Kibernetička sigurnost kritične infrastrukture Republike Hrvatske korištenjem javno privatnih partnerstava

Barišić, Filip

Professional thesis / Završni specijalistički

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:114:775654

Sveučilište u Zagrebu
Fakultet političkih znanosti
Specijalistički studij Vanjske politike i diplomacije

Filip Barišić

Kibernetička sigurnost kritične infrastrukture Republike Hrvatske korištenjem javno privatnih partnerstava

ZAVRŠNI RAD

Zagreb, 2022.

Sveučilište u Zagrebu
Fakultet političkih znanosti
Specijalistički studij Vanjske politike i diplomacije

Kibernetička sigurnost kritične infrastrukture Republike Hrvatske korištenjem javno privatnih partnerstava

ZAVRŠNI RAD

Mentor: izv.prof.dr.sc. Robert Mikac
Student: Filip Barišić

Zagreb, siječanj 2022.

Izjavljujem da sam završni rad „Kibernetička sigurnost kritične infrastrukture Republike Hrvatske korištenjem javno privatnih partnerstava“, koji sam predao na ocjenu mentoru izv.prof.dr.sc. Robertu Mikcu, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Filip Barišić

Sadržaj

1. Uvod

Kibernetički prostor nastaje primarno kao posljedica napretka informacijske i komunikacijske tehnologije. U samom začetku vrlo mali broj ljudi je imao pristup takovoj tehnologiji. Međutim, pojavom Interneta 1990-ih i domene poznate pod nazivom *World Wide Web* započinje značajan rast pristupačnosti kibernetičkom prostoru. Primjerice, do 2010. godine broj korisnika Interneta, na globalnoj razini, se kretao približno 2 milijarde (Statista, 2022), a samo 10 godina poslije ta brojka je narasla za otprilike 3 milijarde što ujedno predstavlja rast većim od 100%, te današnji dostupni podaci ukazuju na brojku od 4,9 milijardi korisnika interneta (Statista, 2022).

Porastom korisnika Interneta, kao najrelevantnijeg pokazatelja dostupnosti kibernetičkog prostora, te razvojem i rastom ekonomija, gospodarstava, boljom pristupačnošću znanja, paralelno su se pojavljivale potrebe za standardizacijom i regulacijom cjelokupnog prostora, uređivanjem odnosa svih dionika, kako javnih tako i privatnih.

Naravno, kako naslov samog rada glasi: „Kibernetička sigurnost kritične infrastrukture Republike Hrvatske korištenjem javno privatnih partnerstava“, važno je u ovom dijelu rada definirati sve ključne pojmove i predstaviti one diskusije oko definicija pojedinih pojmova.

Pojam „kibernetički“ je uveden u hrvatski diskurs u trenutku ratifikacije Budimpeštanske konvencije o kibernetičkom kriminalu 2002. godine (Hrvatski sabor, 2002). Naime, na engleskom jeziku postoji pojam „*cyber*“ za koji se uvriježio pojam „kibernetički“ iako postoje primjeri radova na hrvatskom jeziku koji taj prijevod propituju. U radu pod naslovom „Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj“ Hrvoje Vuković predlaže pojam „kibernetski“ kao naziv kojim će ponajbolje prevesti pojam „*cyber*“ (Vuković, 2012). Još jedan rad pod naslovom „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“ (Vojković i ostali, 2006) razlaže, između ostalog, istu problematiku na koju se ujedno i poziva Vuković u svojem radu, a to je traženje opravdanosti za korištenje točno jednog termina kojim bi se definirala problematika prijetnji u kibernetičkom prostoru. Kako se u svim normativnim aktima i nacionalnim strategijama koristi pojam „kibernetički“ kao jedini pridjev u sintagmama poput kibernetički prostor

ili kibernetička sigurnost (Vlada RH, 2015), (Hrvatski sabor, 2002), (Hrvatski sabor, 2018), tako će se i u ovom radu isključivo koristiti pojam „kibernetički“. Stoga, prvi pojam koji je ključan za pisanje ovog rada jest kibernetička sigurnost, a definicija glasi: „Kibernetička sigurnost obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i raspoloživost podataka i sustava u kibernetičkom prostoru.“ (Vlada RH, 2015: 29). Kibernetički prostor predstavlja infrastrukturu u sklopu koje se odvijaju sve aktivnosti i mjere koje su bitne s aspekta razmatranja kibernetičke sigurnosti, a definicija pojma glasi: „prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća Internet i sve sustave povezane na njega“ (Vlada RH, 2015: 29).

Uz ove pojmove važno je navesti još i definiciju informacijske sigurnosti koja glasi: „stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom odgovarajućih sigurnosnih mjera“ (Vlada RH, 2015: 29). Sličnu definiciju, malo proširenu, pruža Zakon o informacijskoj sigurnosti (Hrvatski sabor, 2007). Dodatno, detaljna analiza o sličnostima i razlikama triju pojmova kao što su informacijska, informatička i kibernetička sigurnost pruža rad pod naslovom „Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture“ (Kezerić, 2017: 6). U tom radu navodi se između ostaloga sljedeće: „Informacijska sigurnost definirana je na prethodnim stranicama. No, kakve ona veze ima s danas, tako popularnim, pojmom cyber (kibernetičke) sigurnosti? Poanta je ustvari vrlo jednostavna – budući da je većina informacija danas u digitalnom obliku, informacijska i cyber sigurnost mogu se smatrati gotovo sinonimima. Definicija cyber sigurnosti navedena u nizozemskoj Strategiji cyber sigurnosti iz 2011., a na koju se poziva Košutić (2012: 24), navodi da cyber sigurnost znači biti slobodan od opasnosti ili štete uzrokovane prekidom, ometanjem ili padom informatičko-komunikacijskih tehnologija (engl. ICT) ili zlouporabom ICT-a.“ Dosta puta, što je očito iz prikazanog citira Košutića (2012) koji također navodi kako je kibernetička sigurnost 95% informacijske sigurnosti upravo iz razloga jer pod okrilje informacijske sigurnosti ne ulazi, na primjer, papir.

Segment nacionalne infrastrukture u sklopu kojeg se promatra dinamika informacijske i kibernetičke sigurnosti jest kritična infrastruktura. Za definiciju kritične infrastrukture koristi se Zakon o kritičnim infrastrukturama, a ona glasi: „Nacionalne kritične infrastrukture su sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na

nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti“ (Hrvatski sabor, 2013). Također, Zakon o kritičnim infrastrukturama definira i pojam europske kritične infrastrukture koji definira kao kritičnu infrastrukturu koja je od interesa za najmanje dvije države članice. Važno je napomenuti da nije svaka komponenta kritične infrastrukture jednako vrijedna te da je popis kritične infrastrukture dinamičan registar koji se s vremenom može mijenjati, a način kako se identificiraju nacionalne kritične infrastrukture je definiran Odlukom o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura (Vlada RH, 2013). Gotovo identične definicije kritične infrastrukture koriste Mikac i ostali u svojem radu (2020: 112) gdje se služe definicijama dokumenata Europske komisije. Također, u ovom dijelu je važno navesti za Republiku Hrvatsku sve sektore u kojima je moguće identificirati kritičnu infrastrukturu sukladno Zakonu o kritičnim infrastrukturama, a oni su sljedeći: energetika, komunikacijska i informacijska tehnologija, promet, zdravstvo, vodno gospodarstvo, hrana, financije, proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe te nacionalni spomenici i vrijednosti.

