STRATEGIJA RAZVOJA INFORMACIONOG DRUŠTVA U REPUBLICI SRBIJI DO 2020. GODINE: BEZBEDNOST INFORMACIJA I KRITIČNA INFRASTRUKTURA

Danijela D. Protić,
Generalštab Vojske Srbije, Uprava za telekomunikacije i informatiu (J-6), Centar za primenjenu matematiku i elektroniku, Beograd

DOI: 10.5937/vojtehg1204082P

OBLAST: informacione tehnologije
VRSTA ČLANKA: originalni naučni članak

Sažetak:

Napredak tehnologije uslovio je razvoj svetske ekonomije i promenu političkih trendova. Države članice Evropske unije, ali i mnoge savremene države koje to nisu, primenjuju strategije razvoja informacionog društva što, pored ostalog, uključuje i podizanje nivoa informacione bezbednosti. Vlada Republike Srbije donela je Strategiju razvoja informacionog društva u Republici Srbiji do 2020. godine, u okviru koje su definisani izazovi razvoja savremenog srpskog informacionog društva. U radu je prikazan osvrt na ovu strategiju, što se posebno odnosi na otvorena pitanja o bezbednosti informacija, kritičnoj infrastrukturi i njenoj zaštiti. Na osnovu javno dostupnih podataka opisana je domaća kritična infrastruktura i prikazana mogućnost zaštite informacija koja je zasnovana na primeni modularnog, objedinjenog informacionog sistema.

Ključne reči: *bezbednost informacija, kritična intrafstuktura, strategija razvoja.*

Uvod

Savremeno informaciono društvo, koje je rezultat razvoja informaciono-komunikacionih tehnologija (IKT), utiče na promene u svim oblastima života. Nivo informatičke pismenosti raste, što je primetno kako kod pojedinaca, tako i u radu organizacija različitih interesnih sfera. Generisanje, procesuiranje i razmena informacija je efikasna i brza, što omogućava kvalitetno poslovanje, smanjenje papirne dokumentacije, bolju komunikaciju sa zaposlenima, korisnicima usluga i poslovnim partn-

adanijela@ptt.rs

erima, i sl. Internet je omogućio razvoj elektronskog poslovanja (e-business), elektronsko bankarstvo (e-banking), on-line kupovinu (e-shoping), učenje na daljinu (e-learning), marketing kroz elektronske medije (e-marketing), itd. Dostupnost internetu uticao je i na razvoj sajtova za socijalno umrežavanje tipa Facebook, MySpace, LinkedIn, Twitter, što je dodatno uticalo na porast razmene podataka različitog sadržaja, u globalnom okruženju. Istovremeno, sve prednosti koje nudi razvoj IKT izvor su potencijalnih napada na poverljive informacije koje mogu postati dostupne neautorizovanim osobama, ili biti izmenjene i uništene. Zbog toga je zaštita informacija u žiži javnosti – nastaju nove poslovne politike, a razvijeni su i standardi za zaštitu podataka i odgovarajuće pravne norme.

Nagli razvoj tehnologije doveo je i do pojave kompleksnih organizacionih sistema. Kao rezultat ovog usložnjavanja nastale su strategije održivog razvoja u različitim oblastima, pa i u oblasti razvoja informacionog društva. U opštem slučaju, okvire strategija predstavljaju zadaci koje je potrebno realizovati, zahtevani vremenski period za realizaciju, nadležna tela, način izveštavanja o postignutim rezultatima, budžet, itd. Nije redak slučaj da realizaciju strategije nadziru nadležna državna ministarstva ili agencije, u zavisnosti od kompleksnosti zadataka koje je potrebno izvršavati. Pojedinačno su, za svaku strategiju, precizno definisane oblast delovanja, razlog zbog kojeg je utvrđena izabrana strateška politika, očekivani rezultati i mogućnost njihove primene u praksi.

Kao važan faktor za razvoj informacionog društva Evropska unija (EU) uvrstila je IKT u grupu faktora koji utiču na ekonomski rast i razvoj. Prateći trendove u EU, Vlada Republike Srbije (Vlada) odredila je najbitnije faktore koji će uticati na razvoj informacionog društva u Republici Srbiji do 2020. godine. Vladini prioriteti su pravni i institucionalni okviri za informacionu bezbednost (IB), borba protiv visokotehnološkog kriminala, naučno-istraživački rad i zaštita kritične infrastrukture. Međutim, kritična infrastruktura u Republici Srbiji (Srbija) nije popisana, što nije slučaj u EU, Kanadi, Sjedinjenim Američkim Državama (SAD), Australiji i određenom broju evropskih zemalja koje nisu članice EU. U Srbiji postoje pojedinačni pokušaji da neke infrastrukture budu „proglašene" kritičnim, ali sveobuhvatnih aktivnosti na ovom polju nema. Jedno od rešenja ovog problema može da obezbedi formiranje nacionalnog, objedinjenog informacionog sistema kritičnih infrastruktura koji bi omogućio interoperabilnost kritičnih infrastruktura na državnom nivou, i lakšu saradnju sa državama iz okruženja. Razmena podataka u ovakvom sistemu bi bila ne samo brža i kvalitetnija nego bi i IB dobila predefinisanu formu, što može biti obezbeđeno infrastrukturom sa javnim ključevima koju karakterišu centralni autoritet u vidu sertifikacionog tela koje izdaje digitalne elektronske sertifikate za zaštićenu komunikaciju korisnika ove infrastrukture. Svaka od kritičnih infrastruktura imala bi svoje sertifikaciono telo podređeno glavnom sertifikacionom telu objedinje-

nog informacionog sistema, što bi omogućilo zaštićenu komunikaciju i procesuiranje podataka u okviru jedne kritične infrastrukture, između različitih kritičnih infrastruktura, i svake od njih sa centralom, u zavisnosti od karakteristika i potreba kako pojedinih kritičnih infrastruktura, tako i celog objedinjenog informacionog sistema.

Rad je organizovan na sledeći način: poglavlje koje sledi je prikaz Strategije razvoja informacionog društva u Republici Srbiji do 2020. godine (Strategija). U trećem poglavlju razmatrana su otvorena pitanja u okviru Strategije, i to prvenstveno o kritičnoj infrastrukturi i zaštiti kritične infrastrukture. Poseban osvrt dat je na otvorena pitanja iz Strategije o zaštiti kritične infrastrukture sa stanovišta IB. Predložen je objedinjeni informacioni sistem kao moguće rešenje problema sa stanovišta IB i interoperabilnosti između kritičnih infrastruktura. Poslednje poglavlje u članku je zaključak rada.

Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine

U okviru EU IKT su prepoznate kao glavni faktor uticaja na ekonomski rast i inovativnost [1]. Između sedam inicijativa ekonomske strategije Evropa 2020 [2], u Digitalnoj agendi za Evropu, takođe je ukazano na značaj IKT. U skladu s evropskim trendovima, na osnovu člana 45. stav 1. Zakona o Vladi („Službeni glasnik RS" br. 55/05, 71/05 – ispravka, 101/07 i 65/8), Vlada je 8. jula 2010. godine donela Strategiju razvoja informacionog društva u Republici Srbiji do 2020. godine [3]. Strategija je posledica razvoja IKT i njihovog uticaja na transformaciju načina interakcije ljudi, preduzeća i javnih institucija u Srbiji.

