Sajber bezbjednost u Republici Srpskoj/Bosni i Hercegovini sa naglaskom na energetski sektor

Dr Mihajlo Travar
Član komisije
Regulatorna komisija za energetiku Republike Srpske
Trebinje, RS/BiH
mihajlo.travar@reers

ma Dragana Travar
Univerzitet Singidunum
Beograd, Srbija
travardragana86@gmail.com

mr Igor Dugonjić
Odjeljenje za planiranje i upravljanje medicinskim tehnologijama UKC RS
Banja Luka, RS/BiH
igor.dugonjic@kc-bl.com

Saša Ristić
Sektor za razvoj poslovanja
Lanaco informacione tehnologije
Banja Luka, RS/BiH
sristic1992@gmail.com

***Sažetak*— Sajber prostor je postao značajna komponenta društva s obzirom da institucije, energetski i finansijski sektor, školstvo pa i cjelokupan društveni život zavisi od interneta i međusobne povezanosti. Na prostoru RS/BiH značajno mjesto zauzima energetski sektor te je njegova bezbjednost osnov funkcionisanja same države. Energetski i sektor informaciono komunikacionih tehnologija predstavljaju dvije tehnološke grane koje djeluju sinergetski na razvoj cjelokupnog društva. Odstupanja od ispravnog rada informacionih sistema ili dijelova u energetskom sektoru ne predstavjaju samo tehničke smetnje, već znatno veću bezbjedonosnu opasnost. S obzirom na trendove povećanja sajber napada na energetske sisteme, važno je razmotriti bezbjedonosne aspekte integracije IKT tehnologija, te predvidjeti alate, procedure, tehnologije i kadrove kako bi energetski sistemi mogli savladati bezbjednosne izazove koji su pred njima.**

Ključne riječi: sajber bezbjednost; energetika; IKT; mreža.

I. UVOD

Cilj ovog rada je da ukaže na značaj bezbjednosti informaciono-komunikacionih tehnologija za energetski sektor i društvo u cjelini te podstakne odgovarajuće državne organe da percipiraju ovo pitanje kao jedno od prioritetnih. Takođe, cilj je da se unaprijedi saradnja svih relevantnih subjekata na unutrašnjem i međunarodnom nivou radi povećanja kapaciteta za efikasnu borbu protiv sajber kriminaliteta.

Društveni razvoj u XXI vijeku usko je povezan i na određene načine uslovljen razvojem informacionih tehnologija. Danas, svaki korisnik interneta ima mogućnost da koristi sve benefite savremenih informacionih tehnologija bez obzira na geografsku pripadnost, razvijenost zemlje ili privrede u kojoj pojedinac ili kompanija egzistira. Razvoj tehnologije donio je sa sobom i nova zanimanja ili bolje reći profesije. Postoje brojna istraživanja o tome koja su to zanimanja ili vještine koja će na direktan ili indirektan način nastati pod uticajem tehnologije.[1] Najčešće se govori u afirmativnom smislu, međutim, pored svih pozitivnih efekata koji su se desili i desiće se, cjelokupnu situaciju je potrebno sagledati i sa druge strane, odnosno razmotriti pitanje negativnih efekata koje tehnologija nosi sa sobom. Jedan od pojavnih oblika sve masovnije primjene savremenih tehnologija je sajber kriminalitet. Ova pojava nosi sa sobom značajne prijetnje čije posljedice su dalekosežne i dovode u pitanje normalno funkcionisanje kako pojedinaca tako i institucija na nacionalnom i globalnom nivou. Takođe, značajno je usmjeriti fokus na trenutne regulative domaćeg ali i zakonodavstva Evropske unije koji se bave pitanjima sajber kriminala i posljedično tome sajber bezbjednosti. Evropska Unija je dala definiciju sajber kriminala: „Sajber kriminal je globalni problem koji prevazilazi fizičke granice i predstavlja sva krivična djela koja su počinjena putem interneta uz pomoć informacionih sistema i računarskih mreža uključujući kriminalne radnje specifične za internet, internetske prevare i krivotvorenja te iliegalni sadržaj na internetu”[2]. Pojam sajber bezbjednost možemo definisati kao odbranu računara, servera, mobilnih uređaja, elektronskih sistema, mreža i podataka od zlonamjernih napada. Izraz se primjenjuje u različitim kontekstima, od poslovnih do mobilnih sistema, a može se podijeliti u nekoliko kategorija kao što su: mrežna bezbjednost, aplikativna, operativna, obezbjeđenje normalnog poslovanja i edukacija krajnjeg korisnika[3]. Ovim problemima su svakako najviše pogođene visoko razvijene ekonomije ali ni zemlje u tranziciji ili nerazvijene zemlje nisu zaštićene od uticaja na polju sajber bezbjednosti i kriminaliteta. Ako govorimo o prostoru Republike Srpske odnosno Bosne i Hercegovine, dodatne komplikaciju u borbi protiv ovakvih oblika kriminala mogle bi se manifestovati kroz najmanje dva pitanja. Prvo se tiče spremnosti države i njenih institucija da adekvatno odgovore na izazove koje sa sobom nosi sajber prostor (usvojena zakonska regulativa i

