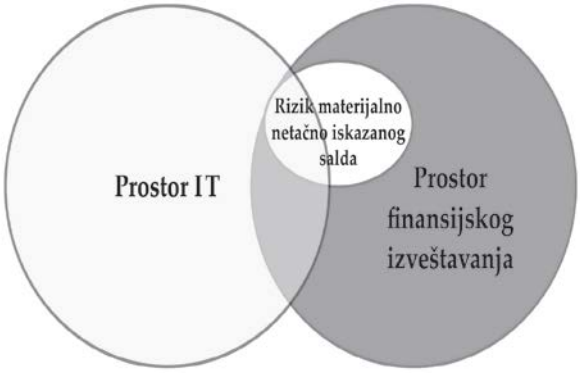
1. UVOD

U korporativnom sektoru Srbije u budućnosti će poslovna funkcija interne revizije igrati značajnu ulogu u procesu bezbednosti informacija, informacionih tehnologija i zaštite privatnosti podataka. Većina preduzeća ne samo da ne obavlja adekvatan proces monitoringa i osavremenjavanja svoje prve i poslednje linije odbrane protiv kiber kriminala, već nema čak ni bazični model odbrane još manje strateški pristup, čemu je glavni uzrok odsustvo funkcije interne revizije. Sve to povećava rizik i enormno rastu troškovi nastali usled probijanja bezbednosnih mera i mehanizama zaštite korporativnih IT sistema i samih informacija. U ovom radu će se šire elaborirati aspekti: Revizije sistema elektronske obrade podataka, Međunarodni standardi interne revizije koji se odnose na bezbednost IT, modeli upravljanja informacijama u reviziji u funkciji bezbednosti.

2. INTERAKCIJA REVIZIJA/ITBEZBEDNOST

Efekti sistema elektronske obrade podataka na reviziju se reflektuju kroz interakciju eksterne i interne revizije i informacionog sistema firma, koji može ali ne mora biti informacioni sistem podršku poslovnom odlučivanju (engl. Management Information System – MIS) [3]a. U ovom metodološkom modelu se ukazuje da je savremeno poslovanje sve više okrenuto protoku bezpapirne dokumentacije kroz telekomunikacione prenose po međunarodno usvojenim standardima. U sklopu takvih

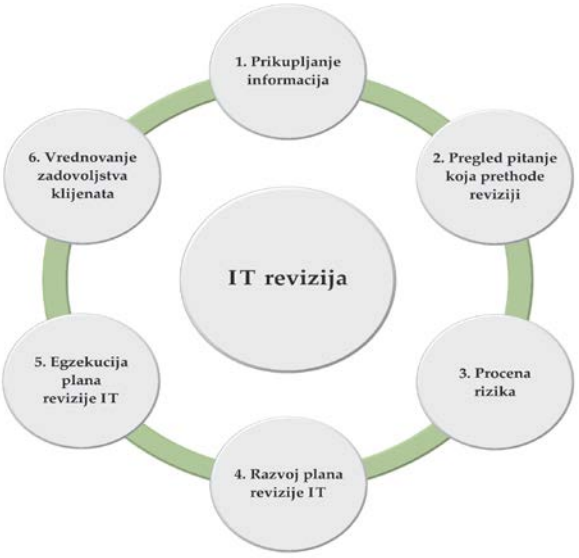
aktivnosti revizori (eksterni, interni) su u okviru poslova revizijske kontrolne i savetodavne revizorske funkcije sve više okrenuti analizi rada i proveri primenjenih *programskih kontrola* koje su sprovedene u okviru informacionih sistema (IS) poslovnih entiteta. Takav prilaz revizorskoj funkciji sve više zahteva neposredno aktivno znanje revizora iz informacionih tehnologija (IT), kao i IT stručnjaka da poznaju bazične revizorske procedure. U sklopu ukupnog koncepta revizije bitan uticaj na prilaz, metodologiju i kvalitet prikazanog računovodstvenog izkaza i pratećih informacija, koje su predmet revizije, ima ostvarena tehnologija rada u računovodstvu, koja je u sadašnjim savremenim uslovima definisana projektnim rešenjem informacionog podsistema finansije-računovodstvo.



Slika 1: Interakcija prostora i slojeva IT i finansjskog izveštavanja u firmi: Materijani rizik

Revizija informacionog sistema firme Informacioni podsistem finansije-računovodstvo se u ovom slučaju pojavljuje u dvostrukoj ulozi, kao tehnički generator računovodstvenih iskaza i poslovnih informacija. Sa jedne strane kao deo tehnologije koja je podložna analizi revizora i sa druge strane, kao poseban predmet revizije o domenu kvaliteta i pouzdanosti rada. IS firme u segmentu modula korporativni menadžment finansije računovodstvo bazira se na sledećim pretpostavkama:

- **Računovodstveni informacioni podsistem.** Revizorski operativni standard zahteva da revizor bude uključen i upoznat sa informacionim sistemom organizacije uključivši snimanje, obradu transakcija i odgovarajuće upite u baze podataka, što treba da mu omogući da razume detalje projektovane tehnologije rade i prihvate adekvatnost obrađenih finansijskih stavki
- **Revizija evidencija.** Zahteva se da revizor dobije bitne i pouzdane evidencije, dovoljno precizne da mu omoguće da iz toga izvlači racionalne zaključke
- **Interna kontrola.** Ako revizor poželi da se u radu osloni na bilo koji deo rada interne kontrole (revizije), korisnik treba da mu omogući pristup tim kontrolama, a revizor će konstatovati i oceniti njihov kvalitet i obaviti odgovarajuće provere u tim operacijama
- **Pregled finansijskih iskaza (obračuna).** Standard zahteva da revizor izvede sveobuhvatan pregled finansijskih iskaza, što će mu u sprezi sa izvedenim zaključkom drugih revizorskih evidencija da omogući formiranje mišljenja o finansijskom obračunu-iskazima
- **Revizorski standardi i direktive** zahtevaju i prezentiraju osnovne principe i postupke, koji treba da koristi revizor u obavljanju revizije. Na slikama 1 i 2 prikazane su šeme toka kontrole automatizovane računovodstvene evidencije, sa osnovnim tokom informacija i akcija revizora.



Slika 2: Ciklus IT revizije u okviru funkcije interne revizije firme

Revizorska direktiva, u okviru revizije IS klasifikuje kontrole na:

- Opšte kontrole
- Administrativne kontrole.

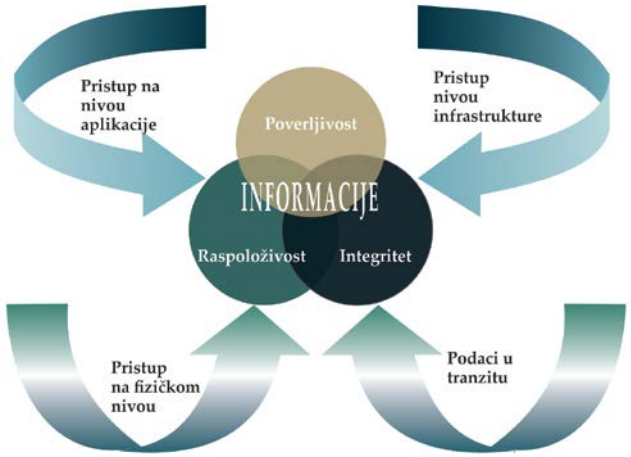
U standardnoj efikasnoj organizaciji korporativne interne revizije predviđa se funkcija na nivou pomoćnika direktora službe – menadžer revizije informacionih sistema kao i revizora informacionih sistema [3]a. Jedno od ključnih pitanja MIS firme jeste revizorsko vrednovanje tačnosti, efektivnosti i efikasnosti korporativnog elektronskog informacionog sistema i sistema obrade podataka. Međunarodni standard interne revizije 310 bavi se aspektima pouzdanosti i integriteta informacija. Interni revizori treba da pregledaju pouzdanost i integritet finansijskih i operativnih informacija i sredstava korišćenih da se identifikuju, mere, klasifikuju i izveste takve informacije. Tako 310.01 određuje da informacioni sistem obezbeđuju podatke za donošenje odluka, kontrolu i usaglašenost sa eksternim zahtevima. Stoga, interni revizori treba da pregledaju informacione sisteme i, ukoliko je odgovarajuće da se uvere da li:

1. Finansijske i operativne evidencije i izveštaji sadrže tačne, pouzdane, blagovremene, kompletne i korisne informacije
2. Kontrole nad vođenjem evidencija i izveštavanjem adekvatne i efektivne.

Primarna misija funkcije revizije informacionih sistema koju obavlja interna revizija je da pruži podršku funkciji interne revizije u vrednovanju tačnosti, efektivnosti i efikasnosti sistema firme za elektronsku i obradu informacija koji se proizvode ili su u fazi razvoja. U domenu konsultantskih usluga top menadžmentu služba interne revizije obezbeđuje da se prezentiraju informacije, podsticaji i pregled bitnih pitanja koja se tiču politika korporacije, procedura i internih kontrola. Pored funkcije revizije informacionih sistema konsultantske usluge jesu proširene da uključuju:

- Pomoć u vrednovanju procedura zaštite podataka (eng. backup) i planiranja za vanredne okolnosti
- Pomoć u pogledu da li definisana arhitektura (prim. autora misli sa ne IT i IS) poseduje odgovarajuće kontrole
- Informacije o kontroli računara
- Pomoć u primeni internog finansijskog sistema.

Menadžer revizije IS izveštava direktora odseka interne revizije o aktivnostima koje obavlja.



Slika 3: Metodologija slojevite IT bezbednosti: Standardi američkog instituta internih revizora

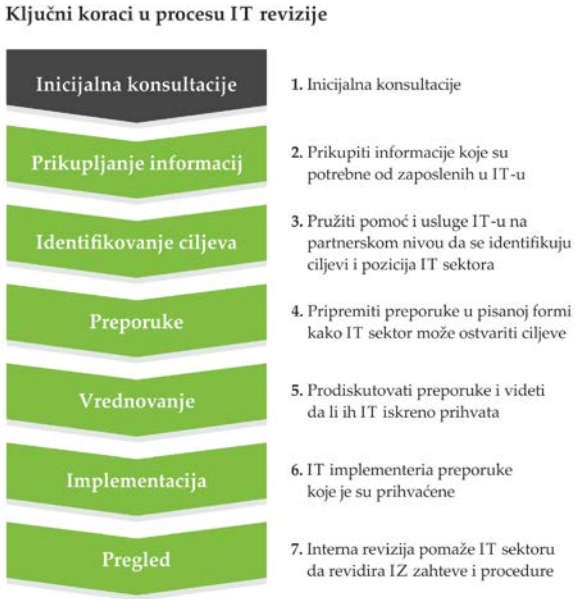
3. UPRAVLJANJE INFORMACIJAMA U INTERNOJ REVIZIJI ZA IT BEZBEDNOSTI

Savremena, uspešna korporacija je rudnik znanja, ako to nije pred stečajem je ili u fazi slabljenja [3]c. Danas se firme u Srbiji suočavaju sa sve nepoštednijom konkurencijom krupnih multionacionalnih korporacija. Stoga korporativni sektor u Srbiji ulaže sve više napora da poslovno opstanu i ostvare performanse. Deficit kadrova u oblasti IT, relativno visoke plate za okruženje jesu za firma sa slabijom pozicijom likvidnosti nepremostiva prepreka, koja im se neposredno vraća kao izraženi negativni povratni efekat. Korporativno preživljavanje nameće novi imperativ menadžment informacija. Implementacija sistema informacionog menadžmenta u firmi(IM) podrazumeva sledeće ključne pristupe:

Integracija – Sistemi IM mora da sadrže tekuće informacije firme koje su bezbednosno zaštićene. Ključni je pristup da je bezbednost IT i zaštita privatnosti informacija rezultat kolaboracije i kolektivnih napora svih relevantnih i odgovornih učesnika u ovom procesu, jer su samo tada poslovne i sa njima povezane informacije kompletne i vrede.

Kulturna promena – U Srbiji su firme već praktično počele da implementiraju elektronsku prijavu poreskih obaveza, što će uskoro biti model i za građane. Za firmu i pojedinca je bitno da definiše i identifikuje svoje potrebe za informacijama i sagleda sledeće aspekte. Koje su informacije potrebne? Zbog čega su potrebne? Šta će se učiniti sa njima? Da li postoji bolji način? Kada su jednom poslovni podaci prikupljeni, može se istinski razumeti da li su procesi u firmi u domenu bezbednosti IT iz "antičkih vremena" i da li postoji i kakva i potreba da se preurede.

Strategija primene efikasne bezbednosti IT – Informacioni menadžment ne treba da bude takav da natkriljuje sve. Sa pažljivim planiranjem "napada", firma može da alocira resurse koji su potrebni da se kompletira transakcija. Kada obavi identifikaciju informacija firma može utvrditi i odrediti prioritete potrebnih promena i alata da zadovolji ove promene. Kao što je pisac Steven Covey jedan od gurua korišćenja vremena rekao *"Počnite sa krajem u mislima"*. Spoznajte koji je vaš cilj i izgradite plan da ostvarite taj cilj.



Slika 4: Ključni koraci u procesu IT revizije

Enormne su koristi od korišćenja sistema IM baziranom na informacionoj bezbednosti u poslovanju firme. U tom slučaju rastu poslovna efikasnost i efektivnost. Kada firma identifikuje svoje potrebe za informacijama, može da započne proces identifikacije IT bezbednosnih rešenja koja zadovoljavaju potrebe i nude najviše ekonomske povraćaje [4].

4. INTERNA REVIZIJA KAO PRVA LINIJA BEZBEDNOSTI IT

Vreme potrebno da firme u Srbiji shvate i potom implementiraju novu strategiju i politiku informacione bezbednosti je veoma dugo. Napadi hakera ali i

konkurenata koji to mogu sprovesti a da ne budu sprečeni ili procesuirani su sve češći. Zbog toga je potrebno da kompanije u Srbiji kreiraju svoje protokole bezbednosti informacija. U tom pristupu će biti ključna uloga odseka za internu reviziju koji će obezbeđivati usluge *uveravanja da su kontrole i politike efikasne u zaštiti privatnosti podataka.* Raste opasnost od upada u sisteme elektronske obrade podataka, gubici od incidenata, krađa, mada se takvi podaci ne evidentiraju u Srbiji moglo bi se oceniti da će rast biti veliki u budućnosti. Rizik hakovanja korporativnih računarskih sistema će rasti iz mnogo razloga.

- Firme i zaposleni su sve prisutniji na internetu, IT tehnologija je sve pristupačnija, mobilni uređaji su veoma jeftini, sve više se koriste računarstvo u oblaku [5]. Radna snage je mobilna, koristi mobilne uređaje što donosi nove rizike i incidentne situacije.
- Firme skladište sve veći broj podataka o građanima i klijentima, zaposlenim, što je za hakere rastući izazov, jer su tu i nelegalne koristi od zloupotrebe takvih informacija.
- Kompanije u Srbiji neopravdano i pogrešno potcenjuju rastuću opasnost od kiber kriminala, uverene da je to odgovornost provajdera internet usluga, softverskih kuća koja su im dobavljači takvih rešenja, ne shvatajući da je kiber bezbednost primarno odgovornost korporacije. Često ne samo da nema bezbednosnih protokola već firme i nemaju stručnjaka zaduženog za bezbednost IT.
- Kompanije u Srbiji nemaju formalne politike IT bezbednosti i zaštite privatnosti ličnih podataka, tako da ono što ne postoji nije moguće ni unapređivati i usklađivati sa novim potrebama.

Troškova propusta u bezbednosnoj zaštiti podataka
U slučaju prodora hakera i razbijanja bezbednosne zaštite IT u različitom obimu po širini i dubini, rastu sledeći troškovi:

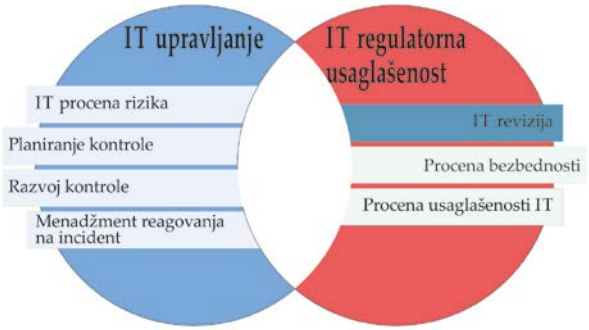
- Dodatnih mera IT bezbednosti
- Pravnih usluga zbog prouzrokovanih šteta
- Samih šteta po sredstva i profite firme, poslovni ugled, propuštena dobit, odgovornost.

Top menadžeri srpskih firmi treba da prihvate jednostavnu činjenicu da je investiranje u bezbednost IT sa većim profitnim stopama od bilo kojih alternativnih ulaganja, mada zbog konzervativizma, inercije, neadekvatnih znanja smatraju da je to "neracionalno trošenje". Kada menadžment shvati i prihvati da je bezbednost IT investiranje u ugled i buduće profite, tada će se promeniti ukupan odnos prema tome. Interna revizija u tome ima ulogu da edukuje top menadžere i informiše ih dodatno o prednostima usluga uveravanja koje se odnose na rizik ugrožavanja bezbednosti IT. Hakeri se brže obrazuju, prihvataju tehnološke promene, revolucionarni su, tako da kompanije treba da se prilagođavaju tome. To po svemu sudeći liči na tandem kriminalci-policija, gde kriminalci donose revolucionarne mada kriminalizovane novine u čemu ih policija prati sa više ili manje uspeha ali uvek sa zaostatkom.

5. LINIJE ODBRANE PREDUZEĆA U SRBIJI PROTIV KIBER KRIMINALA

Menadžment firme Bitno je da top menadžment firme iskreno prihvati i pokrene inicijativu unapređenja sistema efikasne bezbednosne zaštite IT. Menadžment treba formalno na nivou upravnog odbora da kontinuirano procenjuje, kontroliše i ublažava rizika bezbednosti podataka.

Menadžment rizika i zakonska usaglašenost Ova oblast je u Srbiji i dalje na nivou prisutnosti u naučnim i stručnim radovima, u praksi skoro da i nema čak ni početnih koraka. Prvi korak je da se formira tim odnosno radna grupa, sa stručnjacima iz firme i ključnim dobavljačima IT usluga. Bitno je sagledati stepen postojeće zaštite, na toj osnovi kreirati politike bezbednosti IT, kontrole, kao i metodološke postupke implementacije kontrola.

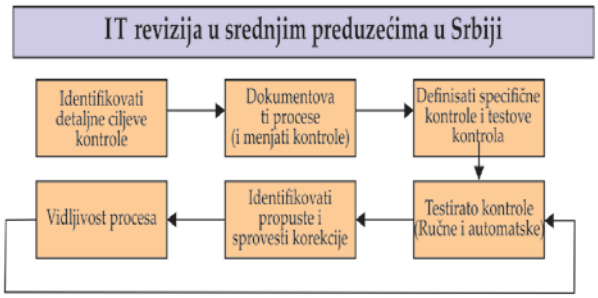


Slika 5: Korporativno upravljanje i regulatorna usaglašenost IT

Interna revizija Cilj funkcije interne revizije je da u firmi obezbedi objektivno i razumno uveravanje (jer revizija nije apsolutna garancija već samo razumno uveravanje) odboru direktora i timu top menadžera da je firma u stanju da objektivno procenjuje bezbednosne rizike po IT, te da efikasno upravlja ovim rizicima kiber bezbednosti. Ukoliko interna revizija ne pruća ove usluge, tada je raste rizik bezbednosti i zaštite privatnosti informacija, tako da čak i ako postoji neki nivo procedura i politika postaje automatski "staro gvožđe" [6].

U ovoj oblasti nema apsolutne bezbednosti, već je relativna i dinamička, vredi samo do tačke kada je ugrožena odnosno kada su probijene linije bezbednosne zaštite. Zbog toga interna revizija mora kontinuirano da atestira model bezbednosnih kontrola IT. Bitno je da se bezbednosne kontrole primenjuju bez kompromisa, konsistentno, uz oslanjanja i podršku odbora za reviziju (ako je velika firma). Interna revizije u svom izveštaju o proceni rizika treba da proceni rizike IT bezbednosti i zaštite privatnosti podataka koji se podnosi na uvid i odobravanje odbora za reviziju (ako ne postoji takvo telo u organizacionoj šemi) ili odbora direktora odnosno upravnog. Top menadžment treba da podržava internu reviziju da ovladava novim znanjima i bude ispred najnovijih pretnji u sferi IT bezbednosti.

Bitan je pristup koji je multidisciplinarni, obuhvatan, integralan. Na tom putu od hiljadu kilometara bitan je prvi korak, a to podrazumeva borbu za promenu mentalnog sklopa i načina razmišljanja i delovanja menadžera. Prvo treba razvejati sumnje da nije potrebno unapređenje bezbednosti IT jer nije bilo problema do sada. Ako sistem nije probijen, svakako ne znači da je neprobojan. Menadžere treba uveriti da je bitno unapređenje interne revizije u domenu kontrole IT rizika. Nezainteresovanost i nemotivisanost menadžera da investiraju u povećavanje stepena bezbednosti IT, jer takav pristup pogrešno vodi ka odsustvu preko potrebnih ulaganja u ovu oblast. U situacijama kada top menadžment smatra ne samo da firma nema potrebe za funkcijom interne revizije nego ni za bezbednošću IT. Zbog toga treba pojedinačne organizacione delove firme (finansije, pravni sektor, računovodstvo, ljudske resurse, IT, marketing, itd.) dodatno obučiti u ovoj oblasti. Time kontrole bezbednosti IT prožimaju firmu, odgovornost za bezbednost IT se proširuje, postaje obuhvatna. Na taj način funkcija interne revizije evoluira u pravom pravcu od prve linije odbrane kao poslednjom spajajući ih u efikasan sistem menadžmenta rizika bezbednosti IT.



Slika 6: Okvir IT revizije u MSP u Srbiji

6. ZAKLJUČAK

Savremeni i još više efikasan menadžment je usko fokusiran na poslovni uspeh. Osnov jeste sistem interne kontrole. Proces kontinuiranog monitoringa obezbeđuje firmi mogućnost bezbednosne zaštite vitalnih informacija, IT privatnosti podataka. U početku je pristup bio usmeren da monitoring obavlja osoblje IT sektora, ali je savremeni trend ka tome da ove usluge komplementarno obavlja sektor interne revizije. Uslov da bi interna revizija bila efikasna u domenu bezbednosti IT i zaštite privatnosti podataka je posedovanja znanja i iskustva u oblasti IT. Bitno je da interni revizori prihvate deo nove uloge koju im dodeljuje poslovni svet, uz podršku menadžmenta na vrhu firme i kreiranje adekvatnih karakteristika poslovne organizacije. Takav pristup podrazumeva transformaciju interne revizije koja pored centralne uloge poverljivog savetnika top menadžmenta dobija zadatke aktivne zaštite bezbednosti IT i privatnosti informacija.

LITERATURA

[1] Collier, M. P. Fundamentals of Risk Management for Accountants and Managers, Tools and Techniques – First Edition, Elsevier ltd, Burlington, 2009

[2] Ljutić, B. Ž., *Bankarsko i berzansko poslovanje: Investicije, institucije, regulativa*: Magistar biznis administracije–MBA Press Inc. ISBN: 86-903871-0-2, Beograd, 2004

[3] Ljutić, B. Ž., *Revizija: Logika, principi i praksa*: Magistar biznis administracije–MBA Press Inc. ISBN: 86-903871-2-9, Beograd, 2005, a: 178-202, b: 326-396, c: 470-476.

[4] Ljutić, B. Ž., Polić,S. *Revizija informacione tehnologije, Most revizije i informacione tehnologije.* Beograd: Narodna banka Jugoslavije: Zavod Za obračun i plaćanje. COBISS.SR-ID 86853644, 2002, 187-197.

[5] Ljutić, B. Ž., Milošević S. *"Menadžment rizika firme računarstva u oblaku".* BISEC 2013, Konferencija o bezbednosti informacija, Beograd: Univerzitet Metropolitan, ISBN 978-86-912685-8-9, 12-16.

[6] Ljutić B. Ž. *Revizija u usluge uveravanja: Integrisani pristup.* Novi Sad: Fakultet za ekonomiju i inženjerski menadžment-Univerzitet Privredna akademija. ISBN 978+86-87619-54-8, 2014, 103-112.

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

SOCIJALNI INŽENJERING MODUS OPERANDI

SOCIAL ENGINEERING MODUS OPERANDI

SAŠA ŽIVANOVIĆ
Ministarstvo unutrašnjih poslova Republike Srbije, Služba za borbu protiv organizovanog kriminala,Beograd,
sasa.zivanovic@mup.gov.rs

SASA ZIVANOVIC
Ministry of Interior Republic of Serbia, Service for Combating Organized Crime, Belgrade,
sasa.zivanovic@mup.gov.rs

Rezime: *Socijalni inženjering u kontekstu bezbednosti informacija, odnosi se na psihološku manipulaciju ljudima u obavljanju poslovnih aktivnosti ili otkrivanju poverljivih informacija. To je vrsta prevare sa ciljem prikupljanja informacija pristupa ili pristupa sistemu, razlikuje se od tradicionalnih prevara po tome što je često pri obavljanju mnogih koraka vodi u složenije šeme prevare.*

Ključne reči: *Socijalni inženjering*

Abstract: Social engineering*, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.*

Keywords: *Social engineering*

1. UVOD

Dinamični razvoj informacionih tehnologija uz gotovo svakodnevno pojavljivanje novih srevisa za elektronsko plaćanje, kao i drugih servisa za obavljanje poslovnih aktivnosti uslovio je nove sofisticirane mehanizme zaštite prilikom obavljanja navedenih aktivnosti. Medjutim, sa pojavom novih servisa paralelno se javljaju i novi servisi zloupotreba, a jedan od prisutnijih je i metod korišćenja tehnika socijalnog inženjeringa koji je usmjeren na ljudski faktor. Socijalni inženjering ne koristi slabosti tehničkih i tehnoloških dostignuća već je usmjeren na tehnike napadača da žrtvu ubedi da ispuni njegove zahtjeve tj. dostavi mu tražene informacije do kojih legitimnim putem ne bi mogao doći. Postoji više definicija socijalnog inženjeringa, jedna od njih socijalni inženjering definiše kao tehniku upotreba psiholoških metoda u svrhu uvjeravanja žrvi u lažni identitet napadača, u cilju pribavljanja osjetljivih informaija sa ili bez upotrebe tehnologije.

2. METODE SOCIJALNOG INŽENJERINGA

Bez upotrebe tehnologije

- Uvjeravanje – osnovni preduslov
- Lažno predstavljanje
- Stvaranje odgovarajuće situacije
- Moralna odgovornost
- Želja za pomaganjem
- Iskorišćavanje starih veza i poslovnih kontakata
- Korupcija

Uz upotrebu tehnologije

- Spam
- Phishing
- Pharming
- Spear phishing
- Vishing
- Hoax
- Maliciozni software

Phishing napadi su najčešće usmjereni slanjem elektronske pošte u kojoj se žrtva navodi da pristupi unapred pripljenom hiperlinku (URL – Uniform Resource Locator adresi) koja vodi do lažne web adrese u kojoj žrtva ostavlja poverljive informacije (npr. podatke o bankovnim računima, platnim karticama i dr.) kroz popunjavanje različitih obrazaca.

