PRAVNI I TEHNIČKI ASPEKTI PRIVATNOSTI DIGITALNIH PODATAKA

LEGAL AND TECHNICAL ASPECTS OF DIGITAL DATA PRIVACY

MsSc Nevena Miladinović, MSc Nataša Simić, mr Zoran Živković, dipl.inž

Towers Net d.o.o.

Abstrakt: *U ovom radu data su tri aspekta problematike očuvanja integriteta i privatnosti digitalnih podataka o ličnosti. Prvo je dat prikaz postojećeg pravnog okvira koji zahetva od rukovaoca primenu tehničke zaštite. Potom su predstavljeni najveći rizici i vektori kiber napada na koje treba obratiti posebnu pažnju. Na kraju dati su predlozi tehničke zaštite koja se može primeniti u zaštiti podataka.*

Ključne reči: *lični podaci, zakonski okvir, tehnička zaštita;*

Abstract: *This paper is focused on data protection issue and its legal framework. It analyzes data protection risks in current state of cyber space and offers several recommendations for technical protection.*

Key words: *data protection, data privacy, cyber threat.*

1. UVOD

Pitanje digitalne privatnosti postaje sve izraženije poslednjih godina kao društveni i tehnološki problem. Usled činjenice da se uz razvoj i široku primenu tehnologije paralelno razvija i njena zloupotreba, pojam privatnosti definisan od strane Luisa Brandeisa i Samuela Vorena krajem 19. veka kao „pravo da budemo ostavljeni na miru“[1], danas postaje sve više okrenut ka problematici zaštite privatnosti komunikacije i sigurnosti podataka.

Da je ovo pitanje već nekoliko decenija podrazumevano kao ozbiljna tematika govori i činjenica da je privatnost definisana kao jedno od osnovnih ljudskih prava u Univerzalnoj deklaraciji o ljudskim pravima Ujedinjenih nacija. Pravni okvir zaštite privatnosti podataka počeo da se razvija još sedamdesetih godina prošlog veka u Evropi. Danas obuhvata veliki broj međunarodnih dokumenata i zakona pojedinačnih država. Od značaja za zaštitu podataka u Republici Srbiji su međunarodni dokumenti Ujedinjenih nacija, regulativa Evropske Unije i naravno Ustav, Zakon o zaštiti podataka o ličnosti donet 2008. godine i Zakon o informacionoj bezbednost donet početkom 2016.

Ispunjavanje zakonskih obaveza o privatnosti podataka u digitalno doba podrazumeva i dobro poznavanje rizika koje kiber prostor donosi kao i metoda prevencije i odbrane od zloupotrebe. Kiber napadi više nisu retkost niti su jednostavno konstruisani. Brzina njihovog razvoja je vremenom sve veća pa je nepohodno da zaštita i odbrana održe barem isti tempo. Pre svega je potrebno shvatiti značaj i neophodnost pravovremene implementacije tehničke zaštite. Posledice njenog izostanka mogu biti ozbiljne i, bilo da su sudski sankcionisane ili ne, skoro uvek povlače ozbiljne financijske reperkusije.

Želja autora ovog rada bila je da istraže aspekte pravne regulative koji obavezuju rukovaoce na tehničku zaštitu podataka o ličnosti kojima barataju, da ukažu na rizike koji na tom planu postoje i da ponude nekoliko rešenja koja mogu da ih preduprede.

2. PRAVNI OKVIR

Zaštitu podataka o ličnosti u našoj zemlji definiše pravni okvir koji čine Ustav, Zakon o zaštiti podataka o ličnosti [2] i Zakon o informacionoj bezbednosti [3]. Zakoni su nastali po ugledu na ostale zemlje Evrope a u skladu sa regulativom Evropske Unije.

