FBIM TRANSACTIONS
DOI 10.12709/fbim.02.02.01.05

INTERNET SIGURNOST MSP SA ASPEKTA SIGURNOSTI ELEKTRONSKE POŠTE

INTERNET SAFETY OF SME REGARDING THE SECURITY OF ELECTRONIC MAIL

Zoran Čekerevac
Business School „Čačak“ & „Union“ University - Faculty of Business and Industrial Management, Belgrade, Serbia

Petar Čekerevac
Libek, Belgrade, Serbia

Jelena Vasiljević
„Union“ University - Faculty of Business and Industrial Management, Belgrade, Serbia

JEL Category: **K18**

Apstrakt

U savremenom poslovanju korišćenje elektronske pošte je praktično neizbežno. Najveći deo bitnih podataka jedne organizacije na ovaj ili onaj način biva prenošen elektronskom poštom, bilo kao prilog, bilo kao deo sadržaja poruke. Samim tim razumljiva je briga poslovnih subjekata o zaštiti informacija koje se prosleđuju elektronskom poštom. Pri tome pri organizaciji zaštite veličina organizacije nije toliko bitna, problemi su veoma slični. Ipak se mora napomenuti da velikim organizacijama na raspolaganju stoje i veći resursi, ali su te organizacije i interesantnije napadačima i izloženije napadima. Međutim, razvojem informacionih tehnologija pojavio se i „višak“ kapaciteta sistema za prisluškivanje, tako da se u poslednje vreme nadgledanje elektronske pošte praktično spustilo i na pojedinačne korisnike. U prvom delu rada je analizirana bezbednost elektronske pošte i elektronskih komunikacija u svetlu afere nastale objavljivanjem tajnih podataka o nadgledanju elektronskih komunikacija u časopisu TheGuardian i na veb sajtu kao i u izjavama Edvarda Snoudena (Edward Snowden). U drugom, obimnijem, delu rada govori se o organizaciji prenosa elektronske pošte, kao i o kritičnim mestima u lancu prenosa poruke na kojima poruka može da bude napadnuta, da se izgubi ili da „samo“ zakasni. Takođe, razmotrene su i mogućnosti zaštite elektronske pošte

The address of the corresponding author:
Zoran Čekerevac
zoran@cekerevac.eu

šifrovanjem u varijantama „s kraja na kraj“, server – server i klijent – server. Razmotreni su i rizici čuvanja pošte kod druge ili treće strane. Na kraju rada su razmotreni pravni aspekti, raspoloživa zakonska regulativa i zaštita elektronskih poruka primenom elektronskog potpisa i javnog i tajnog ključa za šifrovanje. U okviru zaključka izloženo je da se na osnovu izloženog može zaključiti da praktično ne postoji tehnologija koja obezbeđuje apsolutnu zaštitu poruke i da nije dovoljno samo zaštiti važnu poruku za vreme njenog putovanja kiber prostorom, već je treba štititi od njenog nastajanja do njenog čitanja i arhiviranja. Takođe, ne treba očekivati da će se stanje bezbednosti pošte poboljšavati primenom zakonske regulative.

Ključne reči: *elektronska pošta, imejl, Internet, sigurnost, zaštita, bezbednost, server, klijent, elektronski potpis, digitalni potpis, enkripcija, šifrovanje, javni ključ, tajni ključ, Prizma, Tempora, praćenje, MSP*

Abstract

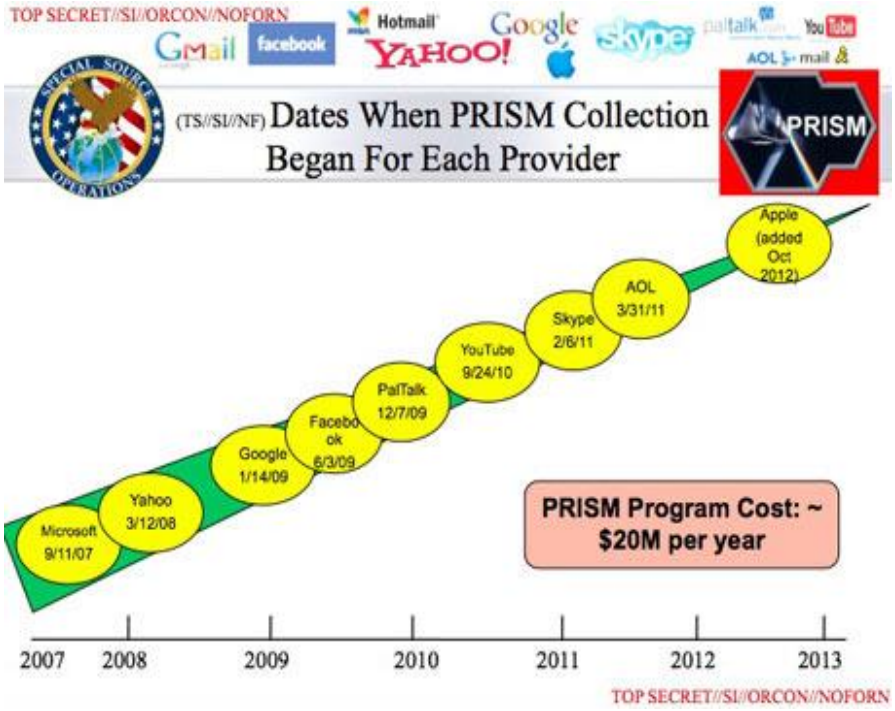
In today's business, use of electronic mail is practically inevitable. Most of the relevant information of an organization in one way or another is transmitted by e-mail, either as an attachment or as a part of the message content. Therefore businesses care about protection of information sent by e-mail. In doing so, the organization of protection doesn't depend much on the size of a company or an organization, the problems are very similar. Here must be noted that large organizations have at their disposal more resources, but also that such organizations are more interesting and more vulnerable to attacks. However, the development of information technology has provided even the "excess" capacities of eavesdropping systems, so lately email monitoring is practically brought down to individual users. In the first part of the paper security of electronic mail and electronic communication is analyzed in the light of the scandal caused by Edward Snowden's publishing of classified information about the monitoring of electronic communications in The Guardian journal and on his Web site as well as in his statements. In the second, more voluminous part the article, the organization of e-mail transmission, as well as the critical points in the chain of transmission of messages where the message can be attacked, lost, or "only" late are analyzed. Also, here are presented some options for e-mail encryption protection in variants: "end-to-end", server - server, and client - server. Certain consideration is given to risks of storing mails at second or third hand. At the end of the article, there are discussed some legal aspects, the available legislation and protection of electronic messages using electronic signatures and public and private keys for encryption. In the conclusion, it is stated that based on the previous analyses it can be concluded that there is virtually no technology that ensures absolute protection of messages and that it is not enough to protect an important message during its trip through cyber space and that the message should be protected from its creation to its reading and archiving. Also, it is not to be expected that the situation with mail security will be improved with new legislation. Hunger for data explodes.

