Zbornik radova
sa nacionalne konferencije

KONFERENCIJA BISEC 2012

IV KONFERENCIJA O BEZBEDNOSTI INFORMACIJA

Izdravanje ovog zbornika pomoglo je
Ministarstvo prosvete i nauke

Univerzitet Metropolitan
Beograd, 27. jun 2012.

Izdavač
UNIVERZITET METROPOLITAN
Tadeuša Košćuška 63, Beograd
E-mail: info@metropolitan.edu.rs;
http://www.metropolitan.edu.rs

Za izdavača
Prof. dr Dragan Domazet

Urednik
Prof. dr Nedžad Mehić

Zbornik priredila
Nina Kovačić

Programski Odbor Konferencije

Prof. dr Dragan Domazet
Prof. dr Miodrag Mihaljević
Prof. dr Nedžad Mehić
Prof. dr Zoran Savić
Doc. dr Miroslava Raspopović
Doc. dr Snežana Vulović
Mr Mateja Opačić
Mr Boris Stevanović

Organizacioni Odbor Konferencije
Nina Kovačić
Jelena Samardžić

Lektura i korektura
Nina Kovačić

Prelom i dizajn
Petar Cvetković

Štampa
.....

Tiraž
100

SADRŽAJ

RADOVI DOSTUPNI SA WEB SAJTU KONFERENCIJE WWW.BISEC.RS

Konferencija o bezbednosti informacija BISEC 2012
Univerzitet Metropolitan

DETALJAN UVID U SAP SIGURNOST

SAP SECURITY IN DEPTH

GORAN RAOVIĆ
Atos IT Solutions and Services, Beograd, goran.raovic@atos.net

---

Rezime: *Ovaj dokument analizira kako se SAP sigurnost menjala tokom zadnjih godina i daje uvid šta organizacije moraju da učine da bi ostale u skladu sa novim sigurnosnim izazovima u ERP svetu.*

Ključne reči: *Informaciona bezbednost, SAP, testiranje sigurnosti software-a, SoD, Atos*

Abstract: *This document analysis how SAP security has been changing over last few years and gives an insight to organisations of what they need to do with SAP security in order to stay ahead of the real threads in ESP security.*

Keywords: *Information security, SAP, penetration testing, SoD, Atos*

1. UVOD

Globalno 1000 najbogatih kompanija, velike državne institucije i odbrambene agencije imaju nešto zajedničko, većina njih koristi SAP kao biznis alat za kritične procese i informacije. Glavni poslovni procesi kao što su prodaja, proizvodnja, HR menadžment i finansijsko planiranje su procesirani i upravljani od strane SAP software-a.

Kritični poslovni sistemi postaju sve više atraktivni za sajber (cyber) kriminalce i sajber teroriste; ako bi maliciozni korisnik mogao da kompromituje SAP sistem od neke organizacije, to bi mu pružilo mogućnost za špijunažu, sabotiranje i finansijske prevare sa veoma jakim uticajem na sam biznis.

2. SAP SIGURNOST

2.1 SAP sigurnost pre pet godina

U SAP sigurnosti pre oko pet godina jedino se govorilo o pravima korisnika na SAP sistemu. Glavna odlika dobro podešenih sigurnosnih pravila bila je da jedan korisnik nema mogućnost kompletne kontrole celog biznis procesa. Takva paradigma i način podele pravila po korisnicima naziva se "Sagregation of Duties controls (SoD)". Ovim načinom podele privilegija sve kritične operacije na samom SAP sistemu podeljene su između više korisnika i ovim je smanjena mogućnost da jedan korisnik izvrši zlonamerne aktivnosti u okviru sistema.

2.2 Zaboravljeni sloj

Iako je SoD jedan od najznačajnih aspekata SAP sigurnosti, on nije jedina komponenta u SAP-u kojom se obezbeđuje sigurnost.

SAP biznis aplikacije se pokreću u izuzetno kompleksnom framework-u, poznatim pod nazivon NetWeaver, ili BASIS komponente (Biznis Infrastruktura). Biznis Infrastruktura je zadužena za poslove kao što su autentifikacija korisnika, autorizacija korisničkih aktivnosti, interfejs između sistema, enkripcija i dekripcija osetljivih podataka..

Sigurnost u ovom sloju najčešće se preskače u toku SAP implementacije i ovaj sloj sigurnosti uglavnom SAP implementatorima predstavlja još jednu barijeru u implementaciji projekta u zadatim rokovima. Još jedan razlog zašto se ovo zanemaruje kao dodatni nivo sigurnosti je i činjenica da je većina konsultanata smatrala da su SoD pravila dovoljan nivo sigurnosti.

Na BlackHat 2007 konferenciji demonstrirano je da je SAP sigurnost mnogo kompleksnija i mnogo šira od dobrog podešavanja SoD pravila. Demonstrirano je kako framework arhitektura na kojoj se pokreću SAP aplikacije takođe može biti podložna napadu i da takvim napadima napadač može da dobije kompletan pristup SAP sistemu. Time zlonamerni korisnik može da izvrši napade kao što su špijunaža, sabotaža i prevare u SAP aplikaciji.

2.3 Različiti tipovi napada

Postoje dva modela napada na SAP sistem, prvi je napad na SoD pravila dok drugi napad predstavlja napad na Biznis infrastrukturu.

Napadi na SoD ranjivosti.

- Napadaču je potreban validan nalog na napadnutom SAP sistemu.
- Napadač pronalazi veće priviligije na sistemu nego što mu je po pravilima dozvoljeno i na taj način dobija pristup osetljivim informacijama za koje nema prava.
- Standardni auditing alati otkrivaju ovaj tip propusta.

Napadi na Biznis Infrastrukturu

- Napadač ne mora da ima validan korisnički nalog na sistem
- Nakon uspešnog napada, napadač može da dobije SAP_ALL privilegije i time dobija kompletnu kontrolu nad SAP sistemom
- Standardni auditing alati i metode ne otkrivaju ovaj tip ranjivosti

Kao što se može primetiti, napadi na Biznis infrastrukturu imaju dosta prednosti u odnosu na napade na SoD pravila; ovi napadi zahtevaju manje znanja o napadnutoj platformi, imaju veći uticaj i teže se detektuju.

2.4 Porast pretnji

Broj prijavljenih SAP sigurnosnih propusta raste dramatično u zadnjih par godina.

Pre pet godina broj objavljenih SAP sigurnosnih biltena bio je 90, sa tendoncijom od 20 prijava po godini.

Od 2007. broj SAP sigurnosnih biltena i zakrpa počeo je da raste u nepredvidivom broju. Ovo je rezultiralo da je broj objavljenih sigurnosnih biltena i update-a bio 1900 do Februara 2012., sa prosečnih 600 prijava po godini.

Razlozi za dramatičan rast broja SAP sigurnosnih ranjivosti su sledeći:

- Povećano interesovanje IT sigurnosnih stručnjaka za tematiku ERP sigurnosti.
- Lakši pristup SAP sistemima.
- Povećana aktivnost SAP stručnjaka oko poboljšanja sigurnosti svog software-a.

U ovom scenariju kompanije se susreću sa velikim problemima:

- Potrebno je da razumeju koji sigurnosni patchevi štite njihove kompleksne sisteme.
- Komplikovanost kod određivanja kojim SAP sistemima nedostaju pojedini sigurnosni patchevi
- Teškoća da se prioritizuje implementacija patcheva i razumevanje rizika koji nosi taj sigurnosni problem
- Potrebno je uložiti mnogo vremena za implementaciju potrebnih sigurnosnih patcheva, u to se uključuje odgovarajuci QA (quality-assurance) da bi se smanjila mogućnost narušavanja postojećeg biznis procesa.

3. SAP SISTEMI NA INTERNETU

Pre deset godina veoma malo SAP sistema moglo se naći online. Danas moderni biznis zahteva da se pojedini elementi SAP sistema pablikuju i budu vidljivi korisnicima, zaposlenima i vendorima. Ovim se naravno povećava rizik, kao i broj potencijalnih napada.

Kako je sve veći broj SAP sistema konektovan na Internet i pruža WEB interfejs prema korisnicima, moguće je dobiti informacije o tom javnom delu SAP sistema preko pretraživača.

3.1 Google

Koristeći google dorks moguće je pronaći SAP WEB-bazirane aplikacije, kao što su ITS services, SAP Enterprise Portal, WEBdynpros i BSP što pokazuje da je SAP aplikativni server konektovan na Internet.

Različite SAP komponente mogu biti pronađene pomoću različitih google dork-a kao što su:

- inurl:/irj/portal (Enterprise Portal)
- inurl:/sap/bc/bsp (SAP Web Application Server)
- inurl: /scripts/wgate (SAP ITS)
- inurl: infoviewapp (SAP Business Objects)

3.2 SHODAN

Shodan je još jedan zanimljiv alat koji nam omogućava da pronađemo SAP online sisteme.

Pretraživač indeksira banere web servera i omogućava da pretražujemo online SAP sistem samo po ključnoj reči SAP.

I ne samo web aplikacije.

U mnogim slučajevima organizacije koje ne publikuju SAP web aplikacije na javnu mrežu, smatraju se sigurnim. Ovo tumačenje je pogrešno.

Kao deo ugovora između SAP-a kao kompanije i korisnika, potrebno je instalirati SAProuter, software koji omogućava SAP-u davanje podrške korisniku.

Konekcija između SAP rutera i SAP-a kao kompanije može biti ostvarena i korišćenjem IPsec tunela, ali većina kompanija ostavlja SAP ruter potpuno vidljiv na Internetu.

4. NAPADI IZ UNUTRAŠNJE MREŽE

Iako omogućavanje pristupa sa Interneta SAP platformi povećava sigurnosne rizike, time što je SAP sistemu omogućen pristup isključivo iz unutrašnje mreže, ne treba smatrati sistem sigurnim, jer ni internu mrežu ne treba tretirati kao potpuno sigurno okruženje.

Velike organizacije imaju na hiljade zaposlenih, outsourcing konsultanata, kontraktora... koji su svakodnevno konekotvani na internu mrežu i mogu se smatrati kao potencijalna pretnja.

U slučaju nedovoljno dobre segmentacije mrežnih resursa kao i loše podele sigurnosnih segmenta u okviru interne

mrežne infrastrukturue, zaposleni mogu direktno da pristupe SAP produkcionim sistemima.

Čak i u slučaju da se SAP sistem nalazi u posebnoj internoj zoni, potrebno je omogućiti SAP Gateway-u pristup SAP sistemu, tu komunikaciju je nemoguće isključiti.

I pored mogućnosti implementacije IPS/IDS rešenja, većina IPS-ova ne poseduje ozbiljnije potpise (signature) za detekciju napada na biznis aplikacije.

Svi ovi scenariji prikazuju koliko je bitno biti potpuno siguran da su SAP sistemi zaštićeni na odgovarajući način.

5. POSTOJECE STANJE U SIGURNOSTI SAP SISTEMA

U istraživanjima nezavisnih *penetration testing* kompanija koje se bave SAP sigurnošću, utvrđeno je da je u više od 95% slučajeva moguće dobiti kompletan pristup sistemu sa SAP_ALL privilegijama.

Samo 5% SAP sistema ima na odgovarajući način podešen audit logova i implementirane najnovije sigurnosne zakrpe.

U većini slučajeva pristup sistemu se dobija korišćenjem ranjivosti starih dve ili više godina.

6. TOP11 SAP RANJIVOSTI

BIZEC je neprofitablina organizacija fokusirana na sigurnost ERP sistema i biznis-kritičnih aplikacija.

U daljem tekstu su dati najveći rizici i njihov uticaj na biznis infrastrukturu:

6.1 BIZEC TEC–01 Korišćenje ranjivog software-a

Rizik:
SAP platforma koristi framework koji ima sigurnosni propust i pri tom nisu implementirne sigurnosne zakrpe.

Uticaj na biznis:
Napadač može da iskoristi propust i dobije pristup svim poslovnim informacijama.

6.2 BIZEC TEC-02 Standardni korisnici sa predefinisanim (default) šiframa

Rizik:
Korisnici koji se kreiraju automatski prilikom SAP instalacije ili neke druge standardne procedure su konfigurisani sa predefinisanim (default) šiframa. Te šifre su javno dostupne.

Uticaj na biznis:
Napadač može da se loguje na SAP koristeći standardni SAP korisnički nalog. Svi ovi nalozi su uglavnom sa visokim privilegijama.

6.3 BIZEC TEC-03: Nesiguran SAP gateway

Rizik:
SAP aplikativni server gateway nema striktno definisana pravila sa kojima eksterni RFC server može da pristupi sistemu.

Uticaj na biznis
Napadač ima mogućnost da dobije punu kontrolu nad SAP sistemom. Dodatno ima mogućnost da presreće i manipuliše sa osetljivim poslovnim informacijama.

6.4 BIZEC TEC-04: Nesigurna SAP/Oracle autentifikacija

Rizik:
Autentifikacija SAP Aplikativnog servera sa Oracle Database serverom zasniva se na poverenju između ovih sistema, a pristup Oracle Listener-u nije restriktivan.

Uticaji na biznis
Napadač može da dobije kompletnu kontrolu nad bazom podataka i time utiče na SAP sistem tako što može da kreira, briše i menja podatke korišćene u SAP sistemu.

6.5 BIZEC TEC-05: Nesigurni RFC interfejs

Rizik:
SAP sistemi poseduju nesigurnu RFC konekciju između sistema sa manjom sigurnosnom klasifikaciom i sistema sa većom sigurnosnom klasifikacijom.

Uticaj na biznis:
Napadač može da izvrši RFC pivoting napad; time što dobije administratorske privilegije na sistemu sa manjim sigurnosnim nivoom, napadač može bez većih problema da pristupi sistemima koji imaju veći nivo sigurnosne klasifikacije.

6.6 BIZEC TEC-06 Nedovoljni sigurnosni i audit logovi

Rizik:
SAP sistemski audit logovi su isključeni ili nisu konfigurisani na odgovarajući način.

Uticaj na biznis:
Korisnik nema mogućnost detekcije bilo kojih sumnjivih aktivnosti ili napada na SAP sistem. Pored toga, korisne informacije o sistemu neće biti kasnije na raspolaganju za detaljniju sigurnosnu analizu.

6.7 BIZEC TEC-07 Nesigurni SAP message serveri

Rizik
Na SAP message server nije restriktovno podešeno koji aplikativni server može da se registruje.

Uticaj na biznis
Napadač može da registruje maliciozni SAP aplikativni server i time izvrši man-in-the-middle napad i dobije pristup osetljivim informacijama kao što su korisnički nalozi i password-i na sistemu.

6.8 BIZEC TEC-08: Opasne SAP WEB aplikacije

Rizik
Ako je SAP aplikativnom serveru dozvoljen pristup WEB aplikacijama koje imaju određene ranjivosti.

Uticaj na biznis
Napadač može biti u mogućnosti da iskoristi ranjivosti na takvoj web aplikaciji i time na posredan način utiče na podatke koji će biti učitani na sam SAP server.

6.9 BIZEC TEC-09 Nezaštićen pristup prema SAP administratorskim servisima

Rizik
Na SAP aplikativnom serveru nije urađena kontrola pristupa osetljivim administrativnim i monitoring alatima.

Uticaj na biznis
Napadač ima mogućnost da pristupi administrativnim i monitoring servisima i izvrši neautorizovane aktivnosti na SAP sistemu.

6.10 BIZEC TEC-10 Nesigurno mrežno okruženje

Rizik
Mrežno okruženje gde se nalazi SAP sistem nije zaštićeno na odgovarajući način kroz implementaciju firewalla, Intrudion Prevention Sistema i aplikativnih gateway-a.

Uticaj na biznis
Napadač bi mogao da dobije pristup SAP servisima i iskoristi ranjivosti ili nesigurne konfiguracije na serverima. Na kraju, napadač može da postigne neautorizovan pristup celom SAP sistemu.

6.11 BIZEC TEC-11 Nekriptovana komunikacija

Rizik
Komunikacija između komponenata u okviru SAP sistema nije kriptovana. Pod ovim se podrazumeva komunikacija između samih SAP servera kao i komunikacija između SAP servera i eksternih sistema i komunikacija između korisnika i SAP servera.

Uticaj na biznis
Napadač može da pristupi osetljivim tehničkim i biznis informacijama koje se prenose od i prema SAP sistemu.

7. ZAŠTITA SAP PLATFORME

Znanje

SAP se sastoji od velikog broja izuzetno kompleksnih komponenti, pri tom svaka komponenta ima svoje osobenosti i drugačiju sigurnosnu arhitekturu.
Posedovanje specifičnog znanja za svaku SAP komponentu je veoma važno da bi bili sigurni da je sistem zaštićen na odgovarajući način.

Obim

Mnoge organizacije štite veoma limitirani deo SAP platforme: tipično su to glavni produkcioni serveri i klijenti koji pristupaju produkcionim sistemima.

Kako bi postigli zaštitu SAP infrastrukture potrebno je osigurati komplentnu SAP infrastrukturu uključujući sve instance SAP sistema kao i sve klijente koji pristupaju SAP komponentama. Jedan propust na bilo kojoj komponenti SAP-a može da ugrozi bezbednost celog SAP sistema.

Periodičnost

Sigurnost u SAP okruženju je izuzetno dinamična. Sa jedne strane, SAP konstantno izbacuje nove Sigurnosne preporuke koje treba da omoguće zaštitu SAP sistema od poznatih ranjivosti. Sa druge strane, SAP administratori, podešavanjem raznih parametara na SAP sistemu, mogu da utiču na stvaranje novih propusta.

Sigurnost SAP sistema mora biti proveravana periodično, najmanje nakon implementacije svake SAP sigurnosne zakrpe, i time bi se verifikovalo da li se pojavio novi rizik i proverila sigurnost koju donosi sigurnosna zakrpa.

7. SAP SIGURNOST – KO JE ODGOVORAN?

Za razliku od drugih IT sistema ili aplikacija kao što su LDAP serveri, WEB serveri, Domen kontroleri itd., u mnogim organizacijama SAP aplikaciji spadaju u biznis okruženje koje nije direktno u nadležnosti ljudi iz IT-a.

Zbog toga u većini kompanija SAP sigurnost predstavlja podešavanje SoD pravila i testiranje istih – da li su u skladu sa kompanijskim standardima.

Iako je prihvatljivo da je u kompanijama SAP tim odgovoran za sigurnost SAP sistema, veoma je važno da lokalni Information Security Manager i odeljenje za IT zaštitu verifikuje sigurnost SAP sistema i proveri da li sigurnost odgovara definisanim sigurnosnim standardima kompanije.

8. ZAKLJUČAK

Bazirano na sprovedenim istraživanjima, većina SAP implementacija nisu zaštićene na odgovarajući način i većina instalacija je izložena visokorizičnim napadima. Većina kritičnih vektora napada omogućava napad na samu biznis infrastrukturu i sam framework SAP-a. U većini slučajeva za uspešan napad nisu potrebni kredencijali na SAP platformi.

LITERATURA

[1] M. Linkies, F. Off , *SAP Security and Authorizations*, SAP PRESS, 2006.

[2] Deloitte ToucheTohmatsu Reasch Team and Issaca, *Securi, Audit and Control Features SAP ERP 3rd, Isaca 3rd Edition 2009*.

Konferencija o bezbednosti informacija BICES 2012
Univerzitet Metropolitan

BEZBEDNOSNI ASPEKTI POSLOVNE PRIMENE INTERNET DRUŠTVENIH MREŽA

SECURITY ASPECTS OF INTERNET SOCIAL NETWORKING

ZORAN SAVIĆ
Fakultet za menadžment, Novi Sad, savicz@famns.edu.rs

Rezime: *Internet društvene mreže, kada se koriste u poslovne svrhe, mogu da donose neke pozitivne poslovne efekte, ali i nove rizike. Pozitivni efektii se ogledaju u mogućnosti kreiranja novih poslovnih prednosti u odnosu na konkurenciju, najčešće u vidu kreiranja novih kanala komunikacije sa postojećim i potencijalnim klijentima. Rizici su mogućnost postavljanja neprikladnih sadržaja, zlonamerni programi koji mogu da naprave određenu štetu, kao i nekontrolisano zadržavanje i brisanje važnih poslovnih informacija.Iako su društvene mreže, u odnosu na elektronsku poštu i klasičan web, relativno novo sredstvo za komunikaciju i upravljanje informacijama, one zahtevaju istu pažnju i sistem upravljanja bezbednošću informacija.*

Ključne reči: *Društvene mreže, bezbednost informacija*

Abstract: *Internet social networks, when used for business, can bring some positive effects, but also new risks. Positive effects are the possibilities of creating new channels of communication with both existing, and new clients. The risks are possibilities of adding inappropriate contents, malware that can cause certain damage, as well as uncontrolled saving and deleting of relevant business information. Although social networks are, in comparison to e-mail and classic web, a relatively new mean of communication and information management, they demand the same attention and information safety management system.*

Keywords: *Social networks, information security*

1. UVOD

Popularnost društvenih mreža stalno raste, sada sve više i među poslovnim korisnicima, bilo da je u pitanju međusobno povezivanje stručnjaka iz određene oblasti, praćenje potreba korisnika, marketinške aktivnosti, poboljšanje prodaje itd.

Korišćenje socijalnih mreža na odgovarajući način može da neposrednim korisnicima, ali i organizacijama, donese brojne koristi. Korisnici imaju stalan izvor aktuelnih informacija, mogućnost saradnje i razmene mišljenja sa drugim osobama unutar i van organizacije.

Organizacije mogu da organizuju praćenje stavova potencijalnih i aktuelnih klijenata, kupaca ili korisnika usluga, da bi ojačale svoje relacije sa njima i obezbedile sebi lidersku poziciju u određenom tržišnom segmentu.

Analiza, ili "mining", društvenih mreža je postala standardna poslovna praksa. Koriste je organizacije iz oblasti osiguranja, u cilju otkrivanja mogućih prevara, kao i organizacije koje se bave ljudskim resursima. Objave (postovi) na društvenim mrežama se već koriste i kao dokazni materijal u sudskim postupcima.

Za razliku od klasičnih reklamnih sajtova, koji se zasnivaju na analizi ponašanja i navika korisnika, društvene mreže dozvoljavaju direktan pristup informacijama o tome šta se korisnicima dopada ili ne dopada, a te informacije eksplicitno postavljaju sami korisnici. Mlađe generacije korisnika imaju prilično neobavezan stav prema poverljivosti informacija koje se objavljuju na društvenim mrežama, što predstavlja idealnu podogu za marketinške aktivnosti, ali i za različite zloupotrebe.

Pored nespornih benefita za organizaciju, korišćenje društvenih medija donosi i određene rizike. Prvo, korisnici mogu, slučajno ili namerno, da odaju neke poverljive poslovne informacije. Postovi tipa "još jedan sastanak u Novom Sadu", mogu konkurenciji da ukažu na neke poslovne pregovore i sl. Drugo, korisnici mogu da postavljaju sadržaje sa neprikladnim ili uvredljivim sadržajima, kojima se narušavaju neke zakonske ili moralne norme, ili organizaciona pravila ponašanja, a što u svakom slučaju može da dovede organizaciju u neku neugodnu situaciju. Treće, određeni sadržaji društvenih medija mogu da predstavljaju neke poslovne podatke koji zahtevaju čuvanje, u skladu sa zakonskim ili organizacionim normama, ali to se iz različitih razloga možda ne radi.

Rastom poslovnog značaja društvenih mreža, rastu i zahtevi vezani za bezbednost, kako ličnih podataka, tako i poslovnih informacija organizacije, objavljenih na njima.

2. INTERNET DRUŠTVENE MREŽE

U svetu postoji veliki broj sajtova društvenih mreža, ali *Facebook*, *Twitter* i *LinkedIn* dobijaju najviše medijske pažnje upravo zbog ogromnog broja individualnih i poslovnih korisnika (prijatelja - *friends*, sledbenika ili pristalica - *followers*, povezanih članova - *connections*).

Facebook je imao 687.1 miliona korisnika u junu 2011. godine, sa mesečnim rastom od 1.7% [1]. Marta 2011. godine, *LinkedIn* je imao 79.2 miliona posetilaca, odnosno 65.3% više u odnosu na prethodnu godinu [2]. *Twitter* je nešto teži za analizu, ali jedna analiza iz februara 2011. godine pokazuje da od 175 miliona naloga, njih 119 miliona je pratilo jedan ili više drugih naloga, a 85 miliona naloga ima bar jednog pratioca [3].

Pored ovih najpoznatijih, među značajnijim internet društvenim mrežama su *Sina Weibo* iz Hong Konga (140 miliona korisnika, sredinom 2011. godine), *Orkut* kompanije *Google* (37 miliona naloga), i *Cyworld* iz Južne Koreje (više od 20 miliona korisnika u 2010. godini) [4,5,6].

Kao svoje osnovne karakteristike, *Facebook* je na početku imao mogućnost dodavanja prijatelja, ažuriranja sopstvenog statusa (profila) i korišćenja određenih aplikacija (igrica i kvizova). "Prijatelj" je bilo ko na toj mreži, kome je dozvoljeno da vidi različite lične informacije (datum rođenja, zanimanje, fotografije, komentare), kao i listu ostalih prijatelja. Na vrhu korisnikovog profila je polje za dodavanje komentara na bilo koju temu, linkova, fotografija i video materijala. Poruke tipa "Kupili nov LED TV !" ili "jedva čekam sledeći vikend zbog porodičnog izleta u Budimpeštu", su vrlo česte i izgledaju bezopasno, ali je putem tih poruka svim prijateljima, kao i prijateljima prijatelja, objavljeno da za vikend neće biti niko kod kuće, a potencijalnim provalnicima i šta od vrednih stvari može da se nađe u kući.

Facebook nudi na hiljade aplikacija koje korisnika može da instalira i pokrene na svom računaru, a mnoge od tih aplikacija su kreirali krajnji korisnici. Iako je većina njih bezopasna, neke od tih aplikacija mogu da sadrže i štetne sadržaje.

Twitter je on line aplikacija koja omogućuje korisniku objavljivanje kratkih komentara o nekoj temi (*tweets*), dok ostali korisnici te mreže mogu da postanu pristalice, koje će redovno pratiti te komentare.

Korisnici moraju da budu veoma pažljivi kada su u pitanju lične ili poslovne informacije koje se objavljuju u tim komentarima. Poslodavci posebno moraju da obrate pažnju na to, kakav uticaj objavljivanje tih informacija može da ima na organizaciju. Na primer, svaka od sledećih poruka:
"Vlasnik je upravo otpustio 10 radnika "
"Priča se da će nas kupiti XYZ"
"Radimo na otklanjanju greške u našem softveru, koju smo upravo pronašli",
može da ima ozbiljne poslovne, odnosno finansijske posledice po organizaciju, čiji članovi na nekoj od društvenih mreža objavljuju te informacije.

3. BEZBEDNOSNI RIZICI

Potencijalni rizici kod korišćenja društvenih mreža su:

- virusi, trojanci, crvi, špijunski programi i ostali zlonamerni programi
- krađa identiteta (zbog objavljivanja veliki količine ličnih podataka)
- gubitak privatnosti (neki sajtovi dozvoljavaju pokretanje aplikacija koje imaju pristup korisničkom profilu)
- nenamerno otkrivanje poverljivih informacija
- zavisnost
- gubitak reputacije, itd.

Društvene mreže mogu, na različite načine, da unesu u organizaciju različite tipove zlonamernih programa. To su, na primer, *Koobface* – crv koji prikuplja login informacije radi kreiranja botnet mreža i čiji cilj je prvenstveno Facebook, ali i Twitter, MySpace i druge društvene mreže; *Boonana* – trojanac, pisan u Javi, koji funkcioniše slično, ali je usmeren na Mac računare; *Bugat* – trojanac, povezan sa keystroke-logging malware Zeus, korišćen u phishing napadu protiv LinkedIn.

Masovno korišćenje socijalnih mreža dovelo je do toga da se pojavljuje sve više poruka elektronske pošte kojima se pozivaju potencijalni prijatelji ili pristalice, da se pridruže određenom profilu. Neke od tih poruka mogu da sadrže i zlonamerne sadržaje, odnosno programe, koji mogu da nanesu štetu korisnikovom računaru i reputaciji.

Potencijalnu pretnju predstavlja i skraćivanje dugačkih URL adresa, koje se postavljaju kao linkovi na društvenim mrežama, a do koga dolazi zbog želje za uštedom u prostoru predviđenom za poruku. Na primer, adresa od 64 karaktera se "kodira" u adresu od 25 karaktera, mnogo pogodniju za kucanje u prostoru za poruke koje imaju ograničen broj karaktera (*TinyURL*). Međutim, ovako skraćena, ili kodirana, adresa ne govori ništa o pravoj destinaciji tog linka, sve dok se ne otvori ta strana, a što može da bude već kasno. Zbog toga, nikad ne treba kliknuti na ovako skraćene adrese ako se nalaze u spam porukama ili na sumnjivim sajtovima.

Brojni su primeri koji govore o odgovornosti i problemima u koje su dovedene organizacije zbog neprikladnog korišćenja društvenih mreža od strane svojih članova.

Objavljivanje informacija o pacijentima na Facebook-u od strane zaposlenih u jednoj bolnici u Kaliforniji, ili objavljivanje na *MySpace* mreži, jednog zaposlenog u bolnici na Havajima, kako jedna osoba ima HIV [7], ili objavljivanje rezultata lokalnih izbora u Nemačkoj na *Twitteru* pre zatvaranja birališta [8], su primeri nekontrolisanog odliva poverljivih informacija.

Jedna službenica u SAD je otpuštena sa posla pošto je na svojoj *Facebook* stranici napisala (po njenoj izjavi - u šali) da je bila zavisnik od droga i alkohola [9].

Po jednoj sudskoj odluci u SAD, ustanovljen je presedan da su poslodavci odgovorni za ono što njihovi zaposleni objavljuju na mreži.

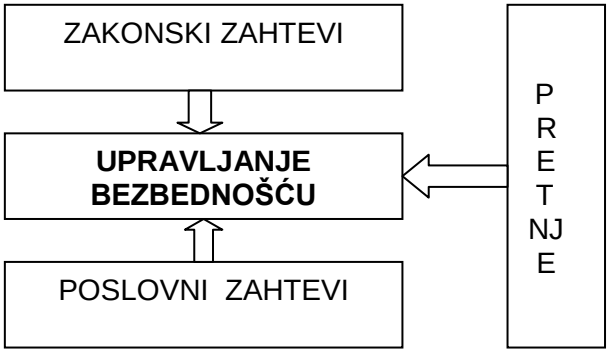
Različite agencije i ministarstva u SAD su objavilli uputstva o čuvanju sadržaja objavljenih na društvenim medijima, izjednačavajući ih sa svim drugim medijima.

4. ZAŠTITA

Naglo prihvatanje društvenih mreža od strane organizacija, dovelo je do toga da su one manje zaštićene od već uhodanih komunikaconih kanala, kao što je elektronska pošta, na primer. Skoro 12% srednjih i velikih organizacija u SAD su bile žrtve zlonamernog softvera, dok je 9% organizacija imalo problem namernog ili slučajnog gubitka informacija putem društvenih mreža ili drugih Web 2.0 aplikacija [10].

Sve to govori da se korišćenje društvenih mreža mora na neki način kontrolisati, bilo putem postojećeg, ili izgradnjom novog sistema za upravljanje informacionom bezbednošću u organizaciji,

Očigledno je da na strukturu upravljanja bezbednošću informacionih sistema u organizaciji, pored pomenutih pretnji, u velikoj meri utiču zakonski zahtevi i zahtevi poslovnog okruženja, koji iako dolaze iz različitih sredina, imaju mnogo zajedničkog u smislu upravljanja bezbednošću (Slika 1.).

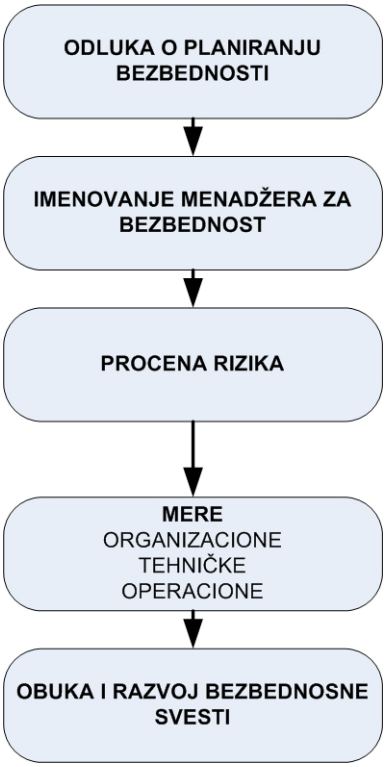


Slika 1.: Uticaji na sistem za upravljanje bezbednošću

Da svi ovi uticaji bili na pravi način obrađeni, neophodno je formirati jednu formalnu strukturu za upravljanje bezbednošću informacionih sistema, unutar zadatih okvira. Struktura bezbednosti informacija se sastoji od niza međusobno povezanih elemenata, koji zajedno čine efikasnu odbranu protiv spoljašnjih napada i unutrašnjih nezgoda i prekršaja.

Na Slici 2. je prikazan predlog modela organizacionog aspekta strukture bezbednosti informacionih sistema, u koji može da se uklopi i bezbedno korišćenje društvenih mreža [11].

Organizacione mere su pretežno usmerene na preventivno delovanje, odnosno na donošenje pravilnika o bezbednosti informacija, uputstava i standarda, koji se sprovode putem operacionih procedura, radi ispunjenja ciljeva i misije organizacije.



Slika 2.: Model organizacione strukture bezbednosti IS

Sam termin, *pravilnik*, može da bude različito tumačen. Obično se pod bezbednosnim pravilnikom podrazumeva formalna izjava najvišeg rukovodstva o pravilima, po kojima moraju da se ponašaju ljudi koji imaju pristup tehnološkim i informacionim resursima organizacije, o ciljevima i merama za postizanje tih ciljeva u određenoj oblasti. U tom smislu, u literaturi može da se nađe i termin *politika bezbednosti*.

Najčešći i najočigledniji razlog za razvoj jednog formalnog pravilnika je zakonska obaveza. Sve je veći broj zakonskih obaveza koje se pojavljuju u oblasti bezbednosti informacija. Proces prenošenja zakonskih odredbi i usaglašavanje ponašanja organizacije sa njima, najefikasnije se obavlja pravilnicima za bezbednost informacionih sistema.

Usaglašenost pravilnika sa propisima je odgovornost čitave organizacije, a sprovodi je informatički deo organizacije. Zakonodavci su jasno naglasili da pravilnik ima smisla, samo ukoliko komunicira sa svim zaposlenim u organizaciji i ugrađen je u sve obavezne obuke zaposlenih, tako da očekuju da se može dokazati, na neki način, da su svi zaposleni pročitali pravilnik.

Nedostatak efikasnog bezbednosnog pravilnika može da potkopa i najbolje tehničke mere zaštite. Ako korisniku nije rečeno, da je instaliranje nepoznatog programa prekršaj bezbednosnog pravilnika organizacije, od male pomoći je najbolji antivirusni program, instaliran na granicama mreže. Ako ne postoji bezbednosni pravilnik koji zabranjuje korisnicima posetu neodgovarajućim sajtovima, od male pomoći je najbolji softver za zaštitu od

zlonamernih internet sadržaja. Korisnici će i dalje raditi loše stvari, a niko neće imati autoritet da ih zaustavi.
Rezultat toga je da svaka organizacija mora da:

1. razvija pravilnike o korišćenju društvenih mreža (definisanje prihvatljivog i neprivatljivog ponašanja)
2. primenjuje tehničke mere za kontrolu i sprečavanje aktivnosti zlonamernog softvera
3. vrši nadzor nad sadržajem postova, u cilju sprečavanja odavanja poslovnih tajni, narušavanja zakonskih ili etičkih normi, rasne ili seksualne diskriminacije itd
4. vrši arhiviranje sadržaja društvenih medija, zbog eventualnih budućih dokaznih postupaka, u slučajevima narušavanja pravila ponašanja.

Istraživanja pokazuju da je primena tehničkih mera, generalno prihvaćena od strane velikog broja organizacija, ali relativno mali broj organizacija ima uređena pravila kada je u pitanju korišćenje društvenih medija [10,12]. Više od 40% ispitanih organizacija nije imalo nikakav pravilnik ni za jednu društvenu mrežu (Tabela 1).

Tabela 1: Postojanje pravilnika o korišćenju druš. mreža

	Postoji detaljan pravilnik	Postoji osnovni pravilnik	Ne postoji nikakav pravilnik
Facebook	18%	41%	41%
Twitter	18%	38%	44%
Linkedin	16%	38%	46%

Nedostatak pravilnika o načinu korišćenja društvenih mreža u organizaciji, dovodi poslodavca u situaciju da preuzima odgovornost za ponašanje svog zaposlenog osoblja, odnosno za sadržaje koje oni postavljaju na društvenim mrežama, a otežava mu i kažnjavanje zaposlenih za neodgovarajuće ponašanje.

Pored toga, nedostatak detaljnih pravilnika dovodi organizacije u problem i kada je u pitanju implementacija određene tehnologije za umanjenje bezbednosnih rizika.

Zbog toga, rukovodstvo organizacije, zajedno sa IT službom, treba da sprovede temeljnu evaluaciju korišćenja društvenih mreža (ko ih koristi, zašto ih koristi i koji se alati koriste). Analiza treba da obuhvati buduće potrebe, kao i ponašanje konkurencije kada su u pitanju društveni mediji. Na osnovu takve analize, određuje se da li se korišćenjem društvenih mreža može postići konkurentska prednost na određenom tržištu.

Ona može da pokaže i razliku u stavovima, kada je u pitanju legitimno korišćenje društvenih mreža, između korisnika iz poslovnih jedinica (ljudski resursi, marketing, zaposleno osoblje) sa jedne strane, i IT sektora, koji najčešće vodi računa o bezbednosti, sa druge strane. Cilj je da se izbalansiraju interesi obe navedene grupe, da bi se ostvarili maksimalni poslovni rezultati, a istovremeno ispoštovali organizacioni bezbednosni pravilnici.