Pharming tehnike imaju za posledicu preusmeravanje web saobraćaja na lažni domen pod kontrolom napadača i dosta često se koriste prilikom zloupotreba u elektronskoj trgovini, kroz ranjivosti DNS servera ili menjanjem host fajla.

Za razliku od tehnika phishing napada, spear phising metode se odlikuju time što je napad usmjeren prema poznatoj tj. ciljanoj žrtvi, koju napadač prethodno opservira i prikuplja sve informacije o njoj iz svih izvora, neretko prateći je, kako bi kasnije napravio scenario napada u cilju pribavljanja osjetljivih informacija od poznate žrtve.

Vishing tehnike se izmedju ostalog baziraju i na zloupotrebi VoIP tehnologije, kroz slanje tekstualnih ili glasovnih poruka ili upućivanja telefonskih poziva.

Hoax napadi se najčešće koriste nakon dešavanja elementarnih nepogoda u svetu kreiranjem lažnih web stranica radi prikupljanja pomoći ugroženom stanovništvu u kojima se navode bankovni računi na koje se usmjeravaju potencijalne žrtve.

3. MODUS OPERANDI PRIMERI

Napadači koristeći tehnike socijalnog onženjeringa pozivaju zaposlene u kompanijama o čijim menažerima su prethodno prikupili informacije kao što su pozicija u kompaniji, sklonosti, poznanstvima i sl. i predstavljaju se kao direktori predmetnih kompanija zahtevajući od zaposlenih da u potpunoj tajnosti šalju velike sume novca na račune u stranim bankama koje se uglavnom nalaze u Kini, ili drugim zemljama, nakon čega se takav novac transferiše na račune u offshore destinacije. Prethodno pripremljen scenario i umetnost ubedjivanja je ključna za ovaj tip prevare. Posledica ovih prevara nisu samo materijalni gubici za kompanije koje se mere na stotine milione evra, već i ljudske žrtve u vidu zaposlenih koji dobijaju otkaza pošto odobre isplate.

Kriminalne grupe pre početka napada prvo istražuju sredinu kompanije koja je meta prevare, kako bi se pribavile informacije o njoj.

U ovoj fazi prikupljanja informacija napadači obilato koriste Internet mrežu, za provere putem specijalizovanih web sajtova koji pružaju jeftin i lak pristup detaljnim informacijama o direktorima kompanija (ime, potpis, broj telefona, pozicija u kompaniji, izvodi iz trgovinskih i privrednih registara, finansijski bilans, ažurirani statusi kompanije, zapisnici sa raznih sastanaka i sl.). Ostale pretrage putem Internet mreže pružaju dodatne informacije, kao što je logo kompanije, njena organizaciona struktura, informacije o zaposlenima, čak i izjave predsednika kompanije, kako bi se bolje upoznali sa svim detaljima bitnim za tu kompaniju.

Informacije koje nisu dostupne putem otvorenih izvora kriminalne grupe kupuju od profesionalaca koji se bave industrijskom špijunažom, ili hakera, kojom prilikom plaćanje takvih informacija vrše sa platnim karticama kod kojih korisnici ostaju anonimni i ne može im se ući u trag.

Koristeći ovakve informacije, prevaranti zovu svoje žrtve sa telefonskih brojeva sa medjunarodnim prefiksom zemlje u kojoj se žrtva nalazi korišćenjem pre-paid sim brojeva i pre-paid platnih kartica koje mogu dopuniti malim novčanim iznosima putem elektronskih platformi za dematerijalizaciju za pretplatničke telefonske brojeve.

Prevara u kojoj se izvršilac predstavlja kao visoki rukovodilac

Na primer, predstavljajući se kao vlasnik kompanije izvršilac zove finansijskog direktora neke kompanije i pokušava da ga ubedi da izvrši uplatu na strani bankovni račun. To obično opravdavaju potrebom da se garantuje investiranje imovinom, predstojećom poreskom revizijom ili javnim tenderom i sl. Tom prilikom objašnjavaju da uplate moraju da ostanu potpuno tajne i poverljive i da će sa žrtvom biti u kontaktu advokatska kancelarija u kontaktu da bi im pružila potrebne informacije.

Uprkos mnogim kamapanjama i edukacijama koje kompanije preduzimaju za podizanje svesti, kriminalne grupe konstantno se prilagodjavaju i menjaju inicijalni modus operandi, stvarajući nove scenarije za napade.

Prevara u kojoj se izvršilac predstavlja kao poslovni partner

U ovom primeru, kriminalci se predstavljaju kao poslovni partneri kompanije koja je žrtva prevare. Odeljenje za računovodstvo ili menadžera kompanije kontaktiraju putem telefona ili elektronske pošte i obaveštavaju ih da je došlo do promene bankovnog računa za promet ili usluge koje treba da se plate i da ubuduće transfer novca mora da se plaća na drugi račun poslovnog partnera koji se nalazi u inostranstvu a ne u zemlji gde se do tada vršilo plaćanje. Tom prilikom kriminalne grupe putem elektronske pošte ili faxa dostavljaju podatke o novom bankovnom računu koristeći isti logo, stil i font pisanja koja koristi kompanija čiji identitet je ukraden. Ukoliko se koristi elektronska pošta za dostavu informacija o novom bankovnom računu kriminalne grupe kreiraju elektronski nalog koji je veoma sličan nalogu kompromitovane kompanije. Ovaj vid prevare u Republici Srbije zabeležen je još od 2012. godine, i dosadašnje materijalne štete po pravna lica iznose više stotina hiljada evra.

Novi trendovi napada: prevare uz korišćenje "SEPA" transfera

Tokom 2013. godine došlo je do posebnog porasta prevara sa "SEPA" transferima (Single Euro Payments Area). Ovaj modus operandi se pojavio nakon što su kompanije, javna administracija i bankarski sektor odlučile da uspostave "SEPA" standard kako bi uskladili elektronske uplate unutar evro zone zemalja.

U probnom periodu, prevaranti su preuzeli identitete zaposlenih u oštećenim bankama i kontaktirali su računovodje kompanija uz izgovor da će ih tokom obaveznog prelaska u "SEPA" sistem kontaktirati tehničari radi obavljanja testova.

Postupajući po primljenim instrukcijama, računovodje se konektuju na njihov web sajt i preuzimaju namensku aplikaciju koja omogućava daljinsku konekciju sa drugim web sajtom.

Izvršioci prevare tada objašnjavaju kako kreirati korisnički nalog dajući podatke žrtvi o stranoj banci koja treba da se koristi za probna plaćanja, posle čega će strane banke poslati izveštaje koji potvrdjuju usaglašenost transakcija sa novim protokolom.

Korišćenje malicioznog softvera

Prilagodjavajući se novim tehnologijama, kriminalne grupe kontaktiraju kompanije pod različitim izgovorima ("SEPA" transferi, lažne fakture, revizija itd.) i šalju im fajl u prilogu elektronske pošte koji sadrži maliciozni kod, obično "Trojanskog konja" u cilju neovlašćenog pristupa žrtvinom računaru ili računarskoj mreži napadnute kompanije.

Maliciozni softver (računarski virus) kreiran je tako da obavlja zadatke kojih korisnik računara nije svestan. Takav zlonamerni softver ili malver omogućuje izvršiocu tajnim pristupom svim funkcijama softvera u računaru žrtve i preuzimanje daljinske kontrole nad kompromitovanim računarom žrtve. Koristeći malver izvršioci-prevaranti prikupljaju sve informacije koje su im potrebne za napad tj. prevaru, kao što su npr. spisak poslovnih partnera, brojevi računa, dosadašnje transakcije, poslovna prepiska, administratorske šifre ovlašćenih osoba koje obavljaju transakcije, korisnička imena i lozinke i dr.

4. ZAŠTITA OD NAPADA KORIŠĆENJEM TEHNIKA SOCIJALNOG INŽENJERINGA

Prevencija i proaktivni pristup je od ključne važnosti za uspešnu odbranu od potencijanih pretnji tehnika socijalnog inženjeringa. Prevencija obuhvaća podizanje svesti u institucijama ne samo menadžera već svih zaposlenih kroz edukaciju, pravljenje kampanja, internih seminara i upoznavanja sa novim modus operandi tehnikama socijalnog inženjeringa, kreiranja internih procedura i pravilnika. Takodje, potrebno je precizno definisati planiranje adekvatnog odgovora na potencijalne incidentne situacije sa procedurama koje sadrže:

- Definisati sigurnosne politike i procedure kao odgovor na potencijalni napad
- Sačiniti podsjetnike u vidu pisanih brošura za odgovor na napad
- Obaveštavanje potencijalnih meta u kompaniji
- Obaveštavanje nadredjenog
- Obaveštavanje nadležnog za korporativnu bezbednost
- Obezbedjivanje dokaza ukoliko ih ima i prijava incidenta nadležnoj instituciji
- Obaveštavanje poslovnih partnera i spoljnih zaposlenih saradnika
- Izvršiti testiranje zaposlenih
- Ažuriranje procedura na odgovor napadu i njihovo prilagodjavanje kako tehnoločkim dostignućima tako i novim modus operandi načinima izvršenja prevara

5. ZAKLJUČAK

Suprotno klasičnim vidovima računarskih prevara, tehnike socijalnog inženjeringa nisu isključivo vezane za računare i računarske sisteme. On je prisutan u svim sferama poslovanja a vektori novih napada koristiće metode kombinovanih napada kako uz pomoć zlonamernog softvera tako i uz korišćenje tehnika socijalnog inženjeringa. Cilj ovog rada je podizanje svesti čitaocima radi upoznavanja i iniciranja podizanja svesti o eventualnim posledicama socijalnog inženjeringa.

LITERATURA

[1] Sarah Granger *Social Engineering Fundamentals,*, Part 1: Hacker Tactics, 2006.

Практични аспекти примене обавезне инструкције МУП о поступању са дигиталним доказима[1]

Practical aspects of Mandatory instructions on procedures with digital evidence[2]

доц. др Звонимир Ивановић, КПУ

Zvonimir.ivanovic@kpa.edu.rs*Апстракт: Аутор у раду покушавају да прикажу стање у погледу поступања надлежних органау вези са обезбеђивањем дигиталних трагова и предмета носилаца таквих трагова. Приликом приказивања стања указује се на слабости и предности постојећег система и области у којима је држава изашла унапред са решењима и пре него у неким другим областима. Наравно у том смислу предњачи област кривичног гоњења која задире дубоко у права и слободе човека, и као најпозитивнији пример управо органи унутрашњих послова. Доношење обавезне инструкције МУП-а уводи ред и изискује поштовање процедура прописаних за сваки од уређаја и носилаца дигиталних података. Аутор указују да би у овој области било неопходно да и други учесници донесу адекватне акте којима би регулисали сопствено поступање на месту догађаја, у првом реду тужилаштво, а такође и у погледу обуке у циљу подизања нивоа знања на виши ниво.*

***Кључне речи**: дигитални трагови, одузимање уређаја и носилаца дигиталних трагова, процедуре поступања на месту догађаја, претресање, увиђај*

***Abstract**: Author is trying to portray the situation in regard to the acting of competent agencies connection with the securing and conserving of digital traces and objects bearers of such traces. While elaborating on the situation author points out the strengths and weaknesses of the current system and areas in which the state has come forward with solutions before in some other areas . Of course, in this sense, the leading one is the criminal prosecution which delves deep into the human rights and freedoms, as the most positive example of just law enforcement agencies – police. Adoption of mandatory instructions MOI introduces order and require compliance procedures prescribed for each of the devices and carriers of digital data . The author suggest that in this area it is necessary that the other participants adopt adequate legislation and policies which would regulate their own treatment at the scene , primarily the prosecution office, and also in terms of training in order to raise the level of knowledge at a higher level.*

***Keywords**:digital traces, procedure for seizure, seizure of devices and bearers of digital traces, procedures for acting on the scene, search and seizure, crime scene procedures*

---

[1] Овај рад је резултат реализовања научноистраживачког пројекта под називом *Развој институционалних капацитета, стандарда и процедура за супротстављање организованом криминалу и тероризму у условима међународних интеграција*. Пројекат финансира Министарство науке и технолошког развоја Републике Србије (бр. 179045), а реализује Криминалистичко-полицијска академија у Београду (2011−2014). Руководилац пројекта је проф. др Саша Мијалковић.

[2] This paper is the result of the realisation of the Scientific Research Project entitled „Development of Institutional Capacities, Standards and Procedures for Fighting Organized Crime and Terrorism in Climate of International Integrations“. The Project is financed by the Ministry of Science and Technological Development of the Republic of Serbia (No 179045), and carried out by the Academy of Criminalistics and Police Studies in Belgrade (2011−2014). The leader of the Project is Associate Professor Saša Mijalković, PhD.

1. УВОД

Поступање са дигиталним траговима и, уопште, њихово коришћење у сврхе кривичног поступка изискује даље и потпуније регулисање. Разлог потпунијег регулисања се везује за карактеристике и могућности злоупотребе ове врсте трагова, као могућих будућих доказа. У том смислу МУП је први покушао да успостави ред у овој области доношењем обавезне иснтрукције о postupanju sa digitalnim dokazima[3] MUP RS[4]. Овом инструкцијом је предвиђен начин и процедуре поступања припадника полиције у вези са дигиталним доказима.

2. ПРАВНИ ОКВИР

Законик о кривичном поступку("Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013) ЗКП одређује као *dominus litis* предистражног и истражног поступка Јавног тужиоца. У том смислу он је као орган поступка у могућности да повери предузимање ове радње овлашћеним службеним лицима полиције, што је редован и уобичајен ток догађаја. Међутим министарство унутрашњих послова је активности у погледу прикупљања и обезбеђивања дигиталних доказа[5] у овом смислу ограничило, уводећи обавезном инструкцијом категорије припадника полиције који могу поступати са дигиталним траговима. Том приликом се и код свих категорија припадника полиције тачно одређују процедуре деловања у односу на телефоне, рачунаре, остале дигиталне уређаје, мрежна окружења и пословне мреже и сложене инфраструктуре.

3. ОПШТИ АСПЕКТИ

Позитивне стране ове инструкције су вишеструке. Успостављањем правила и одрешивањем принципа уређују се области од изузетног значаја и све веће присутности у животима људи. Општи принцип који прокламује инструкција је: поступање службеника полиције омогућава очување веродостојности доказа, а то се постиже поступањем којим се тежи очувању датума на рачунару или уређају за складиштење података. При том службеник полиције бива дужан да о предузетим радњама сачини белешку о поступању[6]. У смислу принципа прокламованог инструкцијом, треба напоменути да се у погледу дигиталних трагова треба придржавати и других принципа, на пример АЦПО[7]. АЦПО има 4 основна принципа који у многоме одсликавају интенције развијених земаља које и јесу изворно креатори ових трагова и информација. Први принцип одсликава став законодавца да се такви трагови и предмети не мењају, не оштећују или не уништавају.

---

[3] Овај термин је несрећно изабран, обзиром да сви ситемски закони из ове области, посебно Законик о кривичном поступку користе термине предмете и трагове. Верујемо да је аутор овог акта желео да да на значају овим траговима и предметима коришћењем термина докази.

[4] Обавезна инструкција о прикупљању и обезбеђењу електронских доказа од 26.02.2013.год.

[5] ЗКП генерално говори о предметима и траговима па терминологија инструкције мало одудара у том смислу у односу на ЗКП, али ово није јединствен случај у српском законодавству. Такав је случај и са Законом о одузимању имовине проистекле из кривичног дела (ЗОИПКД) Сл. гласник РС, бр. 32/13

[6] Инструкција још ближе описује шта би белешком требало обухватити, па тако: наводе се предузете радње, разлози због којих су оне предузете, као и да ли је дошло до измене датума или не и које су последице ове измене.

[7] Асоцијација шефова полиција http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf последњи пут приступљено 19.05.2014.год.

Он гласи: „Ни једна активност или радња предузета од стране органа поступка или његових припадника не би смела мењати податке садржане на рачунару или уређају за складиштење података, а који би се касније могли користити у поступку. Следећи принцип је: У случајевима када се нађе да је неопходно приступити оригиналним подацима на рачунару или на носиоцима података, лице које им приступа мора за то бити компетентно, а такође и у могућности да пружи доказе којима би образложило релевантност и импликације сопствених радњи. Трећи принцип гласи: мора бити створен писани траг или друга врста евиденције у вези свих поступака примењених на рачунарски базиране електронске доказе. Независна трећа страна може имати могућност да испита те поступке и оствари исти резултат. Четврти принцип подразумева да: Лице задужено за поступање у датом случају (задужено ОСЛ) има општу одговорност за осигурање примене ових принципа и закона. Као што се може приметити принципи се значајно разликују, а теже истом резултату. Суштински општи принципи прокламовани обавезном инструкцијом су редуцирани принципи АЦПО, а значајно је рећи и да упрошћено они представљају врсту парафразираних принципа АЦПО. Наиме, не би требало мењати дигиталне трагове, а уколико се и морају дирати у неопходним случајевима, то се мора предузимати од стране стурчног и компетентног лица и уз то се мора направити писани запис или друга врста евидентирања оваквих активности, у том смислу неопходно је одредити и одговорно лице са обавезом примене закона и осталих принципа. Може се видети да је интенција МУП такође била да се уреди ова област на најадекватнији могући начин.

3.1. ОРГАНИЗАЦИОНЕ ЈЕДИНИЦЕ НАДЛЕЖНЕ ЗА ПОСТУПАЊЕ У МУП РС

У том циљу можемо препознати неколико нивоа за поступање припадника полиције. Опште надлежности, специјализоване и уже специјализоване. Сви припадници полиције осим припадника Службе за специјалне истражне мере (ССИМ) и Управе криминалистичке полиције (УКП) Службе за борбу против организованог криминала (СБПОК) - одељења за борбу против високотехнолошког криминала (ВТК). Ова категоризација је везана за ниво и озбиљност приступања прикупљању, обради и очувању дигиталних трагова.

Инструкцијом се прописује и обавезна опрема полицијских службеника за прикупљање електронских доказа. Њом се указује да би припадници полиције требало да поседују специфичне елементе опреме за поступање са оваквим траговима. Најзначајнија опрема (материјал) предвиђен чл.3. инструкције је фотоапарат и/или камера за снимање лица места и информација на екрану, антистатичке кесе и кутије на склапање. Остала опрема је по правилу стандардна за многе друге китове (облике опреме) за вршење увиђаја. Специфичност трагова изискује и опрему која носи са собом специфичности. Антистатичке кесе и кутије за склапање носе са собом могућност да се не оштете или да се не утиче негативно на дигиталне трагове приликом обезбеђења дигиталних трагова. Ова обавезна опрема односи се на прву категорију службеника полиције и сматра се да није неопходна већа или конкретнија опрема у циљу првог поступања на месту догађаја на којем постоје диитални трагови. Могуће је у овом смислу разматрати и питање вршења увиђаја на рачунарима (уређајима за аутоматску обраду података, телефонима, другим дигиталним уређајима, мрежним окружењима, пословним мрежама и сложеним инфраструктурама). Овај облик

обраде места догађаја произилази и из аналогије са судском праксом. У складу са постојећом судском праксом ова радња може бити веома лако дефинисана[8]. У погледу примера из судске праксе није се сматрало претресањем прегледање смс порука на телефону, а како можемо на томе даље разматрати, није се постављало питање проблема надзора комуникације, у више различитих поступака који су се поводом датог предмета водили. Аналогијом изведеном из овог случаја могуће је многе ствари закључити, у правцу питања вршења увиђаја на рачунарима, али при том морамо водити рачуна и о чињеници да је након ових одлука судске праксе донет нови ЗКП. У њему је први пут регулисано претресање уређаја за АОП и носилаца дигиталних доказа. Такође овим законом је предвиђено и вршење увиђаја на стварима. Овде је аналогија увиђаја на покретним стварима управо могућа. Но, инструкција је овај део предвидела као део којим би се бавиле друга и трећа категорија припадника полиције. Најзначајнији моменти којима се бави инструкција се везују за прибављање трагова и предмета претресањем. Тако се инструкција бави претресањем места извршења кривичног дела, предвиђањем обавезе обезбеђења и места и уређаја присутних на том месту. Овај моменат се нарочито подвлачи обавезивањем на одређена поступања за случајеве да рачунар није укључен, односно, када је укључен, дајући надлежност за даље поступање у другом случају лицима која су за то овлашћена из друге и треће категорије ОСЛ.

У случају да је искључен забрањује се укључивање рачунара од стране лица која су из прве категорије. Такође се полицијски службеници обавезују да потраже лозинке и приручнике са упутствима за софтвер у дневницима и белешкама око рачунара, као и све повезане уређаје за складиштење електронских података (њих и обавезно одузима). Описују се и начини поступања са одузетим рачунарима (и другим електронским уређајима), начинима и средствима паковања и поступањем осумњичених лица (у смислу потписивања на облицима паковања), односно њиховог уношења у потврду о привремено одузетим предметима и записнику о претресању. Анализу и вештачење рачунара обавља ССИМ УКП, као трећа категорија припадника полиције. Инструкцијом се разликују поступци привременог одузимања рачунара и рачунарске опреме када су они укључени и када нису, као и у вези категорија да ли су у питању лап топ или слични уређаји. Код њих ће се начин утврђивања да ли су укључени разликовати у односу на друге, као и начин искључивања. Интересантно је да инструкција не разликује и таблете и хибридне уређаје у том смислу па је неопходно вршити аналогије на месту догађаја нпр. за донгл, сматр телевизор, микроталасну пећницу или друге „смарт“ уређаје снабдевене рачунарима. Поступање у случајевима рачунара који су искључени подразумева њихово искључивање из зида и фотографисање свих прикључака пре њиховиг искључивања и обезбеђивања папиром и лепљивом траком преко свих улаза, што је праћено верификовањем печаћењем и потписивањем. У свим случајевима осумњиченима је приступ рачунару у оваквим случајевима строго забрањен. Инструкцијом се припадници прве категорије ОСЛ обавезују да траже од

[8] Према Presudи Okružnog suda u Čačku K. 96/07 od 15. oktobra 2007. godine i presudи Vrhovnog suda Srbije Kž-I-2678/07 od 18. februara 2008. godine pregledanje sms poruka sa telefona ne predstavlja pretresanje telefona već uviđaj na pokretnoj stvari objavљeno y Bilteny sudske prakse Vrhovnog suda Srbije, br. 1/2008

корисника или другог лица од кога се рачунар привремено одузима податке о томе да ли користе неки од програма за шифровану заштиту рачунара (енкрипцију) или неки од сервиса на интернету за складиштење података или комуникацију. Уколико јесте морају се контактирати друге две категорије припадника полиције ради даљег поступања. Њихова обавеза да те податке пруже није санкционисана никаквим прописима у Србији али се ОСЛ на постављање ових питања обавезују. Када је у питању укључен рачунар након обезбеђења простора место и каблове рачунара је обавезно фотографисати. Инструкција строго забрањује претраживање рачунара а обавезује ОСЛ да фотографише активни прозор екрана рачунара и описати у службеној белешци. Оба описана случаја праве проблеме у практичном поступању у којем је у датом тренутку нпр. укључен неки од програма за физичко уништење података на том рачунару или уколико неки од саучесника управо комуницира са осумњиченим. Инструкција предвиђа у овом случају насилно искључење уређаја из струје. Наравно и оваква активност повлачи са собом уништење одређених података, али уз мање последице. Овом инструкцијом се не дају одговори на овакве случајеве, али уколико бисмо применили други принцип АЦПО ово би се могло решити. Инструкција предвиђа и укључивање из стања укљученог скрин сејвера путем миша а не путем тастатуре. Ипак у том смислу се не води рачуна о уређајима са активним екраном на додир (тзв. тачскрин), али опет се аналогијом они и не би могли другачије укључити до додиром екрана. Наравно овде су могуће и различите друге варијације на тему укључивања из стања спавања уређаја. На пример, укључивање на отисак прста лап топ ралунара или преко препознавања лица. Овакви моменти се решавају аналогијом са претресањем стана и осталих просторија. У погледу кућних мрежа предвиђено је да ОСЛ пронађе рутер (модем) и искључи га из телефона (или ЛАН-а), када се треба одузети рутер (модем) неопходно је контактирати другу и трећу категорију ОСЛ. Када су у питању пословне мреже или сервер сложене инфраструктуре одмах се контактирају припадници друге и треће категорије ОСЛ. Инструкцијом се третирају и случајеви одузимања мобилних телефона, где је слична ситуација у погледу поступања као и категоризација у виду укључен и искључен. Али разлика постоји у случајевима када се привремено одузимају телефони у случајевима када се ради о хитним случајевима, односно уколико се очекује остваривање комуникације која би поспешила вођење истраге, мобилни телефон мора остати укључен, у другим случајевима се искључује, након фотографисања и забележавања свега што се налази на екрану. Такође, забрањује се полицијским службеницима да самостално претражују телефон у циљу прибављања доказа. Следи се и аналогија са питањима у вези са енкрипцијоми шифрама, и прављењем белешки у вези свих активности и података који су прибављени у вези са телефоном (шифара, пин бројева или покрета по екрану). Телефони и сви други дигитални уређаји се пакују у антистатичке кесе. Треба поменути да постоји и потреба за фарадејевим кавезима у случајевима дигиталних уређаја, али о њима није много говорено у инструкцији.

4. ЗАКЉУЧАК

Приказани мандаторни поступци су први икада прописани у оквирима министарства унутрашњих послова у вези са овом врстом дигиталних трагова и предмета носилаца. Оваква ситуација била је изнуђена

различитим проблемима до којих се долазило у практичном поступању са дигиталним траговима. Нормално је да овакви поступци који су први пут прописани имају својих мањкавости на које смо посебно указали, као на пример поступање са уређајима са активним екранима на додир, који се не укључују мишем или случај са третирањем увиђаја. Указивањем на овакве недостатке не желимо критиковати постојећа решења, обзиром да су она, ипак до сада, најбоља али као и сама технологија она се константно морају унапређивати, мењати и прилагођавати. Значајан простор остаје и јавном тужилаштву за деловање у овој области, као руководиоцу предистражног и истражног поступка. У том смислу могу се прописати процедуре и овлашћења представника тужилаштва за деловање преко налога припадницима полиције који су дужни по њима поступати. Оне би биле коректив обавезне инструкције поступања припадника полиције, и у том смислу не би постојала потреба за изменом скорије донете инструкције. Тиме би се и добио систем за међусобно допуњавање и кориговање којим би се обезбедиле адекватне и обавезујуће процедуре свих укључених у поступак доказивања.

