Razvoj sustava kibernetičke sigurnosti i nacionalne taksonomije u svrhu zaštite operatora ključnih usluga energetskog sektora

Development of cyber security and national taxonomy for the purpose of protecting key energy system operators

Antonijo Bolanča, univ.spe.mech.et nav.arch.
Hrvatski operator tržišta energije d.o.o.
antonijo.bolanca@hrote.hr

doc. dr. sc. Darko Pavlović
PLINACRO d.o.o.
darko.pavlovic@plinacro.hr

Sanja Šijanović Pavlović, prof.inf., mentor
Gimnazija Vukovar
psijanovic@gmail.com

Ključne riječi: Kibernetička sigurnost, Nacionalna taksonomija, Sigurnost energetskih sustava

Key words: Cyber Security, National Taxonomy, Security of Energy Systems

Sažetak

Energetski i IKT (informacijsko komunikacijske tehnologije) sektor danas predstavljaju dvije tehnološke grane koje sve više funkcioniraju u simbiozi, autori su došli do zaključka da određene IKT tehnologije imaju značajnu primjenu u energetskom sektoru, a energetski sektor pruža podršku IKT sektoru kroz osiguranje potrebne energije kroz primarna i rezervna napajanja. Takvi procesi integracije su neizbježni i predstavljaju evoluciju poslovanja. Autori u ovom stručnom članku analiziraju trenutne promjene u pristupu sigurnosti IKT podrške energetskim kompanijama. Aktivan pristup u praćenju IKT trendova, novih modela poslovanja i industrijskih tehnologija, preduvjet je održivom razvoju i dugoročnoj konkurentnosti energetskih kompanija. Iz tog razloga autori smatraju da će tehnološki naprednije kompanije ostvariti veću sigurnost sustava te lakše širiti poslovanje i prestizati konkurenciju. Razvojni potencijal sigurnosti energetskih sustava predstavlja novi interdisciplinarni izazov kojem se predviđa rast u vrlo bliskoj budućnosti. Cilj ovog rada je analiza trenutnog stanja te osnovno pojašnjenje problematike kibernetičke sigurnosti energetskih sustava sukladno novoj regulativi. S obzirom na trendove brzog povećanja kibernetičkih napada na energetske sustave, autori smatraju da je važno razmotriti sigurnosne aspekte integracije IKT tehnologija te predvidjeti alate, procedure, tehnologije i kadrove kojima takav sustav može nadvladati izazove.

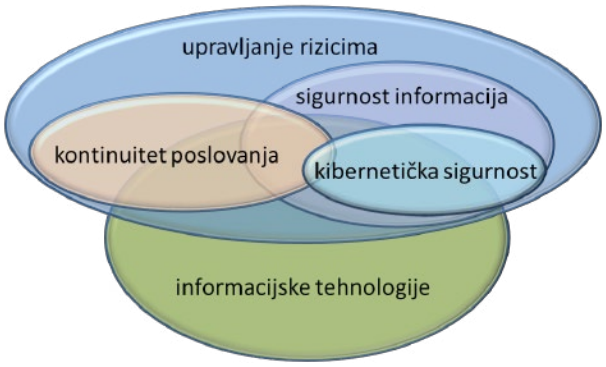
Abstract

The energy and ICT (engl. *Information and Communications Technology*) sectors today represent two technology branches that increasingly function in symbiosis, the authors have concluded that certain ICT technologies have significant application in the energy sector and the energy sector provides support to the ICT sector by providing the necessary energy through primary and backup power supplies. Such integration processes are inevitable and represent the evolution of business. Through this article, authors analyzed the current changes in access to ICT security support for energy companies. An active approach to tracking ICT trends, new business models and industrial technologies is a prerequisite for sustainable development and long-term competitiveness of energy companies. For this reason, authors believe that more technologically advanced companies will achieve greater system security, and will be able to expand their business and become more competitive. The development potential of energy system security represents a new interdisciplinary challenge that is expected to grow in the very near future. The aim of this paper is an analysis of the current state of affairs and the basic clarification of the cyber security of the energy systems in accordance with the new regulations. Given the rapid increase of cyber-attacks on energy systems, authors consider ICT important to consider security aspects of ICT technology integration.

1. Uvod

Kibernetička sigurnost vezana je uz tehnološki razvoj koji nigdje nije bio toliko dinamičan i sveobuhvatan kao što je u području komunikacijske i informacijske tehnologije. Cilj je uvijek usmjeravan ka brzom razvoju i uvođenju novih usluga i proizvoda, dok su sigurnosni aspekti u pravilu imali vrlo mali utjecaj na široko prihvaćanje novih tehnologija.

Korisnici IKT sustava unutar energetskih kompanija najčešće imaju minimalno znanje o tehnologiji koju koriste, a način primjene tehnologije je takav da je vrlo teško procijeniti sigurnosna obilježja većine komercijalnih proizvoda s obzirom na zaštitu povjerljivosti, odnosno privatnosti podataka korisnika. Sve je to dovelo do toga da se odnos energetskih kompanija prema komunikacijskoj i informacijskoj tehnologiji zasniva gotovo isključivo na korištenju bez evaluacije rizika i kontinuiteta poslovanja (Slika 1.).



Slika 1. Kibernetička sigurnost kao dio kompleksnog sustava
Izvor: www.kmco.com/resource-center/article/looking-forward/information-security-cyber-security-it-security-whats-the-difference/

Dok bi odstupanje u normalnom funkcioniranju jedne vrste komunikacijskog i informacijskog sustava energetskog sektora moglo proći nezapaženo, neispravan rad nekih drugih sustava mogao bi imati teške posljedice na funkcioniranje države, dovesti do gubitka života, zdravlja ljudi, velikih materijalnih šteta, onečišćenja okoliša i drugih funkcionalnosti bitnih za kvalitetno funkcioniranje društva u cjelini.

Od početaka razvoja komunikacijsko-informacijske tehnologije do danas, odstupanja u njihovom ispravnom radu nastajala su zbog različitih razloga, od ljudskih pogrešaka ili zlonamjernih postupaka, do tehnoloških grešaka ili organizacijskih propusta.

Digitalnim povezivanjem niza komunikacijskih i informacijskih sustava javnog, akademskog i gospodarskog sektora, stvoren je suvremeni kibernetički prostor koji sačinjava ne samo ova međusobno povezana infrastruktura, već i stalno rastuća količina raspoloživih podataka te korisnici koji međusobno komuniciraju u sve većem broju, pri čemu koriste rastući broj različitih usluga, neke potpuno nove, a neke tradicionalne, ali u novom virtualnom obliku.

Odstupanja od ispravnog rada IKT sustava energetskog sektora ili njihovih dijelova više nisu samo tehničke smetnje, već predstavljaju opasnost globalnih sigurnosnih razmjera. Njima se suvremena društva suprotstavljaju nizom različitih aktivnosti i mjera zaštite, koje skupno nazivamo kibernetička sigurnost.

S obzirom da se računala i računalne mreže danas mogu iskoristiti za izvođenje velikog broja potpuno neprihvatljivih i društveno iznimno opasnih ponašanja, bilo je potrebno žurno neka ponašanja kriminalizirati. U današnjoj IKT eri, brzina (odnosno sporost) kriminaliziranja koja se do prije koju godinu smatrala normalnom, jednostavno je daleko od prihvatljive.

Izvorni pojam kibernetika nastao je sredinom prošlog stoljeća i predstavlja znanost o sustavima automatskog upravljanja te općenito procesima upravljanja u biološkim, tehničkim, ekonomskim i drugim sustavima. Pridjevska inačica „kibernetički" danas se u hrvatskom jeziku uvriježila na sličan način i s istim, prethodno uvedenim značenjem kakvo ima i prefiks „cyber" u engleskom jeziku. Pojam „kibernetika" danas se u hrvatskom jeziku vrlo malo koristi u svom izvornom značenju, slično kao i pojam „cybernetics" u engleskom jeziku. U tehnički usmjerenim znanostima o upravljanju sustavima prevladava pojam automatsko upravljanje, a u širem smislu značenja pojma kibernetika, o procesima upravljanja u različitim sustavima, puno više se koristi teorija sustava, uvedena u drugoj polovini prošlog stoljeća.

Prepoznavanje važnosti sigurnosti kibernetičkog prostora kao zajedničke odgovornosti svih segmenata društva, iznimno je važno. Svrha nove zakonske regulative je sustavno i koordinirano provođenje aktivnosti potrebnih za podizanje sposobnosti RH u području kibernetičke sigurnosti, a s ciljem izgradnje sigurnog društva u kibernetičkom prostoru. Cilj je također i korištenje svih tržišnih potencijala informacijskog društva u cjelini te posebno proizvoda i usluga kibernetičke sigurnosti.