Sledeći korak je razumevanje problema i mogućih konsekvenci koje mogu da nastanu u slučajevima neodgovarajućeg korišćenja društvenih mreža. Na primer, pritužbe zaposlenih, koji na društvenim mrežama komentarišu uslove rada, u nekim zemljama ne smeju da budu blokirane. Poseban problem su multinacionalne organizacije, koje posluju na teritorijama sa različitim propisima.

Brisanje zapisa sa socijalnih mreža se može okarakterisati i kao uništavanje dokaza u sudskom postupku. Ako menadžment organizacije nije sačuvao Twitter poruke sa , na primer, uznemiravajućim seksualnim sadržajem, oštećena strana može u sudskom postupku da traži pristup arhivama postova, koje moraju biti dostupne. U suprotnom, organizacija može da bude odgovorna za uništavanje dokaza, kažnjena i izložena dodatnim sudskim troškovima

Jedna od mogućnosti, koja se koristi kada je u pitanju kontrola korišćenja društvenih medija, je ograničavanje određenih njihovih funkcija, posebno kada su u pitanju funkcije u domenu finansijskih usluga, poslovi investicionih savetnika itd, čiji rad je definisan određenom zakonskom regulativom.

Zbog toga se moraju preduzeti mere u cilju zaštite i same organizacije i zaposlenih u organizaciji.

Ne postoji jednostavno rešenje, ukoliko organizacija ne želi da se, zbog bezbednosti, odrekne mogućnosti koje donosi korišćenje društvenih mreža i potpuno zabrani njihovo korišćenje..

Jedna od mogućih organizacionih mera je implementacija *Pravilnika o prihvatljivom korišćenju* – dokumenta koji detaljno opisuje načine korišćenja društvenih mreža, kao i konsekvence u slučaju nepridržavanja tim pravilima, koje mogu da se kreću od pisane opomene, preko otkaza, do sudskog postupka. Svaki pravilnik treba da je usaglašen sa organizacionom kulturom i kadrovskom strukturom organizacije.

Svi sistemi koji pristupaju internim ili eksternim mrežama i resursima su vlasništvo organizacije, pa u skladu sa tim i njihovo korišćenje treba da bude samo za odobrene namene. Ljudi moraju da budu upozoreni na zabranu korišćenja ili trošenja tih resursa, ako je ono na štetu organizacije. Ovo je jedan od ključnih pravilnika za svaku organizaciju, pa bi svi korisnici trebali da ga pročitaju i potpišu, kao dokaz da su upoznati sa njegovim odredbama. Zbog toga treba da je što eksplicitniji, da bi se izbeglo nerazumevanje ili različita tumačenja.

Bez ovakvog pisanog pravilnika, menadžment nema na šta da se osloni, ukoliko želi da kazni zaposlenog, koji narušava bezbednost računarskog sistema. Generalno, ovaj element bezbednosnog pravilnika izuzetno pomaže prilikom bilo kojih zakonskih aktivnosti, koje sprovodi organizacija, ili koje su uperene protiv organizacije.

Osoblje treba ohrabrivati u nameri da se familijarizuje sa bezbednosnim pravilnicima organizacije i sa time u vezi, novim odgovornostima, koje se javljaju, a vezane su za

obavljanje njihovog posla. Zaposlenima moraju da budu jasne bezbednosne mere koje se od njih očekuju i koje treba da preduzimaju kao deo svog posla, da bi se obezbedila efikasna zaštita informacija.
Pravilnik treba da bude fokusiran na postizanje odgovarajućeg balansa između slobode komuniciranja zaposlenih putem društvenih medija, poslovnih benefita od korišćenja društvenih medija, zakonske regulative i poslovne prakse. On mora da pomogne zaposlenima da razumeju rizike kojima su izloženi i kao pojedinci, posebno kada je u pitanju njihova privatnost i da ih upozorava na opasnost od objavljivanja informacija o brojevima telefona, adresi, rođendanima itd, kao i na opasnost od dodatnih aplikacija koje mogu da prikupljaju lične informacije.

Pravilnici o korišćenju društvenih mreža treba da su sastavni deo pravilnika o korišćenju komunikaconih sredstava, kao što su elektronska pošta, Webmail, instant poruke itd, jer upozoravaju na rizike od kontaktiranja sa potpunim strancima putem društvenih mreža i na lažne poruke elektronske pošte, koje treba da predstavljaju poruke od socijalnih mreža, sa problematičnim linkovima.

Pravilnici treba da razlikuju različite pozicije i vrste komunikacije koje mogu da postoje u organizaciji (eksterno-interno, formalno-neformalno, itd).

Treba da sadrže jasne stavove o onome što je nedozvoljeno (seksualna ili rasna diskriminacija, neodgovarajuće slike ili linkovi na nepodobne sajtove, klevete, narušavanje autorskih prava, objavljivanje tuđih ličnih podataka, itd.) Jasno i uz razumno objašnjenje moraju da se navedu alati koji se ne mogu koristiti (određeni sajtovi, pametni telefoni itd),

Pravilnici moraju jasno da izraze i pravo menadžmenta organizacije da vrši kontrolu komunikacije zaposlenih putem društvenih medija, kao i da, u određenim situacijama, na određeni način reaguje na određeni sadržaj.

Posebno treba obratiti pažnju na "vlasništvo" kada su u pitanju sledbenici ili prijatelji sa društvenih mreža osoba koje su u međuvremenu napustile organizaciju.

Pravilnici treba da sadrže i kaznene za nepridržavanje odredbama pravilnika.

I pored ovakvog pravilnika, organizacija može da ima problem i sa kućnim korišćenjem društvenih mreža od strane zaposlenih, gde je svaka reakcija na neadekvatno ponašanje uglavnom zakasnela.

Primenjene tehničke mere treba da:
- vrše nadzor (naknandni ili u realnom vremenu) nad objavljenim sadržajima
- blokiraju zlonamerne programe koji mogu da uđu preko društvenih mreža (zbog kratkih URL adresa ili mogućnosti da svoj sadržaj postavi i neautorizovana osoba)
- arhiviraju relevantne sadržaje.

U cilju sprečavanja moguće štete potrebno je koristiti ažurnu verziju klijentskog programa za elektronsku poštu, sa aktiviranim filterom za spam i proverom potencijalnih "phishing" poruka kao i ažuran antivirusni softver, u cilju blokade svih zlonamernih sadržaja, odgovarajući i funkcionalni *firewall* i instalirati i pokretati aplikacije koje dolaze iz sigurnih izvora, ili su proverene od strane IT službe.

Većina organizacija integriše arhiviranje sadržaja društvenih mreža sa drugim elektronskim arhivama organizacije. Način arhiviranja u velikoj meri zavisi i od delatnosti organizacije i drugih faktora. Generalno je lakše jednostavno arhivirati sav sadržaj društvenih medija, nego rizikovati da neke važne poslovne informacije nestanu. Ključni deo čuvanja sadržaja društvenih medija je njegovo povezivanje sa identitetom korisnika

Povećana svest o problemima bezbednosti i odgovarajućim procedurama, ne samo da smanjuje rizik od mogućeg bezbednosnog incidenta, nego i povećava verovatnoću da će sumnjive aktivnosti biti prijavljene i preduzete odgovarajuće mere.

Svo trenutno i potencijalno zaposleno osoblje, treba da bude upoznato sa bezbednosnim pravilnikom organizacije, isto kao što su upoznati sa sopstvenim poslovnim funkcijama. Praktično, vremenom to treba da postane jedinstveni proces – razvoj svesti o bezbednosti informacija, u sklopu redovnog posla zaposlenih, odnosno da bezbednost informacije bude sastavni deo ponašanja svakog radnika, a na taj način i deo korporativne kulture. To će uticati na smanjenje broja bezbednosnih incidenata i smanjenje rizika njihovog nastanka.

5. ZAKLJUČAK

Upravljanje društvenim mrežama – gledajući broj korisnika, kao i poslovne potencijale, ne može da bude zanemareno od strane menadžmenta organizacija različitog profila.

Društvene mreže donose i potencijalne rizike organizacijama, bez obzira na njihovu veličinu i oblast delatnosti. Rizici su upadi zlonamernih programa, koji mogu da naprave finansijsku ili drugu štetu organizaciji, postavljanje sadržaja kojima zaposleni mogu da nanesu štetu poslodavcu, kao i brisanje zapisa koji su neophodni radi zadovoljavanja zakonskih i drugih obaveza.

Svaka organizacija, bez obzira da li sankcioniše korišćenje društvenih mreža, mora da definiše detaljna pravila o tome kako i kada društvene mreže mogu da budu korišćene. Na kraju, svaka organizacija treba da, u skladu sa svojim potrebama, a u cilju umanjenja rizika, proceni i potrebu za korišćenjem određenih tehničkih rešenja za kontrolu sadržaja društvenih mreža.

U tome značajno može da pomogne implementacija odgovarajućeg pravilnika o korišćenju društvenih mreža.

Pravilno informisan korisnik, ne samo da doprinosi bezbednosti, nego pomaže i u obuci drugog osoblja, doprinosi povećanju nivoa svesti o bezbednosti, kao i uspostavljanju odgovarajućih procedura i standarda.

LITERATURA

[3] Inside Facebook Gold, *http://gold.insidenetwork.com/facebook/*

[4] comScore Media Metrix

[5] http://www.businessinsider.com/chart-of-the-day-how-many-users-does-twitter-really-have-2011-3

[6] http://www.clickz.com/clickz/news/2078304/sina-weibo-marketers-social-business

[7] http://www.orkut.com/About?page=keep

[8] http://www.google.com/hostednews/afp/article/ALeqM5jTk-b8UadVNyPiEILD-tnjHIv34g?docId=CNG.fe1d0589886b23ad62bffe61357001df.21

[9] *Privacy Rights Clearinghouse (http://www.privacyrights.org/data-breach)*

[10] http://www.hollywoodreporter.com/news/germany-probes-twitter-election-data-88306

[11] http://www.courthousenews.com/2010/05/24/273.htm

[12] *The Risks of Social Media and What Can be Done to Manage Them*, Osterman Research white paper, June 2011.

[13] Savić, Z., *Organizacioni pristup postavljanju formalne strukture bezbednosti IS*, Fakultet za menadžment, Novi Sad, 2005.

[14] Savić, Z., *Istraživanje stanja bezbednosti IS u domaćim organizacijama*, BISEC 2010.

CYBER SECURITY: ON SOME CURRENT ISSUES AND PROSPECTIVES

SAJBER BEZBEDNOST: O REALNOSTI I PERSPEKTIVAMA

MIODRAG MIHALJEVIĆ

Mathematical Institute, Serbian Academy of Sciences and Arts, Keneza Mihaila 36, Belgrade,
miodragm@turing.mi.sanu.ac.rs

Rezime: *Daje se ilustrativan rezime nekih masivnih sajber napada koji ukazuju na rastuci znacaj sajber bezbednosti. Diskutuju se elementi vezani za edukaciju, istrazivanja, razvoj i opsti organizacioni okvir od interesa za sajber bezbednost. Istice se da jedna komponenta naseg privrednog razvoja moze da bude vezana za resavanje aktuelnih i perspektivnih problema sajber bezbednosti..*

Ključne reči: *Informaciona bezbednost, sajber bezbednost, saber napadi, edukacija, istrazivanja, poslovanje, pravni okvir.*

Abstract: *An illustration of massive cyber attacks is given which indicates a high imortance of cyber security. A number of elements regarding education, reserach, development, implementation and legal issues regarding cyber security are discussed. It is pointed out that different acivities within cyber security could be a prospektive economy topics.*

Keywords: *Information security, Cyber Security, Education, Research, Business, Legal Issues.*

ILUSTRATIVNE REFERENCE

[15] United States Patent US 8023649: M.J. Mihaljevic and J. Abe, *Method and apparatus for cellular automata based generation of pseudorandom sequences with controllable period*, 2011.

[16] Japan Patent JP 4863283: M.J. Mihaljevic and H. Watanabe, *Authentication system using light-weight authentication protocol*, 2011.

[17] China Patent CN 1698306: M.J. Mihaljevic and J. Abe, *Data processing method,*, 2010.

[18] Japan Patent JP 4432350: M.J. Mihaljevic and J. Abe, *Data Processing Method, Program Thereof, Data Processor, and Receiver*, 2010.

[19] United States Patent US 7502941: L. Michael and M.J. Mihaljevic, *Wireless data communication method and apparatus for software download system*, 2009.

[20] M.J. Mihaljevic, S. Gangopadhyay, G. Paul and H. Imai, "State Recovery of Grain-v1 Employing Normality Order of the Filter Function", *IET Information Security*, accepted for publication, doi:10.1049/iet-ifs.2011.0107 (accepted for publication).

[21] M. Mihaljevic and H. Imai, "An approach for stream ciphers design based on joint computing over random and secret data", *Computing*, vol. 85, no. 1-2, pp. 153-168, June 2009.

[22] M. Mihaljevic, M. Fossorier and H. Imai, "Security Evaluation of Certain Broadcast Encryption Schemes Employing a Generalized Time-Memory-Data Trade-Off", *IEEE Communications Letters*, vol. 11, no. 12, pp. 988-990, Dec. 2007

[23] M. Fossorier, M. Mihaljevic and H. Imai, "Modeling Block ecoding Approaches for Fast Correlation Attack", *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4728-4737, Dec. 2007

[24] M. Mihaljevic, "Generic framework for secure Yuan 2000 quantum encryption protocol employing the wire-tap channel approach'", *Physical Review A*, vol. 75, no. 5, pp. 052334-1-5, May 2007

Dr Miodrag Mihaljevic je naucni savetnik u Matematickom institutu SANU i njegov osnovni domen interesovanja i rada su kriptologija i tehnike za ostvarivanje zastite informacija i sajber bezbednost.
Dr Mihaljevic je autor vise medjunarodno priznatih patenata, vise od 50 radova objavljenih u vodecim medjunarodnim casopisima i kao poglavlja knjiga i ukupno vise od 100 medjunarodnih publikacija koje su citirane vise od 1000 puta. Dr Mihaljevic je ucestvovao u vise medjunarodnih projekata i odrzava intenzivnu

medjunarodnu saradnju sa Japanom: Sada je po pozivu vodeci istrazivac u "Research Institute for Secure Systems, National Institute AIST", Japan. Njegove ranije gostujuce i aktivnosti po pozivu u Japanu su bile na University of Tokyo (gostujuci profesor), Sony Corporation Laboratories i Research Center for Information Security.

TEKUĆI TRENDOVI U OBLASTI BEZBEDNOSTI INFORMACIJA

CURRENT TRENDS IN THE FIELD OF INFORMATION SECURITY

RADOMIR. A. MIHAJLOVIC
NYIT, P.O. Box 8000, Old Westbury, NY 11568-8000, USA,
email: rmihajlo@nyit.edu

ALEKSANDAR R. MIHAJLOVIC
Technische Universität München, Boltzmannstr. 85748 Garching, Germany,
email: mihajlovic@mytum.de

Rezime: *Ovaj pregledni rad razmatra probleme bezbedniosti informacija koji su trenutno u fokusu pažnje istraživačko razvojnih timova širom sveta. Sa eksplozivnim rastom upotrebe mobilnih telefona i portabilnih računara tipa tablet, u distribuiranim poslovnim sistemima, prirodno prihvatanje privatnih terminalnih uređaja zaposlenih ljudi u skladu sa poslovnom politikom poznatom kao BYOD, dovodi sve računske centre poslovnih i javnih organizacija u situaciju u kojoj se bezbednost informacija i uređaja povezanih sa infrastrukturom računskih centara, bukvalno ne može garantovati. U ovakvoj situaciji intenzivne i teško kontrolisane mobilnosti, maloprodajni prostori bez klasičnih terminala kasa donose nove bezbednosne probleme koji zahtevaju rešenja za podršku ovakvog inovativnog i visoko produktivnog prilaza maloprodaji. Računarski sistemi visokih performansi tipa grid ili računanja u oblačku zasnovani na virtualizaciji računarskih resursa donose potencijalno najopasnije bezbednosne pretnje sa najvećim rizicima a koje bi u realizaciji dovele do najvećih gubitaka. Pored ovih tema, inovacije u areni distribuiranog softvera tipa Web 2.0 sa XML, HTML 5 i Web servisnim tehnologijama praćene nekompletnim standardima su takođe pomenute u ovom radu. Uz sve ovo, vrlo važne teme sajber ratovanja i bezbednog e-upravljanja su takođe predmet ovog kratkog pregleda.*

Ključne reči: *Bezbednost informacija, sajber kriminal, sajber rat, hakerisanje, krekerisanje, SKADA, Stuksnet, kriptovanje, elipitička kriva,multibazni brojni sistem, dupli lanac, RFID, komunikacije bliskim poljem, NFC, virtuelna kartica plaćanja.*

Abstract: *This overview paper elaborates on current information security problems that are in the focus of research and development teams worldwide, as well as on proposed state-of-the-art solutions and those in use today. With the explosive growth of smartphones and tablets used by employees in modern distributed enterprise data processing systems, bring-your-own-device (BYOD) policies are presenting IT departments with the situation where they will hardly be able to guarantee the security necessary to protect data and devices available via enterprise network infrastructure. In addition, mobile computing sales floors without cash registers are bringing another set of security issues, demanding new solutions to support this novel approach to retail. This paper presents some novel and radical ideas to be implemented as mobile computing security solutions. High performance grid and cloud computing (HPC) systems based on virtualization are potential elements of the security arena with the highest possible risks and losses. Special attention to the security problems and solutions relevant to the HPC systems are presented too. New Web advancements such as HTML 5 family of infrastructure products, Web 2.0 and massive networks of Web services, as fairly new technologies, with incomplete standards are also discussed in this paper. Finally, as two essential modern computing application domains that deserve particular attention from the information security point of view, cyber warfare and e-government, are discussed.*

Keywords: *Information security, cybercrime, cyber security, cyber war, hacks, cracks, SCADA, Stuxnet, encryption, elliptic curve, multibase number system, double chain, RFID, near field communication, NFC, virtual payment card.*

1. INTRODUCTION

Various studies such as one performed by ArcSight and HP [1] that have covered a sample of 50 larger US based organizations with more than 700 network nodes, in several industry sectors, indicate that cyber-attack frequency continue to rise causing serious financial losses for targeted businesses and government organizations. The median damage caused by the cybercrime in 2011 was $5.9 million per year, which was 56% higher than the damage reported in the previous year, [1,2].

Annual IT Security and Risk Management investment is on average roughly 5.6% of total IT budget, while approximately 45% of that investment covers infrastructure and applications, disaster recovery and IT risk process management, [3].

2. INFORMATION SECURITY R&D AREAS AND TOPICS

IT infrastructure and application security includes technology, process, and people engaged for the following functions:

- Identity and access management
- Network security
- Endpoint or operating systems security
- Applications or software engineering security, and
- Data Security

R&D work in the area of cyber security revolving around the above mentioned general functions can be classified in several focus-domains according to the current market interest. At the apex of the market and R&D attention in the recent period are areas of:

- mobile computing,
- cloud computing, and
- social networking security.

The other areas fan out of these three focal areas with some R&D topics intersecting with several areas. Topics and interests, range from the economics, socio-technical and pure technological aspects of information security through protocol analysis, to mathematical foundation and provable security.

For instance, a finer grained list of relevant topics can be outlined as follows:

- Mostly technological
    - Access control
    - Authentication
    - Authorization control
    - Accountability
    - Trust and reputation systems
    - Anonymity
    - Privacy
    - Privacy-preserving systems
    - Security and privacy policies
    - Un-traceability
    - Forensics and traceability
    - Hardware security
    - Embedded systems security
    - System security
    - Security architectures
    - Attacks and defense
    - Intrusion detection and prevention
    - Language-based security
    - Application security
    - Protocol security
    - Distributed systems security
    - Security metrics
    - Socio-technical and organizational issues
    - Secure information flow
- Mostly theoretical
    - Symmetric cryptography
    - Public-key cryptography
    - Combinatorial cryptography
    - Computational number theory
    - Pseudo-random sequences
    - Cryptanalytic attacks
    - Lightweight cryptography
    - Cryptographic protocols
    - Key management
    - Applications of cryptography

Some topics, such as attacks and defense, are extremely technological, involving network protocols with packet switching devices, operating systems with hardware platforms, application software architecture and code details, currently available software tools, cryptanalysis, etc. Such topics demand comprehensive expert knowledge and cannot be easily and rapidly mastered.

In the following sections we address just a few areas and/or topics that we consider current higher socio-economic and technical interests. The nature and format of this paper provides limitations within which we take an option of addressing the most pressing and the currently most important information security areas and topics.

3. TRUST AND RISK MANAGEMENT FOR CARD-BASED SYSTEMS

Manual and automatic, physical and virtual card payment and automated subject/user and object/product ident-ification is literally exploding in practical implementation, providing at the same time, a vast space of opportunities for malicious attack. For instance, one

specific topic in this area is advanced transport ticket systems design with most of the world metropolitan public transportation systems being continuously digitized and exposed to tireless offensive and ever more creative forms of attacks.

The massive global applications and potential future use of near field communication (NFC) technologies demands standardization which is accompanied by the complementary R&D efforts. In some discussions, it is well justified to consider NFC devices as virtual smart cards that, like physical equivalents have to be standardized too. For instance, a set of standards for smartphone use to establish close proximity (e.g., few centimeters), radio communication with each other or dedicated device, present an opportunity for implementation in contactless payment transactions or some other sort of commercial application session. Communication between an active NFC device and an unpowered passive NFC integrated electronic circuit, called a "tag" is used in various systems too. NFC standards include protocol sequences and data exchange formats, and are mostly based on existing radio-frequency identification (RFID) solutions and standards. An example of the NFC standard is ISO/IEC 18092 defined by the NFC Forum [4]. Founded in 2004 NFC Forum has more than 160 members which are actively financing relevant R&D efforts. The NFC Forum also certifies compliance of consumer electronics devices and technologies.

To provide easy access to transport and associated services, transportation systems are increasingly employing electronic cards/tickets supported by the IT infrastructure. Over the past decade the technologies used have lagged behind the state-of-the-art and there have been some corresponding deviations from best security practices. The exploits catalogued attacks did highlight the need to, not only adhere to design best practice, but also to the use of physical implementations that can be verified to be tamper-proof and attack resistant. R&D in this direction also emphasizes the value of the back-office transaction processing and the importance of support for forensic and other types of investigation. As we move towards a future with NFC mobile technologies, multiple security elements and powerful parties competing for trust management and ownership roles appear. R&D on electronic card use in mass transportation systems investigates critical aspects of transport ticketing security, including: cryptographic key management, back office processing for security/fraud control, forensics, efficient certification and assurance processes.

4. RFID CARDS OF REDUCED SIZE AND GROUPING PROOF RFID READERS

Radio-frequency identification or RFID tags are small, wireless devices that, as successors to barcoding, help identify objects and people. RFID is the technology of use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking, [5]. Some tags are passive and require no battery and are powered by the wireless energy transferred from the base station used to read them. Others are active and have a local power source and emit high frequency radio waves. The tag contains electronically stored data which can be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

Thanks to dropping costs, RFID tags are proliferating into the billions. RFID tags track items in supply chains, and are working their way into payment cards and other types of cards and even into the bodies of people. Since RFID tags can be attached to human clothing, possessions, or even implanted within people or animal bodies, the possibility of reading personally-linked information without consent has raised privacy concerns. The nature of the RFID technology promises a wide range of benefits but it appears to be accompanied by numerous serious security and privacy related issues, [6]. An eavesdropping attack against an electronic product code (EPC) RFID system using a simple device may be used to record interactions between both RFID Tag and Readers. The device is used to record and decode signals within range and its output may be analyzed to verify that the attack was indeed successful, [7].

There are many theoretical RFID protocols that consider reading individual RFID tags, whereas often in practice one important R&D problem is to read many tags simultaneously and be sure that no tag from a group has been omitted and no genuine tag has been swapped for a 'illegitimate'. Grouping proof research addresses this issue ignoring practical aspects such as tag discovery and anti-collision protocols used commonly by tag readers. [8]

Ultra miniature active RFID tagging based on very small RFID tag is of great interest to many commercial application vendors and R&D teams. However, miniature RFID tags tend to be passive without a power source, and are of very restrictive range where some important tagging applications call for very small, lightweight yet long range active tags. As the power source increases the tag size and weight, and as long distance transmission power could drain a small battery very quickly, this is

quite a challenging direction of R&D effort. Furthermore a long distance tag use would magnify the problem of handling multiple tags, inviting more complex protocols and larger tag sizes.

Various research works in progress are investigating the critical aspects of "card" based payment protocols and standards including:

- The use of contactless/NFC devices as the payment card substitute or virtual payment very smart card.
- Innovations in payment linking with delivery of physical and logical products.
- The Europay-MasterCard-Visa (EMV) payment specifications and defense against attacks.
- Exploration of countermeasures against intrusions such as relay attacks.

Various approaches are proposed and are being investigated for privacy protection and integrity assurance in RFID systems, dealing with the social and technical context.

5. CLOUD COMPUTING DATA PROTECTION

When it comes to the cloud computing the most important problem and question is related to client's data security. To deal with this problem we need to look at different states and processing stages of data and discuss what needs to be done to make data secure. Some possible states of data are:

- Data at rest,
- Data in motion,
- Data in processing, and
- Data lineage

Data at rest are data persistently stored on some storage drive. Since the cloud provider may not be adequately securing data, a client's data can be at risk. The clients of cloud computing services have to realize that in the cloud the logical and physical boundaries between and around the data are gone.

Clients have to make sure that either the cloud computing provider (CCP) has the responsibility to secure client's data or the best available sort of FDE (Full Disk Encryption) is used to secure the data sitting on a drive someplace in the cloud. There are many FDE solutions available in the market and many are under the development currently. There are hardware based full disk encryption solutions as well as software based ones. An interesting example is an encryption solution called "Endpoint Encryption" and offered by Trend Micro, Inc., [9]. Another solution focusing more towards cloud computing and offered by the same vendor is known as "Secure Cloud," [10].

Data in motion as data flowing from one segment to another within the CCP's network, may travel from on provider to another and may travel from the provider to the customer. Having the CCP disclose their policies on the data security of the data in motion is very important. Once the data is inside the cloud then the customer may not have control over the data therefore, applying proper encryption methods is very important. We have to make sure that it is part of the CCP's policy that any motion of data will take place through some sort of encrypted tunnel such as SSL based tunnel.

Data in processing is the toughest state of data to protect. There are not many technologies available that will guarantee the processing of the encrypted data while being processed and the R&D playing field is quite wide here.

Data lineage refers to the origin of the data, the path it traveled through and it's destination. From the security point of view, to keep track of the path of the data is very important. CCP should provide clear policies disclosed about the detailed data lineage.

Data remnants are the residual traces of data if the data has been removed from any computing resource. This is a problem even in the non-cloud environments. The major concern of cloud computing clients is if the data removed are really not removed and remain cached or temporarily stored someplace in the cloud. Cascaded removal of data is one serious cloud security function that R&D has to address.

6. MOBILE COMPUTING SECURITY

Security and privacy in crowd based cloud computing is one active area of R&D. The concept of the crowd based cloud-computing deals with the way in which individual devices in a locality come together in a fluid, dynamic and ubiquitous way to accomplish a task or collection of tasks. It differs from the cloud computing as the service is decentralized and participated by individual devices that advertise their services – in exchange for some services from the requesting entity. Applications of such architectures are in the field of mobile phones, tablets, and sensor networks. Therefore, the research investigates the security, privacy, anonymity, accountability and sharing requirements of such an operational scenario, in order to propose novel protocols that will address security requirements.

Verifying the identity of a user, usually referred to as user authentication, before being authenticated by granting access to the services or objects is a very

important step in many applications and open research field. Recent advances in electronics development offer new opportunities for person authentication based on walking style or gait, using small, light and inexpensive IC sensors.

User authentication based on mobile phones offers multiple possibilities. For instance, modern smart phones have the location tracking GPS ability and motion direction detection based on 3D accelerometer sensor. The research aimed at examining how these mobile phone technologies can be combined, in order to provide the principles of gait based authentication, is one open area.

One of the primary advantages of this approach is that it enables unobtrusive user authentication. Although studies on human recognition based on gait indicate encouraging performances, the security per se (i.e. robustness and/or vulnerability) of gait-based recognition systems has received little or no attention, [11].

It is often the case that mobile devices such as mobile phones are also considered as embedded devices. It is envisaged that increasingly often these devices will be involved in a number of sensitive operations such as payment, social/professional networking, etc. Anonymity techniques for maintaining privacy protection in mobile/embedded systems is receiving a lot of attention. At the same time, enabling these devices to retain anonymity but ensuring fair-exchange of goods and products is also a whole research area by its own. A concept which is closely coupled together with the secure use of these devices (though the use of cryptographic protocols) is related to their ability to generate random numbers. These devices offer a whole new range of sources of randomness. This project aims to explore some of the above security requirements in an attempt to provide efficient and scalable solutions.

The spread and use of mobile devices, has proliferated over the last few years. Bring your own device (BYOD) or own technology (BYOT) refers to the recent trend of employees using personally-owned mobile devices at their place, and using those devices to access privileged company resources such as email, files, and database records. BYOT is a term with broader scope, which not only covers the hardware devices, but also the software used on mobile devices. With regard to new elements of enterprise computing and security, massive R&D effort is directed towards the broad range of new research projects relating to diverse mobile devices, their security and applications. Although BYOD/BYOT devices offer powerful execution and communication capabilities with extraordinary convenience of their portability, their portability poses extraordinary risks.

Research effort attempting to defend easy to lose portable devices are covering the following areas:

- Mobile device malware investigation and the ways in which mobile devices can be infected, subjected to cybercrime and defended.
- Investigation of secure mobile device applications and services development and deployment, (e.g., email, sms, etc.)

7. APPLICAATIONS OF CRYTOGRAPHY

Exponentiation is a mathematical operation, written as b^n, involving two numbers, the base b and the exponent n. Exponentiation is essential in most public key cryptosystems and has been studied extensively in the past. With the advent of composite elliptic curve operations, such as triple and add, it is clear that standard models of execution time are out of date. They simply count the additions and doublings on the curve. The research track in the direction of efficient scalar computation Elliptic Curve Cryptography (ECC) aims at improving the algorithms to generate exponentiation schemes taking into account the different speeds of a much wider range of curve operations, and, in particular, the composite operations, [12, 13].

Message authentication codes (MACs) as fundamentally important cryptographic primitives in secured protocols for over 30 years, remain of vital importance and research interest today. Despite their popularity, their practical use and theoretical results are not synchronized yet. In recent years while a well-developed theory for MACs based on block ciphers exists (e.g., CBC-MACs), schemes favored by theoretical findings have by no means replaced previously used inferior solutions such as the ANSI retail MAC. The older solutions appear to offer a reasonable level of security, which explains their continued use without any formal security proof. Research aiming in that direction seeks to resolve differences between theory and practice by developing the theory and efficient practical and cost effective computation solutions.

Exponentiation cryptographic algorithms in resource constrained environments pose a challenging R&D set of problems. A transparent infrastructure for information access is the backbone for the successful development and deployment of the planned ubiquitous miniaturized mobile applications of the near future. The development of such an infrastructure is a challenge due to the resource constrained nature of the massively used mobile devices or sensor network nodes, in terms of the computational power, storage capacities, wireless communication capacity and battery energy capacity (duration between two recharging instances). For

instance complex queries or complex cryptographic algorithms are hard to execute on handhelds in memory and energy constrained environments. Solving problems in this domain opens many topics for further research.

8. FAULT ATTACKS ON VIRTUAL MACHINES

Fault attack protocols for virtual machines (e.g., JVM), in embedded platforms with processors ill equipped to defend virtualization with compromised or defective code, are subject of advanced security research at several institutes and universities, (e.g., University of London, CMU, etc.).

The concept of introducing fault attacks while cryptographic algorithms are executing in embedded systems and more specifically in smart cards has been studied extensively. At the same time, progressively more embedded devices like smart cards and mobile phones are relying on jailed applications or virtual machines for secure application execution. However, these execution platforms (e.g. Java Card, Globalplatform, Multos, and Android OS) can be subjected to a number of fault attacks in order to bypass the security mechanisms of the underlying platforms. This area of research aims to examine how fault attacks can be combined with logical attacks in an efficient way towards a relatively controlled abuse of the underlying platforms. The main aim of the work involves identifying practical vulnerabilities and more importantly proposing countermeasures, [14].

9. CYBERWARFARE

Cyber warfare is a term used for all efforts, human teams and technologies, organized along nation-state boundaries, in offensive and defensive operations, using computing devices, networks and communications to attack or counterattack other state based target computers or networks through electronic means. Cyber warfare attacks should be capable of disabling official websites and networks, disrupting or disabling essential services, stealing or altering classified data, and crippling financial systems -- among many other possible types of harm aimed at the target country. Since most modern military forces are computing and network-centric and connected to the Internet, which is not secure, not only foreign countries but non-governmental groups and individuals could also launch cyber warfare attacks.

The first cyber war attack launched ever against any nation in the history was the US attack on the electronic infrastructure of the state of Serbia and Montenegro in 1998. To compromise air traffic control of Serbia & Montenegro, and facilitate the bombing of civilian (e.g., public TV stations and broadcast towers), and military targets, the US cyber war forces hacked into Serbia's air defense and communication system. This well documented event of cyber war activities was preceded by the electronic (broadcast) information warfare attack by the same attacker on the same target. Namely, in 1993 the Children's Marathon is held for the first time at the city's centre, Terazije Street. Due to economic and cultural warfare related sanctions and isolation imposed by the U.S., England, Holland and other NATO allied countries upon Serbia and Montenegro, the participants of the marathon race were picked up at the airports of the neighboring countries and transported by land based means to Belgrade, (Capital of Serbia and Montenegro.). As the Belgrade Marathon received support from the entire marathon world community, Romanian born New York City Marathon founder Fred Lebow arrived in Belgrade and symbolically took part in the half marathon race. Despite his terminal illness and the fact that he had less than a year left to live he joined the race and made numerous radio and TV appearances. During the intercontinental satellite TV Belgrade broadcasts, any comments or statements of the late Fred Lebow where blocked by the noise-over played only for the duration of his addresses. Unlike the famous chess player Robert "Bobby" Fischer, Fred Lebow has never been prosecuted for official blockade violation. To be able to intercept and neutralize the voice of Fred Lebow, US cyber war forces had to be able to hack into the Japanese satellite equipment that was serving TV Belgrade.

Initially, hackers and other individual amateurs trained in software programming and exploiting defects and the intricacies of various systems and application software packages and computer networks were the primary executors of these attacks. These individuals often have operated under the auspices and possibly with the direct or indirect support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner with other military units.

Cyber security experts have found a direct link between the recent Flame espionage malware and the infamous Stuxnet worm attack on Iranian nuclear R&D related supervisory control and data acquisition (SCADA), equipment, [15]. Stuxnet computer worm discovered in June 2010 spreads via Microsoft Windows, to Siemens made industrial software and equipment, (e.g., programmable logic controllers or PLCs.) Stuxnet was the first discovered and documented malware that spies on and subverts industrial systems used as a cyber weapon aimed at the foreign country.

Electronic computing and communication equipment and software is becoming a "new center of gravity" in future warfare. Extensive R&D, military and legislative efforts are being made with a focus on issues related to cyber warfare. Nations leading in this area are the U.S., Israel, China, England and Russia.

10. COCNLUSION

This overview work presents a rough outline of the information security areas and topics of current interest of R&D teams and universities. While geared toward the technical specialist, this survey also serves as a reference for some imperfectly documented information and cyber security events and topic classifications.

In conclusion, new Web advancements that are bringing new exploits and security problems with intense interactions on the front end and complex AI algorithms powering the underlined network of Web services on the back end opens another wide research domain that deserves particular attention.

REFERENCE

[1] *Second Annual Cost of Cyber Crime Study; Benchmark study of US companies*, Ponemon Institute, LLC, August, 2011.

[2] *2010 Annual Study: U.S. Cost of a Data Breach*, Research report, Ponemon Institute, LLC, March, 2011.

[3] Jamie K. Guevara, Linda Hall, Eric Stegman

IT Key Metrics Data 2011: Key Information Security Measures: by Industry, Gartner benchmark report, 17 December 2010.

[4] *The NFC Forum*, http://www.nfc-forum.org/aboutus/

[5] Harry Stockman, *Communication by Means of Reflected Power*, Proceedings of the I.R.E. October 1948, pp.1196-1204.

[6] Juels, A., *RFID Security and Privacy: A Research Survey*. IEEE Journal on Selected Areas in Communications, 24(2), 2006, 381-394.

[7] G.P. Hancke, *Eavesdropping Attacks on High-Frequency RFID Tokens*, Proceedings of the 4th Workshop on RFID Security (RFIDsec'08), pp 100–113, July 2008.

[8] Dang Nguyen Duc, Kwangjo Kim, Grouping-Proof *Protocol for RFID Tags: Security Definition and Scalable Construction, Scalable Grouping-proof Protocol for RFID Tags*, 2009/12/9, pp.1-9.

[9] *Data Protection*, Technical spec., Trend Micro Inc., http://www.trendmicro.com/us/enterprise/data-protection/index.html

[10] *Secure Cloud*, Technical note, Trend Micro Inc., http://www.trendmicro.com/us/enterprise/cloud-solutions/secure-cloud/index.html

[11] Davrondzhon Gafurov, *Performance and Security Analysis of Gait-based User Authentication*,

Doctoral Dissertation, University of Oslo, 2008

[12] G.N.Purohit, Asmita Singh Rawat, Manoj Kumar, *Elliptic Curve Point Multiplication Using MBNR and Point Halving*, Int. J. Advanced Networking and Applications, Volume: 03 Issue: 05 2012, pp. 1329-1337

[13] Xu Huang, Pritam Gajkumar Shah, Dharmendra Sharma, *Fast Scalar Multiplication for Elliptic Curve Cryptography in Sensor Networks with Hidden Generator Point*, Proceeding of the 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Pages 243-249

[14] Martin Otto, *Fault Attacks and Countermeasures*, PhD Thesis, Fakult at fur Elektrotechnik, Informatik und Mathematik Institut fur Informatik, Universit at Paderborn, December 2004.