Keywords: *electronic mail, email, Internet, safety, protection, security, server, client, electronic signature, digital signature, encryption, public key, secret key, Prism, Tempora, surveillance, SME*

1 UVOD

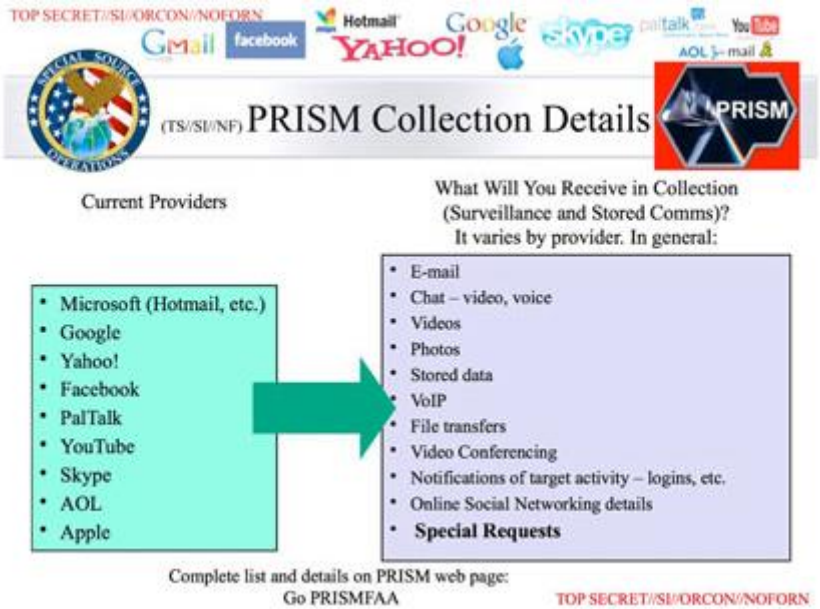
Nema sumnje da savremeno poslovanje zavisi od elektronske pošte. Štaviše, savremeno poslovanje se praktično ne može realizovati bez elektronske pošte. Prema rezultatima Osterman Research (Symantec, 2013), 74% intelektualne svojine organizacija boravi u elektronskoj pošti ili kao tekst ili kao prilog. Polovinom 2013. godine naglo se digla bura oko bezbednosti elektronske pošte i podataka koji cirkulišu elektronskom poštom. Iako se veruje da je primenom desktop računara, gejtveja i enkripcije prenos elektronske pošte bezbedan čak i u oblaku, Edward Snowden (Snowden, 2013) je pokazao da to i nije slučaj, da se elektronska pošta, i ne samo ona, aktivno prati i prisluškuje. Na osnovu The Guardian serijala „O bezbednosti i slobodi“ (Greenwald & MacAskill, 2013) Agencija za nacionalnu bezbednost (NSA) ima direktan pristup sistemima Google, Facebook, Apple i drugih američkih Internet giganata. U strogo poverljivom dokumentu čiji su sadržaj autori objavili, NSA pristup je deo ranije neobjavljenog programa pod

nazivom Prizma, koji omogućava službama da prikupljaju materijal uključujući istorije pretraživanja, sadržaj e-pošte, prenošenje datoteka i razgovora uživo. Dokument tvrdi da se podaci prikupljaju direktno sa servera glavnih američkih provajdera Internet usluga. Zakonska osnova za prikupljanje podataka leži u Patriotskom zakonu (USA Patriot Act, 2001).



Apple	oktobar 2012.
AOL	31.03.2011.
Skype	06.02.2011.
YouTube	24.09.2010.
PalTalk	07.12.2009.
Facebook	03.06.2009.
Google	14.01.2009.
Yahoo	12.03.2008.
Microsoft	11.09.2007.

Slika 1. Datumi kada je prikupljanje podataka po Prizma programu otpočelo kod navedenih provajdera (Izvor: (Greenwald & MacAskill, 2013))



Slika 2 Detalji prikupljanja podataka po projektu Prizma (Izvor: (Greenwald & MacAskill, 2013))

Prema dokumentima koje je objavio The Guardian (Greenwald & MacAskill, 2013), nisu svi provajderi usluga počeli istovremeno da pružaju informacije NSA, a ni u istom obimu. Na

slici 1 prikazani su počeci saradnje pojedinih provajdera sa NSA. Kompanije su zakonom obavezane da se povinuju američkim zakonima, ali je program Prizma omogućio obaveštajnim službama da imaju i direktan pristup serverima provajderima komunikacionih usluga. Na osnovu navedenog dokumenta vidi se da su američki provajderi pružali podršku operacijama.

Grafikon pripremljen od strane NSA, sadržan u strogo poverljivom dokumentu koji je The Guardijan dobio, naglašava širinu podataka koje je NSA u stanju da dobije: e-mail, video i audio ćaskanje, video snimci, fotografije, voice-over-IP (Skype, na primer) ćaskanja, prenošenje datoteka, detalji sa društvenih mreža i još mnogo toga, kao što je prikazano na slici 2.

