Sajber bezbednost u energetskom sektoru

Cybersecurity in energy sector

Biljana Trivić*, Darko Šošić**

* Agencija za energetiku Republike Srbije, Elektrotehnički fakultet Beograd
** Elektrotehnički fakultet Beograd

UDC: 620.XXX.XX
http://dx.doi.org/10.29322/EEE.X.X.2018.pXXXX

Apstrakt **-** Sajber prostor podrazumeva mnoge elemente tehnologije i društva, pa zbog toga predstavlja kompleksno okruženje koga čine mreža hardvera i softvera, interneta, mnogih podataka i sistema, razne dodatne infrastrukture, servisa i dr. Obzirom da internet dobija ključnu ulogu u današnjem društvu to znatno povećava rizike po celokupnu privredu, ljudske slobode i bezbednost jednog društva jer uprkos brojnim prednostima i velikom potencijalu internet ostavlja prostor i za zlonamerne aktivnosti koje se kreću od mogućih napada na internet infrastrukturu i onesposobljavanje servisa u sajber prostoru, uključujući neku kritičnu infrastrukturu poput elektroenergetske mreže, pa sve do krađe i praćenja informacija i komunikacija i zloupotrebe privatnih i tajnih podataka. Zbog toga je upravljanje internetom kao i bezbednost sajber prostora ušlo u fokus nacionalnih i globalnih politika. Mnoge organizacije se sve više bave ovom problematikom. Međutim, paralelno se razvijaju i sajber napadi, koji su postali sve češći i sofisticiraniji, a alati za napad konstantno postaju dostupniji sve većem broju zainteresovanih grupa ili pojedinaca, koje čine razni hakeri, kriminalne i terorističke organizacije, političke organizacije i dr. Zbog toga je sveobuhvatan i sistematičan pristup, koji uključuje različite i mnogobrojne aktere, osnova borbe protiv rizika sajber kriminala. U radu će se dati uvid u postojeću regulativu u oblasti sajber bezbednosti u Evropskoj Uniji, kao i u Republici Srbiji. Takođe, biće opisano stanje u oblasti sajber bezbednosti u elektroenergetskim sistemima, odnosno biće dat pregled korišćenih digitalnih tehnologija u elektroenergetskim sistemima, kao i način zaštite sajber infrastrukture u elektroenergetskim sistemima. U poslednjem poglavlju biće dat predlog mogućih mera za zaštitu od sajber kriminala u elektroenergetski sistemima

Ključne reči **-** internet, sajber bezbednost, sajber napadi, digitalne tehnologije, pametne mreže

Abstract- Cyberspace involves many elements of technology and society, and therefore is a complex environment consisting of a network of hardware and software, the Internet, many data and systems, various additional infrastructure, services and more. Given that the Internet plays a key role in today's society, it significantly increases the risks to the entire economy, human freedoms and security of a society, and despite its benefits and great potential, the Internet also leaves room for malicious activities ranging from possible attacks on the Internet infrastructure and disabling service in cyber space, including some critical infrastructure such as the power grid, to stealing and monitoring information and communications and misusing private and secret information. This is why Internet governance and cybersecurity are the focus of national and global policies. Many organizations are increasingly addressing this issue. However, cyber-attacks are also evolving in parallel, becoming more and more sophisticated, and the tools of attack constantly becoming available to a growing number of interested groups or individuals, consisting of various hackers, criminal and terrorist organizations, political organizations and more. Therefore, a comprehensive and systematic approach, involving different and multiple actors, is the basis of the fight against cybercrime risk.
This paper will give an insight into the existing cybersecurity regulations in the European Union as well as in the Republic of Serbia. Also, the situation in the field of cyber security in power systems will be described. An overview of the used digital technologies in power systems will be given, as well as a method of protection of cyber infrastructure in power systems. The last chapter will propose possible measures to protect against cybercrime in power systems.

Keywords - internet, cybersecurity, cyber-attacks, digital technologies, smart grids

I. UVOD

Obzirom da internet dobija ključnu ulogu u današnjem društvu to znatno povećava rizike po celokupnu privredu, ljudske slobode i bezbednost jednog društva ali i celog sveta jer uprkos brojnim prednostima i velikom potencijalu internet ostavlja prostor za zlonamerne aktivnosti. Ove zlonamerne aktivnosti se kreću od mogućih napada na internet infrastrukturu i onesposobljavanje servisa u sajber prostoru, uključujući finansijski sektor ili neku kritičnu infrastrukturu poput elektroenergetske mreže ili saobraćajne mreže, pa sve do krađe i