ЛИТЕРАТУРА

1. Ивановић, З. Кесић, Т. Правни статус електронског надзора над обавештајцима у САД, Супротстављање савременом организованом криминалу и тероризму, ИВ ЕДИЦИЈА ΑΣΦΑΛΕΙΑ, Књига В Криминалистичко-полицијска академија, Београд, 2013
2. Ivanović, Z. Žarković, M. Scientific approach in building teams for seizure of digital evidence, pp. 399-413 in Thematic proceedings of international significance, Vol I, Academy of criminalistics and police studies, 2013, Ed. Goran Milošević
3. A. C. F. Thomson, Windows 8 Forensic Guide, The George Washington University, Washington, D.C. 2012.
4. Collie, J.: The windows IconCache.db: A resource for forensic artifacts from USB connectable devices, Digital Investigation 9 (2013) pp. 200–210, Discovery Forensics Ltd, 23 Austin Friars, London EC2N 2QP, UK
5. Harms, K. Forensic Analysis of System Restore Points in Microsoft Windows XP, MANDIANT Corporation 675 N Washington Street Suite 210
6. Alexandria, VA 22314Асоцијација шефова полиција http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

KOMPJUTERSKI TIMOVI ZA BRZO REAGOVANJE U ZEMLJAMA BIVŠE JUGOSLAVIJE

COMPUTER EMERGENCY RESPONSE TEAMS IN FORMER YUGOSLAV REPUBLICS

DEJAN VULETIĆ
Institut za strategijska istraživanja, Beograd, dejan.vuletic@mod.gov.rs

---

Rezime: *U radu je dat kratak opis uloge, namene i zadataka tima za odgovor na kompjuterski incident. Razmatrano je aktuelno stanje po pitanju dostignutog nivoa razvoja nacionalnih timova za odgovor na kompjuterski incident u zemljama bivše Jugoslavije.*

Ključne reči: *Kompjuterski incident, odgovor.*

Abstract: *The paper gives a brief description of the role, purpose and mission of a computer emergency response team. The paper contains the current situation regarding the achieved level of development of national computer emergency response teams in former Yugoslav countries.*

Keywords: *Computer incident, response.*

1. UVOD

Kompjuterski tim za brzo reagovanje (*Computer Emergency Response Team - CERT*) je tim za sprečavanje, podršku i odgovore na kompjuterske napade na računarske sisteme.

Istorija CERT-a je vezana za pojavljivanje malicioznih programa. Prvi tim takve vrste formiran je na *Carnegie Mellon University* kao posledica pojavljivanja računarskog crva "Moris" (*Morris Worm*).

CERT je ključni alat za zaštitu kritičnih informacionih infrastruktura (*Critical Information Infrastructure Protection - CIIP*).

Glavna uloga CERT-a je koordinacija i deljenje informacija sa zainteresovanim stranama i ciljnim grupama u javnom i privatnom sektoru i međunarodnim partnerima. Trenutno u svetu ima više stotina CERT-ova.

Nacionalni CERT donosi uputstva, smernice, preporuke, savete i mišljenja u slučaju incidenata u sajber prostoru koji su od značaja za informacionu bezbednost određene zemlje.

Formira se na osnovu zakona (npr. koji reguliše informacionu bezbednost) ili drugom odlukom vlade.

U delokrug rada CERT-a nije uključeno operativno rešavanje problema i briga o zaštiti računarskih sistema, kažnjavanje i arbitraža u sporovima, pokretanje krivičnih prijava i drugo.

Postojanje nacionalnog CERT-a ne isključuje postojanje i drugih CERT-ova u državi. Uloga nacionalnog CERT-a je, između ostalog, da koordinira njihov rad.

Nacionalni CERT sprovodi preventivne tj. proaktivne (praćenje stanja, objavljivanje informacija) i reaktivne mere.

Realizuje značajne aktivnosti po pitanju edukacije korisnika kroz različite forme obuke, publikovanje različitih materijala iz domena informacione bezbednosti.

Nacionalni CERT sarađuje sa relevantnim institucijama telima na nacionalnom (MUP, provajderi internet usluga, privatne IT kompanije…) i međunarodnom planu (npr. *Forum of Incident Response and Security Team - FIRST*)

2. KOMPJUTERSKI TIM ZA BRZO REAGOVANJE NA NIVOU EVROPSKE UNIJE

Evropska agencija za mrežnu i informacionu bezbednost (*European Network and Information Security Agency - ENISA*) je osnovana 2004. godine uredbom Evropskog parlamenta i Veća (EC broj 460). Svrha ENISA-e je da se osigura visok nivo mrežne i informacione bezbednosti Evropske unije [1].

Evropska unija je 11.9.2012. god. formirala stalni tim za odgovor na kompjuterske incidente, CERT-EU, a koji se tiču različitih institucija, agencija i tela Evropske unije [2].
Tim je formiran od eksperata za informacionu bezbednost iz više institucija EU (Evropske komisije, Evropskog Parlamenta, različitih komiteta).

Blisko sarađuju sa ostalim CERT-ovima zemalja članica kao i sa CERT-ovima zemalja koje nisu članice kao i IT specijalistima iz različitih kompanija koje se bave informacionom bezbednošću.

CERT-EU će postepeno proširivati svoje usluge, na osnovu zahteva osnivača i sprovodiće različite akcije u skladu sa raspoloživim kapacitetima, resursima i potrebama.

U svim zemljama Evropske unije i nekim zemljama koje nisu članice EU postoje CERT-ovi koji sarađuju kroz TF-CSIRT (*Task Force Collaboration Security Incident Response Teams*) [3].

TF-CSIRT je radna grupa koja promoviše saradnju između CERT-ova u Evropi, te sarađuje sa sličnim grupama u drugim regionima. TF-CSIRT obezbeđuje forum gde članovi CERT zajednice mogu razmenjivati iskustva i znanja. Članovi TF-CSIRT aktivno su uključeni u osnivanje i rad CERT usluga u Evropi i drugim zemljama.

TF-CSIRT promoviše korišćenje zajedničkih standarda i postupaka za odgovor na incidente u sajber prostoru. Zajednički standardi imaju veliki potencijal za smanjenje vremena potrebnog za prepoznavanje i analizu incidenata, a zatim preduzimanje odgovarajuće akcije.

TF-CSIRT takođe pomaže u uspostavljanju novih CERT-ova, i obučavanje članova postojećih timova o najnovijim alatima i tehnikama za upravljanje incidentima.

3. AKTUELNO STANJE PO PITANJU KOMPJUTERSKIH TIMOVA ZA BRZO REAGOVANJE U ZEMLJAMA BIVŠE JUGOSLAVIJE

Zemlje bivše Jugoslavije su već punopravne članice Evropske unije (Slovenija, Hrvatska) ili nastoje da to postanu te svoje zakonodavstvo i organizaciju moraju usklađivati sa potrebama i zahtevima te organizacije. Organizacijski zahtevi EU u području informacione bezbednosti izraženi su prvenstveno u okviru politike bezbednosti, različitih propisa i preporuka. Motiv za uspostavu CERT-a proizlazi i iz preporuka EU o uspostavi CERT-a u svim državama članicama, kao i zemljama potencijalnim članicama.

Značajan doprinos formiranju CERT-ova doprinele su međunarodne organizacije Međunarodna telekomunikaciona unija (*International Telecommunication Union – ITU*) i Međunarodno multilateralno patnerstvo protiv sajber pretnji (*International Multilateral Partnership Against Cyber Threats – IMPACT*). Edukacijom i dostavljanjem dokumenata procene spremnosti za uspostavljanje nacionalnog CERT-a (*Readiness assessment report to establish a National CERT)* pružili su značajnu pomoć zemljama regiona da formiraju nacionalni tim za odgovor na kompjuterski incident.

Slovenija. Sl-CERT je slovenački nacionalni CERT i predstavlja centralnu organizaciju za prijavljivanje incidenata u računarskim sistemima na teritoriji Slovenije. U skladu sa sporazumom koji je potpisan sa Vladom, obavljaju ulogu nacionalnog CERT-a. Predstavljaju deo Akademske i istraživačke mreže Slovenije (*Academic and Research Network of Slovenia - ARNES*) [4].

Hrvatska. HR-CERT je formiran 2008. godine u skladu sa Zakonom o informacijskoj sigurnosti i prema tom Zakonu jedan od zadataka jeste obrada incidenata na Internetu tj. očuvanje informacione bezbednosti u Republici Hrvatskoj. Prema pomenutom Zakonu, HR-CERT je zasebna jedinica koja se formira u Hrvatskoj akademskoj i istraživačkoj mreži (*Croatian Academic and Research Network - CARNet*) [5].

Prema Pravilniku o radu Nacionalnog CERT-a on se bavi incidentom, ako se jedna od strana nalazi u Hrvatskoj (ako je u .hr domenu ili hrvatskom IP adresnom prostoru).

Misija HR-CERT-a jeste prevencija i zaštita od povrede bezbednosti javnih računarskih sistema u Hrvatskoj. U okviru svog delovanja sprovodi preventivne (praćenje stanja, objavljivanje informacija, sigurnosna upozorenja, edukacija) i reaktivne mere (koordinacija rešavanja problema).

Crna Gora. CIRT.me je formiran 2012. godine sa ciljem reakcije i koordinacije delovanja u slučaju sajber napada [6].

Osnovan je u skladu sa Zakonom o informacionoj bezbjednosti. Formiran je kao posebna organizaciona jedinica Ministarstva za informaciono društvo i telekomunikacije.

Bavi se incidentom ako je jedna od strana u incidentu nalazi u Crnog Gori (odnosno ako je u .me domenu ili u crnogorskom IP adrsnom prostoru.)

Bosna i Hercegovina. Pored Srbije i Makedonije, Bosna i Hercegovina je jedna od zemalja koja nema nacionalni CERT ali se preduzimaju aktivnosti na tom planu. Formiranje tima zavisi od političke odluke. Značajan korak na tom planu predstavlja činjenica da je urađena Strategija uspostave CERT-a u Bosni i Hercegovini a biće najverovatnije vezan za Ministarstvo sigurnosti,

Makedonija. Vlada Makedonije je usvojila Odluku o osnivanju nacionalnog kompjuterskog tima za brzo reagovanje (CERT.mk) i oformljena je radna grupa za osnivanje CERT-a. Prema aktuelnim radnim dokumentima, nacionalni CERT biće pozicioniran u okviru Agencije za elektronske komunikacije.

Srbija. Zakonom o informacionoj bezbednosti, čija je izrada u toku, biće definisan i nacionalni CERT u Republici Srbiji. Očekuje se da pomenuti Zakon bude usvojen do kraja tekuće godine. U aktuelnoj radnoj verziji Zakona o informacionoj bezbednosti, RsCIRT će najverovatnije biti pozicioniran u okviru Akademske mreže Srbije (AMRES).

4. ZAKLJUČAK

Na osnovu navedenog može se zaključiti da dostignuti nivo razvoja kompjuterskih timova za brzo reagovanja nije isti u svim zemljama bivše Jugoslavije.

Timovi su organizaciono i hijerarhijski pozicionirani u različitim strukturama, u sastavu akademske mreže (Slovenija, Hrvatska, verovatno Srbija) ili nekog drugog tela ili instituciju vlade.

Imajući u vidu pretnje u sajber prostoru i spoljnopolitička opredeljenja zemalja bivše Jugoslavije, formiranje kompjuterskih timova za brzo reagovanje se nameće kao potreba ali i obaveza.

Formiranje nacionalnih CERT-ova u zemljama u kojima to još uvek nije učinjeno je samo pitanje vremena te je stoga realno za očekivati da već sledeće godine sve zemlje regiona imaju nacionalni kompjuterski tim za brzo reagovanje na kompjuterski incident, integrisan u FIRST i druge međunarodne organizacije, a nije nerealna opcija formiranje regionalnog CERT-a.

LITERATURA

[1] ENISA, www.enisa.europa.eu

[2] CERT-EU, http://cert.europa.eu

[3] TF-CSIRT, http://www.terena.org/activities/tf-csirt/

[4] Sl-CERT, https://www.cert.si/

[5] HR-CERT, www.cert.hr

[6] CIRT.me, www. cirt.me

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

KORIŠĆENJE FREEIPA SOFTVERA NA CENTOS LINUX SERVERU ZA MENADŽMENT IDENTITETA U MREŽNOM OKRUŽENJU

USING FREEIPA ON A CENTOS LINUX SERVER FOR IDENTITY MANAGEMENT IN A NETWORK ENVIRONMENT

ANDRIJA KARADŽIĆ
Vojna akademija, Beograd, andrija888@yahoo.com

OGNJEN LETIĆ
Vojna akademija, Beograd, ogletic@gmail.com

DUŠAN PERIŠIĆ
Vojna akademija, Beograd, dullle@live.com

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

Rezime: *Sa stanovišta računarskih nauka menadžment identiteta (IDM) predstavlja upravljanje individualnim korisnicima, njihovom autentifikacijom, autorizacijom, privilegijama i ograničenjima u sistemu sa ciljem povećanja bezbednosti i produktivnosti sa istovremenim smanjenjem cene, vremena nedostupnosti usluga i ponavljanja aktivnosti. U ovom radu prikazano je besplatno rešenje otvorenog koda koje se može koristiti na Windows i Linux radnim okruženjima, a predsatvlja alternativu Microsoft-ovom Active Directory sistemu.*

Ključne reči: *FreeIPA, Menadžment identiteta, Open source, CentOS*

Abstract: *From the point of view of computer sciences, identity management (IDM) represents the management of individual users, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks. The main idea of this paper is to present a free, open source alternative to Microsoft's Active Directory system, which can be used on both Windows and Linux server and client environments.*

Keywords: *FreeIPA, Identity management, Open source, CentOS*

1. INTRODUCTION

The Internet is a very widely used form of modern communication technology, despite its many security flaws. Many of the protocols used in the Internet do not provide any security. There are software tools available for download that can allow hackers to intercept and jeopardize information security. Thus, applications that send unencrypted passwords over the network are very vulnerable. An even worse scenario is client/server applications that rely on the clients program to be trustworthy when it comes to the identity of the user currently logged on. Some applications rely on the client to remain within the circle of actions he is allowed to perform, with no other enforcement by the server.

Identity is defined as the distinct personality of an individual (or object) regarded as a persisting entity. It is the perception of an persisting entity formed by an unique combination of characteristics of the entity.[6]

Identity management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. [5]

Basically, identity management is about defining user privileges, i.e. what users can do on the network, on what devices, and under which conditions. A lot of security products focus on controlling mobile access to information systems. In an enterprise setting, identity management is used to increase security and productivity, while decreasing cost and redundant effort.

As a good security practice, tools for managing identity management should be set up as an application on a dedicated server. At the core of an identity management system are policies defining which devices and users are permitted to access the network and what actions a user can perform, depending on his device, location and other factors. All of this also depends on appropriate management console functionality, including policy definition, reporting, alerts, alarms and other common management and operations requirements. An alarm might be triggered, for example, when a specific user tries to access a resource for which they do not have permission. Reporting produces an audit log documenting what specific activities were initiated.

FreeIPA is an open source project whose goal is to provide an easily managed Identity, Policy and Audit environment,

intended to be used on Linux and Unix computer networks.
FreeIPA currently uses 389 Directory Server for its LDAP implementation, MIT's (Massachusetts institute of technology) Kerberos 5 for authentication and single sign-on, the Apache HTTP Server and Python for the management framework and Web UI, and (optionally) Dogtag for the integrated CA and BIND with a custom plug-in for the integrated DNS. [2]

The 389 Directory Server (previously Fedora Directory Server) is an LDAP (Lightweight Directory Access Protocol) server developed by Red Hat, as part of Red Hat's community-supported Fedora Project. The name 389 is derived from the port number for LDAP.[4]

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. It was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

The Apache HTTP Server Project is a collaborative software development effort aimed at creating a robust, commercial-grade, featureful, and freely-available source code implementation of an HTTP (Web) server.[3]

While each of the major components of FreeIPA is a pre-existing open source project, it is the bundling of these components into a single manageable suite with a Comprehensive Management Interface that make FreeIPA more comparable to its proprietary software cousins, Identity Manager and Active Directory.

FreeIPA aims to provide support not just for Linux and Unix based computers but ultimately Microsoft Windows and Apple Macintosh computers also.

2. DESCRIPTION OF THE MAIN COMPONENTS

A. Kerberos protocol

The Kerberos protocol is the key element to secure authentication. Some of the main features of the Kerberos protocol include:

- The user's password must never travel over the network;
- The user's password must never be stored in any form on the client machine: it must be immediately discarded after being used;
- The user's password should never be stored in an unencrypted form even in the authentication server database;
- The user is asked to enter a password only once per work session. Therefore users can transparently access all the services they are authorized for without having to re-enter the password during this session. This characteristic is known as **Single Sign-On**;
- Authentication information management is centralized and resides on the authentication server. The application servers must not contain the authentication information for their users. This is essential for obtaining the following results:

The administrator can disable the account of any user by acting in a single location without having to act on the several application servers providing the various services;
When a user changes its password, it is changed for all services at the same time;
There is no redundancy of authentication information which would otherwise have to be safeguarded in various places;

- Not only do the users have to demonstrate that they are who they say, but, when requested, the application servers must prove their authenticity to the client as well. This characteristic is known as **Mutual authentication**;
- Following the completion of authentication and authorization, the client and server must be able to establish an encrypted connection, if required. For this purpose, Kerberos provides support for the generation and exchange of an encryption key to be used to encrypt data. [1]

B. Kerberos components

This section only lists the components of the Kerberos protocol necessary to explain the principles of its functioning.

Realm
The term realm indicates an authentication administrative domain. Its intention is to establish the boundaries within which an authentication server has the authority to authenticate a user, host or service. This does not mean that the authentication between a user and a service that they must belong to the same realm: if the two objects are part of different realms and there is a trust relationship between them, then the authentication can take place.

Basically, a user/service belongs to a realm if and only if he/it shares a secret (password/key) with the authentication server of that realm.

Principal
A principal is the name used to refer to the entries in the authentication server database. A principal is associated with each user, host or service of a given realm.

Ticket
A ticket is something a client presents to an application server to demonstrate the authenticity of its identity. Tickets are issued by the authentication server and are encrypted using the secret key of the service they are intended for. Since this key

is a secret shared only between the authentication server and the server providing the service, not even the client which requested the ticket can know it or change its contents. Each ticket has an expiration (generally 10 hours). This is essential since the authentication server no longer has any control over an already issued ticket. Even though the realm administrator can prevent the issuing of new tickets for a certain user at any time, it cannot prevent users from using the tickets they already possess. This is the reason for limiting the lifetime of the tickets in order to limit any abuse over time.

Encryption
Kerberos often needs to encrypt and decrypt the messages (tickets and authenticators) passing between the various participants in the authentication. It is important to note that Kerberos uses only symmetrical key encryption (in other words the same key is used to encrypt and decrypt).

Key Distribution Center (KDC)
The authentication server in a Kerberos environment, based on its ticket distribution function for access to the services, is called Key Distribution Center or more briefly KDC. Since it resides entirely on a single physical server (it often coincides with a single process) it can be logically considered divided into three parts: Database, Authentication Server (AS) and Ticket Granting Server (TGS).[1]

C. Kerberos operation

In order to explain the basic principles of Kerberos operation, the list of packets exchanged between the client and the KDC are listed here. It is important to note that an application server never communicates directly with the Key Distribution Center: the service tickets, even if packeted by TGS, reach the service only through the client wishing to access them.

- **AS_REQ** is the initial user authentication request (i.e. made with kinit) This message is directed to the KDC component known as Authentication Server (AS);
- **AS_REP** is the reply of the Authentication Server to the previous request. Basically it contains the TGT (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user);
- **TGS_REQ** is the request from the client to the Ticket Granting Server (TGS) for a service ticket. This packet includes the TGT obtained from the previous message and an authenticator generated by the client and encrypted with the session key;
- **TGS_REP** is the reply of the Ticket Granting Server to the previous request. Located inside is the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS;

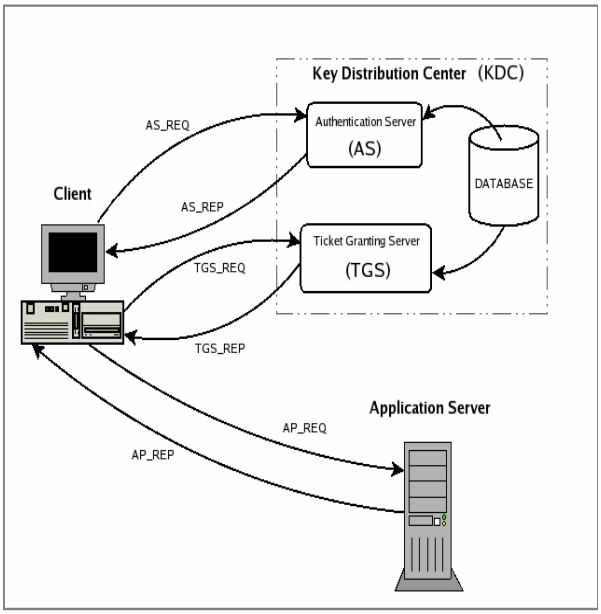


Fig. 1: Packet transmission between the client, KDC and application server

- **AP_REQ** is the request that the client sends to an application server to access a service. The components are the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but this time encrypted using the service session key (generated by TGS);
- **AP_REP** is the reply that the application server gives to the client to prove it really is the server the client is expecting. This packet is not always requested. The client requests the server for it only when mutual authentication is necessary. [1]

3. IMPLEMENTATION

The suggested solution for identity management will take the form of a client-server environment, where the server will host the FreeIPA server authentication software, and clients will establish connection to it using FreeIPA client and Kerberos protocol.

The main idea is to have a CentOS Linux server, that hosts the authentication software, and a Windows XP and CentOS 6.5 clients, to demonstrate how both Linux and Windows based clients are able to successfully authenticate.

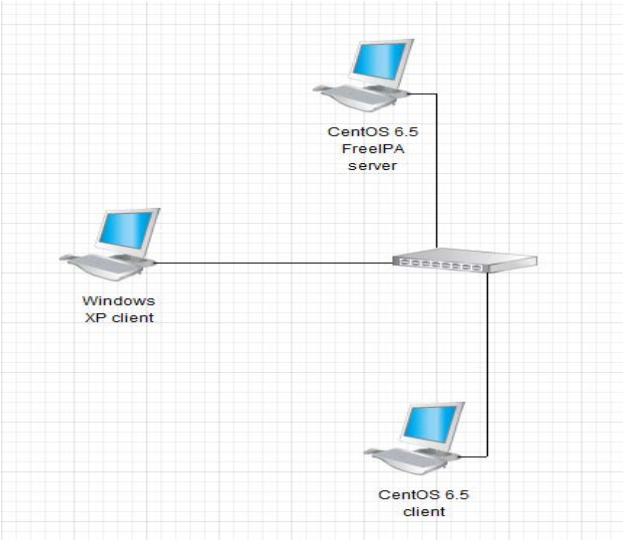


Fig. 2: Scenario network diagram

First of all, the FreeIPA needs to be configured on the CentOS server machine. The basic configuration is the following:

Free IPA Server Name : s1
Free IPA Server IP: 192.168.146.20
Domain: va.test.com

It is necessary to append the IP address to the /etc/hosts file:

```
192.168.146.20    s1.va.test.com s1
```

Then change the `/etc/resolve.conf file:`

```
search va.test.com
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Results of a ping command:

```
[root@s1 ~]# ping s1
PING  s1.va.test.com  (192.168.146.20)  56(84)
bytes of data.
64 bytes from s1.va.test.com (192.168.146.20):
icmp_seq=1 ttl=64 time=0.037 ms
^C
--- s1.va.test.com ping statistics ---

1 packets transmitted, 1 received, 0% packet
loss, time 572ms
```

The next step is the firewall configuration. This is the content of the `/etc/sysconfig/iptables file:`

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
 :OUTPUT ACCEPT [0:0]
 -A INPUT -m state --state ESTABLISHED,RELATED
-j ACCEPT
 -A INPUT -p icmp -j ACCEPT
 -A INPUT -i lo -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 80 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 443 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 389 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 636 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 88 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 464 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 53 -j ACCEPT
 -A INPUT -m state --state NEW -m udp -p udp -
-dport 88 -j ACCEPT
 -A INPUT -m state --state NEW -m udp -p udp -
-dport 464 -j ACCEPT
 -A INPUT -m state --state NEW -m udp -p udp -
-dport 123 -j ACCEPT
 -A INPUT -m state --state NEW -m udp -p udp -
-dport 53 -j ACCEPT
 -A INPUT -m state --state NEW -m tcp -p tcp -
-dport 22 -j ACCEPT
 -A INPUT -j REJECT --reject-with icmp-host-
prohibited
 -A FORWARD -j REJECT --reject-with icmp-host-
prohibited
 COMMIT
```

This enables listening on all ports necessary for the FreeIPA to work. Changing the iptables file requires the iptables service to be restarted. Next comes the installing of the FreeIPA server. During this installation, the host name, domain name and realm name are set up. In order for the authentication server to function a BIND server has to be installed and set up. These are the settings in this scenario (/etc/named.conf) :

```
options {
        listen-on   port   53   {   127.0.0.1;
        192.168.146.100; };
        listen-on-v6 port 53 { ::1; };
        forwarders { 8.8.8.8; 8.8.4.4; };
        directory       "/var/named";
                dump-file
        "/var/named/data/cache_dump.db";
                statistics-file
        "/var/named/data/named_stats.txt";
                memstatistics-file
        "/var/named/data/named_mem_stats.txt";

                allow-query  {localhost;
        192.168.146.0/24;};
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        bindkeys-file "/etc/named.iscdlv.key";

                managed-keys-directory
        "/var/named/dynamic";
        };
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

```
zone "." IN {
        type hint;
        file "named.ca";
};
zone "va.test.com" IN {
        type master;
        file "/etc/named/va.test.com";
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

The BIND server requires a zone file to be set up, as suggested in the previous file. The zone file has to be named va.test.com (for the purposes of this specific implementation) and it has to be located in the /etc/named/ directory. The zone file is set up like so:

```
$ORIGIN va.test.com.
$TTL 86400
@ IN SOA va.test.com. hostmaster.va.test.com.
(
 01 ; serial
 3H ; refresh
 15M ; retry
 1W ; expiry
 1D ) ; minimum
IN NS s1
s1 IN A 192.168.146.100
;
; ldap servers
_ldap._tcp IN SRV 0 100 389 s1
;kerberos realm
_kerberos IN TXT VA.TEST.COM
; kerberos servers
_kerberos._tcp IN SRV 0 100 88 s1
_kerberos._udp IN SRV 0 100 88 s1
_kerberos-master._tcp IN SRV 0 100 88 s1
_kerberos-master._udp IN SRV 0 100 88 s1
_kpasswd._tcp IN SRV 0 100 464 s1
_kpasswd._udp IN SRV 0 100 464 s1
;ntp server
_ntp._udp IN SRV 0 100 123 s1
```

After setting up, and restarting the BIND server, the service can be tested via the nslookup command:

```
nslookup
 > server 192.168.146.100
 Default server: 192.168.146.100
 Address: 192.168.146.100#53
 > s1
 Server: 192.168.146.100
 Address: 192.168.146.100#53
Name: s1.va.test.com
 Address: 192.168.146.100
> s1.va.test.com.
 Server: 192.168.146.100
 Address: 192.168.146.100#53
Name: s1.va.test.com
 Address: 192.168.146.100
> set type=SRV
 > _kerberos._tcp
 Server: 192.168.146.100
 Address: 192.168.146.100#53
_kerberos._tcp.va.test.com service = 0
100 88 s1.va.test.com.
```

The graphical interface of the FreeIPA can be accessed via the link https://s1.va.test.com/ipa/ui/

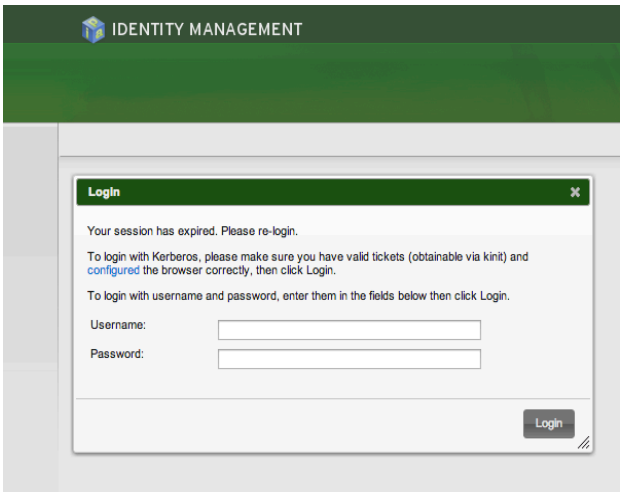


Fig. 3: The FreeIPA graphical interface

The Windows XP client only requires an installation of the Kerberos for Windows software in order to be able to authenticate without the need for the user to input a password.