Iako namenjen zaštiti od terorizma, Patriotski zakon je korišćen (i koristi se) u svrhu prikupljanja najrazličitijih podataka. Po amandmanu iz 2008 godine program Prizma se primenjuje na sve komunikacije u kojima je bar jedan od učesnika stranac. Dokument takođe pokazuje da FBI deluje kao posrednik između drugih agencija i tehnoloških kompanija, i naglašava njegovo oslanjanje na učešće američkih internet firmi, tvrdeći da "pristup 100% zavisi od ISP privilegija". O značaju projekta Prizma govori činjenica da je njegov godišnji budžet 20 miliona USD i da on predstavlja „jedan od najvrednijih, jedinstven i produktivan pristup NSA“. (Greenwald & MacAskill, 2013). Prema tvrđenjima visokih zvaničnika program Prizma se ne odnosi na Amerikance i one koji se nalaze na teritoriji SAD, da je program pokriven brojnim procedurama koje minimiziraju sticanje, zadržavanje i slanje uzgred stečenih informacija o američkim licima. Ta i takve izjave mogu da deluju umirujuće za američke državljane, ali su izazvale burne reakcije u svetu, pre svega u Evropi. Pokrajinski ministar pravosuđa u Hesenu Joerg-Uwe Hahn predložio je uvođenje novog krivičnog dela: pronevera ličnih podataka. (Jungholt, 2013). Međutim, iako se sva pažnja skoncentrisala na prisluškivanja i prikupljanje podataka od strane američkih kompanija i obaveštajnih službi, postoje dokazi da su i nemačke kompanije sarađivale sa obaveštajnim službama SAD, ali i sa drugim obaveštajnim službama. U svojoj izjavi Savezni poverenik za zaštitu podataka Peter Schar je poimence naveo „Vodafon Deutschland“ i „Deutsche Telekom“. (Jungholt, 2013) Marc Kessler je u svom članku objavio da dve trećine nemačkih korisnika smatra da njihovi podaci na Internetu nisu sigurni i to 39% smatra da su podaci „više nebezbedni nego bezbedni“, 27% smatra da su njihovi podaci „potpuno nebezbedni“, a samo 2% smatra da su im podaci „potpuno bezbedni“. Prema istraživanjima iz 2011. godine, ti procenti su bili 43%, 12% i 11% respektivno. (Kessler, 2013) Može se zapaziti da je praktično 15% onih koji su smatrali da su im podaci prilično nebezbedni prešlo u grupu koja smatra da su im podaci potpuno nebezbedni, kao i da se drastično smanjio broj onih koji veruju u potpunu bezbednost podataka na Internetu. Značajan doprinos ovoj promeni shvatanja je dao Edward Snowden objavljivanjem informacija o prisluškivanju početkom juna 2013. Kasnije je objavljeno da je Velika Britanija uspostavila svoj program monitoringa („Tempora“) koji treba i da nadmaši projekat Prizma. Ovaj projekat je još veći razlog za zabrinutost kako zbog svoje veličine, tako i zbog činjenice da je Britanija glavni centar za Internet saobraćaj, kao što se može videti na slici 3 (pozicija 1).

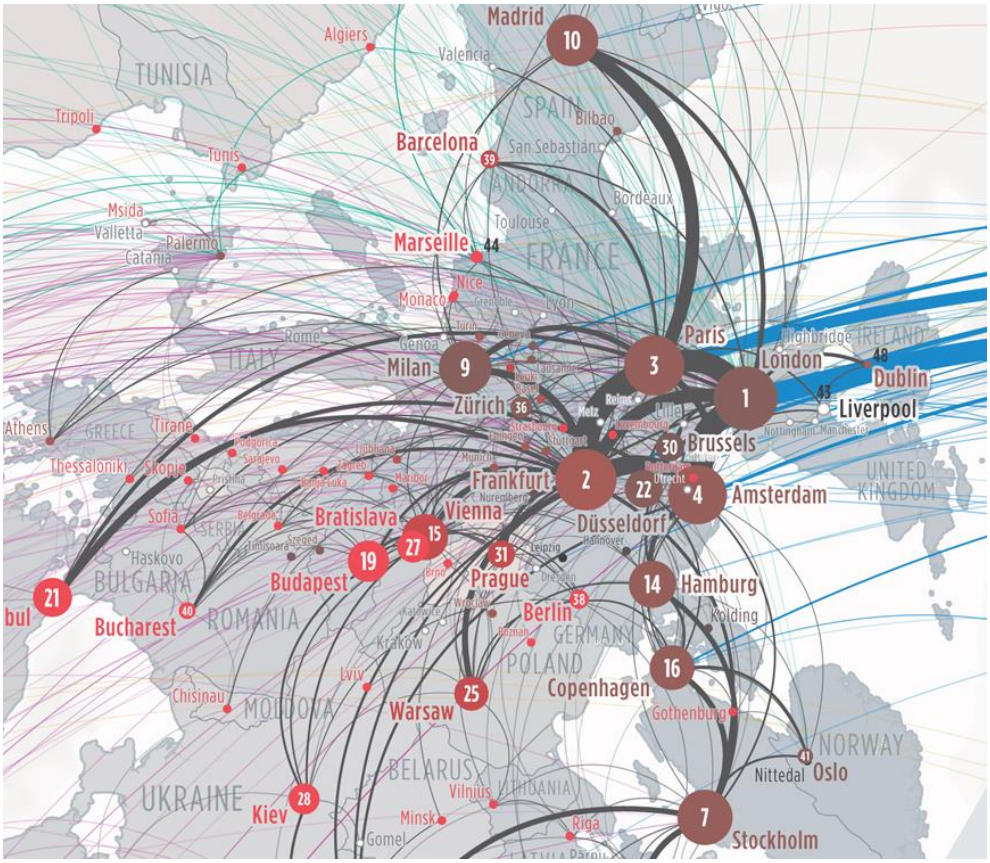
Prema izveštaju časopisa The Guardian, projekat Tempora nije još završen, što znači da se u ovom trenutku ne prati celokupan Internet saobraćaj kroz Veliku Britaniju.

"Od prošle godine, Agencija je stigla na pola puta, priključivši se na 200 fiber-optičkih kablova od kojih svaki ima kapacitet od 10 gigabita u sekundi. Teoretski, GCHK ima pristup protoku od 21,6 petabajta dnevno, što je ekvivalentno 192 zbirki svih knjiga Britanske biblioteke. " (Wheatley, 2013)

Kao rezultat ataka na privatnost korisnika Interneta pojavili su se i aktivisti i udruženja koja se bore za zaštitu privatnosti. Tako je grupa koja sebe naziva „Safari korisnici protiv Guglovog tajnog praćenja“ pokrenula tužbu protiv najvećeg Internet pretraživača Google kog optužuju da je bez njihove volje instalirao „kolačiće“ za praćenje u njihove iPhone i iPad uređaje. Google se trudi na sve načine da izbegne sudski proces van teritorije SAD. Zbog tih kolačića, Google je juna 2012. godine već platio rekordnu kaznu od 22,5 miliona USD nakon što je američka Federalna trgovinska komisija utvrdila da su kolačići za

praćenje bili upotrebljeni nad milionima američkih potrošača. (Charles, 2013)

Nema sumnje da Prizma i Tempora nisu jedini projekti ove vrste u svetu i da ima mnogo sličnih projekata. Takođe, ima mnogo onih koji su zabrinuti za to kuda idu Internet i komunikacione tehnologije. Sigurno je da ima mnogo onih koji opravdavaju preduzete mere špijunaže i da će biti i mnogo dezinformacija u cilju opravdavanja tih mera, pa čak i represivnih mera prozvanih državnih aparata, kao što je bio slučaj uništavanja opreme lista the Guardian 18. avgusta 2013. (Rusbridger, 2013) Međutim, cilj ovog rada nije opredeljivanje za to da li treba ili ne treba dozvoliti prisluškivanje elektronske pošte. Ovaj članak polazi od činjenice da se elektronska pošta prisluškuje i on će se nadalje baviti tehnologijom, time kako se proces prenosa elektronske pošte odvija i, pre svega, time gde i na koji način proces i privatnost mogu da budu ugroženi.