usklađenost iste sa zakonima Evropske unije). Drugo je pitanje spremnosti šire društvene zajednice da se uključi i edukuje o bezbjednosti na internetu.

Na tragu zakonodavnog okvira koji reguliše pitanja sajber bezbjednosti a koji Vlada Republike Srpske planira usvojiti tokom 2020. godine, kroz rad posebno želimo naglasiti potrebu zaštite podataka u energetskom sektoru. Ovaj sektor je od fundamentalnog značaja za funkcionisanje Republike Srpske sa dugom tradicijom i značajnim potencijalima za daljnji razvoj. Podaci koji se generišu radom energetskog sektora direktno su upućeni na građane i privredu pa je zaštita tih podataka ključna. Nadamo se da će ovaj rad i slični radovi, pokrenuti široku raspravu o pitanjima bezbjednosti podataka u energetskom sektoru i na koncu ova pitanja uvrstiti na dnevni red budućih konferencija poput Energetskog samita koji se 2020. godine odžava u Republici Srpskoj.

II. SAJBER BEZBJEDNOST U REPUBLICI SRPSKOJ I BOSNI I HERCEGOVINI

Bosna i Hercegovina kao i sve zemlje u okruženju pa i EU suočava se sa problemima sajber bezbjednosti i izazovima na tom polju. Prema podacima Centralne Obavještajne Agencije iz 2018. godine u Bosni i Hercegovini živi oko 3.856.000 stanovnika.[4] Pri tome Regulatorna agencija za komunikaciju iznijela je podatke prema kojima je stopa korišćenja interneta u 2015. godini iznosila 72,41%[5] dok je u narednim godinama broj korisnika interneta u Bosni i Hercegovini imao tendenciju rasta te je iznosio 86,77%[6] Ovakvo povećanje korišćenja interneta dovelo je do toga da se Bosna i Hercegovina pozicionira na 83. mjesto Međunarodne unije za telekomunikacije.[7] Ministarstvo bezbjednosti je iniciralo donošenje nekoliko dokumenata koji se bave pitanjima sajber bezbjednosti a te dokumente je usvojio i Savjet ministara BiH. Najznačajniji izvještaji su:

1. Strategija za uspostavljanje CERT-a (Computer Emergency Response/Readiness Team) u Bosni i Hercegovini (2011) – prvi dokument na državnom nivou koji se bavi pitanjima sajber bezbjednosti
2. Strategija za borbu protiv organizovanog kriminala u Bosni i Hercegovini (2017-2020)
3. Strategija za borbu protiv terorizma (2015-2020)