Uslijed korona krize koja je zapravo dodatno ubrzala trend digitalizacije diljem svijeta pa tako i u Hrvatskoj, paralelno su se pojavili i sve veći rizici kibernetičkih prijetnji nacionalnoj kritičnoj infrastrukturi. Mora se priznati da je dobar dio hrvatske kritične infrastrukture u javnom vlasništvu dok u nama zapadnim zemljama privatni sektor ima u vlasništvu većinu nacionalne kritične infrastrukture, te za istu odgovaraju različite javne institucije, ovisno o kojoj se vrsti imovine i nadležnosti radi. Također, ako se uzima u obzir i manjak ljudskog kadra koji je osposobljen za pružanje usluga kibernetičke sigurnosti te prevaga koju odnosi privatni sektor prilikom zapošljavanja istog kadra, dolazi se do zaključka kako javne institucije mogu imati ozbiljnih problema prilikom suočavanja s kibernetičkim ugrozama. Drugim riječima, suradnja između javnog i privatnog sektora postaje nužnost koju je potrebno istovremeno kvalitetno regulirati (Schaake, 2020). U Republici Hrvatskoj se ovakva suradnja može temeljiti na Zakonu o privatnoj zaštiti (Hrvatski sabor, 2020). Naime, Zakonom je definirana privatna zaštita kao: „sigurnosna gospodarska djelatnost koja se provodi radi postizanja prihvatljive razine privatne i javne sigurnosti građana i njihove imovine te održavanja reda i mira u ugovornom opsegu“, a za ovaj rad važna je i definicija tehničke zaštite koja glasi: „zaštita osoba i imovine koja se obavlja dominantnom

uporabom tehničkih uređaja i sustava radi stvaranja tehničkih uvjeta za sprječavanje protupravnih radnji usmjerenih prema štićenoj osobi ili imovini“ (Hrvatski sabor, 2020).

Nakon svih navedenih informacija koje ukazuju na relevantnost teme te objašnjenja ključnih pojmova za pisanje ovog rada, dolazi se do definiranja problema istraživanja. Kao što je već navedeno sve učestalije korištenje digitalnih usluga javnih institucija, digitalizacija javne uprave ima za posljedicu izloženost kibernetičkim ugrozama. Istovremeno, zaštita od kibernetičkih ugroza zahtjeva vještine, znanja i iskustvo pomoću kojih se omogućava obrana i sigurnost od različitih prijetnji. Iako određene javne institucije pružaju uslugu kibernetičke sigurnosti javnim, državnim i akademskim institucijama, definitivno ona nije uvijek dostatna te se pojavljuje potreba za suradnjom s privatnim sektorom koji također nudi određene usluge i proizvode kibernetičke sigurnosti. Praksu suradnje javnog i privatnog sektora u kibernetičkom prostoru treba dobro definirati kako ne bi bilo propusta koji će posljedično imati implikacije na nacionalnu sigurnost. Predmet istraživanja je skup kibernetičkih prijetnji koji se pojavljuje na razini EU i RH te njihova dinamika. Nadalje, strateški i normativni akti na temelju kojih se definira i provodi kibernetička sigurnost nacionalne kritične infrastrukture u RH te mogućnosti suradnje javnog i privatnog sektora u kibernetičkoj sferi RH. Temeljna hipoteza, čiju istinitost treba propitati, jest da javno privatna suradnja u kibernetičkom prostoru doprinosi ukupnoj kvaliteti kibernetičke sigurnosti kritične infrastrukture. Proučavanje predmeta istraživanja se provodi na temelju triju istraživačkih pitanja. Prvo pitanje jest, kakvi su trendovi kibernetičkih prijetnji i koje vrste prijetnji su zastupljene na razini EU i RH? Drugo, koji su to strateški i normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture u RH? Treće, koji su uvjeti potrebni te kako se definiraju u slučaju sklapanja javno privatne suradnje u kibernetičkom prostoru u RH?

U istraživanju koristit će se teorija sustava na način da će se propitati interesi javnog i privatnog sektora te njihove isprepletenosti prilikom dogovaranja potencijalne javno privatne suradnje u kibernetičkom prostoru. Teorija sustava pod pojmom sustava podrazumijeva ukupnost međusobno, svrsishodno povezanih i međuutjecajnih elemenata (Zelenika, 2000: 359). Sustav u ovom slučaju predstavlja prvenstveno javni sektor sa svojim institucijama, a drugi dio tog sustava predstavlja privatni sektor, tvrtke koje nude usluge i proizvode kibernetičke sigurnosti.

Nastavno na teorijski okvir, u istraživanju će biti korišten i određen broj znanstvenih metoda pomoću kojih će se doći do očekivanih rezultata. Deduktivnom metodom će se izvoditi zaključci na individualnoj razini na način da će se proučiti određeni dokumenti koje je izdala EU institucija te će se uspoređivati sa stanjem i trendovima u RH. Deduktivna metoda je sustavna i dosljedna primjena deduktivnog načina zaključivanja u kojem se iz općih stavova izvode posebni, pojedinačni (Zelenika, 2000: 325). Induktivna metoda, kao obrnuta deduktivnoj, koristi na način da se zasebnosti kibernetičkih prijetnji u RH usporede s dinamikom istih na EU razini te donesu određeni zaključci. Induktivna metoda je sistematska i dosljedna primjena induktivnog načina zaključivanja u kojem se na temelju pojedinačnih ili posebnih činjenica dolazi do zaključka o općem sudu (Zelenika, 2000: 323). Analiza se koristi iz razloga da se cjelokupni sustav razloži na manje podsustave te uvide određene prednosti i mane na manjim jednostavnijim razinama, dok sinteza služi za povezivanje zaključaka i znanja o manjim jednostavnijim komponentama sustava, poput definiranja određenih pojmova kao što je kritična infrastruktura, u složenije cjeline. Također i metoda ankete s pojedinim privatnim tvrtkama koje nude usluge ili proizvode zaštite kritične infrastrukture od kibernetičkih prijetnji. Na kraju samog rada se očekuje zaključak koji će težiti tvrdnji da javno privatna suradnja u kibernetičkom prostoru pozitivno doprinosi kvaliteti kibernetičke sigurnosti kritične infrastrukture te da takva vrsta suradnje prati EU trendove.

2. Kibernetičke prijetnje informacijskoj sigurnosti

U ovom poglavlju se odgovara na prvo istraživačko pitanje koje glasi: Kakvi su trendovi kibernetičkih prijetnji i koje vrste prijetnji su zastupljene na razini EU i RH? Kibernetičke prijetnje su one prijetnje koje prilikom provedbe uzrokuju nedostatak pouzdanosti, raspoloživosti, cjelovitosti i povjerljivosti kompleksnog okruženja u kojem se događa interakcija ljudi, softvera i usluga putem interneta. Važno je u današnjem vremenu, a bit će sve relevantnije, prikupljati i obrađivati informacije o kibernetičkim prijetnjama. Nadležna agencija na razini EU za provedbu takvih operacija je Europska agencija za kibernetičku sigurnost (ENISA), koja svake godine, počevši od 2012. godine pa do danas, objavljuje godišnja izvješća u kojima prati globalnu dinamiku razvoja te učestalosti pojavljivanja kibernetičkih prijetnji. Do sada je dotična agencija napravila osam godišnjih izvješća. U ovom radu obrađuju se sva ona izvješća koja su nastala tijekom 2020. godine, osvrću se na obradu tematike kibernetičkih prijetnji, a temelje se na podacima koji su prikupljeni tijekom 2019. godine. Naravno, napravit će se uvid i u starija izvješća kako bi se zapazili potencijalni trendovi tijekom prošlog desetljeća.