Strategija

Strategijom su određene aktivnosti kojima je potrebno razvijati informaciono društvo u Srbiji, koje treba da budu odgovor na izazove razvoja IKT (novi aspekti bezbednosti, ugrožavanje privatnosti, tehnološka zavisnost, nedovoljna interoperabilnost institucija, otvorena pitanja zaštite intelektualne svojine). Strategijom je utvrđeno da će u Srbiji do 2020. godine biti uređeni svi navedeni aspekti. U oblasti informacionog društva Vlada definiše Strategiju kroz institucionalni i pravni okvir, pri čemu institucionalni okvir čine Ministarstvo za telekomunikacije i informaciono društvo i drugi državni organi zaduženi za razvoj i implementaciju informacionih sistema za poslove iz svog delokruga, dok pravni okvir određuju zakoni i propisi koji prate promene u skladu sa Strategijom.

Prioritetne oblasti Strategije podeljene su u šest grupa:
– elektronske komunikacije,
– elektronska uprava, zdravstvo i pravosuđe (e-uprava, e-zdravstvo i e-pravosuđe),
– IKT u obrazovanju, nauci i kulturi,
– elektronska trgovina (e-trgovina),
– IKT u poslovnom sektoru, i
– IB.

Informaciona bezbednost kao element Strategije

Kako je definisano Strategijom, IB podrazumeva zaštitu sistema, podataka i infrastrukture radi očuvanja poverljivosti, integriteta i raspoloživosti informacija. Odgovarajući stepen IB u svim oblicima primene IKT jedan je od preduslova stvaranja održivog informacionog društva. Razvojem IB Vlada želi da postigne poverenje korisnika u bezbedno funkcionisanje informacionih sistema i poverenje građana u zaštićenost podataka o ličnosti u informacionim sistemima, širenje svesti o neophodnosti sprovođenja mera IB, zaštitu podataka, zaštitu informacionih i telekomunikacionih sistema, bezbednost elektronskih transakcija, efikasne mehanizme zaštite i ostvarivanje prava u procesima elektronskog poslovanja i elektronske razmene podataka.

Unapređivanje pravnog i institucionalnog okvira za IB Vlada je regulisala Zakonom o tajnosti podataka [4], Zakonom o zaštiti podataka o ličnosti [5], Zakonom o elektronskom potpisu [6], Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [7], Zakonom o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji [8] i Krivičnim zakonikom [9]. U širem kontekstu, pravni okvir čine Zakon o telekomunikacijama [10] i Zakon o odbrani [11]. Naglašeno je da je potrebno doneti propise iz oblasti IB kojima će dodatno biti uređeni standardi IB, kao i nadležnosti i zadaci pojedinih institucija u ovoj oblasti. Takođe, potrebno je formirati instituciju koja u oblasti IB obavlja poslove verifikacije i sertifikacije metoda, softverskih aplikacija, uređaja i sistema, kao i istraživanje i razvoj. Ova institucija treba da nadzire i primenu standarda IB u državnim organima.

Sa stanovišta zaštite kritične infrastrukture potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija (IT) i u vezi s tim potrebno je dodatno urediti kriterijume za utvrđivanje kritične infrastrukture, kriterijume za karakterizaciju napada primenom IT na takve infrastrukture u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti.

Zakonom o organizaciji i nadležnosti organa za borbu protiv visokotehnološkog kriminala, koji je stupio na snagu 2005. godine, prvi put je u domaćem zakonodavstvu definisan pojam visokotehnološkog kriminala, kao „vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i

Protić, D., Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine: bezebednost informacija i kritična infrastruktura, pp. 82–101

njihovi proizvodi u materijalnom ili elektronskom obliku“. Organi za borbu protiv visokotehnološkog kriminala obrazovani su 2007. godine, kada su izvršene i odgovarajuće izmene u drugim propisima. Razvoj novih pravila i propisa treba da prati razvoj informacionog društva do 2020. godine.

Značaj naučnoistraživačkog rada proizilazi iz dinamičnih promena vezanih za izazove u oblasti IB, što zahteva kontinuitet u uvođenju novih metoda i mera zaštite u ovoj oblasti i praćenje svetskih dostignuća kroz međunarodnu saradnju.

Otvorena pitanja o informacionoj bezbednosti u okviru Strategije

U procesu razvoja informacionog društva Vlada je procenila da su, između ostalog, izazovi razvoja informacionog društva i novi aspekti IB. Delovi Strategije koji se odnose na pravnu regulativu ukazuju da postoje organizacije i važeći zakoni koji mogu da podrže razvoj informacionog društva. Međutim, oni ukazuju i na nedovoljnu interoperabilnost institucija, razvoj novih aspekata IB koje je teško pratiti, nedostatak podataka za analizu razvoja informacionog društva u Srbiji, neadekvatan naučno-istraživački rad, itd. Zato, između ostalog, u Strategiji postoje otvorena pitanja o mogućnosti razvoja zaštite IB, kriterijumima za utvrđivanje kritičnih infrastruktura u Srbiji, i mogućnostima zaštite IB u utvrđenim kritičnim infrastrukturama. Odgovori na ova pitanja slede u tekstu.

Kritična infrastruktura

U svakom promenljivom sistemu postoji kritična tačka u kojoj on još uvek funkcioniše – kada je pređe njegove funkcije se ili menjaju ili prestaju. Granica pravilnog rada koja je određena ovim promenama predstavlja okvir kritične infrastrukture. Veliki broj država odredio je njima bitne (kritične) infrastrukture. U SAD je Predsednička komisija za zaštitu kritične infrastrukture 1997. godine odredila osnovne kritične infrastrukture – telekomunikacije, elektroenergetski sistem, skladištenje i transport nafte i gasa, bankarstvo i finansije, prevoz, sistem snabdevanja vodom, hitne službe i kontinuitet vlasti, i dala preporuke za njihovu zaštitu. Komisija je definisala kritičnu infrastrukturu kao onu koja je toliko vitalna da bi njeno onesposobljavanje ili uništenje imalo efekat oslabljivanja odbrambene i ekonomske sigurnosti SAD. U grupu kritičnih infrastruktura dodatno je uvrštena oblast informacija i komunikacija (računarska i telekomunikaciona oprema, softver, procesi i ljudi koji podržavaju procesuiranje, skladištenje i prenos podataka i informacija). U maju 1998. godine predsednik

SAD je odobrio predloge Predsedničke komisije i njegovom odlukom utvrđena je nacionalna politika za zaštitu kritičnih infrastruktura [12]. U okviru EU kritičnu infrastrukturu čine delatnosti, mreže, usluge, materijalna dobra i IT, čiji bi kvar ili uništenje znatno uticao na zdravlje, sigurnost i ekonomski prosperitet građana ili na ekonomiju vlada država članica. Indikativno je da različite države na različite načine određuju kritičnu infrastrukturu. Na primer, u okviru informacija i komunikacija kritične infrastrukture u Velikoj Britaniji, Švedskoj, Holandiji i Švajcarskoj su telekomunikacije, u Kanadi i Australiji su telekomunikacije i masovni elektronski mediji, u Nemačkoj telekomunikacije i komunikaciona infrastruktura, itd. Zanimljivo je i da se, iako svetska ekonomija preživljava finansijsku krizu, u područje javne i nacionalne bezbednosti, sa stanovišta kritične infrastrukture, ulažu velika sredstva. Po Kljajiću, Mandžuki i Škorputu (2010), Evropa, Australija, Kanada i SAD imaju šest istovetnih kritičnih infrastruktura: elektroenergetske sisteme, komunikacije, transport, zdravstvo, bezbednost i organe vlasti. Opciono kritične infrastrukture su i vodosnabdevanje, proizvodnja, skladištenje i prenos nafte i otrovnih materija, odbrambena industrija i pravosuđe [13].