praćenja informacija i komunikacija i zloupotrebe privatnih i tajnih podata. Poslednjih godina širom sveta su zabeležene brojne zlonamerne aktivnosti u sajber prostoru koje su dovele do velikih finansijskih gubitaka, pa čak i do uništavanja imovine i gubitka života. Zbog svega ovoga očekuje se da će u skorijoj budućnosti ovi rizici biti sve veći što znatno može da ugrozi poverenje ljudi u celokupni sajber prostor i da dovede u pitanje korišćenje interneta i informacionih tehnologija. Zbog toga je upravljanje internetom kao i bezbednost sajber prostora ušlo u fokus nacionalnih i globalnih politika pre svega zbog geostrateškog značaja kablova, konekcija, protoka i kontrole protoka digitalnog sadržaja. Međutim, paralelno se razvijaju i sajber napadi, koji su postali sve češći i sofisticiraniji, a alati za napad konstantno postaju dostupniji sve većem broju zainteresovanih grupa ili pojedinaca, koje čine razni hakeri, kriminalne i terorističke organizacije, političke organizacije i dr. Zbog toga je sveobuhvatan i sistematičan pristup, koji uključuje različite i mnogobrojne aktere, osnova borbe protiv rizika sajber kriminala. Oblast sajber bezbednosti je jedna veoma multidisciplinarna oblast i zahteva aktere koji poznaju različite teme, poput digitalne tehnologije, prava, psihologije, sociologije, ekonomije, politike, diplomatije i dr.

II. REGULATIVA U OBLASTI SAJEBR BEZBEDNOSTI

- PREGLED STANJA U EVROPSKOJ UNIJI

Prvi dokument kojim je Evropska komisija uredila strateški pristup pitanju sajber bezbednosti u EU jeste Strategija sajber bezbednosti Evropske unije iz 2013. godine. Tri godine posle usvojena je Direktiva o merama za obezbeđivanje najvećeg nivoa bezbednosti mrežnih i informacionih sistema širom EU (*The Directive on security of network and information systems* - NIS Direktiva) kao obavezujući dokument koji će svaka država članica EU inkorporirati u svoj nacionalni pravni okvir. NIS Direktiva poziva sve države članice EU da na nacionalnom nivou propišu osnovne standarde bezbednosti sajber mreža i informacija (*network and information security*). Previđeno je da se u svakoj državi članici EU uspostave funkcionalni Centri za bezbednost u IKT sistemima (*Computer Emergency Response Team* - CERT), a takođe i da se usvoje nacionalne strategije i plan saradnje u ovoj oblasti. Uloga CERT-a je brzo reagovanje u slučaju incidenata, kao i prikupljanje i razmena informacija o rizicima za bezbednost IKT sistema. U NIS Direktivi je istaknuta potreba za standardizacijom kako bi se osigurala zajednička bezbednost širom EU i predložen je razvoj harmonizovanih standarda. Evropska agencija za bezbednost mreža i informacija (*European Network and Information Security Agency, ENISA*), koja je oformljena 2004. godine, je određena kao ključno telo koje će u saradnji sa državama članicama EU razviti smernice za razvijanje standarda.

NIS Direktiva predviđa da podršku strateškoj saradnji između država članica pruža Grupa za saradnju (Cooperation Group) koju čine predstavnici država članica EU, Evropske komisije i ENISA. Predviđeno je da prvi put 18 meseci nakon usvajanja NIS Direktive, a nakon toga svake druge

godine, Grupa za saradnju definiše plan rada kako bi se postigli ciljevi koji su navedeni u NIS Direktivi. Takođe, predviđeno je da Evropska Unija može da sklopi međunarodne ugovore sa trećim državama ili nekim drugim međunarodnim organizacijama u ovoj oblasti.

NIS Direktiva ističe neophodnost saradnje između javnog i privatnog sektora, koje je istaknuto kao veoma važan koncept u borbi protiv sajber kriminala. Evropska komisija je 2015. godine objavila Bezbednosnu agenda EU (*European Agenda on Security*) za period 2015-2019. godina, koja je zamenila prethodnu Bezbednosnu agendu EU 2010-2014. U Bezbednosnoj agendi EU istaknuta je neophodnost javno-privatnog partnerstva u smislu uspostavljanja lanca za borbu protiv sajber kriminala. Ovo podrazumeva uključivanje različitih aktera, kao što su Centar za sajber kriminal u EUROPOL-u (*European Police Office*), nacionalni CERT-ovi i pružaoci internet usluga koji mogu da upozore krajnje korisnike i pruže tehničku zaštitu.