Od 2020. godine ENISA je počela mijenjati strukturu pisanja izvješća na način da je se maknula od tekstom bogatih izvješća na kraća, vizualno upečatljiva i razlomljena izvješća u kojima se svaka važnija kibernetička prijetnja samostalno razrađuje. U ovom poglavlju predstavit će se 15 najvećih kibernetičkih prijetnji, upravo onim redoslijedom kako su poredani u izvješću ENISA-e naslovljenom *List of Top 15 Threats* (ENISA, 2020a). One su redom: *malware*, *web-based attack*, *phishing*, *web application attack*, *spam*, *Distributed Denial of Service (DDoS)*, krađa identiteta, povreda podataka, unutarnja prijetnja, *botnet*, fizička manipulacija, šteta, krađa i gubitak, curenje informacija, *ransomware*, kibernetička špijunaža i naposljetku *cryptojacking*.

2.1. Kibernetičke prijetnje u Europskoj Uniji

Prva kibernetička prijetnja, trenutno najučestalija je *malware*, uobičajeni kibernetički napad u obliku malicioznog softvera. Postoji više vrsta *malwarea*, a oni su *cryptomineri*, virusi, *ransomwarei*, *wormsi* i *spywarei*, a glavni ciljevi su mu u pravilu krađa

informacija i identiteta te ometanje pružanja usluge (ENISA, 2020b: 2). Nadalje, u prethodnoj godini je zabilježeno 400 000 slučajeva prethodno instaliranih *spywarea* i *adwarea* na mobilnim uređajima diljem svijeta. Zabilježen je rast otkrivenih *malwarea* na operacijskom sustavu Windows od 13%. Zanimljivo je da je 71% tvrtki zabilježilo širenje *malwarea* s jednog zaposlenika na druge te je 67% *malwarea* bilo dostavljeno putem kriptiranih Internet stranica tipa HTTPS (ENISA, 2020b: 3). Najviše zabilježenih napada je razvio *malware* pod nazivom Emotet, a jedne od najznačajnijih napada ove vrste je u zadnjoj godini imala tvrtka Airbus doživjevši povredu podataka koja se odrazila na zaposlenike diljem Europe. Ukradeno je 12 milijuna osobnih podataka pacijenata čiji su se podaci nalazili na web stranici jedne američke medicinske agencije. Također, tvrtka LifeLabs koja se bavi laboratorijskom dijagnostikom je bila žrtva napada *ransomwareom* koji je rezultirao krađom 15 milijuna računa s rezultatima testova te brojevima zdravstvenih kartica. U gradu Pensacola, Florida, putem napada *ransomwareom* je procurilo 2 GB podataka pomoću kojih se može potencijalno identificirati žrtve i još jedan napomenut napad je onaj u Singapuru gdje su žrtve bili vojni službenici, njih 2400, a maliciozni program je ovaj put bio dostavljen putem e-maila (ENISA, 2020b: 13).

Kibernetička prijetnja koja se nalazi na drugom mjestu ljestvice najučestalijih u 2020. godini jest napad baziran na web-u (*web-based attack*). To je vrsta prijetnje koja koristi web sustave i usluge istih kako bi se napad realizirao. Ovakva vrsta prijetnje pokriva jako veliko područje, a primjeri takvih napada su primjerice maliciozne web stranice ili određene skripte koje preusmjeravaju korisnika, odnosno žrtvu, na zaraženu stranicu ili omogućuju skidanje malicioznog sadržaja. Također, cilj može biti i injektiranje malicioznog koda na web stranicu kako bi se došlo do određene koristi (ENISA, 2020c: 2). Neki od zapaženijih slučajeva jest onaj malicioznog programa koji se instalira na web stranice, a poznatiji naziv takove tehnike pod kolokvijalnim izrazom je *formjacking*. Zatim, slučaj zaraze prostora za reklamiranje na web stranicama putem programa „*Magecart*“. Platforme za dopisivanje, ekstenzije poznatih internetskih pretraživača su sve primjeri čime se različite skupine koriste kako bi okoristile i uspješno provele napada ovakvog tipa (ENISA, 2020c: 6-8). Također se u više navrata spominje i grupa pod nazivom *ShadowGate*, a zanimljiv je graf koji ukazuje da dotična grupa nešto više od 50% svoje kriminalne aktivnosti provodi na području Japana (ENISA, 2020c: 9).

Treća po redu kibernetička prijetnja je *phishing*. To je vrsta prijetnje koja se u pravilu provodi slanjem e-mail poruka od naočigled autentičnog autora, a namjera je u pravilu otvoriti privitak koji je zaražen malicioznim softverom ili pritisnuti link koji vodi do zaražene web stranice. Nadalje, pojam *spear phishinga* se odnosi na proučavanje potencijalnih žrtava kako bi se takove poruke činile što autentičnijima (ENISA, 2020d: 2). Zanimljiva je informacija da 42,8% svih malicioznih privitaka su porijeklom dokumenti Microsoft Office-a, 30% ovakvih poruka dolazi ponedjeljkom i 32,5% ovakvih poruka sadrži pojam „plaćanje“ u sebi (ENISA, 2020d: 3). U 2019. godini zdravstveni sektor je bio teško pogođen ovom vrstom napada kao i ostale vladine te institucije javne uprave (ENISA, 2020d: 12). Neki od primjera *phishing* napada u izvješću jest napad na Sveučilište Lancaster koje je rezultiralo gubitkom osobnih podataka, a 2500 korisnika Discord-a je ostalo bez podataka za prijavljivanje na istoimenu stranicu (ENISA, 2020d: 13).

Sve kompleksnije web aplikacije i sve šira upotreba stvara izazove kako zaštiti iste od različitih prijetnji koje su u pravilu, kao i u mnogim drugim slučajevima, uvjetovane stjecanjem financijske koristi, nanošenjem štete ugledu ili krađom osobnih podataka. Web usluge i aplikacije ovise umnogome o bazama podataka, pa je stoga jedan od najučestalijih napada u ovoj sferi umetanje podataka (ENISA, 2020e: 2). Porast napada web aplikacija u 2019. godini, u usporedbi sa 2018. godinom, iznosi 52%, 63% ispitanika jedne ankete je odgovorilo da koristi vatrozid za web aplikacije, 20% tvrtki je prijavilo da doživljava *DDoS* napade na dnevnoj osnovi, a 84% od ukupnih ranjivosti je posljedica pogrešnih konfiguracija (ENISA, 2020e: 3).

Prva *spam* poruka je bila poslana 1978. godine kao dio jedne marketinške kampanje kojom se pokušavao popularizirati jedan novi proizvod. Naime, 393 osobe su bile primatelji *spam* poruka u sklopu te kampanje. Primanje *spamova* može biti iritirajuće kako tada tako i danas. Međutim, glavna karakteristika *spama* je upravo velika količina neželjenih poruka, a takve poruke smatraju se kibernetičkom prijetnjom onda kada za cilj imaju dostaviti druge vrste prijetnji (ENISA, 2020f: 2). Pojedini nalazi u izvješću za 2019. godinu ukazuju da je čak 84% ukupno izmijenjenih e-mailova u travnju 2019. godine bili *spamovi*. Isto tako je i 13% povreda podataka nastalo zbog malicioznih *spamova*, 10% od ukupno detektiranih *spamova* je napadalo njemačke e-mail račune te otprilike 60% e-mailova povezanih s industrijom rudarenja je bilo žrtvom *spama* (ENISA, 2020f: 3). Također, zemlja koja prednjači kao najveći izvor *spamova* u svijetu

je Kina sa udjelom od 20%, a prate ju Sjedinjene Američke Države s udjelom od 13%. Slijede ih redom države poput Rusije, Brazila, Njemačke i Francuske (ENISA, 2020f: 11).