A Kerberos ticket can be acquired by using the kinit command, or simply by setting up the Kerberos to fetch the ticket at startup.

This client also has the capability of authenticating via the WebUI interface of FreeIPA. This is still a valid way of confirming a users identity, though a little less secure than the Kerberos approach.

When it comes to the CentOS Linux client, there are some basic settings that need to be configured before being able to access the FreeIPA server, and authenticate. First the /etc/hosts file needs to contain both the client, and the server entries. Then, running the “ipa-client-install” command configures the client OS. Some of the notable entries from the setup are:

```
Please provide the domain name of your
IPA server (ex: example.com):
va.test.com

Please provide your IPA server name (ex:
ipa.example.com):
s1.va.test.com

Hostname:                    s1.va.test.com
Realm:                          VA.TEST.COM
DNS          Domain:            va.test.com
IPA        Server:           s1.va.test.com
BaseDN: dc=va,dc=test,dc=com
```

Now, the client user can authenticate using both Kerberos, and the WebUI. Using the WebUI is identical to the Windows client, simply inputting a username and a corresponding password, and the server logs the user in. The other method of using Kerberos is much safer, because the password is not sent over the network. A ticket is acquired by using the "kinit" command in the terminal, adding a username, and providing the users password. The KDC than issues a ticket, which is used to log on safely.

4. CONCLUSION

Taking all of the results of this test scenario into account, it is safe to say that the FreeIPA identity management software presents a valid, free, open source method for a high security level client authentication. The work in this paper demonstrates that it is possible to establish a mixed mode network, with both Linux and Windows clients, which is a great advantage, since it does not limit the client to a specific OS to use in a network environment.

REFERENCES

[1] http://www.kerberos.org/software/tutorial.html

[2] http://en.wikipedia.org/wiki/FreeIPA

[3] http://httpd.apache.org/

[4] http://www.freeipa.org/page/Directory_Server

[5] http://searchunifiedcommunications.techtarget.com/definition/identity-management

[6] F. R. Tewar, "Identity management defined," Ph.D. dissertation, Informatics & Economics, Erasmus University, Rotterdam, Netherland, 2005.

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

AUTORIZACIJA PRISTUPA POJEDINAČNIM PODACIMA U BAZI PODATAKA – DEFINICIJE I REŠENJA

ACCESS CONTROL TO SEPARATED DATA IN DATABASE SYSTEM – DEFINITIONS AND SOLUTIONS

MLADEN VIDIĆ
Saobraćajni fakultet Doboj, mladen@matf.bg.ac.rs

Rezime: *Postoji više aspekata zaštite u bazama podataka „spregnutih" sa softverskim rešenjima. Potrebno je proširiti standardne mehanizme zaštite kolekcije podataka u BP u smeru autorizacije pojedinačnih podataka.Ostali aspekti zaštite i diskrecioni aspekt zaštite (DKP) nad kolekcijama podataka su nedovoljni da nas zaštite od neovlaštenog pristupa podacima unutar heterogenog korisničkog okruženja. Postojeći standardi zaštite trebaju biti prošireni na sistematičan način semantičkom zaštitom podataka u skladu sa kompozitnim stepenom ovlaštenja korisnika ili grupe. U SUBP moguće je upravljati sistemskim privilegijama i postići diskrecionu kontrolu pristupa privilegijama nad kolekcijama podataka. Otvorena su pitanja:Da li korisnik ima pravo da izvrši operaciju nad svim ili samo nad nekim pojavljivanjima kolekcije podataka? Kako postići kompletnu i sistematičnu autorizaciju do na nivo pojavljivanja? Može li se proširiti autorizacija i na atribute kolekcije i da li nas taj sistem štiti od SUPER korisnika sistema? Dolazi se do koncepta restriktivne autorizacije pojavljivanja (RA) odnosno kontrole pristupa pojavljivanjima kolekcije podataka. RA rešavamo parcijalnom doradom postojećeg sistema nad DKP autorizacijom ili sistematičnim proširenjem standardnih mehanizama autorizacije. Prikazujemo sopstveno partikularno rešenje i rešenja koja nude Oracle, IBM u DB2 i IDS, Microsoft SQL Server sa osvrtom na teorijsko i praktično opšte rešenje koje do sada ne postoji.Mehanizmi realizacije preporučuju primenu RA kod korisnika.*

Ključne reči: *Bezbednost i autorizacija u bazama podataka, Restriktivna kompletnost baze podataka, R-kompletnost, RA sistem, RA model, Oracle OLS i VPD, IBM LBAC*

Abstract: *There is a few aspects of security in database systems. It is important to get extension of standard procedures and mechanisms for security in databases to gain access control of separated data instead of collections of data. Other aspects of security are also important but semantic security of separated data by restriction and encryptions are required in modern database applications. Separated data control is not covered in DCL. We have to extend DCL language standard which gives access control semantic over objects in database for collection of data. We introduce Discretionary access control (DKP-covers access control over database objects), Application access control (AKP), Restrictive access control (RKP) or Discretionary Restrictive Authorization (DRA). We have e few important questions about protecting data collections against SUPER administrator and performances. These questions make goal for building systematic theorethical aproach for covering restrictive authorization and comparative analyzing of comercial solutions for RKP. At the end we have built general full R-complete solution for authorization and access control of separeted data instances and their attributes by restriction and encryption.*

Keywords: *Security and authorization in databases, Restrictive completeness DBMS, R-completeness, RA system, Restrictive authorization model, Oracle OLS and VPD, IBM LBAC*

1. UVOD

Svaki SUBP, pored ostalih funkcionalnosti, zadužen je za zaštitu i kontrolu pristupa informacijama, odnosno nadzor i praćenje korisnika i izvršavanja operacija nad BP. Podsistem zaštite u SUBP mora da obezbedi minimalno proveru identiteta (*eng. authentification*), definisanje ovlaštenja i kontrolu pristupa (*eng. authorisation)* i praćenje i evidenciju upotrebe ovlaštenja u SUBP (*eng. auditing*). U radu kao sinonimne koristimo sledeće pojmove: Kolekcija pojavljivanja (skup n-torki tabele, kolekcija instanci objekata u objektnoj kolekciji), Skup elemenata i Objekat SUBP (tabela, pogled,...) kao proizvoljan skup n-torki.

Kontrola upotrebe ovlaštenja i izvršenja operacija u sistemu podrazumeva ekstrakciju složene informacije koja daje odgovor na pitanje: (1.) Da li *korisnik* ima *dozvolu* da izvrši neku *operaciju* nad *kolekcijom pojavljivanja podataka (objektom) SUBP*?

Podsistem SUBP zadužen za rešavanje prethodnog pitanja autorizacije nazivamo DKP (diskreciona kontrola pristupa). U dosadašnjoj praksi za većinu sistema odgovor na ovo pitanje je bio dovoljan. U nekim specijalnim slučajevima, zavisno od konteksta poslovne primene, uz pozitivan odgovor na prvo pitanje, važan je i odgovor na sledeće pitanje: (2.) Da li korisnik ima pravo *da pristupi* ili *izvrši operaciju* nad *svim pojavljivanjima* jedne kolekcije (el. skupa) ili *samo nad nekim* od njih? Kako se

utvrđuje koji podskup cele kolekcije pojavljivanja (objekta SUBP) je dostupan korisniku?

Ovo je pitanje restriktivne autorizacije (RA) i ono se u mnogim konkretnim implementacijama IS samo nametalo i nudilo kontekstno zavisno rešenje za kontrolu pristupa pojavljivanjima kroz samu restrikciju predikatima u upitima i operacijama u aplikacijama. Npr., šef skladišta vidi samo izlazne naloge sa skladišta za koje je zadužen; šef prodaje vidi samo prodaju u odelenju prodaje za koje je nadležan; prodavac vidi samo one naloge koje je sam kreirao. Projektanti moraju predvideti, a programeri implementirati te restrikcije u upitima i operacijama nad kolekcijama podataka. Otvaraju se nova pitanja za koja se ne nude kompletni i sistematični odgovori jer je kontrola restriktivnog pristupa uvek kontekstno zavisna od konkretne poslovne funkcije. Parcijalno rešavanje restriktivne autorizacije diskutuje ovu problematiku i uvodi nas u probleme i zadatke rešavanja restriktivne autorizacije.

Poznatiji relacioni, prošireni relacioni i objektno-orjentisani SUBP poseduju razrađen mehanizam autentifikacije korisnika i DKP do na nivo objekta u nekoj shemi baze podataka (odgovor na pitanje br. 1.). Pitanje kontrole pristupa podskupovima pojavljivanja i finog definisanja ovlaštenja korisnika i osetljivosti podataka nije standardizovano niti rešeno na sistematičan način.

Ako SUBP dozvoli pristup za operaciju nad kolekcijom (objektom baze podataka) ukazuje se potreba za komplementarnim podsistemom za kontrolu pristupa pojavljivanjima podataka u kolekcijama pojavljivanja prema ovlaštenjima korisnika nad njima. Imamo brojne primere poslovne potrebe za primenu autorizacije pristupa pojedinačnim pojavljivanjima na osnovu različitih kriterijuma ovlaštenja i osetljivosti podataka. Otvorena su pitanja: Kako postići kompletnu i sistematičnu autorizaciju do na nivo pojavljivanja u kolekcijama pojavljivanja podataka? Da li ovaj novi tip autorizacije možemo iskoristiti da se zaštitimo od SUPER korisnika u SUBP? U nekim relacionim SUBP postoje ponuđene varijante implementacije restriktivne autorizacije za relacioni model i SQL upitni jezik. Imali smo priliku realizovati jedno partikularno rešenje sistema restriktivne autorizacije u relacionom SUBP Oracle pre pojave ponuđenih rešenja od strane proizvođača SUBP.

Analiza ovih rešenja je obuhvatila i kreiranje odgovarajućih modela RA inverznim inženjeringom i usporednu analizu sa razvijenim terijskim modelom MRA C čime utvrđujemo njihove nedostatke. To je bio put za razvoj opšteg rešenja za RA.

2. DISKRECIONA KONTROLA PRISTUPA

Cilj autorizacije u BP je kontrolisati ovlaštenja korisnika za izvršenje određenih operacija u sistemu ili nad pojedinačnim objektom u BP. Veza korisnika, prava, operacija i objekata definisana je uređenim četvorkama DKP A.3.1(korisnik; sistemska privilegija; za operaciju; na objektu; admin), DKP A.3.2(korisnik; grupa privilegija; za operaciju; na objektu; admin), DKP A.3.3(korisnik; privilegija nad objektom; za operaciju; na objektu; grant) .

Logički indikatori *admin* i *grant* služe da se naglasi da li je korisniku dato pravo za prenos ovlaštenja drugom korisniku ili grupi ovlaštenja. Kasnije oduzimanje dodeljenih ovlaštenja se može različito interpretirati, sa ili bez kaskadnog oduzimanja prenesenih ovlaštenja. Uobičajeno je da za sistemska ovlaštenja i za grupe ovlaštenja nema kaskadnog oduzimanja ovlaštenja, dok za ovlaštenja nad objektima primenimo kaskadno oduzimanje ovlaštenja [3]. Moguće je i u drugom slučaju da se izbegnu kaskadna oduzimanja ovlaštenja [2]. S obzirom da indikatori *admin* i *grant* imaju ekskluzivno logičku vrednost true ($\top$) ili false ($\bot$) možemo zanemariti njihovo prisustvo u daljoj analizi kardinalnosti skupa evidencija za DKP sistem autorizacije jer predstavljaju dodatni atribut, a ne deo ključa u relacijama evidencije DKP ovlaštenja. Nemaju uticaj na kardinalnost skupova pojavljivanja u DKP evidencijama. Primeri opisa evidencije ovlaštenja relacijama tipa DKP A.3: (’ADMIN1’, ’CREATE SESSION’, ’CREATE SESSION’, ’SYSTEM’, true), (’USER1’, ’INSERT’, ’INSERT’, ’VLASNIK.RADNIK’, true).

Potrebno je jasno razdvojiti *autorizaciju* (definisanje ovlaštenja, privilegije) od *kontrole pristupa* u sistemu. Kontrola pristupa podrazumeva proveru posedovanja ovlaštenja u odnosu na započetu operaciju. Dodela ovlaštenja je odvojena od kontrole pristupa i podrazumeva aspekt upravljanja evidencijama ovlaštenja. Četvorkama tipa A.3 je mapirana evidencija dodeljenih ovlaštenja pre nego nastupi, u fazi pripreme za izvršenje (slika 1), provera posedovanja ovlaštenja za izvršenje operacije u sistemu ili operacije nad objektom u BP. SUBP može da se proširi i na praćenje aktivnosti korisnika (eng. *Audit*). Na slici [9.5] je dat generalizovani model podataka za DKP dobijen sintezom rezultata primene metode inverznog inženjeringa na konkretne sisteme koji podržava implementaciju sistema diskrecione autorizacije sistemskih privilegija i privilegija nad objektima za SUBP. Dobijeni model je opšti za modele podataka u rečniku podataka najpoznatijih SUBP (Oracle, DB2, MS SQL Server, itd). U modelu su sadržani entiteti sa informacijama i međusobnim vezama dovoljnim da se modelira sistem diskrecione kontrole pristupa DKP A.3.1-3 [9]. Kreirani model je opšte rešenje DKP za definisanje i proveru pristupa u BP. Na slici 1 je dato mesto i opisana uloga provere DKP (prva faza) ovlaštenja korisnika po fazama izvršenja upita i dml operacija u BP.

3. APLIKATIVNA KONTROLA PRISTUPA

Da bi se podržala aplikativna autorizacija u programskom sistemu, mora se realizovati specifičan podsistem autorizacije tih aplikativnih funkcija koji može biti deo nekog šireg administrativnog podsistema. U toj aplikativnoj autorizaciji treba u modelu programskog sistema dinamički održavati dozvole nad modulima sistema koji mogu biti aplikativni moduli, izveštaji, grafici, veb moduli, veb servisi i drugi. Ova specifikacija dozvola je iznad nivoa objekata baze podataka, na nivou poslovnih aktivnosti i može poslužiti za dinamičko kreiranje menija ili aktiviranje i deaktiviranje dozvoljenih

poslovnih aktivnosti za pristup pojedinim aplikacijama. Aplikativna autorizacija utiče samo na dozvole za pojedine module, odnosno njima vođene transakcije, nikako na pojedine operacije nultog nivoa u bazi podataka. Aplikativna kontrola pristupa (AKP) je moguća na sledećim nivoima: (AKP A.1) (korisnik sistema ili grupa korisnika, dodeljeno pravo nad modulom), (AKP A.2) (korisnik sistema ili grupa korisnika, dodeljeno pravo nad grupom modula) i ova autorizacija omogućava semantičku autorizaciju prava korisnika nad modulima u kontekstu konkretnog programskog rešenja i primene. Na slici [9.6] dat je model podataka za implementaciju AKP autorizacije i kontrole pristupa. Složenost implementacije ovog tipa autorizacije zavisi i od razvojnog okruženja i arhitekture programskog sistema.

Kada kombinujemo ova dva tipa autorizacije rezultujuća autorizacija je minimalno 7D autorizacija, dimenzije koja modelira Dekartov proizvod ovih dveju pojedinačnih autorizacija. Zaključujemo da je autorizacija i kontrola pristupa u bazi podataka i informacionom sistemu realizovana minimalno kao ISKP = DKP x AKP i definisana je 7D diskrecionim prostorom autorizacije (definisanih privilegija).

4. RESTRIKTIVNA KONTROLA PRISTUPA

Restriktivna kontrola pristupa ili autorizacija pristupa pojedinačnim podacima u BP podrazumeva mehanizme autorizivanja (davanja prava) korisnika za pristup pojedinačnim pojavljivanjima i mehanizme kontrole tih prava pri izvršenju upita i dml operacija ako korisnik prethodno ima odgovarajuće DKP ovlaštenje. Ostaju otvorena praktična pitanja koja nisu rešena DKP autorizacijom, niti bilo kojom drugom,za pristup podacima. Da li možemo kontrolisati pristup podacima unutar kolekcije podataka istog tipa ili klase, odnosno da li je moguće izvršiti granulaciju dozvola za pristup unutar kolekcija objekata za one korisnike koji ispunjavaju 7D model autorizacije ISKP? Ako bi bilo moguće izvršiti granulaciju ovlaštenja nad pojavljivanjima po modelu diskrecione evidencije ovlaštenja za korisnika nad pojavljivanjima, da li je moguće definisati minimalni semantički ekvivalentan (kompletan) model ovlaštenja korisnika nad pojavljivanjima, optimalan po pitanju performansi operacija u bazi podataka, fleksibilan po broju komponenti definisanih ovlaštenja i proširiv na druge tipove baza podataka? Da li smo sa ISKP modelom zaštite zaštićeni od neovlaštenog uvida i manipulacije podacima od strane SUPER korisnika sistema koji imaju visoka sistemska ovlaštenja u bazi podataka i SUBP? Ako nismo, može li se postići zaštita od SUPER korisnika pomoću novog modela granulacije ovlaštenja nad pojavljivanjima? Praktične primene IS u kojima nije prihvatljivo da svi korisnici vide sva pojavljivanja nisu retke. Prethodna pitanja otvaraju nova koja se tiču implementacije rešenja za autorizaciju pojavljivanja. Kako postići autorizaciju do na nivo pojavljivanja, da implementacija bude funkcionalna i lako upotrebljiva, prihvatljivog uticaja na pad performansi SUBP?

5. PARCIJALNO REŠAVANJE RKP

Moguće rešenje za RKP se vidi u individualnom dorađivanju sistema, partikularnom dorađivanju modela podataka i upotrebi dodatih predikata u WHERE uslovima svih upita, odnosno UPDATE i DELETE operacija za konkretan podsistem. Možemo, za samu implementaciju tih proširenja, značajno situaciju popraviti upotrebom pogleda u bazi podataka (VIEWs) za kontrolu pristupa atributima i podskupovima pojavljivanja baznih tabela, kao i sinonima (SYNONYMs) da obezbede transparentnost pristupa u aplikacijama, u odnosu na shemu objekata. U tom slučaju pogledi i sinonimi bi zamenili originalne nazive i reference na tabele. Da bismo zaštitili originalne tabele, korisnicima dajemo potrebne DKP privilegije nad pogledima, a zabranjujemo pristup originalnim tabelama. Ostaje pitanje zamene imena objekata, ukoliko nismo predvideli rad sa sinonimima. Problem se usložnjava najmanje linearno, u praksi i eksponencijalno, sa povećanjem obima sistema. Sve tabele dobijaju nove atribute što nije povoljno za upite koji nisu pisani sa preciznim navođenjem atributa i izraza u rezultujućoj listi. To je komplikovan zadatak u već razvijenim sistemima kada se ta vrsta autorizacije postavi kao zahtev od strane korisnika što nije redak slučaj. Potrebno je prepravljati celu aplikaciju, često na nesistematičan način. To je moguće realizovati proširenjem tekućeg modela podataka aplikacije za potrebe novih funkcionalnosti, ali i doradama postojećih aplikacija. Ono što je minimalno potrebno uraditi jeste doraditi WHERE uslove svih SELECT, UPDATE i DELETE operacija ali i definisati semantiku dorada INSERT operacija nad tim atributima ili preko bočnih efekata trigerima i podrazumevanim vrednostima.

Rešavanje RKP pomoću pogleda je aplikativno zavisno od primene i zahteva niz dodatnih uslova da bi zadovoljilo minimum uslova bezbednosti. Pošto to nije moguće postići u opštem slučaju (SYNONYMS, uklanjanje pomoćnih alata i SUPER korisnici imaju pristup) postoji niz otvorenih pitanja i potrebnih preciznih intervencija da bi se implementirao kontekstno zavisan parcijalni sistem RKP [9.2.2]. Tako rešen sistem ima niz nedostataka za postojeće aplikacije i stabilnost rešenja tako da prednost ovom načinu rešavanja dajemo ako je potrebno postići ovaj tip autorizacije na brz i efikasan način, za kratko vreme početka primene, dok se ne obezbedi sistematično rešenje.

6. DISKRECIONA RESTRIKTIVNA AUTORIZACIJA I RAZVOJ MODELA

Sistematično rešavanje RKP podrazumeva analizu skupa intervencija za primenu parcijalnog rešenja i liste nedostataka. Dolazi se do skupa zahteva koje treba da zadovolji kompletno sistematično rešenje [9.3].

Definicije pojma kompetnog sistema RKP počivaju na istraživanju kompletnog sistema autorizacije pojavljivanja koji je komplementaran DKP autorizaciji. Diskreciona restriktivna autorizacija definisana je operacijom spajanja relacione algebre

$$DRA = DKPA3 \otimes RAA\ [dkpa3.korisnik=raa.korisnik\ and\ dkpa3.objekat=raa.objekat\ and\ dkpa3.operacija=raa.operacija]$$

gde je RAA relacija koja opisuje skup četvorki kojima se evidentira skup datih prava korisniku za operaciju nad pojavljivanjima. Dobijena relacija ima dimenziju 5 (5D) i

teorijski je kompletan model za opisivanje restriktivne autorizacije. Svi modeli koji u radu nastaju evolucijom i koji su ekvivalentni DRA modelu nazivaju se R-kompletni modeli. Svi upiti i dml operacije nad objektom bi se transformisali u nove kojima su dodati predikati za restrikciju (filtriranje skupa pojavljivanja nad kolekcijom pojavljivanja objekta koji učestvuje u upitu ili nad kojim se izvršava operacija). Predikati se dodaju manuelno ili automatski u uslove restrikcije koji dodefinišu uslov filtriranja za vidljivost samo onih pojavljivanja na koja korisnik ima dozvolu (Tabela 9.5). Ovde izdvajamo samo jedan fragment koji opisuje transformisani upit za SELECT, a ekvivalentno je za DML operacije:

```
(SELECT <izraz1> [<alias1> ], <izraz2> [<alias2> ], ....
 FROM <tabela> [<t1> ], ....|
        <pogled> [<p1> ],.... |
        <podupit> [<p1> ],....
        <Objekat> [ o1 ]
WHERE [<uslovi predikata>....]
[AND] o1.<IDPOJ#> IN (SELECT <IDPOJ#>
                      FROM RA_A_EVIDENCIJA_ZA_Objekat
                      WHERE USER#    =getUserId(USER)
                      AND OBJECT#    =getObjectId('Objekat')
                      AND OPERZATIP# in ('SELECT','ALL') )
[GROUP BY .....]).
```

Transparentnost može da se postigne automatizmom dodavanja predikata svakoj SELECT, UPDATE, INSERT i DELETE operaciji nad baznim kolekcijama pojavljivanja (tabele u RSUBP). Potrebno je zapisati ih u bazi kako bi semantika provere dozvole na pojavljivanju ostala evidentirana i poznata samoj bazi podataka. Proširujemo DRA model relacijama koje dozvoljavaju evidenciju predikata.To je moguće ako se čuva u nekoj prevedenoj funkciji tekstualnog tipa, što bi značilo da se uvede relacija DRAFILTER(objekat;zaoperaciju;pointer dajPredikatZaFilterFunkcija) dok bi se funkcija *dajPredikatZaFilterFunkcija* čuvala već prevedena i proverena u rečniku podataka baze. Novi mehanizam DRA autorizacije podrazumeva sledeće dorade u BP:

- Izgradnju kompletnog DRA proširenja modela BP;
- Pripremu predikata koji se „priključuju" postojećim predikatima u upitima i dml operacijama;
- Evidenciju predikata koji će se automatski dodavati operacijama nultog nivoa za koje su definisani;
- Aktivaciju mehanizma „pripajanja" predikata u fazi pripreme za izvršenje upita i dml operacija;
- Optimizaciju modela i „pripajanja" kako bi uticaj na pad performansi u fazi pripreme i kasnijeg izvršenja upita i dml operacija bio minimalan.

Potrebno je razdvojiti DKP i DRA na nivou modela podataka. Provera DKP i DRA autorizacije se odvija u različitim fazama izvršenja upita, odnosno dml operacija [9.2.3].