Poticanje koordinacije i suradnje svih državnih tijela i pravnih osoba s javnim ovlastima, ali i drugih sektora društva, nužno je kako bi se uspostavile nove funkcionalnosti, podigla učinkovitost rada relevantnih aktera te učinkovitije koristilo već postojeće resurse i bolje planiralo potrebu i ostvarenje novih rješenja.

Također, utvrđena su prioritetna područja kibernetičke sigurnosti za RH, koja su analizirana ponajprije u odnosu na opće ciljeve, a na isti način definirani su i posebni ciljevi svakog od utvrđenih područja kibernetičke sigurnosti za koje će se detaljnije provedbene mjere za postizanje visoke razine kibernetičke sigurnosti.

Posebna pažnja ovdje je usmjerena na definirane sektore društva i utjecaj svake poveznice područja kibernetičke sigurnosti na pojedine sektore društva, oblike suradnje i međusobne koordinacije rada dionika. Kao jedan od najvažnijih sektora društva smatra se energetski sektor. Važnost energetskog sektora proizlazi iz izravnog utjecaja na sve ostale sustave. U slučaju disfunkcije energetskog sustava, dolazi do domino efekta pada ostalih sustava kao što su: telekomunikacije, promet, bankarstvo, trgovina, zdravstvo… Shvaćajući važnost energetskog sektora, dolazimo do spoznaje o važnosti stabilnosti i otpornosti sustava na razne ugroze.

Važno je napomenuti problematiku socijalnog inženjeringa (niz tehnika upravljanja pojedincima), preko kojeg je moguće doći do povjerljivih službenih informacija ili ulaska u zaštićeni IKT sustav. Socijalni inženjering prisutan je u društvu sve od vremena antike i razvijao se sve do danas ali je tek sredinom 20-tog stoljeća poprimio oblik kakav danas postoji i to u četiri segmenta – sakupljanje informacija, uspostavljanje veze, pristupanje žrtvi te realizacija napada.

Metode socijalnog inženjeringa su:

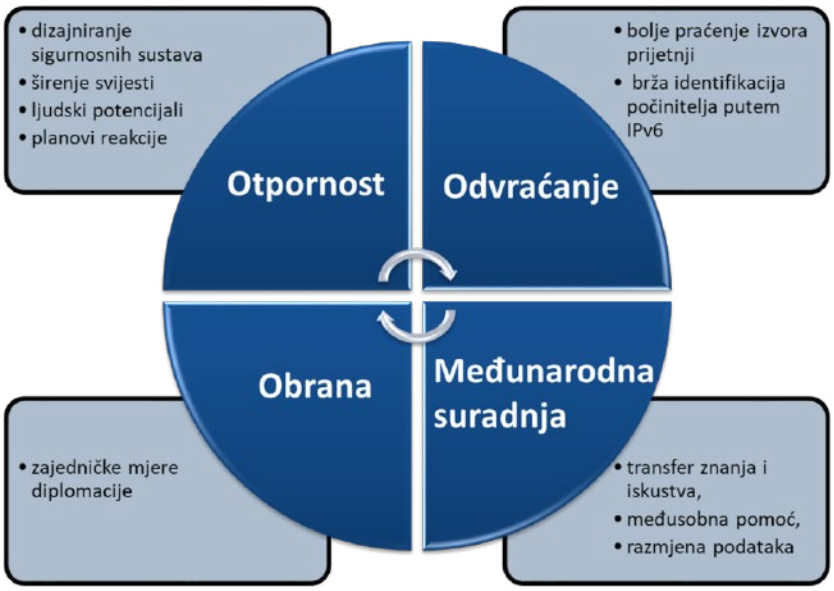
1. „Phishing" – slanje poruka s izvora koji djeluje pouzdano u svrhu dobivanja informacije ili utjecaja;
2. „Vishing" – sakupljanje informacija putem telefona, često uz lažiranje broja pozivatelja;
3. „Impersonation" – varka u kojoj pojedinac uz pomoć lažnog identiteta dobiva pristup informacijama i utjecaju.

Negativne posljedice su: materijalna dobit, gubitak informacija (privatne/službene, povjerljive), emocionalni pritisak (objava privatnih informacija, ucjene), korištenje podataka za daljnje napade te gubitak ugleda. S obzirom da je čovjek najranjiviji dio sustava potrebno je: osvijestiti se, čitati, kritički promatrati te biti savjestan i odgovoran i to kroz upoznavanje s vrijednostima podataka, provjeravanje identiteta, postupanje s povjerljivim podatcima sukladno procedurama te promišljenim djelovanjem.

2. Trenutno stanje

Promatrajući sustave koji su od iznimne važnosti za RH, vidljivo je, da dosad, nije bilo pokušaja da se osigura organizirani model upravljanja na bilo kojoj razini. Svaki od sustava samostalno se razvijao, bez jasnih ciljeva, koordinacije, sustava sigurnosti, komunikacije… Tokom takvih nekoordiniranih aktivnosti nastali su brojni projekti, mnogi od njih bili su iznimno kvalitetni, ali nisu bili dovoljno diseminirani prema ostalim dionicima. Svaki od sustava sam je učio i nadograđivao vlastite sposobnosti. Takav model doveo je do sadašnjeg stanja izrazite rascjepkanosti, gdje ne postoji sustav integralnog upravljanja, kontrole i komunikacije. Stoga je EU predložila jačanje zajedničkog odgovora na temelju: otpornosti, odvraćanja, obrane i međunarodne suradnje (Slika 2.).

Donošenje Nacionalne strategije kibernetičke sigurnosti i akcijskog plana za provedbu nacionalne



Slika 2. Mjere EU za jačanje zajedničkog odgovora

Tablica 1. Rang lista i trendovi kibernetičkih napada u EU za 2016. i 2017. godinu,

Najčešće prijetnje u 2016. trend u 2016.		Najčešće prijetnje u 2017. trend u 2017.		Trendovi rangiranja
Top Threats 2016	**Assessed Trends 2016**	**Top Threats 2017**	**Assessed Trends 2017**	**Change in ranking**
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Izvor: ENISA Threat Landscape Report 2017., 15 Top Cyber–Threats and Trends

strategije kibernetičke sigurnosti dalo je naslutiti brojne promjene u funkcioniranju sustava. Nakon donošenja direktive EU o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, počelo se polako uviđati da područje kibernetičke sigurnosti na nivou države zahtijeva moderniji i kvalitetniji sustav upravljanja. Taj sustav upravljanja trenutno je donesen samo za područje kibernetičke sigurnosti ali njegove poluge i mehanizmi predstavljaju model upravljanja koji će u budućnosti sigurno biti primjer pozitivne transformacije sveobuhvatnog poslovanja. Kako bi znali planirati sigurnosni sustav važno je imati ulazne statističke parametre o napadima u prethodnom razdoblju (Tablica 1).

3. Zakonodavni okvir

Pojam „kibernetički" uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu još 2002. godine. Konvenciju o kibernetičkom kriminalu donijelo je Vijeće Europe 23. studenoga 2001. godine, a stupila je na snagu 1. srpnja 2004.

Ukoliko promatramo zakonodavni okvir, važno je sagledati dvije grupe regulative. Prva grupa odnosi se na pravni okvir RH, a druga na pravni okvir EU. Te dvije grupe imaju različitu dinamiku, ali suštinski konvergiraju jedinstvenim rješenjima. Važno je napomenut da je EU 2004. godine osnovala Agenciju Europske unije za mrežnu i informacijsku sigurnost ENISA (ENISA engl. *European Union Agency for Network and Information Security*) koje predstavlja središte izvrsnosti za kibernetičku sigurnost u EU. Agencija je smještena u Grčkoj sa sjedištem u Heraklionu na Kreti i operativnim uredom u Ateni.