- Kritična infrastruktura

Direktiva o identifikaciji i imenovanju evropske kritične infrastrukture i proceni potrebe unapređenja zaštite iz 2008. godine (*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*) određuje da sve Države članice EU imaju obavezu da identifikuju kritičnu infrastrukturu i da Evropskoj Komisiji dostave informacije o rizicima, pretnjama i slabostima kritične infrastrukture. Ovo podrazumeva i informacije o urađenim i planiranim unapređenjima zaštite identifikovane kritične infrastrukture kao i o posledicama potencijalnih sajber incidenata na nacionalnom i međunarodnom nivou. Ova direktiva je prva koja uređuje osnove određivanja kritične infrastrukture u EU i ona se odnosi pre svega na energetski sektor i sektor transporta ali poziva na primenu istog pristupa u drugim sektorima.

NIS Direktiva definiše obavezu da se identifikuju „operatori osnovnih usluga“ (*Operators of essential services*) čija uloga je izveštavanje o sajber sigurnosti i incidentima utvrđenim u NIS Direktivi. Prema NIS Direktivi "operater osnovne usluge" je javni ili privatni entitet koji ispunjava bilo koji od sledećih kriterijuma:

- pruža uslugu koja je neophodna za održavanje kritičnih društvenih i / ili ekonomskih aktivnosti;
- pružanje tih usluga zavisi od mreže i informacionih sistema i
- incident koji bi se desio na tim sistemima bi imao značajne negativne posledice na pružanje te usluge.

Države članice EU dužne su da redovno, a najmanje jednom u dve godine, ažuriraju listu identifikovanih „operatora osnovnih usluga“ u svojoj državi, koja se zajedno sa metodologijom za identifikaciju i klasifikacijom važnosti navedenih „operatora osnovnih usluga“, podnosi Evropskoj komisiji.

- Standardizacije

EU Strategija jedinstvenog digitalnog tržišta iz 2015. godine (*Digital Single Market Strategy for Europe COM (2015) 192 final*) jasno prepoznaje značaj sajber bezbednosti za funkcionisanje digitalnog tržišta. Ova strategija naglašava potrebu za definisanjem nedostajućih tehnoloških standarda koji podržavaju razvoj digitalnog tržišta i usluga uključujući standarde sajber

bezbednosti i zbog toga je ovom strategijom predviđen proces standardizacije u digitalnom sektoru. *ENISA* Vodič za upravljanje evropskom standardizacijom, osim preporuka za proces standardizacije, navodi i koje još aktere treba uključiti u proces standardizacije. Pored sektora industrije, državne administracije, nacionalnih tela za standardizaciju, korisnika digitalnih usluga kao i sektora obrazovanja, ovaj vodič navodi i trans-nacionalne Evropske organizacije za standardizaciju (*European Standardization Organizations*), a sve u cilju efektivne razmene znanja i iskustava iz prakse i razvoja sprovodljivih mehanizama.

- PREGLED STANJA U REPULICI SRBIJI

Iako sve države u regionu, pa tako i Republika Srbija zaostaju u oblasti sajber bezbednosti, rizici u ovoj oblasti su za Republiku Srbiju i zemlje u regionu isti kao i u državama članicama Evropske Unije, što potvrđuje sve veći broj sajber incidenata. Početkom 2016. godine Republika Srbija je usvojila Zakon o informacionoj bezbednosti, koji uspostavlja osnovni pravni okvir u ovoj oblasti. Zakon o informacionoj bezbednosti predviđa osnivanje CERT-a za prevenciju bezbednosnih rizika u IKT sistemima koji radi u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL). Nacionalni CERT je formiran. Jedan od nedostataka Zakona jeste nedovoljno definisan prostor za javno-privatno partnerstvo. Kritična infrastruktura u Republici Srbiji, kao ni kritična informaciona infrastruktura, nisu jasno zakonski definisani, a pretpostavlja se da će oni kao i njihova zaštita biti definisana u okviru podzakonskih akata. Takođe, dijalog između državnih organa, stručnih organizacija, privatnog sektora, nacionalnog CERT-a i operatora kritične infrastrukture, među kojima je sve više privatnika pogotovo u oblasti energetike, još uvek nije pokrenut, uprkos alarmantnim vestima iz drugih zemalja o teškim posledicama sajber napada na elektroenergetski sistem, železnicu, bankarski sektor i sl.

30. maja 2017. godine Vlada Republike Srbije donela je Strategiju razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine (u daljem tekstu: Strategija). Strategijom su definisani principi na kojima se zasniva razvoj informacione bezbednosti u Republici Srbiji, kao i prioritetne oblasti delovanja koje uključuju bezbednost IKT sistema, informacionu bezbednost građana, borbu protiv visoko tehnološkog kriminala i informacionu bezbednost cele države. Akcioni plan za sprovođenje Strategije usvojen je 28. avgusta 2018. godine za period 2018-2019. godina. Od konkretnih akcija predviđeno je definisanje jasnih kriterijuma za klasifikaciju sajber incidenata, određivanje kritičnih IKT sistema na nacionalnom nivou, kao i razvoj aplikacija koje će služiti za razmenu informacija i saradnju sa CERT-ovima u slučaju incidenta. U Akcioni plan je uvršteno i osnivanje posebnog CERT-a za međunarodnu saradnju pri Ministarstvu spoljnih poslova, kao i uspostavljanje Inspektorata za informacionu bezbednost, kako je i predviđeno Strategijom. Takođe, Akcioni plan propisuje sprovođenje godišnjih analiza pretnji u sajber prostoru, kao i davanje preporuka za ublažavanje rizika.