Zaštita kritične infrastrukture

Definicije zaštite kritične infrastrukture razlikuju se zbog razlika u definicijama kritične infrastrukture. Jedna od njih je: „Zaštita kritične infrastrukture je strategija politike i spremnost koja je neophodna da bi se sprečio napad, odnosno pružio odgovor u slučaju da dođe do napada na kritične infrastrukture“. [14]. Sa stanovišta IB zaštita kritične infrastrukture predstavlja programe i aktivnosti koje realizuju vlasnici, korisnici, operateri, naučnoistraživačke institucije, vlada i regulatorna tela, radi održavanja performansi kritičnih infrastruktura u slučaju otkaza, napada ili incidenata, i minimizacije posledica i vremena oporavka. Evropska unija je 2009. godine usvojila akcioni plan zaštite koji je zasnovan na prevenciji i spremnosti za pojavu incidenata koji mogu da naruše bezbednost kritične infrastrukture, detekciji i odgovoru na narušavanje bezbednosti, oporavku od neželjenih događaja, međunarodnoj saradnji i Kriterijumima za kritične evropske infrastrukture iz oblasti IKT [15]. Jedan od elemenata Evropskog programa za zaštitu kritičnih infrastruktura je i Direktiva o identifikaciji i označavanju evropske kritične infrastrukture [16] po kojoj je IKT sektor deo kritičnih infrastruktura kojem treba posvetiti naročitu pažnju [17]. U Ruskoj Federaciji na nacionalnom nivou postoji strategija zaštite kritične infrastrukture, koja je definisana kroz Nacionalni koncept bezbednosti, aktivnosti Ministarstva informacionih tehnologija i komunikacija, i postojanje tima za reakciju na incidente [18]. U SAD je za svaku kritičnu infrastrukturu formirana posebna agencija koja izrađuje planove zaštite za da-

tu oblast [19]. Problemima zaštite kritičnih infrastruktura bave se i Organizacija ujedinjenih nacija (OUN), Organizacija za evropsku bezbednost i saradnju (OEBS), G-8 i Severnoatlanski savez NATO [20], kao i Svetska banka, Forum za reagovanje na incidente, Savet Evrope i drugi [21].

Srbija ne prati tempo okruženja, što je posebno simptomatično u odnosu na države članice EU (Mađarska, Rumunija, Bugarska). Naime, ove države su formirale timove za reakciju na incidente u kritičnim infrastrukturama – CERT (Computer Emergency Response Team, engl.) koji imaju i savetodavnu funkciju, u smislu prevencije i mera zaštite od incidenata u kritičnim infrastrukturama. Problemi sa kojima se Srbija suočava, a koje u skladu sa Strategijom mora da reši, su nepostojanje CERT-a, tehnička neopremljenost, malo stručnog kadra i neadekvatna međuinstitucionalna saradnja.

Kritična infrastruktura u Republici Srbiji

Odrediti kritične infrastrukture u Srbiji znači prvo proceniti da li neke infrastrukture odgovaraju navedenim grupama kritičnih infrastruktura (elektroenergetski sistemi, komunikacije, transport, organi vlasti), a odrediti kriterijume njihove bezbednosti znači primeniti unapred definisana pravila koja je odredila neka autorizovana institucija. Sa stanovišta IB, kriterijumi zaštite mogu da budu uređeni i primenom standarda, kao što su npr. ISO/IEC 27001-2 [22], [23].

U Srbiji ne postoji zvanična politika kojom bi bile utvrđene smernice za popisivanje domaćih kritičnih infrastruktura. Nacionalni Konvent o Evropskoj uniji (www.eukonvent.org), koji zastupa Evropski pokret u Srbiji (www.emins.org), definiše infrastrukturne oblasti za saobraćaj, enerrgetiku i telekomunikacije, i ukazuje na činjenicu da je stanje ovih infrastruktura poražavajuće, pogotovo sa stanovišta fizičke infrastrukture. Na svom prvom zasedanju ukazuju da jedino u domenu energetike postoje ugovorom definisane obaveze. Takođe, ukazano je na činjenicu da ne postoje relevantni podaci koji su neophodan preduslov za komparativne analize. Na drugom zasedanju Nacionalnog konventa formirana je radna grupa Infrastruktura, koja bi trebala da reši ove probleme, ali rezultati, ukoliko ih ima, još nisu dostupni javnosti. Pored aktivnosti Konventa, na XXVIII Simpoziju PosTel 2010. godine ukazano je na probleme upravljanja kritičnom infrastrukturom u okviru poštanske infrastrukture. U okviru navedenog ukazano je da su poslovi zaštite sve aktivnosti vlasnika/operatera, proizvođača, korisnika i regulatornih organa koje imaju za cilj očuvanje performansi kritičnih infrastruktura u slučaju nemogućnosti pružanja definisanog minimuma nivoa usluga, odnosno aktivnosti minimiziranja šteta i skraćenja vremena oporavka. Transportni i komunikacioni sistemi takođe predstavljaju kritične infrastrukturne sisteme, a osnoovni elementi upravlja-

nja kritičnom infrastrukturom u poštanskom sektoru su procena i upravljanje rizičnim situacijama koje mogu da ugroze upravljanje infrastrukturnih objekata [24]. Upravljanje rizikom predviđa mogućnosti prevencije rizičnih situacija, što ukazuje na preduzimanje adekvatnih mera za smanjivanje, ublažavanje ili eliminaciju rizika, i sanaciju posledica koje izazivaju zaustavljanje rada kritičnih infrastrukturnih sistema [25]. Pored navedenog, poljoprivredna proizvodnja koja zadovoljava potrebe države za sirovinama i proizvodima je, takođe, kritična infrastruktura sa stanovišta nacionalne bezbednosti, pogotovo ukoliko postoji mogućnost da ona bude element bioterorističkog napada [26]. Međutim, u Srbiji se teme vezane za kritičnu infrastrukturu sreću u okviru aktivnosti samo dva ministarstva: Ministarstva za infrastrukturu i energetiku (www.mie.gov.rs) i Ministarstva ekonomije i regionalnog razvoja (www.merr.gov.rs).