Slika 1: Tri koraka procesa izvršenja upita i dml operacija

DRA model jeste kompletan za evidenciju prava korisnika za pojavljivanja i operacije ali nije dobar za realizaciju zbog niza manipulativnih i nedostataka u performansama. Uočimo da je *kard*(DRA) = *kard*(DKP) * *kard*(pojavljivanjazasvakiobjekat). U tom skupu definisanih DRA pojavljivanja, svaki korisnik A u odnosu na svaku moguću operaciju ima poseban skup pojavljivanja (*PA*) koji je podskup ovog DRA 5-dimenzionog diskretnog prostora. Mora se naći način da ovaj 5D model, nastao agregacijom DKPA3 i pojavljivanja instanci objekta u tabelama, možemo pojednostaviti na 4D DKPA3 model proširen *tipom podskupa pojavljivanja* instanci objekta u kolekciji čija će kardinalnost evidencije biti *kard*(DRA) = *kard*(DKP) + *kard*(pojavljivanjazasvakiobjekat) što je značajno manje (zbir) u odnosu na prethodni. Preporučljivo je razdvojiti DKP i restriktivnu autorizaciju na nivou modela podataka, odnosno ukloniti egzistencijalnu zavisnost evidencije dozvoljene vidljivosti korisnicima nad pojavljivanjima od DKP. PA_1, PA_2 ....PA_n skupovi pojavljivanja mogu biti vezani za pojedinačne korisnike i operacije, a u praksi je poželjno da imamo vezanost skupova pojavljivanja za tipove korisnika i operacije ili skupove operacija. To smanjuje kardinalnost i organizuje kompleksnost DRA evidencije. U praktičnim primenama stvarni odnosi korisnika ili tipova korisnika su korelisani:

- *Ekvivaletnom* organizacionom podelom, gde su ovlaštenja identična,
- *Hijerarhijom*, gde nadtip može da radi više od podtipa korisnika,
- *Disjunktnom* organizacionom podelom, gde su ovlaštenja disjunktna,
- *Dvostrukom diskrecionom podelom*, koja znači kombinaciju hijerarhije i podele na disjunktne skupove na istim nivoima hijerarhije,
- *Kombinovanim* korelisanim odnosima što diskrecionom DRA autorizacijom nije moguće modelovati.

Podskupovi pojavljivanja PA_1, PA_2 ....PA_n pridruženi korisnicima ili tipovima korisnika elementi *partitivnog skupa* svih pojavljivanja kolekcije. Oni mogu biti u proizvoljnoj korelaciji ali i da važi pravilo jedinstvenosti korelacije. Ako nad tipovima korisnika za pridružene skupove dozvoljenih pojavljivanja važi jedinstvena korelacija, kažemo da su tipovi korisnika u *dominantnoj korelaciji na skupu svih pojavljivanja*. Zavisno od dominantne korelacije imamo i tipove korisnika u odnosu na pojavljivanja jednog objekta i operacija nad njim. Ako imamo samo jednog korisnika sa jednim korelisanim skupom pojavljivanja, onda iz tog jednog korisnika izvodimo tip korisnika. Dominantna korelisanost može biti: *Dominantna jednakost, Dominantna inkluzija, Dominantna disjunktnost, Kombinovana dominantnost odnosa i nedominantan korelisani odnos.* Ako ne postoji dominantan korelisani odnos ili obavezan korelisani odnos kažemo da važi *nedominantan korelisani odnos* između podskupova pojavljivanja, po tipovima korisnika za operaciju, što je slučaj sa DRA. U praksi je odnos između tipova korisnika korelisan te moramo unaprediti model RA. Otvoreno je pitanje kako modelovati restriktivnu autorizaciju da se postigne prethodna

složenost, a da se pri tome modeluju ostali odnosi korisnika prema podskupovima pojavljivanja na koje imaju dozvole, odnosno da otklonimo nedostatke DRA. Sistematizovali smo zahteve za novim modelom restriktivne autorizacije i u tri etape sazrevanja izgradili model restriktivne autorizacije koji je R-kompletan. U radu [9] je kompletno prikazana sa svim analizama evolucija modela MRA A, preko MRA B u 7D model MRA C. Za uspešnu evoluciju DRA modela u MRA C otklanjajući probleme višeznačne zavisnosti i spregnutost DKP u DRA sa evidencijom ovlašćenja pojavljivanja, uveli smo pojmove *vidljivost pojavljivanja* i *dozvoljena vidljivost korisnika* i operaciju *MozeVideti.* Primer operacije dajemo za model MRA B. Operacija je (MRA MV B):

$$\text{Dozvoljenavidljivost}(\text{Korisnik};\text{Objekat};\text{Zaoperaciju}) \otimes \text{Vidljivost}(\text{Objekat};\text{zapojavljivanje}) = \text{true}(\text{T}) .$$

Istraživanjem se došlo do pojma *obelezjeRA* i *SistemRA* kojim se organizuju grupe obeležja za konkretnu aplikativnu primenu. Obeležja su trojke koje se mogu dodeljivati korisnicima, ali i pojedinačnim podacima. Korisnik može da pristupi pojavljivanju iz kolekcije podataka ako prethodna operacija daje pozitivan rezultat.
U radu je formulisana i precizno formalno dokazana *teorema* i *posledica o restriktivnoj kompletnosti* izgrađenih modela restriktivne autorizacije. Time je potvrđena valjanost i izražajnost izgrađenih modela i dat formalni okvir za dalje unapređenje modela MRA C i operacija MV C. Kompletan model je dat prikazima [9.12-9.16] sa opisom i tumačenjem.

7. MRA C SISTEM RESTRIKTIVNE AUTORIZACIJE

Kreirani model MRA C za RA jeste R-kompletan i uveo je pojam *ImenovanisistemRA, ili aplikativni sistemRA* kojim se naglašava namena određenog skupa obeležja pridruženih toj primeni. Moguće je da u bazi bude istovremeno više primenjenih aplikativnih sistema za RA. Opisana je realizacija koja podrazumeva da korisnik ima pristup nekom obeležju ako operacija *MozeVideti* daje pozitivan rezultat za sve primenjene aktivne ISRA, a ne samo jedan. Model MRA C dozvoljava da se evidentiraju prava korisnika odvojeno od DKP prava korisnika te je održavanje takvih odvojenih skupova olakšano. Da bi podsistem za RA funkcionisao u SUBP, mora pored R-kompletnog modela [9.15] u kojem se čuvaju podaci o datim pravima za implicitno generisanje predikata u upitima, biti realizovano nekoliko dodatnih aspekata kompletnog podsistema RA kao i za DRA sistem. Ti aspekti su sastavni delovi dorade SUBP i baze podataka. Kada se kompletira model koristi se specijalizovan upit za dobijanje skupa svih vidljivih pojavljivanja za datog korisnika koji je optimizovan i brz za izvršenje. Ako želimo nakon kreiranja modela da aktiviramo sistem RKP trebamo ubacivanje filtera u tabelu koja čuva predikate za automatsko dodavanje. Osnovni upit koji vraća sva vidljiva pojavljivanja je poseban za SELECT i DML operacije, nad posmatranim objektom baze, realizovan je pomoću IN operatora. Za kreiranje evidencije predikata koristimo proceduru *Evidentiraj_auto_predikat(objekat, zaoperaciju, PredikatZaFilter)* koja kreira funkciju kompajliranu sa zaštićenim kodom za izvršenje upita koja se čuva u bazi za kasniju upotrebu pri dodavanju predikata. Za evidenciju predikata koristimo relaciju *MRA_C_FILTER(objekat; zaoperaciju; pointer dajPredikatZaFilterFunkcija).* Automatsko „pridruživanje" definisanih predikata u već postojeći predikat upita i dml operacija se realizuje unutar samog SUBP pomoću ugrađenog mehanizma ili otvorenog kôda. Dobijeni efekat je transparentnost izmena prema svim korisnicima, upitima, dml operacijama i aplikacijama. Performanse MRA C sistema restriktivne autorizacije je moguće dodatno optimizovati koristeći razrađene mehanizme rešenja MRA C.

8. PRAKTIČNO REŠAVANJE RKP

U radu su analizirana postojeća rešenja u aktuelnim sistemima za upravljanje bazama podataka koristeći se MRA C dekompozicijom sistema restriktivne autorizacije. Izloženo je jedno sopstveno partikularno rešenje restriktivne autorizacije i rešenja u komercijalnim sistemima za upravljanje bazama podataka Oracle, IBM DB2 i IDS, Microsoft SQL Server. Svako rešavanje RKP praktično podrazumeva realizaciju svih aspekata MRA.

9. JEDNO SOPSTVENO PARTIKULARNO REŠENJE

Scenarij jedne poslovne situacije za primenu restriktivne autorizacije: Na zahtev predstavnika korisnika treba da se u podsistemima KADROVI i ZARADE obezbedi potpuna zaštita podataka, kojim mogu pristupiti rukovodioci, od neovlaštenog uvida ostalih korisnika sistema. U sistemu je zamišljeno da postoje inicijalno 4 kategorije korisnika koji mogu da vide, u skladu sa dodeljenim nivoom, podatke za koje su ovlašteni. Ti nivoi su TOP SECRET, SECRET, CONFIDENTIAL i PUBLIC za dozvoljenu vidljivost korisnika kao i za nivoe vidljivosti kritičnih pojavljivanja podataka. Korisnicima kojima nije dodeljeno pravo ili podacima kojima nije definisan nivo vidljivosti podrazumevat će se najniži (za sada PUBLIC) nivo. U sličnim situacijama može se uzeti da podatak nije vidljiv niti na jednom nivou dok mu se eksplicitno ne definiše, kao i za korisnika da ne vidi niti jedan podatak dok mu se ne dodeli dozvoljeni nivo vidljivosti. Privilegovanim korisnicima se dodeljuju nivoi CONFIDENTIAL, SECRET i TOP SECRET tako da se povećava nivo privilegija od najnižeg (za sada PUBLIC) do TOP SECRET. Da bi se postigla fleksibilnost sistema, moguće je povećati broj nivoa hijerarhije i uvesti dodatne nivoe PUBLIC2, PUBLIC3,....,PUBLICn. Kako bi se zadržao redosled definisan hijerarhijom, uvodimo numeraciju simboličkih imena nivoa obrnutim redosledom (Tabela 1).

Tabela 1 - Nivoi vidljivosti i ovlaštenja

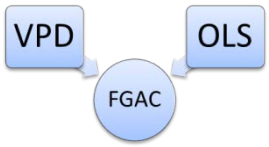
Nivo vidljivosti	Numerička vrednost
TOP SECRET	0
SECRET	1
CONFIDENTIAL	2
PUBLIC	3
PUBLIC2	4
PUBLIC3	5
...	
PUBLICn	3+(n-1)

Primetimo da su viši nivoi vidljivosti identifikovani manjim vrednostima. To nam omogućava da se niži nivoi hijerarhije mogu dodatno rasčlanjivati, odnosno dobijamo

mogućnost za modeliranje hijerarhije po principu *odozgo-nadole* (eng. *top-down*). Ova numeracija daje fleksibilnost broju nivoa, a kod poređenja dva nivoa ovlaštenja zahteva da se koristi obrnuta nejednakost. Dakle, jedan nivo je iznad drugog ako je numerička vrednost prvog manja od numeričke vrednosti drugog nivoa. Pravilo po kojem se određuje vidljivost podataka je definisano na sledeći način: *Korisnik sistema „može videti“ podatke ukoliko je njemu dodeljeni dozvoljeni nivo VEĆI ILI JEDNAK dodeljenom nivou vidljivosti podataka.* Ako govorimo o poređenju numeričkih vrednosti nivoa, onda formulacija glasi: *Korisnik sistema „može videti“ podatke ukoliko je numerička vrednost njemu dodeljenog dozvoljenog nivoa NUMERIČKI MANJA ILI JEDNAKA(<=) numeričkoj vrednosti dodeljenog nivoa vidljivosti podataka.* Možemo ovo proširiti, ukoliko odgovara potrebama: *Korisnik kome nije dodeljen dozvoljeni nivo vidljivosti ne može videti niti jedan podatak (ili tumačiti kao da ima num(PUBLICn)+1 dozvoljeni nivo). Podatak kome nije dodeljena vidljivost nije vidljiv dok mu se ne definiše vidljivost (tumačiti kao da ima num(TOP SECRET)-1 dodeljenu vidljivost).*
Informacije o nivoima vidljivosti podataka se čuvaju u dodatim atributima kritičnih tabela za čuvanje informacija o kadrovima i njihovim osnovnim ili obračunatim vrednostima za izvođenje zarade radnika, odnosno koeficijenata zarada radnika. Podaci o dodeljenim pravima korisnika se čuvaju u posebnoj bazi autorizovanih korisnika koja je kriptovana internim algoritmom. Mehanizam provere prava i vidljivosti podataka je realizovan automatskom transparentnom nadogradnjom prve faze pripreme upita i dml operacija za izvršenje. Stoga alogoritmi za izvršavanje upita i dml operacija uzimaju u obzir prava korisnika i dodeljene nivoe vidljivosti podataka kroz pridružene algoritme. Ovim se obezbeđuje da *korisnici mogu da čitaju, ažuriraju i unose nove podatke ako i samo ako imaju dodeljeno dozvoljeno pravo veće ili jednako pravu vidljivosti čitanih, ažuriranih ili novokreiranih podataka*. Ako numerički izražavamo *„mogu da čitaju, ažuriraju i unose“* onda ćemo obrnuti operaciju poređenja i formulišemo *„akko imaju num(dodeljeno dozvoljeno pravo) <= num(pravo vidljivosti podataka)“*. Detaljan opis implementacije sa svim opisima kreiranja inicijalne baze od jednog korisnika sa ADMIN pravima i dodavanje novih korisnika je u [18.3.2]. Sadrži model podataka proširenja za partikularno rešenje, pomoćne funkcionalnosti za sistem, zaštitu modela od napada i izmena, predikati koji se generišu za transparentno umetanje u upite i operacije, automatizam priključenja predikata i mehanizme za poboljšanje performansi. Na kraju je izložena analiza nedostataka u odnosu na teorijski model MRA C i prednosti korisne za poboljšanje MRA C sistema.

10. ORACLE REŠENJE ZA RKP

Ovo rešenje je diskutovano u svom osnovnom obliku u [10], a u [9] je detaljno analizirana novija verzija i data uporedna analiza prema teorijskom modelu MRA C. Dajemo pregled kako se u Oracle SUBP implementira i koristi *Oracle Label Security* (OLS) opcija koja se instalira kao dodatna opcija u *Oracle Enterprise* verziji. Moguće je pri kreiranju baze ili u već kreiranoj bazi dodati OLS opciju (DBCA ili konfiguracioni skriptovi [6]). Rešenje OLS u Oracle SUBP počiva na mehanizmu FGAC (*Fine Grained Access Control*) i VPD (*Virtual Private Database*) koji je proširenje FGAC-a. OLS je rešenje koje ima svoj model restriktivne autorizacije i koristi FGAC i VPD kao mehanizam za automatizaciju transparentnosti predikata u operacijama i upitima. VPD je mehanizam autorizacije predikatima koji treba da budu eksplicitno ali slobodno definisani. Razlika je što VPD preporučuje kreiranje predikata na osnovu postojećih atributa u tabelama dok je OLS konačan zaseban i kompletan sistem za realizaciju restriktivne autorizacije nezavisan od atributa u tebelama nastao proširivanjem osnovnog modela podataka nekog aplikativnog konteksta.



Slika 2: Zavisnost OLS i VPD od FGAC funkcionalnosti

U radu je dat kompletan relacioni ERD model za VPD, FGAC i OLS generisan metodom reverznog inženjeringa. Na koncu poglavlja za Oracle rešenje rezimirane su osobine i funkcionalnosti OLS rešenja primenjiva za unapređenje MRA C sistema, ali i sličnosti OLS sa MRA C sistemom. OLS rešenje primenjivo je samo u Oracle bazi podataka.

11. IBM DB2 i INFORMIX LBAC REŠENJE

U SUBP DB2 [2] realizovan je sistem za podršku realizacije restriktivne autorizacije pojavljivanja u tabelama i kolona u tabelama. Specifičnost DB2 rešenja za RA je što je to potpuno zatvoren sistem spreman za upotrebu sa specifičnim dodatno razvijenim DCL jezikom za manipulaciju RA privilegijama. Rad sa LBAC sistemom podrazumeva poznavanje skupa i ponašanja komandi dijalekta DCL jezika. DB2 sistem ne otkriva arhitekturu rešenja mehanizma transaprentnog automatizma za primenu predikata, kao što je izloženo za FGAC i OLS u Oracle. LBAC omogućava realizaciju restriktivne autorizacije na drugačiji način nego OLS u Oracle-u. Sve objekte vezane za DB2 LBAC definiše korisnik koji ima minimalno SECADM sistemsku autorizaciju. Osnovni pojam su *LBAC komponente* koje služe da se opišu kriterijumi za složene mehanizme pristupa tabelama. Komponente koje imamo na raspolaganju su tipa ARRAY, SET i TREE kojima se opisuju kriterijumi autorizacije po uređenom nizu, odnosno nivoima, skupovne podele podataka i podela podataka prema pripadnosti nekoj hijerarhiji. Po kreiranju komponenti moguće je kreirati *LBAC polise* koje služe kao imenovani sistemi RA za definisanje kombinacije LBAC komponenti u složeni sistem kriterijuma za opisivanje dozvola i ovlaštenja pristupa podacima i atributima podataka. U DB2 bazi može postojati više polisa i sa jednom polisom je moguće zaštititi više tabela. Jedna tabela može biti zaštićena najviše jednom LBAC polisom bezbednosti. Polisama je opisana moguća kombinacija do 16 različitih komponenti čije ćemo elemente navoditi u labelama. *LBAC labela* je objekat koji se definiše za polisu kao partikularna kombinacija elemenata komponenti definisanih za polisu pri njenom kreiranju. Labele služe za opisivanju složenih ovlaštenja

korisnicima za pristup podacima za čitanje i izmene, odnosno za definisanje zaštite pojavljivanjima i kolonama u tabeli. Pomoću nje možemo kombinovati ovlaštenja prema nivoima, radu u odelenjima ili hijerarhiji grupa korisnika i organizacionih celina. Nakon primene polise na tabelu, labele mogu da se dodeljuju pojavljivanjima u tabeli, odnosno kolonama. Korisnicima se dodeljuju labele čime se definišu ovlaštenja za čitanje, odnosno izmene pojavljivanja i kolona u tabelama. Za jednu polisu, korisnik, rola ili grupa može imati najviše jednu labelu za čitanje i jednu za operacije upisa. Moguće je da korisnik ili rola poseduje ovlaštenja za više LBAC polisa bezbednosti. Ako korisnik ima ovlaštenja da čita pojavljivanja, za izmene i brisanje je potrebno da ima ovlaštenja i za upis i nad pojavljivanjima i nad svim kolonama nad kojim je definisana zaštita. Dodelom izuzetaka za primenu LBAC pravila korisnicima (eng. exemptions), rolama i grupama za polisu, isključuje se primena nekih delova LBAC pravila za kriterijume upoređivanja labela nad pojavljivanjima i kolonama i labela korisnika, rola ili grupe. Imamo kontrolu pristupa i nad kolonama koristeći LBAC labele. Zahtev za pristup kolonama za koje korisnik nema odgovarajuća ovlaštenja prekida upit, odnosno operaciju. Pojavljivanja za koja korisnik nema dovoljna ovlaštenja ne ulaze u rezultate upita. To važi i za dml operacije kao i za agregatne funkcije. U pogledima nad zaštićenim tabelama se takođe primenjuje LBAC zaštita. Primena LBAC zaštite nad pojavljivanjima se obezbeđuje uvođenjem kolone tipa DB2SECURITYLABEL i ažuriranjem vrednosti na labele polise primenjene na tabelu. Primena labela nad kolonama završava se evidencijom informacija u rečniku podataka zajedno sa definicijom tabele i kolona. I za ovo rešenje urađen je reverzni inženjering i objašnjen skriveni mehanizam transparentnosti za predikate, detaljan postupak primene LBAC RA, ERD model podataka. Mehanizam izračunavanja vidljivosti je posebno objašnjen kao i opasnosti od zaobilaženja LBAC polisa. Na koncu poglavlja za LBAC rešenje rezimirane su osobine i funkcionalnosti rešenja primenjiva za unapređenje MRA C sistema i sličnosti sa MRA C.

12. MICROSOFT SQL SERVER REŠENJE

Analizirali smo SQL Server 2000, 2005, 2008 i 2012 u kontekstu zaštite sistema i specijalno mehanizma restriktivne autorizacije (MLS – eng. *Multi Level Security*). U SQL Server ne postoji kompletno sistematizovano rešenje mehenizma restriktivne autorizacije ali se nudi parcijalno rešenje za restriktivnu autorizaciju i autorizaciju pristupa kolonama ([5]) zasnovano na sličnom konceptu koji smo izložili u sekciji rada o parcijalnom rešenju restriktivne autorizacije. Iako elegantno rešenje u osnovi, ono ima niz nedostataka koja ga ograničavaju za primenu u praksi i u postojećim aplikacijama [9].

13. ZAKLJUČAK - REZULTATI ISTRAŽIVANJA

Izgradnjom MRA C sistema moguće je govoriti o autorizaciji na nivou pojavljivanja relacione tabele, odnosno kolekcije instanci objekata u objektnom sistemu. Izgrađen je opšti teorijski okvir za bavljenje problemom restriktivne autorizacije kroz modele DRA, pojam R-kompletnosti i vezane pojmove, odnosno unapređeni model MRA C i aspekti kompletnog sistema. Kroz jedno partikularno rešenje i izložena komercijalna rešenja sa kompletnom analizom u odnosu na MRA C izgrađen je skup zahteva za opšti model. Ako je potrebno realizovati, za specijalne namene, jednostavan i efikasan sistem RA u BP je ponuditi razvijeno i provereno partikularno rešenje za restriktivnu autorizaciju nivovskog tipa. Pored sopstvenog teorijskog modela MRA C za RA koji sistematizovano proširuje diskrecionu kontrolu pristupa i diskrecionu restriktivnu autorizaciju u jedan restriktivno kompletan model, urađene su analize za Oracle OLS, IBM LBAC i SQL Server rešenja za njihovu delimičnu realizaciju R-kompletnog rešenja. Konstatujemo da IBM rešenja imaju elegantniji deklarativni jezik za definisanje LBAC autorizacije, dok Oracle ima vrlo funkcionalan API i grafičke alate za manipulaciju komponentama „vidljivosti“ (labelama) podataka i ovlaštenjima korisnika. Kao rezultat rada napravljena je realizacija opšteg rešenja RKP u RSUBP i proširenim sistemima. Radni naziv tog rešenja je EMRA (eng. Extended model for restrictive authorisation). Izrada opšteg rešenja je korak napred u sistematizaciji pitanja restriktivne autorizacije u bazama podataka [9]. Pitanje restriktivne autorizacije ima smisla proširiti sa relacionog na prošireni relacioni i OO model, odnosno relacije i n-torke relacionog modela zameniti kolekcijama pojavljivanja i pojedinačnim pojavljivanjima instanci objekata OO modela. Slično je i za XML baze podataka.

LITERATURA

[1] Heinz Axel Pürner, *„Label security in DB2 und Oracle”*, IT Focus, 2007.

[2] *„Label-Based Acces Control (LBAC) in DB2“*, IBM DB2 Version 9.5 Information Center for Linux, UNIX, and Windows, IBM, 2008.

[3] *„Oracle Label Security Administrator’s Guide”*, Oracle Documentation, Oracle 10gR2, Oracle Corporation

[4] Mladen Vidić, *„FIS Advanced Security“*, FIS Tehnička dokumentacija, Digit Beograd i Telekom Srbije, 2002.

[5] A.R., D.R., B.N., *“Implementing Row- and Cell-Level Security in Classified Databases Using SQL Server 2005“*, Microsoft TechNet, 2005.

[6] *„Label-Based Acces Control(LBAC) in Informix Dynamic Server“*, IBM IDS Version 11.10 Information Center, IBM, 2008.

[7] *„Security and protection in SQL Server 2008 database Engine”*, SQL Server 2008 Books Online, Microsoft Corporation

[8] *„Security in MySQL Database“*, MySQL Documentation Reference Manual Version 5.1, 5.4, 5.5 and 6.0, MySQL AB and Sun Microsystems, 2009.

[9] Mladen Vidić, *Restriktivna autorizacija u bazama podataka, Magistarski rad,* Matematički fakultet, Beograd,2010.

[10] Mladen Vidić, *„Restriktivna autorizacija u bazama podataka“*, Zbornik radova Infofest 2007, Budva, 2007

[11] Mladen Vidić, *„Podsistem restriktivne autorizacije IBM DB2 LBAC prema teorijskom modelu sistema MRA“*, Zbornik radova Infofest 2011, Budva, 2011.

PREVARE I FOREZNIKA

FRAUD AND FORENSICS

GORDANA VUKELIĆ[1]

Beogradska bankarska akademija, fakultet za bankarstvo, osiguranje i finanasije, Beograd

Rezime: *Računovodstvena dokumenta su izveštaji koji pokazuju stanje o imovinskom, finansijskom položaju i o uspešnosti poslovanja. Manipulisanje u evidentiranju, podrazumeva fiktivnu i nepravilnu obradu podataka, sa namerom da se prikrije prava slika o stanju sredstava, izvorima sredstava ili poslovnom rezultatu. Zloupotrebom zakonskih propisa se stvara slika poštovanja, ali se unutar propisa traže načini da se postigne željeni cilj koji se postiže sa manipulacijama koje stvaraju drugačije vrednosti sredstava, troškova i odliva.*

Prevara ima različite oblike, vrste i forme. Ona podrazumeva profitiranje uz pomoć nedozvoljenih radnji, postupaka ili trikova, često uključuje krađu sredstava, informacija i korišćenje imovine bez dozvole. Statistički podaci ukazuju da se 2.9 triliona dolara izgubi svake godine zbog prevara. Forenzičko računovodstveni i revizorski angažmani nisu samo prevare, već su uključeni u komercijalne parnice, a štete se javljaju u milijardama dolara. Pored biznisa, forenzičke računovođe i revizori se angažuju u pravnim postupcima, problemi skrivene imovine pri razvodima, u prevarama pri falsifikatima i drugim radnjama, a u cilju zaštite interesa.

Ključne reči: *računovodstvo, revizija, prevara, prevencija, postupci, manipulacija, foreznika.*

Summary: *Accounting documents and accounting reports are the main evidence of the property and financial position, as well as the business and monetary success of the enterprise. Manipulating in the accounting treatment, involves fictitious or incorrect processing of data in order to disguise the true picture of the source of funds, resources or business results. When the abuse of legal regulations, in which seemingly create an image of respect for rules, in fact, within the regulations seek ways to achieve the desired business goals. The objective is achieved with a number of manipulations that produce different values of assets, expenses and payments.*

Fraud has diffrent shapes, types and forms. Fraud involves profiting with help unauthorized actions, procedures and tricks, often involving theft of resource, information and use assets without permission. Statistical information show that 2.9 trillion dollars lost each year due to fraud. Forensic accounting engagement not include just scams, they also included in commercial litigation, and damage occure in billions of dollars. Besides business, forensic accountants get involved in a legal proceedings, the problems hidden assets in divorce, in falsification fraud and other actions, in order to protect interest.

Key words: *accounting, auditor, fraud, prevention, procedures, manipulation, forensics.*

[1] Rad finansiran sredstvima Ministarstva prosvete, nauke i tehnološkog razvoja, Projekat 43007.