U izvještaju Cybersecurity the Western Balkans[8] ocjenjuje se da Bosna i Hercegovina nije dovoljno napredovala na polju borbe protiv visokotehnološkog kriminala. Jedan od problema je neusklađenost zakonodavstva između entiteta i državnog nivoa. Takođe, određene međunarodne strategije nisu implementirane u domaće zakonodavstvo. Republika Srpska je na entitetskom nivou preduzela određene mjere sa ciljem suzbijanja kriminaliteta ovog tipa a mjere se odnose na izgradnju pravnog okvira, strateškog pristupa te primjenu odgovarajućih mehanizama prevencije i zaštite fizičkih i pravnih lica. U periodu od 2012. do 2018. godine, Ministarstvo unutrašnjih poslova Republike Srpske je sprovelo 29 kriminalističkih obrada čiji predmet su bila djela vezana za kompjuterske prevare, oštećenje kompjuterskih podataka i programa, neovlašćen pristup zaštićenom računaru računarskoj mreži itd.[9]

Oblast sajber bezbjednosti je u entitetskoj nadležnosti, te je s tim u vezi u Republici Srpskoj uspostavljen pravni okvir kojim je uređena predmetna oblast, prvenstveno imajući u vidu Zakon o informacionoj bezbjednosti ("Sl. glasnik RS", br. 70/2011), Zakon o elektronskom potpisu Republike Srpske ("Sl. glasnik RS", br. 106/2015), Zakon o elektronskom dokumentu Republike Srpske ("Sl. glasnik RS", br. 106/2015), Uredbu o mjerama informacione bezbjednosti ("Sl. glasnik RS", br. 91/2012) i dr. Narodna skupština Republike Srpske je usvojila nacrt strategije za borbu protiv sajber kriminaliteta. Kakve promjene bi trebale da usljede i šta on donosi? Nacrt strategije definiše ciljeve i zadatke koje je potrebno ispuniti kako bi se stekli svi potrebni preduslovi da prostor Republike Srpske ne bude mjesto na kome bi se odvijao sajber kriminal a sajber kriminalci djelovali nekažnjeno. Takođe, cilj je podići svijest šire društvene zajednice, ukazati na problem sajber kriminala i ponuditi adekvatnu prevenciju. Ova strategija u nacrtu je u direktnoj vezi i prepliće se sa drugim usvojenim dokumentima vezanim za oblast organizovanog kriminaliteta, korupcije, finansijskog kriminaliteta itd. Predlagači strategije smatraju da će se na osnovu ovog dokumenta stanje u oblasti sajber kriminaliteta značajno poboljšati te da će Vladi Republike Srpske, uz postojeću regulativu, omogućiti strateški pristup rješavanju problema sajber kriminala. Pored navedenog, bitan element ove strategije je usklađivanje vlastitih odredbi sa standardima Evropske unije koji su ključni za borbu protiv sajber kriminala.

Na osnovu bezbjedonosnih izazova i osnovnih sajber prijetnji, a u cilju efikasnijeg suzbijanja sajber kriminaliteta definisani su sljedeći strateški ciljevi:

- *Podizanje svijesti i edukacija zajednice* – kroz izložen Nacrt strategije predviđeno je da se podigne svijest građana na nekoliko različitih načina. Potrebno je da institucije nadležne za ove oblasti osmisle projekte i provode programe u kontinuitetu kojima bi edukovali korisnike interneta od najranije dobi života. S obzirom na to da se broj napada sajber kriminalaca svakodnevno povećava kao i da smo izloženi sve sofisticiranijim napadima, potrebno je da svaki korisnik interneta samostalno preduzme sve neophodne radnje kako bi nivo vlastite bezbjednosti podigao na odgovarajući nivo.
- *Unaprijeđen zakonodavni okvir za borbu protiv sajber kriminaliteta u Republici Srpskoj* – strategijom je definisano da je potrebno ići u korak sa razvojem informacionih tehnologija odnosno neophodno je pravovremeno ažuriranje i stalno prilagođavanje domaćeg zakonodavstva. Navedena aktivnost podrazumijeva i usklađenost domaćeg zakonodavstva sa zakonskom legislativom na međunarodnom nivou. Neophodno je potpuno

usklađivanje pravnog okvira sa Konvencijom o visokotehnološkom kriminalitetu, direktivama Savjeta Evrope i drugim relevantnim međunarodnim aktima.