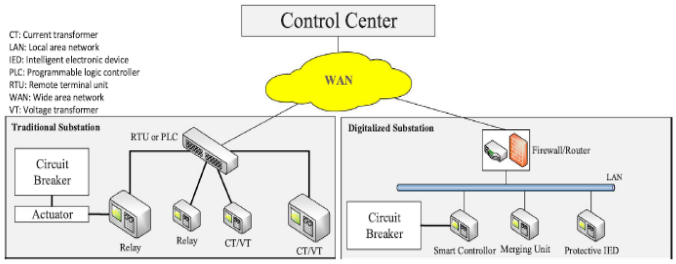
Strategija za borbu protiv visoko tehnološkog kriminala za period 2019–2023. godina doneta je 25. septembra 2018. godine. Donošenje ove strategije proisteklo je iz obaveze Republike Srbije u okviru pregovaračkih pregovora za pristup EU za poglavlje 24 – Pravda, sloboda, bezbednost.

III. SAJBER BEZBEDNOST U ELEKTROENERGETSKIM SISTEMIMA

U poslednje dve decenije urađene su značajne investicije u elektroenergetskom sektoru čiji je cilj unapređenje i poboljšanje efikasnosti i pouzdanost elektroenergetskog sistema. Ovde se pre svega misli na ulaganje u informacione i komunikacione tehnologije koje su dovele do toga da elektroenergetski sistemi budu „pametniji“, povezaniji i više automatizovan. Ovo je olakšalo operatorima elektroenergetskih sistema vođenje sistema jer im je omogućilo da na osnovu mnogih podataka koje dobijaju daljinski odlučuju o izvođenju raznih akcija u svom elektroenergetskom sistemu. Međutim, kako je elektroenergetski sistem geografski raširen po celoj državi, često se radi ekonomičnosti za širenje IKT mreže koristi već postojeća javna ili privatna mreža (optička vlakna, radio talasi, mreže za mobilnu telefoniju i dr.). Ovo otvara prostor za razne napadače u sajber prostoru za lakši pristup elektroenergetskoj mreži koji može da prouzrokuju razne negativne efekte u radu mreže što može da izazove velike posledice.

- PREGLED DIGITALNIH TEHNOLOGIJA U ELEKTROENERGETSKIM SISTEMIMA
  - Digitalni sistemi komunikacija

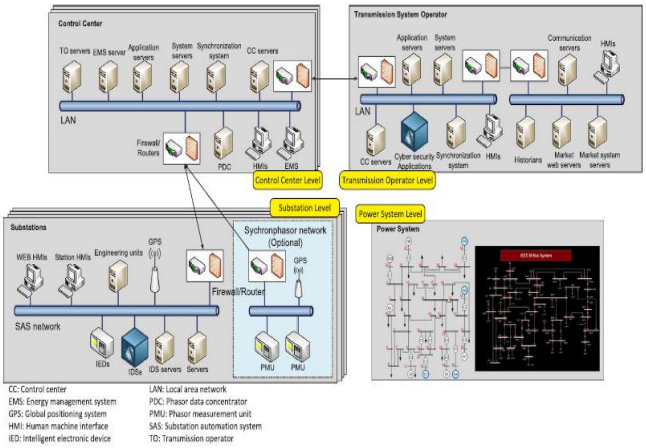
U tradicionalnim transformatorskim stanicama gde se koristi analogna komunikacija potreban je poseban bakarni kabl koji bi međusobno povezao sve uređaje koji se nalaze u transformatorskoj stanici. Međutim, u digitalnoj komunikaciji omogućena je međusobna povezanost mnogih uređaja bez pojedinačnog bakarnog kabla. Ovo dosta smanjuje troškove opreme i komunikacija postaje dosta brža i kvalitetnija zahvaljujući korišćenju LAN mreže (*Local Area Network*) ili interneta. Takođe, na ovaj način povećan je i protok podatka jer digitalna komunikacija omogućava prenos većeg broja podataka preko samo jedne linije. Na slici 1. prikazana je razlika između tradicionalne – analogne transformatorske stanice i digitalne transformatorske stanice.