[15] Dave Lee, *Flame and Stuxnet makers 'co-operated' on code*, BBC News, 11 June 2012. http://www.bbc.com/news/technology-18393985

Analiza i ocena rizika u informacionoj bezbednosti
Analysis and evaluation of risks in information security

Stevan Sinkovski, Udruženje e-Razvoj
Konstantin Sinkovski, ETŠ Zemun

Rezime:
U radu se razmatra upravljanje rizicima u sferi informacione bezbednosti. Pored pojma rizika, prikazan je mehanizam rada algoritma analize i ocena rizika. Posebna pažnja je posvećena modeliranju pretnji informacione bezbednosti.

Ključne reči: informaciona bezbednost, rizik, algoritam analize rizika, modeliranje pretnji informacione bezbednosti.

Abstract:
The paper discusses risk management in the sphere of information security. In addition to the concept of risk, shown is a mechanism of algorithm analysis and risk assessment. Special attention is devoted to modeling of information security threats.

Key words: information security, risk, risk analysis algorithm, modeling threats to information security.

1. Upravljanje rizicima

Upravljanje rizicima (*risk managament*) je proces sistematske identifikacije rizika, analiza i ocena njihovih uticaja i izrada i realizacija kompleksnih rešenja za upravljanje njima. Upravljanje rizicima je savremeni pristup u organizaciji biznisa koji obuhvata sve procese u organizaciji povećavajući njihovu efektivnost i rezultativnost. Koncept upravljanja rizicima je našao široku primenu u raznim sferama ljudske delatnosti pa i u upravljanju informacionom bezbednošću (IB). Prema nekim autorima [1], upravljanje informacionim rizicima je sinonim za informacionu bezbednost. Analiza i ocena rizika predstavlja jednu od osnovnih etapa upravljanja rizicima [1,2,3].

Osnovu upravljanja IB čini analiza rizika. **Tehnologija analize rizika** bazira na mnoštvu različitih prilaza u zavisnosti od konkretne situacije. Osnovna pitanja koja se razmatraju pri analize i upravljanju rizicima su:

- identifikacija rizika (pretnji i ranjivosti),
- ocena rizika (skale i kriterijumi, ocena verovatnoće događaja i tehnologija merenja rizika – po dva ili tri faktora),
- izbor dozvoljenog nivoa rizika i
- izbor kontramera i ocena njihove efektivnosti.

Poseban značaj pripada razradi **korporativnih metodologija analize rizika**[1]. Jedna od poznatijih korporativnih metodologija analize rizika je metodologija analize rizika kompanije Microsoft [4].

U postupku analizi rizika se koriste i neka **programska** - instrumentalna **sredstva** (instrumentarij baznog nivoa i softverski paketi za potpunu analizu rizika – CRAMM, RiskWatch, MethodWare, AvanGard, GRIF).

Upravljanje rizicima je tretirano u svim međunarodnim, nacionalnim i korporativnim standardima IB – ISO 17799, ISO 27000, BSI, NIST 800-300, XBSS.

U tekstu koji sledi objašnjeni su pojmovi pretnji i rizika, data je klasifikacija rizika, prikazani su mehanizmi rada algoritama analize rizika, predstavljeni su metodi ocene rizika i dat je metod modeliranja pretnji IB [1,2,3,4].

2. Osnovni pojmovi i klasifikacija rizika

Termin „rizik" je uveo američki ekonomista Frenk Najt 1921. god. i on označava onu neodređenost koja se kvantitativno može izmeriti.

Termin rizik ima mnogo različitih značenja. Neka od njih su:

- verovatnoća nastanka štete ili gubitka, opasnost;
- faktor, elemenat ili bilo šta u čemu je sadržana neizvesna opasnost;
- verovatnoća gubitaka ili povreda, podvrgavanje – izlaganje opasnostima [3].

U kontekstu IT i IB, pojam rizik se koristi u svim navedenim značenjima.

[1] Osnovni faktor od koga zavisi odnos organizacije prema pitanju IB je **stepen njene zrelosti**. Tako, npr. kompanija Gartner Group i univerzitet Carnegie Mellon predlažu svoj model zrelosti kompanija. Različitom nivou zrelosti odgovaraju različite potrebe u oblasti IB. **Model Gartner Group** ima četiri nivoa zrelosti: nivo 0 – problem IB nije ni identifikovan. Služba IB ne postoji; nivo 1 – IB je isključivo tehničkki problem. Služba IB ne postoji. Ne postoje ni organizacione mere zaštite informacija, a ni budžet za IB; nivo 2 – IB je kompleks organizacionih i tehničkih mera. Analiza rizika se provodi na baznom nivo. Postoji politika IB i standardna služba IB. Postoji odvojeni budžet. Koriste se osnovna sredstva zaštite informacija; nivo 3 - egzistira kultura IB, analiza rizika se provodi za potpuni nivo, postoji direktor službe IB, služba unutrašnjeg audita IB, grupa za sprečavanje kompjuterskih incidenata, grupa ekonomske bezbednosti. Pored klasičnih sredstava postoje i sredstva centralnog upravljanja IB i mrežnim resursima. **Model Carnegie Mellon University** ima pet nivoa zrelosti kompanije.

Kakav je odnos između pojmova „pretnja“ i „rizik“? Rizik je kombinacija pretnje i ranjivog mesta informacionog sistema (IS). Pretnja bez ranjivog mesta, kao i ranjivo mesto bez pretnje ne daju rizik. Osnovna karakteristika rizika je pojava gubitka i postojanje verovatnoće realizacije pretnje.

Rizik je mogućnost slučajnog ili namernog narušavanja bezbednosti. Reč je o potencijalno mogućim događajima, dejstvima, procesima ili pojavama koji mogu dovesti do gubitaka. Pod gubicima se podrazumeva narušavanje osnovnih svojstava informacija (poverljivosti, integriteta i dostupnosti) koje imaju svoj ekonomski ekvivalent – cenu gubitaka.

Tradicionalni pristup (“Kriterijum ocene kompjuterskih sistema”, MO SAD, 1983.) razlikuje tri vrste rizika: rizike narušavanja poverljivosti (kopiranje ili oticanje), rizike dostupnosti (blokiranje informacija) i rizike integriteta (modifikacija, negiranje originalnosti informacije ili unošenje lažne informacija). U slučaju kompjuterskih sistema, ovakva klasifikacija se može smatrati korektnom. U drugim slučajevima, ona rezultira sa više dilema nego što daje odgovora.

Namački standard BSI definiše pet vrsta rizika (fors-mažor, organizacioni nedostaci, greške operatora – korisnika, tehničke otkaze i namerna dejstva).

Evropska konvencija o kiberprestupima daje mnogo detaljniju klasifikaciju rizika (nezakonit pristup, nezakonito preuzimanje informacija, narušavanje funkcionisanja sistema, protivpravno korišćenje uređaja, falsifikate uz pomoć kompjutera, narušavanje integriteta podataka i narušavanje autorskih prava).

Ocena rizika IB se provodi ne jedan od dva moguća načina:

- putem ocene usaglašenosti sa definisanim skupom zahteva i preporuka za obezbeđenje IB ili
- putem ocene rizika IB zasnovanih na oceni verovatnoće realizacije napada i veličine nastale štete [4].

Ocena usaglašenosti sa definisanim skupom zahteva se vrši u odnosu na:

- normativno-pravna dokumenta kompanije u oblasti IB,
- zahteve postojećeg zakonodavstva,
- preporuke međunarodnih standarda - ISO 17799, ISO 27001, OCTAVE, CoBIT itd. i
- preporuke kompanija-proizvođača – MicroSoft, Oracle, Cisco itd. [4].

Ocena rizika[2] na osnovu procene verovatnoće realizacije napada i veličine nastale štete podrazumeva primenu različitih metoda (statističkih, ekspertskih itd.).

Ocena rizika se može realizovati na osnovu kvalitativih i kvantitativnih skala.

Najpoznatije metodologije za ocenu rizika su: CRAMM, NIST-800, OCTAVE, RiskWatch, Grif itd. Postojeće metodologije podrazumevaju modeliranje pretnji za informacione aktive i modeliranje informacionih sistema.

[2] U literaturi se sreću različiti modeli upravljanja rizicima. U okviru njih je različit tretman pojmova analiza rizika i ocena rizika. U ovom radu, ocena rizika podrazumeva kvalitativno i kvantitativno određeivanje rizika dok analiza obuhvata širi spektar radnji i postupaka.

Ocena rizika na osnovu procene verovatnoće realizacije napada i veličine nastale štete podrazumeva primenu različitih metoda. Danas su u upotrebi dva osnovna metoda ocene rizika IB.

- metod ocene rizika zasnovan na modelu pretnji i ranjivosti i
- metod ocene rizika zasnovan na modelu informacionih tokova.

Kada je reč o rizicima, važan pojam je **smanjenje rizika**. Pod smanjenjem se podrazumeva apsolutno sve što smanjuje negativnu prirodu rizika. Preko analize rizika, politike bezbednosti i plana rekonstrukcije havarijskih situacija dolazi se do preaostalog rizika. Važno je uočiti da rizik uvek postoji jer nekada nema smisla trošiti novac na neke rizike, a, sa druge strane, uvek postoje nepoznate neizvesnosti [1,2,3,4].

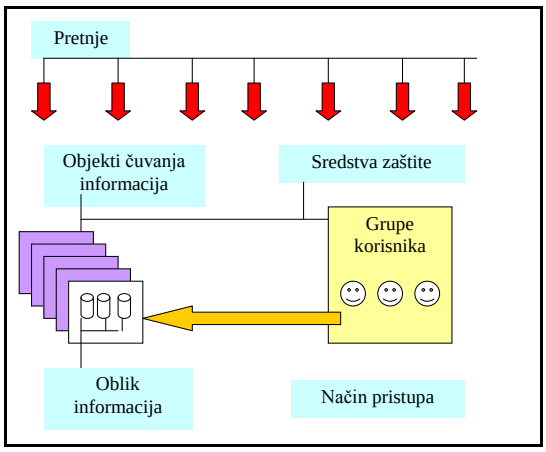
3. Mehanizmi rada algoritama analize rizika

Kao što je rečeno, osnova upravljanja informacionom bezbednošću je analiza rizika. Analiza informacionih rizika je, u stvari, proces ocene zaštićenosti IS. Rezultat analize su kvalitativni ili kvantitativni pokazatelji rizika.

Analiza rizika se deli, uslovno, na analizu baznog i analizu potpunog nivoa. Analiza rizika baznog nivoa podrazumeva proveru ispunjenosti zahteva opšteprihvaćenog standarda bezbednosti (recimo ISO 17779) i dobijanje, na izlazu, kvalitativne ocene rizika (visok, srednji, nizak).

Potpuna analiza informacionih rizika je ozbiljniji zadatak i, kao takav, predmet sukobljavanja specijalista i mnogih rasprava. Zbog čega potpuna analiza rizika izaziva toliko spornih pitanja? Zbog čega u svetu postoji malo sistema analize i upravljanja informacionim rizicima?

Osnovno razlika između analize baznog i potpunog nivoa je neophodnost formiranja punog modela analiziranog IS. Model treba da obuhvati: oblik (vrste) informacija, objekte čuvanja, grupe korisnika i načine pristupa ka informacijama, sredstva zaštite (uključujući i politiku bezbednosti) i vrste pretnji (slika 1).



Slika 1: Sistemsko modeliranje IS

Na osnovu modela IS, vrši se analiza njegove zaštićenosti. Problemi su: kako algoritamski oceniti zaštićenost IS? Kako algoritamski odrediti sve klase ranjivosti? Kako oceniti štetu po

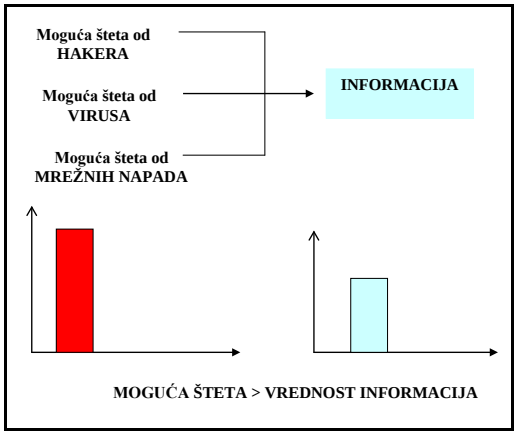
svim vrstama pretnji? I na kraju: kako oceniti verovatnoću realizacije skupa pretnji, ako je rizik po svojoj prirodi stohastički?

Kao primer savremenog algoritma analize rizika, razmatramo algoritam GRIF koji je realizovan u istoimenom programskom paketu. Pri razradi algoritma GRIF učinjeni su pokušaji da se otklone nedostaci postojećih sistema i da se algoritam učini komfornijim za korisnike [5,6,7].

Analiza tehnoloških osobenosti zaštićenosti IS kod algoritma GRIF je realizovana aktivnom upotrebom eksperata. Algoritam je zasnovan na sledećim principima:

- princip predaje svojstva objekta drugim objektima datog skupa,
- princip izbora nivoa zaštićenosti objekata jednog skupa po nivou najmanje zaštićenog objekta skupa,
- princip ocene nivoa zaštićenosti uzajamih delovanja između subjekata i objekata u odnosu na onaj koji je najmanje zaštićen:
  - pri oceni nivoa zaštićenosti uzajamnog delovanja između subjekta (korisnika) i objekta (informacija na objektu), bira se najmanje zaštićeni objekat uzajamnog delovanja,
  - pri oceni zaštićenosti vrste informacija (objekat uzajamnog delovanja), razmeštenih na jednom od objekata IS, nivo zaštićenosti svake vrste informacija se bira po najmanje zaštićenom,
  - pri oceni zaštićenosti objekata uzajamnog delovanja (koji se nalaze fizički u jednom segmentu), nivo zaštićenosti se bira prema najmanje zaštićenom objektu.

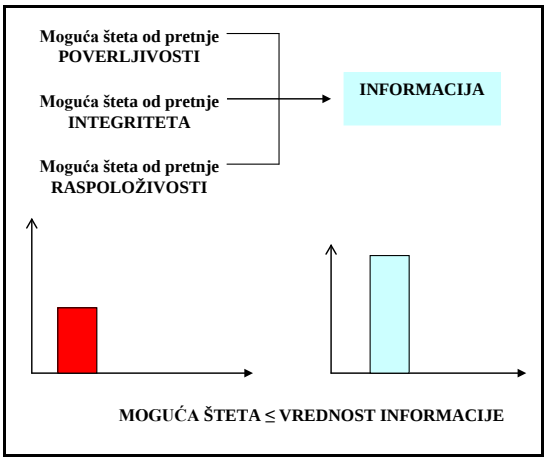
Na završnu ocenu zaštićenosti IS, uticaj imaju i organizacioni aspekti. Algoritam GRIF uzima u obzir zahteve standarad IB ISO 17799 [5].



Slika 2: Metodologija izračunavanja moguće štete u algoritmu RiskWatch

Ocena štete od pretnji bezbednosti – ovo je klasičan problem analize rizika. Neki od postojećih algoritama (npr. američki program RiskWatch) koriste metod **određivanja štete po konkretnim**, specifičnim za dati sistem, **pretnjama** što konačnu štetu, gledano ukupno, čini većom od realne (slika 2). Naime, konačni elemenat zaštite – informacija i šteta se definišu prema informaciji. Stvar je u tome što se na jedan te isti oblik informacije može usmeriti više pretnji što za posledicu ima činjenicu da sumarna šteta, izračunata prema svim pretnjama, bude neadekvatna realnoj.

U algoritmu GRIF je primenjen novi **metod klasičnih nepresecajućih polja pretnji informacija**: pretnja poverljivosti, pretnja integriteta i pretnja raspoloživosti. Algoritam GRIF zahteva od korisnika unos štete po sva tri vida pretnji za svaki oblik informacije (slika 3).



Slika 3: Metodologija izračunavanja moguće štete u algoritmu GRIF

Ovaj metod omogućava:

- apstrakciju konkretnih pretnji bezbednosti (jer svaka konretna pretnja se u stvari raspada na te tri pretnje),
- izbegavanje sumiranja preobilja informacija po šteti,
- algoritam omogućava razbijanje procesa analize zaštićenosti IS na skup elementarnih situacija u kojima algoritam analizira mogućnost realizacije datih klasičnih pretnji u odnosu na svaki oblik informacija na svakom resursu i
- da se u toku analize ne vezuje za konkretne realizacije pretnji [5].

Ocena verovatnoće realizacije detekcije pretnji predstavlja fundamentalni problem svakog algoritma analize rizika. Prilaz "pojedinačne pretnje" (algoritam RiskWatch) zahteva da se unese verovatnoća realizacije date pretnje. U algoritmu GRIF modelira se pristup svih grupa korisnika ka svim oblicima informacija i u zavisnosti od načina pristupa i vrste resursa razmatraju se konačni skupovi očiglednih elementarnih situacija za koje se jednostavno i tačno mogu odrediti početne verovatnoće realizacije pretnji. U algoritmu GRIF se primenjuje tipičan algoritamski prilaz kod koga se rešenje velikog sistema razbija na skup malih prostih zadatak [5].

Kao rezime, može se konstatovati da je završna ocena rizika, kod algoritma GRIF, zasnovana na kompleksu parametara koji su definisani zaštićenošću analiziranog objekta. Jedan od parametara je tehnološki aspekt zaštićenosti. On vodi računa o zahtevima standarda Good Practice, ISO 15408 itd. Drugi parametar je kompleks bezbednosti baziran na standardu ISO 17779 (organizacija, administriranje, fizička bezbednost itd.). Na taj način dobija se svestrana, kompleksna ocena rizika [5].

4. Modeliranje pretnji

Modeliranje pretnji je posebno dobilo na značaju sa pojavom koncepta detekcije pretnji, a ne napada u realizaciji sistema detekcije i prevencije napada.

Najpoznatiji pristupi u modeliranju pretnji IB su [4].:
- "trijada CIA",
- "heksada Parkera",
- klasifikacija 5A Brusa Šnajera i
- model pretnji IB STRIDE.

Osnovne karakteristike pojedinih pristupa modeliranja pretnji su:

Trijada CIA - pretnje IB opisuje pomoću tri klasična servisa bezbednosti:

- poverljivost (***c**onfidentiality*) – čuvanje informacije kao tajne, nemogućnost obelodanjivanja informacije bez saglasnosti drugih zainteresovanih strana;
- integritet (***i**ntegrity*) - zaštita informacije od neatorizovanih modifikacija;
- raspoloživost (***a**vailability*) - obezbeđenje informacija i radna sposobnost usluga u vreme kada su potrebne korisnicima.

Ovaj model pretnji se koristi u programskom paketu GRIF.

Alternativa modelu CIA je model "**heksada Parkera**" koja obuhvata više bezbednostnih servisa (ukupno šest). Naime, ona pored gore pomenitih servisa, za opis pretnje se koriste još tri servisa, i to:

- autentičnost (*authenticity*) – originalnost korisnika i izvora poruke;
- upravljivost, ili vladanje (*possession or control*) **–** garancija da samo vlasnik može menjati informacije ili realizovati pristup istima;
- korisnost (*utility*) – praktičnost, komfor upotrerbe informacija u datoj formi zapisa.

U pristupu modeliranju pretnji IB, Brus Šnajer, jedan od najpoznatijih savremenih kriptografa, je pobornik modela poznatog pod nazivom **klasifikacije 5A**:

- authentication - autentifikacия (ko si ti?);
- authorization - autorizacija (šta je tebi dozvoljeno da radiš?);
- availability - raspoloživost (da li može da se dobije saglasnost za rad sa podacima?);
- authenticity - autentičnost (da li su podaci originalni?);
- admissibility - prihvatljivost (da li su podaci verni, aktuelni i korisni?).

Microsoft metodologija SDL (*Secure Development Lifecycle*) je zasnovana na modelu pretnji poznatim pod nazivom STRIDE*:*

- Spoofing – pretvaranje,
- Tampering – promene,
- Repudiation **–** nepriznavanje (odustajanje od) odgovornosti,
- Iinformation Disclosure – oticanje podataka,
- Denial of service (DoS) – otkaz u obsluživanju (servisu) i
- Elevation of privilege – analiza privilegija.

Model pretnji STRIDE proširuje mogućnosti u odnosu na tradicionalni model (CIA) jer omogućava pogled na IS i sa pozicije napadača. Naime, model CIA odgovara samo delu modela STRIDE (CIA = Tampering + Information Disclosure + Denial of Service).

5. Ocena rizika

Suštinski posmatrano, pogled na rizike u teoriji informacione bezbednosti je kao i kod osiguranja od nesrećnih slučajeva. Sumarni rizik se definiše kao matematičko očekivanje štete, tj. kao suma proizvoda verovatnoća svakog od negativnih događaja i veličine gubitaka koji su nastali kao njihova posledica (1):

$$R = \sum_{i=1}^{n} P(u_i)L(u_i) \qquad (1)$$

gde su: $P(u_i)$ – verovatnoća događaja i

$L(u_i)$ - veličina gibitaka događaja.

Osobenosti vezane za izračunavanje ukupnog rizika:

- Ocena rizika se odnosi na neki vremenski period (3 - 5 godina). Ako je verovatnoća događaja mala, razmatrani period treba povećati. U slučaju informacionih sistema, to je period u kome se dešavaju značajne promene tako da upotreba starih ocena gubi smisao. U slučaju rizika čija je verovatnoća nastanka ispod nekog praga, iako su štete velike, vrši se njihovo zanemarivanje. U praksi, u prvom planu su rizici sa umerenom štetom i velikom verovatnoćom nastanka (npr. napadi štetnih programa).
- Verovatnoću pojave negativnog događaja nije moguće tačno oceniti.
- Negativni događaji mogu da budu zavisni kao i što mogu međusobno da se isključuju (npr. požar i poplava).

Zbog navedenih razloga, rizici se ne tretiraju kao numeričke vrednosti, već kao **tačke u ravni** gde se kao koordinate koriste veličine: verovatnoća događaja i veličina gubitaka. Ovo je jedna od metodologija prikazivanja rizika.

Upravljanje rizicima je adekvatno premeštanju tačaka rizika u koordinatnoj ravni. Obično se nastoji približiti koordinatnom početku duž jedne ose ne menjajući vrednost druge koordinate. Promena obe koordinate daje tačnije rezultate, ali zahteva veća finansijska sredstva.

Zasnovano upravljanje rizicima je moguće samo u relativno uskim oblastima gde su poznati mogući negativni događaji, kada je njihov broj relativno mali (recimo nekoliko desetina) i kada postoje realne ocene verovatnoća događaja i gubitaka. U drugim slučajevima ekonomska celishodnost neutralizacije rizika se može proceniti samo intuitivno. Istina, neutralizacija mnogih rizika je predviđena postojećim normativnim dokumentima (npr. obezebeđenje zaštite od požara - ZOP) i zbog toga se adekvatne mere smatraju obaveznim.

Predstavljanje rizika u obliku tačaka u ravni je pogodno sa psihološkog aspekta ukoliko ono omogućava da se razdvojeno prikažu aspekti delovanja verovatnoće nastanka događaja i rezultata preduzetih mera – pomeranje tačaka rizika ka koordinatnom početku. Važan aspekt ovog procesa je i cena smanjenja rizika.

Rizici se mogu predstavljati i u obliku **drveta ranjivosti**, **pretnji i kontramera**. U ovom slučaju posmatraju se sledeće veličine: Vi – ranjiva mesta; Ti,j – pretnje bazirane na ranjivim mestima; Ci,j – kontramere neutralizacije pretnji i,j i; Li,j – nedostatak kontramera za pretnje i,j.

Vrednosti Vi, Ti,j i Ci,j se normiraju tako da sume po Vi i Ti,j budu jednake 1, odnosno da je: Li,j + 0,45Ci,j = 1.
Osim parametara verovatnoće, u oceni rizika učestvuju i konstante – kritičnost aktiva (CA) i vrednost aktiva (CC).

Opšta očekivana suma gubitaka se izražava kao proizvod ostatka rizika, kritičnosti i vrednosti aktiva:

Suma gubitaka = Opšti ostatak rizika * CA * CC (2)

Mogući su i drugi načini predstavljanja rizika. Pretpostavimo da aktiv i pretnja čine „par". Za svaki takav **„par" - (aktiv, pretnja)** rizik se izračunava po formuli:

Rk = Pj * Lj (3)

gde su: Rk – veličina rizika

Lj – posledica realizacije pretnje na aktiv

Pi – verovatnoća realizacije pretnje u odnosu na "par"

K – broj „para"

Za ocenu stanja organizacija u oblasti informacione bezbednosti nisu važne samo apsolutne vrednosti rizika, već i njihovo smanjenje nastalo kao posledica upotrebe kontramera. Pri tome, u svojstvu kvantitativne mere rizika može biti upotrebljeno **vreme koje je potrebno za uspešan napad** na sistem, uz zadatu motivaciju i kvalifikaciju napadača. Povećanje tog vremena svedoči o povećanju nivoa bezbednosti.

6. Modeliranje pretnji u algoritmu GRIF

Kao ilustracija modeliranja pretnji IB, u tekstu koji sledi, prikazan je model analize pretnji i ranjivosti u algoritmu GRIF (algoritam je realizovala firma Digital Security).

Model analize pretnji i ranjivosti u sistemu GRIF je projektovan u skladu sa modelom pretnji CIA (poverljivost, integritet, raspoloživost).

Ocena rizika IS organizacije se određuje uz pomoć analize pretnji (koje deluju na konkretni resurs) i ranjivosti (preko kojih date pretnje mogu biti realizovane). Informacioni rizici se analiziraju u odnosu na dva parametra:

- na verovatnoću realizacije pretnje i
- na stepen uticaja pretnje na resurse [6].

Princip rada algoritma GRIF:

Osnovni koraci:

1. Unošenje ulaznih podataka – resursi, kritični resursi, organizacione celine, pretnje koje deluju na resurse, ranjivosti, verovatnoća realizacije pretnje kroz datu ranjivost, kritičnost realizacije pretnje kroz datu ranjivost. Algoritam radi u dva režima: jedna osnovna pretnja i tri pretnje (poverljivost, integritet, raspoloživost).

2. Skala po nivoima se razbija na 100 nivoa (odgovara opsegu od 0 do 100%). Skala može biti linearna ili logaritamska.

3. Tok izračunavanja rizika:

Izračunavanje nivoa pretnje po ranjivosti Th – nivo pretnje pokazuje koliko je kritično delovanje pretnje na resurs sa uzimanjem u obzir kolika je verovatnoća njene realizacije. Nivo pretnje je funkcija kritičnosti realizacije pretnje ER (ranjivost je data u %) i verovatnoće realizacije pretnje P(V) (data u %). U zavisnosti od režima rada, izračunava se nivo pretnje za jednu ili tri pretnje. Nivo pretnje se nalazi u intervalu od 0 do 1.

$$Th = \frac{ER}{100} x \frac{P(V)}{100} \quad (4)$$

Izračunavanje nivoa pretnje po svim ranjivostima CTh – kao rezultat zbira po svim ranjivim mestima. Nivo pretnje po svim ranjivim mestima se nalazi u intervalu od 0 do 1.

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th) \quad (5)$$

Izračunavanje opšteg nivoa pretnji po resursu CThR - dobije se sumiranjem po svim pretnjama. Nivo pretnji po resursu se nalazi u intervalu od 0 do 1.

$$CTh = 1 - \prod_{i=1}^{n} (1 - CTh) \quad (6)$$

Izračunavanje rizika po resursu R – predstavlja proizvod opšteg nivoa pretnji po resursu i kritičnosti resursa D:

$$R = CThR \times D \quad (7)$$

Izračunavanje rizika za ceo IS CR – dobije se sabiranjem rizika po svim resursima:

$$CR = \sum_{i=1}^{n} Ri \quad (8)$$

Efektivnost primenjenih mera zaštite E se izračuva tako što se, posle definisanja mera zaštite, pređe ceo ciklus sa kontramerama pa se primeni realacija:

$$E = \frac{Rold - Rnow}{Rold} \quad (9)$$

Primer:

Kao primer proračuna rizika IB na osnovu modela pretnji i ranjivosti, dat je server IS. Ulazni podaci o resursima, verovatnoći realizacije pretnje, kritičnosti realizacije pretnje, nivou pretnje, opštem nivou pretnje po resursu i riziku resursa su dati u tabelama od 1 do 5 [6].

Tabela 1: Ulazni podaci o resursima

Resurs	Pretnja	Ranjivost

Server (kritičnost resursa D=100 uj)	Pretnja 1: Neautorizocvani ulazak napadača unatar branjenog perimetra (jednog od parametara)	Ranjivost 1: Nedefinisanost pristupa prostorijama sa resursima koji sadrže vredne informacije.
		Ranjivost 2: Odsustvo sistema osmatranja (video nadzor, senzori i sl.) objekata (ili postojeći sistemi ne pokrivaju sve značajne objekte).
	Pretnja 2: Neautorizovana modifikacija u sistemu elektronske pošte koja se čuva na resursu	Ranjivost 1: Nepostoji autorizacija za unošenje izmena u sistemu elektronske pošte.
		Ranjivost 2: Nedefinisane preporuke o radu sa kriptografskom zaštitom elektronske pošte.
	Pretnja 3: Razglašenje poverljive informacije saradnicima kompanije	Ranjivost 1: Odsustvo saglasnosti o poverljivosti.
		Ranjivost 2: Distribucija atributa bezbednosti (ključevi pristupa, šifrovanja) između nekoliko poverljivih saradnika.

Tabela 2: Ulazni podaci o verovatnoći realizacije pretnje P(V) i kritičnosti realizacije pretnje ER

Rb	Pretnja/ranjivost	Verovatnoća realizacije pretnje kroz datu ranjivost u toku godine (%), P(V)	Kritičnost realizacije pretnje (%), ER
1.	Pretnja 1/ Ranjivost 1	50	60
2.	Pretnja 1/ Ranjivost 2	20	60
3.	Pretnja 2/ Ranjivost 1	60	40
4.	Pretnja 2/ Ranjivost 2	10	40
5.	Pretnja 3/ Ranjivost 1	10	80
6.	Pretnja 3/ Ranjivost 2	80	80

Tabela 3: Nivo pretnji Th

Rb	Pretnja/ranjivost	Nivo pretnji (%), Th	Nivo pretnji po svim ranjivostima (%), CTh
1.	Pretnja 1/ Ranjivost 1	0,3	0,384
2.	Pretnja 1/ Ranjivost 2	0,12	
3.	Pretnja 2/ Ranjivost 1	0,24	0,270
4.	Pretnja 2/ Ranjivost 2	0,04	
5.	Pretnja 3/ Ranjivost 1	0,08	0,669
6.	Pretnja 3/ Ranjivost 2	0,64	

Tabela 4: Opšti nivo pretnje po resursu CThR

Rb	Pretnja/ranjivost	Nivo pretnji po svim ranjivostima (%), CTh	Opšti nivo pretnje po resursu (%), CThR
1.	Pretnja 1/ Ranjivost 1	0,384	0,8511
2.	Pretnja 1/ Ranjivost 2		
3.	Pretnja 2/ Ranjivost 1	0,270	
4.	Pretnja 2/ Ranjivost 2		
5.	Pretnja 3/ Ranjivost 1	0,669	
6.	Pretnja 3/ Ranjivost 2		

Tabela 5: Rizik resursa

Rb	Pretnja/ranjivost	Opšti nivo pretnje po resursu (%), CThR	Rizik resursa (%), R $R = CThR \times D$
1.	Pretnja 1/ Ranjivost 1	0,8511	85,11
2.	Pretnja 1/ Ranjivost 2		

3.	Pretnja 2/ Ranjivost 1		
4.	Pretnja 2/ Ranjivost 2		
5.	Pretnja 3/ Ranjivost 1		
6.	Pretnja 3/ Ranjivost 2		

Leteratura

1. Петренко С. А., Симонов С. В.,Управление информационным рисками. Экономически оправданная безопасность, Компания АйТ: ДМК Пресс, 2004.
2. Гладких А. А., Дементев В. А., Базовые принципы информационной безопасности вычислительных систем, учебное пособие, Уляновск: УлГТУ, 2003.
3. Пастоев А., Методологија управления ИТ-рисками, Открытые системы, 8/2006.
4. Авдошин С.М., Савельева А.А., Сердюк В.А., Технологии и продукты Microsoft в обеспечении информационной безопасности, УнИТ, Масква, 2011.
5. Медведовский И., Современные методы и средства анализа и контроля рисков информационных систем компаний, Учёбный центр «Информзащита», 12. 01. 2004.
6. Куканова Н., Методика оценки риска ГРИФ, Digital Security, 2005.

Konferencija o bezbednosti informacija BISEC 2012
Univerzitet Metropolitan

DIREKTIVE ZA INFORMACIONU BEZBEDNOST "PAMETNIH" ELEKTROENERGETSKIH MREŽA

(DIRECTIVES FOR CYBER SECURITY OF „SMART" POWER GRIDS)

SLOBODAN JOVANOVIĆ
Univerzitet Metropolitan, Fakultet informacionih tehnologija, Beograd, www.metropolitan.edu.rs,
slobodan.jovanovic@fit.edu.rs

Rezime: *U celom svetu, a najviše u USA, je započela velika transformacija infrastrukture elektroenergetskih mreža. Ovaj rad diskutuje ključne karakteristike informacione bezbednosti „pametnih" elektroenergetskih mreža, kao i njihovu komunikacionu arhitekturu, i njihove tačke ranjivosti. Zatim, opisuje direktive koje je potrebno primeniti da bi se postigla informaciona bezbednost u „pametnim" elektroenergetskim mrežama, kao i pitanje razvoja njihovih informacionih bezbednosnih standarda. Takodje, prikazuje se plan za razvoj informacione infrastrukture „pametnih" elektroenergetskih mreža u EPS (Elektroprivredno preduzeće Srbije) za sledećih 10 godina.*

Ključne reči: *Informaciona infrastruktura, Logički interfejs, Distribuirana inteligencija, Distribuirani generatori*

Abstract: *In the whole world, especially in USA, a huge power grid infrastructure transformation has started. This paper discusses the key characteristics of cyber security of smart power grids, and their communication architecture, and their vulnerability points. .Then, it describes guidelines which are needed to be implemented to achieve cyber security in smart power grids, and a question of development of their cyber security standards. Finally, the plan for development of information infrastructure of smart power grids in Serbia (EPS – Electris power of Serbia) in next 10 years is presnted here..*

Keywords: *Information infrastructure, Logical interface, Distributed intelligence, Didtributed generation*

1. UVOD

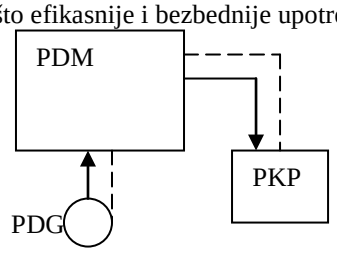
Elektroenergetska mreža koja radi blizu svojih limita tj. blizu svog maksimalnog kapaciteta, zahteva sve više i više primenu „pametnih" tehnologija. Naime, buduće distributivne mreže radiće u uslovima gde se koristi veliki procenat DG (*distributed generation, tj. embeded generation*), a DG može da ima veoma varijabilnu i nepredvidljivu izlaznu snagu. Takodje, energija postaje sve skuplja, i ide se na minimizaciju učešća fosilnih izvora energije, i uopšte na minimalnu potrošnju energije. Dakle, distributivne mreže budućnosti radiće sa velikim učešćem DG, i sve više se nameće potreba za „pametnim" mrežama **[1],** gde se omogućuje primena

- Distribuirane inteligencije
- Digitalne komunikacije
- Softvera za upravljanje

Digitalne dvosmerne komunikacije, tj. *two-way fast digital communications*, mogu biti različitog tipa:

- Fiksni i bežični telefoni
- Radio veza
- Optički kablovi
- Energetski vod (*power line carrier*)
- Satelit
- Intenet

Na slici 1 je prikazana „pametna" distributivna mreža PDM tj. tzv. *„smart" power grid SPG*. „Pametni" krajnji potrošač PKP i „pametni" distribuirani generatori PDG su ključni elementi u okviru PDM. Pri tome, distribuirana inteligencija je deo PKP i PDG. Dakle, PDM i PDG se „inteligentno" ponašaju tj. prilagodjavaju uslovima rada u sistemu, u cilju što efikasnije i bezbednije upotrebe PDM.



Slika 1: Pametna disdtributivna mreža PDM (isprekidana linija predstavlja komunikacioni kanal)

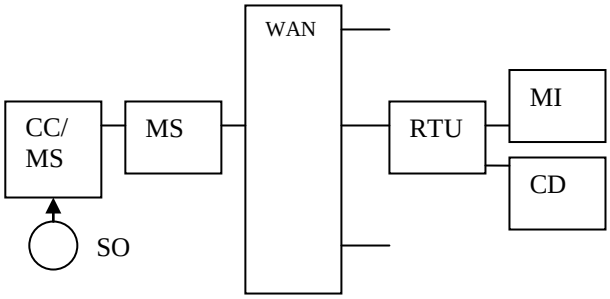
Smart grid je kišobran koji pokriva modernizaciju kako distributivne tako i prenosne elektroenergetske mreže. Kod prenosne meže, umesto upravljanja malim generatorima DG i krajnjim potrošačima KP, cilj je primena „pametnih" tehnologija na upravljanje elementima u prenosnom sistemu.

2. SCADA ARHITEKTURA

Svaki moderan distributivni sistem opremljen je SCADA sistemom. SCADA sistem označava sistem za *supervisory control and data acquisition*. On obuhvta telemerenje podataka pomoću mernih instrumenata MI na terenu, pa prikupljanje ovih podataka preko inteligentnih elektronskih uređaja, tzv. *remote terminal units* RTU, i onda njihovog transfera do glavne stanice, *master-station*

MS, da bi se primenili razni procesirajući i kontrolni algoritmi. MS je povezana sa centralnim kompjuterom CC. Rezultati procesiranja se prikazuju na monitorima MS (*monitoring screens*) lociranih kod sistem-operatora SO. A upravljačke tj. kontrolne akcije se šalju nazad na teren, u realnom vremenu. MI i RTU su povezani komunikacionim kolom. Pri tome, MI su povezani sa uredjajima koji se kontrolišu. A RTU su povezane sa mernim uredjajima i prikupljaju podatke koji se mere pomoću MI, i memorišu te podatke i šalju ih u MS preko komunikacione mreže, *communication network* CN, ali isto tako primaju kontrolne signale iz MS i šalju ih prema kontrolnim uredjajima, *control devices* CD, npr. releji ili motori itd., koji služe za upravljanje opremom u mreži (vodovi, generatori, krajnji potrošači). RTU su geografski disperzovane, i povezane sa MS pomoću različitih komunikacionih kanala, npr. radio-veze, iznajmljene telefonske linije, optički kablovi. U SCADA sistemu se informacije transferišu kako od RTU do MS, tako i od MS do RTU, i ovo je dakle obostrana komunikacija, *two-way communication*. Operator sistema SO nadgleda sistem i po potrebi sprovodiu upravljačke akciuje. Neke upravljačke akcije se sprovode automatski pomoću kompjutera, a SO ih samo nadgleda.