DDoS napadi nastupaju u trenutku kada korisnici sustava ili usluge ne mogu pristupiti relevantnim uslugama, informacijama ili resursima (ENISA, 2020g: 2). 2019. godine dogodio se rast *DDoS* napada od 241% u odnosu na 2018. godinu. 86% spriječenih napada u 2019. godini je koristilo dva pravca napada na pojedini sustav. 84% napada je trajalo manje od 10 minuta, a najdulji napad u 2019. godini je trajao 509 sati (ENISA, 2020g: 3). Trenutno najpoznatija tehnika *DDoS* napada, koju je najteže spriječiti, naziva se *Syn Flood* (ENISA, 2020g: 6)

Krađa identiteta predstavlja nedopuštenu upotrebu osobnih podataka kako bi se netko predstavio kao osoba čiji su podaci ukradeni te na osnovu toga steći financijsku ili drugu vrstu koristi. Primjer otkrivanja otprilike 106 milijuna osobnih podataka američkih i kanadskih korisnika bankovnih računa. Također, slučaj kompromitiranja osobnih podataka 600 000 vozača *Ubera* i 57 milijuna korisnika u studenom 2019. godine. Zatim, otkrivanje 170 milijuna korisničkih imena i zaporki korisnika poznate online poker verzije pod nazivom *Zynga* te ostali slučajevi (ENISA, 2020h: 2). Nadalje, dobro je napomenuti da je broj incidenata po tvrtki iznosio 3,2 u 2019. godini, a postotak uspješno provedenih napada koji se dovodi u vezu s ljudskim nemarom iznosi čak 63% (ENISA, 2020h: 3). Isto tako, kako bi se dobio dojam kako građani EU-a percipiraju krađu identiteta, najbolje govori anketa koju je proveo Eurobarometar, a u kojem se 95% ispitanika izjasnilo o krađi identiteta kao ozbiljnom zločinu (ENISA, 2020h: 9). Dodatno, vrsta podataka koja se najčešće gubi su e-mailovi i zaporke (ENISA, 2020h: 11).

Povreda podataka je vrsta kibernetičkog incidenta u kojem je pristup informaciji ili dijelu informacijskog sustava omogućen bez pravovaljane autorizacije. U pravilu se radi o zlućudnim namjerama kojima je cilj gubitak ili zloupotreba informacije (ENISA, 2020i: 2). Rast ove kibernetičke prijetnje u 2019. godini iznosi 54%. Također, 71% počinjenih povreda podataka je bilo motivirano financijskom koristi, 32% povreda podataka je prvotno uključivalo aktivnost phishinga, 52% povreda podata dogodilo je se uslijed hakiranja sustava, 70% ovakvih incidenata završava otkrivanjem e-mailova te 55% ispitanika ankete koju je proveo Eurobarometar su zabrinuti za svoje podatke ako su isti u posjedu kriminalaca (ENISA, 2020i: 3). Zanimljivo je napomenuti kako su

financijske posljedice povrede podataka, po zaposleniku neke tvrtke, skoro 20 puta veće za male tvrtke u odnosu na velike (ENISA, 2020i: 7). Vrsta podataka koje su najčešće otkrivene uslijed ovakvih propusta su e-mailovi i zaporke (ENISA, 2020i: 9), a od sektora se najgore pogođeni javni i zdravstveni sektor kojem se predviđa rast povrede podataka u bližoj budućnosti od 10% do 15% (ENISA, 2020i: 10-11).

Unutarnja prijetnja je akcija koja može završiti incidentom, a provode ju osobe ili grupe koje su povezane ili rade za žrtvu. Poznati primjer ovakve prijetnje je suradnja vanjskog aktera s unutarnjim akterom s ciljem dobivanja pristupa imovini (ENISA, 2020j: 2). Nadalje, posljedica 65% unutarnjih prijetnji jesu gubici ugleda dotične organizacije i financijski gubici, 88% ispitanih organizacija tvrdi da su unutarnje prijetnje znak za uzbunu, 11,45 milijuna eura je prosječna šteta nametnuta organizaciji uslijed ovakvih prijetnji te 40% ispitanih organizacija se osjeća ugroženo u trenutku kada su im otkrivene povjerljive poslovne informacije (ENISA, 2020j: 3). Također, ova vrsta prijetnje dobiva sve više na značaju iz razloga jer tehnički pravci napada na sustave postaju sve skuplji, stoga kao najbolja moguća alternativa se nudi podmićivanje unutarnjih aktera, a cijene mita mogu oscilirati ovisno o poziciji osobe koju se želi podmititi (ENISA, 2020j: 6). Ova vrsta prijetnje je imala rast od 47%, a trošak koji je nastao kao posljedica ove prijetnje je rastao 31% u 2019. godini (ENISA, 2020j: 7).

Botnet je mreža spojenih uređaja koji su zaraženi *bot malwareom*, a ove uređaje u pravilu koriste zlonamjerne skupine s ciljem pokretanja *DDoS* napada (ENISA, 2020k: 2). Osnovna ciljna skupina ove kibernetičke prijetnje je internet stvari, a činjenica od 7,7 milijuna uređaja interneta stvari spojenih na internet svaki dan ide u prilog tome. Nadalje, 300 000 obavijesti o prometu *Emotet botnetom* je zabilježeno 2019. godine, 60% novih *botneta* je povezano s krađom osobnih podataka i 17 062 je brojka pronađenih *botnet* servera što ujedno predstavlja rast od 71,5% (ENISA, 2020k: 3), zemlja s najviše *botnet* servera, njih čak 58% jesu Sjedinjene Američke Države, druga zemlja s udjelom od 14% broja takovih servera je Velika Britanija i treća je Kina s udjelom 9,5% (ENISA, 2020k: 15). Zanimljivo, da je *Mirai*, koji je jedan od najpoznatijih verzija botneta, doživio rast od 57% u 2019. godini (ENISA, 2020k: 13).

Fizička manipulacija, šteta, krađa i gubitak kao oblik prijetnje se značajno izmijenio u posljednjih par godina a napredak u području interneta stvari ovdje igra značajnu ulogu. Naime, internet stvari može doprinijeti fizičkoj sigurnosti s naprednim i

kompleksnim rješenjima koristeći se, između ostaloga, i konceptima umjetne inteligencije, odnosno strojnog učenja (ENISA, 2020l: 2). Zapravo, trend koji obilježava dinamiku ove prijetnje jest konvergencija kibernetičkog i fizičkog elementa obrane (ENISA, 2020l: 3). Međutim, 4% povreda se dogodilo zbog fizičkih akcija, ali je 20% kibernetičkih incidenata započelo ili završilo fizičkom akcijom. Čak 54% povreda podataka se dogodilo zbog fizičkog napada. S druge strane, 48% IT menadžera koristi nadgledanje prostora kamerama i kontrolu pristupa (ENISA, 2020l: 9).