Slika 1. Poređenje sistema komunikacije kod tradicionalnih i digitalnih TS

- IKT u prenosnom elektroenergetskom sistemu

Osnovna uloga elektroenergetskog sistema jeste da prenese električnu energiju od centara proizvodnje do centara potrošnje. Stalnom interakcijom između velikog broja elementa prenosne mreže koji su raspoređeni svuda po državi (generatori, elektroenergetski vodovi, transformatorske stanice, transformatori, prekidači, merači, potrošači i druga oprema) utiče se na stabilnost prenosnog sistema (stabilnost napona, tranzijentna stabilnost, rešavanje malih poremećaja frekvencije i dr.). IKT sistemi prikupljaju podatke koji služe za praćenje i kontrolu rada prenosnog sistema.

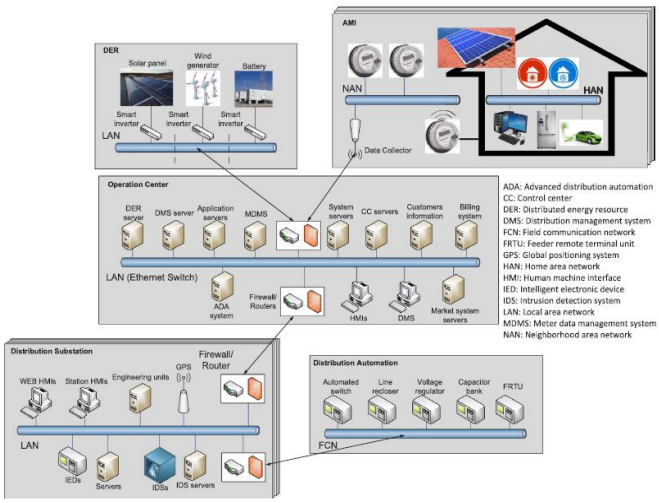


Slika 2. IKT model u prenosnom sistemu

Neki od digitalnih sistema koji se koriste u prenosnim sistemima su: *Supervisory Control And Data Acquisition (SCADA), Substation Automation System (SAS), Phasor Measurement Unit (PMU).*

- IKT u distributivnom elektroenergetskom sistemu

U poslednjih desetak godine uloženi su veliki napori da se elektroenergetska distributivna mreže automatizuje i na taj način dosta se povećala njena pouzdanost i sigurnost, a takođe povećala se sposobnost za njeno automatsko praćenje i vođenje. U većinu distributivnih mreža se sve više ugrađuju razni digitalni uređaji, a tu se misli na daljinski upravljive prekidače, releje za zaštitu, regulatore napona, pametne merače, sisteme za kontrolu isključenja, a takođe pojavljuje se sve veći broj proizvođača koji se priključuju na distributivnu mrežu. Zbog svega ovog postoji potreba da se komunikaciona mreža unapredi i da se omogući daljinsko prikupljanje svih relevantnih podataka. Neki od digitalnih sistema koji se koriste u distributivnim sistemima su: *Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DER), Distribution Automation (DA).*



Slika 3. IKT model u distributivnom sistemu

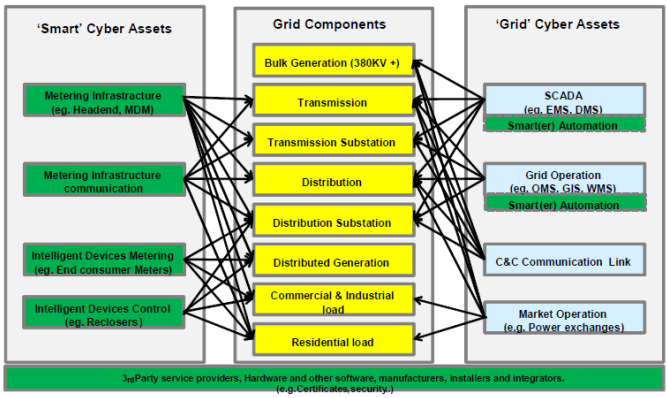
- ZAŠTITA SAJBER INFRASTRUKTURE

Da bi se sajber prostor zaštitio od raznih neautorizovanih upada, ispred svake sajber infrastrukture postavlja se fajervol (*firewall)*, odnosno zaštitna ograde koja služi kao odbrana i filter od raznih malicioznih digitalnih podataka. Fajerfol na osnovu informacija iz svake digitalne pošiljke (vremenska odrednica, izvorna i krajnja IP adresa i broj porta) ima mogućnost da izvrši proveru i da detektuje sumnjive pošiljke. Međutim, osobine, funkcije i rad fajervola zavisi od unapred podešenih pravila, pa se tako mogu javiti i propusti jer se svaki fajervol sastoji od više stotina pravila koja često mogu da budu u međusobnom konfliktu ili se propust može javiti zbog nedovoljnog poznavanja unutrašnje digitalne mreže, a svako uvođenje novih softvera u sistem sve više komplikuje proces formiranja fajervola. Pored toga fajervol može da ima propust jer može da se desi da nije u stanju da pruži zaštitu od dobro osmišljenih opasnih poruka koje premoste postavljena pravila zaštite. Većina protokola za digitalnu komunikaciju je uvedeno u elektroenergetske sisteme za prenos i distribuciju pre nego što je problem sajber bezbednosti postao toliko dominantan i zbog toga oni ne sadrže jaku zaštitu koja je u današnje vreme potrebna.