- *Unaprijediti kapacitete republičkih organa (ljudski i materijalno-tehnički) za borbu protiv sajber kriminaliteta* – kroz Nacrt strategije je istaknuta potreba za kontinuirano jačanje kapaciteta republičkih organa koji se bave pitanjima sajber kriminala. Konkretno, unapriđenje kapaciteta se sastoji od:
  1) jačanje kapaciteta (ljudskih i materijalno-tehničkih)
  2) specijalizacija kapaciteta Ministarstva za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo
  3) unapriđivanje kapaciteta za digitalnu forenziku
  4) jačanje kapaciteta tužilaštava u oblasti sajber kriminaliteta i elektronskog dokaznog materijala
  5) obuke sudija, tužilaca i organa za sprovođenje zakona u oblasti sajber kriminaliteta
  6) unapređivanje finansijskih istraga i sprečavanja prevara i pranja novca na internetu

Pored navedenog, institucije imaju obavezu da procjene stepen ugroženosti računarskog sistema, da uspostave mjere fizičke zaštite i kontrole pristupa. Na osnovu navedenog potrebno je pripremiti plan postupanja u slučaju sajber napada.

- *Unapriđena saradnja između svih organa koji učestvuju u borbi protiv sajber kriminaliteta (javni i privatni sektor)* – da bi se postigli konkretni rezultati a djelovanje sajber kriminalaca svelo na najnižu moguću mjeru, neophodan je sinergijski efekat državnih institucija, privatnog sektora i građana. Posebno važno je unaprijediti komunikaciju sa udruženjima građana, strukovnim ili profesionalnim udruženjima koji mogu da prepoznaju potencijalnu opasnost.
- *Unapriđena međunarodna saradnja u cilju efikasne razmjene informacija i zajedničkih istraga* – negativan uticaj sajber kriminalaca nije fizički ograničen. Kao po pravilu se dešava situacija da sajber napadi unutar jedne države dolaze sa teritorije druge države. Sve ovo dodatno usložnjava problem te je neophodno da Ministarstvo unutrašnjih poslova jača saradnju sa drugim međunarodnim institucijama čiji predmet rada je sajber kriminal. Saradnja podrazumijeva razmjenu znanja i iskustava, sprovođenje zajedničkih istraga i učešće u radu međunarodnih tijela iz oblasti sajber kriminaliteta. Izolovano djelovanje država na problem sajber kriminala koji je međunarodni, ne bi donijelo gotovo nikakav efekat.

Bosna i Hercegovina nema zakon o bezbjednosti informacija na državnom nivou. Jedini dokument koji se na državnom nivou bavi pitanjima sajber kriminala je Strategija za uspostavljanje CERT-a. S druge strane Republika Srpska je usvojila zakon o sajber bezbjednosti i osnovala Agenciju za informaciono društvo koja djeluje od juna 2015. godine a danas je dio novog Ministarstva za naučno tehnološki razvoj, visoko obrazovanje i informaciono društvo.