Slika 3 Globalna mapa Interneta za 2012. godinu (Izvor: modifikovana mapa (TeleGeography, 2013))

2 KAKO SE PORUKA PRENOSI I KAKO MOŽE DA ZAKASNI ILI DA SE IZGUBI

Prva kritična tačka u prenosu poruka je mesto nastanka same poruke, npr. PC. Upad u sistem može da bude ostvaren i na nivou softvera i na nivou hardvera. Nedavno je Internet preplavljen informacijom da je kineskom gigantu Lenovo zabranjeno da proda komplete mreža različitim agencijama tzv. Five Eyes alijanse (UK, SAD, Kanada, Novi Zeland i Australija), jer su pri testiranju opreme pronađena slabe tačke kroz koje je moguće daljinski ući u sistem bez znanja korisnika. (Muncaster, 2013) O špijuniranju Windowsa i njegovim „zadnjim vratima“ („back door“) na Google pretraživaču ima više od 80 miliona dokumenata (05.08.2013.) I dok je kod ovih napada potrebno da korisnik bude interesantan napadaču, u slučajevima primene onlajn softvera (besplatnog ili sa pretplatom) korisnik sam svesno ili nesvesno deli svoje podatke direktno sa ponuđačem softvera. Malo je verovatno da ponuđač softvera neće napraviti kopiju dokumenta ili da ga neće pregledati pri njegovoj izradi.

Kada je jednom poruka napisana i kada su prilozi kompletirani, treba poslati imejl. Za slanje poruke mogu se koristiti web-mail onlajn servisi (Gmail, Hotmail, Yahoo itd.) ili posebne softverske aplikacije, posebni klijentski programi za e-poštu, tzv. MUA – mejl korisnički agenti (Thunderbird, Microsoft Outlook, Apple Mail itd.). Mnogi Internet provajderi pružaju i uslugu web-maila, pri čemu se najčešće nude specijalizovani programi kao npr: SquirrelMail, RoundCube, BlueMamba i drugi. Osnovna prednost web-maila je to što se celokupna pošta može držati na serveru provajdera i desetak godina, ali tu je i nedostatak, jer je celokupna korespodencija izložena monitoringu u bilo kom trenutku. Iako je web-mail prvenstveno namenjen online pristupu, neki provajderi omogućavaju i pristup MUA primenom SMTP/POP3/IMAP protokola. Na taj način se pošta može preuzeti i skloniti sa servera provajdera. U slučaju korišćenja POP3 imejl servisa poruke se po prijemu prebacuju na računar primaoca i brišu sa servera što je dobro sa aspekta bezbednosti, ali je nepovoljno u slučaju kada jedan korisnik koristi više različitih računara. Alternativa su i IMAP imejl serveri koji korisniku pokazuju zaglavlje poruke, pošiljaoca i predmet poruke, a preuzimanje same poruke se radi na poseban zahtev korisnika.

Sama tehnologija slanja i prijema elektronske pošte je detaljno opisana u brojnoj literaturi (Wikipedia, 2013), (Čekerevac, 2012), (Čekerevac, 2009, p. 44), (Schindler, 2008), (Vicomsoft, 2012) tako da ovde neće biti posebno opisivana, ali treba napomenuti da pri slanju mejla, imejl klijent pronalazi meil server primaoca koristeći Domain Name System (DNS) i kontaktira ga primenom Simple Mail Transfer Protocol-a (SMTP). Kada se jednom uspostavi veza, počinje primopredaja poruke. Iako izgleda sasvim jednostavno, mora se napomenuti da na putu od pošiljaoca do primaoca svaki imejl prođe dug put, nekoliko mejl servera. Na tom svom putu poruka je izložena i brojnim proverama i brojnim iskušenjima. Posebno su ugrožene poruke koje preduzeće šalje na adrese svojih brojnih klijenata. U cilju borbe protiv spem poruka (85% pa i više od svih imejl poruka čine spem poruke (Schindler, 2007)) većina mejl servera svaku poruku propušta kroz niz filtera pre nego što uopšte prihvati podatke, pre nego što je zabeleži i prosledi primaocu. Jedan od kriterijuma je i broj poruka koji stiže sa jednog domena. Vrlo često je ta granica postavljena na 250 poruka sa jednog domena na sat, pa ako preduzeće treba da dostavi veći broj poruka mora da računa ili sa gubitkom vremena ili sa otvaranjem naloga na različitim serverima.

Pri prijemu pošte server proverava reputaciju servera pošiljaoca, pa u slučaju da je server pošiljaoca „na lošem glasu“, dešava se da server odbije prijem poruke ili, u najboljem slučaju, da poruku proglasi za spem i smesti u spem folder. Tako se može desiti da vrlo važna očekivana poruka završi u spem folderu i da posle izvesnog vremena bude izbrisana i bez znanja primaoca i pošiljaoca.

Svima je poznato da je Internet najčešće brz, veoma brz, da su mejl serveri veoma brzi, ali dešava se da kada su uobičajene brze rute i serveri zagušeni, ili u rekonstrukciji, da poruke moraju da se rerutiraju i da čekaju u redu za slanje satima. Kretanje poruke po Internetu je nevidljivo i pošiljaocu i primaocu poruke, a svaki čvor kroz koji poruka prolazi podrazumeva aktivnosti „sačuvaj i prosledi“. Što je više rerutiranja, to se poruka zadržava na više servera i postaje podložnija monitoringu, uz povećanje šanse da poruka putuje duže, pa da se čak i izgubi.

Mogućnosti da je poruka spem ili da je inficirana virusima i trojanskim konjima, da masovno slanje dugih poruka izazove zagušenje linija i servera, stimulišu administratore da postavljaju odgovarajuće zamke za nepoželjnu poštu. Ne postoji savršen filter za spem, ali zato svaki gejtvej troši vreme i usporava saobraćaj slično naplatnim rampama na autoputevima. Savremeni mejl serveri zbog optimizacije svog rada skoro uvek postavljaju i vremenska ograničenja, pa je moguće da zbog minornih faktora poruka bude ugrožena, pa čak i neprosleđena.

Poseban problem se javlja ako i-mejl klijent i i-mejl server nisu usklađeni sa pravilima za slanje elektronske pošte. U takvim situacijama primaočev i-mejl server vrlo često odbija da prihvati poruku, poruka kasni zbog uzastopnih odbijanja prijema, a neretko se i izgubi. Mali broj servera obaveštava pošiljaoca o odbijanju poruke, što pošiljaoca može da navede na zaključak da je poruka poslata i preuzeta.