Povreda podataka nastaje u trenutku kada organizacija, koja je odgovorna za te podatke, postaje žrtvom sigurnosnog incidenta koji ima posljedice povrede povjerljivosti, raspoloživosti i cjelovitosti. Povreda podataka, s druge strane, uzrokuje curenje informacija koje su najčešće osobni podaci, financijski podaci ili osobni zdravstveni podaci (ENISA, 2020m: 2). U 2019. godini potvrđeno je 2013 otkrivanja podataka, 14% svih incidenata u financijskom sektoru jesu otkrivanja podataka, a u 47% slučajeva žrtve su bile banke. 4,1 milijarda podataka je bila otkrivena na globalnoj razini u 2019. godini (ENISA, 2020m: 3). Zanimljiv je podatak iz siječnja 2019. godine o curenju privatnih razgovora, osobnih i financijskih podataka njemačkih političara iz svih stranaka osim iz stranke AfD (*Alternative fur Deutschland*) te podatak o otkrivanju stotina milijuna korisničkih računa *Facebooka* i *Instagrama* (ENISA, 2020m: 6). Najučestaliji razlog curenja informacija jesu zlonamjerni kriminalni napadi na baze podataka pojedinih organizacija, a njihov ukupni udio je 51%, dok su greške u sustavu krive u 25% slučajeva, a ljudska greška u 24% slučajeva (ENISA, 2020m: 7).

Ransomware, kao vrsta *malwarea*, je postao popularno oružje zlonamjernih aktera koji nanose štetu vladama, tvrtkama i individualcima na dnevnoj bazi. U ovom slučaju, žrtva ovakve vrste napada ponajprije trpi financijsku štetu plaćanjem iznosa zatražene otkupnine ili plaćanjem troškova oporavka od napada (ENISA, 2020n: 2). Nadalje, 10,1 milijardi eura je procijenjena vrijednost plaćenih otkupnina u 2019. godini, za 365% je porasla detekcija *ransomwarea*, više od dvije trećine zdravstvenih organizacija je pretrpilo napad ove vrste. Čak 45% napadnutih organizacija je pristalo platiti otkupninu, a pola njih je svejedno izgubilo podatke (ENISA, 2020n: 3). Popularnost ove kibernetičke prijetnje u posljednje tri godine pada, ali sve veća pažnja se okreće prema visoko profiliranim metama. Također, kao jedan od mogućih alternativa kako se braniti od ovakve vrste prijetnje jest plaćanje polica osiguranja za ovu vrstu napada (ENISA,

2020n: 6). Najučestaliji *ransomware* napadi u 2019. godini su bili *WannaCry* i *Trojan-ransom.win32.Phny* (ENISA, 2020n: 14).

Iduća kibernetička prijetnja, kibernetička špijunaža, smatra se istovremeno i prijetnjom i motivom, a definirana je kao korištenje računalnih mreža za stjecanje neovlaštenog pristupa povjerljivim informacijama koje su uglavnom u vlasništvu vlade ili neke organizacije. Kibernetičku špijunažu ponajviše karakterizira nastanak i rast državno sponzoriranih skupina koje provode kibernetičke napade na različite komponente kritične infrastrukture, od vladinih ministarstava, željeznice, telekomunikacija, energetskih tvrtki, bolnica i banaka (ENISA, 2020o: 2). Od povreda podataka njih ukupno 20% je motivirano kibernetičkom špijunažom, 38% svih zlonamjernih aktera je povezano s nacionalnim državnim strukturama, 11,2% incidenata je motivirano špijunažom te u 63% slučajeva kibernetičke špijunaže akteri se koriste metodom *phishinga* (ENISA, 2020o: 3).

Pod pojmom *cryptojacking* se podrazumijeva neovlašteno korištenje resursa drugih uređaja za rudarenje kriptovaluta, a potencijalni uređaji koji su ciljevi ovakvih napada su osobna računala, mobiteli, a u zadnje vrijeme sve više žrtvom postaju infrastrukture oblaka. Najučestaliji *malwarei* korišteni za *cryptojacking* u 2019. godini su *Jsecoin*, *XMRig*, *Cryptoloot* te *Coinhive* (ENISA, 2020p: 2). U 2019. godini je zabilježeno 64,1 milijun slučajeva *cryptojackinga*, 78% slučajeva je bilo manje u drugoj polovici godine nego u prvoj, a oko 40% ukupnog broja slučajeva se dogodio u Japanu, 20% u Indiji te 14% u Tajvanu (ENISA, 2020p: 3). Zanimljivo je da je upravo kriptovaluta Monero bila glavna meta za rudarenje prilikom *cryptojackinga*, te da je *cryptojacking* u 2019. godini doživio padajući trend (ENISA, 2020p: 8-9).

2.2. Kibernetičke prijetnje u Republici Hrvatskoj

U ovom podpoglavlju predstavit će se kibernetičke prijetnje koje su se pojavljivale tijekom 2019. i 2020. godine, ovisno o tome koja su izvješća dostupna. Naime, izvješća koja se izdaju u Republici Hrvatskoj, a prate tematiku, između ostaloga, trenutnog stanja i dinamike kibernetičkih prijetnji, jesu izvješća institucija poput Sigurnosno obavještajne agencije (SOA), nacionalnog CERT-a te objave Zavoda za sigurnost informacijskih sustava (ZSIS). Važno je napomenuti kako ove tri institucije dolaze do

podataka na kojima se temelje njihova izvješća ili druge javno dostupne objave. SOA-in rad je primarno definiran Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske (Hrvatski sabor, 2006) što zasigurno pruža šire mogućnosti dolaska do podataka o kibernetičkim incidentima. Nadalje, ZSIS koji je ujedno i dionik obavještajne zajednice te štiti državni sustav od kibernetičkih ugroza, također raspolaže širim mogućnostima dolaska do podataka kao i u slučaju SOA-e. Te naposljetku nacionalni CERT, koji dolazi do podataka prvenstveno opcijom prijave incidenta na web stranici istoimene institucije.

SOA svake godine, u skladu s politikama transparentnosti, izdaje godišnja izvješća u kojima pokriva teme od ključnog značaja za nacionalnu sigurnost te pravni i ustavni poredak Republike Hrvatske. U trenutku pisanja ovog rada zadnje izvješće dostupno javnosti je izdano 2020. godine s osvrtom na stanje nacionalne sigurnosti u 2019. godini. Napominje se kako kibernetički napadi, zbog velikog udjela državno sponzoriranih napadača, postaju sve sofisticiraniji, a posljedice mogu biti goleme, pogotovo za kritičnu infrastrukturu. Dakako, kao i u brojnim izvješćima ENISA-e kao jedan od najvećih rizika uspješno provedenih kibernetičkih napada se spominje krađa klasificiranih, osobnih i drugih osjetljivih podataka (SOA, 2020: 12). Nadalje, kao glavna prijetnja u kibernetičkom prostoru se spominju napadi koji su temeljito planirani, napredni i ustrajni (APT – *Advanced Persistent Threat*), a takvu razinu kompleksnosti napada mogu izvršiti uglavnom državno sponzorirane skupine. Također, ovakve vrste napada se koriste za provedbu napada *ransomwareom*, a ciljevi su financijskog karaktera (SOA, 2020: 23). Uslijed COVID-19 pandemije dogodio se rast takovih napada, a INA se spominje kao primjer žrtve (SOA, 2020: 24).