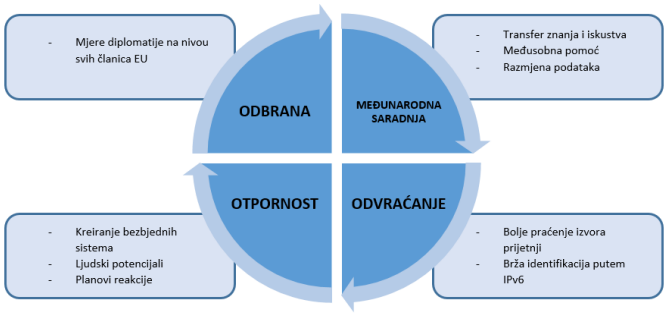
III. ZAKONODAVNI OKVIR SAJBER BEZBJEDNOSTI ENERGETSKOG SEKTORA U EU I BIH

Tokom posljednjih godina, nekoliko značajnih informatičkih prijetnji je postalo uočljivo, a određen broj njih se odnosio na energetski sektor. Evropska unija i Energetska zajednica se trude da primjenom raznih mjera, kroz zakonodavstvo, strategije i finansiranje istraživanja smanje ovu vrstu rizika. Energetski sektor Evropske unije trenutno je u fazi digitalne transformacije koja se ogleda u digitalizaciji mrežnih resursa i stvaranju pametne energetske mreže. Internet of things (IoT) danas je postao trend u energetskom sektoru. Pametna brojila, senzori i aktuatori međusobno su uvezani putem interneta i dostupni 24/7. Ovakav iskorak u načinu rada bi se mogao smatrati revolucionarnom promjenom i nosi sa sobom benefite čije reperkusije će se odraziti na cjelokupno funkcionisanje pojedinih država a time i Evropske unije u cjelini. Sa druge strane, ovakvim načinom rada energetski sektor je izložen različitim rizicima koji prijete da ugroze stabilno snadbijevanje energijom. Učesnici energetskog sektora na prostoru Evropske unije imaju zajednički cilj koji se ogleda u stvaranju preduslova za normalno funkcionisanje sistema. Kako bi se takav cilj ostvario, sajber bezbjednost mora da bude prioritet. Energetski sektor je u posljednjem vremenu bio predmet nekoliko sajber prijetnji te je Evropska unija i Energetska zajednica donijela niz različitih mjera, definisala strategije i finansirala istraživanja kako bi smanjila rizik u sajber prostoru. Najznačajni dokumenti koji su usvojeni a regulišu pitanja bezbjednosti Energetske zajednice su:[11]

- *Uredba EU 2016/679 Evropskog parlamenta i Savjeta od 27. aprila 2016.* – predstavlja akt o zaštiti ličnih podataka koji unapređuje prava pojedinaca i definiše odgovornost strana kojima su dostupne baze podataka. Ova uredba odnosi se na sve organizacije u Evropskoj uniji koje elektronski obrađuju lične podatke, pa tako i na energetske kompanije. Kako zahvaljujući pametnim brojilima kupci imaju mogućnost da kontrolišu sopstvenu potrošnju i eventualno uštede novac kroz odluke o potrošnji energije, uvođenje pametnih mreža zahtijeva od kompanija da se pridržavaju ovog zakonodavstva koje propisuje zaštitu privatnosti i podataka.
- *Paket Evropske komisije "Čista energija za sve Evropljane"* – predviđene su odredbe o sajber bezbjednosti za energetski sektor. Nedostatak ovog paketa je u tome što se regulatornim komisijama ne daje nikakav određen zadatak u vezi s tim. Agencija za saradnju energetskih regulatora (ACER) je zadužena za ova pitanja, što znači da postoji mogućnost uključenja ostalih relevantnih subjekata.

- *Direktiva 2008/114/ES* od 8. decembra 2018. godine – govori o identifikaciji kritične infrastrukture i analizira mogućnost konstantnog poboljšanja zaštite.
- *Direktiva 2016/1148* – govori o mjerama koje je potrebno preduzeti kako bi se obezbijedio visok nivo bezbjednosti mreža i informacionih sistema u Evropskoj uniji. Ova direktiva zahtijeva od zemalja članica Evropske unije da prepozna operatere javnih usluga do 9. novembra 2018. godine, što je većina zemalja i uradila. Direktiva je inicirala osnivanje novih tijela u zemljama članicama EU, kao što su Nacionalne agencije za sajber bezbjednost sa postojećim CERT timovima – Computer Emergency Response Team.

Evropska komisija je izdala prateće dokumente odnosno uputstva kojima se traži priprema mrežnog koda za električnu energiju i rad na sertifikaciji energetskih tehnologija. Posebno važna je priprema mrežnog koda za električnu energiju u oblasti sajber bezbjednosti. Ovim se zahtijeva primjena specifičnih pravila po pitanju sajber bezbjednosti u sektoru električne energije uključujući planiranje, nadzor, izvještavanje i kordinacija u vandrednim okolnostima. U dijelu sertifikacije, identifkovana je potreba za Evropskim sertifikatom za sajber bezbjednost za energetske proizvode, procese i usluge koji bi bio važeću širom EU. Planirana je i implementacija ovih odredbi u budući mrežni kod.