SCADA arhitektura, koja je prikazana na slici 2, je hijerarhijska, na dva nivoa. Donji nivo obuhvata RTU na raznim udaljenim lokacijama, a viši nivo je MS. Komunikacija izmedju RTU i MS se ostvaruje preko CN, a CN je ustvari tzv. *wide area network* WAN. SCADA sistem se može organizovati i na tri nivoa, gde se RTU dele na grupe, i svaka grupa je povezana sa komunikacionim serverom, a svaki komunikacioni server je povezan sa MS. Pri tome, komunikacioni serveri i MS mogu biti povezani sa LAN, *local area network*.



Slika 2: *Two-level* SCADA sistem

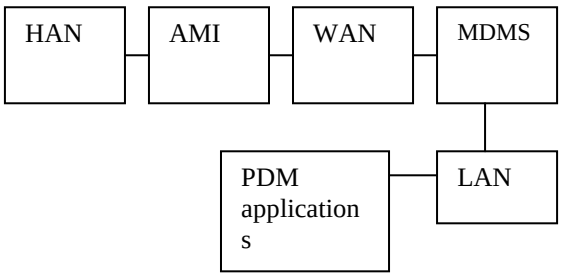
Tradicionalni SCADA sistemi predstavljaju u stvari začetak „pametnih“ elektroenergetskih mreža. Tj. SCADA je najranija *smart grid* tehnologija. Ipak, tradicionalna SCADA doseže samo do podstanica (i to ne svih), glavnih vodova, i malog broja daljinsko-kontrolisanih uredjaja (npr. rastavljača). Pošto je u distributivnoj mreži DM broj vodova i čvornih tačaka ogroman, a kapitalni troškovi (investicije) za RTU su veliki (RTU su vrlo skupe), onda je i broj RTU limitiran u tradicionalnoj distributivnoj mreži. Ipak, SCADA je fundament tj. osnova na kojoj se bazira „pametna“ distributivna mreža PDM. SCADA i podaci u okviru SCADA igraju važnu ulogu u bilo kojoj implementaciji „pametne“ elektroenergetske mreže. Dakle, do razvoja „pametne“ mreže dolazi se polazeći od postojeće mreže i SCADA sistema kao ključnog elementa.

3. KOMUNIKACIONA ARHITEKTURA I TAČKE RANJIVOSTI

Od početka 21-og veka, poboljšanje i pojeftinjenje komunikacionih tehnologija pružili su mogućnost da se unapredi upravljanje elektroenergetskim sistemima tj. elektroenergetskim mrežama. Vetrogeneratori i sunčevi generatori (*wind power , solar power*) imaju veoma promenljivu izlaznu snagu, pa je sofisticiranije tj. „inteligentno“ upravljanje ovim izvorima neophodno. Digitalne komunikacije i digitalno procesiranje i distribuirana inteligencija su osnovne osobine „pametne“ elektroenergetske mreže. Pametna brojila (*smart meters*) su digitalna brojila koja čitaju i memorišu u realnom vremenu, i koja mogu da isključe pojedine potrošače u vreme maksimalnih tj. kritičnih opterećenja sistema.

Pametna mreža isporučuje energiju od proizvodjača do potrošača koristeći *two-way Smart Meter technology* (pametna brojila), koja može daljinski da kontroliše upotrebu energije korisnika. Ovo omogućuje konzervaciju energije, redukovane troškove, veću pouzdanost i efikasnost. Ali, takvi IT-bazirani elektroenergetski sistemi dramatično povećavaju ranjivost informacione bezbednosti (*cyber security vulnerabilities*), i ovo dovodi do dramatično povećanog značaja informacione bezbednosti.

Advanced Metering Infrastructure (AMI) i *Meter Data Management System* (MDMS) su osnovne komponente komunikacione arhitekture pametne distributivne mreže. AMI prikuplja i transmituje *Smart Meter data*, a MDMS prikuplja, memoriše i operiše ovim podacima **[2].** Na slici 3 je prikazana komunikaciona arhitektura pametne mreže, koja obuhvata HAN (*Home Area Network*), AMI komunikacionu mežu i WAN (Wide Area Network), i MDMS.



Slika 3: Komunikaciona arhitektura pametne mreže

Sa razvojem MDMS tehnologije, MDMS podaci se koriste za novije aplikacije, uključujući aplikacije za

- Web portale potrošača,
- interne Web portale,
- *independents system operators* ISO,

- i proizvodjače energije

Ovo omogućuju efikasnije upravljanje sistemom, a potrošačima energije pružaju bolje informacije o njihovoj potrošnji. Ali, ovde se pojavljuju novi rizici. Naime, kako elektroprivredne kompanije primenjuju savršenije tehnologije i dodaju inteligenciju elektroenergetskoj mreži, ove nove tehnologije donose nove tačke ranjivosti u pametnu mrežu (komunikacioni protokoli, logički interfejsi, HAN, *customer portals*, hardver) [2]:

1) Npr. **komunikacioni protokoli** kod komunikacija izmedju AMI aparata i MDMS, i ova komunikacija može biti ugrožena ako komunikacija nije šifrovana od početka do kraja (*encrypted end-to-end*). Naime, autentifikacija i autorizacija izmedju aparata treba da se šifruje.

2) **Logički interfejsi** pametne mreže, kao što su Web-bazirane aplikacije, su predmet ranjivosti u vezi sa protokolima i aplikacijama koje se koriste u pametnoj mreži.

3) **HAN** tj. aparati u okviru HAN su takodje tačka ranjivosti. Pri tome, bežična komunikacija izmedju pametnih aparata i centralnog sistema treba da se zaštiti protiv napada.

4) Napadači na pametnu mrežu mogu da koriste ***customer portals*** da pristupe računima potrošača i promene podešenja tj. podatke o potrošačima. I ovo može da utiče na mrežu a i potrošače.

5) **Hardver** takodje donosi tačke ranjivosti. Naime, pametno brojilo (Smart Meter) je povezan sa AMI, i ovo donosi rizik sličan sa rizikom od bežičnog HAN. Neka neautorizovana osoba mogla bi da kontroliše brojilo, da ga uključi ili isključi ili modifikuje podešenje. Ovo ima posledice za potrošača a i za proizvodjača energije.

4. DIREKTIVE I STANDARDI ZA INFORMACIONU BEZBEDNOST

U celom svetu, a najviše u USA, je započela velika transformacija infrastrukture elektroenergetskih mreža. Ova ogromna nadogradnja infrastrukture se dešava u svim delovima, od domaćinstava do velikih elektrana, i do vetrofarmi i DG. Ova promena je istovremeno i evolutivna i revolucionarna. U USA je CSWG grupa (Cyber Security Working Group) zadužena da daje direktive, i ona je objavila dokument „*Guidelines for Smart Grid Cyber Security*“ **[3].** Ovaj dokument se korisi u mnogim organizacijama da one razviju efektivne strategije za informacionu bezbednost, i to za njihovu konkretnu kombinaciju *smart-grid* karakteristika i konvencionalne mreže. *Smart-grid* je koncept, a ne unificirana kombinacija hardvera. Elktroenergetski sistemi se dramatično menjaju poslednjih godina, i ovo će potrajati još niz godina **[4].**

U današnjoj (tradicionalnoj) elektroenergetskoj mreži, puno komunikacije se sprovodi pomoću telefona. Medjutim, protok podataka postao je vrlo važan za jednu elektroenergetsku mrežu. Npr. raspad sistema od 14.8.2003. u USA je bio uzrokovan kašnjenjem u komunikaciji uzbune u sistemu. Takodje, mnogi drugi ispadi u sistemu su rezultat kašnjenja ili greške u informaciji. Takodje, dolazi do kvarova u IT infrastrukturi, koji nisu rezultat terorističkog ili hakerskog napada. Tako da informaciona bezbednost treba da se bavi ne samo namernim napadima na sistem, već i kvarovima u IT infrastrukturi i protoku informacija.

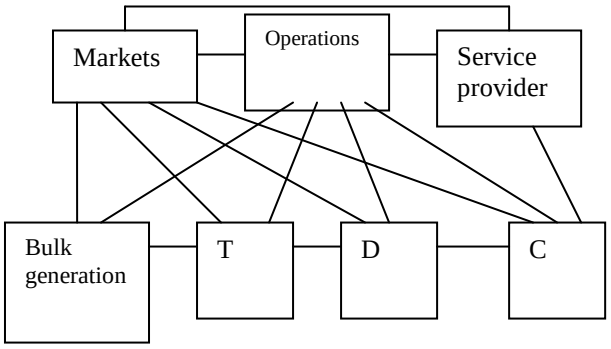
Može se definisati 7 informacionih domena i 15 tokova informacija u jednoj pametnoj prenosno-distributivnoj mreži: Prenos, Distribucija, Operacije (tj. Upravljanje), Velike elektrane, Tržišta, Potrošači, Servis provajder **[3].** Ovih 7 domena je povezano tokovima informacija, kao što se vidi na slici 4. Ovih 7 domena sadrže 46 poddomena tj. aktera. Npr. ISO operatori (*Independent system operator*) su prisutni kako u domenu Operacije tako i u domenu Tržišta.

Takodje, identifikovano je 130 mogućih tipova logičkih interfejsa. I ovih 130 tipova interfejsa se može razvrstati u 22 kategorije. Za svaki od ovih interfejsa, može se proceniti uticaj nenamernog ispada ili namernog napada na ovaj interfejs.

Lako je doći do zaključka, da s obzirom na mnogo raznih interfejsa, da treba posmatrati bezbednost u nekoliko slojeva. Npr.

- *loss of confidentiality* (razotkrivanje informacije)
- *loss of integrity* (modifikacija/destrukcija informacije)
- *loss of availability* (gubitak pristupa informaciji)

Preko analize domena, aktera, i komunikacionih zahteva, u pametnoj mreži, mogu se razvrstati logički interfejsi u razne kategorije.



Slika 4: Informacioni domeni „pametne“ prenosno-distributivne mreže i tokovi komunikacija (T-Transmission, D – Distribution, C - Customer)

IEC TC57 je familija internacionalnih standarda za pametne mreže, uključujući IEC61850. Na osnovu USA *Energy Independence and Security Act* iz 2007., NIST (*National Institute of Standards nd Technology*) je zadužena za identifikaciju i selekciju stotine standarda koji će biti potrebni da se implementiraju u *Smart Grids*

u Americi (USA). Ovi standardi se podnose kod FERC (*Federal Energy Regulatory Comission*). Ovaj rad na standardima tj. njihovom razvoju, je započet, i niz standarda je već izabrano.

Sada postoji trend da se koriste TCP/IP tehnologije kao zajedničke komunikacione platforme za primenu pametnih brojila, tako da elektroprivredne organizacije mogu da primene različite komunikacione sisteme, ali korišćenjem IP tehnologije kao zajedničke platforme.

Dokument NIST SP 1108 (National Institute of Standards and Technology Special publication) je posvećen sigurnosti pametnih elektroenergetskih mreža, i u njemu je dato 75 standarda, specifikacija, direktiva, i zahteva koji su bitni za *smart grids* **[5].** Od ovih 75 preporuka, njih 13 odnosi se na *cyber security*. Od ovih 13, njih 4 je posebno važno za *cyber security* :

- NIST SP 800-53
- NIST SP 800-82
- ISO 27000
- NIST FIPS 140-2

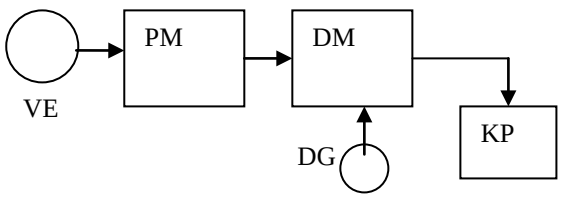
I oni se mogu naći na Web-u:

- http://csrc.nist.gov/publications/
- www.27000.org/

5. RAZVOJ *SMART GRID* U EPS

Postoje dve vrste elektroenergetskih mreža, prenosne i distributivne mreže. Prenosna mreža (PM) koristi napone od 110 kv pa na više (110 kV, 220kV i 400kV), dok distributivna mreža (DM) koristi napone srednjeg nivoa (10 kV, 20kV, itd) i niskog nivoa (220 V, 400V). Distributivna mreža je veza izmedju prenosne mreže i krajnjih potrošača KP, dok je prenosna mreža veza izmedju velikih elektrana (VE) i distributivne meže, kao što je prikazano na slici 5. Male elektrane tj. tzv. distribuirani generatori (DG) su priključeni na distributivnu mrežu. DG se često definiše kao proizvodnja locirana kod potrošača (neki potrošači proizvode el. energiju koristeći sopstvene generatore, npr. od 1kW ili npr. 100 kW).

Distributivni sistem obuhvata DM (distributivna mreža), DG i KP, ali DM takodje obuhvata HV/MV i MV/LV trafostanice TS, MV i LV vodove (glavne i sporedne vodove, *feeders/subfeeders*), kao i MV i LV čvorne tačke (MV i LV podstanice).



Slika 5: Prenosna i distributivna elektroenergetska mreža

U EPS postoji plan za implementaciju projekta „EPS *Metering*“ **[6, 7].** U EPS ima oko 3.5 miliona potrošača, od kojih oko 3.1 milion domaćinstava. Postoji plan da u roku od 10 godina se preuzmu merna mesta od kupaca. I uspostavljanje AMI-MDM sistema. U fazi 1 zamena merne infrastrukture kod velikih potrošača i uvodjenje kontrolnih mernih mesta u TS x/0.4 kV. Po završetku prve faze, planira se verifikacija funkcionalnosti AMI-MDM sistema. U fazi 2a, zamena 50.000 mernih uredjaja u domaćinstvima i instalacijom 3.000 AMI koncentratora. U fazi 2b, zamena 300.000 menih uredjaja u domaćinstvima i ugradnjom 5.000 AMI koncentratora. Po završetku faze 2, masovna ugradnja kod ostalih potrošača a gde je to ekonomski opravdano, oko 80%, u roku od 7 godina. Faza 3 obuhvata zamenu oko 2.2 miliona mernih uredjaja domaćinstava, i ugradnjom potrebnog broja koncentratora.
Faza 1 trajaće oko 1.5 godina, faza 2a oko 1 godine, faza 2b oko 2.5 godine, i faza 3 oko 7 godina. Ukupno trajanje projekta je oko 10 godina. Tabela 1 sumarizuje razvoj pametne distributivne mreže u EPS. Prenosna mreža Srbije EMS, je posebna organizacija koja je izvan EPS.

Tabela 1: Razvoj pametne distributivne mreže u EPS

Faza	Broj instalisanih *smart-meters*
1	Veliki potrošači i TS x/0.4
2a	50.000 domaćinstava
2b	300.000 domaćinstava
3	2.250.000 domaćinstava

6. ZAKLJUČAK

Ovaj rad diskutuje neke ključne karakteristike informacione bezbednosti „pametnih“ elektroenergetskih mreža, i pri tome razmatra njihovu komunikacionu arhitekturu, kao i njihove tačke ranjivosti. Rad specificira direktive koje je potrebno primeniti da bi se postigla informaciona bezbednost u „pametnim“ elektroenergetskim mrežama, kao što i dotiče pitanje razvoja informacionih bezbednosnih standarda „pametnih“ mreža. Takodje, definišu se informacioni domeni u prenosno-distributivnoj „pametnoj“ elektroenergetskoj mrežii, i tokovi informacija medju ovim domenima. Konačno, prikazuje se plan za razvoj informacione infrastrukture „pametnih“ distributivnih elektroenergetskih mreža u Srbiji tj. u EPS (Elektroprivredno preduzeće Srbije) za sledećih 10 godina.

ZAHVALNICA
Ovaj rad podržan je od strane Ministarstva za nauku i obrazovanje (Projekat III44006).

LITERATURA

[25] A.Sellim, O.Malik, Electric distribution systems, Wiley, 2011.

[26] KPMG, The increasing importance of security for the smart grid, www.kpmg.com .

[27] Cyber Security Working Group (CSWG)., *Guidelines for Smart Grid Cyber Security*, http://nist.gov./smartgrid/ .

[28] M.Stevens, „Smart“ power grids a prime target in cyber warfare, http://www.securityweek.com/smart-power-grids-prime-target-cyber-warfare

[29] www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf;2010

[30] Javno Preduzeće EPS, Plan za implementaciju projekta „EPS METERING“, mart 2012.

[7] S.Jovanović, Cyber security and vulnerability of smart power grids, Časopis InfoM, June 2012.

Konferencija o bezbednosti informacija BISEC 2012
Univerzitet Metropolitan

IT BEZBEDNOSNA OBUKA U CILJU ZAŠTITE I BEZBEDNOSTI INFORMACIJA U BANKARTSVU

IT SECURITY TRAINING FOR PROTECTING AND SECURING INFORMATION WITHIN THE BANKING SECTOR

VIKTOR KANIŽAI
OTP banka Srbija a.d. Novi Sad, Novi Sad, viktor.kanizai@otpbanka.rs

Rezime: *Osnovu savremenog bankarskog poslovanja predstavlja infrastruktura Informacionih Tehnologija (IT), ono je naprosto nezamislivo bez savremenih dostignuća u oblasti IT-a i svih mogućnosti koje ona pruža – neophodne su baze podataka, komunikacioni tokovi, trenutačna obrada podataka, uvek dostupan pristup servisima i proizvodima banke. Sa druge strane, razvoj IT –a prati i nastanak određenih pojava negativnog karaktera kojima se ugrožava bezbednost informacija, podataka i IT. Vanredni događaji u funkcionisanju IT-a mogu prouzrokovati direktne materijalne i reputacione gubitke, upotreba IT infrastrukture u bankarstvu nosi veliki stepen rizika, pri čemu najveći ne predstavljaju napadi na IT od spolja, već interne namerne i/ili nenamerne zloupotrebe. IT bezbednosna obuka o zaštiti i bezbednosti informacija u oblasti bankarstva je jedna od najvažnijih odgovornosti banke kao značajne finansijske institucije, čije delatnosti podrazumevaju novčane transakcije, finansijske usluge i druge osetljive zadatke. Adekvatna obuka zaposlenih iz oblasti IT bezbednosti predstavlja prvi vid preventivne zaštite.*

Ključne reči: *Zaštita podataka, bezbednost informacija, bankarstvo, bezbednosna obuka*

Abstract: *Information Technology (IT) presents the basis of modern banking, which is simply unimaginable without modern achievements in the field of IT and all the opportunities it offers - the necessary data bases, communication flows, instant data processing, always available access to bank services and products. On the other hand, the development of IT is followed by the emergence of certain events of negative character which threatens the security of information, data and IT. Extraordinary events in the functioning of IT can lead to direct financial and reputational losses, the use of IT infrastructure in banking carries a high degree of risk, while the highest risk values do not represent attacks on the IT from outside, but internal intentional and/or unintentional misuse. IT security training on protection and information security in the banking sector is one of the most important responsibility of the Bank as a major financial institution, whose activities include money transactions, financial services and other sensitive tasks. Adequate training of employees in the field of IT security is the first aspect of preventive protection.*

Keywords: *Data protection, information security, banking sector, security training*

1. UVOD

„Bezbednosni sistemi moraju uvek pobediti, ali je napadaču dovoljno da samo jednom pobedi.“ – Dustin Dykes.

Živimo u eri kompjuterizacije, spojenih mreža i naglog razvoja Informacionih Tehnologija. Moderno poslovanje je jednostavno nezamislivo bez upotrebe automatizovanih računara. Tako je i u finansijkom, bankarskom sektoru. U pogledu IT-a, obrada podataka je najosnovnija delatnost jedne banke, a to se efikasno može postići isključivo pomoću računara i IT mreže.

Za uspešno obavljanje i izvršavanje poslovnih procesa neophodno je adekvatno rukovanje ovom opremom, ono je od ključnog značaja za poslovne uspehe. A kako bi se funkcionisanje vršilo na željeni način neophodno je da računarima i mrežom upravljaju dobro obučeni ljudi.

Međutim, mali je broj onih koji su svesni da pored „tipičnih“ korisnika postoje i oni koji imaju druge ciljeve od uobičajenog funkcionisanja IT sistema. Većina pretpostavlja da je svaki korisnik „dobronameran korisnik“ koji za cilj ima isključivo upotrebu odgovarajućeg servisa, ali je nezamarljiv broj onih koji imaju nameru da dati informacioni sistem iskoriste za pribavljanje materijalne koristi sebi ili drugima putem kriminalnih delatnosti, kao i da nanesu reputacionu štetu.

Bankarstvo počiva na IT infrastrukturi u celini, zbog čega vanredni događaji iz ove oblasti imaju ključan uticaj na poslovanje banke. Jednostavno rečeno, ako IT sistem ne nije u stanju operativnosti, banka ne može efikasno da funkcioniše. Upravo je zbog te činjenice od velikog značaja da korisnici IT sistema budu dobro obučeni. I to ne samo iz oblasti ispravne upotrebe sistema, nego dati i odgovore na to kako zaštiti taj sistem, i kako ga iskoristiti za zaštitu. Zbog toga bi svi zaposleni morali da pohađaju IT bezbednosnu obuku koja bi pokrivala oblast adekvatnog i bezbednog rukovanja svih Informacionih Tehnologija u banci, kao i zaštitu i bezbednost informacija.

Klijenti i korisnici svih finansijskih institucija imaju velika očekivanja od službenika, koja nije lako zadovoljiti. Samo dobro obučena lica mogu ispuniti zahteve ovih očekivanja i zbog toga je vrlo važno održavati redovne IT bezbednosne obuke u bankarstvu.

2. ZNAČAJ IT BEZBEDNOSNE OBUKE

Kriminalno ugrožavanje finansijskih institucija se može realizovati eksternim, internim ili spregom tih dva faktora. Najveći rizik ne predstavljaju razni mogući napadi preko interneta, tj. spoljne mreže, već su to interni faktori – sami zaposleni te institucije, bilo da se radi o namernim zloupotrebama, slučajnim greškama, ili greškama iz neznanja. Najveću potencijalnu štetu mogu prouzrokovati eksterno – interni faktori. Prvu liniju odbrane od kriminalnih ugrožavanja ne čini fajervol, već su to zaposleni, te je neophodno postojanje njihove adekvatne bezbednosne svesti i obučenosti u oblasti bezbednosti informacija.

IT bezbednosna obuka zaposlenih u banci treba da pokriva mogućnosti, načine i ciljeve upotrebe računara i celokupne IT infrastrukture. Takođe, bilo bi od velikog značaja ako bi se obukom obuhvatili i klijenti, korisnici finansijskih institucija. Naglim razvojem modernih tehnologija, neophodno je da i klijenti budu upoznati sa bezbednim načinom upotrebe tih tehničko-tehnoloških dostignuća. Nije dovoljno dati uputstvo za upotrebu neke funkcionalnosti, nepohodno je da znaju i kako da zaštite istu. Na primer, novčane transakcije se danas mogu izvršiti i upotrebom mobilnog telefona. Klijentu se jasno daju instrukcije o načinima upotrebe raznih funkcionalnosti mobilnog bankarstva, ali se retko kada skreće pažnja na bezbedno rukovanje istima, o načinima zaštite i mere opreza.

Pri obuci iz oblasti zaštite informacija treba naglašavati da računar ne samo da može biti objekat napada, već i:

- Resurs za izvršenje kriminalnih delatnosti, kao i
- Resurs za planiranje, skrivanje i organizovanje kriminalnih delatnosti sa velikim gubicima.

Takođe, bezbednosna obuka treba da naglašava da se računar može upotrebiti kao:

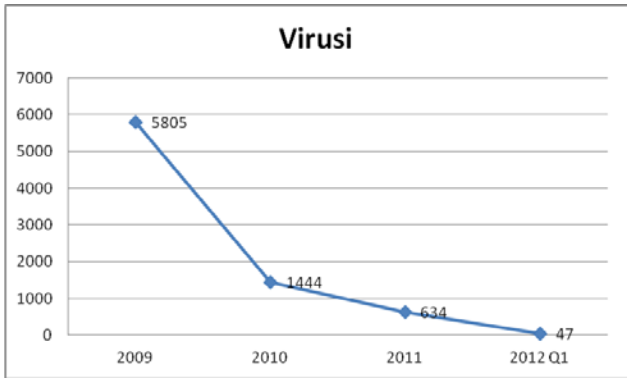
- Resurs za borbu protiv kriminalnih delatnosti koji ugrožavaju obradu podataka i tako i celokupno bankarsko poslovanje – preventivna zaštita,
- Resurs za otkrivanje, razjašnjavanje i dokazivanje kriminalnih dela protiv banke – represivna zaštita.

Pri obuci potrebno je dati jasne odgovore na sledeća pitanja:

- Šta treba štititi? Zaposleni treba da su svesni da banka rukuje sa osetljivim informacijama (podaci o klijentima, zaposlenima, poslovnim procesima, transakcijama, stanjima na računima, itd.) i da te informacije, podatke, kao i infrastrukturu koja obrađuje te podatke moraju zaštititi.
- Koji su izvori ugrožavanja? Kod ovog pitanja potrebno je identifikovati rizike, definisati od koga i od čega treba štititi informacije i celokupnu IT infrastrukturu.
- Zašto treba štititi informacije? Potrebno je utvrditi moguće posledice i gubitke, tj. štetu koju banka, pa samim tim i klijenti, može pretrpeti u slučaju ostvarivanja nekih od pretnji. Sa aspekta bezbednosti informacija, tri ključna faktora za razmatranje su integritet, poverljivost i raspoloživost informacija.
- Čime i kako štititi informacije? Odgovor na ovo pitanje treba da sadrži izbor mera i sredstava koja će se koristiti u cilju zaštite informacija. U osnovi, zaštita može biti preventivna i represivna.

Obuka mora biti kontinualna. Isto kao što se tehnologije i metode napada kontinualno razvijaju, menjaju, tako i metode preventivne i represivne zaštite informacija. Zaposleni moraju biti svesni za potrebom IT bezbednosne obuke kako bi bili otvoreni za prihvatanje znanja iz ove oblasti. Treba da im je jasno da iako bezbednost nije poslovni proces koji donosi profit, ona je sastavni deo poslovnog procesa i itekako je važna za osiguranje neprekidnog poslovanja, pa samim tim i za osiguranje profita. Bezbednost ne treba da sprečava izvršenje poslovnih procesa, već treba da osigura bezbednost istih. Upravo zbog toga zaštitu informacija i IT bezbednost ne treba gledati kao trošak, već kao investiciju.

Slika 1. prikazuje primer očekivanog rezultata dobre obuke zaposlenih iz oblasti zaštite i bezbednosti informacija, u korporativnom okruženju. Grafikon prikazuje broj virusnih događaja u jednoj domaćoj banci u periodu od 2009 – 2012 Q1.

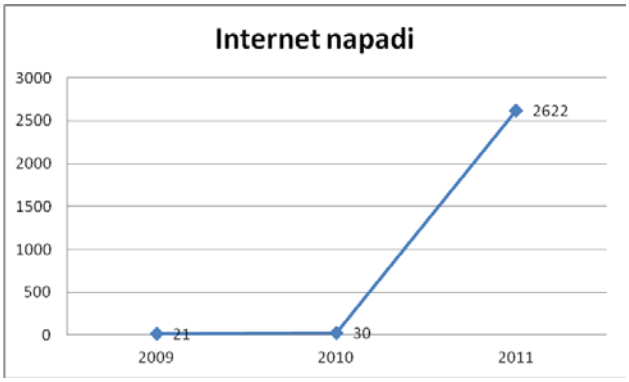


Slika 1: Broj virusa naglo opada

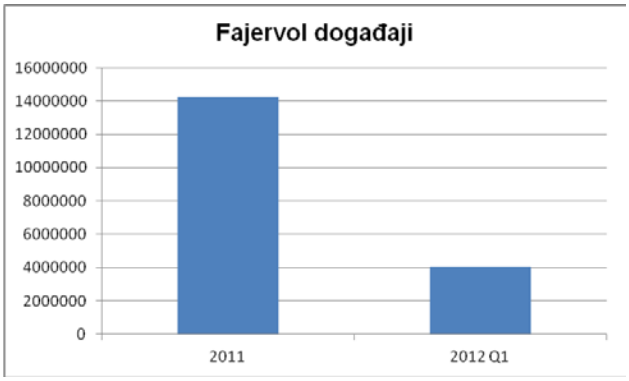
Jasno se vidi da pored odgovarajućeg tehničkog rešenja za antivirusnu zaštitu, zahvaljujući kontinualnoj IT bezbednosnoj obuci u cilju zaštite i bezbednosti informacija, zaposleni su sve više i više oprezniji pri upotrebi svojih računara u obavljanju dnevnih aktivnosti na svojim radnim mestima. Slika pokazuje da iako se broj virusa u svetu konstantno povećava pojavom sve više i više zlonamernih softvera, koji na razne načine ugrožavaju bezbednost informacija pohranjenih u informacionom sistemu, broj virusnih pojava u IT sistemu banke je vremenom sve manji i manji. Broj se verovatno neće svesti na nulu, ali je od ključnog značaja da taj broj teži nuli, tj. da se beleži konstantno smanjenje. Postići ovaj rezultat nije bilo moguće bez fundamentalne i kontinualne obuke zaposlenih.

Slike 2. i 3. pokazuju da su pretnje i napadi konstantni i da se mora obezbediti adekvatna preventivna zaštita, bilo da je reč o tehničkoj ili zaštiti putem preduzimanja adekvatnih mera od strane zaposlenih. Direktni napadi

preko interneta na neke od IT sistema banke, kao i fajervol događaji su stalni i učestali.

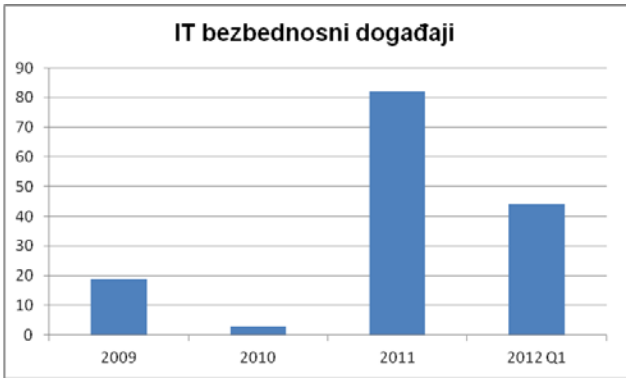


Slika 2: Broj direktnih napada preko interneta



Slika 3: Broj fajervol događaja u periodu od 2011 – 2012 Q2

Broj otkrivenih i obrađenih događaja iz domena zaštite informacija i bezbednosti IT je u porastu. Ova činjenica ukazuje na to da je obuka u cilju zaštite i bezbednosti informacija neophodna i nezaobilazna kako bi se adekvatno izborili sa sve više i više pretnji koji ugrožavaju ispravan rad sistema, a samim tim i banku u celini. Slika 4. Pokazuje broj događaja u periodu od 2009 – 2012 Q1.



Slika 1: Broj događaja raste

3. MODEL IT BEZBEDNOSNE OBUKE

Savremeni model obuke podrazumeva upotrebu usvajanja cikličnog znanja. Svi zaposleni treba da aktivno učestvuju u obuci, koja treba da obuhvati i praktična iskustva, kako lokalna, tako i u svetu. Obuka treba da se oslanja na moderne tehnologije, da ove tehnologije iskoristi za postizanje krajnjeg cilja: pružiti osnovnu IT bezbednosnu svest i znanje svim zaposlenima. Obuka treba da bude aktivna i da pruži motivaciju. Treba da je sveobuhvatna, planirana i dobro organizovana.

Na tržištu postoje razni komercijalni, kratkoročni kursevi, koji traju samo jedan dan, ili svega nekoliko sati. Međutim obuka iz oblasti zaštite i bezbednosti informacija ne treba da bude pitanje kursa, već obrazovanja. Naravno, uvek je lakše platiti neku uslugu nego je samostalno izvršiti, ali kada je u pitanju bezbednost ključno je posedovati sveobuhvatno i efikasno obrazovanje, iako to znači dodatan posao onima koji su određeni za poslove bezbednosti u banci. Obuka je najbolji način preventivne zaštite i bezbednosti informacija. Ako zaposleni poseduju odgovarajuću svest i znanje iz oblasti IT bezbednosti, tada je i sama banka bezbednija, i to nezavisno od tehničko – tehnoloških rešenja zaštite. Ne treba zaboraviti, prvu liniju odbrane čine sami zaposleni.

Obuka se može izvoditi na licu mesta ili udaljeno. U slučaju obuke na licu mesta, predavač treba da se pripremi sa prezentacijom za datu priliku, a treba i da organizuje mesto održavanja obuke. Pored toga, neophodno je i organizovati zaposlene koji će prisustvovati i učestvovati na obuci, što i nije tako trivijalan zadatak. U slučaju da zaposlenima u predavanju nešto nije jasno, oni svoja pitanja mogu trenutačno postaviti predavaču, mogu ga zaustaviti u svakom trenutku. Kod izvođenja obuke udaljenom metodom, ona se može realizovati ili preko e-mailova ili preko onlajn sistema u ili izvan IT mreže firme. Ako se predavač odluči za model izvođenja obuke putem e-mailova, treba da bude svestan da slanje materijala za obuku velikom broju primaoca može imati negativan uticaj na opterećenje e-mail servera, kao i mrežne komunikacije. Ako neko od zaposlenih ima pitanje, ono se može postaviti putem e-maila ili preko telefona. U slučaju odabira onlajn obuke, predavač ima nekoliko mogućih izbora. Obuka se može realizovati preko intraneta ili interneta. Mrežno opterećenje i pristup internetu je u ovom slučaju ključno za razmatranje ove opcije.

Onlajn obuka koja se izvodi unutar IT mreže firme može biti realizovana na nekoliko načina:

- Kreirati prezentaciju sa slajdovima (npr. PowerPoint odštampan u PDF) i učiniti ga dostupnim za zaposlene za daunlodovanje.
- Kreirati internet prezentaciu (sajt) i poslati link zaposlenima na taj sajt.

Koristeći opciju internet prezentacije postoje razne mogućnosti: upotreba PHP, HTML, SharePoint, Shockwave animacije, itd. Takođe, postoji i opcija vremenskog ograničenja, tj. da prezentacija nije dostupna kontinualno, već samo u zadatim vremenskim intervalima.

Ako firma poseduje dobru IT infrastrukturu i širokopropusnu IT mrežu, tada se obuke mogu organizovati i u obliku video konferencija, „webinara“.

Vrlo je važno dobro proceniti očekivani broj učesnika i očekivano mrežno opterećenje.
Izvođenje udaljene obuke takođe donosi i uštedu troškova, što u vreme finansijske krize predstavlja možda i najveći adut u odnosu na obuku na licu mesta. Nema troškova putovanja, organizovanja prostora za izvođenje obuke. Takođe, udaljena obuka znači i vremensku uštedu, što je isto tako ključno kada vreme znači i novac.
Nakon završenog kruga obuke, treba da postoji i način procene uspešnosti izvođenja iste, da bi se mogla utvrditi efikasnost same obuke, kao i potrebna poboljšanja u vezi izvođenja obuke za sledeći ciklus. Jedan od načina koji bi ovo obezbedio jeste testiranje zaposlenih nakon održane obuke. Pri tome bi se testiranje koristilo isključivo za procenu efikasnosti obuke, a ne i za utvrđivanje buduće radne pozicije, niti bilo kakav vid sankcionisanja.
Testiranje se, takođe, može izvršiti na licu mesta ili udaljeno. Test se može uraditi na papiru, potpisanu verziju uvek poslati nazad predavaču, ili se može realizovati i preko popunjavanja onlajn upitnika. U slučaju papirnatog oblika testa, predavač mora da sakupi sve popunjene testove i da ih ručno ocenjuje i analizira. Dok kod onlajn testiranja, obrada podataka vrši se preko nekog, automatizovanog IT sistema koji ima razne mogućnosti analiza i kreiranja statističkih izveštaja u vezi rezultata. Pri onlajn testiranju kako bi se izbegli neki od mogućnosti varanja, može se uvesti i autorizovan pristup samom testu, tj. da pristup bude ograničen korisničkim nalogom i lozinkom. Takođe, postoji i mogućnost da se test zatvori ukoliko korisnik napusti dati prozor u kome je otvorio test, kako bi pronašao odgovor na internetu.

4. IT BEZBEDNOSNA OBUKA U JEDNOJ DOMAĆOJ BANCI

Iskustva iz prošlog perioda

Do 2011. godine obuke iz oblasti zaštite i bezbednosti informacija su se izvodili na licu mesta. Obukom nisu bili obuhvaćeni svi zaposleni, već nekoliko odabranih za svaki geografski region. Oni koji su pohađali obuku imali su obavezu da stečeno znanje prenesu svojim kolegama. Ako je tokom obuke neko imao neko pitanje, mogao je da ga postavi odmah. S obzirom da nije bilo nikakve druge povratne informacije, ukoliko nije bilo pitanja, nije se znalo da li je učesnicima bilo sve jasno, ili jednostavno nisu bili zainteresovani. Pre svake obuke, bilo je neophodno organizovati mesto izvođenja obuke, učesnike i put do mesta održavanja obuke – ponekad i nekoliko stotina kilometara.
U 2011. godini došlo je do poboljšanja u izvođenju obuke. Obuka više nije održavana na licu mesta, već onlajn, preko IT mreže banke, i to preko e-mail sistema. Materijal za pobuku je poslat rukovodiocima zaposlenih, koji su bili u obavezi da ga proslede neposredno podređenim zaposlenima. I u ovom slučaju, obuka nije izvođena odjednom svima, već su se formirale grupe i obuka je održava po grupama. Kao krajnji rezultat, obuku su pohađali svi zaposleni. Ukoliko nekome nešto u materijalu nije bilo jasno, pitanja su mogli postaviti ili preko e-maila ili preko telefonskog razgovora. Kao još jedno poboljšanje, uvedeno je i testiranje zaposlenih, u papirnatom obliku. Svi zaposleni koji su pohađali obuku, popunili su test, potpisali ga i dostavili predavaču. Ove novine su se dobro pokazale, jer su svi zaposleni bili uključeni u obuku, bilo je povratne informacije preko rešavanja testova, i nije bilo troškova putovanja, niti potrebe za organizovanjem mesta izvođenja obuke. Međutim, obuka izvođena na ovaj način rezultirala je dodatnim opterećenjem e-mail sistema (poslat materijal i primljen skeniran test), a prikupljanje i obrada testova od svih zaposlenih (preko 500) nije bio jednostavan zadatak.