2.1. REGULATIVA EVROPSKE UNIJE

Evropska Unija je prvi dokument kojim definiše ovu oblast donela 1995. godine. U pitanju je Direktiva 95/46/EC Evropskog parlamenta i Saveta [4] koja se odnosi na zaštitu ličnih podataka pri procesiranju. Ova direktiva je obavezujuća za sve države članice i države koje žele da postanu deo Unije.

Članovima 16. i 17. definisane su obaveze rukovaoca ličnim podacima u pogledu poverljivosti i bezbednosti rukovanja. Od rukovaoca se traži da primeni adekvatne tehničke i organizacione mere koje će zaštititi lične podatke od slučajne ili nezakonite destrukcije, slučajnog gubitka, izmene, otkrivanja ili pristupa, naročito kada procesiranje uključuje prenos podataka kroz mrežu, i od svih drugih oblika procesiranja. Zaštitne mere treba da budu u skladu sa tehnološkim razvojem i troškovima koji su srazmerni riziku koje procesiranje sa sobom nosi i tipu podataka kojim se rukuje.

Države članice su svoje zakone vremenom uskladile sa ovom direktivom ili donele nove koji bi ispunili potreban standard. Većina je na temu tehničke zaštite navela praktično ono što je traženo u Direktivi 95/46/EC.

Nekoliko zemalja kao što su Italija, Španija, Poljska i Slovačka su postavile dodatne uslove. Njihovi zakoni se ne odnose na rukovanje ličnim podacima na našoj teritoriji ali mogu biti primer dobre prakse kada je njihova zaštita u pitanju. Tako Slovačka traži da rukovalac ima pripremljen poseban sigurnosni projekat za svoj informacioni sistem i da ima osobu posebno zaduženu za bezbesnost ličnih podataka ako zapošljava više od pet ljudi [5], Španija definiše tri tipa zaštitnih mera koje treba primeniti u zavisnosti od osetljivosti podataka [6] dok Poljska uz to traži da rukovalac poseduje dokumentaciju koja opisuje procese nad podacima i bezbednosne mere i da obavi autorizaciju i evidenciju osoblja koje ima pristup podacima [7].

Možda najrigoroznije mere zaštite zahteva italijanski zakon koji od rukovalaca eksplicitno traži primenu kompjuterske autentifikacije, implementaciju sistema za upravljanjem dozvola pristupa, upotrebu autorizacionog sistema, primenu posebnih softverskih rešenja za sprečavanje nedozvoljenog rukovanja i pristupa, primenu procedura za arhiviranje i oporavak, posedovanje redovno ažuriranog dokumenta o bezbednosnoj politici i primenu kriptografskih tehnika ili identifikacionog koda za posebne procedure rukovanja u okviru sistema zdravsvene zaštite. [8]

Pored osnovnog dokumenta iz 1995. godine, potrebno je napomenuti da Evropska Unija i njene članice imaju razvijeno zakonodavstvo kada je upitanju informaciona bezbednost. Prvi takav dokument Evropska Unija je donela 2001. godine - Budimpeštanska konvencija [9]. Potom je razvoj regulative nastavljen donošenjem dokumenata o privatnosti elektronske komunikacije (2002) [10], o napadima na informacione sisteme (2013) [11], Strategije o informacionoj bezbednosti (2013) [12] kao i mnogim drugim koji se direktno ili indirektno odnose na temu zaštite privatnosti ličnih podataka. Pre svega čine nelegalnim narušavanje bezbednosti IKT sistema, ugrožavanje bezbednosti, neovlašćeni pristup podacima (bilo da su lični ili ne) ili njihovo uništavanje, dok se od operatera traži da definiše i primenjuje mere zaštite i prijavi odgovarajućim nadležnim organima ukoliko dođe do incidenata.

2.2. ZAKONI U REPUBLICI SRBIJI

Na teritoriji Republike Srbije relevantan je Zakon o zaštiti podataka o ličnosti objavljen u "Službenom glasniku RS", br. 97/2008 od 27.10.2008. godine. Članom 47. definisane su organizacione i tehničke mere zaštite ličnih podataka:

"Podaci moraju biti odgovarajuće zaštićeni od zloupotreba, uništenja, gubitaka, neovlašćenih promena ili pristupa.