ENISA aktivno pridonosi visokoj razini mrežne i informacijske sigurnosti, takozvani NIS (engl. *Network and Information Security*) unutar EU. Nakon toga EU je 2. veljače 2013. donijela Strategiju kibernetičke sigurnosti, a Vlada Republike Hrvatske 7. listopada 2015. Odluku o donošenju Nacionalne strategije

Tablica 2. Popis ključnih usluga energetskog sektora nafte i plina

Energetski sektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Nafta	Transport nafte naftovodima	Bez iznimke	–
Nafta	Proizvodnja nafte	Proizvedeno nafte pojedinog naftnog polja u tonama godišnje	50.000 t/god
Nafta	Proizvodnja naftnih derivata	Proizvedeno naftnih derivata pojedine rafinerije u tonama godišnje	Motorni benzini: 200.000 t/god Dizelsko gorivo: 200.000 t/god Plinska ulja: 100.000 t/god
Nafta	Skladištenje nafte i naftnih derivata	Ukupni skladišni kapacitet nafte pojedinog terminala u m^3	1.000.000 m^3
Nafta		Ukupni skladišni kapacitet naftnih derivata pojedinog skladišta (na istoj lokaciji) u m^3	60.000 m^3
Plin	Distribucija plina	Broj krajnjih kupaca priključen na distribucijski sustav	Više od 100.000 obračunskih mjernih mjesta.
Plin	Transport plina	Bez iznimke	–
Plin	Skladištenje plina	Potrošnja plina u RH, u kWh	25 % potrošnje plina u RH u prethodnoj godini
Plin	Prihvat i otprema UPP – a	Kapacitet uplinjavanja UPP u m^3/h	Više od 500.000 m^3/h
Plin	Proizvodnja prirodnog plina	Godišnja proizvodnja plina predana u transportni sustav na pojedinom ulazu, u kWh	1.000.000 kWh

Izvor: Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)

kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/15). Potom je 6. srpnja 2016. donijeta Direktiva 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, takozvana NIS Direktiva (engl. *concerning measures for a high common level of security of Network and Information Systems across the Union*).

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga stupio je na snagu 26. srpnja 2018. (NN 64/18) Zakonom je propisan rok od 90 dana da svako nadležno sektorsko tijelo provodi postupak identifikacije operatora ključnih usluga po sektorima s popisa iz priloga I., gdje su navedeni i kriteriji za naftu i plin (Tablica 2.).

Također je propisano da svako nadležno sektorsko tijelo mora dostaviti obavijest u roku od 8 dana. Tada počinje teći rok od 30 dana nakon kojeg su Operatori ključnih usluga dužni obavijestit tijelo nadležno za prevenciju i zaštitu od incidenata (CSIRT engl: *Computer Security Incident Response Team*), bez neopravdane odgode te ga obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. Krajnji rok za početak slanja obavijesti, sukladno zakonu, je 1. prosinac 2018. Operatori ključnih usluga dužni su provesti mjere za osiguravanje visoke razine kibernetičke sigurnosti najkasnije do 1. studenoga 2019. godine.

Nakon zakona donesena je Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18), koja je stupila na snagu 4. kolovoza 2018. Uredbom je propisano da će u roku od 90 dana tijelo nadležno za prevenciju i zaštitu od incidenata, donesti smjernice za dostavu obavijesti o incidentima sa znatnim učinkom, kojima se određuje način dostave obavijesti i obrasci za obvezno obavješćivanje o incidentima sa znatnim učinkom. Konačni rok za donošenje smjernica je 2. studeni 2018. Iz dinamike implementacije proizlazi da su rokovi relativno kratki i da se od sudionika očekuje brza kadrovska i tehnološka transformacija.

Kao standard komunikacije dionika kibernetičke sigurnosti u lipnju 2018. donesena je Nacionalna taksonomija računalno-sigurnosnih incidenata. Nacionalna taksonomija računalno-sigurnosnih incidenata nastala je temeljem Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti. Prvi korak u provođenju ovog cilja definiranje je samog pojma računalno-sigurnosnog incidenta i njegove klasifikacije na nacionalnoj razini.

Kako bi svi dionici na području informacijske i kibernetičke sigurnosti na nacionalnoj razini imali ujednačene kriterije pri klasifikaciji događaja u svojim informacijskim sustavima i računalnim mrežama te kako bi uspješno generirali i razmjenjivali informacije o tim događajima potrebno je utvrditi zajednički jezik odnosno taksonomiju. Nakon prihvaćanja i usvajanja Nacionalne taksonomije računalno-sigurnosnih incidenata stvorit će se preduvjeti da sva tijela i institucije koje će razmjenjivati informacije o računalno-sigurnosnim događajima to čine tako da su svim sudionicima u toj razmjeni u potpunosti jasni i kontekst i detalji o pojedinom događaju ili incidentu.

Također će bit moguće započeti rad na ostalim dijelovima mjera koje uključuju definiranje protokola za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka. Bez prihvaćenog nacionalnog sustava klasifikacije, izgradnja platforme ili tehnologije za razmjenu podataka nije moguća.

Važno je znati da EU planira kontinuirano poboljšavati zakonodavni okvir, prateći nove tehnologije, prijetnje, napade, potreba zajednice gospodarstva i institucija. Sukladno tome, početkom ove godine raspisana je poziv vrijedan 50 miliona eura za pilot projekt razvoja mreže centara kibernetičke sigurnosti širom EU.

Osim zakonodavnog okvira koji se izravno tiče energetskog sektora, 30. siječnja 2018. donesena je Provedbena uredba komisije (EU) 2018/151, koja se odnosi na pružatelje digitalnih usluga. Uredba obuhvaća upravljanje rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava. S obzirom da su danas sve energetske kompanije primatelji digitalnih usluga, iznimno je važno da se proces podizanja kibernetičke sigurnosti usporedni i koordinirano provodi kod svih dionika kritične infrastrukture unutar kibernetičkog prostora.

4. Osnovna taksonomija računalno–sigurnosnih incidenata

Nacionalna taksonomija izrađena je korištenjem modela AVOIDIT taksonomije (engl. *Attack Vector, Operational impact, Defense, Information Impact, and Target*) razvijene na Odjelu za računalne znanosti Sveučilišta u Memphisu, SAD (*University of Memphis, Department of Computer Science*) uz uvažavanje iskustva i lokalnih specifičnosti u obradi računalno-sigurnosnih incidenata u RH. Namjena AVOIDIT taksonomije je da se računalni događaj,

Tablica 3. Tri bitna obilježja taksonomije prema ENISA–i

Klasifikacijska shema	• mogućnost da se povezani događaji svrstavaju u grupe
Rječnik	• važan za opis znanja i entiteta. Ovo je obilježje osobito bitno u hrvatskom jeziku, budući da velik dio pojmova iz domene kibernetičke sigurnosti nije moguće precizno označiti.
Mapa znanja	• mogućnost da korisnici u kratkom roku mogu razumjeti cjelokupnu strukturu računalno-sigurnosnog incidenta obrađenog taksonomijom.

odnosno incident klasificira korištenjem više atributa. Korištenjem te metode omogućava se jasno i precizno definiranje i međusobno razlikovanje pojedinih događaja i incidenata.

Taksonomija se također zasniva na korištenju atributa koji bi na nacionalnoj razini trebali omogućiti sveobuhvatan opis svih računalno-sigurnosnih incidenata i događaja čije uklanjanje zahtijeva razmjenu informacija i pravovremene odgovore s nadležnim CERT timovima.

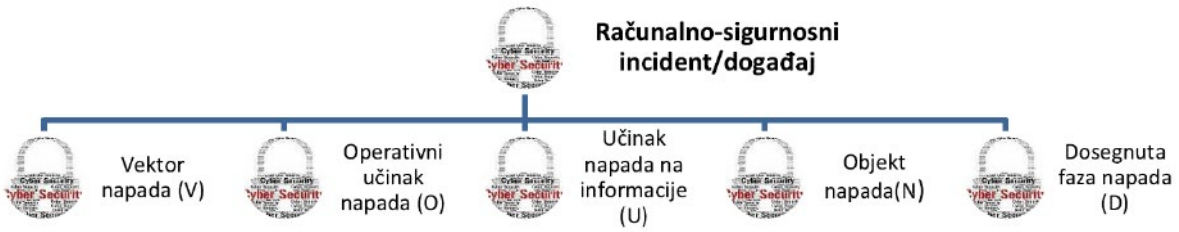
Kvalitetna klasifikacija računalno-sigurnosnih incidenata kompleksan je postupak budući da u kibernetičkom prostoru postoji više dionika koji kibernetičke događaje i računalno-sigurnosne incidente promatraju iz različite perspektive na različite načine. Primjerice, iako CERT-ovi *(engl. Computer Emergency Response Team)* i LEA *(engl. Law enforcement agency)* imaju isti zajednički cilj, oni na različiti način doprinose rješavanju i istrazi kibernetičkih incidenata. LEA prikupljaju informacije koje se mogu koristiti tokom istrage kako bi se utvrdili dokazi počinjenja kaznenog djela ili identificirao napadač ili napadači, dok su CERT-ovi ponajprije usmjereni na prikupljanje i obradu informacija o trenutačnim prijetnjama i vektorima napada s ciljem njihova otklanjanja te daljnjeg jačanja prevencije unutar kibernetičkog prostora. U Tablici 3. prikazana su tri bitna obilježja taksonomije prema ENISA-i.

Izrada taksonomije vođena je tako da zadovolji sva tri prethodno navedena obilježja te da bude prilagođena za korištenje što širem krugu budućih korisnika u Republici Hrvatskoj.