Ministarstvo za infrastrukturu i energetiku:

„Ministarstvo za infrastrukturu i energetiku obavlja poslove državne uprave u oblasti železničkog, drumskog, vodnog i vazdušnog saobraćaja, koji se odnose na: uređenje i obezbeđenje saobraćajnog sistema; realizaciju projekata izgradnje saobraćajne infrastrukture; unutrašnji i međunarodni prevoz i intermodalni transport; uređenje i bezbednost tehničko-tehnološkog sistema saobraćaja; obligacione i svojinsko pravne odnose; inspekcijski nadzor; strategiju razvoja saobraćaja, planove razvoja i planove vezane za organizaciju saobraćajnog sistema i organizaciju prevoza; izdavanje upotrebne dozvole za saobraćajni objekat i infrastrukturu; homologaciju vozila, opreme i delova; organizovanje finansijske i tehničke kontrole; međunarodne poslove u oblasti saobraćaja; stvaranje uslova za pristup i realizaciju projekata iz delokruga tog ministarstva koji se finansiraju iz pretpristupnih fondova EU, donacija i drugih oblika razvojne pomoći; mere za podsticanje istraživanja i razvoja u oblasti saobraćaja, kao i druge poslove određene zakonom. Ministarstvo za infrastrukturu i energetiku obavlja poslove državne uprave koji se odnose i na: energetiku, energetski bilans Republike Srbije, naftnu i gasnu privredu, bezbedan cevovodni transport gasovitih i tečnih ugljovodonika, nuklearna postrojenja čija je namena proizvodnja električne, odnosno toplotne energije, proizvodnju, korišćenje i odlaganje radioaktivnih materijala; preduzimanje mera radi obezbeđivanja uslova za funkcionisanje javnih preduzeća u oblastima za koje je ministarstvo obrazovano; nadzor u oblastima iz delokruga ministarstva, kao i druge poslove određene zakonom“.

Pored toga što radi pod nadzorom Vlade, Ministarstvo za infrastrukturu i energetiku nadležno je za javna preduzeća (JP Srbijagas, Naftna industrija Srbije (NIS), Elektroprivreda Srbije (EPS), Elektromreža Srbije (EMS), Železnice Srbije, Putevi Srbije, Jat Airways, Aerodrom „Nikola Tesla“) i agencije (za bezbednost saobraćaja, energetiku, energetsku efikasnost, kontrolu letenja Srbije i Crne Gore, Direktorat civilnog vazduho-

plovstva, Uprava za utvrđivanje sposobnosti brodova za plovidbu) koje obavljaju delatnosti iz odgovarajućih oblasti. Međutim, na osnovu javno dostupnih informacija, samo nekoliko preduzeća ima odeljenja, razvijene strategije ili planove vezane za kritične infrastrukture:

– Železnice Srbije imaju odeljenje za razvoj infrastrukture,

– EPS je definisala: (1) strateško planiranje u vezi sa proizvodnjom električne i toplotne energije i energije iz obnovljivih izvora, distribuciju, snabdevanje, i javno snabdevanje električnom energijom; (2) IT, što uključuje infrastrukturu, sistemski softver i specijalizovani softver za baze podataka; (3) telekomunikacije, što uključuje saradnju sa elektroenergetskim sistemima u okruženju, razmenu podataka prilikom upravljanja elektroenergetskim sistemima i vezu domaće telekomunikacione mreže sa mrežama susednih zemalja; (4) distributivne sisteme za izgradnju, revitalizaciju, unapređenje i modernizaciju opreme, sistema upravljanja potrošnjom, sistema telekomunikacija, sistema naplate električne energije, itd.

– JP Srbijagas, čije su funkcije transport i distribucija prirodnog gasa i upravljanje sistemima za transport i distribuciju; strateški ciljevi su intenziviranje razvoja gasovodne infrastrukture Srbije i povezivanje sa zemljama u okruženju, i revitalizacija postojećeg, proširenje i poboljšanje sistema nadzora i upravljanja gasovodnim sistemom.

– EMS ima Sektor za informatiku i telekomunikacije koji obavlja poslove u oblasti poslovne i upravljačke informatike i telekomunikacija, vrši sistemsku IT podršku i obezbeđuje funkcije telekomunikacionog sistema za potrebe upravljanja i prenosa u EMS.

Ministarstvo ekonomije i regionalnog razvoja:

Po Strategiji regionalnog razvoja Republike Srbije za period od 2007. do 2012. godine, ovog Ministarstva: “Saobraćajna infrastruktura je bitan faktor efikasnosti celokupnog saobraćajnog sistema, ali i ključni preduslov za ostvarivanje održivog privrednog i društvenog razvoja Republike Srbije i njenog integrisanja u EU“. Nisu tačno definisane karakteristike saobraćajnog sistema, način ulaganja sredstava za rekonstrukciju i razvoj, itd., osim što je konstatovano da je potrebno obratiti pažnju na saobraćajnu infrastrukturu.

Na osnovu prethodno navedenog, u Srbiji je moguće izdvojiti sledeće kritične infrastrukture, u skladu sa kritičnim infrastrukturama drugih država:

– saobraćaj, transport i komunikacije (putnički, poštanski, železnički, vazdušni, plovni, vodovodi, cevovodi, itd.),

– elektroenergetika (proizvodnja i distribucija električne i toplotne energije, naftna i gasna privreda i distribucija nafte i gasa, proizvodnja, korišćenje i odlaganje radioaktivnih materijala, itd.),

– telekomunikacije i IT.

Postoje infrastrukture koje neke organizacije ili institucije smatraju kritičnim za svoje poslovanje, za koje su one odredile načine održavanja, proširenja i razvoja. Međutim, rešenja na državnom nivou nema. U tom smislu, potrebno je odrediti raspoložive ljudske, materijalne, finansijske i druge resurse kako bi bili postignuti ciljevi u zadatim vremenskim rokovima, po dozvoljenom budžetu i uz zadovoljenje interesa svih strana učesnika u realizaciji ovakvog projekta [27]. Treba imati u vidu da, u realizaciji Strategije, treba da postoje dva pravca delovanja, jedan fokusiran na državni, a drugi na privatni sektor. Trenutno je kooperacija na nivou privatni sektor – država na dobrovoljnoj osnovi (i slaba), ali bi postojanje agencije za zaštitu kritične infrastrukture i CERT-a omogućilo Vladi da asistira u procesima razvoja kritičnih infrastruktura privatnog sektora [28]. Uticaj ovakvog „ponašanja" Vlade posebno je bitan kod onih grana privrede u kojima je izvršena privatizacija društvenog kapitala.

Informaciona bezbednost i zaštita kritične infrastrukture u Republici Srbiji

Komunikacije, izvori energije, transport, vodosnabdevanje, javne institucije i druge kritične infrastrukture u velikoj meri zavise od računarskih mreža čije su funkcije generisanja, obrade, skladištenja i prenosa podataka ranjive. Istraživanja pokazuju da onesposobljavanje računarskih mreža koje održavaju funkcije kritičnih infrastruktura može negativno da utiče na kvalitet života, destabilizuje ekonomiju, ugrozi nacionalnu bezbednost i slično [29]. Na koji način onda zaštititi kritičnu infrastrukturu sa stanovišta IB?