Rukovalac i obrađivač dužni su da preduzmu tehničke, kadrovske i organizacione mere zaštite podataka, u skladu sa utvrđenim standardima i postupcima, a koje su potrebne da bi se podaci zaštitili od gubitaka, uništenja, nedopuštenog pristupa, promene, objavljivanja i svake druge zloupotrebe, kao i da utvrde obavezu lica koja su zaposlena na obradi, da čuvaju tajnost podataka."

Članom 48. definisana je obaveza rukovaoca da vodi evidenciju koja, pored standardnih

informacija o vrsti podataka, tipu i svrsi obrade, treba da sadrži i preduzete mere zaštite podataka.

Članom 57. definisane su kaznene odredbe Zakona. Za postupanje suprotno odredbama člana 47. stav 2. predviđa se novčana kazna od 50.000 do 1.000.000 dinara za prekršaj rukovalac, obrađivač ili korisnik koji ima svojstvo pravnog lica.

Pored Zakona o zaštiti podataka o ličnosti relevantan je i Zakon o informacionoj bezbednosti objavljen u "Službenom glasniku RS", br. 6/16 koji je stupio na snagu 5. februara 2016. godine. Ovaj zakon se na nekoliko nivoa odnosi na IKT sisteme koji sadrže lične podatke građana Srbije.

Operator IKT sistema koji sadrži podatke građana Srbije obavezan je da u slučaju incidenta koji narušava pravo na zaštitu podataka o ličnosti o tome obavesti nadležni organ a on o tome izveštava i Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

Članom 6. (tačka 2) je definisano da se IKT sistemi za obradu naročito osetljivih podataka (podaci koji se odnose na nacionalnu pripadnost, rasu, pol, jezik, veroispovest, zdravstveno stanje, primanje socijalne pomoći, žrtvu nasilja itd) kategorišu kao sistemi od posebnog značaja.

Operator sistema od posebnog značaja je na osnovu člana 7. odgovoran za bezbednost IKT sistema i preduzimanje mera zaštite u cilju prevencije incidenta i prevencije i minimizacije štete koja bi tako nastala. Mere zaštite treba da obuhvate uspostavljanje organizacione strukture, klasifikaciju i ograničenje pristupa podacima, zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera, zaštitu od gubitaka podataka, zaštitu od zloupotrebe tehničkih bezbednosnih slabosti sistema, postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja, edukaciju zaposlenih itd. Potrebno je da se donese akt o bezbednosti sistema u kome se navode preduzete mere zaštite, primenjeni principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti, kao i ovlašćenja i odgovornosti i da se najmanje jednom godišnje vrši provera usklađenosti primenjenih mera i da se o tome sačini izveštaj (član 8.).

Primenu ovog zakona kontrolisalaće inspekcija za informacionu bezbednost pri ministarsarstvu zaduženom za telekomunikacije a kazne za nepoštovanje zakona mogu da iznose od 50.000 do 2.000.000 dinara.

3. UGROŽAVANJE PRIVATNOSTI I INTEGRITETA PODATAKA U SAVREMENOM KIBER PROSTORU

Današnji kiber prostor nije okruženje u kojem je preporučljivo ostaviti bilo koji tip podataka nezaštićen, a tako nešto učiniti sa podacima o ličnosti je i zakonski kažnjivo. Rizici kojima su izloženi podaci i informacioni sistemi obuhvataju široki opseg napada. Oni mogu biti relativno jednostavni ali i visoko sofisticirani, najčešće u zavisnosti od koristi koja se napadom može ostvariti.

Po zaštitu privatnosti i integriteta podataka naročito su značajni napadi koji bi doveli do neovlašćenog pristupa, izmene i preuzimanja podataka, slučajnog „curenja", namernog ili nenamernog uništavanja ili, što je u poslednjih par godina naročit problem, njihovog namernog zaključavanja zarad ostvarivanja finansijske dobiti.