U cilju zaštite podataka korisnik može da koristi SSL (Secure Sockets Layer) što bi trebalo da obezbedi komunikacionu sigurnost na Internetu. U tu svrhu postoji i niz sofverskih rešenja koja šifruju poruku i prosleđuju je „od vrata do vrata“, ali takve poruke ne prolaze kroz programe za zaštitu od virusa, pa se može dogoditi da sa porukom dođe i neželjeni pratilac. O prijemu takve poruke antivirusna zaštita obaveštava primaoca i na njemu je da odluči da li će poruku otvoriti ili ne.

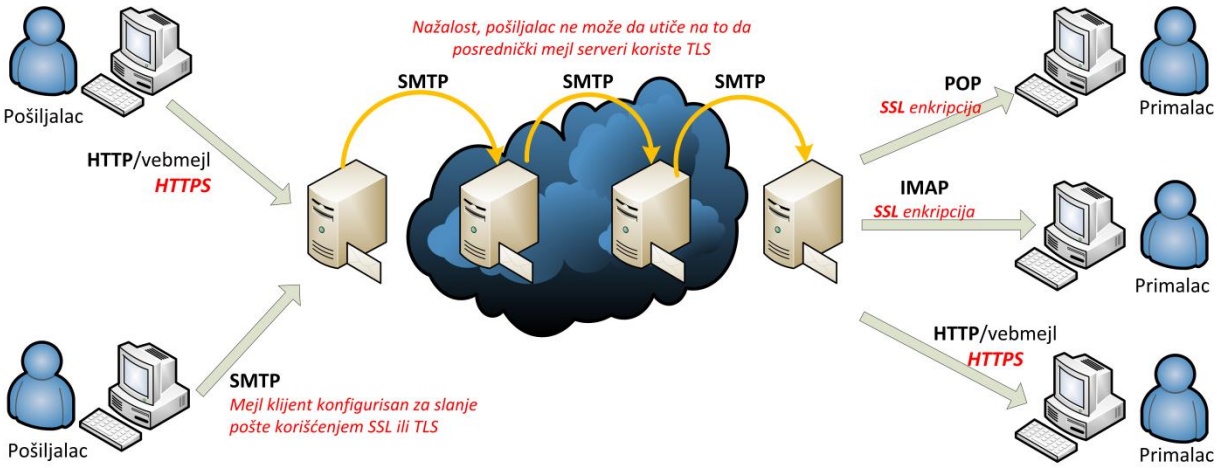
3 ZAŠTITA ELEKTRONSKE POŠTE ŠIFROVANJEM

Šifrovanje elektronske pošte danas, još uvek, nije široko rasprostranjeno. Većina imejl poruka neke tipične organizacije i dalje se šalje u obliku čistog teksta što omogućava da poruke budu lako presretnute. U 2013-oj godini manje od jedne polovine, 44% organizacija omogućava korisnicima manuelnu enkripciju, a nešto više od jedne trećine, 35% organizacija ima mogućnost da u zavisnosti od sadržaja poruke i vrste podataka poruku šifruje. Situacija je bila još nepovoljnija u prethodnoj godini kada su odgovarajući procenti bili 40 i 27. (Osterman Research, 2013)

Da bi se obezbedio šifrovani prenos podataka između korisnika i Internet servis provajdera (ISP) potrebno je podesiti Secure Socket Layer (SSL) i Transport Layer Security (TLS) enkripciju. SSL konekcija se može aktivirati na veb pretraživaču ili na imejl programu. Poruke se mogu (i trebaju) šifrovati pri prenosu, ali da bi to bilo moguće, potrebno je da to bude urađeno i kod pošiljaoca i kod primaoca.

Za šifrovanje imejl poruka mogu da se koriste funkcije ugrađene u uslugu e-pošte, ili može da se preuzme softver za šifrovanje ili klijent dodaci (kao što su oni koji koriste OpenPGP (Constantin, 2011)). U slučaju nužde, mogu se koristiti Veb-bazirani servisi za šifrovanje e-pošte kao Sendinc ili JumbleMe, mada taj način primorava korisnika da veruje trećoj strani, određenoj kompaniji. (Geier, 2012)

Na slici 4 prikazana je ilustracija opšteg slučaja kretanja elektronske pošte od računara pošiljaoca do računara primaoca, kao i protokoli koji se koriste u određenim fazama. Crvenom bojom (*italik*) su naznačeni mogući tipovi enkripcije u pojedinim fazama. Za šifrovani prenos pošte potrebno je da mejl server pošiljaoca podržava SMTP preko TLS. Kao što se na slici 4 može videti, iako je sve učinio da poveća bezbednost, pošiljalac ne može da utiče na trasu i na način rada posredničkih mejl servera.



Slika 4 Ilustracija tipičnog prenosa elektronske pošte od pošiljaoca do primaoca u varijantama bez kriptovanja (crna boja) i sa kriptovanjem (crvena boja) (izvor: autori na osnovu *(Anon, Email, 2013)*)

Najčešći oblici enkripcije podataka, uključujući S/MIME (Secure/Multipurpose Internet Mail Extensions) i OpenPGP, podrazumevaju instalisanje bezbednosnog sertifikata na korisnički računar primaoca poruke i davanje pošiljaocu poruke niza karaktera, javnog ključa. Mnogi imejl klijenti, kao i dodaci za veb pretraživače podržavaju S/MIME standard.

Moguće je kupiti i kompletna softverska rešenja za potpuno šifrovano prenošenje poruka od pošiljaoca do primaoca.

U slučaju korišćenja prenosnih uređaja, tableta, notbukova, telefona i drugih mobilnih uređaja, za zaštitu elektronske pošte pogodno je koristiti šifrovanje preuzete pošte, ali je još preporučljivije kriptovati ceo uređaj i sve podatke kako bi ostali zaštićeni i u slučaju gubitka uređaja. Uz kriptovanje poruka treba i definisati odgovarajuću politiku brisanja podataka, kako bi se racionalno koristili raspoloživi resursi.

3.1 S kraja na kraj (end-to-end) enkripcija

Šifrovanje e-pošte s kraja na kraj, tj. od pošiljaoca do primaoca, je uvek bilo teško, iako su sredstva za postizanje ove vrste enkripcija sve bolja i lakša za korišćenje. Pretty Good Privaci (PGP) i njegov rođak besplatna verzija GNU Privacy Guard (GnuPG) danas su standardni alati za ovu svrhu. Oba ova programa mogu da obezbede zaštitu imejla u tranzitu, a takođe štite i sačuvane podatke. Glavni imejl klijenti, kao što su Mozilla Thunderbird i Microsoft Outlook mogu da se konfigurišu tako da nesmetano rade sa softverom za šifrovanje i omogućavaju pošiljaocu da jednim klikom potpiše, potvrdi, šifruje i dešifruje imejl poruke.