Slika 1. Mjere Evropske unije u cilju jačanja zajedničkog odgovora na izazove sajber bezbjednosti

Strateški cilj Bosne i Hercegovine je pristupanje Evropskoj uniji te je u Bosni i Hercegovini na snazi Sporazum o stabilizaciji i pridruživanju s Evropskom unijom. Suština djelovanja sajber bezbjednosti u energetskom sektoru je obezbijediti zaštitu u slučaju bilo kakvog sajber napada. Funkcionisanje energetskog sektora za razliku od drugih sistema koji su oslonjeni na informacione tehnologije odlikuje specifičan način rada. U slučaju sajber napada kod određenih sistema se može onemogućiti njegovo djelovanje na način da se obustavi rad sistema do momenta neutralisanja napada. Problem u energetskom sektoru kao što je sajber napad nije moguće jednostavno rješiti s obzirom da isključenje sa mreže pojedinih dijelova u energetskom sektoru može bitno narušiti funkcionisanje cijelog sistema. Ministarski savjet Energetske zajednice je donio Odluku broj 2018/2/MS-EnC o uspostavljanju Koordinacione grupe za sajber bezbjednost i kritične infrastrukture. Osnovni razlozi za donošenje ove odluke su stalna potreba za podizanjem nivoa bezbjednosti snabdijevanja na jedinstvenom regulatornom prostoru u Energetskoj zajednici, kao i pristup svih zemalja potpisnica stabilnom i neprekidnom snadbijevanju energijom. Takođe, zaštita za određene kritične infrastrukture, čijim bi oštećenjem ili poremećajem bilo pogođeno više država potpisnica ugovora, zahtijeva uspostavljanje određenog mehanizma koordinacije na nivou Energetske zajednice. Zadaci grupe su obezbjeđenje strateških smjernica za sajber bezbjednost, razmjena najboljih praksi, pomoć i podrška zemljama potpisnicama u izgradnji kapaciteta, prikljupanje najboljih praksi, istraživanje na godišnjoj bazi, identifikacija kritičnih infrastruktura, izrada metodologija za upravljanje rizikom itd. Kako bi se obezbijedila sajber bezbjednost u energetskom sektoru potrebno je ispuniti tri najznačajnija cilja: povjerljivost, integritet, dostupnost[11]. Ukoliko podaci nisu dospuni u predviđenom vremenu ili ukoliko su modifikovani usred sajber napada oni mogu bitno uticati na konfiguraciju uređaja čime je lančanom reakcijom izazvano pogrešno funkcinisanje istih. Povjerljivost se u najvećoj mjeri ogleda u ličnim podacima korisnika koji se nalaze u bazi pružaoca energetskih usluga a mogu biti zloupotrebljeni putem sajber napada. Primjena savremene tehnologije u energetskom sektoru kao što su digitalni uređaji, softverska biling rješenja ili novi oblici komunikacije bitno povećavaju rizik od sajber napada. Uređaji nove generacije koji imaju komercijalne operativne sistem, protokole i aplikacije omogućavaju lakše napade pa je i rizik od sajber napada veći. Energetski sektor mora da preduzme sve aktivnosti kako bi mogao adekvatno odgovoriti na izazove sajber bezbjednosti. Najvažniji bi se mogli podjeliti u nekoliko grupa:[11]

- Stabilnost prekogranične energetske mreže
- Zaštita od svakodnevnih napada
- Uvođenje novih tehnologija i usluga koji su povezani u jednu cjelinu
- Outsourcing infrastrukture i usluga
- Povećana zavisnost tržišnih učesnika
- Dostupnost ljudskih resursa i njihove kompetencije