Nacionalni CERT, nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj (CERT, 2021). Izvještaj CERT-a iz 2020. godine govori o općem rastu kibernetičkih prijetnji od čak 66% za razliku od 2019. godine, koji je između ostaloga posljedica većeg broja prijava, a u samom vrhu po zastupljenosti svih prijetnji jesu različite verzije *phishinga*, pogađanje zaporki, *web defacement* te zaraza *malwareom* (CERT, 2020: 10-11). Zanimljivo je da se *cryptojacking* nalazi na zaleđu po zastupljenosti svih prijetnji kao i u izvještajima ENISA-e.

Naposljetku, Zavod za sigurnost informacijskih sustava (ZSIS), koji je zadužen za pružanje usluga kibernetičke sigurnosti tijelima državne uprave, ne izrađuje godišnje izvještaje ali na svojim web stranicama redovito osvježava sadržaj najnovijih kibernetičkih prijetnji i konkretnih slučajeva kibernetičkih napada koji su se dogodili. Naravno, uz sve to pružaju se i savjeti kako se zaštititi (ZSIS, 2021).

U trenutku pisanja ovog rada pandemija COVID-19 traje već dulje od godinu dana. Ona nije donijela nikakve nove trendove već je postojeće, poput digitalizacije, ubrzala. Sve većim digitalnim prostorom povećava se i prostor potencijalne ugroze jednom od mnogih kibernetičkih prijetnji. Dakako, po svemu sudeći, svi trendovi upućuju na to da će prilike za potencijalne ugroze rasti, napadi će biti sve sofisticiraniji uslijed korištenja novijih tehnologija i znanstvenih dostignuća poput umjetne inteligencije ili čak kvantnih računala u svakodnevnoj primjeni. Nove tehnologije poput 5G mreža, interneta stvari i pametnih auta će biti sve više u centru pažnje zlonamjernih aktera u kibernetičkom prostoru (ENISA, 2020q: 8-15). Za razliku od europskih, pa i svjetskih trendova, kibernetičke prijetnje u domeni hrvatskog kibernetičkog prostora imaju sličnu dinamiku. Naime, brojke prijetnji rastu, ali je redoslijed učestalosti pojedinih kibernetičkih prijetnji donekle izmijenjen. Sve ove neizbježnosti dovode do zaključka da će proračuni za kibernetičku sigurnost rasti, a ažuriranje analiza kibernetičkih prijetnji doprinositi kvalitetnijim strategijama kibernetičke sigurnosti (ENISA, 2020r: 4-6).

3. Politike zaštite kritične infrastrukture

U ovom, trećem poglavlju, detaljnije se razrađuju politike zaštite kritične infrastrukture i odgovara na drugo istraživačko pitanje: Koji su to strateški i normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture u RH? Naravno, posebna pažnja se pridaje kibernetičkoj komponenti zaštite infrastrukture. Iako je već u uvodu definirana osnovna terminologija, treba napomenuti da je u Zakonu o kritičnim infrastrukturama definiran pojam nacionalne kritične infrastrukture kao: „… sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.“ A zatim se, naknadno u sljedećem članku istog Zakona, definira lista pojedinih sektora kritičnih infrastruktura koje su redom: energetika, komunikacijska i informacijska tehnologija, promet, zdravstvo, vodno gospodarstvo, hrana, financije, zatim proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe te nacionalni spomenici i vrijednosti. Dakako, ova lista može biti izmijenjena na inicijativu Vlade RH. U Zakonu je naznačeno da kriteriji, kojima se neka mreža, sustav ili objekt određuju kao nacionalna kritična infrastruktura, predstavljaju klasificirane podatke, a dodatno je još razrađena, kao posebno poglavlje, analiza rizika kojom se utvrđuju ukupni učinci prekida rada kritične infrastrukture (Hrvatski sabor, 2013). Dakako, na drugu stranu od normativnog akta, treba odmah uvidjeti i stanje provedbe istoimenog Zakona. Ovdje se naši stručnjaci za nacionalnu sigurnost uvelike slažu. Primjerice, u jednom javno objavljenom intervjuu stručnjak za nacionalnu sigurnost Robert Mikac napominje da nikada nije točno određeno koje su to komponente kritične infrastrukture te da posljedično tome, postojeći Zakon, donesen 2013. godine, nikada nije u potpunosti zaživio, ali napominje da je novi Zakon koji će definirati područje kritične infrastrukture u izradi (Zaštita, 2021: 23). Također, Mikac napominje da javno-privatno partnerstvo u zaštiti kritičnih infrastruktura nije definirano te nije opisano kako ga ostvariti (Zaštita, 2021: 24). Jedno od zadnjih misli u ovom intervjuu je važnost suradnje javnog, privatnog i akademskog sektora (Zaštita, 2021: 25). Dodatno, stručnjak za nacionalnu sigurnost Gordan Akrap tvrdi da je Zakon definirao okvir, ali nije uspješno proveden u praksi te napominje važnost potrebnih izmjena i dopuna Zakona (Akrap, 2019: 39). U više navrata Akrap predlaže da se ulaganja u kritičnu infrastrukturu predstavljaju kao proračunska obrambena izdvajanja (Akrap, 2019: 39, 47). Iako za RH nisu imenovane

konkretne komponente kritične infrastrukture svakog pojedinog sektora, ovdje će se nabrojati za svaki sektor kritične infrastrukture konkretne organizacije koje bi trebale pripadati pojedinim sektorima sukladno Zakonu o kritičnoj infrastrukturi. U sektoru energetike organizacije koje bi trebale pripadati kritičnoj infrastrukturi jesu Hrvatska elektroprivreda (HEP), Industrija nafte (INA), Prvo plinarsko društvo (PPD), Jadranski naftovod (JANAF), HEP operator prijenosnog sustava (HOPS). U sektoru komunikacijske i informacijske tehnologije organizacije koje bi trebale pripadati kritičnoj infrastrukturi jesu Hrvatski Telekom, A1 te ostale značajnije privatne korporacije IT sektora koje imaju određenu poslovnu suradnju s državnim institucijama. U sektoru prometa takve organizacije bi bile Hrvatske željeznice, Hrvatske ceste, Hrvatske autoceste, zračne i morske luke diljem RH te ACI marina. U sektoru zdravstvene zaštite to bi bile KBC-ovi u RH, PLIVA, HALMED, Imunološki zavod i ostali. U vodnom gospodarstvu takva organizacija jesu Hrvatske vode. U sektoru hrane organizacije koje bi trebale pripadati jesu Podravka te načelno stanje OPG-ova i ostalih poljoprivrednih gospodarstava. U sektoru financija to su privatne i javne banke, Zagrebačka burza, FINA, HANFA, sustav Porezne uprave i osiguravateljske tvrtke poput Croatia osiguranja. U proizvodnji, skladištenju i prijevozu opasnih tvari zasigurno bi trebala pripadati NE Krško. U javnom sektoru to su tijela državne uprave poput ministarstava i ostalih te sve vrste hitnih službi. Od nacionalnih spomenika i vrijednosti su zasigurno svi oni nacionalni parkovi te spomenici i građevine zaštićene UNESCO-m. I naposljetku, u sektor znanosti i obrazovanja trebaju pripadati institucije poput Sveučilišta u Zagrebu i svih ostalih gradova te znanstveni instituti poput Instituta Ruđera Boškovića.