Iako naizgled jednostavno, korišćenje GnuPG i/ili PGP podrazumeva da i pošiljalac i primalac koriste isti softver, što je sada redak slučaj. Ako jedna od strana ne podržava GnuPG/PGP nema ni šifrovanog prenosa poruke s kraja na kraj.

Drugi preduslov je da pošiljalac mora da poseduje i verifikuje javne ključeve primalaca kojima se poruka namenjena. Tu je bitno i da pošiljalac poruke ne upadne u zamku poznatu po imenu „čovek u sredini“ (eng. „man in the middle“) kojom prisluškivači mogu da navedu pošiljaoca da koristi pogrešni javni ključ. Čovek u sredini napad se obično bazira na znatiželji, lakovernosti ili nepažnji korisnika koji svoje podatke čini dostupnim napadaču, kao što je objašnjeno u radu Srđana Nikića (2010) ili npr. u prikazu Margaret Rouse (2007) ili detaljnije u (Admin, 2011).

U svakom slučaju, podešavanje imejl klijenta za kriptovani rad, pre početka korišćenja, zahteva dosta strpljenja.

3.2 Server – server enkripcija

Kad jednom poruka napusti server pošiljaoca, ona kreće pre polaska na put nepoznatim rutama. Pri tom putovanju najčešće prolazi preko nekoliko servera. Lista servera preko kojih je stigla poruka pojavljuje se u zaglavlju poruke i moguće ju je videti koristeći odgovarajuću opciju mejl klijenta, npr. kod imejl klijenta Thunderbird: <Other Actions> → <Viev Source>.

Deo zaglavlja jednog imejla prikazan je na slici 5. U zaokruženom delu se vidi da je prvi server podržavao kriptovani prenos podataka preko sigurnih veza (ESMTPS i TLS). U pravougaonom uokvirenom delu se vidi da server podržava ESMTP protokol, ali ne i TLS/SSL.

```
Received: from hermes2.der.ac.uk ([128.231.238.2]:40426)
      by cocha3004.cochahost.com with esmtps (TLSv1:DHE-RSA-AES256-
 SHA:256)
      (Exim 4.80.1)
      id 1P65M8-002T20-2F
      for este@este.com; Sun, 04 Aug 2013 16:57:51 -0400
Received: from CISVIRHUB02.mds.ad.der.ac.uk (cisvirhub08.der.ac.uk
 [10.234.250.42])
      by hermes2.der.ac.uk (8.14.4/8.14.4) with ESMTP id r75RvRWB009044
      for <este@este.com>; Sun, 4 Aug 2013 21:57:31 +0100
```

Slika 5 Deo zaglavlja jedne poruke (modifikovan)

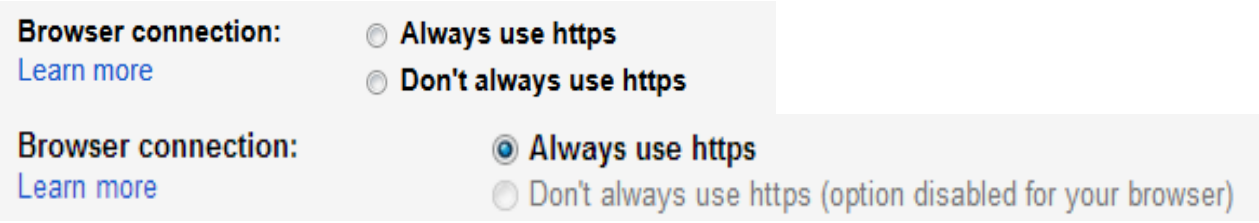
U svakom slučaju, da bi organizacija uopšte mogla da ima šansu da pošalje kriptovanu poruku, potrebno je da njen mejl server podržava TSL enkripciju u komunikaciji sa drugim serverima.

3.3 Klijent – mejl server enkripcija

Za bezbednost poruke bitna je i faza prenosa poruke sa korisnikovog računara na mejl servera i obrnuto, sa servera na korisnikov računar. I u

ovoj fazi treba koristiti kriptovani IMAP ili POP. U slučaju kada korisnik koristi vebmejl usluge potrebno je da obezbedi da njegov vebmejl nalog uvek koristii HTTPS.

Mnogi vebmejl provajderi koriste HTTPS samo pri prijavljivanju, a potom prelaze na brži HTTP, što smanjuje bezbednost poruke. U Gmail-u u podešavanjima (Settings) u listiću „General" postoji opcija kojom se može izabrati stalna ili povremena upotreba HTTPS (Slika 6 gornji deo). Ukoliko je veb pretraživač već podešen za stalnu upotrebu HTTPS, opcija povremene upotrebe HTTPS je isključena (Slika 6 donji deo).



Slika 6 Opcije primene HTTPS u Gmail-u za različite veb pretraživače
(izvor: Autori na osnovu https://mail.google.com/mail/?tab=....settings/general)

3.4 Čuvanje pošte kod drugog ili kod treće strane

Najveći broj korisnika elektronske pošte čuva sve primljene i poslate poruke. To istovremeno znači da se svaka poruka, ma koliko poverljiva bila i ma kako zaštićivana bila nalazi bar na još jednom mestu koje treba štititi. Vrlo je verovatno da se neka kopija poruke nalazi i kod ISP primaoca. Pored toga kopije se mogu naći i kod osoba ili organizacija koje rade bekap računara koji krisnik koristi. Tako, da bi se zaštitio sadržaj poruke od neželjenih očiju, jedno od rešenja može da bude primena PGP, mada, ukoliko se radi o vrlo važnim porukama, ni to nije garancija, jer je moguće da primalac poruke bude izložen pritisku (pravnom ili nekom drugom) da poruku dešifruje i da je nekom preda (kao što je izloženo u poglavlju 1). Za vrlo važne poruke treba razmotriti i mogućnost slanja poruke na neki drugi način.