IV. AKTIVNOSTI RS PO PITNAJU SAJBER BEZBJEDNOSTI ENERGETSKOG SEKTORA

Sektor energetike u Republici Srpskoj uređen je Zakonom o energetici, Zakonom o električnoj energiji, Zakonom o nafti i derivatima nafte, Zakonom o gasu i Zakonom o obnovljivim izvorima energije i efikasnoj kogeneraciji. Navedenim aktima propisane su i nadležnosti Regulatorne komisije, kao regulatornog tijela u Republici Srpskoj. Regulatorna komisija nastoji da kreira atmosferu razumijevanja i saradnje u kojoj će se izvršiti razmjena mišljenja, preporuka i najboljih praksi po pitanju sajber bezbjednosti između regulatora i korisnika dozvola u sektoru u cilju usklađivanja sa zakonodavstvom Evropske unije i Energetske zajednice i poštovanja smjernica i preporuka koje su dale različite institucije zadužene za pitanja sajber bezbjednosti i sigurnosti snabdijevanja (ENISA, ACER,

CEER i sl.). S ozbirom da je za normalan život i sigurnost stanovništva u RS potrebna efikasna upotreba energije te stabilno, pristupačno i održivo snabdijevanje energijom, Regulatorna komisija je pokrenula aktivnosti na izradi strategije sajber bezbjednosti. U tom smislu, misija Regulatorne komisije, u pogledu sajber bezbjednosti je:

- Sprečavanje informacionih napada na osnovnu infrastrukturu tako što će elektroenergetski subjekti zaštiti svoju mrežu i uređaje na odgovarajući način
- Smanjenje osjetljivosti na sajber napade (npr. projektovanjem otpornih sistema sa integrisanim komponentama sajber bezbjednosti) i
- Smanjenje štete i vremena oporavka od sajber napada ukoliko do njega dođe.

Jedan od alata kojima se mogu vršiti procjene sajber bezbjednosti u energetskom sektoru, može biti i praćenje usklađenosti sa nekim od postojećih standarda koji obuhvataju segment sajber bezbjednosti i sigurnosti napajanja. Neki od tih standarda su sljedeći:

- ISO/IEC 27001 Security Audit (General at Information System level)
- ISO/IEC 27002 further specifies controls defined in ISO/IEC 27001
- ISOIEC 27019 focused specifically on the Energy Utilities
- NIST Cyber Security Framework
- NISTIR 7628 Smart Grid Security Guidelines
- NERC Critical Infrastructure Protection (CIPs)
- IEC 62443-2-1, 2-2, 2-3, 2-4, and 4-1 Security Programs
- IEC 62443-3-3 System security requirements
- IEC 62443-4-2 Security for products
- IEC 62351-12 Resilience of the power system with DER
- IEEE 1686 Security for substations

Regulatorna komisija je svjesna činjenice da između standarda i primjene najboljih praksi postoje odstupanja, ali će sarađivati sa korisnicima dozvola u energetskom sektoru i odgovarajućim institucijama, kako bi definisala odgovarajuća očekivanja i podsticala primjenu dobre i efikasne prakse sajber bezbjednosti. Neke od aktivnosti koje je potrebno provesti kako bi se obezbijedila bezbjednost svih učesnika u energetskom sektoru su:

- Identifikovati osnovna sredstva (uređaje, mrežu i sl.), moguće prijetnje, slabosti sistema i dimenzije i posljedice koje može imati sigurnosni indicent
- Zaštititi informacije kvalitetnim projektovanjem sistema, kontrole pristupa, procedura za zaposlene, obukom zaposlenih i odgovarajućim tehnologijama
- Detektovati pokušaj sajber napada kroz kontinuirano praćenje i detekciju događaja, uz procjenu ozbiljnosti ovih sigurnosnih incidenata
- Pravovremeno planirati i primijeniti procedure i tehnologije, te odgovoriti na sigurnosne incidente kako bi se ublažio njihov uticaj
- Procjena rizika, ublažavanje rizika i kontinuirano ažuriranje procedura kao osnova za unapređenje bezbjednosti
- Redovna provjera i revizija uspostavljenih procedura sajber bezbjednosti