Jedno od mogućih rešenja je modularni, objedinjeni informacioni sistem (OIS) za kritične infrastrukture (OIS-u mogu da budu dodavane nove kritične infrastrukture[1], a svaka nova infrastruktura je novi modul). Objedinjeni informacioni sistem sadrži tri komponente: hardver, softver i personal, a njegovu funkciju određuju i podaci sa terena. Hardver čine računari (PC, laptop), prateća oprema (monitori, štampači) i oprema za prikupljanje podataka (GPS, radne stanice). Softver je delom autohton, a delom integrisan. Integrisanost obezbeđuje interoperabilnost različitih infrastruktura, u smislu prikupljanja, obrade i razmene podataka. Personal podrazumeva edukovane osobe čiji su zadaci nadzor, upravljanje i obrada podataka bitnih za funkcionisanje OIS-a. Osnova OIS-a je softver (na serveru) koji služi za prikupljanje i integraciju podataka u jedinstvenu bazu, i njihov prenos putem računarskih mreža. Drugi deo softvera OIS-a je softver za rad pojedinih resursa (desktop računar, laptop, resursi za udaljenu komunikaciju) koji služi za pristup lokalnim bazama podataka i za obradu, analizu, uređivanje i administraciju tih podataka. Komunikacija

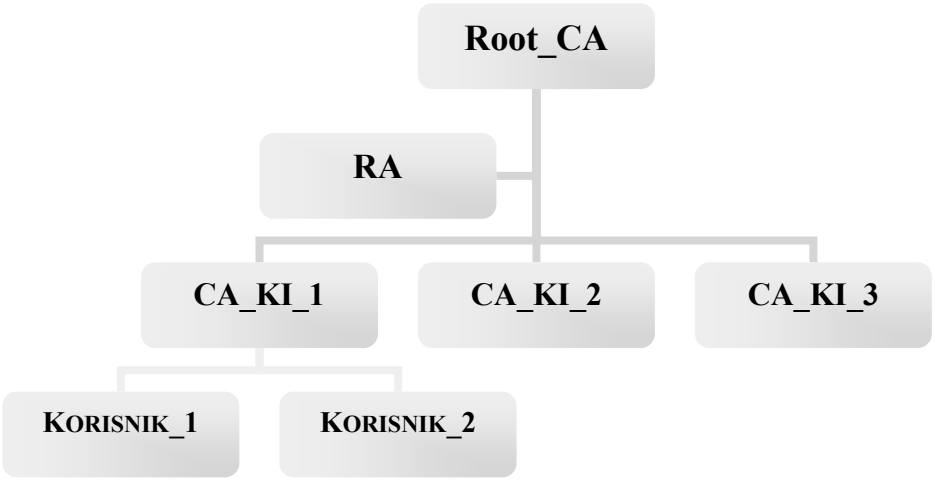
[1] Predlog rešenja daje autorka, na osnovu javno dostupnih komercijalnih rešenja u svetu.

Protić, D., Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine: bezebednost informacija i kritična infrastruktura, pp. 82–101

unutar OIS-a može i ne mora da bude zaštićena, u zavisnosti od stepena tajnosti podataka određene kritične infrastrukture. Svaka kritična infrastruktura može da ima različit, sopstveni korisnički interfejs. Neophodan je 24/7 monitoring svih funkcija i infrastrukture, a posebno je bitno da personal bude dobro obučen i po potrebi doobučavan. Kraljevina Norveška donirala je Srbiji web-baziran geografski informacioni sistem (Web GIS), user-friendly aplikaciju koja dozvoljava prostorno planiranje i analizu podataka dobijenih na osnovu karata različitih domena, kao što su: komunikacije (putevi, pruge, nadvožnjaci, tuneli), elektroenergetski sistemi (hidro i termo elektrane, dalekovodi, trafo-stanice), granice naselja i administrativnih oblasti, privredni objekti, turistički sadržaji, reljef, itd. (www.mem.gov.rs). Primenom aplikacija sličnih Web GIS aplikaciji moguće je urediti okvir za jedan interoperabilni OIS. Zaštitu informacija u OIS-u moguće je obezbediti primenom infrastrukture sa javnim ključevima (PKI[2]), koja je definisana standardom ITU-T X.509. PKI čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata, kroz sertifikaciono (CA[3]) i registraciono telo (RA[4]). Sertifikaciono telo je izdavalac sertifikata, strana od poverenja koja je za sve učesnike u komunikaciji centralni autoritet, a RA je entitet odgovoran za identifikaciju učesnika u komunikaciji, i kreator zahteva za dodelu sertifikata. Sertifikat je, uslovno, dozvola za razmenu podataka na zaštićen način između korisnika, koji mogu biti pravna ili fizička lica. Spisak digitalnih sertifikata je javan podatak, može se nalaziti na web sajtu agencije za dodelu sertifikata ili biti dostupan na drugi način. U opštem slučaju, učesnici u komunikaciji nemaju uspostavljen lanac poverenja kako bi zaštićeno komunicirali. Zbog toga se oni odlučuju da veruju sertifikacionom telu. Na drugoj strani, pre nego što izda digitalni sertifikat, CA proverava podatke korisnika koji je podneo zahtev za izdavanje sertifikata, a proveru njihove tačnosti vrši posredstvom RA, odnosno, da bi korisnik uopšte mogao da dobije digitalni sertifikat, potrebna je prvo provera podataka, nakon čega sledi proces registracije. Posle uspešne provere, CA izdaje digitalni sertifikat, koji javno objavljuje i koji garantuje identitet korisnika. U slučaju da je korisnik institucija, digitalni sertifikat izdaje se korisničkim serverima, zbog čega postoji faza predregistracije u kojoj institucija dostavlja podatke i o osobama koje će biti ovlašćene da podnose zahteve za sertifikat za potrebe te institucije. Nivo provere identiteta zavisi od tipa sertifikata, što je uslovljeno stepenom poverljivosti podataka, a definisano dokumentom koji predstavlja politiku sertifikacije [30]. Digitalni sertifikat ima određeni rok trajanja, ali može biti privremeno ili trajno ukinut u slu-

[2] PKI – Public Key Infrastructure, engl.
[3] CA – Certification Authority, engl.
[4] RA – Registration Authority, engl.

čajevima kao što su kompromitacija podataka, na zahtev korisnika, i slično. IB u PKI zasnovana je na poverljivosti, integritetu i dostupnosti podataka, dok bezbedna komunikacija podrazumeva i autentikaciju, integritet, tajnost i neporecivost. Autentikacija je proces identifikacije učesnika u komunikaciji, integritet garantuje da nije došlo do izmene podataka na putu od izvora do odredišta, tajnost garantuje da su podaci dostupni samo onima kojima su namenjeni, a neporecivost obezbeđuje da korisnik koji je učestvovao u procesuiranju podataka ne može da porekne takvu aktivnost. Na koji način će u određenoj PKI korisnici tražiti, dobijati i koristiti svoje digitalne sertifikate zavisi od njegove potrebe da zaštite svoje podatke ili komunikaciju jednom od navedenih metoda. Na slici 1. prikazan je primer realizacije jedne PKI.



Slika 1 – Infrastruktura sa javnim ključevima
Figure 1 – Public Key Infrastructure

Glavno sertifikaciono telo Root_CA u ovoj infrastrukturi izdaje digitalne sertifikate za komunikaciju između tri kritične infrastrukture: CA_KI_1, CA_KI_2 i CA_KI_3, tako da sve kritične infrastrukture mogu zaštićeno da razmenjuju podatke. Međutim, CA_KI_1 takođe može da izda sertifikate svojim potčinjenim korisnicima (KORISNIK_1 i KORISNIK_2), na osnovu sertifikata koji je dodelio Root_CA. Na primer, CA_KI_1 može biti glavni server neke organizacije, a korisnici fizička lica kojima su dodeljeni sertifikati za pristup industrijskim tajnama, ulazak u prostorije posebnih namena, upravljanje automatizovanim proizvodnim procesima, i slično.