Ako pošiljalac nema sopstveni mejl server, onda je sigurno da mora da koristi mejl server trećeg lica koje može da bude ili ISP, ili poslodavac, ili vebmejl provajder. To znači da će treće lice obezbeđivati (vrlo verovatno i čuvati) svu elektronsku poštu klijenta, a podrazumeva se da će poruke elektronske pošte biti rasute po računarima i memorijskim kapacitetima tog trećeg lica. Tako, pored rizika otkrivanja poruke na lokaciji primaoca poruke, javlja se i niz rizika na lokaciji trećeg lica. Jedan od načina za smanjivanje ovog rizika je da se poverljiva pošta briše sa lokacije provajdera. Ovo je podrazumevano kod POP, ali kod korišćena IMAP ili vebmejla moraju da se preduzimaju posebne akcije. Međutim, čak i kada serveri dobiju naredbu za brisanje poruke i kad poruka ne bude vidljiva korisniku, ne znači da će poruka tog trenutka nestati. Ona se na računarima provajdera zadržava još danima i nedeljama. Ukoliko je poruka šifrovana PGP/GnuPG njen sadržaj će biti nečitljiv na toj lokaciji, ali zato čitljivo ostaje zaglavlje koje sadrži podatke o adresi primaoca i predmet poruke (Anon, Email, 2013)

4 PRAVNI ASPEKTI ELEKTRONSKE POŠTE

Da bi se obezbedilo pravno valjano i bezbedno korišćenje elektronske pošte, potrebno je posedovati i pravnu regulativu. Pre svega, potrebno je korišćenje elektronskog odnosno kvalifikovanog elektronskog potpisa. Termin elektronski potpis je primenjen u legislativi Republike Srbije, ali mnogi autori smatraju da je adekvatniji termin digitalni potpis (digital signature). Korišćenjem elektronskog potpisa se obezbeđuje kriptovanje poruke, potvrda identiteta pošiljaoca i nepromenjenost (integritet) poruke. Korišćenjem kvalifikovanog elektronskog potpisa se postiže pravna valjanost identična svojeručnom potpisu, osim u slučajevima kada je zakonom propisano da pravna valjanost kvalifikovanog elektronskog potpisa nije jednaka svojeručnom potpisu. Uključivanjem vremenskog žiga se obezbeđuje podatak o trenutku nastanka (slanja) poruke, što je značajno u određenim situacijama.

Zakonom o elektronskom dokumentu (2009) definisani su elektronski dokument i njegova primena, a posebnim pravilnikom (Pravilnik o izdavanju vremenskog žiga, 2009) je utvrđeno izdavanje vremenskog žiga.

U Republici Srbiji su obezbeđeni svi preduslovi za primenu elektronskog potpisa. Slična situacija je i u zemljama regiona. Tako npr. u Hrvatskoj je 2006. godine stupio na snagu Zakon o elektroničkoj ispravi (Zakon HR, 2005). Zakon o elektronskom dokumentu Republike Srpske je usvojen 2008. godine, u Distriktu Brčko je usvojen Zakon o elektroničkoj ispravi 02.06.2010. (Zakon BD, 2010) itd. Drugi bitan zakon iz ove oblasti, Zakon o elektronskom potpisu, iako je u različitm zemljama nekoliko puta modifikovan, primenjuje se u Sloveniji od 2000, u Makedoniji od 2001, Hrvatskoj od 2002, u Crnoj Gori od 2003, a u BiH od 2006.

Na taj način su stvoreni uslovi da se elektronska pošta može koristiti ravnopravno sa do sada uobičajenim papirnim dokumentima.

Kada pošiljalac poruke primeni svoj elektronski potpis to ne garantuje da poruku ne može da pročita, u slučaju da do nje dođe, neko kome nije namenjena. U tom slučaju, primenom javnog ključa pošiljaoca poruka može biti pročitana. Da bi se ovo onemogućilo, potrebno je da pošiljalac poruku prvo potpiše svojim elektronskim potpisom a zatim primeni javni ključ primaoca. Tako samo primalac, kome je poruka upućena, na takvu poruku može primeniti svoj tajni ključ i tek onda primenom javnog ključa pošiljaoca doći do originalne poruke. Na taj način se postižu: bezbednost u smislu potvrde identiteta pošiljaoca, celovitost poruke i pravi primalac. Kao što se vidi, iako automatizovana, procedura prenosa, šifrovanja i dešifrovanja, podrazumeva i niz preduslova, što opet ukazuje na to da je zaštitu lakše obezbediti u slučaju komunikacija korisnika koji imaju čvrsto uspostavljene veze.

5 ZAKLJUČAK

Iako je danas elektronska pošta nezamenljivo sredstvo komunikacije korisnici moraju da budu svesni ograničenja i rizika koje elektronska pošta nosi. Na osnovu izloženog može se zaključiti da praktično ne postoji tehnologija koja obezbeđuje apsolutnu zaštitu poruke i da nije dovoljno samo zaštiti važnu poruku za vreme njenog putovanja kiber prostorom, već je treba štititi od njenog nastajanja do njenog čitanja i arhiviranja. Iskustvo je pokazalo da većina korisnika još uvek vrlo retko koristi šifrovanje po sistemu „s kraja na kraj“ iz različitih razloga, uključujući pri tom i navike korisnika e-pošte. Čak i u slučajevima primene zaštite „s kraja na kraj“ pošiljalac poruke šalje šifrovanu poruku verujući trećem licu, verujući kompaniji koja mu je prodala softver da nije ugradila dodatke koji bi preuzeli poruku. U svetlu događaja u vezi sa Edvardom Snoudenom pošiljalac poverljive pošte treba dobro da razmisli o načinu slanja poverljivih podataka i načinu korišćenja elektronske pošte. Prema jednoj opasci jednog od učesnika diskusije na ovu temu, izgleda da je još uvek najbolje za šifrovanje koristiti dovoljno dugačku knjigu i simetričnu enkripciju.

Na to da se stanje u ovoj oblasti neće poboljšavati posredno ukazuje izjava Michaela Hajdena (direktor NSA od 1995 do 2005) u kojoj je praktično opisao sve one koji su zabrinuti zbog projekta Prizma i koji žele transparentnost u upravljanju državom kao: „nihiliste, anarhiste, Lulzseke, Anonimuse, dvadesetogodišnjake koji sa suprotnim polom nisu kontaktirali pet ili šest godina“ (Moore, 2013) (Ackerman, 2013)

CITIRANI RADOVI

Ackerman, S. (2013, 08 06). *Former NSA chief warns of cyber-terror attacks if Snowden apprehended.* Preuzeto sa theguardian: http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden

Admin, J. (2011, 07 2). *Man In The Middle Attack Using Ettercap.* Preuzeto sa Hackaholic: http://www.101hacker.com/2011/03/man-in-middle-attack-using-ettercap.html

Anon. (2009). *Pravilnik o izdavanju vremenskog žiga.* Preuzeto sa Digitalna agenda: http://www.digitalnaagenda.gov.rs/FileSystem/SiteDocuments/zakoni/Pravilnik%20o%20izdavanju%20vremenskog%20ziga%202009.pdf

Anon. (2013, 08 01). *Email.* Preuzeto sa Surveillance Self-Defense: https://ssd.eff.org/tech/email

Čekerevac, Z. (2009). *Internet tehnologije i Internet poslovanje* (Vol. 4). (P. d. Bulat, Ed.) Kruševac, Srbija, Srbija: ICIM+.

Čekerevac, Z. (2012). *Elektronsko poslovanje.* Beograd, Srbija, Srbija: Visoka poslovna škola strukovnih studija.