1. UVOD

Prevare i pitanje rizika od prevare ukazuju na nedostatke specijalizovanih znanja i potrebe da osim iskustava internih i eksternih revizora, uključe se računovođe, inspektorati koji prilikom istraga i drugih nedozvoljenih dela, mogu dati mišljenja u vezi sa pravnim, poslovnim i drugim potrebama. Forenzičko računovodstvo treba da sprečava malverzacije u okvirima poslovanja finansijskog sektora i privrednih subjekata. Svaki subjekat mora imati odgovarajući sistem vođenja i upravljanja, koji sprečava i otkriva nastajanje nezakonitih radnji, prevara koje su kriminalne radnje. Potrebno je naglasiti da top menadžment preuzima glavnu odgovornost za istinito i fer finansijsko prezentovanje, pri čemu svakako od velike pomoći mogu biti interna kontrola, interna revizija i računovođe forenzičari.

2. O PREVARAMA

Nema jasne definicije šta je to prevara. Uz pomoć ovoga termina opisuju se postupci kao što su obmane, iznude, krivotvorenje, pronevere, skrivanje materijalnih činjenica. Prevare se uglavnom dešavaju tamo gde su kontrole slabe, odnosno gde se ne primenjuju ili ne postoje. Zbog toga je veoma važno da se u bankama utvrdi stepen internih kontrola, upravo to jačanje kontrola smanjuje mogućnost nastanka prevara. Ako pod prevarama podrazumevaju se „sve vrste kriminalnih radnji“ u finansijama, potom posmatrano sa strane forenzičkih računovođa i revizora prevare se mogu podeliti na sledeće grupe: korupcija, otuđivanje imovine i lažiranje finansijskih izveštaja.

Značajna je razlika između revizije i forenzike, pa u narednoj slici prikazane su aktivnosti obe, a time i tvrdnja da su neophodne u sprečavanju prevara, svaka sa svog stanovišta.

Slika 1: Upoređivanje revizije i forenzike

Za prevare može se reći da ih je veoma teško identifikovati. Moguće rešenje je forenznika ona ne otkriva sve prevare i pronevere, ali povećava nadu da će one tokom vremena biti rasvetljene. Delovanje forenzičara se može posmatrati sa dva aspekta a to su: ***ex-ante*** (podrazumeva odvraćanje od prevara) i ***ex-post*** (nakon sumnje da je prevara nastala ili nakon otkrića same prevare). Poznato je da forenzičari mogu delovati interno i eksterno, pri čemu interno delovanje uključuje istraživanje svih mogućih prevara od strane zaposlenih i menadžera, dok eksterno podrazumeva istraživanje mogućih prevera od strane kupaca, dobavljača, kreditora (banaka). U praksi sve više postoji potreba za sprečavanjem rizika od prevare, bolje je prevaru sprečiti nego rešavati posledice. Ideja o prevari kreće od zaposlenih, a skrivene su u neverodostojnom računovodstvenom izveštavanju i u poslovno–organizacijskom neredu uz neodgovarajući unutrašnji nadzor.

Prilikom formiranja funkcionalnih sistema vođenja i upravljanja, ključna je organizacija ciljnog i decentralizovanog vođenja poslovanja, sa jasnim određenjem sistema. Tako, top menadžment finansijskih institucija treba da se bavi tekućim poslovanjem i razvojem, a ne poslovno - izvršnim zadacima, koji se delegiraju na izvršavanje nižim nivoima menadžmenta. U svakoj finansijskoj instituciji moguće je da se pojavi u manjoj ili većoj meri preduzetnički kriminal i upravo to dovodi do potrebe za postojanjem tj. formiranjem organa za nadzor. Na osnovu ovoga može se zaključiti da je neophodno postojanje interne kontrole, koja razmatra bonitet u samom sistemu poslovanja, i na taj način, utiče na sprečavanje i otkrivanje prevara i drugih kažnjivih dela. Neverodostojni računovodstveni i finansijski izveštaji, proizvod su manipulativnog računovodstva, a za manipulativno (kreativno) računovodstvo može se reći da predstavlja proces u kome računovođe koriste svoje poznavanje računovodstvenih pravila da bi manipulisali ciframa iskazanim u poslovnim računima. Tada dolazi do:

- Maštovite upotrebe računovodstva,
- Korišćenje legalnih mogućnosti izbora fleksibilnih računovodstvenih metoda, postupaka i procena,
- Zloupotreba računovodstvenih procena, metoda i tehnika, sa ciljem što boljeg prikaza finansijskog stanja, uspeha i
- Promena stvarnih finansijskih izveštaja u ono što se želi pokazati.

Kada se govori o lažnim podacima, čija je glavna svrha i cilj lažno prikazivanje ekonomskih okolnosti i uspeha finansijskih institucija, a rezultat su zloupotreba pravnih i drugih profesionalno - etičkih normi, pri njegovim odlukama. Da bi banka otkrila i sprečila kriminalne i druge nedozvoljene radnje mora da ima:

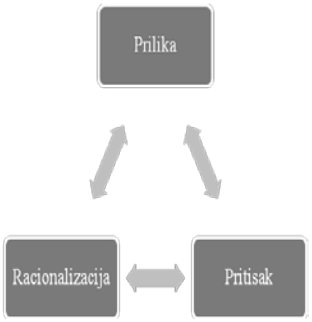
- Profesionalno upravljanje,
- Potporni mehanizmi (kvalitetno izgrađen sistem interne kontrole i interne revizije, a na čelu svega odgovarajuća poslovna kultura),

- Poslovno-organizacijski red i
- Dugoročni (strateški) poslovni ciljevi.

Upravo smo svedoci da tokom prošle i ove godine pojavili su se problemi u finansijskom sektoru Srbije i da je zbog neverodostojnog izveštavanja pokrenut postupak stečaja Agrobanke, zatvaranje Privredne banke i Univerzal banke Beograd.

2.1 TROUGAO PREVARA

Odavno se razmatraju okolnosti koje dovode do prevara i u literaturi može se uočiti da se okolnosti pod kojima prevara nastaje grupišu u takozvani "Trougao prevara". Slika koja sledi prikazuje trougao prevara:



Slika 2: Trougao prevara

Trouga prevara, (fraud triangle), kako i na slici prikazano čine:

- Prilika (Opporttunity) predstavlja okolnost koja je plodno tlo za prevaru, jer lice prosto ima mogućnost da je izvrši;
- Racionalizacija (Rationalization) je vrsta okolnosti pri vršenju prevara gde lice nalazi niz opravdanja koji njegovu nameru za vršenje kriminalne radnje opravdaju;
- Pritisak (Pressure) to su okolnosti koje od lica koje čine prevaru imperativno, zahtevaju likvidna sredstva koja on na taj način pokušava obezbediti.

2.2. CRVENI INDIKATORI (RED FLAGS)

Ono što je najbitnije jeste znati: ***Gde tražiti?*** Poznato je da "nema zločina bez motiva", pa tako poznavanje moguće motivacije za činjenje nekog prestupa u domenu finansija, ali i identifikacija računa koji bi mogli biti predmet prevare je od krucijalnog značaja u forenzičkom računovodstvu. Isto ovo važi i za transak-cije i poznate crvene identifikatore koji identifikuju i podstiču dalje ispitiva-nje. U poslovnom svetu se sve više javlja potreba za forenzičkim računovodstvom. Najčešći razlozi za razvoj forenzičkog računovo-dstva su nedostaci specijalizovanih znanja i iskustava koji su neophodni u forenzičkom ispitivanju. Forenzičke računovođe za otkrivanje i rešavanje finansijskih i računovodstvenih problema u poslovanju finansijskih institucija i/ili bilo kojih drugih institucija, nastalih kao posledica neprofesionalizma i neetičnosti, primenjuju računovodstvo, reviziju i istražna razmišljanja i druge veštine.

Poznato je, da su na razvoj forenzičkog računovodstva i revizije, najviše uticala empirijska znanja dobijena kroz poslovnu praksu, a u manjoj meri teorijska znanja. U forenzičkom računovodstvu podrazumeva se primena znanja iz različitih disciplina, kao što su: računovodstvo, ekonomija, revizija, statistika, istraživačke veštine i slično. Poznato je da su forenzičke računovođe osposobljeni da posmatraju "iza brojeva" i samim tim se suočavaju sa realnom situacijom u poslovanju.

Kao prvu odrednicu forenzičkog računovodstva izdvaja se analiza, koje razrađuju i objašnjavaju uzrok i posledice određene pojave, uključujući otkrivanje prevare i njenih posledica. Posmatrajući forenzičko računovodstvo kao primarnu metodologiju koja navodi objektivnu verifikaciju, orjentisano je na dokaze o ekonomskim transakcijama, na izveštavanje i sastavni je deo računovodstvenog sistema i zakonske mreže koja podržava ovakav tip dokaza. Sa druge strane kada se govori o forenzici može se reći da ona predstavlja ***"dubinsko"*** istraživanje događaja, koji dovode do pojave sumnje da se nešto pogrešno radi ili sa druge strane da je prevara moguća.

3. CILJ FORENZIKE

Za forenzičko računovodstvo i reviziju je karakteristična istražiteljska funkcija i kao takvo ono predstavlja zanimanje u kome su zastupljeni računovodstvo, pravo i informaciona tehnologija i drugi neophodni integrativni delovi. Slučaj kada su rukovodioci poslovnog subjekta zabrinuti zbog odstupanja u finansijskim izveštajima i finansijskih pronevera, tada su njima potrebne mnogo kompleksnije usluge od onih koje nude računovođe, odnosno u tom slučaju njima su potrebne forenzičke računovođe.

Primarni cilj forenzičkog računovodstva izdvaja se objektivna verifikacija finansijskih događaja. Upravo ovaj cilj je razlog da forenzičke računovođe veoma često se pozivaju na sudove kao svedoci, eksperti na sudovima, kako na strani tužioca tako i na strani odbrane. Na osnovu ovoga može se zaključiti da računovođe forenzičari mogu raditi na slučajevima građanske i krivične parnice. Kada se

govori o građanskim parnicama u tom slučaju se od forenzičkih računovođa može zahtevati da procene ekonomske štete koje su nastale usled prekida ugovora. Sa druge strane u krivičnim parnicama od forenzičkog računovođe se može tražiti da, prezentuje činjenične podatke o počinjenoj prevari u oblasti osiguranja, da identifikuje prevaru, pranje novca itd. Postoje događaji koji su doveli do porasta broja forenzičara i potrebe za ovom profesijom a to su:

- veliki broj kompanija bile su žrtve prevara,
- sve više raste broj kompanija koje su imale slučajeve korupcije i podmićivanja,
- porastao je broj finansijskih izveštaja u kojima je utvrđeno pogrešno prikazivanje,
- prevare u obliku prikazivanja gubitaka na imovini u proseku rastu,
- preko trećine prevara otkrivene su slučajno, primenom uobičajenih postupaka detekcije prevara.

Forenzičke računovođe koriste kao alat svoju veštinu razumevanja informacija o poslovanju, te finansijski sistem izveštavanja, računovodstvene i revizorske procedure, tehnike istraživanja i slično. Forenzičko računovodstvo i revizija nema samo zadatak da pronađe neslaganja, već pronalazi čitav niz prevara, a naravno daje i odgovore na pitanja kao što su: **ko, šta, gde, zašto?**

3.1. ZADACI FORENZIKE

Pri svakoj forenzičkoj istrazi kao glavno načelo izdvaja se ocena činjenica. Glavni zadaci forenzičkog računovođe i revizora su: analiza, interpretacija, sumiranje i prezentovanje međusobno povezanih poslovno-finansijskih stavki, tako da budu razumljivi i na odgovarajući način potkrepljene. Forenzičari često učestvuju u sledećim aktivnostima:

- vrše analiziranje i istraživanje dokaza o počinjenoj prevari,
- vrše prezentaciju rezultata istraživanja i to u vidu izveštaja i kompletiranja dokumentacije,
- učestvuju u razvijanju kompjuterizovanih aplikacija koje će poslužiti u analizama i prezentacijama o finansijskim dokazima, asistiraju u pravnim postupcima

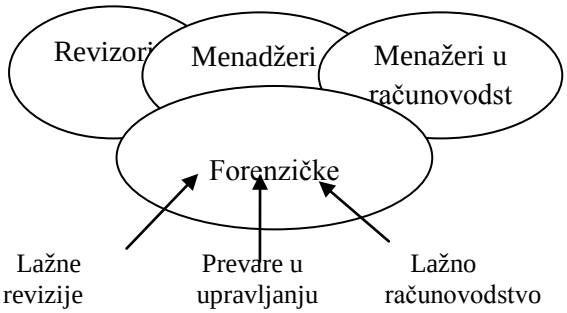
U sledećoj tabeli prikazane su informacije o načinima otkrivanja prevara i njihovom učešću u prevarama.

Tabela 1: Najčešće zabeleženi načini otkrivanja prevara u SAD-u

Ko je otkrio prevaru	Procenat
1. Prema dojavi zaposlenih	22,3
2. Slučajno	16,7
3. Interna revizija	16,6
4. Interna kontrola	13,4
5. Eksterna revizija	11,5
6. Dojave od strane kupaca	6,6
7. Anonimne dojave	6,2
8. Dojave od strane dobavljača	5,1
9. Ostalo	1,6
Ukupno	100,0

Izvor: samostalan rad autora ovog rada, a na osnovu rada Belak V.: Poslovna forenzika i forenzično računovodstvo - borba protiv prevare, Zagreb, str. 37, 2011.)

Može se zaključiti na osnovu navedenih podataka iz prethodne tabele da se unutar institucije uglavnom detektuju signali i elementi prevara a da je najčešće prepoznaju zaposleni. Forenzičari uz adekvatna znanja koje poseduju iz oblasti računovodstva, revizije, upravljanja i sa drugim menadžment veštinama umeju da uoče i uvide (ne) pravilnosti i (ne) pravednosti koje se javljaju u bilo kom društvu, signaliziraju moguću prevaru, zato je neophodno obratiti posebnu pažnju na sve one zaposlene koji mogu učiniti prevaru kad tad. Upravo nijedan organizacioni deo nije isključen od rizika prevare nose ih svi zaposleni na svim nivoima menadžmenta od top ka nižem i obrnuto.



Slika 3: Odnos između mendžera, poslovnih menadžera, revizora i forenzičkih računovođa

Pozicija računovođa je izuzetno nezahvalna, prvenstveno zbog uslova i okruženja u kome oni obavljaju svoj posao a razlozi za to su:

- nedovoljan razvoj svesti o potrebi, odnosno navike celoživotnog učenja,
- nedovoljno uređena računovodstvena legislative sa pratećim propisima,
- neredovno obnavljanje informacija o izmenama MRS/MSFI,
- neadekvatno valorizovanje računovodstva kao profesije i njenih pripadnika i
- ostali subjektivni i objektivni razlozi.

Danas se računovodstvu kao profesiji daje veći značaj kako od strane menadžmenta tako i od strane vlasnika kapitala, ali i od samih računovođa, koji nastoje da postupaju u skladu sa pravilima struke. Bez obzira na pozitivne trendove, celokupna slika računovodstva kao profesije u Srbiji i to u smislu pristupa računovodstvenim tehnikama i metodama, još uvek se može reći da je konzervativna, jer kada se govori o forenzičkom računovodstvu potrebno je naglasiti da naša računovodstvena praksa još ne poznaje zvanje "forenzički računovođa".

3.2. ANALITIČKE PROCEDURE U FORENZICI

Da bi utvrdili područje počinjenih prevara, računovođe i revizori forenzičari primenjuju različite procedure. Analitičke procedure su one koje razlažu problem do detalja i deluju u kontekstu formiranja uporednih određenih uzajamno povezanih segmenata poslovanja, a ti odnosi na kraju impliciraju mogućnost prevara. Analitičke procedure u forenzici imaju tri primarna cilja, a to su:

- Preliminarne analitičke procedure - koriste se za otkrivanje područja visokog rizika od prevara, vremena i stepena potrebnih forenzičkih procedura;
- Nezavisne analitičke procedure - koriste se za prikupljanje dokaza na temelju upoređivanja i usklađivanja podataka, te utvrđivanje verodostojnosti dokumentacije, knjiženja i obračuna;
- Konačne analitičke procedure - koriste se za donošenje zaključaka o uticaju problematičnih transakcija na finansijske izveštaje.

Forenzičari koriste i analitičke tehnike za analizu odnosa između stavki u finansijskim izveštajima, odnosno analizu poslovnih transakcija. Istraživačke tehnike forenzičkog računovodstva su:

- Horizontalna analiza - upoređuje stavke iz tekućeg perioda sa istim stavkama iz prethodnog perioda,
- Vertikalna analiza - upoređuje postotne udele pojedinih stavki u finansijskim izveštajima,
- Upoređivanje detaljnih stavki u finansijskim izveštajima- sa istim ili sličnim stavkama iz prethodnih perioda i
- Analiza odnosa u finansijskim izveštajima u područijima profitabilnosti, likvidnosti, solventnosti, aktivnosti i stvaranja vrednosti.

Tipični aspekti forenzičkih analitičkih procedura su poređenja određenih kategorija, kao što su: tekući podaci nasuprot podacima iz prethodnog perioda; stvarni podaci nasuprot budžetu, prognozama i projekcijama; podaci preduzeća nasuprot očekivanim rezultatima forenzičara.

3.3. TEHNIKE FORENZIKE

Forenzičko računovodstvo i revizija je kao profesija razvilo neke specifične tehnike, ali naravno upotrebljava i neke tehnike tradicionalnog računovodstva i revizije. Prilikom revizije može imati reaktivni i proaktivni pristup, pri čemu koristi različite tehnike.

3.3.1. BENFORDOV ZAKON

Ovaj zakon pozajmljen je iz matematike. Primarno je nastao pri kontroli numeracije u bibliotekama, ali naravno ima široku primenu u finansijama. Benfordov zakon pokazuje nam kolika je verovatnoća da se neka cifra nađe na pravom mestu u broju. Matematička formulacija ovoga zakona je:

$$P(D=d) = log_{10}(1+1/d/1), \text{ gde je } d = 1,2,...9 \quad (1)$$

Benfordov zakon primenjuje se u mnogim oblastima, tako se primenjuju u forenzici elektronike, pravu, osiguranju, hidrologiji, otkrivanju falsifikovane medicinske dokumentacije. U forenzičkoj reviziji, kao pomoćno sredstvo se koristi na taj način da se prevara može očekivati, ukoliko je razlika između očekivane Benfordove veličine i veličine do koje dođemo posmatranjem. Kada imamo veću količinu podataka i sama upotreba Benfordovog zakona je veća, dok sa druge strane u posmatranju bilansa njegova upotreba je ograničena, a razlog za to je mala količina ulaznih veličina, kao što su na primer sumarne bilansne pozicije.

3.3.2. TEORIJA RELATIVNE VELIČINE FAKTORA (THEORY OF RELATIVE SIZE FACTOR)

Teorija relativne veličine faktora ima posebnu upotrebnu vrednost kao pomoćno analitičko sredstvo. Ova tehnika je zasnovana na upoređivanju dve veličine iz seta podataka i to kao racio velikog broja u odnosu na drugi veliki broj. Definiše se određeni limit za različite kategorije,

kao što su sve vrednosti koje su van određenog ranga i koje treba ispitati (Ghosh i Banerjee 2011).

3.3.3. KOMPJUTERSKI PODRŽANE TEHNIKE REVIZIJE (COMPUTER ASSISTED AUDITIN OOLS- CAATS)

Kompjuterski podržane tehnike revizije predstavljaju praktičnu primenu informacionih tehnologija u poslovima revizije, pa samim tim i forenzičke revizije i računovodstva. Kada je reč o softverima koji se primenjuju u reviziji izdvajaju se dve varijante:

- Softverom ekstraktovani podaci i
- Softverska finansijska analiza.

Uz pomoć softvera znatno se efikasnije manipuliše različitim podacima, kao što su računi, potraživanja, plaćanja dobavljačima i drugi. Uz pomoć softverskih rešenja mogu se kreirati najrazličitije vrste izveštaja ali uvek je sve najbolje logično proveriti, posebno neobične transakcije, (Ghosh i Banerjee 2011). Računovodstveni softveri praktično primenjuju se prilikom:

- Detaljno testiranje transakcija i stanja;
- Identifikovanje nezakonitosti i značajnih fluktuacija;
- Programi uzorka za izvlačenje podataka za revizorsko testiranje;
- Testiranje generalno kompjuterskih sistema;
- Ponovno kalkulisanje u računovodstve-nim sistemima.

3.3.4. TEHNIKE PRETRAŽIVANJA PODATAKA (DATA MINING TECHNIQUES)

Tehnike pretraživanja podataka je set tehnika dizajniranih za automatsko pretraživanje velike količine podataka sa ciljem pronalaska informacija, koje će pomoći u otkrivanju prevara. Ovde se izdvajaju tri načina koja koriste tehniku za pretraživanje podataka i to su:

- Otkrivanje - posmatranje podataka bez apriori poznavanja prevara, ovde posmatramo različite trendove, varijacije.
- Modeliranje - proces u kome se već otkrivena struktura u bazi podataka koristi za predviđanje dolazećeg podatka.
- Devijaciona analiza - kod koje se na osnovu utvrđenih normi detektuju elementi koji se razlikuju od običnih i označavaju se sumnjivim i koje dalje treba istražiti.

3.3.5. RACIO ANALIZA

Ova analiza ima veliku pomoćnu i analitičku ulogu u forenzičkoj reviziji. Na bazi analiziranih podataka se dolazi do određenih simptoma. Tri najznačajnija racija, koja imaju široku primenu u forenzici su:

- Racio visoke vrednosti u odnosu na nižu vrednost,
- Racio visoke vrednosti u odnosu na drugu visoku vrednost,
- Racio tekuće godine u odnosu na prethodnu.
- Svaki od ovih racia pojedinačno ima veliki značaj, jer predstavljaju prilično pouzdan trag u otkrivanju potencijalnih kriminalnih radnji.

4. ZAKLJUČAK

Potreba za forenzičkim računovodstvom i revizijom u okviru računovodstveno revizorske profesije je neophodno, posebno u vremenu ekonomske i privredne globalizacije i finansijske krize i sve češćih prevara u svim oblastima poslovanja. Primena ovog znanja iz ove disipline treba da bude model preventive (sprečavanja) prevare, a njen razvoj treba da smanji prevare i druge vrste destrukcije u finansijskom sektoru i ekonomiji uopšte, jer negativno deluju ne samo na privredne tokove već i na druge svere života zaposlenih i stanovništva uopšte.

Opravdanosti uvođenja forenznike u računovodstvu i reviziji ima najvažniju ulogu ljudski resursi što podrazumeva da zaposleni moraju biti obrazovani i sa iskustvom, moraju stalno da rade na sopstvenom usavršavanju koje svakako nije samo iz oblasti ekonomije, već njihova znanja moraju biti na vrlo visokoj lestvici u oblasti informatike, prava, finansija i svih drugih neophodnih disciplina. Zaposleni u forenznici moraju imati visoke moralne i profesionalne kvalitete, ovo je preduslov obavljanja ovog posla, zatim slede sva ostala neophodna znanja, iskustva, lične sposobnosti kao i tehnički uslovi kako bi sva stečena znanja na što brži i efikasniji način upotrebili.

Neumanjujući potrebe forenzike u razvijenim privredama ono je svakako u tranzicionim privredama mnogo važnije s obzirom da se tranzicija smatra aktivnošću koja je podložna svim vrstama manipulacija i prevara. Način obavljene tranzicije i sadašnje stanje privrede u Srbiji zahteva da se ova računovodstvena disciplina što brže inkorporira u zakonske propise i naravno da se što hitnije primenjuje.

LITERATURA

(1) Belak,V.: *„Poslovna forenzika i forenzično računovodstvo- borba protiv prijevare“*, Zagreb, Belak Excellens d.o.o. sre.37, 2011.

(2) Crumbley L. D., L. E. Heitger, S. G. Smith: *Forensic and Investigative Accounting.* CCH a Wolters Kluwer business, 2007.
(3) Ghosh, K., I, i K Banerjee*:"Forensic Accounting", The chartered accountant*, 62, october 2011.
(4) F.Koletnik i I. Kolar: *„Forenzično računovodstvo",* Ljubljana, Zveza računovodij, finančnikov in revizorjev, Slovenija, str.128, 2008.
(5) Nigrini, J. M.: *Benford's Law*, New Jersey: Johan Wiley & Sons, 2012.
(6) Skalak L.S.; T., Golden M., Clyton, Pill J.: *„A Gude to Forensic Accounting investigations"*, Second edition, New Jersey: John Wiley & Sons Inc. Hoboken, page 34, 2011.

Konferencija o bezbednosti informacija BISEC 2014
Fakultet informacionih tehnologija

PREGLED TEHNIKA MULTIMEDIJALNE PASIVNE FORENZIKE ZA DETEKCIJU KRIVOTVORENJA SLIKA

REVIEW OF MULTIMEDIA PASSIVE FORENSIC TECHNIQUES FOR IMAGE FORGERY DETECTION

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

Rezime: *Zahvaljujući velikom kapacitetu, širokoj zastupljenosti interneta i dostupnim digitalnim foto-aparatima, kamerama i računarima, digitalna multimedija danas predstavlja jedno od osnovnih sredstava komunikacija. Pored brojnih prednosti, široka primena multimedijalnih sadržaja je dovela do problema koji se odnose na njihovu autentičnost i bezbednost. Kako bi se izborila sa time, istraživačka zajednica je usredsredila svoje aktivnosti na polju tehnika digitalne forenzike. Postupci pasivne forenzike, koji se primenjuju u odsustvu posebnog hardvera, se predlažu u ovom radu u svrhu autentifikacije. Osnovna ideja je da manipulacija nad digitalnim medijem može da ne ostavi vizuelne tragove, ali menja statistiku sadržaja. Bez prethodnog poznavanja sadržaja, takve promene mogu da se uoče i da budu uzete kao dokaz za krivotvorenje.*

Ključne reči: *Digitalna forenzika, multimedija, slika, komunikacije, autentifikacija*

Abstract: *Thanks to their huge capability, coupled with the widespread use of the Internet and affordable cameras and computers, digital multimedia represents nowadays one of the principal means of communication. Besides the many benefits, the wide proliferation of multimedia contents has lead to problematic issues regarding their authenticity and security. To cope with such problems, the research community has focused its attention on digital forensic techniques. Passive forensics approaches, which work in absence of special hardware, have been proposed in this paper for authentication purposes. The basic idea is that the manipulation of a digital media may not leave any visual trace of its occurrence, but it alters the statistics of the content. Without any prior knowledge about the content, such alterations can be revealed and taken as evidence of forgery.*

Keywords: *Digital forensics, multimedia, image, communications, authentication*

1. UVOD

U današnjem digitalnom dobu susrećemo se u svakodnevnom životu sa digitalnim multimedijalnim sadržajima kao jednim od osnovnih vidova komunikacija. Štaviše, multimedijalne informacije mogu da se formiraju, memorišu, prenose i obrađuju u digitalnom formatu na veoma jednostavan način, zahvaljujući širokoj zastupljenosti interneta kao sredstva za masovnu komunikaciju, jeftinih digitalnih fotoaparata visoke rezolucije, računara i korisnički orijentisanih alata za editovanje informacija.