- Osetljivost i ranjivost sajber infrastrukture u pametnim mrežama

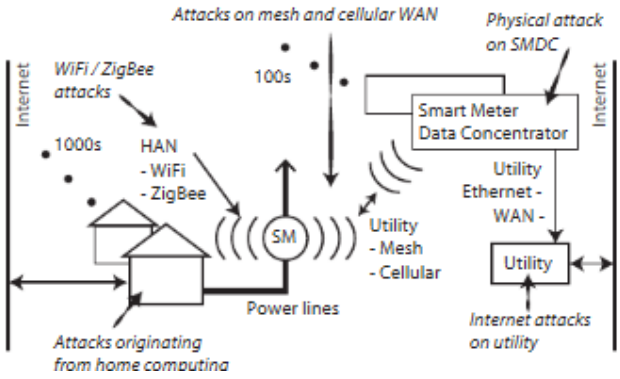
Pametna elektroenergetska mreža je mreža koja koristi analogne i digitalne IKT u cilju prikupljanja informacija o snabdevanju i potrošnji električne energije. Glavni cilj pametnih elektroenergetskih mreža je poboljšanje efikasnosti, pouzdanosti, ekonomičnosti i održivosti proizvodnje i distribucije električne energije. Pametne elektroenergetske mreže koriste digitalna

(pametna) brojila za praćenje potrošnje električne energije u realnom vremenu. Pametna brojila su elektronski uređaji koji imaju dvosmerni komunikacioni modul koji šalje i prima podatke u oba smera (od naprednog mernog uređaja prema kontrolnom centru se šalju podaci o merenju, a u obrnutom smeru se primaju razne komande). Podaci prema kontrolnom centru se šalju u proseku na svakih 5-60 minuta, a to zavisi od performansi naprednog mernog uređaja i od performansi distributivne mreže. Arhitekturu pametnih mreža čine mnogi uređaji i oprema od kojih su neke komponente tradicionalni uređaji i oprema, dok su druge komponente delovi pametne mreže, odnosno „pametniji“ uređaji i oprema. Na osnovu ove podele svi uređaji i oprema koji čine jednu pametnu mrežu mogu se klasifikovati na sledeći način: „pametni“ delovi pametne mreže (*Smart cyber assets*), mrežni delovi pametne mreže (*Grid components*) i mrežni sajber delovi pametne mreže (*Grid Cyber assets*). Ova klasifikacija komponenata pametne mreže je potrebna jer je veoma važno da se identifikuju svi njeni sastavni delovi da bi mogla da se izvrši procena rizika od sajber napada i na osnovu toga da se izvrše analize koje će služiti odabiru mera za zaštitu od sajber napada.



Slika 4. Podela opreme u pametnoj mreži

Najčešća meta sajber napada u elektroenergetskim sistemima je *SCADA* sistem pošto je on ključna komponenta svakog elektroenergetskog sistema i povezuje mnoge podsisteme koji se koriste u pametnim mrežama kao što su *AMI*, *DER* i *DA* u distributivnom sistemu. U slučaju kada sajber napadači uspeju da pristupe uđu u *SCADA* sistem, sajber napad postaje veoma opasan za taj elektroenergetski sistem jer može da izazove kaskadni efekat.



Slika 5. mogući pravci napada na *AMI* sisteme

- Identifikacija sajber pretnji u pametnim mrežama

Pametne mreže u Evropi podrazumevaju učešće mnogih učesnika među kojima su operatori prenosnog i distributivnog sistema, konvencionalni i obnovljivi proizvođači električne energije, snabdevači električne energije, milioni potrošača od kojih neki istovremeno mogu da budu i proizvođači – pro-trošači (*eng. prosumer*), milioni raznih uređaja, pametnih i tradicionalnih, električna vozila i dr. Zbog ovako velikog broja različitih učesnika postoji i veliki broj pretnji od sajber napada. Potrebno je identifikovati sve slabosti pametne mreže da bi se kasnije na osnovu toga mogle izvršiti procene rizika od sajber napada.