Prema modelu za navedenu AVOIDIT taksonomiju, Nacionalna taksonomija računalno-sigurnosnih incidenta koristit će akronim VOUND dobiven korištenjem početnih slova ključnih riječi pet atributa predloženih za opis računalno-sigurnosnih incidenta u Republici Hrvatskoj (Slika 3.):

- Vektor napada;
- Operativni učinak napada;
- Učinak napada na informacije;
- Objekt napada;
- Dosegnuta faza napada.

Prihvaćena Taksonomija koristit će se na nacionalnoj razini od strane energetskog sektora, tijela državne uprave te ostalih pravnih i fizičkih osoba. Kako bi se omogućilo prikupljanje i razmjena informacija među svim dionicima koji će koristiti



Slika 3. Atributi za opisivanje računalno–sigurnosnih incidenata
Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

predloženu Taksonomiju, neovisno o razini znanja o računalno-sigurnosnim incidentima te kako bi se omogućila adekvatna klasifikacija događaja/incidenata, na temelju eCSIRT.net klasifikacije incidenta, definiran je minimalni set informacija (atribut Operativni učinak napada kojim se opisuje direktan utjecaj napada na informacijski sustav ili njegove dijelove) koje je potrebno prikupiti i obraditi za svaki pojedini događaj/incident.

Taksonomija ima sljedeće karakteristike:

a) Jednostavno korištenje u svakodnevnom radu;
b) Jednoznačna klasifikacija računalno-sigurnosnog incidenta;
c) Jasna interpretacija klasificiranih računalno-sigurnosnih incidenta.

5. Vektor kibernetičkog napada

Vektor napada koristi se kao atribut opisa računalno-sigurnosnog incidenta kako bi se shvatio i opisao način (ruta) na koji napadač ostvaruje inicijalni pristup sustavu, odnosno napad. Identifikacija atributa Vektor napada može predstavljati izazov osobito kod napada visokog stupnja kompleksnosti gdje napadači posvećuju izuzetnu pažnju kamufliranju svakog koraka napada pa se tako i Vektor napada u velikom postotku slučajeva čini kao legitiman ili uobičajen tijek aktivnosti.

Tijekom napada nije neuobičajeno da napadači koriste više dostupnih vektora, ovisno o postojećim ranjivostima mete pa ovaj atribut ne predstavlja jedinstvenu metodu u identifikaciji napada. Identifikacija

Tablica 4. Vrijednosti koje ovaj atribut može poprimiti

Oznaka	Vrijednost	Opis
(V1)	Prijenosni mediji / uređaji	Napad je izveden korištenjem prijenosnog medija ili perifernog uređaja. Primjer: Širenje zlonamjernog koda putem zaraženog USBa ili CD/DVD-a.
(V2)	Napad na *web* tehnologije	Napad je izvršen korištenjem metoda povezanih s *web* tehnologijama i ranjivostima *web* aplikacija. Ovaj vektor napada između ostalog podrazumijeva: • *XSS* • *SQL injection* • *DNS Hijacking* • *Brute force* napadi na autentifikacijske mehanizme *web* aplikacija, zaporke, *CAPTCHA* zaštitu ili digitalne potpise • Napad na internetske preglednike u korisničkom okruženju.
(V3)	Napad na dostupnu mrežnu i računalnu opremu	Napad koji iskorištava ranjivosti računalnih mreža, ranjivih mrežnih uređaja, javno dostupnih poslužitelja ili računala. Ovaj vektor napada podrazumijeva između ostalog: • *(D)DoS* • *Man-ln-The-Middle* • Skeniranje javno dostupnih resursa • Lažne *wireless* pristupne točke • Utjecaj na otvorene portove javno izloženih poslužitelja.
(V4)	Fizički napad	Gubitak ili krađa opreme, računala ili medija za pohranu podataka. Namjerno ili nenamjerno fizičko djelovanje na opremu, računala ili medije. Ovaj vektor napada podrazumijeva između ostalog: • Otuđenje i instalaciju zlonamjernoga koda na • prijenosna računala, mobilne uređaje i sl. • Instalaciju zlonamjernoga koda ili uređaja na fizički izložene uređaje kao što su bankomati, POS uređaji i sl. • Instalaciju zlonamjernoga koda ili zlonamjernih dijelova operativnog sustava prilikom proizvodnje ili isporuke računalne opreme.
(V5)	Socijalni inženjering	Vektor napada koji se oslanja na ljudsku interakciju i najčešće uključuje navođenje ljudi na kršenje uobičajenih sigurnosnih procedura. Ovaj vektor napada podrazumijeva između ostalog: • Pokušaj otkrivanja povjerljivih informacija lažnim predstavljanjem • *Phishing* - slanje e-mail ili SMS poruka s priloženim zlonamjernim dokumentima ili poveznicama na zlonamjerne *web* sadržaje • Navođenje na preuzimanje zlonamjernog sadržaja, zlonamjernih mobilnih aplikacija i sl.
(V6)	Napad iz unutrašnjeg okruženja	Napad koji uključuje korištenje informacija, pristupnih podataka i resursa dostupnih isključivo legitimnom korisniku koji te resurse koristi u zlonamjerne svrhe ili suprotno internim politikama i standardima.
(V7)	Nepoznato	Rana faza otkrivanja incidenta u kojem još nije poznat vektor napada.

Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

Tablica 5. Klasifikacija napada prema operativnom učinku

Oznaka	Vrijednost	Oznaka	Potkategorije	Opis
(01)	Kompromitacija	(011)	*Malware URL*	*Malware URL* podrazumijeva kompromitiran *web* poslužitelj s postavljenim zlonamjernim kodom.
		(012)	*Phishing URL*	*Phishing URL* podrazumijeva kompromitiran *web* poslužitelj s postavljenom lažiranom stranicom čija je svrha krađa podataka.
		(013)	*Spam URL*	*Spam URL* podrazumijeva kompromitiran *web* poslužitelj s neovlašteno postavljenim reklamnim sadržajem.
		(014)	*Web Defacement*	*Web Defacement* podrazumijeva kompromitiran *web* poslužitelj s izmijenjenim izgledom i sadržajem *web* stranice.
		(015)	Sustav zaražen zlonamjernim kodom	Podrazumijeva računalo ili neki drugi uređaj zaražen zlonamjernim kodom. Botovi, tj. računala pod kontrolom napadača spadaju u ovu kategoriju.
		(016)	C&C	C&C podrazumijeva kontrolni poslužitelj za nadzor i upravljanje računalima koja su dio botneta.
		(017)	Korisnički račun	Korisnički račun podrazumijeva kompromitaciju korisničkog računa.
(02)	Prikupljanje informacija	(021)	Skeniranje	Skeniranje podrazumijeva neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima.
		(022)	Phishing	Navođenje korisnika na odavanje podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte).
		(023)	Sniffing	Sniffing podrazumijeva neovlašteno presretanje mrežnog prometa.
(03)	Pokušaj neovlaštenog pristupa	(031)	Pogađanje zaporki	Pogađanje zaporki podrazumijeva neovlašten pokušaj pristupa računalnom sustavu višestrukim pogađanjem zaporke.
		(032)	Pokušaj iskorištavanja ranjivosti	Pokušaj iskorištavanja ranjivosti podrazumijeva pokušaj iskorištavanja ranjivosti na računalnom sustavu kako bi se ostvario neovlašten pristup ili utjecalo na tajnost ili cjelovitost podataka.
(04)	Uskraćivanje dostupnosti	(041)	Volumetrički napad	Volumetrički napad podrazumijeva napad slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti.
		(042)	Napad na aplikacijskom sloju	Napad na aplikacijskom sloju podrazumijeva slanje većeg broja zahtjeva prema računalnom sustavu s ciljem iskorištavanja resursa sustava ili iskorištavanje sigurnosnog propusta koje dovodi do prestanka rada aplikacije.
(05)	Neželjene elektroničke poruke, uvredljiv sadržaj, uznemiravanje, dezinformiranje	(051)	Spam	Spam podrazumijeva neželjenu elektroničku poruku reklamnog sadržaja.
		(052)	Hoax	Hoax podrazumijeva poruku elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja.
(06)	Ciljani napad - *APT (engl. Advanced persistent threat)*			*APT* podrazumijeva ciljani napad na određenu žrtvu uz korištenje većeg broja naprednih tehnika i tehnologija.
(07)	Prijevare			Ova klasa događaja uključuje događaje koji se mogu kategorizirati kao kibernetički kriminal, a podrazumijeva razne vrste prijevara na internetu, od lažnog predstavljanja, prijevara prilikom trgovine na internetu i sl. U ovu klasu događaja ne spadaju financijske prijevare koje uključuju instalaciju zlonamjernoga koda.
(8)	Ostalo			Podrazumijeva sve događaje koji ne mogu biti opisani ranije navedenim atributima, a za koje korisnik smatra da se radi o računalno-sigurnosnom incidentu.

Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

i shvaćanje atributa Vektor napada vrlo često može predstavljati jedan od ključnih koraka u atribuciji napada (Tablica 4.).

6. Operativni učinak kibernetičkog napada

Klasifikacija napada prema operativnom učinku predstavlja atribut kojim se opisuje izravan utjecaj napada na IKT sustav ili povezane dijelove. Atribut Operativni učinak napada određen je kao osnovni set informacija koje je potrebno prikupiti, obraditi i analizirati, jer daje odgovor na pitanje što se zapravo dogodilo s napadnutim IKT sustavom ili računalnom mrežom. Identifikacija atributa Operativnog učinka napada parcijalno odgovara i na pitanje koja je motivacija i cilj napadača u provođenju napada.

U Tablici 5. navedene su vrijednosti koje ovaj atribut može poprimiti. Tokom konkretnog napada atribut Operativnog učinka napada najčešće preuzima različite vrijednosti ovisno o fazi napada, pa tako najčešće prilikom prikupljanja informacija u kasnijoj fazi napada prelazi u vrijednost kompromitacije ili pokušaja neovlaštenog pristupa. Iz tog je razloga često nemoguće nedvosmisleno identificirati vrijednost ovog atributa, odnosno on se mijenja ovisno o fazi napada.

7. Učinak kibernetičkog napada na informacije

Krajnji cilj svakog kibernetičkog napada ostvarivanje je učinka na podatke/informacije u smislu narušavanja jednog od tri osnovna principa IKT sigurnosti: povjerljivosti, cjelovitosti i dostupnosti podataka. Kroz atribut Učinak napada na informacije klasificira se utjecaj napada na štićene informacije te pojašnjava kriterije za odabir vrijednosti atributa (Tablica 6.).

8. Objekt kibernetičkog napada

Kroz atribut Objekt napada klasificira se vrsta IKT infrastrukture koja je meta kibernetičkog napada. Pravilnom klasifikacijom ovog atributa moguće je donijeti zaključke o motivima napadača te o budućem tijeku širenja incidenta. Slično kao i kod atributa

Tablica 6. Učinak kibernetičkog napada na informacije

Oznaka	Vrijednost	Opis
(U 1)	Izmjena / iskrivljavanje	Narušavanje cjelovitosti informacije, uobičajeno tako da tijekom napada dođe do promjene ili »iskrivljavanja« podataka.
(U 2)	Nedostupnost (Uskraćivanje pristupa ili sl.)	Uskraćivanje dostupnosti servisa koji omogućava pristup informaciji, uobičajeno uslijed (D)DoS napada.
(U 3)	Uništenje	Do uništenja informacija uobičajeno dolazi kada napad za konačni cilj ima brisanje podataka ili uklanjanje pristupnih prava.
(U 4)	Otkrivanje	Otkrivanje informacija podrazumijeva situaciju u kojoj napadač ostvari »uvid« u informacije kojima u normalnim okolnostima ne bi imao pravo pristupa.
(U 5)	Nepoznato	Rana faza otkrivanja incidenta u kojoj još nije poznat učinak napada na informacije.

Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

Tablica 7. Objekt kibernetičkog napada

Oznaka	Vrijednost	Opis
(N 1)	Upravljačka infrastruktura	Napadna kritične dijelovesustava koji koordiniraju aktivnosti i upravljaju resursima informacijskog sustava (npr. Active Directory).
(N 2)	Računalna mreža	Napad na mrežnu infrastrukturu.
(N 3)	Lokalno računalo	Napadkojem jekrajnji cilj kompromitacija lokalnog računala (pojedinačnog korisnika).
(N 4)	Korisnik	Napad na korisnika predstavlja napad koji za cilj ima prikupljanje korisnikovih osobnih informacija.
(N 5)	Aplikacijski sustav	Napad na aplikacijski sustav predstavlja napad na specifičnu aplikaciju ili njen dio u svrhu uskraćivanja dostupnosti, kompromitacije podataka ili daljnjeg širenja opsega napada.
(N 6)	Ostalo	Objekt napada koji nije opisan prethodno definiranim vrijednostima.

Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

Operativni učinak napada i ovaj atribut najčešće mijenja vrijednost ovisno o fazi napada. Iz tog je razloga često nemoguće nedvosmisleno identificirati vrijednost koje ima ovaj atribut (Tablica 7.).

9. Dosegnuta faza kibernetičkog napada

Kroz atribut Dosegnuta faza napada identificira se trenutni stadij kibernetičkog napada. Iako se u stvarnim situacijama faze kibernetičkog napada najčešće izmjenjuju u izrazito kratkim vremenskim intervalima, moguće je identificirati trenutnu fazu u kojoj se zlonamjerni akteri i zlonamjerna kampanja nalaze. Ispravnom i pravovremenom klasifikacijom ovog atributa moguće je donijeti ispravne odluke o obrambenim strategijama koje mogu spriječiti napadača u prelasku u daljnje faze napada, nakon čega obrambeno djelovanje može imati značajno sužene mogućnosti (Tablica 8.).

10. Mogućnosti daljnje razrade taksonomije i primjene u budućnosti

Taksonomiju je potrebno koristiti kao alat koji će omogućiti efikasnu razmjenu informacija u svrhu bržeg uočavanja i sprječavanja računalno-sigurnosnih incidenta. Nacionalna taksonomija računalno-sigurnosnih incidenata omogućava:

a) Brzu identifikaciju i opis računalno-sigurnosnog incidenta i događaja kroz pet atributa karakterističnih za svaki kibernetički napad.
b) Otvaranje prostora za dodatnu nadogradnju pojedinih atributa u slučajevima pojave novih vrsta prijetnji (npr. nova vrsta vektora napada).
c) Korištenje atributa za izradu detaljnih statističkih izvještaja unutar pojedine organizacije ili na nacionalnoj razini za potrebu praćenja trendova i uspješnosti korištenja obrambenih mehanizama.

Korištenjem atributa Objekt napada i Dosegnuta faza napada pruža mogućnost praćenja tijeka napada ili kampanje uz mogućnost brzog predviđanja sljedećeg koraka napadača.

Postoje smjerovi koji primarno nisu u opsegu izvornog cilja uspostave sustava za razmjenu informacija i razvoja Nacionalne taksonomije računalno-sigurnosnih incidenata, ali se mogu razmatrati kao nadogradnja i budući smjerovi razvoja sustava.

Tablica 8. Dosegnuta faza kibernetičkog napada

Oznaka	Vrijednost	Opis
(D1)	Izviđanje	Faza napada u kojoj napadač prikuplja informacije o meti i priprema strategiju napadaovisno o otkrivenim ranjivostima. Ova faza najčešće uključuje skeniranje automatiziranim alatima, prikupljanje e-mail kontakata za potencijalnu upotrebu mehanizama socijalnog inženjeringa i sl.
(D2)	Isporuka	Faza napada u kojoj napadač aktiviramehanizme provođenja kibernetičkog napada. Ovu fazu uobičajeno obilježava slanje e-mail poruka sa zlonamjernim sadržajem ako se radi o kibernetičkom napadu koji koristi zlonamjeran kod ili pokretanje alata za generiranje zlonamjernih upita ako se radi o napadu uskraćivanja dostupnosti.
(D3)	Ostvarivanje pristupa	Faza napadau kojoj napadač iskorištavauočene ranjivosti sustava i ostvaruje pristup ciljanom sustavu. Uobičajeno, napadač u ovoj fazi instalira zlonamjeran kod,maksimal noeskalirapriviligije,ovisno o cilju proširuje djelokrug napadaširenjem na povezane sustave i računala i sl.
(D 4)	Potpuna kompromitacija	Završna faza napada iz perspektive napadača u kojoj se ostvaruju ciljevi i motivacija za napad. Ova faza uobičajeno podrazumijeva eksfiltraciju, uništenje ili izmjenu podataka, uskraćivanje usluge i servisa, pokretanje novih napada korištenjem resursa kompromitiranog sustava i sl.
(D 5)	Perzistencija	Faza napada u kojoj napadači ostvaruju trajnu prisutnost u kompromitiranom sustavu uz aktivirane sposobnosti sprječavanja detekcije.
(D 6)	Nepoznato	Nije moguće odrediti fazu napada.

Izvor: Nacionalna taksonomija računalno–sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava

Planiranje sustava nacionalne procjene rizika kibernetičkih napada. Također, moguće je razviti i integraciju sa sustavom klasifikacije incidenata/događaja TLP (TLP, engl: *Traffic Light Protocol)*.

Automatizacija - potencijalnim automatiziranjem postupka prepoznavanja incidenta i klasificiranjem moguće je razviti sustav predlaganja strategije i mehanizma obrane u ranoj fazi kibernetičkog napada.