Trenutno rešenje

U 2012. godini uspostavlja se poptuna onlajn obuka iz oblasti zaštite i bezbednosti informacija u banci. Materijal je zaposlenima dostupan onlajn preko intranet mreže banke, u svakom trenutku. Materijal je PowerPoint prezentacija odštampana u PDF, i sadrži sledeća poglavlja:

- Odgovornost zaštite informacija.
- Koristiti i zaštiti svoju lozinku.
- Internet koristiti u skladu sa normativnim aktima banke.
- Službeni e-mail koristiti u skladu sa normativnim aktima banke.
- Zaštititi svoj računar.
- Zaštititi podatke.
- Zaštititi nosioce podataka.
- Zaštititi podatke od posetilaca.
- Zaštititi informacije van banke.
- Prijaviti sve incidente i kvarove nosilaca podataka.

Nakon odabira grupe učesnika, link na materijal je poslat rukovodiocima koji imaju obavezu da ga proslede neposredno podređenim zaposlenima. Ako je neko od zaspolenih odsutan, tađa će on biti izabran i u drugoj grupi. Nakon dostavljanja linka, daje se izvesno vreme za upoznavanje sa materijalom, posle čega se popunjava test. Test je kreiran PHP programiranjem, postoji 12 pitanja, od kojih svi imaju istu težinu i koeficijent. Zaposleni pristupaju materijalu za obuku bez autentifikacije, ali je test dostupan samo uz korisničko ime i lozinku. Tako je obezbeđeno da predavač zna ko je popunio test. Ako bi učesnik sam popunjavao svoje ime i prezime, tada ne bi postojala adekvatna kontrola kako bi se eliminisala mogućnost popunjava testa u ime nekog drugog – bilo da je reč o nameri pomaganja, ili da se nekom nametnu loši rezultati. Nakon što se korisnik uloguje na test, ima 20 minuta da ga popuni. 70% datih tačnih odgovora se smatra pozitivnim rezultatom. S ozbirom da se testiranje koristi samo da bi se procenila efikasnost obuke, ocene pokazuju da li ima potrebe za dodatnom obukom za datog zaposlenog. Ukoliko neko ne postigne pozitivan rezultat tada se organizuje dodatna obuka na licu mesta.
Odabir onlajn obuke iz oblasti zaštite informacija znači veću efikasnost pošto pokriva sve zaposlene, a ne samo nekoliko odabranih. Rezultati testiranja se lako analiziraju s obzirom da dolazi u formi Excel tabele, iz koje se

podaci mogu obraditi na razne načine za potrebe raznih izveštavanja. Takođe, ovaj oblik obuke znači i finansijsku uštedu jer nema troškova putovanja – u banci ima preko 500 zaposlenih širom Srbije. I na kraju, štiti se i životna sredina s obzirom da se testiranje vrši onlajn, a ne popunjavanjem papira.

5. ZAKLJUČAK

IT bezbednosna obuka u cilju zaštite i bezbednosti informacija u bankarstvu je od ključnog značaja, kako za zaposlene, tako i za poslovne procese i banke u celini. Obuka mora biti ciklična i kontinuirana, a ne da traje svega nekoliko sati na nekom od komercijalnih kurseva. Zaposlenima treba da je jasno da oni predstavljaju prvu liniju odbrane u zaštiti poslovanja banke od kriminalnih delatnosti, koji mogu biti rezultat internih, eksternih i kombinovanih zloupotreba. Zaposleni moraju biti svesni svojih odgovornosti, kao i da prepoznaju potencijalne vanredne događaje iz oblasti bezbednosti informacija, i ukoliko je moguće treba da spreče takve događaje. Adekvatna obuka zaposlenih predstavlja prvi vid preventivne zaštite.

Na osnovu iskustava iz prošlosti može se zaključiti da je model onlajn obuke najefikasniji. Pokriva sve zaposlene, bez obzira na njihov ukupan broj i geografski položaj. U odnosu na model obuke na licu mesta, smanjuje troškove i uloženo vreme. Takođe, izvođenje obuke na ovaj način štiti se i životna sredina.

Ovim radom, autor je želeo da ukaže na značaj IT bezbednosne obuke, i doprinese njenom prisutnošću u svim sektorima gde se obrađuju osetljivi, poverljivi i tajni podaci.

LITERATURA

[31] Mitnick D. K., Simon L. V., A megtévesztés művészete, Perfact-Pro Kft., Budapest, 2003.

[32] Mitnick D. K., Simon L. V., A behatolás művészete, Perfact-Pro Kft., Budapest, 2006.

[33] Petrović R. S., Kompjuterski kriminal, II izdanje, Ministarstvo unutrašnjih poslova Srbije, Beograd, 2001.

[34] Sotirović V., Egić B., Pravna informatika, INED Grafomedia d.o.o., Novi Sad, 2008.

[35] *Informatikai Tárcaközi Bizottság ajánlásai*, Informatikai Koordinációs Iroda, Miniszterelnöki Hivatal, http://www.itb.hu/ajanlasok/a8/

Konferencija o bezbednosti informacija BICES 2012
Univerzitet Metropolitan

BEZBEDNOST INFRASTRUKTURE I PODATAKA U CLOUD COMPUTING OKRUŽENJU

INFRASTRUCTURE AND DATA SECURITY IN CLOUD COMPUTING ENVIRONMENT

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

Rezime: *U ovom radu biće razmatrane pretnje i izazovi u vezi obezbeđivanja IT infrastrukture na nivoima mreže, hosta i aplikacije, kao i u kontekstu modela isporuke cloud servisa (Softver-kao-Servis, Platforma-kao-Servis i Infrastruktura-kao-Servis). U slučaju privatnih oblaka, razmatranja o bezbednosti infrastrukture su ograničena na one slojeve infrastrukture koji se nalaze van domašaja kontrole korisnika i predstavljaju odgovornost servis provajdera (tj. odgovornost za bezbednost infrastrukture se prenosi na cloud servis provajdera, na osnovu modela isporuke cloud servisa). Razmatranja data u ovom radu su od suštinske važnosti za razumevanje toga za koje aspekte bezbednosti infrastrukture je odgovoran cloud servis provajder a za koje sam korisnik.*

Ključne reči: *Informaciona bezbednost, Infrastruktura, Servisi, Cloud Computing, Kriptografija*

Abstract: *In this paper, we discussed the threats and challenges related to securing the IT infrastructure at the network, host and applications level, as well as in the context of cloud service delivery model (Software-as-a-Service, Platform-as-a-Service and Infrastructure-as- a-service). In the case of private clouds, considerations about infrastructure security are limited to those layers of infrastructure that are beyond the reach of the user's control and they represent the responsibility of service providers (ie. responsibility for the security infrastructure is transferred to the cloud service provider, based on cloud model of delivery service). The considerations presented in this paper are essential to understanding for which aspect of the security infrastructure is responsible the cloud service provider and for which is responsible the user.*

Keywords: *Information security, Infrastructure, Services, Cloud Computing, Cryptography*

1. UVOD

Razvoj računara se kroz istoriju najviše zasnivao na povećavanju računarske snage. Redovno su izlazile nove verzije procesora različitih namena, koji bi dodatno podigli granicu u odnosu na prethodnu generaciju. Pojavom *multicore* procesora pojačao se i razvoj metoda paralelizacije, pa su, osim brzine, proizvođači pojačali i razvoj programske potpore za efikasno korišćenje novih arhitektura, a programi su počeli da im se prilagođavaju. Međutim, za krajnjeg korisnika, osim kupovine novih računara, danas postoji još jedna vrlo popularna alternativa. Razvojem interneta, njegovim širenjem i povećavanjem brzina pristupa, omogućeno je da se određeni zadaci obavljaju udaljeno. Ideja je da korisnik, umesto ulaganja u nove računare i opremu, može sa postojećom ili čak slabijom opremom dobiti uslugu za koju je potrebna naprednija arhitektura. Pomoću tih uređaja korisnik pristupa preko interneta sa zahtevom na koji dobija natrag rezultat. To se naravno naplaćuje; ipak, za neke korisnike je isplativije od nabavljanja nove opreme. Takav oblik pružanja usluga se naziva *cloud computing*-om i bazira se na iznajmljivanju vlastite arhitekture za obavljanje raznih zadataka, od običnih usluga poput pisanja dokumenata do izvođenja složenijih virtuelnih zadataka. Sva komunikacija između korisnika i iznajmljenih računara odvija se preko interneta [1].

Tokom 2008. godine *cloud computing* našao se u središtu zbivanja medija posvećenim informacionim tehnologijama (IT). U roku od samo nekoliko meseci, *cloud computing*, nekada relativno malo poznat koncept, postao je najprimamljivija tehnologija godine. Čitav niz kompanija pridružio se novom trendu, lansirajući nove usluge vezane za *cloud computing*. U mnogim slučajevima, radilo se samo o preimenovanju postojeće ponude kako bi se iskoristile nove okolnosti. Ukratko, radilo se o medijskoj groznici najvišeg nivoa.

Međutim, strasti se polako smiruju i IT mediji, kao i analitičari i sama informatička industrija, danas imaju u mnogo većoj meri realističan pogled na tehnologiju *cloud computing*-a. Na primer, *Gartner* ide toliko daleko da predviđa da će *cloud computing* proći kroz period razbijanja iluzija – tj. fazu u medijskom ciklusu u kojoj nove tehnologije ne uspevaju da ispune očekivanja i brzo izlaze iz mode.

Uprkos senzacionalizmu i za razliku od mnogih tehnologija koje su joj prethodile, kao što su video telefonija, kancelarija bez papira i mobilna televizija, *cloud computing* će sasvim sigurno ostati prisutan i

evoluirati tokom godina koje slede. Potpuno će izmeniti način rada ljudi, kao i poslovanje kompanija, omogućavajući im da koriste usluge na ekonomičniji način.

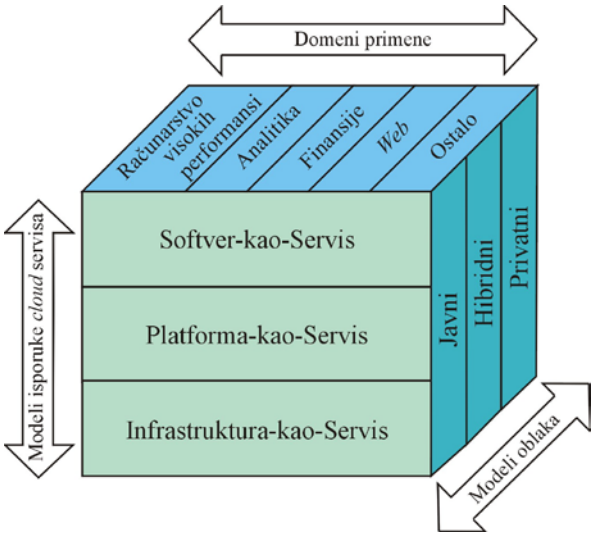
Usluge *cloud computing*-a naročito su privlačne za male ili početničke kompanije koje ne mogu da priušte velike inicijalne investicije u informatičku opremu. Ipak, nije verovatno da će veće organizacije potpuno napustiti model informatičkih aktivnosti na licu mesta ili da će informatičke kapacitete koji imaju centralnu ulogu u njihovoj tržišnoj konkurentnosti, zameniti uslugama *cloud computing*-a. Mnoge kompanije i dalje će zahtevati nivo bezbednosti, performansi ili specijalizacije aplikacija koji ne može biti dostignut korišćenjem javnih usluga *cloud computing*-a. One će možda formirati sopstvenu privatnu arhitekturu *cloud computing*-a, skrivenu iza korporativnih zaštitnih zidova *(firewall)*, kako bi iskoristile njihovu efikasnost, ali uz veću bezbednost i kontrolu [2].

Ukratko, *cloud computing* ne predstavlja prolaznu modu, ali ni revoluciju u elektronskom poslovanju. Umesto toga, većina kompanija verovatno će koristiti kombinovano informatičko okruženje, u kojem će aplikacije, infrastruktura i u pojedinim slučajevima, svi poslovni procesi, biti realizovani putem javnih i privatnih oblaka.

Posle uvodnog dela, u ovom radu biće opisani aspekti koji se odnose na bezbednost infrastrukture i to na nivou mreže, hosta i aplikacije. Bezbednost aplikacija je razmatrana u okviru nekoliko *cloud computing* modela. Posebno je uzeto pri tome u obzir ograničenje bezbednosti u javnom oblaku. U nastavku će biti reči o bezbednosti podataka u *cloud computing* okruženju, imajući posebno u vidu bezbednost podataka provajdera i odgovarajuće kriptografske metode za unapređenje bezbednosti podataka korisnika.

2. BEZBEDNOST INFRASTRUKTURE

Framework koji se koristi za opisivanje *cloud computing* servisa poznat je pod akronimom *SPI* i označava tri najveća servisa, tj. usluge koje se pružaju putem oblaka, a to su: Softver-kao-Servis *(SaaS, Software-as-a-Service)*, Platforma-kao-Servis *(PaaS, Platform-as-a-Service)* i Infrastruktura-kao-Servis *(IaaS, Infrastructure-as-a-Service)* [3].



Slika 1: SPI *framework* za *cloud computing*

Slika 1 ilustruje vezu između ovih servisa, njihove upotrebe i modela oblaka.

2.1 BEZBEDNOST INFRASTRUKTURE NA NIVOU MREŽE

Za razmatranje bezbednosti infrastrukture na nivou mreže, važno je uočiti razliku između javnih i privatnih oblaka.

U slučaju privatnih oblaka, ne postoje nove vrste napada, ranjivosti ili bilo kakvih drugih promena vezanih za rizik, koje bi bile specifične za ovu topologiju. Iako može doći do promene u IT arhitekturi preduzeća nakon implementacije privatnog oblaka, topologija mreže se verovatno neće značajnije promeniti.

S druge strane, korišćenje usluga koje se pružaju putem javnih oblaka zahteva određene promene mrežne topologije. Važno je znati u kakvoj su interakciji postojeća mrežna topologija i topologija mreže provajdera oblaka. U ovom slučaju postoje tri značajna faktora rizika:

- Obezbeđivanje poverljivosti i integriteta podataka u tranzitu *(data-in-transit)* do i od provajdera javnog oblaka;
- Obezbeđivanje adekvatne kontrole pristupa (što podrazumeva proveru autentičnosti, autorizaciju i proveru) svim resursima smeštenim u javnom oblaku;
- Zamena uspostavljenog modela mrežnih zona domenima.

Preduzeća koja koriste usluge javnog oblaka suočavaju se sa značajnim porastom rizika koji preti podacima zato što su, u tom slučaju, pojedini resursi (ili čak svi) izloženi internetu i javnoj deljenoj mreži koju poseduje provajder oblaka. Mogućnost provere rukovanja mrežom od strane provajdera javnog oblaka (a kamoli nadgledanje rada u realnom vremenu, kao u slučaju posedovanja sopstvene privatne mreže) praktično ne postoji. Takođe su

ograničene mogućnosti sprovođenja istrage i prikupljanja forenzičkih podataka u slučaju incidenta neovlašćenog pristupa.

Faktori rizika na nivou mreže postoje bez obzira na model isporuke servisa u *cloud computing*-u (Softver-kao-Servis, Platforma-kao-Servis ili Infrastruktura-kao-Servis). Određivanje nivoa rizika, stoga, ne zavisi od modela isporuke *cloud* servisa, već od tipa oblaka koji se koristi (javni, privatni ili hibridni oblak). Naravno, korišćenjem privatnog oblaka rizici će biti umanjeni. Postavlja se pitanje: da li je rizik korišćenja javnih oblaka veći od rizika sa kojima se preduzeća danas suočavaju? U mnogim slučajevima, odgovor je najverovatnije ne – ne postoji viši nivo rizika [3].

2.2 BEZBEDNOST INFRASTRUKTURE NA NIVOU HOSTA

Prilikom razmatranja bezbednosti infrastrukture na nivou hosta i procenjivanja rizika, u obzir treba uzeti kontekst modela isporuke *cloud* servisa (*SaaS*, *PaaS* i *IaaS*) i tipova oblaka (javni, privatni i hibridni). Iako ne postoje nove pretnje hostovima koje su specifične za *cloud computing*, dinamična priroda, tj. elastičnost *cloud computing*-a, može doneti nove izazove iz perspektive upravljanja bezbednošću. Pored toga, činjenica da oblaci koriste snagu hiljada računarskih čvorova znači da se pretnje mogu proširiti brzo i lako, što se može nazvati faktorom brzine napada u oblaku.

Uobičajeno je da *cloud* servis provajderi ne puštaju u javnost informacije vezane za platforme hostova, operativne sisteme, kao i načine na koje obezbeđuju hostove, zbog toga što hakeri mogu da iskoriste takve informacije prilikom napada.

Suštinska razlika između modela isporuke *cloud* servisa koji se koristi ogleda se u tome da je, u slučaju upotrebe Softvera-kao-Servisa i Platforme-kao-Servisa, za bezbednost na nivou hosta odgovoran *cloud* servis provajder, dok su, u slučaju korišćenja Infrastrukture-kao-Servisa, za bezbednost hostova u najvećoj meri odgovorni korisnici [3].

2.3 BEZBEDNOST INFRASTRUKTURE NA NIVOU APLIKACIJE

Za bezbednost infrastrukture na nivou aplikacije odgovornost snose i korisnik i *cloud* servis provajder; njihov udeo u toj odgovornosti zavisi od modela isporuke *cloud* servisa *(SPI)*. Ključno je shvatiti koje su odgovornosti korisnika a koje provajdera oblaka.

Nedavna istraživanja su istakla činjenicu da je nedostatak transparentnosti u radu zaposlenih od strane *cloud* servis provajdera prepreka za usvajanje koncepta *cloud computing*-a. Upravo zbog tog nedostatka transparentnosti, korisnicima ne preostaje ništa drugo osim da veruju svojim provajderima da će na adekvatni način zaštititi poverljivost, integritet i dostupnost njihovih aplikacija [3].

Softver-kao-Servis model podrazumeva da provajder upravlja čitavim paketom aplikacija koje se isporučuju korisnicima. Stoga su provajderi *SaaS* modela u velikoj meri odgovorni za bezbednost aplikacija i komponenti koje nude korisnicima. Korisnici su najčešće odgovorni za operativne bezbednosne funkcije, uključujući upravljanje pristupom.

Posebnu pažnju treba posvetiti funkcijama provere autentičnosti i kontrole pristupa, koje nudi *cloud* servis provajder *SaaS* modela. To je najčešće jedini način kontrole bezbednosti koji je dostupan za upravljanje rizikom kome su informacije izložene.

Mnogi provajderi nude korisnički interfejs sa alatima za proveru autentičnosti i kontrolu pristupa aplikacijama. Pojedine *SaaS* aplikacije imaju ugrađene funkcije pomoću kojih korisnici mogu da dodele privilegije čitanja i pisanja drugim korisnicima. Međutim, upravljanje takvim privilegijama može imati slabe tačke zbog kojih njihovo korišćenje ne bi bilo u skladu sa standardima kontrole pristupa nekog preduzeća. Primer koji ukazuje na ovakvu vrstu problema odnosi se na mehanizam koji *Google Docs* koristi za rukovanje slikama ugrađenim u dokumentima**,** kao i na privilegije pristupa starijim verzijama dokumenata. Jasno je da slike ugrađene u dokumentu uskladištenom u *Google Docs* nisu zaštićene na isti način kao dokument nad kojim su kontrole deljene. To znači da će, ukoliko je dokument koji sadrži ugrađene slike deljen, drugi korisnik uvek biti u stanju da ih pregleda, čak i nakon što se ukine dozvola za deljenje dokumenta. Izvesni bloger je otkrio i skrenuo pažnju *Google*-a na ovaj propust. Iako je *Google* priznao da problem postoji, saopšteno je da takav propust ne predstavlja značajni rizik po bezbednost [3].

PaaS model, bilo da se radi o javnom ili privatnom oblaku, nudi integrisano okruženje za projektovanje, razvoj, testiranje, implementaciju i podršku korisničkim aplikacijama razvijenim na jeziku koji platforma podržava. Bezbednost aplikacija u Platforma-kao-Servis modelu obuhvata dva softverska sloja:

- Bezbednost same *PaaS* platforme;
- Bezbednost korisničkih aplikacija na *PaaS* platformi.

Uopšteno govoreći, *cloud* servis provajderi *PaaS* modela su odgovorni za obezbeđivanje platforme na kojoj se pokreću korisničke aplikacije. Aplikacije *PaaS* modela mogu da koriste komponente ili *web* servise koje pruža treća strana, tj. provajder aplikacija, pa je u tom slučaju provajder aplikacija odgovoran za bezbednost svojih usluga. Dakle, korisnici bi trebalo da razumeju zavisnost njihovih aplikacija od svih usluga i procene rizike koji se odnose na pružanje usluga od strane trećeg provajdera. Sve do sada, *cloud* servis provajderi nisu bili voljni da

otkrivaju informacije koje se tiču bezbednosti platforme, koristeći kao argument da bi takve informacije hakeri mogli da upotrebe u svoju korist. Ipak, korisnici bi trebalo da zahtevaju transparentnost od *cloud* servis provajdera i da traže pristup informacijama neophodnim za procenjivanje rizika i upravljanje bezbednošću.

U slučaju *PaaS* modela isporuke servisa, osnovni principi bezbednosti su čuvanje i izolacija aplikacija jednih korisnika od aplikacija drugih korisnika. *Cloud* servis provajder je odgovoran za praćenje novih grešaka i ranjivosti koje mogu biti iskorišćene za eksploataciju *PaaS* platforme. Takva situacija predstavlja najgori scenario za *PaaS* usluge; implikacije vezane za privatnost osetljivih korisničkih informacija su nepoželjne i mogu da nanesu veliku štetu poslovanju. Stoga bi korisnici trebalo da budu upoznati sa načinom na koji *cloud* servis provajderi upravljaju platformama [3].

U slučaju *IaaS* modela, korisničke aplikacije i platforma na kojoj se pokreću rade na virtuelnim korisničkim serverima; instaliraju ih i njima upravljaju sami korisnici. To znači da korisnici snose punu odgovornost za bezbednost aplikacija smeštenih u oblaku, pa ne bi trebalo da očekuju pomoć u obezbeđivanju aplikacija od strane *cloud* servis provajdera, osim dobijanja osnovnih smernica i upoznavanja sa karakteristikama zaštitnog zida koje mogu da utiču na komunikaciju korisničkih aplikacija sa drugim aplikacijama, korisnicima i uslugama, u okviru ili izvan oblaka.

Web aplikacije smeštene u javnom oblaku moraju biti projektovane tako da poseduju standardne bezbednosne mere protiv uobičajenih pretnji koje sa sobom nosi korišćenje interneta. Korisnici su isključivo odgovorni za čuvanje svojih aplikacija, postavljanje sigurnosnih zakrpa i zaštitu sistema od malicioznih programa i hakera koji pokušavaju da neovlašćeno pristupe njihovim podacima smeštenim u oblaku [3].

3. OGRANIČENJE BEZBEDNOSTI U JAVNOM OBLAKU

Korisnici bi trebalo da imaju u vidu da postoje izvesna ograničenja kada je u pitanju podrška bezbednosnim funkcijama u javnom oblaku. Bezbednosni zahtevi, kao što su postavljanje zaštitnog zida ili upotreba kriptografije, ne mogu biti ostvareni u Softver-kao-Servis, Platforma-kao-Servis, niti Infrastruktura-kao-Servis modelu u okviru javnih oblaka. Očekuje se da će u budućnosti *cloud* servis provajderi *PaaS* i *IaaS* modela ponuditi sofisticiranije bezbednosne funkcije, u zavisnosti od zahteva korisnika [4].

Važno je istaći da *cloud computing* sam po sebi nije uzrok nedostataka vezanih za bezbednost infrastrukture na bilo kom nivou (mreže, hosta ili aplikacije); u *cloud computing*-u su ovi izazovi naprosto došli do izražaja. Pitanja bezbednosti infrastrukture u *cloud computing*-u svode se na razumevanje u vezi sa tim koja strana pruža određene aspekte bezbednosti (da li je za njih odgovoran sam korisnik ili *cloud* servis provajder); drugim rečima, potrebno je definisati granice poverenja. Granice poverenja između korisnika i *cloud* servis provajdera su se pomerile; što je još važnije, korisnicima nije najjasnije gde se sada zapravo nalaze. Mnogi provajderi nisu jasno odredili te granice, niti su one jasno definisane u ugovorima između korisnika i provajdera *(SLA, Service-Level Agreements)* [5].

4. BEZBEDNOST PODATAKA

Bezbednost podataka uključuje u sebi više aspekata, kao što su:

- Podaci-u-tranzitu *(data-in-transit)*;
- Podaci-u-mirovanju *(data-at-rest)*;
- Obrada podataka;
- Ostaci podataka *(data remanence)*;
- Podaci provajdera;
- Skladištenje-kao-Servis *(Storage-as-a-Service)*.

Kao i u slučaju drugih aspekata bezbednosti *cloud computing*-a, nisu svi ovi aspekti bezbednosti podataka od jednakog značaja u svim topologijama, tj. razlikuju se u slučaju korišćenja javnih i privatnih oblaka, kao što postoje razlike između osetljivih i manje osetljivih podataka.

Kada su u pitanju podaci-u-tranzitu, glavni rizik po bezbednost predstavlja nekorišćenje ispitanog i proverenog kriptografskog algoritma, u slučaju korišćenja javnog oblaka, bez obzira na model isporuke *cloud* servisa (*SaaS*, *PaaS* ili *IaaS*). Takođe je važno da protokol koji se koristi pruža poverljivost i integritet (npr. *Hypertext Transfer Protocol Secure*, tj. *HTTPS*), naročito ukoliko se protokol koristi za prenos podataka preko interneta. Samo kriptovanje podataka uz korišćenje protokola koji ne osigurava bezbednost (npr. *HTTP, Hypertext Transfer Protocol*) može da obezbedi poverljivost, ali ne osigurava integritet podataka.

Iako se korišćenje kriptovanja u cilju zaštite podataka-u-mirovanju čini očiglednim rešenjem, sprovođenje ove ideje u stvarnosti nije tako jednostavno. Ukoliko se koristi *IaaS* model (bilo u okviru javnog ili privatnog oblaka) samo za skladištenje podataka, kriptovanje podataka-u-mirovanju je moguće, čak je i preporučeno. Međutim, kriptovanje podataka-u-mirovanju koje koristi aplikacija *PaaS* ili *SaaS* modela nije uvek izvodljivo. Podaci-u-mirovanju, koje koristi aplikacija bazirana na oblaku, obično se ne kriptuju, zato što bi kriptovanje onemogućilo indeksiranje ili pretraživanje podataka.

Podaci-u-tranzitu mogu biti kriptovani za vreme njihovog transfera do i od provajdera oblaka, kao što podaci-u-

mirovanju mogu biti kriptovani ukoliko se samo skladište. Međutim, podaci ne mogu biti kriptovani ukoliko je potrebno obraditi ih u oblaku (javnom ili privatnom). Da bi bilo koja aplikacija bila u stanju da obradi podatke, ti podaci ne smeju biti kriptovani. Do juna 2009. godine nije bio poznat nijedan metod za potpunu obradu kriptovanih podataka.

IBM (International Business Machines) je u junu 2009. godine objavio da je jedan od njihovih istraživača, u saradnji sa izvesnim studentom Univerziteta *Stanford*, razvio u potpunosti homomorfnu kriptografsku šemu koja dozvoljava obradu podataka bez potrebe za njihovim prethodnim dekriptovanjem [6]. Ovo predstavlja ogromni napredak u kriptografiji i imaće značajni pozitivni uticaj na *cloud computing* čim se počne sa primenom, a prema rečima *Ronalda Rivesta* (profesora *MIT*-a, *Massachusetts Institute of Technology* i ko-pronalazača čuvene *RSA*, tj. *Rivest, Shamir and Adleman* kriptografske šeme), primena nije daleko. Napori drugih istraživača su u toku i usmereni su na ograničenje količine podataka koji bi trebalo da budu dekriptovani da bi bila omogućena njihova obrada u oblaku, kao što je predikatno kriptovanje.[3]

Još jedan aspekt bezbednosti podataka predstavlja *data remanence*, a odnosi se na ostatke podataka koji su na neki način bili uklonjeni ili izbrisani. Ovi ostaci se mogu pojaviti kada nominalna operacija brisanja ostavi podatke netaknutim ili usled fizičkih karakteristika medija za skladištenje. Ostaci podataka mogu dovesti do nenamernog otkrivanja osetljivih informacija, ukoliko se taj medij za skladištenje podataka nađe u nekontrolisanoj sredini (ako je, na primer, bačen u smeće ili predat trećem licu).

Rizik da će doći do nenamerne izloženosti podataka neovlašćenom licu postoji bez obzira na model isporuke *cloud* servisa koji se koristi (Softver-kao-Servis, Platforma-kao-Servis, ili Infrastruktura-kao-Servis). U slučaju *SaaS* i *PaaS* modela isporuke *cloud* servisa, do otkrivanja podataka gotovo uvek dolazi nehotice, tj. nenamerno, što korisnicima ne pruža nikakvu utehu nakon što dođe do neovlašćenog pristupa njihovim podacima.

Uprkos povećanom značaju bezbednosti podataka, pažnja koju *cloud* servis provajderi obraćaju na ostatke podataka je zapanjujuće niska; mnogi od njih čak ni ne spominju ostatke podataka svojim korisnicima [3].

4.1 PODACI PROVAJDERA I NJIHOVA BEZBEDNOST

Pored bezbednosti sopstvenih podataka, korisnici bi takođe trebalo da obrate pažnju na podatke koje prikuplja *cloud* servis provajder, kao i na način na koji ih štiti. Korisnici bi trebalo da znaju koje podatke o njihovim podacima *(metadata* ili *data about data)* provajderi poseduju, na koji način su zaštićeni i kakav pristup tim podacima imaju oni kao korisnici.

Pored toga, provajder prikuplja i dužan je da štiti velike količine podataka vezanih za bezbednost. Na primer, na nivou mreže, provajder bi trebalo da prikuplja, nadgleda i štiti podatke u vezi zaštitnog zida i sistema za prevenciju upada *(IPS, Intrusion Prevention System)*; na nivou hosta bi trebalo da prikuplja sistemske log fajlove, a na nivou aplikacije podatke o autentičnosti i autorizaciji.

Informacije o podacima koje *cloud* servis provajder prikuplja i načinu na koji ih nadgleda i štiti, bitne su i za provajdere i za korisnike u slučaju da dođe do incidenta neovlašćenog pristupa, kao i za potrebe digitalne forenzičke istrage (za analizu incidenta) [3].

4.2 SKLADIŠTENJE-KAO-SERVIS

Skladištenje-kao-Servis se odnosi samo na podatke povezane sa aplikacijama *IaaS* modela, a ne na podatke u vezi aplikacija koje se u pokreću u oblaku u okviru *SaaS* i *PaaS* modela.

Zabrinutost za bezbednost podataka uskladištenih u oblaku je ista kao i za podatke uskladištene na bilo kom drugom mestu i odnosi se na poverljivost, integritet i dostupnost podataka.

Kada je reč o poverljivosti podataka uskladištenih u javnom oblaku, postoje dva potencijalna razloga za zabrinutost. Prvo, kakva kontrola pristupa u cilju zaštite podataka postoji? Kontrolu pristupa čine provera autentičnosti i autorizacija. *Cloud* servis provajderi obično koriste slabe mehanizme za proveru autentičnosti (npr. korisničko ime + lozinka) i autorizaciju.

Drugi potencijalni razlog za zabrinutost predstavlja pitanje: na koji način se podaci uskladišteni u oblaku zapravo štite? Za sve praktične svrhe, zaštita podataka smeštenih u oblaku podrazumeva upotrebu kriptovanja.

S tim u vezi, potrebno je imati uvid u to da li se korisnički podaci kriptuju prilikom smeštanja unutar oblaka. U slučaju da se kriptuju, bitno je znati koji algoritam se koristi i sa kakvom jačinom (tj. neprobojnošću) ključa; sve navedeno zavisi od *cloud* servis provajdera. Na primer, *MozyEnterprise* kriptuje korisničke podatke, dok ih *Amazon*-ov *web* servis *S3 (Simple Storage Service)* ne kriptuje. Korisnici imaju mogućnost da kriptuju svoje podatke pre nego što ih smeste u oblak, ali *S3* ne nudi opciju kriptovanja podataka.

U slučaju da *cloud* servis provajder kriptuje podatke svojih korisnika, sledeće što treba razmotriti je vrsta

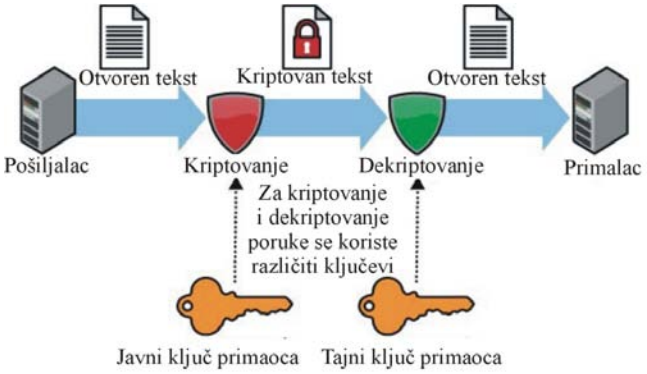
[3] Predikatno kriptovanje je oblik asimetričnog kriptovanja gde je omogućeno da različiti pojedinci (ili različite grupe pojedinaca) selektivno dekriptuju podatke, umesto da dekriptuju sve podatke. Videti: 'Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products', Jonathan Katz, Amit Sahai, and Brent Waters, http://eprint.iacr.org/2007/404.pdf.

kriptografskog algoritma koju koristi. Nisu svi kriptografski algoritmi isti; mnogi od njih ne pružaju adekvatni nivo zaštite. Trebalo bi koristiti samo algoritme koji su odobreni od strane regulatornih tela (kao što je *NIST - National Institute of Standards and Technology*), ili barem one koji su dobili neformalnu potvrdu od strane kriptografskih zajednica. Bilo kakve privatne algoritme bi trebalo izbegavati bez izuzetaka. Treba primetiti da je ovde reč o simetričnim kriptografskim algoritmima. Simetrično kriptovanje (ilustrovano na Slici 2) podrazumeva upotrebu jednog tajnog ključa i za kriptovanje i za dekriptovanje podataka. Samo simetrično kriptovanje ima dovoljnu brzinu i efikasnost za kriptovanje velike količine podataka. Korišćenje asimetričnog algoritma u tu svrhu bilo bi krajnje neuobičajeno.

Iako se primer ilustrovan na Slici 2 odnosi na *e-mail*, isti koncept (tj. jedan zajednički tajni ključ) se koristi za kriptovanje podataka koji se skladište.

Slika 2: Simetrično kriptovanje

Primer sa Slike 3 se odnosi na asimetrično kriptovanje; međutim, ovaj koncept (korišćenje javnog i tajnog ključa) se ne koristi prilikom kriptovanja podataka koji se skladište.



Slika 3: Asimetrično kriptovanje

Sledeće što treba razmotriti je dužina ključa. U slučaju simetričnog kriptovanja, što je ključ duži (tj. što je veći broj bita), kriptovanje je neprobojnije. Iako duži ključevi pružaju bolju zaštitu, mogu da dovedu do opterećenja računarskih procesora. Preporučena minimalna dužina ključa iznosi 112 bita za *Triple DES (Data Encryption Standard)* i 128 bita za *AES (Advanced Encryption Standard)* – oba algoritma su odobrena od strane *NIST*-a.[4]

Za razmatranje poverljivosti podataka i kriptovanja, u obzir bi trebalo uzeti i upravljanje ključem. Poveravanje upravljanja ključevima provajderu oblaka nije preporučljivo, barem ne istom provajderu koji rukovodi podacima korisnika.

Upravljanje ključevima je teško i složeno pojedinačnom korisniku, a *cloud* servis provajderima je još teže da na odgovarajući način upravljaju ključevima većeg broja korisnika. Iz tog razloga, postoje provajderi koji ne rade dobro svoj posao kada je u pitanju upravljanje ključevima. Na primer, uobičajena je praksa da provajder koristi jedan jedini ključ za kriptovanje svih podataka jednog korisnika; što je još gore, pojedini provajderi koriste samo jedan ključ za kriptovanje podataka svih svojih korisnika [3].

5. ZAKLJUČAK

Treba imati na umu da *cloud computing* ne predstavlja novu tehnologiju, već samo menja postojeće modele poslovanja. Posmatrano iz perspektive informacione bezbednosti, najveća promena koju donosi *cloud computing* je upotreba zajedničkih resursa, tj. opsluživanje većeg broja korisnika istovremeno. Ta promena za posledicu ima pomeranje granica poverenja; gde se tačno te granice nalaze još uvek nije jasno. Granice poverenja su različite za svaki od *SPI* modela (Softver-kao-Servis, Platforma-kao-Servis i Infrastruktura-kao-Servis); pa čak i u okviru svakog od tih modela granice se razlikuju u zavisnosti od *cloud* servis provajdera.

Nivo bezbednosti koji pruža *cloud* servis provajder zavisi i od perspektive iz koje se posmatra. Na primer, profesionalcima IT sektora jedne velike i razvijene kompanije nivo bezbednosti u *cloud computing*-u može biti neprihvatljiv u poređenju sa trenutnim položajem. S druge strane, nivo bezbednosti koji pruža *cloud computing* malom ili srednjem preduzeću može biti prihvatljiv, pa čak i veći u odnosu na trenutno stanje.