Kiber kriminal dosegao je nivo razvoja koji daje tehničke mogućnosti napadaču da se na različite načine infiltrira u sistem koji čuva podatke i nakon toga načini štetu. Najznačajniji vektori napada su email korespondencija, nebezbedan pristup internetu i presretanje transfera osetljivih podataka.

Email komunikacija, uprkos svojoj širokoj primeni, donosi veliki broj bezbednosnih izazova. Najveći problem *email* poruka predstavljaju prilozi koje one sadrže ili linkovi koji se nalaze u tekstu poruke. Otvaranjem priloga ili linka zlonamerne poruke može da dovede do pokretanja skrivenog malvera različitih namena i dometa u pogledu štete koju može da načini.

Zlonamerne *email* poruke mogu najčešće da se klasifikuju u tri grupe: spam, *phishing* i *spear-phishing.* Problem spama je prisutan jako dugo. Zaštita od njega postoji i primenjuje se na tehničkom nivou ali su i sami korisnici email servisa dovoljno informisani da ga u principu prepoznaju i brišu iz svog inboksa. Međutim, što zbog sve kvalitetnije konstruisanih poruka, što

zbog nepažnje, pada koncentracije ili zamora korisnika neretko se događa da se spam poruke otvore i da se tako napadaču otvore vrata u informacioni sistem.

Spam je vremenom evoluirano u *phishing* (pecanje), napredniji vid napada preko *email*-a. Poruke su pažljivije konstruisane, njihov sadržaj i pošiljalac deluju legitimno ali ako se pažljivije pogledaju njihove karakteristike može se primetiti da su maliciozne. Za razliku od spama, *phishing* poruke su uglavnom napisane na jeziku koji potencijalna žrtva koristi u svojoj korespondenciji i manjeg je obima u količini poslatih poruka.

Poslednji evolutivni nivo predstavljaju *spear-phishing* poruke koje su uglavnom u upotrebi prilikom ciljanih (APT) napada. Usmereni su ka malom broju email korisnika konkretne organizacije koja je meta napadača.

Internet konekcija sistema koji skladišti osetljive podatke nosi slične rizike kao i otvaranje email poruka od strane njegovih korisnika. *Web* protokoli su sveprisutni, podržavaju web pretraživanje, mobilne aplikacije i veb servise. Međutim kompleksnost aplikacija koje ih koriste i opštost HTTP-a vodi do curenja informacija i može dovesti do zloupotrebe. Takođe pristupi nebezbednim stranicama može da dovede do prodora malvera u računar i informacioni sistem kojem on pripada.

Značajan vektor napada, takođe, predstavlja prenos fajlova sa osetljivim podacima preko nebezbedne konekcije ili prijem fajlova čija struktura i sadržaj nisu podrobno provereni.

4. TEHNIČKA REŠENJA ZA OČUVANJE PRIVATNOSTI I INTEGRITETA PODATAKA

Razvoj velikog broja kiber pretnji pratio je i razvoj tehničke zaštite privatnosti i integriteta podataka i informacionih sistema. Zaštitna rešenja su nastajala na osnovu potrebe da se spreče potencijalni vektori napada, određeni tipovi pretnji ali i da se ponude različiti nivoi bezbebednosti u skladu sa sigurnosnim potrebama i financijskim mogućnostima organizacije koja odluči da ih primeni.

Velike kompanije i državne institucije širom sveta odavno su svesne neophodnosti očuvanja integriteta i privatnosti podataka koje čuvaju. Iskustva kompanija koje su pretrpele napade pokazuju da, pored neizbežnih pravnih konsekvenci, ni malo nije zanemarljiv gubitak poverenja klijenata i opadanje prihoda i ugleda. Tako se, iz zakonske i poslovne nužde, okreću primeni zaštitnih rešenja.