Danas je naša realnost nezamisliva bez digitalnog multimedijalnog sadržaja, kao što su slike i video signali. Multimedijalni sadržaji se veoma lako distribuiraju preko web zasnovanih alata za razmenu sadržaja, kao što su društvene mreže, *Youtube*, *Picasa*, *Flickr*. Osim toga, veoma su zastupljeni u oblastima kao što su: novinarstvo, sport, naučne publikacije, političke kampanje i forenzička istraživanja.

Pored ekonomskih i tehničkih prednosti, digitalna informaciona revolucija je dovela i do problematičnih aspekata vezanih za bezbednost i pouzdanost multimedijalnih informacija.

Imajući to u vidu, postalo je sve značajnije da se obezbedi automatska zaštita digitalnih sadržaja kako bi se garantovala njihova verodostojnost i bezbednost. Istraživačka zajednica je veoma aktivna na ovom polju, što je dovelo do razvoja sofisticiranih i pouzdanih metoda za autentifikaciju i zaštitu informacija [1].

Rastuća količina multimedijalnog sadržaja na internetu, zahvaljujući sajtovima za razmenu fajlova i društvenim mrežama, dovela je do potrebe za tehnikama multimedijalne forenzike koje obrađuju problem autentifikacije multimedijalnih informacija. Slično kriptografiji, autentifikacija multimedijalnih sadržaja pomoću metoda aktivne i pasivne forenzike, predstavlja igru "mačke i miša", gde je lopta naizmenično u rukama istražitelja i krivotvoritelja. Bilo kako, važno je igrati ovu

igru kako bi se došlo do novih i boljih rešenja u cilju otkrivanja manipulacije nad multimedijalnim sadržajima.

Korišćenje digitalnog dokaza u sudovima je postalo značajno poslednjih godina kroz navođenje mejlova, digitalnih fotografija, tekstualnih dokumenata, istorije instant poruka, istorije pretraživanja interneta, baza podataka, sadržaja računarske memorije, tragova sistema za globalno pozicioniranje, kao i digitalnih video i audio zapisa. Kao i svaki dokaz, tako i digitalni dokaz zahteva postupak u kome sud može da se uveri u autentičnost [2].

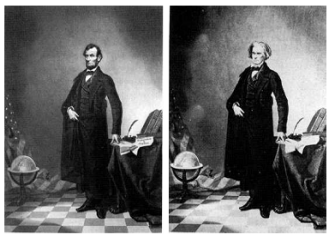
Multimedijalna forenzika se bavi digitalnom reprezentacijom delova realnosti, kao što su slike, video i audio zapisi koji su snimljeni digitalnim fotoaparatima, kamerama, ili sličnim uređajima. Glavni zadatak multimedijalne forenzike je da pokaže da digitalni dokaz može da se koristi na sudu jer je pouzdan i autentičan, ili obrnuto, da ne može da se prihvati kao dokaz ako ne može da se dokaže njegova autentičnost.

Tradicionalno stanovište posmatra fotografije i video zapise kao verno i blisko predstavljanje stvarnosti. Međutim, u današnjem digitalnom dobu ova pretpostavka se više ne može uzimati u obzir, zbog mogućih manipulacija digitalnim multimedijalnim sadržajima. Manipulacije postaju moguće zahvaljujući širokoj dostupnosti računara visokih performansi, digitalnih kamera visoke rezolucije, kao i sofisticiranih softverskih alata za foto-editovanje i računarsku grafiku, kao što je to *Photoshop*. I korisnici koji nisu eksperti mogu lako da manipulišu i menjaju multimedijalne sadržaje, bez ostavljanja očiglednih tragova manipulacije. Kao posledica toga više se ne može pretpostavljati vernost i autentičnost slika i video zapisa, posebno kada se uzimaju u obzir forenzička i kriminalna istraživanja, sistemi za nadzor, medicinske slike i žurnalizam. Štaviše, promenjeni multimedijalni podaci mogu da utiču na mišljenje ljudi i čak da menjaju njihove stavove u odnosu na predstavljene događaje.

Posle uvodnog razmatranja, razmotrena su neke mogućnosti krivotvorenja digitalnih slika. Zatim su navedene i analizirane metode multimedijalne pasivne forenzike. U nastavku je dat pregled tehnika za detekciju krivotvorenja slika. Na kraju su data zaključna razmatranja.

2. MOGUĆNOSTI KRIVOTVORENJA SLIKE

Lažni multimedijalni sadžaji imaju dugu istoriju, verovatno od nastanka fotografije u prvoj polovini XIX veka. Vrlo brzo nakon što su se pojavile komercijalne analogne kamere fotografije su postale predmet manipulacije i nasilnog menjanja sadržaja. Neki od ranih primera menjanja realnosti se odnose na generale i političare. Na Slici 1 je pokazan portret američkog predsednika Abrahama Linkolna, koji potiče iz 1860. godine a koji je, zapravo, lažan jer je generisan spajanjem glave Linkolna sa telom političara Džona Kalhuna.

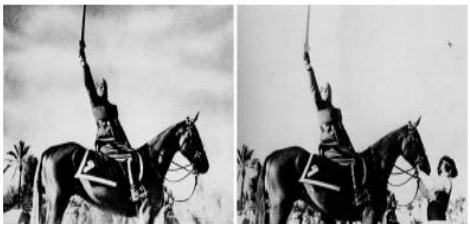


Slika 1. Fotografija iz 1860. godine koja pokazuje kako je nastala slika predsednika Abrahama Linkolna [3]

Na Slici 2 je pokazana fotografija iz 1864. godine koja pokazuje generala Granta ispred svojih trupa u Siti Pointu u Virdžiniji, za vreme Američkog građanskog rata. Istraživači iz Kongresne biblioteke u Vašingtonu su ustanovili da je fotografija zapravo sastavljena iz tri odvojene fotografije: glava je preuzeta sa drugog portreta generala Granta, konj i telo pripadaju generalu Mekkuku, dok je pozadina preuzeta sa fotografije zatvorenika koji su pripadali Konfederaciji.

Slika 2. Fotografija generala Granta iz 1864. godine koja je nastala kompozicijom tri druge fotografije snimljenih u različitim trenucima i uslovima [4]

Naredni primer potiče iz II svetskog rata, kada je 1942. godine izmenjen portret italijanskog vođe Musolinija uklanjanjem lika koji je držao konja, kako bi vođa na fotografiji izgledao monumentalnije, što se vidi na primeru sa Slike 3.



Slika 3. Fotografija iz 1942. godine koja pokazuje kako je promenjena originalna slika brisanjem lika [4]

U to vreme bio je potreban visoki stepen tehničke ekspertize i specijalizovana oprema kako bi fotografija bila izmenjena. Danas postoji moderni softver koji veoma lako može da menja sadržaj fotografija, a od skoro i video zapisa, jednostavnije nego ikada i teže za otkrivanje.
Sa masovnijom primenom digitalnih fotoaparata, snažnih personalnih računara, kao i razvojem sofisticiranog softvera za foto-editovanje, manipulacija nad digitalnim

slikama je postala znatno jednostavnija. Digitalne slike se nalaze svuda: na naslovnim stranicama časopisa, u novinama, svuda po internetu. Sa druge strane, jednostavnost manipulacije nas navodi na pomisao da li su te slike zapravo realne ili ne. Alati za krivotvorenje su danas postali sofisticirani, pružajući mogućnost da se krivotvorene slike javljaju u nauci, pravu, politici, medijima i poslovanju. Sa druge strane, alati za detekciju krivotvorenja se nalaze na svom početku razvoja i postoji jasna potreba za ovim alatima u domenu forenzike.

Svedoci smo pretrpanosti retuširanim slikama, pogotovo u časopisima i prostorima za oglašavanje. Dobro poznati slučaj se odnosi na reklamu preparata kozmetičke industrije *Olay*, što je pokazano na Slici 4.

Slika 4. Oglašavanje u časopisu koje pokazuje značajno retuširanje originalne fotografije [4]

Poruka na reklami kaže: "*Olay* je moja tajna za svetle oči i smanjuje bore i tamne tragove, kako bi moje oči bile svetle i mlade". Sa slike se vidi da je nekadašnji model Tvigi primetno retuširana kako bi izgledala mlađe. Međutim, pošto je uočeno značajno retuširanje u post-produkciji, udruženje potrošača je pokrenulo akciju da se ova reklama zabrani, budući da može da dovede do pogrešnog zaključka o reklamiranom proizvodu.

Na Slici 5 je pokazan primer manipulacije slike koja pokazuje naslovnu stranicu časopisa "*The Economist*" sa američkim predsednikom Obamom. Naime, sa desne strane je prikazan originalni snimak sa još dve osobe, koje su naknadno uklonjene manipulacijom.

Slika 5. Krivotvorena slika američkog predsednika Obame [3]

Primer lažne slike je registrovan 2011. godine kada su španske sportske novine objavile izmenjenu fotografiju meča između Atletika Bilbao i Barcelone, sa namerom da se prikaže ofsajd. Međutim, originalni frejm pokazuje da je odbrambeni igrač digitalno izbrisan sa fotografije i prema tome nije bilo incidenta, što je pokazano na Slici 6. Novine su objavile javno izvinjenje, tvrdeći da je do toga došlo zbog greške u štampi.

Slika 6. Fotografija iz 2011. objavljena u španskom sportskom časopisu [4]

Sledeći primer na Slici 7 pokazuje fotografiju iranskih raketnih proba, koja se pojavila 2008. godine na naslovnoj stranici mnogih časopisa. Posle publikovanja ove fotografije, ustanovljeno je da je digitalno dodata raketa na levoj slici, dok desna slika predstavlja original.

Slika 7. Krivotvorena slika raketa [3]

Kao što pokazuju navedeni primeri porast krivotvorenja slika je u značajnom porastu u svakodnevici i ima uticaj u našim životima i društvu. Pouzdanost digitalnih sadržaja ne može biti verno uzeta i može se postaviti pitanje da li multimedijalni sadržaji zaista predstavljaju verni prikaz realnosti. Odakle zaista potiče neka slika? Kakva je, zapravo, njena predistorija? Da bi se odgovorilo na ova pitanja, pasivna digitalna forenzika je privukla pažnju naučne zajednice u poslednjoj deceniji, imajući u vidu porast broja publikacija iz ove oblasti [5]. Za ovaj pristup digitalne forenzike kaže se da je pasivan ili slep, jer ne uzima u obzir a priori informacije o dostupnom sadržaju, a sa druge strane nisu primenjivani mehanizmi zaštite integriteta, kao što je digitalni votermarking.

3. METODE MULTIMEDIJALNE PASIVNE FORENZIKE

Multimedijalne pasivne tehnike se odnose na novi pravac bezbednosti digitalne multimedije budući da se, za razliku od tehnika aktivne forenzike, primenjuju u odsustvu posebne opreme i ne zahtevaju prethodno poznavanje multimedijalnih sadržaja. Osnovna pretpostavka za ove metode je da originalni sadržaj koji nije krivotvoren poseduje neke statističke oblike koji su uneti prilikom generisanja sadržaja. Takvi oblici su uvek prisutni u originalnim signalima, ali se obično menjaju prilikom nekog krivotvorenja. Iako ne mogu da se uoče vizuelno, te promene mogu da se detektuju statističkom analizom sadržaja, bez potrebe da se prethodno zna sadržaj. Zbog toga se za ove metode kaže da su pasivne i slepe.

Identifikacija uređaja može da se koristi kada se digitalne kamere upotrebljavaju od strane pirata u bioskopima da bi se snimile kopije filmova relativno dobrog kvaliteta koje kasnije mogu da se prodaju na crnom tržištu i koduju na

niskim protocima radi ilegalne distribucije na internetu. Forenzičke metode mogu da ukažu da dva video zapisa potiču sa iste kamere ili da dve kodovane verzije jednog filma imaju isti izvor. Na taj način može da se pomogne istražiteljima da nađu vezu između različitih entiteta ili subjekata i mogu da budu krucijalni dokaz u kažnjavanju piraterije.

Forenzička analiza može da pomogne u istrazi da se pronađe razlika između originalnog multimedijalnog sadržaja i ilegalne kopije. Različiti tipovi uređaja za akviziciju podataka mogu da budu uključeni u ovaj scenario, kao što su: digitalni fotoaparati, kamere, mobilni smart telefoni, skeneri, tablet uređaji, kao i fotorealistične slike generisane grafičkim softverom. U svim ovim primerima od vitalnog značaja je dokazati autentičnost i pouzdanost digitalnih slika.

Pasivna multimedijalna forenzika je tesno povezana sa brojnim različitim naučnim disciplinama kao što su: računarska nauka, obrada signala i procesiranje kriminala. Imajući u vidu literaturu iz ove oblasti, mogu da se definišu sledeća istraživačka polja u okviru pasivne forenzike [1]:

- **Identifikacija izvora slike** ima za cilj da uspostavi vezu između slike i uređaja pomoću koga je generisana, na primer digitalnog foto-aparata, mobilnog telefona, ili skenera. Osnovna pretpostavka je da se digitalne slike koje su uzete sa istog uređaja odlikuju jedinstvenim otiskom uređaja za akviziciju.

  Kod identifikacije izvora cilj je da se identifikuje uređaj koji je prikupio sadržaj, istraživanjem tragova ostavljenih pri različitim koracima u procesu akvizicije slike. Osnovna ideja potiče iz klasične forenzičke nauke, gde se analiza metaka sprovodi na osnovu oznaka koje su jedinstvene za svako posebno oružje i prema tome može da se uspostavi veza između metka i oružja iz kojeg je ispaljen. Slično tome, kada se snimi slika postoji jedinstveni otisak koji se uvodi u sadržaj i koji ukazuje na uređaj pomoću koga je slika snimljena. Kada se slika prikupi ustanovi se šum u vidu artefakata na slici, distorzije ili statističkih osobina podataka. Takav šum je nevidljiv za ljudsko oko, ali može da se analizira uspešno doprinoseći procesu identifikacije [6].

  Tehnike za identifikaciju izvora se fokusiraju na poreklo digitalnih slika i video zapisa. Treba voditi računa o dva aspekta tom prilikom: prvi aspekt se odnosi na otkrivanje kojim uređajem su generisani digitalni signali (digitalna kamera, skener, mobilni uređaj), dok se drugi aspekt odnosi na određivanje specifične kamere ili skenera koji je upotrebljen radi akvizicije sadržaja, tj. na prepoznavanje modela i brenda, što je ilustrovano na Slici 8.

Slika 8. Postupak prepoznavanja modela uređaja

Digitalne slike, koje mogu da budu memorisane u različitim formatima, kao što su JPEG (*Joint Photographic Expert Group*), GIF (*Graphic Image Format*), PNG (*Portable Network Graphic*), TIFF (*Tagged Image File Format*). Format sam po sebi nosi dosta informacija vezane za sliku. JPEG slike sadrže dobro definisane metapodatke, tabele kvantovanja za kompresiju slike, kao i komprimovane podatke sa gubicima. Metapodaci opisuju izvor slike, koji obično uključuje tip kamere ili fotoaparata, rezoluciju, podešavanje fokusa, i druge podatke. U slučaju da je korišćen RAW (sirov, neobrađen) format, kamera generiše heder koji sadrži nivo oštrine, kontrast i zasićenje, temperaturu boje, i tome slične parametre. Slika se ne menja postavljanjem ovih parametara, oni su jednostavno prilepljeni na podatke o slici. RAW format zapisa fotografije je, u stvari, format u kome foto-aparat beleži sve podatke koje je zabeležio i sam digitalni senzor foto-aparata.

Uprkos tome što metapodaci pružaju značajnu količinu informacija, oni imaju i neka ograničenja: mogu da se edituju, brišu i mogu da se unose lažni podaci o tipu kamere. Zbog toga je važno da se obezbedi pouzdana identifikacija izvora, nezavisno od tipa metapodataka, što predstavlja pasivan forenzički pristup.

U literaturi postoji dosta radova koji se odnose na identifikaciju izvora a koji obrađuju oštećenja koja unose sočiva (aberacija sočiva), ili artefakte u vezi otklanjanja mozaičke strukture. Druga grupa radova se odnosi na ograničenja senzora, kao što su pikseli sa defektom, ili šum usled neuniformnosti foto-odgovora (*photo-response non-uniformity*, *PRNU*). Slični koncepti mogu da se primene na video signal. Parametar PRNU može da se koristi kao jedinstveni otisak za identifikaciju izvorne kamere. Signali niže rezolucije mogu da se koriste za analizu povezivanja video zapisa sa youtjuba sa izvorima tih signala.

- Druga klasa tehnika digitalne forenzike ima za cilj **diskriminaciju (odvajanje) između realnih i računarski generisanih slika**, što se zasniva na pretpostavci da je danas računarska tehnologija sofisticirana i pouzdana i da je teško da se jednostavno razlikuju virtuelne i realne slike putem jednostavnog vizuelnog uvida. Naime, virtuelne slike se danas odlikuju visokim stepenom fotorealizma. Istraživanja na ovom polju su danas intenzivna, posebno imajući u

vidu povezanost sa pravnim sredstvima. Brojne tehnike su predložene u literature [1]. Generalno, cilj se postiže pomoću algoritama za mašinsko učenje koji su podešeni da klasifikuju prirodne i veštačke slike, koristeći bilo statističke informacije prisutne u prirodnim slikama, bilo razliku u procesu akvizicije ove dve klase slika.

Kod diskriminacije između realnih I sintetičkih slika cilj je da se obavi diferencijacija između realnih i računarski generisanih slika, imajući u vidu povećani fotorealizam slika formiranih pomoću sofisticiranih trodimenzionalnih (3D) grafičkih alata čineći dati zadatak izazovnim kada je u pitanju samo vizuelna inspekcija. Zadati cilj se postiže preko algoritama za mašinsko učenje koji su modifikovani tako da klasifikuju prirodne i veštačke slike. Lyu [7] je imao pristup da se statistika višeg reda transformacionih koeficijenata koristi za klasifikaciju i taj pristup se pokazao efikasnim pri diskriminaciji realnih i računarski generisanih slika. Prateći ključnu ideju, metode za identifikaciju izvora su razvijene sa pretpostavkom da se proces generisanja računarske grafike suštinski razlikuje od realnih slika koje su prikupljene u procesu akvizicije.

- Treća klasa pasivne forenzike ima za cilj otkrivanje **detekcije krivotvorenja** multimedijalnog sadržaja koje se moguće dešava. Naime, kada se slika falsifikuje obično se ne javljaju vizuelna artifakta u digitalnim slikama i onda je teško da se uoči manipulacija jednostavnim vizuelnim uvidom. Međutim, prilikom manipulacije dolazi do izmene statistike slike koja omogućava uočavanje krivotvorenja. S tim u vezi, dosta tehnika je predloženo u literaturi, što ukazuje na povećano interesovanje istraživača na ovom polju.Kod detekcije krivotvorenja cilj je autentifikacija digitalnih sadržaja, uključujući slike i video zapise, što se zasniva na pretpostavci da krivotvorenje može da ne ostavi nikakvu indiciju o tome da se dogodilo, ali može da promeni statistiku sadržaja.

Navedene tehnike su inovativne i dosta obećavaju, ali imaju i svoja ograničenja. Nijedna od njih ne pruža za sada definitivno rešenje za detekciju krivotvorenja i autentifikaciju, ali generalni okvir može da bude objedinjavanje nekoliko tehnika koje se odnose na različita pitanja u digitalnoj fornzici.

4. DETEKCIJA KRIVOTVORENJA SLIKA

Uopšteno govoreći, forenzički alati za autentifikaciju slika i detekciju krivotvorenja mogu da se grupišu u sledeće kategorije:

- Tehnike zasnovane na pikselima;
- Tehnike zasnovane na formatima;
- Tehnike zasnovane na kamerama;
- Fizički zasnovane tehnike;
- Geometrijski zasnovane tehnike.

Osnovna pretpostavka **tehnika koje su zasnovane na pikselima** je u tome da bilo koji vid manipulacije, ako je obavljen valjano, nije vidljiv, ali može da promeni specifičnu statistiku na nivou piksela. Na primer, statističke regularnosti u prirodnim slikama koje su nezavisne od sadržaja slike se upotrebljavaju za autentifikaciju slika.

Kloniranje (ili metod "*copy and paste*") je verovatno najjednostavniji način krivotvorenja i obično se obavlja tako što se objekti u nekoj sceni prekrivaju drugim delovima te iste slike. Uprkos tome što je vizuelno teško uočljivo, neka vrsta falsifikovanja može da se uoči posmatranjem statistički sličnih delova u okviru sadržaja slike. Međutim, ovaj postupak može da bude računarski kompleksan jer zahteva pretraživanje po celoj slici. Da bi se redukovala računarska kompleksnost i ubrzao proces koriste se postupci koji koriste diskretnu kosinusnu transformaciju (*Discrete Cosine Transform – DCT*), diskretnu wavelet transformaciju (*Discrete Wavelet Transform – DWT*), PCA (*Principal Component Analysis*) analizu, Furije-Melin (*Fourier-Mellin*) transformaciju, kao i pretraživanje oblika (*feature matching*). Slični koncepti se koriste i za detekciju duplikata video signala.

Ponovno odmeravanje (*resampling*) je postupak koji se dešava pri promeni veličine slike, rotaciji ili skupljanju slike, odnosno pri formiranju lažne (*fake*) slike. Navedeni postupak uvodi neke specifične korelacije između susednih piksela, koje mogu da se koriste kao dokaz manipulacije. Istraživanja u ovom pravcu pokazuju da interpolirani signali sadrže specifične periodične osobine koje mogu da se detektuju.

Kada se spoje dve ili više slika onda se menja Furijeova statistika višeg reda i ta promena može da se koristi kao dokaz krivotvorenja.

Uklanjanje pokretnog objekta u video signalu generalno uvodi artefakte u vidu senke duhova („*ghost shadow*"), koje mogu pouzdano da se otkriju u video sekvenci i da se onda koriste kao dokaz falsifikovanja video signala.

Tehnike zasnovane na formatima upotrebljavaju statističke korelacije koje uvode sistemi za kompresiju signala. JPEG kompresija je algoritam sa gubicima, što znači da se neke informacije gube u procesu kompresije. Korak kvantovanja nad DCT koeficijentima je pogotovo odgovoran za taj gubitak. Kvantovanje se odvija nad tabelom od 192 vrednosti, povezanih sa frekvencijom koja može da se podešava u okviru blokova veličine 8x8 piksela, zavisno od željenog kvaliteta. Tabela može da se estimira i ekstrahuje iz sadržaja slike. Nekonzistencije koje se na to odnose mogu da se koriste kao dokaz krivotvorenja slike ili video zapisa. Štaviše, kada se JPEG kompresija obavi dva puta, to uzrokuje specifične artefakte koji se javljaju kod slike i video signala. Osim standarda JPEG za kompresiju mirnih slika, pokazano je i da standard JPEG 2000 može da se koristi za duplu kompresiju. Manipulacije nad slikama mogu da menjaju artefakte usled blok-efekta koji se javljaju kod JPEG kompresije na granicama susednih piksela. Imajući to u vidu, kvantovani koeficijenti mogu da se uzmu kao dokaz

krivotvorenja, jer nije verovatno da se sadrži isti nivo kvantovanja kod dve spojene slike.

Tehnike zasnovane na kamerama koriste analizu tragova koji se ostavljaju pri različitim koracima obrade slike. Ti artefakti mogu da se koriste kao dokaz pri krivotvorenju. Hromatska aberacija je promena koja nastaje zbog prostornog pomeranja na lokaciji gde svetlo sa različitim talasnim dužinama pogađa senzor. Lokalna aberacija može da se posmatra u odnosu na sliku u celini kao dokaz krivotvorenja. Većina digitalnih kamera je opremljena sferičnim sočivima koja prouzrokuju radijalna oštećenja na slikama. Kada se dve slike spoje takve neregularnosti mogu da se koriste kao dokaz. Štaviše, većina kamera je opremljena jednim senzorom i boja se formira preko dela koji se zove *color filter array*. Za svaki piksel se snima samo jedan odmerak boje, dok se oni koji nedostaju dobijaju procesom interpolacije. Kao posledica toga se javljaju specifične korelacije za koje nije verovatno da će opstati pri krivotvorenju. Forenzički alati za detekciju su često zasnovani na linearnim relacijama između nivoa svetlosti izmerenog od strane senzora, kao i odgovarajućih vrednosti piksela tj. odgovora kamere. Korelacije koje uvodi kamera ili algoritam za obradu video signala mogu da se koriste za autentifikaciju video zapisa, kroz analizu nekonzistentnosti koje se javljaju u video sekvenci.

Fizički zasnovane metode proučavaju nekonzistentnosti koje nastaju u osvetljenju. Naime, teško je proceniti efekat osvetljenja na svaki deo neke celine, tako da razlike u osvetljenju cele slike mogu da se uzmu kao dokaz za krivotvorenje. Džonson [8] je razmatrao normale na dvodimenzionalne (2D) površine za procenu pravaca svetlosti različitih objekata u sceni. Ova ideja je zatim proširena na trodimenzionalne (3D) modele, koji koriste refleksiju svetlosti u očima. Međutim, razmotreni modeli koriste pojednostavljenu sliku, dok je osvetljavanje scene složeniji postupak.

Geometrijski zasnovane metode javljaju se kao kontrast statističkim tehnikama i zasnivaju se na merenju pozicije objekata u realnom svetu i njihove relativne pozicije u odnosu na kameru kroz analizu projektivne geometrije. Naime, treba imati u vidu da tipične slike mogu da prolaze kroz niz postupaka post-procesiranja i ponovne kompresije, što može da umanji efikasnost tradicionalnih metoda za detekciju krivotvorenja. Prednost ovih metoda u odnosu na statističke metode se sastoji u tome što su modelovanje i procena geometrije manje osetljivi na rezoluciju i kompresiju koja se primenjuje kod statističke analize slika i video signala.

Geometrijski zasnovana forenzika slika za detekciju manipulacije nad tekstom ima za cilj da detektuje krivotvorenje teksta na znacima i bilbordima. Dodavanje ili promena teksta na slici je relativno jednostavno, tako da je teško da se detektuje promena jednostavnim vizuelnim uvidom. Metod se sastoji u tome što se modeluje projekcija sa znaka na sliku da bi se odredilo da li projekcija zadovoljava očekivano planarno preslikavanje. U stvari, nije verovatno da naknadno uneti tekst precizno ispunjava ovo pravilo, pa zbog toga ovaj model može da se koristi kao dokaz za falsifikovanje.

Geometrijski zasnovana video forenzika za autentifikaciju balističkih pokreta – postavljanje i preuzimanje video zapisa je postalo danas veoma popularno na sajtovima za razmenu video materijala. Neki video zapisi su realni, ali neki su i lažni. Postoje geometrijski zasnovane forenzičke metode za autentifikaciju ukoliko se u tim zapisima javlja projektil, koji može da bude, recimo, u obliku bačene lopte. Navedena metoda može da posluži za modelovanje 3D balističkih pokreta i 2D projekcija trajektorije projektila. Odstupanja od modela mogu da posluže kao dokaz da je bilo krivotvorenja. Analiza projektila u video signalu do sada nije bila predmet istraživanja u okviru forenzičke zajednice, već u okviru robotike i računarske vizije.