Za dalji razvoj *cloud computing*-a potreban je veći uvid u rad *cloud* servis provajdera, odnosno transparentnost u vezi načina na koji se brinu o bezbednosti. Ipak, to samo po sebi nije dovoljno za povećanje nivoa bezbednosti; potrebna su i značajna poboljšanja tehnologije bezbednosti u vidu proaktivne i reaktivne zaštite.

[4] NIST's 'Special Publication 800-57, Recommendation for Key Management-Part 1: General (Revised)', March 2007, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.

Današnje mogućnosti upravljanja ključevima (prilikom kriptovanja) nisu u stanju da ni u najmanjoj meri zadovolje potrebe preduzeća. Očekivanje da se potrebne tehnologije 'popnu do oblaka' i pruže jednostavno upravljanje složenim zahtevima je, jednostavno rečeno, pusta želja. Potrebne su radikalne promene u mogućnostima upravljanja ključevima da bi se zadovoljili zahtevi *cloud computing*-a. Neuspeh bi sasvim sigurno sputao njegov razvoj.

Cloud computing predstavlja novi model, još uvek uglavnom nepoznat i mali broj ljudi ga razume u dovoljnoj meri za donošenje odgovarajuće procene. Realna pitanja bezbednosti postoje bez ikakve sumnje. Ipak, bolje razumevanje, veća transparentnost i poboljšanje tehnologija dovešće do toga da brige oko bezbednosti u *cloud computing*-u izblede i postanu deo prošlosti.

LITERATURA

[36] Caceres J., Vaquero L., Polo A., 'Service Scalability over the Cloud', *Handbook of Cloud Computing*, Springer, USA, 2010.

[37] Jin H., Bell T., Wu S., 'Cloud Types and Services', *Handbook of Cloud Computing*, Springer, USA, 2010.

[38] Mather T., Kumaraswamy S., Latif S., *Cloud Security and Privacy*, First edition, O'Reilly, USA, 2009.

[39] Carlin S., Curran K., 'Cloud Computing Security', *14 International Journal of Ambient Computing and Intelligence*, UK, January-March 2011, pp. 14-19

[40] Catteddu D., 'Cloud Computing: Benefits, Risks and Recommendations for Information Security', *Communications in Computer and Information Science*, Vol. LXXII, Part 1, 2010.

[41] Prince B., 'IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering', *eweek.com*, 2009.

OCENA KVALITETA NIZOVA STATISTIČKIM TESTIRANJEM GENERATORA SLUČAJNIH I PSEUDOSLUČAJNIH BROJEVA

RATING THE QUALITY OF STATISTICAL TESTING OF GENERATOR SETS OF RANDOM AND PSEUDORANDOM NUMBERS

MILORAD S. MARKAGIĆ
Vojna akademija, Beograd, milmarkag@yahoo.com

MILICA M. MARKAGIĆ
Vojna akademija, Beograd, mima_hip@hotmail.com

Rezime: *U radu su razmotreni osnovni pojmovi slučajnih brojeva, generatora slučajnih i pseudoslučajnih brojeva, njihovo nastajanje i implementacija.*

Delimično su prikazane i metode ispitivanja karakteristika nizova slučajnih i pseudoslučajnih brojeva, kao i neki od metoda testiranja pouzdanosti i kvaliteta nizova.

U praksi se kvalitetu niza slučajnih brojeva poklanja pažnja u verifikovanim institucijama i kod edukovanih korisnika, dok se zbog manjeg poznavanja osnovnih teorijskih odredbi ili zbog namernog zaobilaženja procesa testiranja zbog velikog vremena i sredstava koje je potrebno uložiti, u velikom broju nizovi uvode u upotrebu bez predhodne validacije i verifikacije.

Ovo za posledicu ima i znatno snižen nivo bezbednosti aplikacije u kojoj su primenjeni.

Ključne reči*: slučajni brojevi, pseudoslučajni brojevi, generatori, kvalitet, testiranje*

Abstract: *This paper reviews the basic concepts of random number generators and pseudo random numbers, their formation and implementation.*

Partially shows test characteristics for random and pseudorandom sequences of numbers, and some methods for testing reliability and quality series.

In practice, the quality of series for random numbers is given attention in the verified institutions and by trained users, while the less basic theoretical know ledge of the law or the deliberate circumvention of the testing process because of the large time and resources needed to invest in a large number of sequence sare introduced into service without prior validation and verification.

This results in a significantly reduced level of security application in which they are applied.

Keywords: *random numbers, pseudorandom numbers, generators, quality, testing*

1. UVOD

U mnogim programima javlja se potreba za korišćenjem slučajnih brojeva. Različiti kriptološki algoritmi i kriptografski protokoli zahtevaju u izvesnim situacijama slučajni niz brojeva, kao što su: generisanje javnih ključeva, generisanje slučajnih bitova za postupak autentifikacije, izrada ključeva u digitalnom potpisu i pečatu i sl. Veoma često se slučajni brojevi primenjuju u računarskim simulacijama, gde se simulacijom stohastičkog sistema dolazi do rešenja problema koga je nemoguće rešiti analitičkim putem.

Slučajni brojevi mogu se između ostalog, a i najčešće se primenjuju u kriptografiji i računarskoj simulaciji. U oba modela postavlja se zahtev da slučajni brojevi koji se upotrebljavaju budu zaista slučajni brojevi.
Slučajni brojevi u praksi se mogu javiti samo u prirodnim pojavama i situacijama koje je nemoguće predvideti, kao što je bacanje novčića.

Međutim u praksi se koriste rešenja za koja se smatra da su su dobijeni brojevi manje ili više slučajni. Ako se uzme u obzir da sama pojava niza slučajnih brojeva predstavlja nepredvidivi, stohastički sistem, nemoguće je sa apsolutnom sigurnošću za neki niz brojeva reći da li je slučajan ili nije.

Formalno se može dokazati da je svaki niz brojeva slučajan kao i bilo koji drugi niz brojeva. U praksi se pri proučavanju slučajnosti nekog niza brojeva zapravo gleda skup odabranih testova koji proveravaju određene karakteristike ulaznog niza brojeva.

Ovim testovima se pokušava ustanoviti javljaju li se u ulaznom nizu nekakve zakonitosti koje se statistički ne bi smele javiti, pa se na osnovu procene i testiranja odlučuje da li se niz prihvata kao slučajan ili odbacuje. Niz se može smatrati slučajnim ako pokazuje neke karakteristike koje se očekuju od niza slučajnih brojeva.

Slučajni brojevi generišu se pomoću generatora slučajnih brojeva. Generatori brojeva mogu se podeliti na dva tipa: generatori slučajnih brojeva i generatori pseudoslučajnih brojeva.

2. GENERATORI SLUČAJNIH BROJEVA

Ovaj tip predstavljaju generatori koji generišu slučajne brojeve na principu prirodnih pojava, što znači da je izvor slučajnih brojeva nedeterministički i da je svaki slučajni broj u nizu nezavisan od predhodnog i da ne uslovljava javljanje narednog.

Ovi generatori su u potpunosti ili većim delom mehaničke prirode pa je njihova proizvodnja vrlo osetljiva i skupa, a praktična primena im je ograničena. Generisanje slučajnih brojeva je spor proces, a sam mehanički uređaj je podložan kvarovima i otkazima.

Zato se se ovi generatori najčešće koriste u simulacijskim metodama. Izvore slučajnih brojeva možemo svrstati u dve kategorije:mehanički i programski izvori.

2.1. Mehanički izvori:

Kod primene ovakvih izvora potrebno je dodatno programski obraditi dobijene podatke, jer je dobijeni niz često nebalansiran- pojava određenih brojeva može biti verovatnija, a moguća je i međusobna povezanost brojeva u nizu pojava jednog broja u nizu povećava verovatnoću da sledeći broj bude neki tačno određeni broj. U ovom slučaju generator predstavlja periferni uređaj i mora se povezati sa računarom.

Neki od načina generisanja slučajnih brojeva ovom metodom su:
- šum u poluvodičkoj diodi,
- vreme između emisija čestica u toku raspada radioaktivnog elementa,
- zvuk iz mikrofona ili video ulaz iz kamere i
- frekventna nestabilnost oscilatora.

2.2. Programski izvori:

Iako se pretpostavlja da ovaj skup izvora može dati nepredvidivi niz brojeva, to ne mora nužno biti slučaj. Na primer ponašanje sistemskog sata se lako može predvideti. Takođe, interakcija korisnika kod prvog i četvrtog izvora u praksi sledi određenu pravilnost koja se može preslikati na generisani niz brojeva.

Neki od predstavnika ovih izvora su:
- vreme između pritisaka na dirku tastature ili miša,
- specifične varijable operativnog sistema,
- sistemski sat i
- sadržaj memorije.

Kombinacijom više različitih izvora slučajnih brojeva moguće je dobiti dobar generator slučajnih brojeva, a samim tim i kvalitetniji slučajni niz.

3. GENERATORI PSEUDOSLUČAJNIH BROJEVA

Kod ovog tipa generatora primenjena je funkcija koja na osnovu početnih uslova slučajnog niza, daje izlazni niz pseudoslučajnih brojeva. Ulaz u generator mora biti slučajan i dobija se iz generatora slučajnih brojeva. Posle postavke početnih uslova, svaki broj u nizu je predvidiv, što dovodi do determinističke karakteristike generatora, pa se dobijeni brojevi nazivaju pseudoslučajnim.

Niz se može rekonstruisati uz znanje početnih uslova pa, ako je potrebno da se ista vrši, dovoljno je na nezavisnom mediju ili u sklopu generatora sačuvati samo početne uslove. U nekim ispitivanjima, pseudoslučajni brojevi pokazali su se uspešnijim od slučajnih brojeva dobijenih iz fizičkih izvora. Izborom generatora i kvalitetnih početnih uslova, determinističke metode koje se upotrebljavaju moguće je prikriti tako da izlazni niz u mnogim karakteristikama liči na niz slučajnih brojeva.

Generatori pseudoslučajnih brojeva su brži, lakši za manipulaciju i prenosni su. Posebnu pažnju treba posvetiti izboru generatora, bilo da se generator upotrebljava u simulacijske svrhe ili u kriptografskom uređaju i sistemu.
Očekivana svojstava koja treba da ispuni generisani niz su:

- Brojevi u nizu trebaju da budu ravnomerno raspoređeni u prostoru. Verovatnoća pojave jednog broja treba biti jednaka za sve brojeve u prostoru u kome se generšu brojevi. Ovo mora da važi i za ceo generisani niz i za bilo koji podniz generisanog niza.
- Među podnizovima generisanih brojeva ne sme biti korelacije - nijedan podniz u nizu ne sme da zavisi od nekog drugog podniza.
- Perioda generatora mora biti što veća. Generisanje pseudoslučajnih brojeva se vrši determinističkim putem, pri čemu generator prolazi kroz niz stanja. Iako je taj broj stanja ogroman, treba imati u vidu da je ipak reč o konačnom broju stanja. Kao posledica ovoga javlja se da će se generator u jednom trenutku naći u stanju u kome se već nalazio, pa će doći do cikličkog ponavljanja nekog već generisanog podniza. Period generatora je broj brojeva u nizu koji se ciklički ponavlja.

Takođe se kao zahtevi postavljaju i mogućnost reprodukovanja niza, prenosivost i velika brzina rada uz minimalne memorijske zahteve.

Mogućnost reprodukovanja niza je važna zbog detekcije i ispravljanja grešaka uzrokovanih od strane generatora jer loš generator slučajnih brojeva može prouzrokovati neispravan rad čitavog programa. Pred prenosni generator se postavlja zahtev da pokazuje ista svojstva u različitim uslovima rada- različiti uređaji, različiti operativni sistemi i programski jezici.

Bitno je da uz iste početne uslove generator uvek generiše isti niz brojeva. Brzina je zahtev koji je veoma važan u simulacijskim primenama gde se generše veliki broj slučajnih brojeva. Neophodno je da pri generaciji velikog broja nizova generator mora biti veoma brz. Takođe je važno napomenuti da brzina predstavlja sekundarni zahtev a da je prioritet kvalitet generisanog niza.

Osnovna svrha generatora brojeva je generisanje niza brojeva koji pokazuju određene slučajne karakteristike, pa pri optimizaciji generatora treba voditi računa da se kvalitet generisanog niza ne smanji.

4. ISPITIVANJE GENERATORA SLUČAJNIH I PSEUDOSLUČAJNIH BROJEVA

Kada se upotrebljava izraz ispitivanje generatora prvenstveno se misli na ispitivanje kvaliteta generisanog niza. Prilikom ispitivanja ustanovljava se da li generisani niz pokazuje neke poželjne karakteristike kao što je nedostatak pravilnosti u nizu, ispravna distribucija brojeva i sl.

Cilj svakog ispitivanja je da se iz beskonačnog skupa karakteristika niza izvuku bitni testovi.

U praksi postoji veliki broj različitih testova, ali ni jedan od njih ne može proglasiti niz generisanih brojeva apsolutno slučajnim. Moguće je samo doći do zaključka da li niz poseduje neka svojstva, koja bi pokazao niz generisan od strane idealnog generatora. Na osnovu rezultata se može sigurno zaključiti da neki niz nije slučajan odnosno da generator ne radi ispravno.

Osnovu za ispitivanje predstavlja statistički test. Pre ispitivanja, postavlja se nulta hipoteza (H_0) i alternativna tvrdnja (H_a). Pri ispitivanju generatora slučajnih brojevahipoteze imaju oblike:

- H_o: niz koji se ispituje predstavlja niz slučajnih brojeva
- H_a: niz koji se ispituje ne predstavlja niz slučajnih brojeva

Za svako ispitivanje potrebno je odrediti statističku vrednost koja se ispituje tj. vrednost pomoću koje se odlučuje koja će od tvrdnji biti prihvaćena kao istinita - uvek se prihvata samo jedna od navedenih hipoteza.

Nakon toga, potrebno je teoretski, matematičkim postupcima, odrediti očekivani rezultat nulte hipoteze u uslovima normalne, referentne raspodele. Nakon toga se određuje kritična vrednost za koju se ne očekuje da će se premašiti u uslovima normalne raspodele. Na kraju se na temelju generisanog niza računa tražena statistička vrednost. Ako merena vrednost prelazi teoretski određen prag, može se sa određenom sigurnošću reći da generisani niz nije niz slučajnih brojeva- prihvata se H_a. Važi i suprotna relacija- ako merena vrednost ne prelazi određeni prag, moguće je sa određenom sigurnošću prihvatiti H_0.

U testiranjima se upotrebljavaju dve standardne raspodele: normalna raspodela - očekivana raspodela merenih vrednosti u nekom prostoru i X^2 raspodela - očekivana raspodela učestanosti pojave nekih događaja.

Izbor raspodele zavisi od karakteristike koja se ispituje, a dodatno je u posebnim ispitivanja moguće uzeti i neku drugu raspodelu. Proces ispitivanja zahteva

generisanje velikog niza brojeva raspona od 10^3 do 10^6 brojeva u nizu.

Svako ispitivanje meri neku od poželjnih karakteristika slučajnih brojeva. Nakon serije ispitivanja u najboljem slučaju moguće je zaključiti da ispitivani generator poseduje željena svojstva te da bi mogao biti dobar generator slučajnih brojeva ili je moguće zaključiti da ispitivani generator nije odgovarajući.

5.NEKI TESTOVI ZA ISPITIVANJE GENERATORA:

5.1.Ispitivanje učestanosti u nizu

U ovom testu meri se odnos jedinica i nula u nizu bitova. Cilj je da se utvrdi da li je u toku testiranja broj jedinica i nula približno jednak. Očekivanja su da kvalitetni generator slučajnih bitova daje približno jednak broj jedinica i nula.

Ostala testiranja zavise od uspešnosti ovog testa. Ovo jeste nužan, ali ne i dovoljan uslov za donošenje zaključka da li se radi o nizu slučajnih bitova ili ne.

5.2.Ispitivanje učestanosti u bloku

U ovom testu ispituje se odnos jedinica i nula u M-bitnim blokovima u nizu. Cilj je da se uoči da li je broj jedinica i nula isti u svakom M-bitnom bloku. Za blok dužine M=1 ovaj test se pretvara u test učestanosti u nizu.

5.3.Ispitivanje ponavljanja istih bitova u nizu

Ovim testom se utvrđuje da li je ukupan broj uzastopnih ponavljanja jednog broja u nizu jednak na svakom delu niza. Uzastopno ponavljanje predstavlja pojavu dva ili više ista broja za redom.
Potrebno je uočiti da li se broj uzastopnih ponavljanja poklapa sa očekivanim brojem koji bi bio u savršenom slučajnom nizu

5.4.Ispitivanje najdužeg uzastopnog ponavljanja jedinica u bloku

Ovde se meri da li i kakvo je najduže uzastopno ponavljanje jedinica u M-bitnim blokovima. Svrha je da se odredi da li se dužina najdužeg uzastopnog ponavljanja poklapa sa dužinom koja bi se očekivala u nizu slučajnih bitova. Nepravilnost u dužini najdužeg uzastopnog ponavljanja jedinica u bloku povlači za sobom i nepravilnost u dužini najdužeg uzastopnog ponavljanja nula u bloku, pa nije potrebno obaviti posebno ispitivanje za ponavljanje nula u M-bitnim blokovima.

5.5.Testiranje ranga matrice

Osnovna karakteristika koja se meri ovim testom je rang matrica koje se dobiju iz podniza ispitivanog niza. Ovim testom se ustanovljava da li postoji linearna međuzavisnost između podnizova fiksne dužine u ispitivanom nizu.

5.6.Spektralno ispitivanje

U ovom testu mere se amplitude u diskretnoj Fourierovoj transformaciji posmatranog niza. Svrha testa je otkrivanje periodičnih pojava u testiranom nizu koje bi ukazale na odstupanja od niza slučajnih bitova.

5.7.Ispitivanje slučajnog hoda

Slučajni hod na temelju kumulativne sume dobije se nakon što se sve nule u nizu zamene sa –1. Prolaskom kroz bitove posmatranog niza računa se suma. Trenutna vrednost u nekom koraku označava stanje.

Ciklus u slučajnom hodu sastoji se od niza koraka koji počinju i završavaju na istom mestu. Cilj testa je da se odredi da li broj svakog stanja u jednom ciklusu značajno odstupa od očekivanog broja za niz slučajnih bitova.

Pored navedenih poznati su još i testovi: Ispitivanje ponavljanja predloška u generisanom nizu, Maurerov univerzalni statistički test, Ispitivanje na temelju Lempel-Ziv kompresije, Ispitivanje linearne složenosti, Ispitivanje preklapajućih uzoraka, Ispitivanje približne entropije, Ispitivanje kumulativne sume itd.

ZAKLJUČAK:

U eri vrtoglavih masovnih komunikacijskih i informatičkih promena, potreba za pre svega zaštitom podataka o ličnosti, organizaciji, kompaniji i zaštitom poslovnih tokova, nameće potrebu iznalaženja novih modela i algoritama za realizaciju ovih procesa.

U tom, mahom nevidljivom svetu, brojevi, kao osnova statistike imaju ogroman značaj, kako u generisanju nizova, tako i u praktičnim implementacijama u određenom sklopu ili aplikaciji.

Težnja naučnika i proizvođača softvera da korisnicima usluga pruže što elegantnije korišćenje sredstava masovne komunikacije, uz istovremenu zaštitu podataka, bazirane su na kvalitetnim algoritmima i kvalitetnim ključevima, pre svega u oblasti kriptografije, a čija bi proizvodnja bila znatno usporena ili onemogućena, bez primene modela računarske simulacije.

Slučajni i psudoslučajni nizovi, slični po svojim karakteristikama, a istovremeno različiti u segmentu produkcije i primene imaju značajno mesto i ulogu, ali bi njihova primena bez predhodne validacije, nekim od testova, bila obezvređena, pa bi se kao što je često slučaj u praksi koristili dosta nesigurni nizovi, što za

posledicu ima umanjenje ili izostanak bezbednosti podataka.

Pseudoslučajni brojevi imaju primenu pri generisanju sesijskih ključeva, inicijalinih vektora, parametara digitalnog potpisa kao i veliku primenu u bezbednosnim protokolima. Kriptografske aplikacije je nemoguće zamisliti bez upotrebe generatora pseudoslučajnih brojeva.

LITERATURA:

[42] Menezes, P. van Oorschot, S. Vanstone. ``Handbook of applied cryptography.`` CRC Press, 1996.

[43] ``A statistical test suite for random and pseudorandom number generators for cryptographic application``. National Institute of Standards and Technologies, 2000.

[44] Markagić M. Interni radovi i istraživanja, Beograd 2000-2012.

[45] Internet stranica.http://random.mat.sbg.ac.at

[46] B. Schneier. ``Applied Cryptrography``. John Wiley & Sons, Inc, 1996.

POLITIKA BEZBEDNOSTI I PREPORUKE ZA POVEĆANJE BEZBEDNOSTI BAZA PODATAKA U PRAVOSUDNOM INFORMACIONOM SISTEMU

SECURITY POLICY AND RECOMMENDATIONS FOR INCREASING SECURITY DATABASE IN THE JUSTICE INFORMATION SYSTEM

RADE DRAGOVIĆ
Ministarstvo pravde, Beograd, dragovic@mpravde.gov.rs

BOJAN PEROVIĆ
Ministarstvo pravde, Beograd, bojanp@mpravde.gov.rs

Rezime: *Pravosudni informacioni sistem sa specifičnostima kao sistem koji opslužuje posebnu granu vlasti, svojom strukturom obuhvata veoma složene poslovne procese, poslovne funkcie, događaje, analize kao i druge specifičnosti po pitanju zahtevanog nivoa bezbednosti podataka koji egzistiraju u sistemu. Potreba za formiranjem bezbedonosno pouzdanog sistema koji će voditi računa o ponašanju u sistemu koja mogu da ukažu na ozbiljne probleme usmerene ka ugrožavanju bezbednosti a koja proističu iz upotrebe takvih podataka mora biti bazirana na pravnoj regulativi države i standardima bezbednosti. Ovakav specifičan sistem je veliki izazov za poslove zaštite od nedozvoljenih radnji i zloupotreba. U ovom radu prikazane su iskustvene smernice za povećanje stepena bezbednosti Pravosudnog informacionog sistema u vidu preporuka u domenu baza podataka i to posebno u delu podataka koji se klasifikuju kao poverljivi podaci.*

Ključne reči: *Informaciona bezbednost, baza podataka, standard SRPS ISO 27001, preporuke, pravosuđe.*

Abstract: *Judicial Information System is a specific system that serves the special branch of government, its structure includes the highly complex business processes, business functions, events, analysis and other specifics regarding the required level of data security that exist in the system. The need for the establishment of security in a reliable system that will take into account the behavior of the system, which may indicate serious problems aimed at endangering the security arising from the use of such data must be based on the national legal regulations and safety standards. This specific system is a major challenge for protection from abuse and illicit activities. In this paper, the empirical guidelines for increasing the level of security of judicial information system in the form of recommendations in the area of databases particularly in the area of data classified as confidential information.*

Keywords: *Information security, database, standard SRPS ISO 27001, recomendation, judiciary.*

1. UVOD

Obezbeđenje zaštite podataka jedno je od najznačajnijih i najdelikatnijih pitanja sa kojima se susreću sva demokratska društva i informacioni sistemi u njima. Pravosudni informacioni sistemi posebno su značajni, jer je potreba za razmenom podataka unutar pravosuđa ogromna, kao i mogućnost njihove zloupotrebe. Da bi se onemogućila zloupotreba i obezbedila zaštita podataka preduzimaju se određene pravne, tehničke, organizacione i druge posebne mere kao preventivne aktivnosti.

Zaštita podataka predstavlja skup metoda i tehnika kojima se ograničava pristup podacima od strane programa koji se izvršavaju, ili u jednom širem smislu zaštita podrazumeva skup metoda, tehnika i pravnih normi kojima se ograničava pristup podacima od strane programa i ljudi. Putem zaštite štiti se fizički i logički integritet celokupnog informacionig sistema, bilo da je distribuiran ili ne, odnosno centralizovan ili decentralizovan. Decentralizovani informacioni sistemi su posebno složeni za sprovođenje poslova bezbednosti i kao takvo arhitektonsko rešenje nose veće rizike u domenu zaštite podataka.

Zaštita podataka obuhvata skup međusobno povezanih aktivnosti, metoda, tehnika i normi kojima se obezbeđuje privatnost, sigurnost, poverljivost, raspoloživost i integritet podataka od svih opasnosti koje im prete. Aktivnosti, metode, tehnike i norme moraju biti definisane usvojenim standardima i *ICT Security Policy* dokumentima koje će IKT eksperti primenjivati i striktno ih se pridržavati u svakodnevnom radu sa korisnicima sistema.

Primetna je pasivnost države u razvoju normativnog okvira za informacionu bezbednost i primenu postojećih propisa.

2. STANDARDI

SRPS ISO/IEC 27001 (Informacione tehnologije - Tehnike bezbednosti - Sistemi menadžmenta bezbednošću informacija - Zahtevi) je nacionalni standard koji je nastao kao rezultat potrebe definisanja međunarodno prihvaćenih normi, koji će svojim zahtevima definisati okvir formiranja sveobuhvatnog sistema zaštite i ciljeve njegovog delovanja kako bi se na efektivan i efikasan način upravljalo bezbednošću informacija. Ovaj standard je identičan standardu ISO/IEC 27001 i specifikuje zahteve za uspostavljanje, implementaciju, primenu, praćenje, preispitivanje, održavanje i poboljšavanje dokumentovanog ISMS unutar konteksta ukupnih poslovnih rizika u organizaciji; specifikuje zahteve za implementaciju bezbednosnog upravljanja prilagođenog potrebama pojedinih organizacija ili njihovih delova. Standard ISO 27001 je koncipiran u pet poglavlja i to: Sistem za upravljanje bezbednošću informacija (ISMS), Odgovornost rukovodstva, Interna provera ISMS, Preispitivanje ISMS od strane rukovodstva i Unapređenje ISMS. ISO 27001 je multidisciplinaran, jer tretira bezbednosti informacija sa tri aspekta:

• Informacionog – analizirajući i definišući performanse IT opreme, prava pristupa, kriptovanja, lozinke, protokole, politike sa aspekta pojave rizika po bezbednost podataka i informacija

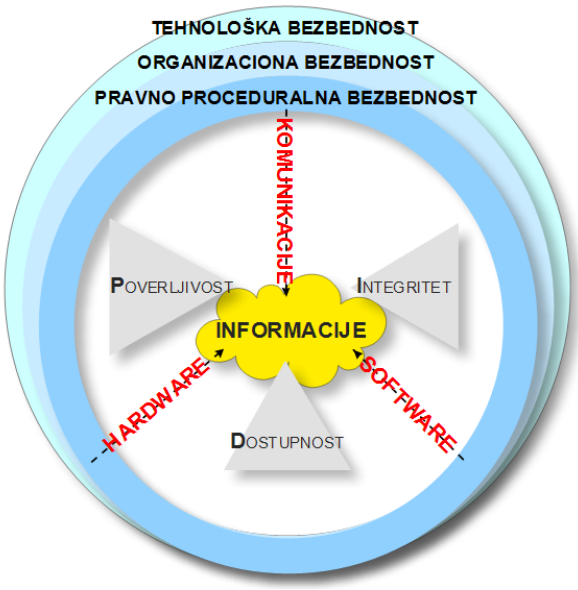
• Administrativnog – definišući jasna uputstva, politike i procedure za generisanje informacija, njihovu distribuciju, čuvanje (skladištenje)

• Fizičkog – fizička kontrola pristupa, evidencija zaposlenih, video nadzor, zaštita radnih prostorija.

Prednosti koje implementacija i sertifikacija ISO 27001 nosi sa sobom, mogu se sažeti u dva segmenta. Prvi segment je zaštita i bezbednost informacija kroz sistematski i proaktivan pristup za identifikovanje i delovanje protiv čitavog niza potencijalnih rizika kojima su izložene informacije organizacije. Upravljajući rizikom po bezbednost informacija, umanjuje se verovatnoća pojave nepredviđenih situacija.

Komponente Bezbednosti informacija: Poverljivost (Confidentiality), Integritet (Integrity) i Dostupnost (Availability) - PID (CIA). Informacioni sistemi u tom smislu grupišu se u tri celine: hardver, softver i komunikacije sa ciljem da se identifikuju i primene standardi bezbednosti informacija, kao i mehanizmi zaštite i prevencije na tri nivoa ili sloja: pravno proceduralni, organizacioni I tehnološki (Slika 1.). U suštini, procedure ili pravila se sprovode da kažu službenicima (administratoru, korisniku i operateru) kako da koriste IKT kako bi se osigurala bezbednost informacija u okviru Pravosudnog informacionog sistema.

Standard SRPS ISO 27001 je stupanjem na snagu Uredbe o posebnim merama zaštite tajnih podataka u informaciono - telekomunikacionim sistemima („Službeni glasnik RS“, broj 53/2011 od 20. jula 2011. godine) od preporuke postao pravno proceduralni okvir i neizostavni činilac svih informacionih sistema države Srbije. Članom 10 ove uredbe prepoznat je nacionalni standard SRPS ISO/IEC 27001 u skladu sa kojim će se sprovoditi zaštita tajnih podataka u informaciono - telekomunikacionim sistemima.



Slika 1. Komponente bezbednosti informacija

Dobiti od implementacije Sistema menadžmenta bezbednosti informacija (ISMS), saglasno zahtevima ISO 27001:2005, u Pravosudni informacioni sistem mogu biti sledeći:

•"Just in time" efekat – Prava informacija na pravo mesto u pravo vreme,
•Zaštita i očuvanje know-how,
•Povećanje efektivnosti i efikasnosti sistema,
•Povećanje poslovnog kredibiliteta i poverenja od strane klijenata i partnera,
•Ušteda vremena racionalizacijom količine i sadržine informacija,
•Optimizacija resursa potrebnih za distribuciju i čuvanje podataka,
•Rana identifikacija ranjivosti, pretnji i potencijalnih negativnih uticaja na poslovanje,
•Smanjenje rizika od zapošljavanja ljudi koji bi mogli naškoditi sistemu,
•Postizanje sinergetskog efekta timskog rada,
•Promptna usklađenost sa zakonskom regulativom,
•Brži protok informacija između zaposlenih,
•Stvaranje preduslova za određivanje odgovornosti,
•Smanjenje nesporazuma kod zaposlenih usled "ukrštanja informacija",

Značajne su koristi koje model za uređenje sistema za bezbednost informacija ISO 27001 ostvaruje organizacijama koje se odluče da ga implementiraju, pre svega u smislu poboljšavanja svojih organizacionih performansi. Izvesno je da ovaj model predstavlja najbolju praksu u oblasti zaštite i bezbednosti informacija koja je pretočena u zahteve standarda.

3. PRAVOSUDNI INFORMACIONI SISTEM

Pravosudni informacioni sistem u Republici Srbiji razvija se sa svim specifičnostima, karakterističnim za sudstvo kao posebnu granu vlasti, državno tužilaštvo, Ministarstvo pravde sa zatvorskim sistemom koji svojom strukturom obuhvataju veoma složene poslovne procese, poslovne funkcije, događaje, analize i probleme kao i druge specifičnosti po pitanju toka podataka koji egzistiraju u sistemu [2]. Pravosudni informacioni sistemi posebno su značajni, jer je potreba za razmenom podataka unutar pravosuđa ogromna, kao i mogućnost njihove zloupotrebe. Uspostavljanje efikasnog produkcionog okruženja sa rad pravosudnih organa nosi sa sobom rizike u domenu mogućeg lakog pristupa struktuiranim podacima neovlašćenih lica. Ovaj scenario se svakako mora izbeći. Svest o informacionoj bezbednosti u Pravosudnom informacionom sistemu je nedovoljno razvijena jer su donosioci odluka lica sa osnovnim znanjem iz oblasti IKT, sa nepoznavanjem i potcenjivanjem potencijalnih opasnosti. Postoji odsustvo šire stručne analize i kritike stanja bezbednosti, malo javnih e-servisa. Primetna je pasivnost države u razvoju i uvođenju normativnog okvira za informacionu bezbednost i primenu postojeće pozitivne pravne regulative. Zbog svega navedenog kao jedna od funkcionalnih preporuka za uspostavljanje pravosudnog informacionog sistema prepoznata je bezbednost podataka [1]. Tehničke mere moraju da obezbede funkcionalnost Pravosudnog informacionog sistema uz potpuno uvažavanje pozitivnih propisa u ovoj oblasti, ali i sagledavanja tog sistema u realnom tehničko tehnološkom okruženju. Sve tehničke mere moraju se definisati u tehničkoj dokumentaciji. Tehničke mere podrazumevaju direktne mere za tehničke sisteme i podsisteme, ali i indirektne infrastrukturne sisteme podrške radu na kojima se bazira potpuno funkcionisanje Pravosudnog informacionog sistema.

Organizacione mere definišu nakritičniji deo zaštite informacionih sistema – IKT osoblje unutar sistema. To podrazumeva osnivanje takve organizacije koja će se baviti razvojnim, stručnim i regulatornim poslovima od interesa za pravosuđe i građane, a pogotovo što ovi poslovi ne zahtevaju stalan i neposredan politički nadzor i što takva organizacija može bolje i delotvornije da ih vrši nego organ državne uprave ili pravosudni organ. Značajno je i to da se u celini ili pretežno Pravosudni informacioni sistem, zajedno sa svim javnim registrima u njemu (sudski tumači, veštaci, izvršitelji, medijatori, beležnici), može delimično finansirati od cene koju plaćaju korisnici usluga, odnosno građani, preduzeća, advokati, investitori i dr. Ovakvom organizacijom obezbedili bi se stručni i motivisani službenici, adekvatno informatički obrazovani, a ne priučeni ili „obučeni", i ujedno disciplinovani da sprovode poslove zaštite podataka. Izazvano nedavnim događajima, u praksi poznato već duže vreme, nameće se neophodnost uspostavljanja radnog mesta IT administratora za bezbednost podataka (Data Security Administrator) koji ne bi bili podređeni rukovodiocu pravosudnog organa u kome rade, već direktno rukovodiocu bezbednosti Pravosudnog informacionog sistema (Chief Security

Officer) kako bi svoj posao obavljali nesmetano u skladu sa pravilima struke.

Zaštita podataka predstavlja skup metoda i tehnika kojima se ograničava pristup podacima od strane programa koji se izvršavaju, ili u jednom širem smislu zaštita podrazumeva skup metoda, tehnika i pravnih normi kojima se ograničava pristup podacima od strane programa i ljudi. Putem zaštite štiti se fizički integritet celokupnog informacionig sistema, bilo da je distribuiran ili ne, odnosno centralizovan ili decentralizovan.

U informacionom društvu se kao neželjeni efekat pojavljuje ugrožavanje informacione bezbednosti. Informaciona bezbednost je proces stalnog održavanja sigurnosti korisnika i informacionih sistema. Strateško opredeljenje srpskog pravosuđa svakako mora biti bezbednost Pravosudnog informacionog sistema. Glavni zadaci strategije moraju biti:

- Prevencija – preventivno delovanje je najefikasnije, ali je i najskuplje, jer zahtava stalno praćenje trendova u pojedinačnim domenima zaštite. Ovakav model zahteva veću kadrovsku jednicu.
- Detekcija – kada dođe do detektovnja problema bolje je da ta detekcija bude rana detekcija, jer olakšava odbranu od napada, sa delovanjima u cilju što manjeg nanošenja štete.
- Ograničavanje štete – minimizovati i ograničiti štetu kada se neispravnost pojavi. Potrebno je razviti metode za
kontrolu štete u pojednim segmentima IKT sistema..
- Oporavak – IKT sistem projektovati na način da se, iz stanja u otkazu, oštećeni informacioni sistem vrati u potpuno funkcionalno stanje u što je moguće kraćem roku.
- Korekcije stalno unapređenje uočenih (interno ili eksterno) uzroka koji dovode ili potencijalno mogu dovesti do oštećenja sistema
- Opreznost i disciplina - svi članovi organizacije moraju da budu upoznati sa opasnostima i moraju da se pridržavaju sigurnosnih pravila i regulativa – ICT Security Policy.
- Uspostavljanje funkcionalnog nadzora – svaka odbrambena strategija mora da ima dvostepeni nadzor nad primenom IKT standarda i propisa. Ove poslove treba da obavljaju najiskusnija i najstručnija lica.

4. POLITIKA INFORMACIONE BEZBEDNOSTI U PRAVOSUĐU

Politika informacione bezbednosti su posebna vrsta dokumentovanih poslovnih pravila za zaštitu podataka i sistema koji skladište i obrađuju informacije. U odeljku 5 ISO/IEC 27002:2005 *Information technology - Security techniques - Code of Practice for Information Security Management* definisana je Politika informacione bezbednosti (*ICT Security Policy*). Menadžment treba da definiše sveobuhvatan paket detaljnije korporativne politike bezbednosti informacija, u vidu informacija za korisnike bezbednosne politike. Politika informacione bezbednosti je opisana [4] kroz 39 kontrola ciljeva standarda ISO/IEC 27002 koji su napravili odličan sveobuhvatan ali i sažet skup aksioma politike. Sadržaj je prilagođen da odražava ono što rukovodstvo zapravo želi da postigne u odnosu na poslovne organizacije ciljeva bezbednosti. Dva su pristupa definisanju Politike informacione bezbednosti:

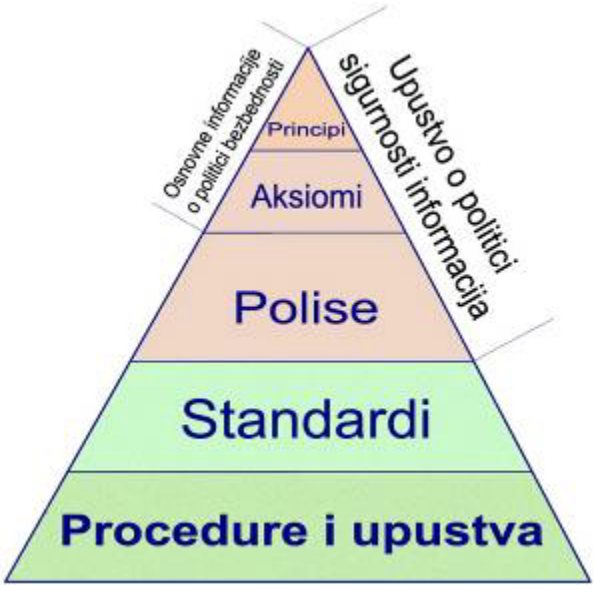
1. Pojedinačne politike pokrivaju specifična pitanja bezbednosti kao što su "politika Email sigurnosti" i "politika lozinki". One definišu odgovornost i sigurnost ključnih grupa, funkcija i timovi ljudi. Trebalo bi da te politike budu referentne na višim i nižim nivoima hijerarhije politike.
2. Sveobuhvatna politika za korisnike koja sadrži jezgrovite politike izjava za odražavanje cele ISO/IEC 27002, sa brojnim ugrađenim unakrsnim referencama između povezanih politika izjava i pozivanje na veze aksioma, standarda, procedura i smernica. Za potrebe Pravosudnog informacionog sistema važno je izraditi i pojedinačne i sveobuhvatne politike, zbog složenosti organizacije i lakšeg upravljanja informacionom bezbednošću.