Međutim, jedan od trendova 2015. godine je to što se kiber kriminal u velikoj meri okreće ka srednjim i malim preduzećima. Uzrok tome je što su bili posmatrani kao „lake mete“ očekujući da zbog manjeg budžeta neće uložiti u zaštitu svojih podataka i sistema.

Značajno je i to da tehnička zaštita potrebna bez obzira na domen kojim se kompanija/organizacija /institucija bavi. Dokle god skladišti lične podatke dužna je da se brine o njima.

Izbor rešenja može biti izvršen na osnovu nivoa zaštite koji je potrebno ostvariti, vektora napada koje treba štititi i finansijskih mogućnosti kojima se raspolaže.

4.1 REŠENJE KOJE ZAUSTAVLJA VIŠE VEKTORA NAPADA

Organizacije koje raspolažu manjim brojem zaposlenih, manjom infrastrukturom koju treba da štite i manjim budžetom, svoje informacije mogu da zaštite primenom rešenja koja brane od više vektora napada.

Ovakva rešenja vrše proveru više različitih tipova saobraćaja i sprečavaju ulazak zlonamernog sadržaja i curenje podataka. Filtriranje je potrebno izvršiti za tri najkritičnija tipa komunikacije (*mail, web* i *file transfer*). Postavljaju se na granici sistema organizacije i štite njenu celokupnu infrastrukturu.

Sprečavanje prodora zlonamernog sadržaja u sistem se pre svega može obaviti filtriranjem dolaznih datoteka vršenjem njihove dubinske provere. Dubinskom proverom analiza se unutrašnji sadržaj datoteka koji može biti različite strukture i karaktera. Datoteka može da ima u sebi druge datoteke, pa tako dubinska provera treba da bude višeslojna. Nakon provere datoteke je

potrebno ponovo sastaviti uz izostavljanje pronađenih zlonamernih sadržaja.

Blokiranje se primenjuje u slučaju prisustva aktivnih objekata kao što su skripte, interaktivne forme ili *flash*. Na taj način sprečava se da u sistem uđe *spyware*, *ransomware* ili neki drugi vid *malware* koji bi oštetio podatke, izbrisao ih, neautorizovano im pristupio ili omogućio njihovo curenje.

Zlonamernu prirodu datoteke napadači često pokušavaju da prikriju menjanjem njene ekstenzije. Tako jedna maliciozna skripta za postavljanje backdoor-a promenom ekstenzije može da postane .pdf ili .doc tekstualni fajl poslat uz komplementarnu poruku u *mail*-u, pa je potrebno da zaštitno rešenje bude sposobno da to prepozna.

Curenje podataka u vidu nepromišljenog ili namernog slanja osetljivih podataka van sistema može da bude sprečeno odgovarajućom administratorskom politikom definisanom pomoću ključnih reči na osnovu kojih bi se vršila provera sadržaja koji izlazi iz sistema.

Jedno od rešenja koje se može preporučiti za zaštitu sistema od više vektora napada je SelectorIT [13], u proizvodnji kompanije *YazamTech*. Ovo rešenje vrši proveru i filtriranje različitih tipova datoteka koje ulaze u sistem. Ima mogućnost integracije sa popularnim aplikacijama za *email*, *web* pretragu i transfer fajlova a skeniranje vrši pomoću 13 antivirusnih rešenja bez međusobne kolizije.

4.2 REŠENJA SPECIJALIZOVANA ZA POJEDINAČNE VEKTORE NAPADA

Veliki informacioni sistemi operatora ili kompleksnih organizacija mogu imati potrebu za kompleksnijom zaštitom, pa njihove potrebe ne može uvek da podmiri jedno rešenje koje pokriva sve potencijalne vektore napada. U tom slučaju primenjuju se zasebna rešenja za određene tipove komunikacija.

Kada je u pitanju zaštita privatnosti i integriteta podataka od posebnog je značaja u kompleksnim sistemima implementirati rešenja za zaštitu *email* komunikacije, pristupa internetu i transfera fajlova.