11. Razvoj kibernetičke sigurnosti

Budući razvoj kibernetičke sigurnosti energetskog sektora vezan je uz penetraciju interneta u brojne nove uređaje i sustave, odnosno Internet of Things (skraćeno: IoT) u hrvatskom jeziku slobodno prevedeno kao Internet stvari te njegov napredniji oblik nazvan Internet of Everything (skraćeno IoE) u hrvatskom jeziku slobodno prevedeno kao Internet svega, predstavljaju mrežu elemenata opremljenih za prikupljanje obradu i razmjenu podataka.

IoE čine četiri ravnopravna ključna elementa: ljudi (njihovo međusobno povezivanje), procesi (isporuka pravih podataka pravoj osobi (stvari) u pravo vrijeme), podaci (pretvaranje podataka u vrijednije informacije radi donošenja efikasnijih i efektivnijih odluka) i stvari (fizički uređaji i objekti povezani internetom i između sebe radi donošenja kvalitetnijih odluka) dok je fokus IoT-a pomaknut na stvari - različite vrste uređaja koji su opremljeni senzorima i spojeni preko interneta kako bi mogli komunicirati. Osim toga, IoE dodatno unapređuje moć IoT-a kroz poboljšanje rezultate poslovanja i industrije, te u konačnici poboljšao živote ljudi prateći napredak IoT-a.

Iako IoT nudi još mnogo neistraženih mogućnosti, iznimno je brzo evoluirao od prve glasine do gotovo neprimjetnog dijela našeg života. Ta transformacija protekla je tako glatko, gotovo da je nismo bilo niti svjesni. Kao primjer danas naši telefoni sadrže različite senzore koji stalno bilježe i prenose ogromne količine informacija bez da mi primjećujemo ili smo svjesni toga, naše kuće i automobili jesu »Pametniji« nego ikada prije, infrastruktura koja nas okružuje (ulica, svjetla, dizala, stepenice, transport, tvornice, energetski sustavi) sadrži bezbroj senzora koji su neophodni za njihovo održavanje i sigurnost.

Riječ je, dakle, o različitim vrstama uređaja koji su opremljeni senzorima i spojeni preko interneta kako bi mogli međusobno komunicirati, komunicirati s nama, našom kućom, uređajima, vozilima te kako bi mogli pratiti privatne i poslovne aktivnosti, kako bi nas mogli savjetovati, upozoriti ili na kraju krajeva, sami obaviti dio posao za koji su im dane informacije, alati i ovlasti.

IoT je bitan pokretač za inovacije usmjerene prema kupcima, takav sustav podiže optimizaciju i automatizaciju podataka, digitalnu preobrazbu i omogućava potpuno nove aplikacije, modele poslovanja i tokove prihoda u svim sektorima. IoT je treći val u ciklusu razvoja interneta i predstavlja logičan sljedeći korak u razvoju.

IoT konvergira industrije i specijalizacije, spaja informacijsku tehnologiju i operativnu tehnologiju (IT i OT) te pridonosi industrijskoj preobrazbi (industrija 4.0) i valom primjene slučajeva koji su međusektorski ili tipični za određeni sektor.

Svaka stvar je jedinstveno prepoznatljiva kroz ugrađeni računalni sustav IoT-a ali je također u stanju surađivati unutar postojeće internetske infrastrukture. Pravni stručnjaci upućuju da pojam stvari u nazivu predstavlja neodvojivu mješavinu hardvera, softvera, podataka i usluga. Takvi uređaji prikupljaju korisne podatke uz pomoć različitih postojećih tehnologija a zatim samostalno prenose, dijele i obrađuju podatke između drugih uređaja. Koncept IoT-a odnosi se na povezanost različitih fizičkih objekata putem interneta, a prvi put ga je spomenuo britanski poduzetnik Kevin Ashton, iz Procter & Gamblea, kasnije zaposlenik MIT-ovog Auto-ID Centra, 1999. godine.

IoT postaje veliki posao budućnosti te će zasigurno biti u fokusu četvrte industrijske revolucije odnosno sveopće digitalizacije koja podrazumijeva senzore u svim područjima, život u cloudu (oblaku) i internetsku povezanost ne samo nas već i svega što nas okružuje. Prema nedavnoj Gartnerovoj analizi 15 % kompanija već koristi IoT u svom poslovanju, najčešće logistici. Predviđanja stručnjaka su da će taj postotak izrazito brzo će rasti u sljedećim godinama.

IoT omogućava tri tipa komunikacije:

- Komunikacija stvari (uređaja) s ljudima;
- Komunikacija između stvari (uređaja);
- Komunikacije između uređaja (engl. machine to machine / M2M).

IoT koncept omogućuje interakciju ljudi s uređajima i uređaja s uređajima, integrirajući ih u mrežu kojom se upravlja putem web-aplikacija. Mogućnosti primjene IoT aplikacija su široke i raznolike, a prožimaju gotovo sva područja ljudskog djelovanja pa tako između ostalog i područja energetskog sektora.

Važna djelatnost energetskog sektora predstavlja uravnoteženje proizvodnje energije s potražnjom na ekonomičan način.

Za većinu svijeta energija je vrlo pouzdana i relativno jeftina ali to nije uvijek postignuto na najučinkovitiji način. Ovo je područje gdje IoT može imati veliki utjecaj, utječući na način generiranja, distribucije, potrošnje i pohrane energije. Više nego ikada prije, postoje brojne mogućnosti za postojeće tvrtke i nove start-up kompanije da značajno unaprijede sektor energetike. IoT donosi potpuno novu dimenziju u pogledu poslovanja. Uvid koji proizlazi iz podataka prikupljenih s internetom povezanih uređaja može se koristiti za razvoj novih usluga, povećanje produktivnosti i učinkovitosti, poboljšanje donošenja odluka u stvarnom vremenu, rješavanje ključnih problema i stvaranje novih i inovativnih poslovnih odluka.

Procesno gledajući, Internet stvari predstavlja integraciju različitih sustava, koji trenutno pružaju potporu poslovnim procesima ali su u svojoj strukturi odvojeni i pružaju potporu na različitim nivoima poslovanja. IoT na nivou tipične energetske kompanije predstavlja integraciju i komunikaciju sljedećih sustava:

- ERP - Enterprise resource planning;
- MES - Manufacturing execution system;
- SCADA - Supervisory control and data acquisition.

12. Kibernetička sigurnost SCADA sustava

Velik dio kritične infrastrukture u Europi koja se nalazi u sektorima kao što su energetika, transport i vodoopskrba uglavnom se upravlja i kontrolira sustavima SCADA (nadzorno upravljanje i prikupljanje podataka), podskupine industrijskih sustava kontrole (ICS engl. *Industrial Control Systems*). U proteklom desetljeću SCADA tehnologija prošla je transformaciju, od izoliranih sustava u otvorene arhitekture i standardne tehnologije koje su visoko povezane s drugim korporativnim mrežama i internetu.

Posljedica ove transformacije je povećana ranjivost prema vanjskim napadima. Jedan od načina da se poboljša sigurnost SCADA-e je pravovremena i kvalitetna primjena zakrpi. Dva od ključnih važnih problema s zakrpama u ovom trenutku su stopa neuspjeha zakrpi i nedostatak zakrpi za SCADA sustave.

Primjena zakrpi mogla bi imati značajan utjecaj na operativno ponašanje SCADA sustava. Kada zakrpa nije temeljito testirana, može uvesti nepoznanice u sustav, što nije prihvatljivo za okoliš koji koristi. SCADA sustavi obično se primjenjuju kako bi ostali operabilni duže od redovitih IKT sustava. Tijekom tog vremena potrebne su zakrpe za ispravljanje sigurnosnih i funkcionalnih problema softvera i firmwarea.

Iz perspektive sigurnosti, zakrpe su važne jer ublažavaju ranjivosti softvera, primjena zakrpa smanjuje mogućnost incidenata. Zakrpe se također mogu koristiti za dodavanje novih značajki ili poboljšanje postojećih značajki softvera i firmwarea. Međutim, sa sigurnosne točke gledišta, zakrpe i ažuriranja softvera također mogu predstavljati rizik jer mogu nenamjerno promijeniti ponašanje komponente na način koji ugrožava stabilnost procesa. Zbog toga potrebno je razdvojiti razvojnu, testnu i produkcijsku okolinu te provesti testiranje i provjera ranjivosti prije uvođenja u rad nove zakrpe ili sustava.