V. ZAKLJUČAK

Činjenica je da Bosna i Hercegovina tek razvija mehanizme za borbu protiv sajber kriminala i za očekivati je da sajber bezbjednost energetskog sektora bude prioritet prilikom kreiranja akcionih planova. Neophodno je da se kroz zakonsku regulativu definiše pravni okvir ali obezbijedi i edukacija kako bi subjekti koji djeluju u sajber prostoru mogli preduzeti mjere prevencije i zaštite od sajber napada. Pored dobre saradnje između institucija u Republici Srpkoj, neophodno je uspostaviti koordinaciju na nivou Bosne i Hercegovine a zatim i na nivou Evropske unije. Još jedan važan element borbe protiv sajber kriminala a koji se ne eksploatiše dovoljno, je privatni sektor koji može biti podrška republičkim organima. Kako bi obezbijedile kontinuiran rast i razvoj, te konkurentnost i bezbjednost, energetske kompanije moraju aktivno pratiti trendove u oblasti informaciono komunikacionih tehnologija. Poznato je da energetski sektor obezbjeđuje energiju kroz primarna i rezervna napajanja za IKT, dok IKT tehnologije imaju sve veću primjenu u energetskom sektoru. Takvi procesi integracije i zajedničkog djelovanja su neizbježni. Neophodno je da BiH prepozna prijetnje po svoj energetski sektor i definiše jasne strategije sajber bezbjednosti na ovom ali i svim drugim poljima od posebnog značaja. Trenutno stanje je takvo da možemo sa sigurnošću reći da je sajber bezbjednost energetskog sektora na izuzetno niskom nivou. Ovakva situacija je alarmantna s obzirom na važnost energetskog sektora te je potrebno da odgovorni što prije daju prijedloge za kreiranje sajber bezbjednog poslovnog okruženja. Raduje činjenica da Vlada Republike Srpske i Regulatorna komisija za energetiku RS prati razvoj ovog segmenta i inicira donošenje kvalitetnih rješenja na nivou Republike Srpske. Kao što smo u uvodu spomenuli, rad će biti dobra osnova autorima i stručnoj javnosti, kako bi u regulatornim tijelima i energetskoj zajednici pokrenuli diskusiju o ovim pitanjima.

LITERATURA

[1] The Future of Work Jobs and Skills in 2030 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/303335/the_future_of_work_key_findings_edit.pd

[2] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3] https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

[4] CIA. World Factbook. Bosnia and Herzegovina. Available at https://www.cia.gov/library/publications/

[5] world-factbook/geos/bk.html (Accessed 16/12/2018)

[6] Communications Regulatory Agency (2015) Available at https://www.rak.ba/news/500 (Accessed 16/12/2018)

[7] (ITU) Global ICT Development Index (2017) Available athttps://www.itu.int/net4/ITUD/idi/2017/index.html#idi2017economycard-tab&BIH (Accessed 16/12/2018)

[8] Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities

[9] Nacrt/Strategija za borbu protiv sajber kriminaliteta u Republici Srpskoj od 2019. do 2023.

[10] https://www.undp.org/content/dam/bosnia_and_herzegovina/docs/News/E&E%20Sector/TNC/TNC%20Report%20%20LAT.pdf

[11] https://erranet.org/download/cyber-security-energy-sector/

ABSTRACT

Cyber Space has become an important component of society, considering that institutions, energy and financial sector, school system and social life in general depend of internet and interconnectedeness. On a teritory of Republic of Srpska/ Bosnia and Herzegovina significant place takes energy sector, so its security is a basis of this countrys functioning. Energy sector and sector of information and communication technologies are two technological branches that act synergistically on the development of the whole society. Deviations from the proper functioning of information systems or parts in the energy sector not only present technical difficulties, but a much greater security hazard. Considering the trends of increasing cyber attacks on energy systems, it is important to consider security aspects of the integration of IKT tecnologies, as well as predict tools, proceedures, technologies and human resources so that energy systems can overcome security challenges ahead.

CYBER SECYRITY IN REPUBLIC OF SRPSKA/BOSNIA AND HERZEGOVINA WITH AN ACCENT ON ENERGY SECTOR

Mihajlo Travar, Dragana Travar, Igor Dugonjić, Saša Ristić