Zaštitna rešenja ovog tipa koriste različite mehanizme filtriranja saobraćaja. Preporuka autora je primena tehnologija koje pored ostalih metoda koriste i prekid TCP/IP konekcije na granici sistema. Ovaj pristup omogućava dodatni stepen izolacije štićenog sistema. Naime, za svaki dolazni tok saobraćaja prekida se TCP/IP konekcija i primljeni saobraćaj se analizira i filtrira. Nakon povere uspostavlja se nova TCP/IP konekcija koja omogućava prenos odobrenih podataka u drugu mrežu. Tako ni u jednom trenutku ne postoji TCP/IP konekcija koja povezuje obe mreže i daje napadaču uvid u nju.

4.2.1 ZAŠTITA EMAIL KOMUNIKACIJE

Organizacije koje raspolažu velikom količinom *mail* saobraćaja, kao što su telekomunikacioni operateri ili druge organizacije koje imaju svoje *mail* servere, mogu da primene tome posebno namenjenu zaštitu.

Rešenja namenjena *mail* zaštiti omogućavaju administratoru da za specifične potrebe sistema formira posebna pravila za ograničavanje saobraćaja. Mogu da se definišu u zavisnosti od potreba poslovanja i da budu različita za pošiljaoca i primaoca ili različit tip poruke i sadržaja.

Dolazni *mail* saobraćaj je potrebno filtrirati tako da se spreči ulaz nebezbednih priloga koji u sebi sadrže *ransomware*, *spyware* ili skripte koje mogu da postave *backdoor*, dok se odlazni saobraćaj ograničava tako da iz sistema ne izađu poruke koje sadrže osetljive podatke.

Poruke koje nisu u skladu sa bezbednosnom politikom mogu biti tiho odbačene, odbačene bez slanja povratnog izveštaja ili stavljene u karantin dok administrator ne odluči pojedinačno šta treba sa njima da bude učinjeno.

Zaustavljanje lažnih *email*-ova i pokušaja socijalnog inžinjeringa se vrši proverom adrese pošiljaoca, autentifikacije i dodelom digitanih identiteta. Curenje podataka tokom tranzita poruke se dodatno može sprečiti upotrebom enkripcije.

Primer rešenja koje može da obezbedi visok nivo zaštite *email* komunikacije može biti *Mail Guard* proizvođača *Deep Secure* [14]. Ovo rešenje je dizajnirano da štiti i od veoma naprednih napada i

zloupotreba fokusirajući se na sadržaj. Preporučuje se njegova primena ukoliko je potrebna stroga kontrola ovog vida komunikacije.

4.2.2 ZAŠTITA WEB SAOBRAĆAJA

Organizacije čiji sistemi upravljaju velikom količinom *web* saobraćaja imaju potrebu da taj saobraćaj prilagode svojim bezbednosnim politikama.

Rešenja za konrolu *web* saobraćaja vrše proveru korisnog segmenta HTTP paketa (*payload*) na različite vrste malvera i osetljive podatke. Dozvoljavaju administratoru da definiše bezbednosnu politiku na osnovu identiteta klijenta i servera i upotrebljene HTTP metode. To omogućava da se pravila posebno definišu da bi se ostvario najviši stepen bezbednosti.

HTTP zaglavlja takođe mogu biti proverena, modifikovana ili potpuno uklonjena i zamenjena. Na ovaj način sprečava se upotreba *cookies*-a i tajnih tokova informacija koje bi koristio kontrolni centar naprednih napada.

Kao primer rešenja koje štiti od napada koji može doći putem *web* saobraćaja može se uzeti srodno rešenje, *Web Guard* takođe proizvodnje kompanije *Deep Secure* [15]. Namenjen je preciznoj kontroli saobraćaja Internet pretraživanja i *web* protokola koje koriste različite aplikacije za razmenu podataka.