Važan dokument kojim se naznačuju načelni pravci zaštite kritične infrastrukture je Strategija nacionalne sigurnosti Republike Hrvatske (Hrvatski sabor, 2017). U Strategiji se iznosi devet strateških ciljeva, a jedan se odnosi, između ostaloga i na kritičnu infrastrukturu. Dotični strateški cilj glasi: „Dostizanje najvišeg stupnja sigurnosti i zaštite stanovništva te kritičnih infrastruktura.“ U daljnjem tekstu, ponajviše u poglavlju u kojem se razrađuje konkretan strateški cilj, napominje se da je za sigurno društvo nužna zaštita života, spašavanje ljudi i dobara te zaštita kritične infrastrukture. Nadalje, nabrajaju se mjere, politike, kojima će se postići zaštita kritične infrastrukture: „…usmjerit će se na prevenciju, uklanjanje ili ublažavanje rizika koji mogu izazvati ranjivost kritičnih infrastruktura te jačanje njihove otpornosti. Sustav upravljanja i

nadzora nad pojedinim kritičnim infrastrukturama potrebno je kontinuirano nadograđivati i poboljšavati, uz primjenu najboljih iskustava koja na tom području imaju druge države.“ Spominje se i razvoj modela razmjene podataka između državnih tijela i agencija te operatora kritične infrastrukture. Napominje se kako će država, na temelju dokumenata kojima se definira upravljanje kritičnom infrastrukturom, odrediti one komponente infrastrukture koji će morati ostati u većinski državnom vlasništvu u slučaju poslovnih nestabilnosti. Također, prilikom izrade Strategije očito se jasno naglašava potreba za koordiniranom suradnjom javnog i privatnog sektora kako bi se poboljšali izgledi za jačanje otpornost kritične infrastrukture. Naravno, pod privatnim sektorom se ponajviše misli na sektor privatne zaštite te općenito mogućnosti civilnog dijela stanovništva.

Još jedan ključan strateški dokument je Nacionalna strategija kibernetičke sigurnosti (Vlada RH, 2015). Strategija obuhvaća sigurnosne mjere u području komunikacijske i informacijske infrastrukture i usluga, a razlikuju se javne elektroničke komunikacije, elektronička uprava i elektroničke financijske usluge. Važno mjesto u Strategiji te definiranju kibernetičke sigurnosti ima kritična komunikacijska i informacijska infrastruktura koja se može nalaziti u svakoj pojedinoj komponenti maloprije nabrojane infrastrukture te se u Strategiji ukazuje na važnost definiranja kriterija za utvrđivanje kritične komunikacijske i informacijske infrastrukture. U jednom dijelu Strategije definira se dotična infrastruktura: „Kritičnu komunikacijsku i informacijsku infrastrukturu predstavljaju oni komunikacijski i informacijski sustavi koji upravljaju kritičnom infrastrukturom ili su bitni za njezino funkcioniranje, neovisno o kojem sektoru kritične infrastrukture je riječ“ (Vlada RH, 2015: 14). U slučaju dotične Strategije koja je trenutno na snazi te se njezino provođenje prati na godišnjoj razini, važno je napomenuti da 16. prosinca 2020. godine Europska komisija donijela novu Strategiju za kibernetičku sigurnost za predstojeće desetljeće (Europska komisija, 2020). Naravno, pošto se RH usklađuje sa svim relevantnim aktima ovakvog tipa, moguće je u skorije vrijeme očekivati i obnovljenu Strategiju kibernetičke sigurnosti na nacionalnoj razini.

Od ostalih značajnih normativnih aktova koji doprinose definiranju politika zaštite nacionalne kritične infrastrukture jesu izvori sekundarnog zakonodavstva Europske unije – NIS direktiva i GDPR uredba. NIS direktiva stvara primjerene okvire prevencije i zaštite društva od kibernetičkih prijetnji te teži usklađenim vertikalnim sektorskim

pristupima, a GDPR uredba sličan pristup osigurava horizontalnim pristupom kroz sve segmente društva (Srce, 2018: 4). U RH NIS direktiva je uvedena u hrvatski zakonodavni okvir pod imenom Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (ZKS) (Hrvatski sabor, 2018), dok je GDPR uredba uvedena u hrvatski zakonodavni sustav 25.05.2018. pod nazivom Opća uredba o zaštiti podataka (EU, 2016) za čiji nadzor provedbe je nadležna Agencija za zaštitu osobnih podataka (AZOP). Nadalje, stručnjak za nacionalnu sigurnost Željko Cvrtila u jednom intervjuu spominje da ZKS nikada nije implementiran (Zaštita, 2021: 20). S druge strane, predstojnik Ureda za korporativnu sigurnost HEP-a Miljenko Filipović u intervjuu govori sljedeće: „Naime, ZKS je jednoznačno odredio pružatelje ključnih usluga za funkcioniranje društva i gospodarstva Republike Hrvatske. ZKS je u potpunosti upotrebljiva osnova te dorečen i zaokružen zakonodavni okvir za provedbu aktivnosti i mjera zaštite i obrane kritičnih sustava od prijetnji iz kibernetičkoga prostora.“ (Zaštita, 2021: 27). Međutim, bez obzira na različita mišljenja ZKS je implementiran i provodi se u praksi, za razliku od Zakona o kritičnim infrastrukturama koji nije „zaživio“ u praksi.

Zanimljivo je spomenuti da je Vlada tijekom 2021. godine donijela Odluku na temelju koje se omogućava uključenje u sustav SK@UT operatorima ključnih usluga, davateljima digitalnih usluga, operatorima kritične nacionalne infrastrukture te drugim pravnim osobama registriranim u RH (SOA, 2021: 17). Dakako, sustav SK@UT su osmislili SOA i ZSIS u cilju podizanja nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od kibernetičkih napada, a cilj mu je nadasve otkrivati upravo one sofisticirane napade poput APT napada koje u pravilu provode državno sponzorirane organizacije ili pak same države (SOA, 2021: 17).

Iz perspektive strateškog i normativnog okvira RH, stanje u području zaštite nacionalne kritične infrastrukture se u potpunosti podudara s regulativama EU-a. Međutim, neminovno je izbjeći kritike stručnjaka u području nacionalne sigurnosti koji uočavaju nedostatke prilikom provedbe zakona koji se tiču definiranja politika povezanih s kritičnom infrastrukturom. Mora se navesti da osim strateškog i normativnog okvira postoje i materijali znanstvenog karaktera u hrvatskom znanstvenom opusu u ovom području. Isto tako, postoje i časopisi koji također prate ovu tematiku te pojedinci iz javnog i privatnog sektora koji se susreću s problematikom sigurnosti kritične infrastrukture na dnevnoj, operativnoj, tehničkoj razini. Sve ovo

govori da potencijal za kvalitetnu suradnju između javnog, privatnog i akademskog sektora, u području zaštite kritične infrastrukture, postoji.

3.1. Europske politike zaštite kritične infrastrukture

U ovom dijelu poglavlja o politikama zaštite kritične infrastrukture posvetit će se pažnja ovoj tematici iz perspektive EU-a. Velikim dijelom se za pisanje ovog dijela poglavlja koristi dokumentacija koju je izdala ENISA, a komponente kritične infrastrukture koje su obrađene tim dokumentima su kritična informacijska infrastruktura, internet, industrijski upravljački sustavi (*ICS* i *SCADA*), pametne mreže (*Smart Grid*), financijski sektor, zdravstvo, pomorstvo i naposljetku željeznice.