Posmatrano sa stanovišta OIS-a, problemi vezani za integraciju kritičnih infrastruktura u direktnoj su vezi sa zaštićenom komunikacijom. Malo je organizacija i institucija u Srbiji koje su registrovale svoja sertifikaciona tela

Protić, D., Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine: bezebednost informacija i kritična infrastruktura, pp. 82–101

[31]. U ovom trenutku postoje tri registrovana CA javnih institucija u Srbiji: Ministarstva unutrašnjih poslova Republike Srbije (MUP), javnog preduzeća PTT saobraćaja „Srbija“ (Pošta) i Privredne komore Srbije (PKS), i jedno sertifikaciono telo akcionarskog društva Halcom a.d. Na sajtovima ovih institucija postoje obrasci zahteva za izdavanje digitalnih sertifikata. Na 35 lokacija u Srbiji dostupni su kvalifikovani elektronski sertifikati Sertifikacionog tela Pošte. Digitalni sertifikati ovog tela namenjeni su svim učesnicima e-poslovanja u Srbiji, kako fizičkim, tako i pravnim licima (državna uprava, lokalna samouprava, javne službe, preduzeća, banke, osiguravajuća društva, organizacije, institucije). Primena CA Pošte počela je 2008. godine, i to je najstarije CA telo u državi [32]. Sertifikaciono telo PKS (PKS CA) uspostavljeno je 2009. godine. Ono je pravno lice čiji su elektronski sertifikati, u skladu sa odredbama Zakona o elektronskom potpisu, namenjeni svim učesnicima u e-poslovanju u Srbiji [33]. Od 2010. MUP primenjuje Ugovor o izdavanju i korišćenju kvalifikovanih elektronskih sertifikata na ličnoj karti sa čipom, na osnovu Zakona o elektronskom poslovanju, Uredbe o određivanju MUP-a za izdavanje kvalifikovanih elektronskih sertifikata i Odredbe o upisu podataka u obrazac lične karte. Sertifikaciono telo je obeleženo kao MUP CA, a u ugovoru koji potpisuje korisnik definisana su prava i obaveze obe strane [34]. Od 2010. godine Halcom a.d. deluje na polju e-bankinga, elektronskih obrazaca sa digitalnim potpisom, arhiviranju digitalno potpisanih dokumenata, klirinških sistema i upotrebe PKI tehnologije za zaštitu podataka [35].

Po standardu ITU-T X.509, registrovana CA formiraju javno dostupan dokument Pravila rada sertifikacionog tela koji mora, između ostalog, da sadrži podatke o učesnicima u PKI, načinu autentikacije i identifikacije korisnika, operativnim zahtevima u vezi životnih ciklusa i validnosti sertifikata, načinu upravne, operativne i bezbednosne kontrole, itd. U okviru ovog dokumenta nalaze se i imena odgovornih lica, identifikacione oznake politike sertifikacije, identifikacione oznake institucije koja izdaje Pravilo o radu sertifikacionog tela, itd.

U slučaju OIS-a, bilo bi potrebno je registrovati glavno sertifikaciono telo Root_CA, koje bi izdavao digitalne sertifikate svakoj kritičnoj infrastrukturi. Zaštićena komunikacija u okviru OIS-u bi na ovaj način bila omogućena pomoću digitalnih sertifikata u okviru definisanog PKI. Root_CA trebao bi da bude uvršćen u republički spisak sertifikacionih tela.

Zaključak

Rastući problem IB je posledica razvoja sistema za procesuiranje informacija, pomoću kojih je moguće veliki broj podataka generisati, obraditi, skladištiti ili prenositi elektronskim putem. U zavisnosti od stepena poverljivosti, informacije je potrebno zaštititi tako da ne postanu dostupne

osobama s malicioznim namerama, pa je IB postala gorući problem za organizacije i institucije različitih delatnosti. Savremene države prihvataju zajednički model „ponašanja“, kako bi obezbedile zaštitu svojih (kritičnih) infrastruktura. Formirana su nacionalna tela za reagovanje u kriznim situacijama, donesene strategije razvoja na različitim nivoima društva, primenjeni standardi za IB, itd. Dok države iz okruženja primenjuju metodologiju EU za zaštitu kritičnih infrastruktura, Srbija u ovoj oblasti kasni. Postoje pojedinačni pokušaji da organizacije ili institucije zaštite svoje infrastrukture koje smatraju kritičnim, što je posebno uočljivo kod saobraćaja, transporta, elektroenergetskih sistema, u domenu telekomunikacija i primeni IKT. Ipak, globalni plan na republičkom nivou ne postoji.

Jedno je od mogućih rešenja problema zaštite u kritičnim infrastrukturama je OIS Republike Srbije. Objedinjavanjem informacionih sistema različitih, prethodno popisanih kritičnih infrastruktura, moguće je pratiti rad svake od njih i obezbediti interoperabilnost. Moguća je i razmena informacija sa državama iz okruženja. Podaci i razmena podataka u okviru OIS-a mogu da budu zaštićeni primenom PKI. S obzirom na to da je OIS organizovan tako da je informacioni sistem svake kritične infrastrukture „podređen“ OIS-u, IB može biti obezbeđena infrastrukturom sa javnim ključevima, u kojoj bi postojali zajedničko sertifikaciono telo Root_CA, a svaka kritična infrastruktura ponaosob imala bi svoje sertifikaciono telo CA_KI.

U Srbiji je u Registar sertifikacionih tela upisano samo četiri organizacije, pa je očito da postoje problemi oko registracije CA. Ipak, ukoliko na osnovu Strategije budu postojale aktivnosti za popis i primenu IB u kritičnim infrastrukturama, upis novog sertifikacionog tela ne bi trebao da predstavlja problem. Međutim, neophodno je prvo popisati kritične infrastrukture, potom formirati CERT, zatim tehnički i organizaciono podržati OIS i uskladiti informacione sisteme pojedinih kritičnih infrastruktura, otkloniti nedostatke koji mogu da budu uočeni tokom probnog rada, i podneti zahtev za upis CA u Registar. Operativna upotreba OIS-a bi, u kratkom periodu, obezbedila relevantne podatke za naučno-istraživački rad i razmenu podataka sa drugim državama, što bi ubrzalo razvoj drugih pravaca delovanja koji su prioriteti Strategije.

Literatura

[1] Commission of the European Communities, Commission staff working Document, Accompanying document to the communication from the commission to The European Parliament, The Council, The European Economic and Social committee and The Committee of the Regions, *i 2010 – Annual Information Society Report 2007 {COM(2007) 146 final}* Brussels, 30. 3. 2007, SEC(2007) 395, Volume 3, Dostupno na http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2007/sec_2007_395_en_documentdetravail3_p.pdf.

[2] European Commission, Communication from the Commission Europe 2020, A Strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels, 3. 3. 2010. Dostupno na http://eunec.vlor.be/detail_bestanden/doc014%20Europe%202020.pdf.