Instalacija i distribucija zakrpa na redovnoj osnovi teško je organizacijama i dobavljačima zbog proceduralnih i tehničkih problema vezanih uz njega. Zakrpa se ne smije smatrati jedinstvenom metodom obrane, dobra je praksa povećati obranu u dubini (engl. DiD - *defense in depth*) pomoću kompenzacijskih kontrola. Pojam »obrana u dubini« izraz koji se odnosi na strategiju u kojoj se koriste višestruki slojevi obrane kako bi se spriječili napadi.

Važni elementi obrambene strategije za SCADA sustave su:

a) Stvoriti svijest i razumijevanje u organizacijama o tome što neuspjeh SCADA sustava može značiti za rad organizacije i koje su politike i najbolje prakse vezane uz upravljanje zakrpama i sigurnost u cjelini. Potrebno je uspostaviti program osposobljavanja s relevantnim informacijama o poslovanju kako primijeniti sigurnost i kako odgovoriti na situacije koje ugrožavaju sigurnost.

b) Stvrdnjavanje SCADA sustava, otvrdnjavanje sustava znači uklanjanje nepotrebnih značajki i zaključavanje funkcionalnosti raznih komponenti SCADA sustava. Na primjer, Microsoft Windows sadrži mnoge različite aplikacije i usluge koje nisu potrebne za operacije, te ih treba ukloniti ili onemogućiti.

c) Vatrozid bi trebao biti konfiguriran na način koji omogućuje samo povezivanje između pouzdanih računala i pouzdanih portova. Drugi portovi trebaju biti zatvoreni kada nisu u uporabi. Vatrozidi bi također trebali implementirati mehanizme za izvješćivanje o alarmima kako bi upozorili kada se otkriva ponašanje izvan zadanih parametara. Sustavi za otkrivanje upada (engl. IDS - *Intrusion Detection System*) također

se mogu koristiti za otkrivanje takvog ponašanja. Tamo gdje je to primjenjivo, jednosmjerne komunikacijske diode mogu pružiti još višu razinu zaštite. DPI vatrozidni paketi (engl. *Deep Packet Inspection*) također se mogu koristiti za provjeru prometa za čudno oblikovane poruke ili neobičnog ponašanja.

Povećajte obranu u dubini kroz segmentaciju mreže. Segmentacija mreže je složena mjera ali osnove su jednostavne. Skup opreme trebao bi se utvrditi temeljem povjerenja i sličnosti i postaviti u različite zone. Sljedeći korak je identificirati koje komunikacije trebaju proći između zona. Na mjestima gdje zone komuniciraju potrebno je postaviti kontrole pristupa kao što su vatrozidi.

Provođenje redovitih procjena rizika i sigurnosti radi smanjenja mogućih sigurnosnih rizika. Smanjuju se rizici koji se ne mogu otkloniti i preostali rizik kontrolira.

AWL, odnosno aplikacija bijelog popisa (AWL engl. *Application White Listing*) za kompromitaciju malwarom i izvođenja zlonamjernog softvera definiranjem dopuštenih aplikacija na sustavu i ograničavanjem ostalih aplikacija iz pokretanja.

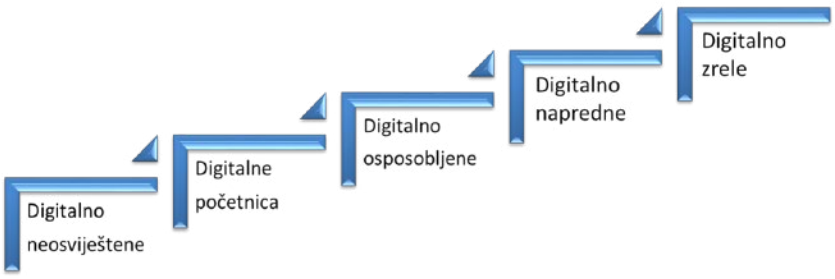
Između vremena kada se otkrije i / ili objavljuje ranjivost, druge se kontrole također mogu koristiti za privremeno ublažavanje ranjivosti. Postavke ili konfiguracija sustava mogu se promijeniti (privremeno) za blokiranje poznatih napadačkih vektora. Ove izmjene neće ispraviti temeljnu ranjivost, ali će smanjiti rizik da se te ranjivosti iskoriste. Dobavljači osnovne telekomunikacijske opreme često predlažu promjene konfiguracije svojim klijentima. Microsoft također nudi tu uslugu, koji je uključen u većinu sigurnosnih biltena, dio je »Rješenja za rješavanje problema« koji opisuje kako se sustav može mijenjati kako bi se smanjio rizik mogućeg iskorištavanja. Nema puno SCADA dobavljača nude sličnu strategiju, ali postoje brojne mogućnosti. Na primjer, ako se na web poslužitelju pronađe ranjivost, a poslužitelj ne upotrebljava nikakva poslovna kritična operacija, web poslužitelj bi se mogao privremeno onemogućiti ili se na vatrozidu ili IDS-u mogu implementirati posebna pravila za otkrivanje zlonamjernog ponašanja. Buduće aktivnosti oko održavanja i nadogradnje SCADA sustava, sigurno će morati uzeti u obzir nove sigurnosne politike i procedure. Takav pristup u početku dovodi do sporije implementacije, ali dugoročno podiže sigurnost sustava te predstavlja jedini ispravan put daljnjeg razvoja.

13. Trenutni projekti u obrazovanju

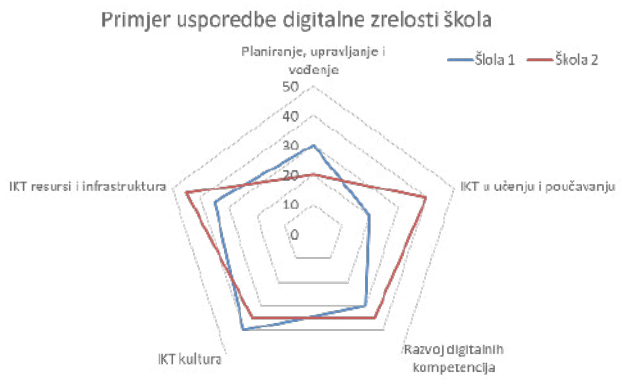
Razvoj sustava kibernetičke sigurnosti uvelike ovisi o znanju i vještinama. Takva specifična znanja važno je razvijati kroz programe obrazovanja, a kasnije ih usavršavati i nadograđivati na akademskom nivou. Iznimno je važno da obrazovni sustav prepozna i na vrijeme započne sa projektima i edukacijama o sigurnom korištenju IKT sustava kako bi stvorili temelje za nadgradnju u kasnijem obrazovanju. Portal antibot.hr je Nacionalni centar potpore koji korisnicima omogućuje detekciju i uklanjanje zlonamjernih programa s računala.

To je usluga Nacionalnog CERTa (engl. *Computer Emergency Response Team*) koji je odjel Hrvatske akademske i istraživačke mreže – CARNET. Nacionalni CERT bavi se incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru, osim tijela državne uprave za koje je nadležan CERT ZSIS (CERT Zavoda za sigurnost informacijskih sustava).

Oni u sklopu projekta e-Škole razvijaju pilot projekt pod nazivom Uspostava sustava razvoja digitalno zrelih škola, održavaju sustav za upravljanje sigurnosnim informacijama i događajima (engl. *Security Information and Event Manager* - SIEM) s ciljem sigurnosnog nadzora CARNET-ove mreže,



Slika 4. Razine digitalne zrelosti škole koje se promatraju za svako područje



Slika 5. Primjer usporedbe digitalne zrelosti škola prema područjima

CARNET-ovih kritičnih usluga te škola uključenih u projekt e-Škole.

Nacionalni CERT kao partner sudjeluje u provedbi europskog projekta CEKOM (Centar kompetencija). Cilj projekta je povećati konkurentnost hrvatskog gospodarstva poticanjem inovativnosti poslovnog sektora i suradnje sa znanstveno-istraživačkim institucijama u području kibernetičke sigurnosti upravljačkih sustava (uključujući i industrijske upravljačke sustave – engl. *Industrial Control System*, ICS).

E-školstvo je globalni izazov a uspješna informatizacija je dugoročna strateška vizija školstva koja podrazumijeva kontinuirani razvoj nastavnih planova, načina učenja i poučavanja, stručno usavršavanje nastavnika i školskih rukovodećih kadrova uz korištenje IKT-a. U izazov se upustio CARNet (Hrvatska akademska i istraživačka mreža) pokrenuvši pilot projekt "e-Škole: Uspostava sustava razvoja digitalno zrelih škola ". Pilot projekt e-Škole dio je šireg programa e-Škole pri čemu se program e-Škole provodi kroz više projekata informatizacije školskog sustava, u razdoblju od 2015. do 2022. godine. Program se sastoji od pilot projekta čija je provedba započela 2015. godine i završila u kolovozu 2018. te druge faze projekta čija se provedba planira u razdoblju od 2019. do 2022. godine, a koja će počivati na rezultatima pilot projekta. Puni naziv cjelokupnog programa glasi "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće". U pilot projektu e-Škole sudjelovala je 151 škola među kojima je i Gimnazija Vukovar. Projekt je obuhvatio više od 7000 nastavnika i preko 23 000 učenika.