5. ZAKLJUČAK

Univerzalna dostupnost interneta, razvoj visokokvalitetnih tehnologija digitalnih kamera i računarske tehnologije, doveli su do toga da su digitalni multimedijalni sadržaji primarni izvor vizuelnih informacija u brojnim scenarijima, zamenjujući tradicionalne medije, kao što su analogni film ili analogna fotografija. Digitalizacija ovih sadržaja dovela je do značajnih tehnoloških i ekonomskih dobitaka, ali takođe i do problematičnih aspekata vezanih za autentičnost sadržaja. Naime, sofisticiran i korisnički orijentisan softver za editovanje grafike je omogućio lako manipulisanje digitalnim slikama i video zapisima.

Istinitost multimedijalnih sadržaja time se dovodi u pitanje i njihova pouzdanost vernog predstavljanja realnosti ne može a priori da bude uzeta, posebno u okruženju osetljivih podataka, kao što su forenzička istraživanja, medicinske slike ili novinska fotografija. U ovom radu ukazali smo na značaj efikasnih tehnika koje se odnose na pitanja bezbednosti multimedijalnih informacija.

LITERATURA

[1] H. T. Sencar, N. Memon: „Overview of state-of-the-art in digital image forensics“, *Statistical Science and Interdisciplinary Research*, Vol. 3, pp 325-347, 2008.

[2] 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.

[3] I. Amerini: „*Image forensics: source identification and tampering detection“*, PhD dissertation, Universita degli studi di Firenze, Italy, 2010.

[4] V. Conotter: „*Active and passive multimedia forensics“*, PhD dissertation, University of Trento, Italy, 2011.

[5] T.T. Ng, S.F. Chang, C.Y. Lin, Q. Sun: „Passive-blind image forensics“, in *Multimedia Security Technologies for Digital Rights*, pp 383-412, Academic Press, 2006.

[6] N. Khanna, G.T.C. Chiu, J.P. Allebach, E.J. Delp: „Forensic techniques for classifying scanner, computer generated and digital camera images“, *International Conference on Acoustics, Speech and Signal Processing* ICASSP 2008, pp 1653-1656, 2008.

[7] Y. Liu, D. Liang, Q. Hang, W. Gao: „Extracting 3D information from broadcast soccer video“, *Image and Vision Computing*, Vol. 24, No. 10, pp 1146-1162, 2006.

[8] M.K. Johnson, H. Farid: „Exposing digital forgeries by detecting inconsistencies in lighting“, *ACM Multimedia and Security Workshop*, pp 1-10, 2005.

Konferencija o bezbednosti informacija BISEC 2014
Univerzitet Metropolitan

BEZBEDNOST MOBILNIH PLATFORMI, PAMETNIH UREĐAJA I KOMUNIKACIJA

SECURITY ISSUES OF MOBILE PLATFORMS, SMART DEVICES AND COMMUNICATION

NEBOJŠA P. TERZIĆ
Telekom Srbija a.d. Beograd, nebojsa.terzic@telekom.rs

Rezime: *Svakoga dana sve više ljudi u svetu a i kod nas koristi personalni računar, laptop, navigaciju u automobilu, ali ni jedan uređaj na svetu nije ušao u svaku poru ljudskog života kao što je to uradio mobilni telefon. Prepoznajući tu činjenicu, proizvođači mobilnih telefona odavno više ne nude samo opciju pukog biranja broja, već široki spektar mogućnosti, koje su mobilni telefon pretvorile u pametan ili smart uređaj. Zbog svih tih prednosti ovog pokretnog uređaja, koji koristi toliko veliki broj ljudi, bilo je neizbežno da on postane meta kriminalaca. Veoma je veliki broj kriminogenih radnji vezanih za ove uređaje. Od najobičnije krađe telefona, koje počine nisko obrazovani kriminalci, pa do sofisticiranih hakerskih napada urađenih od strane visoko obrazovanih i inteligentnih ljudi. Ovaj rad će obuhvatiti sve do sada poznate vidove napada i ponuditi bezbednosna rešenja.*

Ključne reči: *presretanje komunikacije, napad posrednika, zlonamerni programi, trojanci, prisluskivanje*

Abstract: *Every day more and more people in the world and in our country uses a personal computer, laptop, navigation in the car, but no device in the world has not entered into every pore of human life as it the mobile phone did. Recognizing this fact, mobile phone manufacturers has no longer offered only the simple dialing a number option, but a wide range of options, which are mobile phone turned into a clever or a smart device. Because of all these advantages of a mobile device, which is used by so many people, it was inevitable that he becomes the target of criminals. A very large number of criminogenic activities are related to these devices. From ordinary phone stealing, committed by under-educated criminals, to the sophisticated hacker attacks done by the highly educated and intelligent people. This work will cover all aspects of the currently known attacks and provide a security solutions.*

Keywords: *packet sniffing, man in the middle attack, malware, trojan, spying*

1. UVOD

Nalazimo se u periodu razvoja čovečanstva gde informatičku kulturu više ne smemo razdvajati od opšte kulture i opštu pismenost od informatičke pismenosti.

Smatra se da na planeti Zemlji živi sedam milijardi ljudi, a da šest milirajdi ljudi ima mobilni telefon, a prema izveštaju Ujedinjenih Nacija trenutno u svetu postoji jedan presedan, koji kako stvari stoje teško da će uskoro biti prevaziđen, a to je da više ljudi u svetu poseduje mobilni telefon, nego pristup čistom toaletu.

Dakle na osnovu ovoga može se reći da je mobilni telefon postao nešto bez čega se više ne može zamisliti normalno funkcionisanje čoveka.

U evolucionom smislu počeci ili ono što bi se reklo komercijalna primena mobilnih telefona, vezana je za Japan i 1979. godinu. Američka firma IBM, 1994. godine pravi uređaj, kombinaciju mobilnog telefona i personalnog računara i naziva ga Personal Digital Assistant (PDA) koji u sebi ima Palm OS, preteču operativnog sistema za mobilne uređaje. Američka firma Microsoft, 2002. godine pravi prvi mobilni računar, poznatiji kao Tablet, sa operativnim sistemom Windows XP Tablet.

Od 2002. godine pa na ovamo, razvijaju se pametni uređaji sa operativnim sistemima: BlackBerry, iPhone/iOS i Android.

Mogućnosti ovih uređaja su ogromne. Sa pametnim uređajem se sada može ostvariti snimanje i reprodukovanje audio i video sadržaja visokog kvaliteta. Svi vidovi komunikacije putem interneta (pristup sajtovima, mejl nalozima, socijanim mrežama, elektronsko poslovanje, plaćanje računa, kupovina). Video pozivi, VoIP (Voice over IP) pozivi, instaliranje i deinstaliranje korisničkih aplikacija, skladištenje velikih količina raznih vrsta podataka, GPS navigacija, Wi-Fi i Bluetooth komunikacija i još mnogo toga.

Činjenica je, a toga su veoma svesni i kriminalci, da je veliki broj korisnika pametnih uređaja nedovoljno upoznat sa načinom rada, mogućnostima, i komunikacijom uređaja sa spoljnim svetom. Zbog toga je i dijafazon kriminogenih radnji vezanih za ove uređaje veliki.

Počev od krađe pametnog uređaja, koja bi se mogla svrstati u posebnu grupu napada i kojom se ovde nećemo baviti, pa do presretanja bežične komunikacije pametnog uređaja, izrade i širenja zlonamernog softvera za mobilne

platforme i prisluškivanja pametnog uređaja. O svemu ovome će u daljem tekstu detaljno biti reči.

2.PRESRETANJE BEŽIČNE KOMUNIKACIJE PAMETNOG UREĐAJA

Korisniku pametnog uređaja ponuđeno je da internet komunikaciju ostvari preko usluge EDGE ili 3G mobilnog provajdera ili preko WiFi bežične mreže.

Usluge EDGE i 3G mobilni provajderi dodatno naplaću, a sa druge strane WiFi bežične mreže su uglavnom otovrenog tipa, besplatne su, omogućavaju veće brzine i široko su dostupne.

WiFi signali se mogu naći na centralnim gradskim trgovima, tržnim centrima, kafićima i sl. Što veliki broj korisnika pametnih uređaja obilato koristi.

U normalnim okolnostima, pametni uređaj uspostavi komunikaciju sa WiFi ruterom koji ga povezuje sa internetom.

Slika 1: Standardna WiFi komunikacija

Sa druge strane, uz pomoć takozvanog *Napada posrednika* (eng. Man In The Middle Attack - MITM), koji se satoji u tome da haker, koristeći bezbednosne propuste WiFi rutera, pristupi ruteru uz pomoć laptopa ili svog pametnog uređaja i sa posebnim programom prati i snima sav paketni saobraćaj koji prolazi kroz ruter. Ovo se ujedno zove *pasivna varijanta napada*, uz pomoć koje haker može preuzeti vaše cookie i pristupiti vašem mejl nalogu ili videti vaše korisničko ime i lozinku za pristup forumima.

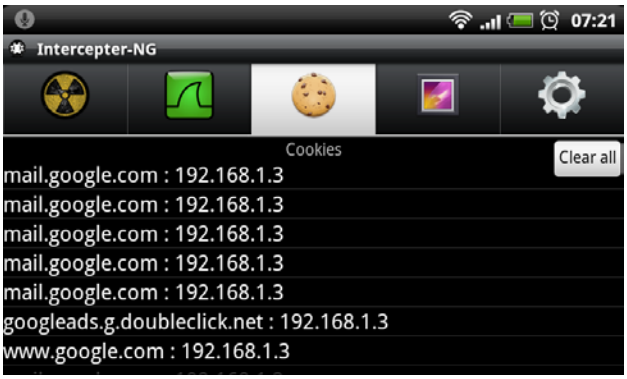
Slika 2: Napad posrednika – pasivna varijanta

Za razliku od pasivne, *aktivna varijanta napada* se sastoji u tome da haker, pošto je presreo vaše pakete, uz pomoć posebnog programa, izmeni odgovor koji očekujete u vidu internet stranice ili nekog drugog upita (npr. izveštaja iz banke), ubacivanjem drugog teksta, slike ili Javascript naredbe u povratni paket ka pametnom uređaju i time korisnika dovede u zabludu.

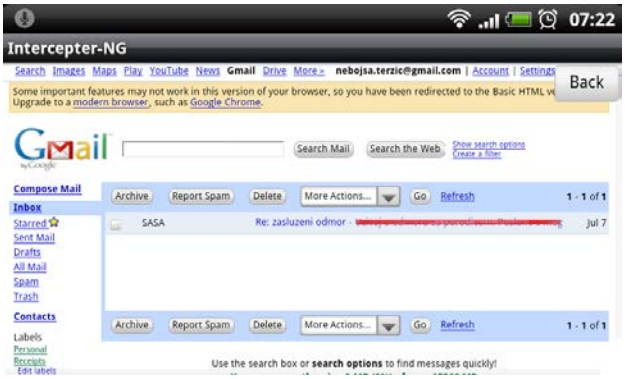
Slika 3: Napad posrednika – aktivna varijanta

Programi sa kojima se vrši napad posrednika se relativno lako mogu naći na internetu, kao i tekstualna i video uputstva za njihovo korišćenje, što za posledicu ima da veliki broj osoba i sa manjim informatičkim znanjem mogu izvoditi ove vidove napada, a time se povećava i broj potencijalnih žrtava.

Na sledećem primeru se vidi kako uz pomoć pasivne varijante napada posrednika i posebnog programa, haker presreće Gmail pakete, cookie i pristupa mejl nalogu.



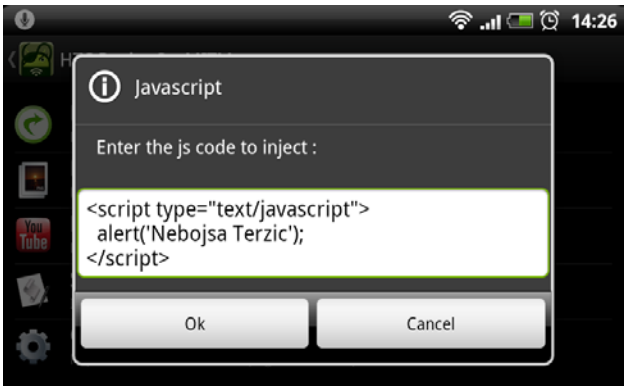
Slika 4: Preuzimanje Gmail cookie



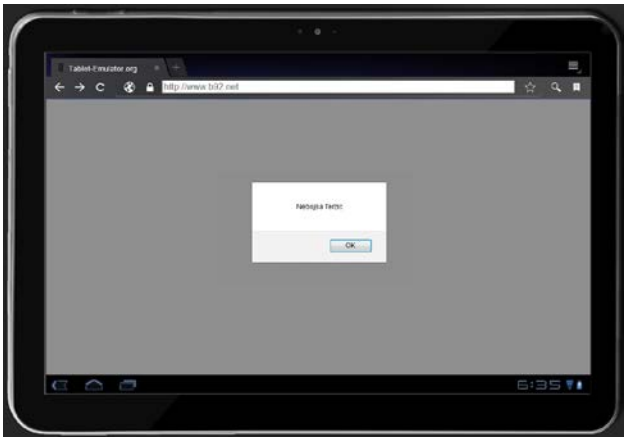
Slika 5: Pristupanje Gmail nalogu

Pasivnom varijantom se takođe mogu preuzeti i korisnički nalozi foruma. I to sajtova koji koriste samo HTTP protokol, bez obzira da li se radi o GET ili POST metodi prilikom logovanja, zato što su paketi u komunikaciji pametan uređaj WiFi ruter za hakera transparentni.

U aktivnoj varijanti napada posrednika, haker presreće paket u kome vidi da korisnik želi pristup nekom određenom sadržaju i kao povratni paket umesto pravog sadržaja ubacuje svoj sadržaj, pa čak i Javascript naredbu koja ce se izvršiti na pametnom uređaju korisnika.



Slika 6: Javascript naredba koja će se izvršiti



Slika 7: Naredba se izvršava na pametnom uređaju korisnika

Da bi se zaštitili od *Napada posrednika*, potrebno je pridržavati se sledećih pravila:

- Ako je moguće izbegavati javne bežične mreže
- Pristupati nalozima preko HTTPS protokola (podesiti opciju)
- Instalirati Anti-Virus aplikaciju
- Koristiti 3G mrežu mobilnog provajdera prilikom prenosa poverljivih podataka
- Ograničiti pristup u okviru svoje bežične mreže (filtriranje po MAC adresi)

3. IZRADA I ŠIRENJE ZLONAMERNOG SOFTVERA ZA MOBILNE PLATFORME

Prema statističkim podacima International Data Corporation (IDC), Wikipedia, Mobilnisvet i Kaspersky, najveću zastupljenost na tržištu imaju pametni uređaji koji poseduju Android mobilnu platformu (operativni sistem), za njim sledi Windows, BlackBerry i Symbian koji nekada lider sada polako odlazi u istoriju.

Slična je situacija i po broju modela, kao i po broju korisničkih aplikacija koje se mogu naći na tržištu.

Tabela 1: Statistika

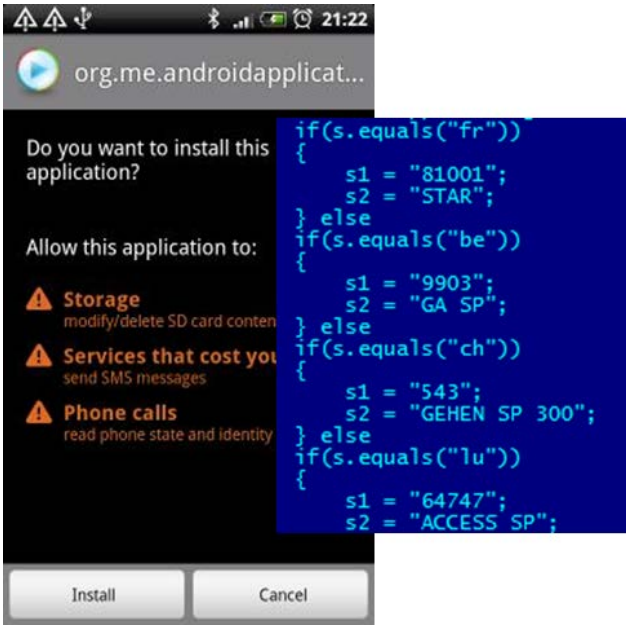
	Zastupljenost	Ponuda modela	Broj aplikacija	Meta napada
Android	75%	>200	>800.000	98,96%
iPhone	17,3%	<10	>900.000	1%
Windows	3,2%	<10	>160.000	
BlackBerry	2,9%	<15	>100.000	
Symbian	0,6%	<40	--	0,04%

Sve to za posledicu ima da su pametni uređaji sa Android operativni sistem ubedljivo najčešća meta napada hakera.

Dalje statistike pokazuju da se u skoro 80% slučajeva zlonamerni softver inastalira uz pomoć tojanca, naizgled legitimnih aplikacija koje u pozadini pokreću zlonamerni softver. U ostalim slučajevima korisnik usled neznanja ili greškom instalira trojanca.

Trojanci se mogu najčešće naći u igricama, uslužnim aplikacijama, kao i u aplikacijama za poboljšanje rada sistema i bezbednosti, a načini širenja su preko ne akreditovanih izvora, a neretko i preko Google Play marketa.

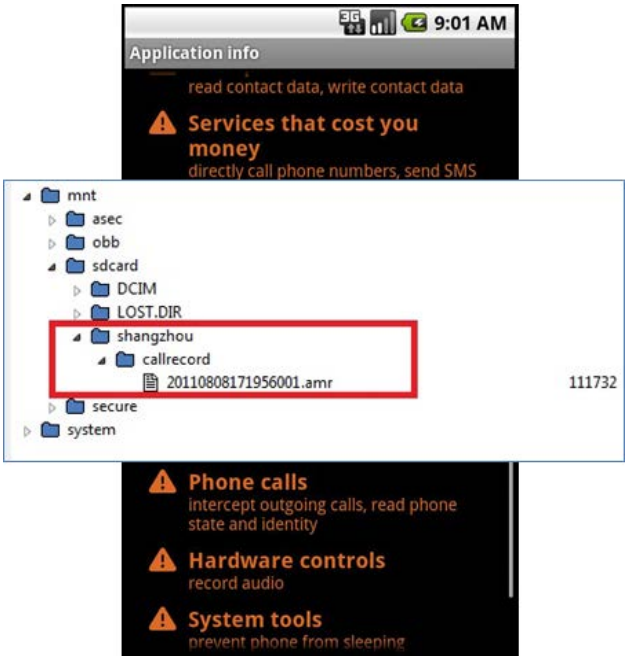
Kreativnošću i znanjem autora za posledicu imao veliki broj pod grupa zlonamernog softvera. To su najčešće aplikacije koje šalju SMS poruke po posebnim tarifama,



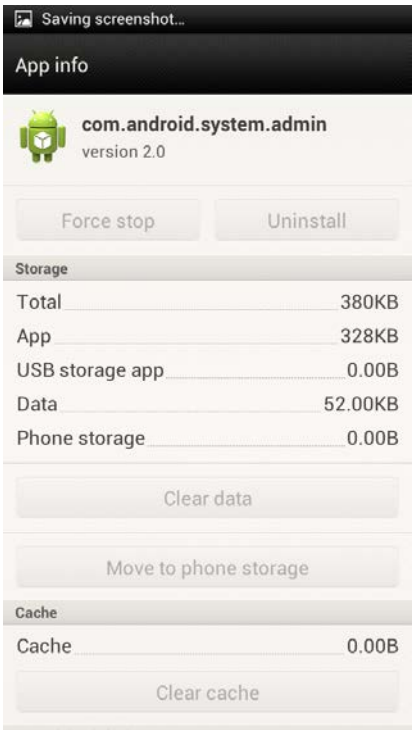
Slika 7a: SMS malware

izbacuju neželjene – dvosmislene reklame, snimaju i šalju razovore i poverljive podatake sa pametnog uređaja na udaljeni računar, aplikacije koje zahtevaju otkup pametnog uređaja i na kraju možda i najopasnije, aplikacije koje u potpunosti preotimaju operativni sistem.

Slika 8: Neželjene – dvosmislene reklame



Slika 9: Snimanje i slanje poverljivih podataka



Slika 10: Zlonamerni softver (ne može deinstalirati)

Mere zaštite od zlonamernog softvera za pametne uređaje bi se sastojale u tome da:

- Ne posećivati i ne preuzimati aplikacije sa foruma ili ne akreditovanih sajtova
- Pre preuzimanja aplikacije sa marketa, pročitati komentare onih koji su je već instalirali
- Prilikom instalacije proverite koja prava traži aplikacija da ima na pametnom uređaju
- Ako je moguće ažuriranjem preuzeti najnoviju verziju Android OS
- Skenirati aplikaciju pre instaliranja Anti-Virus programom

Posebno bih izdvojio kao najvazniji faktor u zaštiti od zlonamernog softvera, informatičku pismenost korisnika, jer bez toga svi ostali vidovi zaštite gube smisao.

4. PRISLUŠKIVANJE PAMETNOG UREĐAJA

Na početku treba razdvojiti prisluškivanje pametnog uređaja koje obavljaju bezbednosne strukture države i koje je regulisano zakonima i prisluškivanje koje obavljaju lica koja za to nemaju dozvolu.

Prisluškivanje pametnog uređaja od strane bezbednosnih struktura, kao što je BIA se obavlja preko brendiranih uređaja koje prave specijalizovane firme i podaci o tim uređajima su teško dostupni ali posto se ovaj vid prisluškivanja obavlja u zakonskim okvirima o njemu u ovom radu neće biti reči.

Sa druge strane neovlašćeno prisluškivanje pametnog uređaja, kao kriminogena aktivnost, se obavlja uz pomoć opreme manjeg dometa, koja se najčešće proizodi u Rusiji i Americi, a može se kupiti preko interneta. Oprema se takodje može napraviti i u kućnoj izradi uz pomoć lako dostupnih delova za koje se detaljna dokumentacija može naći na intrentu.

Cena takvog uređaja se kreće već od 650€ plus laptop koji je neophodan zbog snimanja razgovora i komunikacije koju obavlja pametni uređaj. Prisluškivanje se obavlja uz pomoć softvera koji je javno dostupan na internetu i koji je otvorenog tipa (open source).

Na osnovu razotkrivenih slučajeva koji su objavljeni u javnosti, neovlašćenim prisluškivanjem se najčešće bave kriminogene grupe radi ucena, medijske kuće radi dobivanja eksluzivnih informacija i povećanja tiraža i pojedinci iz emotivnih razloga (ljubomore).

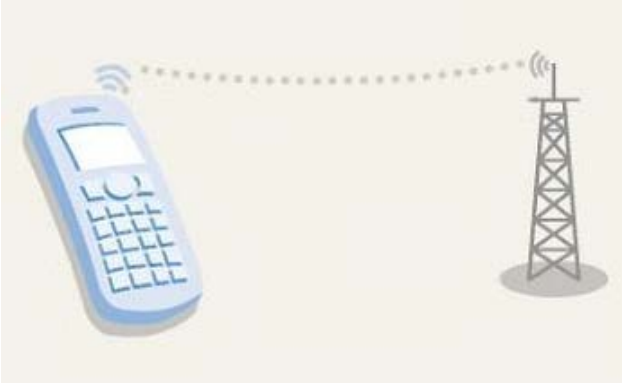
Postoje dve vrste prisluškivanja pametnog uređaja, *pasivno* i *aktivno* prisluškivanje.

Pasivno prisluškivanje se sastoji od snimanja razgovora, SMS poruka i prikupljanja podataka o pozivu (ko je zvat, koliko je trajao poziv).

Aktivno prisluškivanje pametnog uređaja, pored mogućnosti koje pruža pasivno prisluškivanje, omogućava i ometanje određenog pametnog uređaja, uključivanje mikrofona na pametnom uređaju, zvanje ili

slanje SMS poruke sa broja koji se prisluškuje i menjane SMS poruke „u letu“.

U normalnim okolnostima, pametni uređaj se povezuje na baznu stanicu koja ima najjači signal.



Slika 10: Povezivanje pametnog uređaja na baznu stanicu

Koristeći tu činjenicu, haker sa svojim uređajem, koji je u blizini pametnog uredjaja, ne većoj od stotinak metara, jačinom svoje antene se nameće kao najjači signal i pametni uređaj njega bira umesto prave bazne stanice.

Slika 11: Princip prisluskivanja pametnog uređaja

Uređaj za prisluškivanje se zatim predstavi baznoj stanici kao pametni uređaj korisnika i započinje snimanje svih aktivnosti pametnog uređaja.

Primarna zaštita od prisluškivanja bi se sastojala u tome da korisnik pametnog uređaja koristi isključivo 3G mrežu mobilnog provajdera jer je 3G standard bolje koncipiran po pitanju zaštite od prisluškivanja.

Sekundarna zaštita podrazumeva da se koristite aplikacije za kriptovanje razgovora i na strani korisnika i na strani osobe sa kojom korisnik pametnog uređaja komunicira.

5. ZAKLJUČAK

Posle svega prikazanog nameće se zaključak da postoje velike šanse da će svako od nas, jednog dana na ovaj ili na onaj način postati meta hakera.

Da li ovaj zaključak treba da nas zabrine? Odgovor je NE! Jer ako idemo tom logikom onda ne bi trebalo da izlazimo napolje da se ne bi razboleli ili da ne sedamo u auto jer mozemo da imamo udes.

Zapitaj te se ili što bi se stručnom terminologijom reklo uradite svoj bezbedonosni profil sa pitanjima:

- Da li, ako ste osoba koja poseduje važne informacije, morate te informacije da držite na pametnom uređaju?
- Da li preko javnih mreža morate da proveravate stanje na svom bankovnom računu?
- Da li morate da instalirate aplikacije nepoznatih autora?
- Da li poverljivu komunikaciju morate obavljati preko pametnog uređaja, a ne u četri oka?

Dakle, preventiva, informatička pismenost i saveti dati u ovom radu mogu vas i vaš pametni uređaj u velikoj meri zaštiti od napada hakera.

LITERATURA

[1] Man-in-the-middle attack https://www.owasp.org/index.php/Man-in-the-middle_attack

[2] Intercept the planet! http://intercepter-ng.blogspot.ru/

[3] IDC, *Android and iOS Continue to Dominate the Worldwide Smartphone Market*, Framingham, 2014.

[4] SMS Trojans: all around the world http://www.securelist.com/en/blog/208193261/SMS_Trojans_all_around_the_world

[5] The most sophisticated Android Trojan https://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

[6] Chris Paget, *DEFCON 18: Practical Cellphone Spying*, Las Vegas, 2010.