Politike informacione bezbednosti, principi i detaljne politike, treba da budu formalno pregledane i usvojene od strane višeg rukovodstva koje treba da prihvati čitav program IKT bezbednosti jer će dovesti do promene dotadašnje prakse u celoj organizaciji. Najviše rukovodstvo mora biti svesno opštih ciljeva i podržati promene.

Politika bezbednosti podataka, standarda, procedura i smernica nikada se neće zaista "završiti" već je potrebno da se ažuriraju s vremena na vreme i da prate promene unutar i izvan organizacije (npr. pojava novih pretnji bezbednosti informacija može biti povod za izmenu postojećih politika i sl. ili bar generaciju dodatnih materijala bezbednosne svesti o promeni pretnji).

Međusobni odnos procedura, standarda, polisa, aksioma i principa bezbednosti ISO/IEC 27002 kao i sadržaja Uputstva o informacionoj bezbednosnoj politici I korporativne informacione bezbednosne politike dat je na Piramidi bezbednosti, slika 2. Potpun pristup bezbednosti mora sadržati principe, aksiome, polise, standarde i procedure i uputstva kojima se potpuno definiše bezbednost.

Standard ISO 27001 svakako nije jedini okvir koji treba primenjivati u zaštiti podataka već treba primeniti zakone, podzakonska i druga akta države.



Slika 2. Piramida bezbednosti

Standardom je trenutno definisano 39 kontrolnih ciljeva standarda ISO/IEC 27002 – aksioma koji opisuju Politiku informacione bezbednosti kao što sledi:
- *Information Security Overview*
- *Acceptable Use Policy*
- *Analog Line Policy*
- *Backup Procedures Policy*
- *Business Continuity Plan (BCP) Policy*
- *Computer Lifecycle Program (CLP) Policy*
- *Data Breach Policy*
- *Data Classification Policy*
- *Data Collection Policy*
- *Data Lifecycle Policy*
- *Data Storage Policy*
- *Database Credentials Policy*
- *Digital Signature Policy*
- *Disaster Recovery Plan (DRP) Policy*
- *Electronic Mail (e-mail) Retention Policy*
- *Encryption Policy*
- *Firewall Security Policy*
- *Identity Theft Prevention Policy*
- *Incident Response Policy*
- *Information Asset Issue Policy*
- *Information Assurance (IA) Policy*
- *Information Security Management System (ISMS) Policy*
- *Intranet Policy*
- *Malicious Software (Malware) Policy*
- *Non-Regulatory Compliance Policy*
- *Operating System Policy*
- *Operational/Technical/Management Security Policy*
- *Password Policy*
- *Personal Communication Device (PCD) Policy*
- *Personal Use Policy*
- *Privacy & Monitoring Policy*
- *Regulatory Compliance Policy*
- *Remote Access Policy*
- *Risk Assessment Policy*
- *Router Security Policy*
- *Service Provider Policy*
- *User Security Training Policy*
- *Vulnerability Assessment Policy*
- *Wireless Communications Policy*

Navedene politike su svakako smernice za definisanje svih pitanja vezanih za bezbednost Pravosudnog informacionog sistema. Ukoliko postoje još neke specifičnosti koje ne spadaju u navedenih 39 aksioma bezbednosti preporučuje se da se dodaju kao posebne politike bezbednosti u dodatku. Pored aksioma bezbednosti, Politika informacione bezbednosti mora sadržati i sledeće priloge:
- Termini i definicije
- Obrasci i uputstva o priznanju politike sigurnosti
- Popis korisničke opreme – prijem, izdavanje
- Formulari sporazuma o čuvanju poverljivih informacija za outsorsing poslove
- Formulari za reagovanje u incidentnim situacijama
- Nalozi za imenovanje glavnih/og službenika za bezbednost informacija
- Usklađenost sa zakonima
- Uputstva međunarodne organizacije za standarde
- Politika sigurnosti informacija, priručnik, dokumentacija

Navedeni prilozi predstavljaju onaj deo koji je namenjen korisnicima u sistemu i treba svojim sadržajem da otkloni sve nedoumice u radu korisnika. Ovi dokumenti tako i trebaju da budu koncipirani, kako bi korisnik u nekoj od kriznih situacija po IKT sistem, mogao da reaguje na najbolji način. Korisniku treba objasniti da iza njegove uloge u procesu stoji ceo IKT sistem koji zahteva reagovanje po određenim procedurama i pravilima. Nakon upoznavanja sa svim sadržajima koji su od interesa za određenog korisnika, u prilozima se nalaze i obrasci o odgovornosti korisnika, koje svaki korisnik u okviru organizacije mora da potpiše.

5. PREPORUKE ZA MONITORING BAZA PODATAKA

Da bi se sagledala celinu informacionog sistema i aplikativnih sistema u njima putem kojih se smeštaju podaci u bazu podataka, treba poći od bezbednosnih rešenja, koja se u najopštijem smislu mogu posmatrati sa tri aspekta [3]:
A1) Provera pristupa aplikativnom sistemu (autentifikacija korisnika),
A2) Obezbeđenje potpune funkcionalnosti aplikativnog sistema kroz proveru akcija i privilegija izvršavanja od strane korisnika u radu sa izabranom funkcionalnošću (autorizacija korisnika),
A3) Obezbeđenje integriteta podataka kroz proveru privilegija nad podacima.

U tom smislu potrebno je da se, pri projektovanju aplikativnog sistema, posebno razmatra i projektuje funkcija sigurnosti uzimajući u obzir gore navedene aspekte. Kada se kaže projektovanje funkcije sigurnosti misli se na klasičnu funkcionalnu analizu kao i definisanje modela podataka sigurnosnog modula u odnosu na sve navedene aspekte sa početka teksta.

Provera ulaska u aplikativni sistem podrazumeva funkciju kontrole ulaska korisnika u aplikaciju (autentifikacija korisnika). Jasno je da je u modelu podataka za ovaj aspekt potrebno prvo definisati sve korisnike (u tabelama za USER-e) kojima će se dodeliti pravo ulaska u aplikativni sistem. Provera akcija i privilegija izvršavanja, kao deo sigurnosnog modula, omogućava da se na osnovu projektovanih uloga u aplikativnom rešenju (datih u tabelama koje opisuju uloge) i vezama sa konkretnim aplikativnim modulima verifikuju privilegije korisnika nad određenom funkcionalnošću. Iz ovoga sledi da se uloge mogu dodeliti samo već definisanim korisnicima, odnosno userima koji imaju pravo ulaska u aplikaciju. Radi lakšeg rada sa ulogama potrebno je voditi računa o mehanizmima nasleđivanja uloga.

Obezbeđenje integriteta podataka kroz proveru privilegija nad podacima je deo sigurnosnog modula koji omogućava kontrolu rada nad već unetim podacima. Njegov model podataka se takođe oslanja na već definisane korisnike. Određenim korisnicima se dodeljuju privilegije i uloge i uz pomoć tih mehanizama imaju pravo rada nad već unetim podacima. Poseban segment u okviru ovog dela sigurnosnog modula je kontrola prikazivanja podataka koji u modelu podataka takođe ima svoje uloge i privilegije.

Za sva tri gore opisana aspekta potrebno je definisati funkciju neporecivost aktivnosti kojom se kroz tabele arhiva aktivnosti (u modelu podataka sigurnosnog modula) hronološki prati rad korisnika u sistemu. Opisani aspekti bezbednosti pokrivaju primarne bezbedonosne ciljeve (raspoloživost, integritet i poverljivost) date u skupu ciljeva zaštite u relevantnim standardima zaštite (SRPS ISO/IEC 27001, BS 25999, NIST,…). U domenu sistema upravljanja kvaliteta poslovanja potrebno je utvrditi ledeće kategorije mera:

- potvrda prirode i stepena incidenta,
- preuzimanje kontrole i koordinacija reakcije na incident
- komunikacija sa interesnim stranama, i
- obnavljanje aktivnosti organizacije.

Ovo je najopštije sagledavanje bezbednosti u aplikativnom sloju. Međutim, kako aplikativni sloj direktno zavisi od baze podataka, odnosno operativnog sistema kao nosioca baze i srednjeg sloja, to je i bezbednost aplikativnog rešenja direktno zavisna od sigurnosnih propusta u sloju operativnog sistema. Naime, kako je osnovni koncept u radu informacionih sistema da viši sloj programa prihvata servise iz nižeg sloja (operativni sistem, baze podataka, srednji sloj, aplikacija) to je i zaštita viših slojeva direktno zavisna od zaštite na nižim slojevima. Drugačije rečeno, onaj ko kontroliše operativni sistem praktično kontroliše i sve slojeve iznad njega. Način ponašanja provosudnih organa i pojedinaca koji imaju pristup bazama podataka pravosuđa mogu da ukažu na ozbiljne probleme koji mogu uticati na bezbednost, privatnost, poverljivost i dostupnost podataka. Potrebno je da se razvije sistematski proces za monitoring ovih ponašanja, kao i da se sprovode kontrole kako bi se ublažili rizici u vezi sa bazama podataka. U nastavku je dat pregled potencijalnih korisnika u jednom sistemu sa njihovim mogućim načinima pristupa podacima pohranjenim u bazama podataka. Uz svaki od ovih načina date su i preporuke za neutralisanje rizika:

a) PRIVILEGOVANI KORISNICI

Korisnici sa posebnim ovlašćenjima, na visokom nivou privilegije - administratori baza podataka i sistem administratori - treba uvek da budu predmet intenzivnog ispitivanja u organizaciji sa aspekta bezbednosti i to od posebnog lica zaduženog za bezbednost. Razlog za navedene radnje je očigledan jer ovi korisnici imaju uvid i pristup svim podacima i osnovama sistema, tako da potencijalno mogu da pričine ogromnu štetu. Oni treba da budu predmet rigoroznih rutinskih provera, i treba da se prate i revidiraju za sledeće potencijalne probleme/aktivnosti:

- Pristup, brisanje ili promena podataka,
- Pristup preko neodgovarajućih ili neodobrenih kanala,
- Šema modifikacije,
- Neovlašćeno dodavanje korisničkih naloga ili modifikacija postojećih naloga.

b) KRAJNJI KORISNICI

Krajnji korisnici - fizička lica koji imaju legitiman pristup podacima kroz neku vrstu primene poslovne aplikacije npr. suda predstavljaju ozbiljan rizik za namerne i nesvesne zloupotrebe tih podataka u sudskom, odnosno šire posmatrano pravosudnom sistemu. Bezbednosni stručnjaci bi trebalo da ulože posebnu pažnju na tri potencijalna problema ponašanja:

- Pristup prekomernoj količini podataka ili podatacima koji nisu potrebni za svakodnevni dodeljeni rad,
- Pristup podacima van standardnog radnog vremena,
- Pristup preko neodgovarajućeg ili neodobrenog kanala.

c) PROGRAMERI, SISTEM ANALITIČARI, ADMINISTRATORI

Ovi korisnici predstavljaju dve posebne vrste IKT rizika. Prvi rizik je potencijal za povrede podataka kao i kompromitovanje intelektualne svojine ili ličnih privatnosti. Ovi korisnici zbog prirode svog posla moraju da imaju izuzetno visok nivo privilegija za pristup. Mnogo ozbiljniji problem je što ovi tehnički najveštiji zaposleni u sudu imaju mogućnost pristupa ili promena delova sistema koji su u živoj produkciji, što može dovesti do lošeg rada, padova sistema i, u nekim slučajevima, dirigovanim bezbednosnim propustima. Primarno ponašanje IKT kadra u sudovima na koje bi trebalo obratiti pažnju je:

- Pristup živim podacima u poslovnim sistemima.

d) IKT OPERACIJE

IKT poslovanje sudova, ne samo pojedinačnih zaposlenih, ali i procesi za koje je odgovoran sud imaju značajan uticaj na pravilno funkcionisanje i upravljanje bazama podataka hijerarhijski nižih sudova. Njihove baze podataka vezane su za aktivnosti koje treba da budu revidirane u dve ključne oblasti:

- Neodobrene promene na bazama podataka ili aplikacijama,
- Vanciklusne zakrpe poslovnog sistema.

6. ZAKLJUČAK

Informaciona bezbednost u savremenom svetu postala je jedan od osnovnih izazova civilizacije, a njeno ugrožavanje potiče od zloupotreba informaciono komunikacionih tehnologija, malicioznih kodova, uništavanja i gubljenja podataka, *cyber* kriminala, zloupotrebe ličnih podataka, i drugih ilegalnih radnji [5]. Politika bezbednosti podataka, standarda, procedura i smernica nikada se neće zaista "završiti" već je potrebno da se ažuriraju s vremena na vreme i da prate promene unutar i izvan organizacije (npr. pojava novih pretnji bezbednosti informacija može biti povod za izmenu postojećih politika i sl. ili bar generaciju dodatnih materijala bezbednosne svesti o promeni pretnji).

Svest o informacionoj bezbednosti u Pravosudnom informacionom sistemu je nedovoljno razvijena jer su donosioci odluka lica sa osnovnim znanjem iz oblasti IKT, sa nepoznavanjem i potcenjivanjem potencijalnih opasnosti. Uvođenjem Politike informacione bezbednosti mogu se rešiti problemi i nedoumice: vremena čuvanja podataka, ograničavanje upotrebe resursa, odgovornost, zabrana postojanja vanproceduralnih sistema za prikupljanje i čuvanje podataka, prava i obaveze subjekata o kojima se i od kojih se podaci pribavljaju, korisnost, autentičnost podataka, dostupnost korisničkih uputstava, način skladištenja rezervnih kopija, pristup Internetu, način uništavanja neipravnih nosača podataka, itd.

Bezbednost nije samo tehnološka funkcija već je i pravno proceduralni okvir baziran na organizacionim promenama.

LITERATURA

[1] Dragović R., *Funkcionalne preporuke za uspostavljanje pravosudnog informacionog sistema*, Zbornik radova ISDOS, 2010.

[2] Dragović R., Ivković M., Perović B. Klipa Đ., *Dataveillance i data mining kao tehnološka podrška procesu istražnih radnji*, Zbornik radova TELFOR, 2011

[3] Dragović R., Perović B., Pešić Lj., Nuhović E., Klipa Đ., *Preporuke za unapređenje bezbednosti baza podataka u pravosudnom informacionom sistemu*, Zbornik radova YUINFO 2012,

[4] Dragović R., Kačanovski V. Perović B., *Politika bezbednosti pravosudnog informacionog sistema*, Zbornik radova YUINFO, 2011

[5] Ivanović Z., Dragović R., Uljanov S., *Strategic regulation model on the high-tech crime vulnerable targets*, Proceedings of Western Balkans: from stabilization to inte

ANALIZA PRIMENE NORMI O ZADRŽAVANJU PODATAKA KONVENCIJE CETS 185 U SRBIJI[5]
APPLICATION ANALYSIS OF THE RETENTION NORMS OF THE CONVENTION CETS 185 IN SERBIA

IVANOVIĆ ZVONIMIR
Kriminalističko – policijska akademija, Beograd, zvonimir07@sbb.rs
ANA BRANKOVIĆ
Kriminalističko – policijska akademija, Beograd, ana.brankovic@kpa.edu.rs

Apstrakt: U poslednje vreme veoma aktuelna problematika prenela se i na naše tlo, naime većina zemalja Evropske Unije ima problema sa famoznim zadržavanjem podataka o komunikacijama i pratećim direktivama i drugih akata Evropske Komisije i Evropskog parlamenta. U tom cilju autori ovde pokušavaju da daju analizu normi koje je država Srbija u obavezi da primeni po osnovu potpisane i ratifikovane Konvencije o visokotehnološkom kriminalu u svetlu poslednjih aktuelnih dešavanja. Pitanja poštovanja ljudskih prava i sloboda čoveka i građanina proklamovanih Ustavom Republike Srbije, kao i osnovne vrednosti, Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda (ESLJP) u ovom slučaju nisu u potpunosti očuvana pa je iz ovog razloga neophodno dati potpunu analizu primenjenih pravno tehničkih rešenja uz moguće korekcije na forenzičkoj i pravnoj ravni. Forenzička rešenja primenjena u normama kojima se pokušalo parirati usvojenim pravilima iz CETS 185 su u ovom radu objašnjena na jedan drugačiji način, koji daje nove aspekte problemu. Krajnji dometi ove analize jesu mogući predlozi koje autori nude u svom radu kao i poseban ugao gledanja na celokupnu problematiku.

Ključne reči: zadržavanje podataka, nadzor komunikacija, slobode i prava, ustav, policija, krivično procesno pravo

Abstract: In recent years a very actual issue is transposed into our territory, as in most EU countries, there are problems with the famous retention of communications data and related directives and other acts of the European Commission and European Parliament. To this end, the authors try to give here an analysis of standards that the state of Serbia is obliged to apply on the basis of signed and ratified the Convention on Cybercrime (CETS 185) in the light of recent events. Issues of human rights and freedoms of man and citizen proclaimed the Constitution of the Republic of Serbia, as well as basic values, proscribed in the European Convention on Human Rights and Fundamental Freedoms (ECHR) in this case are not fully preserved, so for this reason it is necessary to give full legal and partial forensic analysis of the applied technical solutions with a possible correction in forensic and legal level. Forensic solutions applied in the standards that attempt to convene the adopted rules of CETS 185 are explained in this paper in a sort of different way, which gives new aspects of the problem. The ultimate scope of this analysis are possible suggestions which the authors offer in their work as a special angle on the whole issue.

Keywords: data retention, monitoring communications, freedom and rights, constitution, police, criminal procedural law

[5] 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.

Uvod

Analizom CETS 185 možemo utvrditi da je niz ovlašćenja koje ona propisuje procesne prirode a da kod nas ista nisu predviđena procesnim zakonodavstvom. Velikaćina ovih mera je bila predvena podzakonskim aktima, a nakon donošenja zakona o elektronskim komunikacijama (ZOEK) ova materija biva regulisana njime i Zakonikom o krivičnom postupku. U ovom tekstu mi ćemo odbiti pomenute akte. Konvencijom o VTK – CETS 185 propisane su određene mere, a Srbija kao njen potpisnik u obavezi je da te mere primeni. Drugi deo drugog poglavlja CETS 185 pod nazivom „Procesno pravo“, bavi se procesnim ovlašćenjima državnih organa prilikom istraživanja krivičnih dela vezanih za nove te hnologije . Konvencija uvodi stare instrumente procesuiranja krivičnih dela u novoj srediništupći specifičnu prirodu kiber-prostora, i time stavlja na raspolaganje organima gonjenja nova sredstva u borbi protiv kriminala.

Osim opštih odredbi kojeah ažu državama da u svoje krivično pravo uvedu pomenuta krivična dela, kao i druga dela koja se ne nalaze u tekstu Konvencije a koja se mogu podvesti pod ovu grupu, obzirom na materijalne i procesne domete Zakona o organizaciji i žnosti državnih organa u borbi protiv VTK , velika žnja se posvećuje načinu prikupljanja podataka koji se nalaze na računarima ili prenosnim dajima, kao štita osnovnih prava pojedinca garantovanih Evropskom konvencijom o ljudskim pravima i Paktovima o ljudskim pravima UN . Pravne okvire postavljene u Konvenciji možemo posmatrati kao okvire kojima se omogva: Efikasnost rada organa gonjenja; Štiti mogućnost pružanja usluga pružalaca Internet usluga (Internet provajdera - ISP); obezbeđuje da se nacionalni standardi uskla de sa globalnim; promoši u globalni standardi načuma izolovanih nacionalnih; omogava primena principa legaliteta, proporcionalnosti i neophodnosti, kao i vladavina zakona; štita prava i slobodaveka i građana

Razrada

Proceduralna pravila bi se morala poštovati u pogledu dela propisanih prethodno opisanim Konvencije, ali i drugim kim delima izvšenim računarom, računarskim sistemima i mrežama, kao i kod pronalaženja, izazivanja, obezđenja i prikupljanja tragova u elektronskoj formi vezanih za ovakva krivična dela. Prema Konvenciji, nadležni organi gonjenja imaju ovlašćenja: da narede ili, načsli način, priave ili ostvare hitnu štitu određenih računarskih podataka, uključujući i podatke o saobraćaju koji su bili pohranjeni posredstvom računarskog sistema, u onim slajevima kada postoji osnovana sumnja da su ti podaci podli izmenama ili gubitku ova mera se kod nas predvi čl.128 ZOEK; da narede predaju određenih računarskih podataka određenim licima, učijem posedu (državin i - imaju faktičku vlast nad istim) se isti nalaze u određenom računarskom sistemu iliđenom mediju z pohranjivanje podataka, kao i Internet provajderima predaju podataka o korisnicima usluga vezanim za ovakve usluge a, koje su u posedu Internet provajdera ili u njegovoj fakkoj vlsti ; da zahtevaju parcijalno otkrivanje podataka o saobraaju , ova mera se, takde, predviđa istim članom ZOEK st.6. i suštinski kod nas ona predstavlja sastavni deo prethodno opisane mere; da pregledaju (pretresu) i zaplene svaki računar ili deo kao i računarske podatke pohranjene na njima, kao i medij za smeštanje (arhiviranje) čunarskih podataka ukoliko postoji osnovana sumnja da se nalaze inkrimini materijali U vezi ove mere možemo govoriti samo o ZKP –u i aktuelnom članu 504e odnosno novom ZKPčl.166; kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose, pre svega, na upotrebu Interneta i kreditnih kartica, a na osnovu kojih se žeo doći do identifikacije korisnika određene tehničke opreme (imena ili IP adrese potencijalnogčinioca krivičnog dela) ova mera je u Srbiji predviđena čl.129. ZOEK.

Hitna zaštita sačuvanih računarskih podataka predvda mogućnost nadležnih državnih organa da narede ili slčan način ostvare zštitu određenih računarskih podataka (uključujući tu podatke o saobraćaju sačuvane preko računarskog sistema), posebno u slajevima kada se veruje da su takvi podaci podložni gubitku ili izmeni, kao i da se lice ili ustanova na koje se takva naredba odnosi obaveže da štiti i ašuva celovitost tih čunarskih podataka za neophodan vremenski period a najviše do 90 dana kao i da se obaveže da štiti tajnost takvih postupaka. Praktično u pitanju su slučajevi kada postoji operativna, forenzička ili praktična potreba za ču vanjem istih. Lica zadužena za zadavanje ovakvih podataka i dajuga moraju čuvati podatke o njima kao poverljive . Kod nas je rok obavezivanjačuvanja ovih podataka kašto je već pomenuto 12 meseci, što je izuzetno dug period i pred obveznike ove mere stavlja veoma tešku dužnost. Naime, podaci o kojima je reč mogu biti značajnih gabarita, pa se postavlja pitanje pretežnosti značaja obaveze u odnosu na troškove koji se njenom primenom stvaraju. Takođe, od značaja je i okolnost o kojoj je već razmatrano ob aveza je 90 dana, pa čemu onda postavljanje mnogo širih okvira?

Hitna zaštita i delimično otkrivanje podataka o saobraćaju u realnom vremenu predvi mogućnost hitne ašite podataka o saobraćaju u odnosu na podatke iz prethodne mere, bez obzira da li je u prenosu poruke učestvovao jedan ili više davalaca usluga, kao i mogućnost otkrivanja količine podataka o saobraćaju dovoljne za identifikaciju davalaca usluga i putanje kojom je saobraćaj izvršen (član 17). čl.128 st.3 i 6, se ove ovom obavezom u Srbiji pa navodi da: „operator nije dan da zadži podatke koje nije proizveo niti obradio.što će reći ad posebno za svakog od operatera korišćenih u ovoj komunikaciji mora biti poslat poseban akt za svakogćeodh kori komunikacionih sredstava. Ova situacija je veoma problematična u lčnom smislu jer će akvu imt slučajevima biti nepremostivih pretnji, zamislimo samo mnogo prenetih brojeva iz nekoliko nacionalnih operatera mobilnih telefonija i više uključenih skajp ili drugih VoIP mesindžera u datoj komunikaciji, to je šuma veza, a voleli

bi se zapitati kako izgledaju akta koja treba da isprate ovakvu komunikaciju.

Izdavanje naredbe predviđa mogućnost nadležnih državnih organa da narede licu na svojoj teritoriji da preda određene računarske podatke koje poseduje ili kontroliše, a sačuvani su u računarskom sistemu ili na medijumu za čuvanje računarskih podataka, kao i davaocu usluga koji pruža usluge na teritoriji strane ugovornice da preda podatke o pretplatniku koji se odnose na usluge koje taj davalac usluga poseduje ili kontroliše (član 18). Ova materija se reguliše normama koje se odnose na privremeno oduzimanje predmeta prema ZKP – u. U pitanju su odredbe čl.82.

Pretraživanje i zaplena (privremeno oduzimanje) sačuvanih računarskih podataka predviđa mogućnost nadležnih organa da na svojoj teritoriji pretraže određeni računar , računarski sistem, računarski program ili njegov deo i u njemu sačuvane računarske podatke, medije za čuvanje računarskih podataka ili da, ukoliko su traženi podaci sačuvani na nekom drugom računarskom sistemu, pri čemu tim podacima može da se pristupi sa početnog računarskog sistema, prošire pretragu ili na drugi sličan način pristupe tom računarskom sistemu(član 19). Predviđena je mogućnost da nadležni organi zaplene ili na sličan način obezbede računarski sistem ili njegov deo kao i medije za čuvanje podataka, naprave i zadrže kopije tih računarskih podataka, čime se održava celovitost bitnih računarskih podataka čine računarske podatke nedostupnim ili ih uklone iz računarskog sistema, k om je pristupljeno. Postoji mogućnost da se svakom licu koje poznaje način rada računarskog sistema ili mere primenjene za zaštitu podataka, na tom sistemu, naredi da, u razumnoj meri, pruži neophodne podatke, kako bi se omogućilo preduzimanje opisanih mer a. Neophodno je ovde razmotriti i pretrage u povezanim sistemima . Ukoliko razmatramo pretrage koje se u virtuelnom svetu prostiru i na teritorije drugih država neophodno je predvideti i mogućnosti sprovođenja ovakvih pretraga od strane drugih država i njihovih policija (organa gonjenja). Uslovi su: da se predmet pretrage javlja dostupnim sa: računara, sistema, programa ili njegovog dela,čiji vlasnik ima pristup ili mogućnost kontrolea za kojeg postoji osnov za pretresanje, pa je zato neophodno dati legislativnu mogućnost proširenja pretraga i kroz ovakve mogućnosti. U ovom smislu posebno treba voditi računa o: tzv. open source (otvorenim) izvorima, koji su svima dostupni, bez obzira gde se nalaze, ali i javno dostupnih pohranjenih podataka, programa, podataka o saobraćaju komunikacija i sadržaju istih, bez obzira načijoj teritoriji se nalaze. Što se tiče privremenog oduzimanja predmeta ono se odnosi na prethodno pominjane digitalne podatke i podrazumeva sledeće : zaplenu ili slična sredstva za obezbeđenje računara, računarskog sistema ili njegovog dela, ili medijuma za pohranjivanje podataka; pravljenje i zadržavanje „imidža“ (image) pominjanih podataka; očuvanje integriteta ovih podataka i obezbe dokumentovanja ovakvog čuvanja integriteta putem primene sredstava matematičkih algoritama; izazivanja prikrivenih ili nepristupačnih podataka i njihovo izuzimanje sa računara (sistema). Sve opisano se odnosi na pravila o pretresanju stana i ostalih prostorija koja su regulisana ZKP – om, čl.78-81.

Prikupljanje podataka o saobraćaju u realnom vremenu predviđa ovlašćenja nadležnih organa da prikupljaju ili pohranjuju u realnom vremenu podatke o saobraćaju određenih komunikacija prenetih prekoračunarskog sistema ili da prikupljaju ili snimaju podatke o saobraćaju povezane sa određenim komunikacijama, koje se prenose na teritoriji države primenom tehničkih sredstava koja se nalaze na toj teritoriji (član 20 Konvencije). Interesantno je pomenuti i da se daje mogućnost da se u ovom smislu koriste i provajderi usluga – da se putem akta nadležnog organa oni prinude (ili od njih zahteva) da preduzmu ovakve radnje . Ova mera je jedna od najspornijih mera i mnoge države, pa i naša, pokušale su da ovu meru propišu i u tome nisu bile uspešne. Problem se može svesti n sledeće okolnosti:

U okvirima rasprave o komunikacijama od značaja je nekoliko nacionalnih zakona i Ustav. U Zakonu o elektronskim komunikacijama, a i u podzakonskim aktima, koji se na osnovu njega imaju doneti, kao podzakonski pravni akti kojim se potpunije reguliše njihova primena, prava i slobode čoveka i građana koja se ograničavaju su: garantovana tajnost pisama i drugih sredstava komunikacije predviđenih u članu 41. Ustava Republike Srbije (US) i garantovana zaštita privatnosti ličnih podataka iz člana 42., kao i člana 46. US u pogledu slobode mišljenja i izražavanja. Naravno svako ograničavanje sloboda i prava mora biti propisano zakonom, obrazloženo i ono mora biti opravdano, srazmerno koristi koja iz istih proizilazi, a kako dolikuje demokratskom društvu.

U pravcu razmatranja ove problematike svojevremeno su krenule i određene institucije Republike Srbije koje su garant zaštite sloboda i prava građana – Zaštitnik građana i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, inicijativom za ocenu ustavnosti i zakonitosti . Ona se odnosila na član 128. Zakona o elektronskim komunikacijama („Službeni glasnik RS“, br. 44/2010) i to: stava 1., u delovima koji glase „u skladu sa zakonom kojim se uređuje krivični postupak“ i „u skladu sa zakonima kojima se uređuje rad službi bezbednosti i rad organa unutrašnjih poslova“ i stava 5. u delu koji glasi „na zahtev nadležnog državnog organa, u skladu sa stavom 1. ovog člana“; ali i člana 13. stav 1. u vezi sa članom 12. stav 1. tačka 6) Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji ("Službeni glasnik RS", br. 88/2009) ana čl16. stav 2. Zakona o vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji (VBA i VOA) . Ovakav stav ne odgovara dosadašnjoj praksi i zakonom propisanim okvirima. Značajno je pomenuti da je ova inicijativa bila samo delimično uspešna. Saopštenje sa 7. sednice Ustavnog suda , održane 19. aprila 2012. godine: Ustavni sud je na 7. sednici odlučivao o 7 predmeta. I U predmetima ocene ustavnosti i zakonitosti opštih pravnih akata Ustavni sud (US) je: - utvrdio da odredbečlana 13. stav 1. u vezi sa

članom 12. stav 1. tačka 6) i član 16. stav 2. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji ("Službeni glasnik RS", broj 88/09) nisu u saglasnosti sa Ustavom. Sud je odbacio zahtev za obustavu izvršenja pojedinačnih akata donetih, odnosno radnji preduzetih na osnovu osporenih odredaba navedenog Zakona. (predmet IUz-1218/2010) Ovo samo po sebi predstavlja jedan pravni paradoks.

U pogledu osporene odredbe Zakona o elektronskim komunikacijama (ZEK) nije još ništa odlučeno. Osporene odredbe člana 128. stavova 1. i 5. ZEK, prema mišljenju inicijatora ocene ustavnosti i zakonitosti, nesaglasne su sa odredbom člana 41. stav 2. US, jer dozvoljavaju primenu posebnih mera kojima se odstupa od tajnosti pisama i drugih sredstava komunikacije ne samo u skladu sa sudskom odlukom, već i bez naredbe suda - kada je takva mogućnost propisana zakonom, odnosno na zahtev nadležnog državnog organa .

Suštinski problem se svodi na dve osnovne komplikacije – pitanje tretmana forme i sadržaja komunikacija i dosadašnju praksu u vezi sa njima, kao i pitanja korenite reforme zakonodavstva u oblasti nadzora komunikacija.

Na osnovu pomenute inicijative i paradoksa koji je prikazan neophodno je dalje opisati dramu pravosudja i praktične policijske primene mera, koje su gore opisane. Nakon ovakve odluke US o neustavnosti i obaveštavanja o njoj javnosti preko zvanične internet prezentacije, na sastanku održanom na inicijativu Zaštitnika građana, predstavnici Vojnobezbednosne agencije obavestili su Zaštitnika građana i Poverenika da će zakon primenjivati sve dok sud svoju odluku ne objavi u Službenom glasniku (što se još nije desilo). Policija i Tužilaštvo su, međutim, na istom sastanku, istakli da će nastaviti da bez odluke suda prikupljaju podatke o komunikacijama građana jer oni ne primenjuju zakon čija je neustavnost utvrđena, već Zakonik o krivičnom postupku, koji do tada nije bio osporen pred Ustavnim sudom. Novim predlogom Ustavnom sudu, Zaštitnik i Poverenik su sada osporili i Zakonik .

Od svih službi koje, obavljajući svoju delatnost, mogu da zadiru u privatnost komunikacija građana, jedino je Bezbednosno-informativna agencija obavestila Zaštitnika građana i Poverenika da je spremna da, budući da već doneta odluka Ustavnog suda sadrži jasan stav da je svako prikupljanje podataka o komunikacijama građana, bez odluke suda – neustavno, bez odlaganja uskladi svoj rad sa odlukom Ustavnog suda, iako se ona na BIA formalno ne odnosi.

S obzirom da je Ustavni sud čak više puta stao na stanovište da je za zadiranje u privatnost komunikacija građana neophodna, kako Ustav izričito nalaže, odluka suda, a ne drugog organa, a da preti opasnost čak i od odluke Ustavnog suda hiljade građana biti predmet neustavne kontrole opštenja, inicijatori su zatražili od Ustavnog suda privremenu meru zabrane Policiji da prikuplja podatke o komunikacijama građana bez odluke suda, do donošenja konačne odluke o predlogu za ocenu ustavnosti. O ovome se još nije odlučivalo i veoma je veliko pitanje domašaja inicijative, čak i mogućih privremene mere.

Presretanje podataka iz sadržaja predviđa ovlašćenja nadležnih organa da prikupljaju ili snimaju u realnom vremenu podatke iz sadržaja određenih komunikacija prenetih preko računarskog sistema ili da prikupljaju ili snimaju podatke o saobraćaju koji se odnose na određene komunikacijama, koje se prenose na teritoriji države (čija je jurisdikcija) primenom tehničkih sredstava, koja se nalaze na toj teritoriji (član 21). U određenim zemljama mera ima naziv prospektivni nadzor, ona podrazumeva pretraživanje Interneta u realnom vremenu i „osluškivanje“ saobraćaja. U pitanju su za Srbiju već pominjani čl.504e ZKP ili 166. novog ZKP. Mere sadržane u Konvenciji, prihvaćenju međunarodne zajednice, predstavljaju neophodan minimum standarda za obezbeđenje preduslova za uspešno suzbijanje visokotehnološkog kriminala koje bi trebalo ugraditi u nacionalna zakonodavna rešenja. Ipak, državama koje su potpisale i ratifikovale Konvenciju ostavljena je mogućnost stavljanja rezerve na primenu mera u vezi prikupljanja podataka o saobraćaju u realnom vremenu i presretanja podataka iz sadržaja. Svrha stavljanja rezerve je da se stranama ugovornicama omogući da odobre uspostavljanje, sprovođenje i primenu ovlašćenja iz Konvencije usaglase sa uslovima i ograničenjima predviđenim domaćim zakonodavstvom, koje treba da omogući odgovarajuću zaštitu ljudskih prava i sloboda.

Zaključak

Ovako prikazane mere predstavljaju jedan zaokružen sistem koji nudi Konvencija o VTK – CETS 185, i za jednu slobodnu, demokratsku zemlju predstavljaju minimum prava i sloboda u okvirima komunikacionog spektra. Naravno ovako propisane mere suštinski su smernice državama potpisnicama i jedan zdrav pravni okvir na osnovu kojeg je ostavljeno tim državama da ga dalje razrađuju i inkorporiraju u svoja zakonodavstva. Problem koji je opisan u ovom radu nije problem koji se dešava samo nama, slično se dogadalo i u Bugarskoj, Češkoj, Nemačkoj, Poljskoj...ali ovo je naš problem u ovom trenutku ipak sui generis u smislu određenih normi, određenih zakona, teorijskih postavki i koncepata shvatanja komunikacija, praktično razmimoilaženje ovih koncepata sa konceptima koje nude odluke Evropskog suda za ljudska prava (ESLJP) u Strazburu – konsekventno poslednja remarka vodi i problemu primene standarda predviđenih odlukama pomenutog suda u budućim postupcima pred ovim sudom a u kojima bi naši građani bili tužioci a naša država tužena upravo u ovoj oblasti a u vezi primene čl.8. Evropske konvencije o ljudskim pravima i osnovnim slobodama koji se odnosi na Pravo na poštovanje privatnog i porodičnog života, a posebno u svetlu objašnjenja koje je dato gore i u jednoj i u drugoj krajnosti. Naravno da nije ovog momenta nije toliko blisko, ali verujemo da će u budućnosti (bilo ona bliska ili ne) biti dostupno i u smeru koji nam nudi ESLJP a u nekim specifičnijim formama, makar one bile u

potpunosti propisane neprocesnim ili procesnim zakonodavstvom.