Charles, A. (2013, 08 19). *Google trying to evade UK privacy laws, campaigners claim.* Preuzeto sa The Guardian: http://www.theguardian.com/technology/2013/aug/19/google-privacy-laws-uk-lawsuit

Constantin, L. (2011, 11 21). *OpenPGP JavaScript Implementation Allows Webmail Encryption.* Preuzeto sa PCWorld: http://www.pcworld.com/article/244406/openpgp_javascript_implementation_allows_webmail_encryption.html

Geier, E. (2012, 04 25). *How to encrypt your email.* Preuzeto sa PCWorld: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html

Greenwald, G., & MacAskill, E. (2013, 06 07). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Preuzeto 08 04, 2013 sa http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Jungholt, T. (2013, 08 03). FDP-Minister will "Datenuntreue" bestrafen. *Die Welt*. Retrieved 09 20, 2013, from http://www.welt.de/politik/deutschland/article118648774/FDP-Minister-will-Datenuntreue-bestrafen.html

Kessler, M. (2013, 07 23). *Deutsche User: Zwei Drittel halten ihre Daten im Netz für unsicher.* Preuzeto 08 05, 2013 sa teltarif.de: http://www.teltarif.de/bitkom-internet-nutzer-daten-unsicher-befragung-prism/news/51871.html

Moore, A. (2013, 08 07). *Former NSA boss compares PRISM critics to Al Qaeda.* Preuzeto sa deathandtaxes: http://www.deathandtaxesmag.com/203430/former-nsa-boss-compares-prism-critics-to-al-qaeda/

Muncaster, P. (2013, 07 29). *Western spooks banned Lenovo PCs after finding back doors.* Preuzeto sa The Register: http://www.theregister.co.uk/2013/07/29/lenovo_accused_backdoors_intel_ban/

Nikić, S. (2010, 03 05). *Najčešće metode napada cyber kriminalaca i kako se odbraniti.* Preuzeto sa IT Veštak: http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf

Osterman Research. (2013, 07). *Why Should You Encrypt Email and What Happens if You Don't?* Preuzeto sa Osterman Research White Paper: http://www.ostermanresearch.com/whitepapers/orwp_0194.pdf

Rouse, M. (2007, 06). *Man in the middle attack (fire brigade attack).* Preuzeto sa SearchSecurity: http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack

Rusbridger, A. (2013, 08 20). I would rather destroy the copied files than hand them back to the NSA and GCHQ - video. (J. Borger, Novinar) theguardian.com. London. Preuzeto sa http://www.theguardian.com/world/video/2013/aug/20/alan-rusbridger-miranda-snowden-nsa-gchq-video

Schindler, E. (2007, 02 15). *Getting clueful: Five things you should know about fighting spam.* Retrieved from CIO: http://www.cio.com/article/28830/Getting_Clueful_Five_Things_You_Should_Know_About_Fighting_Spam

Schindler, E. (2008, 01 07). *E-Mail Technology Definition and Solutions.* Preuzeto sa CIO: http://www.cio.com/article/169700/E_Mail_Technology_Definition_and_Solutions?page=2&taxonomyId=3071

Snowden, E. (2013, 06 23). *Edward Snowden News*. Preuzeto sa Edward Snowden News: http://edward-snowden.net/category/edward-snowden/

Symantec. (2013, 03 13). *Symantec Encryption Solutions for Email, Powered by PGP Technology.* Preuzeto 08 01, 2013 sa Symantec: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-solutions-for-email.pdf

TeleGeography. (2013). *Global Internet Map 2012.* Preuzeto 08 05, 2013 sa TeleGeography Authoritative Telecom Data: http://www.telegeography.com/telecom-resources/map-gallery/global-internet-map-2012/

USA Patriot Act. (2001, 10 24). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.* Preuzeto 08 03, 2013 sa epic.org: http://epic.org/privacy/terrorism/hr3162.html

Vicomsoft. (2012, 11 29). *Email and email servers - Part two.* Preuzeto sa Vicomsoft: http://www.vicomsoft.com/learning-center/email-and-email-servers-part-2/

Wheatley, M. (2013, 06 24). *Project Tempora: How the British GCHQ Helps the NSA Spy on US Citizens.* Preuzeto sa siliconANGLE: http://siliconangle.com/blog/2013/06/24/project-tempora-how-the-british-gchq-helps-the-nsa-spy-on-us-citizens/

Wikipedia. (2013, 08 05). *Email.* Preuzeto sa Wikipedia The Free Encyklopedia: https://en.wikipedia.org/wiki/Email#Operation_overview

Zakon. (2009). Zakon o elektronskom dokumentu. *„Službeni glasnik RS"*(51). Preuzeto sa Republika Srbija - Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija: http://mtt.gov.rs/download/1/Zakon_o_elektronskom_dokumentu.pdf?lang=lat

Zakon BD. (2010, 06 02). *Zakon o elektroničkoj ispravi Brčko Distrikta Bosne i Hercegovine.* Preuzeto sa Skupština Brčko Distrikt BiH: http://www.skupstinabd.ba/zakoni/164/Zakon%20o%20elektronickoj%20ispravi%20BOS%2039-10.pdf

Zakon HR. (2005, 12 29). *Zakon o elektroničkoj ispravi.* Preuzeto sa Zakon HR: http://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi

Received for publication: 23.08.2013
Revision received: 05.09.2013
Accepted for publication: 20.09.2013

How to cite this article?

Style – **APA** *Sixth Edition*:

Čekerevac, Z., Čekerevac, P., & Vasiljević, J. (2014, 01 15). Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte. (Z. Čekerevac, Ed.) *FBIM Transactions, 2*(1), 45-56. doi:10.12709/fbim.02.02.01.05

Stile – **Chicago** *Fifteenth Edition*

Čekerevac, Zoran, Petar Čekerevac, and Jelena Vasiljević. "Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 2, no. 1 (01 2014): 45-56.

Style – **GOST** *Name Sort:*

Čekerevac Zoran, Čekerevac Petar and Vasiljević Jelena Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Belgrade : MESTE, 01 15, 2014. - 1 : Vol. 2. - pp. 45-56. - ISSN 2334-704X (Online); ISSN 2334-718X.

Style – **Harvard** *Anglia:*

Čekerevac, Z., Čekerevac, P. & Vasiljević, J., 2014. Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte. *FBIM Transactions,* 15 01, 2(1), pp. 45-56.

Style – **ISO 690** *Numerical Reference:*

Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte. **Čekerevac, Zoran, Čekerevac, Petar and Vasiljević, Jelena.** [ed.] Zoran Čekerevac. 1, Belgrade : MESTE, 01 15, 2014, FBIM Transactions, Vol. 2, pp. 45-56. ISSN 2334-704X (Online); ISSN 2334-718X.