[3] Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, 2010, *Službeni Glasnik Republike Srbije* br. 5/2010, Dostupno na http://paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.htm.

[4] Zakon o tajnosti podataka – Ukaz o proglašenju, 2009, *Službeni glasnik Republike Srbije*, br. 104/2009, Dostupno na www.yucom.org.rs/upload/vestgalerija_77_4/1263380892_GS0_Zakon_o_tajnosti_podataka.pdf.

[5] Zakon o zaštiti podataka o ličnosti, 2008., *Službeni glasnik Republike Srbije*, br. 97/08, Dostupno na www.poverenik.org.rs/index.php/yu/doc/zakoni/52-zakon-o-zastiti-podataka-o-licnosti.

[6] Zakon o elektronskom potpisu, 14. 07. 2009., *Službeni glasnik Republike Srbije*, br. 51/2009, Dostupno na http://ca.mup.gov.rs/zakon%20o%20elektronskom%20potpisu.pdf.

[7] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, 2009., *Službeni glasnik Republike Srbije* br. 61/2005, 104/2009, Dostupno na http://zakon.co.rs/zakon-o-organizaciji-i-nadleznosti-drzavnih-organa-za-borbu-protiv-visokotehnoloskog-kriminala.html.

[8] Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, 2009., *Službeni glasnik Republike Srbije* br. 88/2009, Dostupno na http://paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html.

[9] Krivični zakonik, 2009., *Službeni glasnik Republike* Srbije, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009 i 111/2009, Dostupno na http://paragraf.rs/propisi/krivicni_zakonik.html.

[10] Zakon o telekomunikacijama, 2006., *Službeni glasnik Republike Srbije* br. 44/2003 i 36/2006, Dostupno na www.mtid.gov.rs/wp_content/uploads/Dokumenti/Zakoni/Zakon_o_telekomunikacijama.pdf.

[11] Zakon o odbrani, 2009., *Službeni glasnik Republike Srbije* br. 116/2007, 88/2009, 88/2009 – dr. zakon i 104/2009 – dr. zakon, Dostupno na http://paragraf.rs/propisi/zakon_o_odbrani.html.

[12] O'Neil M. J., J. X. Dempsey, 1999/2000., Critical infrastructure protection: Threats to privcay and other civil liberties and concerns with government mandares or industry, *Depaul Business Law Journal*, Vol 12, pp. 97.

[13] Kljajić, Z., Mandžuka, S., Škorput, P., 2010., Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskom zemljama, *18. Telekomunikacioni forum TELFOR 2010. Srbija*, pp. 75–78.

[14] Lewis, G., 2006., Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation, John Wiley & Sons Inc., Hoboken, New Jersey (USA).

[15] Critical information infrastructure protection, 29. 06. 2011. Dostupno na http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

[16] CIIP Action Plan in its Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacked cyberdisruptions: enhancing, preparedness, security and resilience' – COM (2009) 149, 2009. Dostupno na http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

[17] Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, *EN Official Journal of the European Union* L 345/75, 23. 12. 2008. Dostupno na http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[18] Bruner, E., Suter, M., International CIIP Handbook 2008/2009. *Center for Security Studies*, ETH Zurich.

[19] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection, 17. 12. 2003. Dostupno na http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[20] Vuletić, D., 2011., Zaštita kritičnih informacionih infrastruktura, *Zbornik radova Konferencije o bezbednosti informacija 2011*, pp. 55–60.

[21] Buckland, B. S., Schreier, F., Winkler, T. H., 2010., Democratic Governance Challenges of Cyber Security. Annex 2, DCAF, Geneva, Switzerland.

[22] ISO/IEC 27001:2005., 2005., Information technology – Security techniques – Information security management systems.

[23] ISO/IEC 27002:2005., 2007., Information technology – Security techniques – Code of practice for information security management.

[24] Bojović, N., Knežević, N., Macura, D., Milenković, M., 14–15. 12. 2010., Model upravljaja kritičnom infrastrukturom za održivi razvoj poštanskog srktora, *XXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel.*

[25] Karović, M. S., Komazec, N. M., 2010., Upravljanje rizicima kao preduslov integrisanog menadžment sistema u organizaciji, *Vojnotehnički glasnik/Military Technical Courier,* Vol. 58, No. 3, pp.146–161.

[26] Radosavljević, V., Stojković, K., Anđelković, R., Andrejić, M., 2010., Agroterorizam kao akuelni izazov, *Vojnosanitetski pregled*, Volumen 67, Broj 11, pp. 933-940.

[27] Andrejić, D. M., Đorović, D. B., Pamučar, D. D., 2011., Upravljanje projektima po pristupu projekt menadžmenta, *Vojnotehnički glasnik/Military Technical Courier,* Vol. 59, No. 2, pp.142-157.

[28] O'Neil, M. J., Dempsey, J. X., 1999/2000., Critical infrastructure protection: Thereats to privacy and other civil liberties and concerns with government mandates on industry, *Depaul Business Law Journal*, Vol 12, p. 97.

[29] Gellman, V., october 2002., U. S. Friends Clues to Potential Cyber-attack, *The Mercury News* (June 27, 2002), *First Monday*, Volume 7, Number 10, Dostupno na http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/998/919

[30] Kovinić, M., 2010., Uvod u kriptografiju i infrastrukturu javnih ključeva, *Akademska mreža Srbije*, pp. 4–10.

[31] Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata, januar 2012. Dostupno na http://www.digitalnaagenda.gov.rs/aktivnosti/euprava/elektronski-potpis/registar-sertifikacionih-tela/.

[32] PKI i Sertifikaciono telo pošte, januar 2012. Dostupno na www.ca.posta.rs.

[33] PKS, Izdavanje kvalifikovanih elektronskih sertifikata, 2012. Dostupno na http://217.24.23.93/Usluge.aspx?IDUsluge=4.

[34] Opšti postupak izdavanja kvalifikovanog elektronskog sertifikata MUP (na ličnoj karti), januar 2012. Dostupno na http://www.euprava.gov.rs/eusluge/opis_usluge?generatedServiceId=558.

[35] Halkom BG CA, 2012. Dostupno na http://www.halcom.rs/index.php?section=4#Q.

THE STRATEGY FOR THE DEVELOPMENT OF INFORMATION SOCIETY IN SERBIA BY 2020: INFORMATION SECURITY AND CRITICAL INFRASTRUCTURE

FIELD: IT
ARTICLE TYPE: Original Scientific Paper

Summary:

The development of technology has changed the world economy and induced new political trends. The European Union (EU) and many non-EU member states apply the strategies of information society development that raise the level of information security (IS). The Serbian Government (Government) has adopted the Strategy for Information Society in Serbia by 2020 (Strategy), and pointed to the challenges for the development of a modern Serbian information society. This paper presents an overview of the open-ended questions about IS, critical infrastructures and protection of critical infrastructures. Based on publicly available data, some critical national infrastructures are listed. As a possible solution to the problem of IS, the Public Key Infrastructure (PKI)-based Information security integrated information system (ISIIS) is presented. The ISIIS provides modularity and interoperability of critical infrastructures both in Serbia and neighboring countries.