4.2.3 ZAŠTITA TRANSFERA DATOTEKA

Organizacije koje imaju potrebu da pažljivo kontrolišu transfer datoteka sa Internet serverima ili imaju potrebu da razmenjuju datoteke između internih zona sistema mogu da primene rešenja za konrolu ovog vida razmene podataka.

Bezbednosnim pravilima koje postavlja administrator ograničava se sadržaj i određuje kako se tretira datoteka koja se prenosi. Dubinskom proverom se uklanja malver i zaustavlja curenje osetljivih podataka.

Curenje podataka može da bude sprečeno primenom bezbednosnih oznaka koje čine unapred definisane reči ili fraze. Prilikom transfera datoteka pored drugih provera vrši se i provera da li datoteka sadrži definisane reči ili fraze u svom sadržaju i pratećim karakteristikama (*properties*, *header* i *footer*).

Bezbednosna pravila mogu biti uslovljena identitetom klijenta koji se utvrđuju pomoću lozinke ili digitalnog potpisa. Na taj način se sprečava da neautorizovane osobe ostvare pristup datotekama sa osetljivim podacima.

Primer rešenja koje može obezbediti siguran transfer datoteka sa osetljivim podacima je *File Transfer Guard* takođe proizvođača *Deep Secure* [16].

Rad ovog rešenja je zasnovan na terminaciji konekcije transfera i dubokoj proveri datoteka koje se razmenjuju pre nego što se uspostavi nova konekcija i obavi prenos do odredišta. Podržava prenos pomoću FTP protokola koji koristi različite konekcije za transfer datoteka i kontrolu sesije, pa se terminacija vrši za obe konekcije.

4.3 ZAŠTITA POSEBNO OSETLJIVIH BAZA PODATAKA

Zaštita posebno osetljivih podataka se može konstruisati na različite načine. Postavlja se pitanje koji nivo zaštite je potreban, kakav pristup podacima se očekuje.

Nivo zaštite se definiše na osnovu nivoa rizika koji postoji u čuvanju osetljivih podataka. Obično se u osnovnim arhitekturama koriste *firewall* uređaji u kobinaciji sa IPS (*Intrusion Prevention System*) rešenjima.

U pojedinim sistemima potrebno je napraviti posebno bezbedni i izolovani *backup*. Tada je moguće kao poseban vid zaštite upotrebiti jednosmerne *data* diode. Ovi uređaji su zasnovani na jednosmernom prenosu podataka. Jednosmernost može biti obezbeđena na softverskom i hardverskom nivou. Obično se hardverski nivo obezbeđuje upotrebom jednosmernih optičkih vlakana i koristi se kao dopuna već postojećoj softverskoj jednosmernosti zarad ispunjavanja različitih standarda zaštite.

Jednosmeran uređaj ovog tipa može biti postavljen na ulazu u *backup* sistem, tako da dozvoljava samo ulaz podataka u zaštićenu zonu. Na taj način

omogućava se unos najnovijih podataka u skladištenu memoriju ali se sprečava njihovo curenje.

Drugi način može biti njihovo postavljanje ispred sistema u kojem se čuvaju podaci kojima može biti dopušteno da napuste štićenu zonu ali je imperativ da njihov integritet bude apsolutno očuvan. U ovom slučaju dioda bi omogućila dostupnost podataka i sprečila njihovo kompromitovanje usled napada.

Pored same jednosmernosti, bitno je da *data* diode u sebi sadrže i mehanizme za kontrolu sadržaja koji bi uklonio potencijalne zlonamerne softvere. U prvom scenariju, bez ovakvog mehanizma moguće je da malver dospe do štićene zone i naruši integritet podataka iako nikako ne može da dovede do njihovog curenja.