Literatura

[1] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[2] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

[3] http://www.ombudsman.rs/attachments/1151_Predlog%20Ustavni%20sud%20final%202%20(2).doc

[4] http://www.ustavni.sud.rs/page/view/149-101597/saopstenje-sa-7-sednice-ustavnog-suda-odrzane-19-aprila-2012-godine-kojom-je-predsedavao-dr-dragisa-slijepcevic-predsednik-ustavnog-suda

[5] Urošević, V. Ivanović, Z. Ujanov, S. Mi u www – u: Izazovi VTK, Eteral mix, Beograd, 2012.

[6] Ivanović, Z. u a Harmonizacija zakono davstava Republike Srbije sa pravom EU, Analiza harmonizacije propisa u oblasti VTK, IMPP, IUP, HSS Beograd, 2012, str.795-808,

Konferencija o bezbednosti informacija BICES 2012
Univerzitet Metropolitan

KVALIFIKOVANI ELEKTRONSKI POTPIS U ELEKTRONSKOJ UPRAVI

QUALIFIED ELECTRONIC SIGNATURE IN E-GOVERNMENT

ALEKSANDAR IVIĆ
Uprava za Digitalnu agendu, Beograd, Aleksandar.Ivic@digitalnaagenda.gov.rs

Rezime: *Komunikacija putem interneta sa Državnom upravom je od višestruke važnosti za razvoj ekonomije znanja jedne zemlje. Korišćenje Kvalifikovanog digitalnog sertifikata izdatog od strane Sertifikacionog tela, omogućava benefit kako korisniku tako i samoj Državnoj upravi putem mehanizama za obezbeđenje integriteta, neporecivosti i jednoznačne autentifikacije. Zakonski okvir u Republici Srbiji prepoznaje i reguliše upotrebu ovih mehanizama zakonskim i podzakonskim aktima.*

Ključne reči: *Kvalifikovani elektronski potpis, eUprava, Digitalni sertifikati*

Abstract: *Communication via the internet from Citizen to Government has multiplied significance to develop knowledge economy. Using qualified electronic certificates issued from Certified Authority gain benefits to owner of certificate and to Government itself through system for authentication, integrity and non-repudiation. Legal framework in Serbia recognize those mechanisms and regulate its usage.*

Keywords: *Qualified Electronic Signature, eGovernment, Digital Certificates*

1. UVOD

Elektronska uprava (eUprava) obezbeđuje građanima i privredi jednostavnije i brže obavljanje poslova pred organima državne uprave. Upotreba alata i sistema baziranih na informaciono-komunikacionim tehnologijama obezbeđuje promenu procesa i načina rada i omogućava pojednostavljeni pristup korisnika javnim uslugama. Efikasnost elektronske uprave ogleda se u pojednostavljenju administracije za rezidencijalne korisnike i pravna lica, povećanje transparentnosti i odgovornosti, što za posledicu ima i smanjenje korupcije u svim segmentima javne uprave[1].

Svim građanima, preduzećima i organizacijama se uvođenjem e-uprave omogućava da poslove pred organima vlasti završavaju jednostavnije, brže i jeftinije. Građanima je omogućeno da sve javne usluge, za koje je to pogodno, koriste posredstvom Interneta i svog ličnog računara, drugog kućnog ili mobilnog uređaja. Preduzećima je omogućeno da javne usluge koriste posredstvom Interneta, sa mogućnošću elektronske razmene podataka između informacionih sistema preduzeća i organa vlasti. eUprava obuhvata više od tehnologija i tehničkih sredstava koji omogućavaju tzv bespapirnu (paperless) komunikaciju između države i građana tj. države i preduzeća. Ovakav pristup uključuje i promenu propisa i zakona, organizacije, postupaka i načina rada organa vlasti kako bi se javne usluge efikasnije pružale licima kojima su potrebne.

Uspostavljanje elektronskih javnih servisa se vrši preko portala e-uprave i zajedničke elektronske usluge. Portal e-uprava predstavlja jedinstvenu tačku pristupa većem broju e-servisa, pri čemu su na njemu implementirane i zajedničke elektronske usluge koje su od značaja za realizaciju više e-servisa, kao što su centralni sistemi za proveru elektronskog identiteta, elektronsko plaćanje, preuzimanje elektronskih formulara i sl. E-servisi mogu biti različitog nivoa sofisticiranosti, od dobijanja informacije do najvišeg nivoa personalizovanog servisa, sa autentifikacijom, podnošenjem zahteva, plaćanjem potrebnih taksi, digitalnog potpisivanja i izvršenja i dostavljanja elektronskog ili papirnog odgovora organa Uprave kom je upućen zahtev [1]

2. PREDUSLOVI ZA REALIZACIJU ELEKTRONSKE UPRAVE

Osnovne pretpostavke za realizaciju inicijative eUprava su:
ICT Infrastruktura pod kojom pre svega podrazumevamo:

- komunikaciona infrastrukturu koja omogućava računarsku povezanost organa vlasti, kao i vezu sa Internetom;
- računarske centre sa serverima i drugim informaciono-komunikacionim resursima gde će se smeštati baze podataka, izvršavati aplikacije i tehnološki realizovati elektronske usluge
- infrastruktura na pojedinim lokacijama koja uključuje lokalne računarske mreže, računare, drugu računarsku opremu i softver.

Elektronske službene evidencije. Pored vođenja evidencija u elektronskoj formi, potrebno je obezbediti efikasan i bezbedan pristup elektronskim putem podacima iz evidencija od strane službenika koji vode postupak, da bi se eliminisala potreba da stranka u postupku pribavlja dokaze o činjenicama iz evidencije.

Standardizacija u oblasti primene ICT i koordinacija ICT projekata u organima dovodi ne samo do postizanja efikasnosti neponavljanjem već postignutih rešenja već omogućava i povezivanje raznorodnih sistema kao preduslov za automatizaciju procesa u Upravi.

Elektronski identitet, elektronski potpis i elektronski dokument. Potrebno je obezbediti pouzdano i bezbedno utvrđivanje identiteta potpisnika elektronskog dokumenta i korisnika elektronske usluge. Osnov za to je tehnologija elektronskog potpisa. Takođe je potrebno postići da se elektronski dokument koristi kao original

3. UPRAVLJENJE ELEKTRONSKIM IDENTITETIMA - PRAVNI OKVIR

Neophodna zakonska regulativa za implementaciju mehanizama za podizanje nivoe sofisticiranosti servisa eUprave nije prepoznata isključivo od strane implementatora rešenja Elektronske Uprave. Potpisivanjem eSEE agende obavezali smo se na ispunjavanje preduslova za stvaranje platforme za bezbedno e-poslovanje uvođenjem zakonskog okvira za infrastrukturu javnih ključeva. Ova obaveza podrazumeva i harmonizaciju radi postizanja prekogranične interoperabilnosti za elektronski potpis i elektronski identitet, a u skladu sa preporukama Evropske komisije. [eSEE referenca]

Zakonskom regulativom u Srbiji prepoznat je Elektronski dokument kao punovažan način komunikacije u pravnom prometu, ali i u Upravnom, Sudskom ili bilo kom drugom postupku. Zakon o elektronskom dokumentu [referenca] precizira se način izrade, razmene, dostave, kopiranja u papirnu formu. Ovim zakonom se postavlja okvir za formiranje infrastrukture za vremenski žig. Na žalost, deo zakona koji se odnosi na čuvanje ovakvih dokumenata se poziva na regulativu vezanu za zakon o Arhivskoj građi, što je izazvalo nedoumice a samim tim u nedovoljnu primenu ovog zakona u praksi.

4. ASIMETRIČNA KRIPTOGRAFIJA

Zakonska regulativa i rad Sertifikacionih tela u Srbiji se bazira na principima asimetrične kriptografije, te je ovo prilika da se kaže par reči o ovom, u praksi široko korišćenom, obliku kriptografije

Asimetrična kriptografija ili kriptografija sa javnim ključem je oblik kriptografije gde se ključ za kriptovanje poruke razlikuje od ključa za dekriptovanje poruke. Jedan od ova dva ključa koji može biti javno dostupan ili distribuiran zainteresovanim stranama se naziva Javnim ključem a drugi, koji se čuva, Privatni ključ. Iako su ova dva ključa matematički povezana, privatni ključ ne može biti otkriven preko javnog ključa kod algoritama koji se koriste u ove svrhe u praksi.

I bez znanja kombinatorike jasno je da postoje dve mogućnosti za objavljivanje jednog od ključeva u javnost. Nama posebno interesantan je slučaj da se ključ za dekriptovanje daje kao javni ključ. Tada se sistem Javnih ključeva koristi za proveru potpisnika poruke, koji poseduje privatni ključ za kriptovanje. Obzirom da je kriptovanje cele poruke odnosno fajla procesorski zahtevan proces, u praksi se kriptuje samo checksum, tzv. hash poruke. Ova, nazovimo je ušteda, nam omogućava da sadržajni deo poruke, odnosno fajla, može da se vidi bez znanja konkretnog javnog dela ključa. Kreiranjem kriptovanog hash dela fajla formira se Digitalni potpis.

Ovakvim postupkom se pored utvrđivanja identiteta onog ko je izvršio kriptovanje – u našem slučaju Potpisnika onemogućava bilo kakva izmena prvobitne poruke, tj postiže se neoporecivost kao dodatni kvalitet digitalno potpisane poruke.

Druga mogućnost je da se javno daje ključ za kriptovanje, koji služi za kodiranje poruke. U tom slučaju bilo ko, sa dovoljno tehničkih znanja i entuzijazma, može da kodira poruku tako da je može dešifrovati samo ponosni vlasnik privatnog ključa. Čak ni sam pošiljalac više neće imati uvid u sadržaj poruke (ukoliko nije sam sebi uputio poruku).

Sa sertifikatima koji su kod nas u upotrebi kao Kvalifikovani sertifikati, dakle, nije moguće kodirati poruku. Ova grana kriptografije sistemom javnih ključeva nije predmet interesovanja u ovom radu, a kao dobar primer implementacije preporučujem korišćenje softverskog rešenja pod nazivom PGP koje je kreirao Phill Zimmerman 1991 godine.

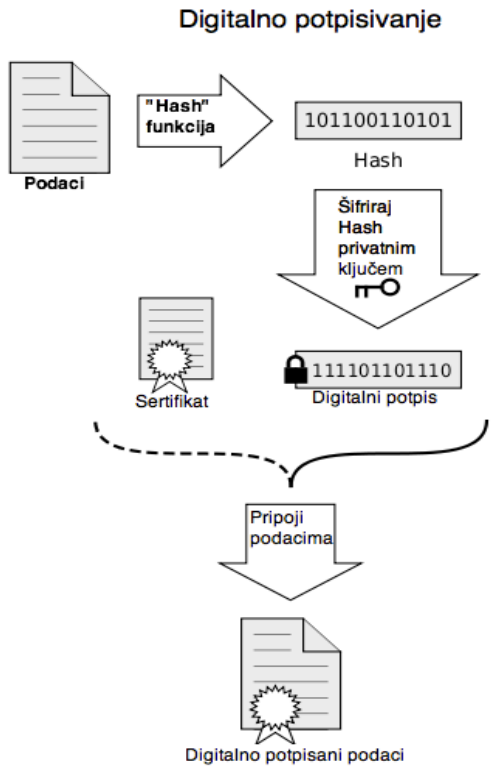
4. (KVALIFIKOVANI) ELEKTRONSKI POTPIS

"Elektronski potpis" je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika. - Zakon o Elektronskom potpisu[2] Elektronski potpis je širi pojam od pojma Digitalni potpis.

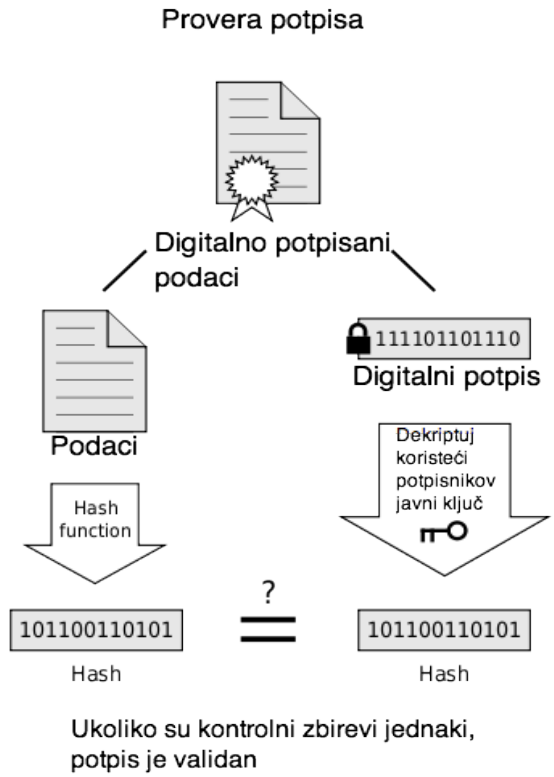
Digitalni potpis je matematička šema koja dokazuje autentičnost digitalne poruke odnosno dokumenta. U Zakonu o Elektronskom potpisu ovaj pojam je nazvan "Kvalifikovani elektronski potpis" - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene ovim zakonom.

Šema digitalnog potpisa se, tipično, sastoji od tri postupka - algoritma:

- *Generisanje ključeva* gde se privatni ključ bira na slučajan način iz skupa privatnih ključeva i generiše se odgovarajući javni ključ
- *Algoritam potpisivanja* na osnovu poruke ili fajla i privatnog ključa generiše se potpis
- *Algoritam provere potpisa* gde se na osnovu poruke, javnog ključa i potpisa proverava validnost samog potpisa.



Slika 1: Digitalno potpisivanje



Slika 2: Provera validnosti digitalnog potpisa

Razlozi za korišćenje ove tehnologije su:
Autentifikacija: Pošto je vlasništvo nad privatnim ključem kontrolisano dodeljeno vlasniku uz utvrđivanje njegovog identiteta, za šta garantuje Sertifikaciono telo koje dodeljuje Elektronski sertifikat, samo vlasnik tog sertifikata može da potpiše poruku. U Zakonu o el. potpisu: Član 7. - nedvosmisleno identifikuje potpisnika
Integritet poruke: Iako enkripcija poruke krije njen sadržaj, za pretpostaviti je da je moguće izmeniti sadržaj poruke bez njenog razumevanja. Digitalno potpisana poruka nakon bilo kakve izmene neće proći korak provere potpisa. Član 7. Zakona: Kvalifikovani el. potpis direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka;
Neoporecivost: Potpisnik poruke ne može naknadno da tvrdi da je nije potpisao. Ekvivalentna tvrdnja je da nije moguće krivotvoriti validan digitalni potpis. U Zakonu je neoporecivost izražena kao: isključivo je povezan sa potpisnikom. Ukoliko vlasnik privatnog ključa želi da porekne da je potpisao neku poruku može da tvrdi da je došlo do gubljenja tj. kompromitovanja privatnog ključa. Zakonska regulativa nalaže da se takvi slučajevi odmah prijave a nakon toga Sertifikaciono telo povlači sertifikat.

4. ELEKTRONSKI SERTIFIKAT

U šemi asimetrične kriptografije najslabija karika je očuvanje privatnog ključa zaista privatnim. Korišćenjem privatnog ključa koji bi bio lokalno skladišten na disku računara kojim se potpisuje ima slabu stranu što bi tada ključ ostajao na svakom računaru kojim vršimo digitalno potpisivanje. Tada bi sigurnost privatnog ključa zavisila od sigurnosti samog računara.

Sigurniji način čuvanja privatnog ključa je na Smart kartici. Sistem funkcioniše tako što se Hash izračunat iz dokumenta šalje na Smart karticu čiji procesor uz privatni ključ koji je smešten na Smart kartici enkriptuje Hash i vraća ga računaru. Dodatna zaštita je što Smart kartice koje su u upotrebi su tipično zaštićene PIN-om, što je slučaj sa svim Smart karticama koje su u upotrebi za ovu svrhu u Srbiji. Ovo obezbeđuje zaštitu u dva koraka.

Privatni ključ sa Smart kartice ne bi trebalo da je moguće kopirati. Sa druge strane samo Sertifikaciono telo koje je izdalo sertifikat ne bi trebalo da poseduje kopiju privatnog ključa.

5. ZAKLJUČAK

Zakonski okvir u Srbiji daje osnov za upotrebu digitalnog potpisa i elektronskih dokumenata kako u pravnom, sudskom tako i u upravnom postupku. Podzakonska akta u obliku Uputstava i Uredbi su donesena u velikoj meri. Korišćenjem infrastrukture razvijene od strane sertifikacionih tela, upisanih u Registar sertifikacionih tela koje vodi nadležno Ministarstvo, omogućeno je smanjenje rizika od napada na informacione sisteme, veća dostupnost i bolja zaštita samih sistema.

Demonstracija u obliku implementacije mehanizama od autentifikacije, preko digitalnog potpisivanja, vremenskog žiga, ali i daleko složenijih kao što su elektronsko plaćanje i povezivanje putem web servisa sa raznorodnim

registrima u Državnoj upravi je sprovedena na Državnom portalu eUprava. Ključni mehanizmi su dati na raspolaganje potpuno besplatno i drugim organima Državne uprave.

Pored navedenog navedeni mehanizmi se više koriste kao izuzetak nego kao pravilo. Osnovni problemi su u nepostojanju koordinacije u izradi IKT rešenja između raznih ministarstava, nedovoljna informisanost donosilaca odluka, kao i nedostatak volje da se stvari menjaju. O inertnosti sistema govori i podatak da je Zakon o Elektronskom potpisu donesen još pre osam godina.

LITERATURA

[47] *Strategija razvoja elektronske uprave za period od 2009. do 2013. godine zajedno sa Akcionim planom*, „Službeni glasnik RS", br. 83/09 i 5/10

[48] *Zakon o elektronskom potpisu*, „Službeni glasnik RS", br. 135/2004

[49] *Zakon o elektronskom dokumentu*, „Službeni glasnik RS", br. 51/2009

[50] Introduction to Cryptography, Network Associates, 1999, http://www.pgpi.org/doc/guide/6.5/en/intro/

UPRAVLJANJE INCIDENTIMA U SKLADU SĄ ZAHTEVIMA STANDARDA ISO 27001:2005

INCIDENT MANAGEMENT IN ACCORDANCE WITH THE REQUIREMENTS ISO 27001:2005 STANDARD

DRAGAN MARKOVIĆ
HDL Design House, Beograd, d-markovic@hdl-dh.com

Rezime: *U radu su prikazani osnovni zahtevi za upravljanje incidentima (Incident Management) prema standardu ISO/IEC 27001:2005 i standardu ISO/IEC 20000-1:2011 i veza izmedju zahteva ova dva standarda. Opisani su glavni elementi u praktičnoj primeni upravljanja incidentima uz korišćenje smernica iz standarda ISO/IEC 27035:2011 Upravljanje incidentima bezbednosti informacija. Prikazan je uporedni pregled statističke obrade podataka o incidenatima unutar ISMS u preduzeću HDL Design House za poslednje tri godine. U zaključku je ukazano na značaj primene više ISO standarda za efikasno i efektivno upravljanja incidentima unutar ISMS.*

Ključne reči: *Bezbednost informacija, upravljanje incidentima, ISO/IEC 27001:2005, ISO/IEC 27035:2011, ISO/IEC 20000-1:2011*

Abstract: *The paper shows basic requirements for Incident Management according to ISO/IEC 27002:2005 standard, ISO/IEC 20000-1:2005 standard, and the relation between the requirements of the two standards. The main elements in practical application of incident management are described using ISO/IEC 27035:2011 standard – Information security incident management. A comparative review of statistical data regrading incidents within ISMS of the company HDL Design House for the last three years is shown. The conclusion indicates the importance of application of several ISO standards for effective and efficient incident management.*

Keywords: *Information security, upravljanje incidentima, ISO/IEC 27001:2005, ISO/IEC 27035:2011, ISO/IEC 20000-1:2011*

1. UVOD

Višegodišnji eksponencijalni razvoj informacionih tehnologija je omogućio višestruko povećanje obima razmene informacija u svim oblastima života i rada (od obrazovanja do svemirskih istraživanja) i na svim nivoima (od kućnog okruženja do velikih multinacionalnih kompanija). Posledica takvog obima razmene je dovelo i do potrebe za zaštitom informacija koja se ogleda u očuvanju integriteta, raspoloživosti i poverljivosti informacija.

Svako narušavanje jednog od ova tri svojstva se može smatrati neželjenim događajem – incidentom. Pod incidentom se moze smatrati i "pojedinačan događaj ili seriija neželjenih ili neočekivanih događaja u vezi sa bezbednošću koji imaju značajnu verovatnoću kompromitovanja poslovnih informacija ili pretnji bezbednosti informacija" [1].

Pod upravljanjem incidentima možemo smatrati niz postupaka u kome se na tačno utvrđen način, kontinuiranio i sistematično vrši praćenje, beleženje, rešavanje i ponovno preispitivanje incidenata u vezi bezbednosti informacija.

Upravljanje postojećim (identifikovanim) incidentima neće sprečiti pojavu novih incidenata sigurnsti informacija, ali za cilj svakakako ima pravovremeno delovanje kako bi se njihovo dejstvo neutralisalo ili eventalne posledice minimizirale.

2. ZAHTEVI STANDARDA ISO/IEC 27001:2005

Upravljanje incidentima prema standardu ISO/IEC 27001:2005 nije nigde eksplicitno zahtevano, ali se ovaj zahtev "krije" u zahtevu tačke 4.2.3 – Nadzor i preispitivanje ISMS gde se od organizacije trazi da:

a) 2. promntno identifikuje pokušavana i uspešna narušavanja bezbednosti informacija i incidente vezane za nji

4. pomogne u otkrivanju događaja vezanih za bezbednost i na taj način spreči incidente bezbednosti informacija upotrebom indikatora i
5. utvrdi da li su akcije preduzete da se razreše narušavanja bezbednosti informacija bile efektivne [2]

Ovih nekoliko tačaka pred organizaciju postavljaju osnovne zahteve (elemente) za upravljanje incidentima bezbednosti informacija.

3. ZAHTEVI STANDRADA ISO 20000-1:2011

Standard ISO/IEC 20000-1:2011 se odnosi na opšte upravljanje IT uslugama (IT Service Management) i u odnosu na svoje prvo izdanje iz 2005. god. postavlja posebne zahteve za upravljanje incidentima bezbednosti informacija. Poglavlje 6.6 ovog standarda se bavi opštim upravljanjem bezbednosti informacija. U odnosu na ranije zahteve sada se eksplicitno, u tački 6.6.3 zahteva da organizacija:

- ima procedure za upravljanje incidentima koje moraju biti korišćene u upravljanju incidentima bezbednosti informacija
- mora da analizira tip, obim i posledice svakog incidenta bezbednosti informacija
- mora da zabeleži i preispita sve incidente da bi se identifikovale mogućnosti za unapređenje [3]

Ovi zahtevi u osnovi imaju širi kontekst po organizaciju, jer se odnose i na izveštvanje klijenata i mogućnost posrednog uticaja incidenata na procese i opšte poslovanje klijenta. Ovo je u potpunosti u skladu sa zahtevima standarda ISO/IEC 27001:2005. ISO je najavila da će u budućim izdanjima ova dva standarda biti sve više komplementarna, što će omogučiti, pored ostalog, njihovu laksu primenu i integraciju (u jedan sistem).

4. PRIMENA STANDARDA ISO/IEC 27035:2011, KAO PREPORUKA DOBRE PRAKSE

Detaljno upravljanje incidentima bezbednosti informacija, u seriji standarda ISO 27000, je definisano standardom ISO/IEC 27035:2011. Ovaj standard je zamenio standard ISO/IEC TR 18044:2004, ali je u osnovi preuzeo njegovu osnovnu strukturu.
Opšti prikaz upravlljanja informacijama dat je opštom šemom koja ima sve elemente klasičnog Demingovog PDCA ciklusa.
Na Slici 1. je prikazana opšta šema upravljanja incidentima prema standardu ISO/IEC 27035:201.

Ovaj standard nije obavezujući (sertifikacioni), ali daje veliki broj preporuka i smernica u cilju efikasnog i efektivnog upravljanja incidentima bezbednosti informacija. Svaki od elemenata ovog PDCA ciklusa je do detalja opisan u standardu uključujući i

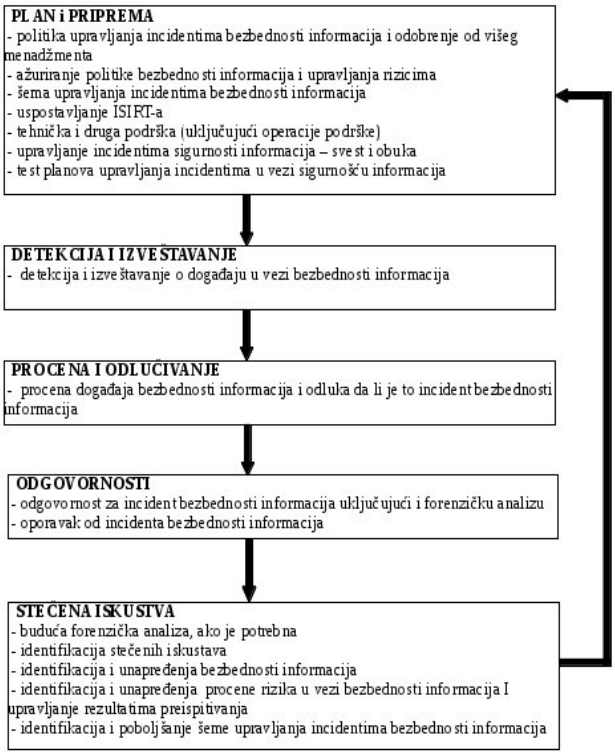
- razliku između događaja i incidenta u vezi sa bezbednošću informacija,
- potrebne resurse za upravljanje incidentima bezbednosti informacija,
- formiranje tima odgovornog za incidente bezbednosti informacija (engl. Information Security Incident Response Team - ISIRT),
- operativnu efikasnost i kvalitet,
- poverljivost,
- značajne operacije i
- odgovornosti i ovlašćenja.

Veliki značaj se posvećuje forenzičkoj analizi, koja mora doprineti da se otkrije stvarni uzrok incidenta u vezi bezbednosti informacija. Insistiranje na učenju na greškama i stečenim iskustvima se zasniva na formiranju baze podataka poznatih i/ili potencijalnih incidenata koja mora biti operativna i činiti osnovu za opis potrebnih mera koje imaju za cilj prevenciju pojave incidenata.

Standard ima nekoliko priloga (aneksa) koji treba da omoguće njegovu lakšu primenu. Tako su u prilogu B dati primeri incidenata bezbednosti informacija sa njihovim uzrocima.
U prilogu C su dati primeri kategorizacije i klasifikacije događaja i incidenata bezbednosti informacija koja uključuju analizu:

- finansijskih gubitaka,
- komercijalnih i ekonomskih interesa,
- ličnih informacija,
- zakonskih i drugih obaveza,
- upravljačkih i poslovnih operacija i
- gubitka ugleda [1]

Prilog D obuhvata primere obrazaca izveštaja o dogadjajima, incidentima i ranjivostima koje se odnose na bezbednost informacija, dok prilog E obuhvata zakonsku i drugu regulativu.
Ostaje na organizacijama da, u zavisnosti od svoje veličine i poslovnih funkcija, izvrše procenu kako primeniti ove zahteve koji u stvari predstvaljaju pravu dopunu i pomoć za funkcionisanje sistema menadžmenta bezbednosti informacija (engl. Information Security Management System - ISMS).



Slika 1. Šema upravljanja incidentima bezbednosti informacija prema standardu ISO/IEC 27035:201

5. KAKO SE UPRAVLJANJE INCIDENATA MOŽE PRIMENITI U PRAKSI ?

Velika dilema se postavlja pred organizaciju, u smislu kako i u kojoj meri primeniti zahteve standarda ISO/IEC 27035:2011, a da se pri tome ispuni osnovni cilj: ispuniti zahteve standarda ISO/IEC 27001:2005

Ovo se kod srednjih i malih preduzeća pre svega može odnositi na:

- ljudske resurse (koliko se ljudi može angažovati na ovim poslovima)
- obim analize incidenata (potrebni kriterijumi za analizu u odnosu na samu organizaciju)
- vrstu i obim forenzičke analize (kompetencija i potreba za specifičnim analizama)
- formiranje tima odgovornog za incidente bezbednosti informacija (eng. ISIRT – Information Security Response Team)

Preduzeće HDL Design House se upravo suočilo sa ovakvom vrstom dileme. Po svojoj veličini odgovara srednjim preduzećima (oko 50 zaposlenih), a pred sobom je postavila zadatak da sto je moguće kvalitetnije upravlja incidentima bezbednosti informacija.
Preduzeće je postavilo sledeće osnove za upravljanje incidentima:

- periodično se održava obuku zaposlenih u cilju prepoznavanja događaja i incidenata bezbednosti informacija i načina njihovog prijavljivanja
- svi zaposleni imaju obavezu prijavljivanja incidenata bezbednosti informacija u skladu sa svojim delokrugom rada i svojim ovlašćenjima
- imenovana je osoba koja ima zadatak da ove incidente ažurira i izvrši početnu bezbednosnu analizu
- održava prema potrebi hitne sastanke rukovodstva sa osobama zaduženim za otklanjanje posledica incidenata
- rukovodstvo analizira i preispituje incidente bezbednosti informacija, kako po određenim grupama tako i one koje imaju posebne uticaje na poslovanje preduzeća i donosi odluke o izmeni postojećih kontrolnih mera
- Mogući incidenti bezbednosti informacija sa velikim značajem po poslovanje su tretiraju na poseban način i opisani su u Planu kontinuiteta poslovanja

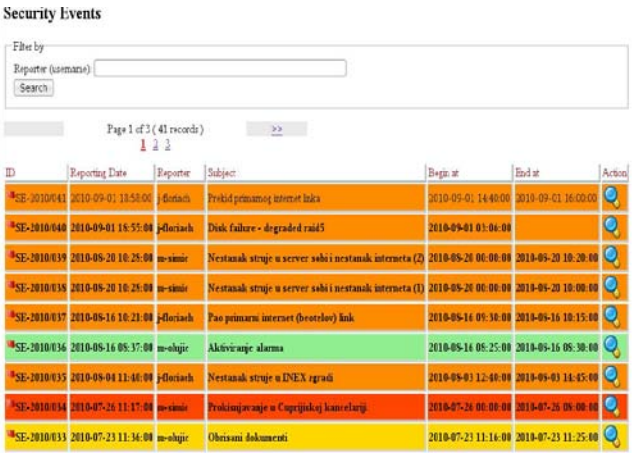
Prijavljivanje incidenata bezbednosti informacija se vrši u okviru softverskog alata PlumISMS, koji je razvijen kao podrška integrisanom sistemu QMS i ISMS. Svi obrasci u okviru ovog sofverskog alata za prijavu incidenata su rađeni u skladu sa preporukama standarda ISO/IEC 27035:2011. Na Slici 2. je prikazan je za prijavu incidenta bezbednost informacija u softverskom alatu Plum ISMS.

Slika 2. Obrazac za prijavu incidenata u softverskom alatu Plum ISMS

Ovaj izveštaj o incidentu se automatski (putem e-maila) prosleđuje osobi zaduženoj za prikupljanje i obradu incidenata, koja pokrece novu fazu, trenutno preduzimanje korektivnih i preventivnih akcija u vezi sa sa incidentom, a rukovodstvo verifikuje preduzete mere.
Preduzeće nije u mogucnosti da formalno formira ISIRT, zbog svoje operativnosti, ali je definisala odgovornosti za svaku pojedinačnu vrstu incidenata. Nekada (naročito u IT sektoru/odeljenju) izvestilac (reporter) o

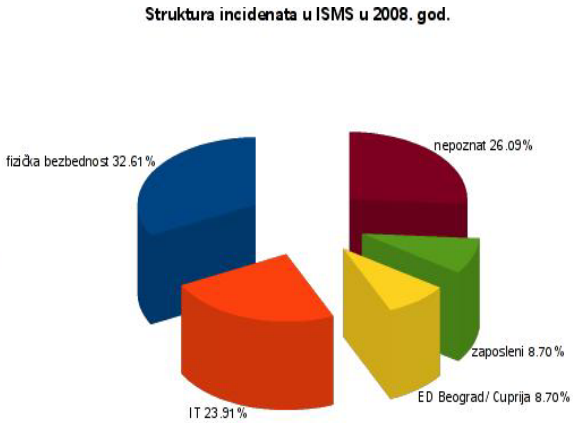
identifikovanom incidentu po prirodi posla odmah pristupa i njegovom otklanjanju, ali ga to ne oslobađa odgovornosti da incident prijavi i da se on naknadno analizira.

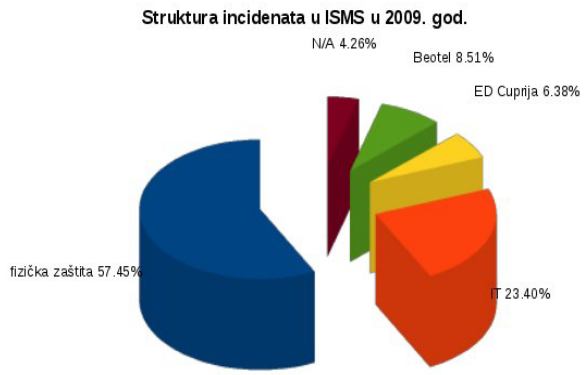
Za analizu i preispitivanje upravljanja incidentima se koriste zbirni izveštaji o incidentima bezbednosti informacija u okvitu softverskog alata Plum ISMS. Na Slici 3. je prikazan deo zbirnog izveštaja o prijavljenim događajima i incidentima bezbednosti informacija.

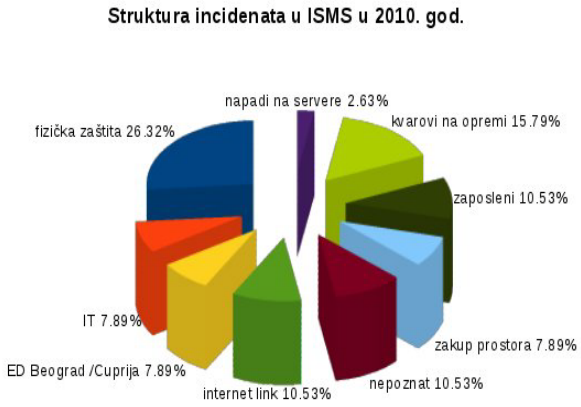


Slika 3. Deo zbirnog izveštaja o prijavljenim događajima i incidentima bezbednosti informacija

Ovi izveštaji su jedan od ulaznih elemenata u preispitivanju celokupnog ISMS od strane rukovodstva. Na Slici 5. su prikazani statistički podaci – uporedni pregled incidenata, po kategorijama, u preduzeću HDL Design House za period od 2008. do 2010. god.







Slika 2. Uporedni pregled incidenata, po kategorijama, u preduzeću HDL Design House za period od 2008. do 2010. god.

Periodično se radi statistička obrada podataka na osnovu izveštaja i radi analiza incidenata bezbednosti informacija koja može u početnom koraku da usmeri preventivno delovanje preduzeća na pojedine segmente bezbednosti informacija.

U toku preispitivanja ISMS od strane rukovodstva analizom je utvrđeno da se pojedine kategorije incidenata moraju detaljnije sagledati radi adekvatnijeg delovanja u slučaju ponovne pojave. Takođe se primećuje, tokom godina, smanjenje incidenata koji su za uzrok imali fizikču bezbednost, a uzrok tome je dodatna obuka zaposlenih. Uočava se i povećan broj tehničkih kvarova na opremi što je posledica povećanja broja servera i novog radnog okruženja.

Zbog bolje strukturne analize Plan kontinuiteta poslovanja je naknadno dopunjen i prilagođen realnim potrebama i mogućnostima preduzeća.

6. KOLIKO SE RAZLIKUJEMO OD SVETSKIH ISKUSTAVA ?

Svetska iskustva su takva da se može govoriti o specifičnim odstupanjima o incidentima bezbednosti informacija u Srbiji. Uopšteno, globalne statistike pokazuju da je za oko 80 % svih incidenata vezanih za sigurnost informacija odgovoran ljudski faktor [4], dok se samo na primeru HDL Design House uočava da je ovaj procenat manji. Razlog toga je nerazvijena informatička infrastruktura i opšta pouzdanost tehničkih sistema u

našem okruženju. Nestanci struje (nenajavljeni od strane vlasnika poslovnog prostora ili elekrodistribucije), prekid internet linkova, nabavka rezervnih delova za složene sisteme su čest uzrok pojave incidenata bezbednosti informacija.

7. ZAKLJUČAK

Upravljanje incidentima u okvirima ISMS-a je jedan od klučnih elemenata za njegovo efektivno funkcionisanje. Da bi upravljanje incidentima, koji se odnose na bezbednost informacija, bilo efikasno i ispunili zahtevi standarda ISO/IEC 27001:2005 neophodni za sertifikaciju sistema menadžmenta bezbenošću informacija treba primenjivati zahteve i preporuke standarda ISO/IEC 27035:2011.

Sva odstupanja od zahteva ovog standarda mogu biti uslovljena veličinom organizacije i njenom delatnošću. Identifikacija događaja i incidenatabezbednosti informacija i njihova analiza, kao i stalno preispitivanje postojećih postupaka i procedura za upravljanje incidentima bezbednosti informacija u velikoj meri će sprečiti ponavljanje nekih i minimiziranje posledica pojave novih incidenata.

LITERATURA:

[51] [1] ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management

[52] [2] ISO/IEC 27001:2005 Information technology - Security techniques – Information security management systems – Requirements

[53] [3] ISO/IEC 20000-1:2011 Information technology – Service management – Part 1 : Specification

[54] [4] http://www.kvalis.com/

CIP - Katalogizacija u publikaciji
Narodna biblioteka Srbije, Beograd

007:004.056(082)

FORUM BISEC (4, 2012 ; Beograd)

Zbornik radova sa nacionalne konferencije Forum BISEC 2012 : (takođe) IIII konferencija o bezbednosti informacija, Beograd 27. jun 2012. / (Urednik Nedžad Mehić). -Beograd : Univerzitet Metropolitan, 2012.

Radovi na srp. i engl. jeziku. - Tekst štampan dvostubačno. Tiraž 100. - Bibliografija uz svaki rad. - Abstracts.

ISBN 978-86-912685-6-5

a) Informacije - Zaštita - Zbornici
COBISS.SR-ID 184560396