Jedna od osnovih slabosti pametnih mreža koja utiče na njihovu veliku izloženost sajber napadima jeste činjenica da pametnu mrežu čine tradicionalne mrežne komponente i pametni delovi, a da je trenutna zaštita elektroenergetskih sistem podešena uglavnom prema tradicionalnim mrežnim delovima pametne mreže i dešava se da se takva zaštita nije dovoljna za celu pametnu mrežu, odnosno za njene pametnije komponente. Većina tradicionalnih delova pametne mreže ima ugrađenu stariju analognu opremu, pa je potrebno da se ona unapredi da bi bila kompatibilna sa ostalom opremom u pametnoj mreži.

Druga slabost pametnih mreža može da bude problem sinhronizacije podataka koji se dobijaju putem *GPS (Global Positioning System)* zbog toga što neki *GPS* sistemi koji se ugrađuju u domaćinstva nemaju mogućnost da daju tačnu informaciju o vremenskoj odrednici podatka, pa tako potencijalni sajber napad na ove podatke (menjanje vremenske odrednice) može da utiče na ostale podatke o stanju u celom sistemu i tako izazove loše funkcionisanje celog prenosnog ili distributivnog elektroenergetskog sistema. Zbog ovoga je potrebno da se uvede zaštita čiji bi funkcija bila da štiti vremensku odrednicu očitanih podataka.

Sledeće slabost pametnih mreža jeste korišćenje bežične komunikacije za prenos podataka. Bežična komunikacija ima prednost jer ne zahteva korišćenje kablova i ne zavisi od konfiguracije terena ali ona uglavnom koristi već postojeće kanale za komunikaciju koju su javni, pa je rizik od sajber napada veliki. Zbog toga je potrebno uvesti otporan sistem za prenos podatak putem bežične komunikacije.

Da bi se izvršila kvalitetna procena rizika od sajber napada potrebno je da se sve ove pretnje identifikuju i klasifikuju. One mogu da se klasifikuju na sledeći način:

1. Pretnja tipa 1: mogući sajber napad se odnosi na IKT strukturu u pametnim mrežama koja se odnosi na podatke o snabdevanju električnom energijom;
2. Pretnja tipa 2: mogući sajber napad se odnosi na IKT strukturu u pametnim mrežama koja se odnosi na podatke o potrošnji električne energije;
3. Pretnja tipa 3: mogući sajber napad se odnosi na IKT strukturu u pametnim mrežama koja se odnosi na podatke o proizvodnji električne energije;
4. Pretnja tipa 4: mogući sajber napad se odnosi na IKT strukturu u pametnim mrežama koja se odnosi na podatke o trenutnom balansu između potrošnje i proizvodnje električne energije, odnosno trenutnoj adekvatnosti sistema;

Neki od primera sajber napada koji spadaju u prethodne kategorije su:

- Uticaj na tržište električne energije zbog menjanja trenutnih stvarnih podataka o proizvodnji, potrošnji i snabdevanju, a ponekad i o cenama na tržištu električne energije;
- Uticaj na rad komponenti elektroenergetskih sistema koji mogu da izazovu nestanak struje kod potrošača ili proizvođača električne energije, a koji dalje mogu da dovedu do velikih finansijskih gubitaka pogođenih potrošača;
- Uticaj na rad elektroenergetskog sistema zbog menjanja podataka o potrošnji i proizvodnji, koje dalje uzrokuju akcije operatora distributivnog i prenosnog sistema za rešavanje tokova snage koji u realnosti ne postoje. Rezultat ovoga mogu da budu veliki kvarovi ili nestanci struje koji mogu da dovedu do velikih finansijskih gubitaka i operatora sistema i pogođenih potrošača,
- Upad u baze podatak i krađu podatak o potrošačima i dr.

- Predlog mogućih mera za zaštitu od sajber kriminala u pametnim mrežama

Na osnovu identifikacije ključnih elementa pametnih mreža i mogućih pretnji, koje su identifikovane u prethodnim poglavljima mogu da se razviju mere za zaštitu od sajber napada na pametne mreže. Ove mere su neophodne da bi se osiguralo da cela pametna mreža bezbedno radi i da bi se obezbedila sigurnost snabdevanja potrošača, što jeste osnovna uloga elektroenergetskih mreža, pa tako i pametnih mreža. Ovo uključuje sve IKT komponente koje u elektroenergetskom sistemu učestvuju u praćenju, kontroli i prikupljanju podataka (*SCADA, AMI* i dr.) kao i softvere za podatke o tržištu električne energije.