Škole koje su uključene u pilot projekt značajno su napredovale u primjeni digitalnih tehnologija. Okvir za digitalnu zrelost škola, izrađen u suradnji sa stručnjacima Fakulteta organizacije i informatike Sveučilišta u Zagrebu, definirao je pet područja (Planiranje, upravljanje i vođenje, IKT u učenju i poučavanju, Razvoj digitalnih kompetencija, IKT kultura i IKT resursi i infrastruktura) i pet razina digitalne zrelosti škola (Digitalno neosviještena, Digitalna početnica, Digitalno osposobljena, Digitalno napredna i Digitalno zrela) te je predstavljao temelj za vanjsko vrednovanje digitalne zrelosti (Slika 4. i 5.).

U listopadu 2016. godine provedeno je početno vanjsko vrednovanje digitalne zrelosti koje je pokazalo kako su na skali od 1 (digitalno neosviještene škole) do 5 (digitalno zrele škole), naše škole u prosjeku na razini 2, odnosno u kategoriji digitalnih početnica. Nakon 18 mjeseci provođenja projekta, promatrajući ukupnu razinu, čak 93 % škola uključenih u pilot projekt sada se nalazi na razini digitalno osposobljenih (razina 3) odnosno digitalno naprednih (razina 4) škola.

Organizacija Ujedinjenih naroda za obrazovanje, znanost i kulturu (UNESCO) proglasila je CARNET-ov pilot projekt „e-Škole: Uspostava sustava razvoja digitalno zrelih škola" jednim od 12 najboljih projekata u svijetu u području primjene IKT-a u obrazovanju za 2017. godinu u konkurenciji od 143 prijavljena projekta iz 79 zemalja.

14. Zaključak

Internet je razbio prepreke između država i građana, čime je omogućeno dijeljenje informacija širom svijeta. Danas mreže i informacijski sustavi podupiru usluge koje podržavaju funkcioniranje našeg društva i gospodarstva. Kibernetička sigurnost sve više postaje ključni prioritet u svjetlu iznimno važne uloge informacija i komunikacija u gospodarskom i društvenom razvoju. Energetski sektor i usluge koje pruža predstavljaju glavni primjer važnosti kibernetičke otpornosti i sigurnosti, uz ostale sektore, kao što su financije, transport i zdravlje. To je potkrijepljeno učinkovitom suradnjom i razmjenom informacija među dionicima energetskog sektora, javnim tijelima na razini EU i nacionalnim regulatornim tijelima omogućiti im da bolje rješavaju rizike, ranjivosti i prijetnje.

Velike energetske kompanije za naftu, plin i električnu energiju metom su sve većeg broja kibernetičkih napada motiviranih komercijalnim i kriminalnim namjerama. Kibernetički napad 23. prosinca 2015. na elektrane u Ukrajini, pokazali su da je razmjena informacija ključna u identifikaciji koordiniranog napada i usmjeravanja odgovarajućih akcija odgovora. Svrha ovog članka je pružanje široj

stručnoj javnosti osnovnih informacija o trendovima razvoja kibernetičke sigurnosti, kao i relevantnih inicijativa za standardnu razmjenu informacija o incidentima u energetskom sektoru.

Većina „curenja“ podataka unutar organizacija rezultat su ljudskih čimbenika, iako su politike kibernetičke sigurnosti uobičajene među organizacijama, zaposlenici na njih mogu gledati kao na smjernice, a ne na pravila. Slično tome, tehnologije ne mogu zaštititi organizacije ako su pogrešno integrirane i korištene. U skladu s tom pozadinom, razvoj kulture kibernetičke sigurnosti među svim djelatnicima, postiže promjenu načina razmišljanja, potiče svijest o sigurnosti i percepciju rizika i održava blisku organizacijsku kulturu.

Kao zaključno razmatranje autori žele naglasiti potrebu za kontinuirano ulaganje u inovacije i vještine. Izgradnja otpornog i stabilnog sustava također znači imati ljude s pravim vještinama, potičući tehnološke inovacije da ostanu ispred onih koji nas žele napasti. EU se suočava s deficitom znanja o kibernetičkoj sigurnosti, manjak se procjenjuje na oko 350.000 ljudi do 2022. godine. Suočavanje s ovim deficitom vještina ključno je za učinkovitu kibernetičku otpornost. Dakle, kibernetička sigurnost mora biti uvrštena i postati prioritet u nastavnim planovima i programima obrazovanja i osposobljavanja.

Krivulja učenja kibernetičke zaštite IoE sustava mora biti izrazito strma, kako bi mogla pratiti brzu dinamiku razvoja i osigurati dugoročnu fleksigurnost. Nesumnjivo je da IoT i IoE predstavljaju sljedeće korake u digitalnom poslovanju i pružaju priliku za nove modele poslovanja energetskih kompanija te da pravovremena implementacija novih digitalnih procesa stvara temelje sigurnosti i kontinuiteta poslovanja. S obzirom da postoji izrazita dinamika u razvoju novih IKT sustava te svakim danom nastaju nove varijante kibernetičkih ugroza i sustava za zaštitu, autori smatraju da bi sljedeći citat mogao plastično objasniti kako je nemoguće postići 100% siguran IKT sustav.

“Jedini informacijski sustav koji je zaista siguran je onaj koji je isključen iz napajanja, zaliven u betonski blok te zaključan u sobu obloženu olovom koju čuvaju dobro naoružani čuvari – čak ni tada, ne bih se baš kladio na njega.”

Eugene H. Spafford
Computer Operations, Audit and
Security Tehnology (COAST)
Purdue University

Literatura:

1. Internet of Things i Blockchain kao alati razvoja fleksigurnog energetskog sektora, časopis „Nafta i Plin“ broj 153/2018., Autori: Antonijo Bolanča, mag. ing., doc. dr. sc. Darko Pavlović, Sanja Šijanović Pavlović, prof. inf.
2. Internet of Things i Blockchain kao temelj sigurnosti energetskih sustava s visokim udjelom intermitentnih izvora, časopis plin, br. 2, lipanj, 2018, Autori: doc. dr. sc. Darko Pavlović, Antonijo Bolanča, mag. ing., Sanja Šijanović Pavlović, prof. inf.
3. S.P. Šijanović: Gimnaziji Vukovar priznanje Međunarodnog programskog odbora za najbolji stručni rad na 19. CUC-u, Portal za škole, 11.11.2017. web mjesto: http://www.skole.hr/nastavnici/iz_prakse?news_id=15170 (pristupljeno 30.08.2018.)
4. S.P.Šijanović: Što smo sve napravili... dosadašnje aktivnosti djelatnika Gimnazije Vukovar u sklopu projekta e-Škole: Uspostava sustava razvoja digitalno zrelih škola, Portal za škole, 3.4.2017. web mjesto: http://www.skole.hr/nastavnici/iz_prakse?news_id=14286 (pristupljeno 30.08.2018.)
5. S.P.Šijanović: Završetak stare i početak nove kalendarske godine u Gimnaziji Vukovar obilježen aktivnostima u sklopu pilot projekta e-Škole, Portal za škole, 11.1.2018. web mjesto: http://www.skole.hr/aktualno/vijesti-iz-skola?news_id=15405 (pristupljeno 30.08.2018.)
6. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)
7. www.kmco.com/resource-center/article/looking-forward/information-security-cyber-security-it-security-whats-the-difference/
8. Nacionalna taksonomija računalno-sigurnosnih incidenata, Verzija 1, Zavod za sigurnost informacijskih sustava
9. Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. godine o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije
10. Budimpeštanska konvencija o kibernetičkom kriminalu, NN 9/02
11. Konvencija o kibernetičkom kriminalu i kazneni zakon republike hrvatske, Mr. se. Goran Vojković Marija Štambuk-Sunjić, 2005.
12. Strategija nacionalne sigurnosti Republike Hrvatske, NN 73/2017
13. Zakon o sustavu domovinske sigurnosti, NN 108/2017
14. Zakon o informacijskoj sigurnosti, NN 79/2007
15. Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, NN 108/2015
16. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih, NN 64/18
17. Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 68/18
18. Window of exposure… a real problem for SCADA systems?, European Union Agency for Network and Information Security, 2013.
19. Report on Cyber Security Information Sharing in the Energy Sector, European Union Agency For Network And Information Security, 2016
20. Norma ISO 27001:2013, Information security management systems
21. Norma ISO 22313:2014, Business continuity management system
22. Norma ISO 31000:2009, Risk management