Introduction

The development of information society that is the result of the information and communication technologies (ICTs) development influenced changes in all aspects of life. Businesses are more effective, paper documentation is reduced, communication with customers and business partners is faster and easier, etc. At the same time, confidential information can be modified, destroyed or become available to unauthorized people. That is why the information protection is in the focus of the public eye. It caused a new way of business planning, standardization and changes in the law. The rapid technology development has led to the occurrence of complex

systems, and induced the occurrence of strategies for the sustainable development. In general, strategy frameworks are comprised of tasks that must be carried out, time for the realization of those tasks, budget, etc.

According to the EU trends for the development of the information society, ICTs are one of the factors that influence economic growth and development. Following the trends, Government has determined essential factors that would affect development of the information society in Serbia by 2020 – one of these is information security. Government's priorities are legal and institutional frameworks for IS, fight against cyber crime, scientific research, and critical infrastructure protection. However, critical infrastructures in Serbia have not been listed yet, so it is impossible to control them and monitor their work.

In this paper, Serbian infrastructures which are considered to be critical are listed and compared to the known world's critical infrastructures. The IS of critical infrastructures is achieved by ISIIS that is also presented in this paper. ISIIS provides IS, modularity and interoperability amongst different organizations and institutions.

The Strategy for the development of the information society in Serbia by 2020

The strategy should follow the challenges of ICTs (new aspects of security, technological dependence, lack of interoperability, open questions of intellectual property protection, etc.). Government has authorized the Ministry of Telecommunications and Information Society, and other government authorities for the development and implementation of information systems activities within its jurisdiction. Strategy priority areas are: e-communication, e-government, health and justice, ICT in education, science and culture, e-commerce, ICT in business, and IS. IS means to protect the information system, data and infrastructure in order to preserve confidentiality, integrity and availability of information. Government's goal is to achieve the trust of information system users. To improve the legal framework Government improved legal procedures, but did not make additional regulations to determine standards for IS. It is necessary to promote the protection of critical infrastructure against attacks using information technology (IT). It is also necessary to determine critical infrastructures according to the IS and the data protection measures, as well as to examine possible attacks to critical infrastructures.

Open issues on information security within the Strategy

New aspects of IS are the challenges of information society development. The parts of the Strategy related to the regulations indicate that there are existing laws and organizations that support the development of the information society, but insufficient interoperability between institutions has been noticed as well as lack of data for the analysis of the information society development, etc. That is why there are some open questions about the possibility of protection against attacks on IS. One of the issues relates to the unknown number of critical infrastructures in Serbia in terms of critical infrastructure information protection.

A number of states determine their critical infrastructures in different ways. For the U.S. these are telecommunications, power systems, storage and transport of oil and gas, banking and finance, transporta-

tion, water supply, emergency services, information and communication. The U.S. critical infrastructure is defined as one that is so vital that its disabling or destruction would weaken the defense and economic security. The EU critical infrastructure consists of services, networks, IT and material goods, whose damage or destruction could have a considerable impact on health, safety and economic prosperity of the citizens or the economy of member state governments, etc.

Data protection relates to the activities implemented by owners, users, operators, research institutions, government and regulatory authorities, in order to maintain the performance of critical infrastructure in case of incidents or attacks on the IS, by minimizing the effects of such events and reducing recovery time. The EU has adopted an action plan for IS based on the activities of prevention and preparedness for the occurrence of incidents that can harm information systems, detection and response to it, mitigation and recovery from unwanted events, international cooperation, etc. The Russian Federation also has a strategy for critical infrastructure protection that is determined by the National Security Concept. In the U.S., separate agencies for each critical infrastructure have been established by the government. The United Nations, OSCE, G-8, NATO, World Bank, Council of Europe, and many other organizations are also interesred in critical infrastructues and IS.

Serbia does not follow the region. Countries which are EU-members have established emergency teams – CERTs (Computer Emergency Response Teams), which also provide educational help about the prevention and protection against IS accidents. Problems that Serbia faces with are the absence of CERT, inadequate technical equipment, lack of professionals and inefficient cooperation among institutions.

There is no official policy in Serbia about critical infrastructure protection. The National Convent on the EU founds transport, energy and telecommunications devastating. The PosTel Symposium 2010 pointed to the critical management problems of postal infrastructure. Transportation and communication systems are also recognized as critical infrastructures, etc. The infrastructures in Serbia are responsibility of the Ministry of Infrastructure and Energy and the Ministry of Economy and Regional Development. The Ministry of Infrastructure and Energy performs activities of transport, oil and gas industry, transfer of toxic materials, supervision of the power systems, etc. The Ministry of Economy and Regional Development drew attention to transport in Serbia and nothing else. Based on the above, there are the following critical infrastructures in Serbia: transportation, communications, electrical power systems, IT and telecommunications.

A possible solution to the problem of IS in Serbia's critical infrastructures is ISIIS, which consists of hardware, software and well-educated personnel. Its function is also determined by collected data. Hardware consists of computer networks, supporting equipment and devices for remote access. Software for integration of different information systems ensures interoperability (collecting, processing and exchanging information amongst critical infrastructures). A part of software is used for accessing the databases

and for performing data processing. The complexity of hardware and software is the main reason why personnel have to be properly trained. Also, 24/7 monitoring of all ISIIS functions and infrastructure is needed. Norway has donated Serbia Web GIS application for regional planning and analysis of data obtained at the basis of maps in different domains such as communications, border settlements, electrical power systems, relief, etc. It is possible to develop ISIIS using applications that are similar to the Web GIS.

The IS at OIS is based ob PKI that provides authentication of the participants as well as integrity, confidentiality and non-repudiation of data. PKI includes hardware, software, policies and procedures, which are necessary for managing, generating, storing and distribution of cryptographic keys and digital certificates. The Certification Authority (CA) generate certificate. The Registration Authority (RA) is the creator of certificate, but it is not authorized to generate it. The CAs in Serbia are assigned to Halcom, police, post office and Serbian Chamber of Commerce (SCC). The register of CAs is available on the website www.digitalnaagenda.gov.rs. To implement OIS, it is necessary to register root_CA, which generates CA_KI. In that way, secure communications will be granted only to authorized persons.

Conclusion

Depending on confidentiality, information has to be protected and become unavailable to people with malicious intentions. Modern countries accept the common model of "behavior" to protect theirs critical infrastructures. CERT's work, development strategies are evolved, standards applied, etc. The countries in the region implement this methodology, but Serbia is lagging behind. There is no national plan about critical infrastructures, although there are some attempts of organizations and institutions to number them. The solution to the problem of IS offers OIS that monitors all critical infrastructures, and provides modularity and interoperability. The exchange of Information is protected by a PKI system. Since OIS is organized so that each critical infrastructure subordinates to a central information system, its IS is enabled by PKI, root_CA and CA_KI.

Only four organizations from Serbia are registered in the Serbian Register of CAs. Obviously there are some problems with the registration. However, by the Strategy, the registration of a new CA should not be a problem anymore. Still, the necessity is to make a list of critical infrastructures, establish CERT, do technical and organizational support to OIS, and coordinate critical infrastructure information systems to registrate a CA. OIS's everyday operation will ensure data for further research in a short time. The positive result will also be the development of other Strategy topics.

Key words: *information security, critical infrastructure, development strategy.*

Datum prijema članka/Paper received on: 29. 12. 2011.
Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 15. 02. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 17. 02. 2012.