Da bi se uspostavile odgovarajuće mere za zaštitu od sajber kriminala u pametnim mrežama potrebno je da budu ispunjeni sledeći uslovi:

- Potrebno je da postoji jasna politika na koji način se koristi pametna mreža i koje je njena svrha;
- Potrebno je da se unapred definiše arhitektura pametne mreže, kao i odgovarajuća zaštita za sve elemente definisane infrastrukture, kao i zajednička zaštita za ceo sistem pametne mreže;
- Potrebno je da se uradi procena rizika za sistem pametne mreže na osnovu kojeg bi se napravio plan delovanja zaštite u slučaju sajber napada.

Pri definisanju mera za zaštitu od sajber napada potrebno je imati u vidu i još jedan bitan uslov koji važi za prenosne elektroenergetske sisteme, a to je zahtev da prenosna mreža ne sme ni u kom slučaju da se raspadne, jer su direktni troškovi raspada jedne prenosne mreže ogromni, zbog njene međunarodne povezanosti, a indirektni troškovi, koji su i veći od direktnih, ne mogu tačno ni da se utvrde. Ovo znači da otpornost prenosne elektroenergetske mreže mora da bude 100% i u skladu sa tim je potrebno kreirati mere zaštite od sajber napada.

Neke od mera za zaštitu od sajber napada na pametne mreže mogu da budu:

1. Procena otpornosti pametne mreže na sajber napad – bitno je da pametna mreža ima dobro organizovanu metodologiju koja se koristi kao odbrana od sajber napada i da se ta metodologija periodično ispituje i nadograđuje;
2. Uvođenje sistema koji se bavi poboljšanjem sigurnosti IKT sistema - kao što je prethodno pomenuto u nekim pametnim mrežama kao što je prenosni elektroenergetski sistem potreba je sigurnost od 100%, pa je zato potrebno uvesti sistem koji se bavi sigurnošću. Na primeru *Stuxnet* napada može se videti kako je u sistemima gde sigurnost IKT sistema nije bila 100% lako došlo do sajber napada;
3. Uvođenje standarda zaštite koji bi se koristili u raznim sektorima kao i raznim organizacijama i kompanijama;
4. Konstantno informisanje o pretnjama i napadima koje su se desile, kao i razmena iskustva i deljenje prakse u ovoj oblasti;
5. Uvođenje *Highest Security Control Network (HSCN)* – ovo je koncept u kojem nije dozvoljena greška i gde je sigurnost stoprocentna. U ovakvom konceptu se radi na tome da se postigne sistem u kojem nema grešaka tako što se uvode tehnologije za zaštitu od grešaka i kvarova, uvode se dodatna redudantnost sistema, osobine samo-popravke kao i druge slične tehnologije koje omogućavaju da budu ispunjeni kriterijumi sigurnosti n-1, n-2 i n-3 (n-3 kriterijum sigurnosti znači da 3 komponente sistema mogu da budu u kvaru, a da sistem i danje sigurno funkcioniše).

LITERATURA

[1] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. JOIN(2013) 1 final

[2] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. L 194/1.

[3] Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security. 2014. Internet Governance Forum (IGF). https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. The European Agenda on Security. 28.4.2015. COM (2015) 185 final.

[5] Council Directive 2008/114/EC of 8 December 2008 on the identification and designations of European critical infrastructures and the assessment of the need to improve their protection. 23.12.2008. Official Journal of the European Union. L 345.

[6] Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. „Protecting Europe for large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience“. 30.3.2009. COM(2009) 149 final.

[7] V. Radunović. 2013. DDoS - Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR).

[8] Nešković, A. Krajnović, N. Nešković, N. 2016. Studija izvodljivosti izgradnje nacionalnog CERT-a. Katedra za telekomunikacije Elektrotehničkog fakulteta Univerziteta u Beogradu.

[9] Cyber security of a power grid: State-of-the-art, Chih-Che Sun, Adam Hahn, Chen-Ching Liu;

[10] Cyber Security of the Smart Grids http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2712

[11] Закон о информационој безбедности, „Службени гласник РС“ бр. 6/2016 и 94/2017;

[12] Стратегија развоја информационе безбедности Републици Србији за период од 2017. до 2020. године, "Службени гласник РС", број 53 од 30. маја 2017.

[13] Стратегија за борбу против високотехнолошког криминала за период 2019–2023. године "Службени гласник РС", број 71 од 25. септембра 2018.

[14] E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” *IEEE Trans. Antennas Propagat.*, to be published.

[15] J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” *IEEE J. Quantum Electron.*, submitted for publication.

AUTORI

Prvi autor – Biljana Trivić, diplomirani inženjer elektrotehnike, Agencija za energetiku Republike Srbije, Elektrotehnički fakultete Beograd, biljana.trivic@aers.rs

Drugi autor – Darko Šošić, docent, Elktrotehnički fakultet Beograd, sosic@etf.rs