Primera ovakvih uređaja ima više. *Minerva* dioda u proizvodnji kompanije *Deep Secure* [17] nudi pouzdanu softversku jednosmernost prenosa podataka uz mogućnost primene i fizičke jednosmernosti. Naime, realizovana je u vidu dva servera (prijemni i predajni) koji se ako je potrebno mogu povezati optičkim linkom. Kao drugi primer može se uzeti *Arow* dioda u proizvodnji kompanije *Somerdata* [18]. Ova *data* dioda je realizovana tako da je u potpunosti hardverski jednosmerna jer su predajni i prijemni moduli (dati u redundansi) međusobno povezani optičkim linkovima. Obe ove diode sadrže mehanizme za detekciju i uklanjanje zlonamernog sadržaja iz saobraćaja koji prolazi kroz njih.

5. ZAKLJUČAK

Sa rapidnom ekspanzijom kiber pretnji, pitanje zaštite i privatnosti ličnih podataka postaje sve aktuelnija tema. Međutim, bez obzira ili baš uprkos sve većim izazovima principijelan pristup privatnosti mora biti očuvan.

Jedan faktor postizanja tog cilja je pravni okvir koji će primorati rukovaoce podacima o ličnosti da ozbiljno shvate neophodnost primene tehničke i organizacione zaštite.

Drugi faktor predstavlja praćenje tehnološkog razvoja i složenosti kiber pretnji, njihovih vektora napada i posledica koje mogu da proizvedu.

Treći faktor predstavlja adekvatna, blagovremena i sveobuhvatna primena tehničke zaštite koja treba da bude sposobna da odgovori na sve zahtevnije i kompleksnije probleme informacione bezbednosti.

Sva tri faktora su podjednako neophodna da bi se ostvarila privatnost i integritet podataka. Vremenom će njihova složenost prirodno rasti jer će, sudeći po dosadašnjim prilikama, ozbiljnost kiber pretnji postati samo veća.

LITERATURA

[1] U.Mišljenović, B.Nedić i A.Toskić, *Zaštita privatnosti u Srbiji*, Partneri za demokratske promene Srbija, 2013.

[2] Zakon o zaštiti podataka o ličnosti, *Službeni glasnik RS*, br. 97/2008, 27.10.2008.

[3] Zakon o informacionoj bezbednosti, *Službeni glasnik RS*, br. 6/16, 5.2.2016.

[4] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[5] *National Council of the Slovak Republic, Act No. 122/2013 Coll. on Protection of Personal Data*

[6] *Organic Law 15/1999 of 13 December on the Protection of Personal Data,*

[7] *Personal Data Protection Act of 29 August 1997 (*consolidated text Journal of laws of 2002, No 101, item 926)

[8] *Legislative Decree no. 196 of 30 June 2003, (Codice in materia di protezione dei dati personali)*

[9] *Convention on Cybercrime, Budapest, 23.11.2001.*

[10] *Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic sector*, Brussels 12.7.2012.

[11] *Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems*, Brussels, 12.2.2013.

[12] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013.

[13]http://www.towersnet.rs/wp-content/uploads/2016/03/SelectorIT.pdf

[14]http://www.towersnet.rs/wp-content/uploads/2015/06/Mail-Guard-flyer.pdf

[15]http://www.towersnet.rs/wp-content/uploads/2015/06/Web-Guard-flyer.pdf

[16]http://www.towersnet.rs/wp-content/uploads/2015/06/File-Transfer-Guard-flyer.pdf

[17]http://www.towersnet.rs/wp-content/uploads/2015/06/Minerva-flyer2.pdf

[18]http://www.towersnet.rs/wp-content/uploads/2015/06/Arow-flajerZ.pdf

[19] Sophos, *Our Cybersecurtiy Predictions for 2016*, https://blogs.sophos.com/2015/12/11/our-cybersecurity-predictions-for-2016/#top

[20]Kaspersky Lab, *Top 7 Cyberthreats*, https://usa.kaspersky.com/internet-security-center/threats/top-7-cyberthreats

[21] Kaspersky Lab, *Kaspersky Security Bulletin 2015*, https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

[22]Kaspersky Lab, *Kaspersky Security Bulletin 2015. Overall statistics for 2015*, https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/