U pravilu, ENISA za svaki od maločas nabrojanih sektora objavljuje relativno česta izvješća u kojima analizira trenutno stanje u pojedinom sektoru kritične infrastrukture. Veliki broj izvješća ENISA radi u suradnji s javnim, privatnim i akademskim sektorom na način da provodi intervjue među odabranicima, provodi ankete i druge slične metode koje služe za prikupljanje različitih i relevantnih mišljenja. U jednom od takvih izvještaja je obrađeno trenutno stanje europske sigurnosne telekomunikacijske legislative (ENISA, 2021). Na samom početku izvješća se spominje trenutak kada je Europska komisija objavila listu preporuka u 2019. godini o kibernetičkoj sigurnosti 5G mreža, a napominje se i kako je objavljen prijedlog Europske komisije za novu, NIS2 direktivu krajem 2020. godine, koja bi dovela pravila europske telekomunikacijske sigurnosti pod NIS direktivu (ENISA, 2021: 2). Također, jedan od ciljeva ovog izvješća je i upoznavanje s direktivom o europskom zakoniku elektroničkih komunikacija. Zaključci ovog izvješća jesu da europska telekomunikacijska legislativa ima pozitivan utjecaj, nekoliko stručnjaka za sigurnost je navelo da je nacionalna telekomunikacijska legislativa kompleksna, razina moći je na zadovoljavajućoj razini ali resursi nisu, objava incidenata može biti poboljšana te suradnja na nacionalnim i europskim razinama je dobra (ENISA, 2021: 3).

Od internetske infrastrukture pridaje se pažnja *Border Gateway Protocolu* (*BGP*), razvijen prije 25 godina, koji ujedno predstavlja kralježnicu interneta globalno te ga pružatelji usluga interneta koriste za prijenos internet prometa (ENISA, 2019: 3). U ovom izvješću se ne pridaje važnost normativnim i strateškim dokumentima na

europskoj razini, ali se kroz 7 konkretnih savjeta nadasve tehničkog karaktera pokušava dati konstruktivan obol za buduće djelovanje u ovom sektoru kritične infrastrukture (ENISA, 2019: 4).

Nadalje, industrijski upravljački sustavi (IUS) predstavlja pojam koji opisuje automatizirane industrijske sustave za akviziciju podataka, vizualizaciju i upravljanje industrijskim procesima, a često su prisutni u različitim industrijskim sektorima i kritičnim infrastrukturama (ENISA, 2015: 6). Iz cijelog izvješća u suštini proizlazi 6 preporuka (ENISA, 2015: 7). Treba uskladiti napore u IUS području s nacionalnim strategijama kibernetičke sigurnosti i ostalim regulativama koje se tiču zaštite kritične informacijske infrastrukture, razviti dobre prakse specifične za kibernetičku sigurnost IUS sustava, standardizirati dijeljenje informacija između kritičnih sektora i zemalja članica, graditi svijest o kibernetičkoj sigurnosti IUS-a, njegovati stručnost zajedno s provedbom treninga i edukativnih programa u području kibernetičke sigurnosti IUS-a te promocija i podrška istraživanju kibernetičke sigurnosti IUS-a (ENISA, 2015: 7).

Pametne mreže (engl. *Smart Grid*) mogu biti definirane kao nadogradnja postojeće električne mreže kroz dvosmjernu digitalnu komunikaciju između dobavljača i potrošača, inteligentnog mjerenja i sustava za nadzor (ENISA, 2012: 1).

Također, i ovo izvješće nudi 10 preporuka s kojima bi se podigla kvaliteta kibernetičke sigurnosti pametnih mreža. Primjerice, prva preporuka ide u smjeru poduzimanja inicijative Europske komisije i država članica EU-a za poboljšanje regulatornog okvira kibernetičke sigurnosti pametnih mreža. Europska komisija u suradnji s ENISA-om i zemljama članicama treba promovirati javno-privatna partnerstva kako bi koordinirala inicijative u sferi kibernetičke sigurnosti pametnih mreža. ENISA i Europska komisija bi trebale poticati svijest o ovom području te poticati edukacijske inicijative, Europska komisija i zemlje članice, zajedno s ENISA-om, bi trebale poticati inicijative širenja i dijeljenja znanja. Nadalje, ova tri dionika bi također trebala pokušati propisati set sigurnosnih mjera temeljenih na trenutnim standardima i vodičima. Europska komisija i zemlje članice bi trebale promovirati razvoj shema sigurnosnih certifikata za komponente, proizvode i organizacijsku sigurnost. Također, ista dva dionika bi trebala promovirati kreiranje sustava za testiranje i sigurnosne procjene. Sva tri dionika bi trebala dalje proučavati i doraditi strategije za koordiniranje mjera koje služe za odgovor kibernetičkim incidentima u energetskim mrežama na paneuropskoj razini. Zemlje članice bi trebale zajedno s nacionalnim CERT-ovima

inicirati aktivnosti koje bi uključivale savjetodavnu ulogu prilikom susretanja s kibernetičkim incidentima u energetskom sustavu te na kraju, Europska komisija i zemlje članice trebaju zajedno s akademskim sektorom poticati istraživanje i razvoj u segmentu kibernetičke sigurnosti pametnih mreža (ENISA, 2012: 1-2).

Financijski sektor je iznimno reguliran te su odredbe kibernetičke sigurnosti već uključene u različite politike EU-a i njezinu legislativu, te je trenutno par inicijativa posvećeno poboljšanju iste sigurnosti (ENISA, 2021b: 3). Ono što je obrađeno u ovom izvješću je razvoj i implementacija politika za financijski sektor gdje su predstavljene neke inicijative poput Akcijskog plana za *Fintech* industriju, strategija za digitalne financije iz 2020. godine te prijedlog *Digital Operational Resilience Act-a* koji ukazuje na važnost informacijske komunikacijske tehnologije u financijskom sektoru (ENISA, 2021b: 4). Zatim je obrađena tematika dijeljenja informacija i predstavljen prvi europski okvir za dijeljenje informacija između vlasti, financijskih institucija i timova koji provode kontrolirane kibernetičke napade (*Red Team*) (ENISA, 2021b: 7). Isto tako, tijekom 2020. godine je pokrenuta inicijativa *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU) koja također služi za razmjenu informacija i najboljih praksi između javnih i privatnih dionika (ENISA, 2021b: 7). Zatim je spomenuto kako ENISA igra važnu ulogu prilikom koordiniranja odgovora na nastale eventualne incidente u kibernetičkoj sigurnosti (ENISA, 2021b: 10). Također, i u ovom se dijelu spominje važnost podizanja svijesti te organiziranja edukacijskih predavanja (ENISA, 2021b: 10,11). Isto tako, ukazuje se na važnost standardizacije i certificiranja (ENISA, 2021b: 12) te je predstavljena jedna mreža za istraživanje i razvoj na razini EU-a u sferi kibernetičke sigurnosti koja se zove CONCORDIA i znanstveni projekt pod nazivom *Cybersecurity for Europe* (ENISA, 2021b: 13).

Zdravstveni sustav, odnosno njegove bitne komponente bolnice, su definirane kao jedna od segmenata kritične infrastrukture. A kako kibernetička sigurnost biva od sve veće važnosti za bolnice, važno je da je kao takva ugrađena u različite procese, komponente i razine koje utječu na sveukupno stanje informacijskih tehnologija bolničkog sustava (ENISA, 2020s: 5). U ovom izvješću se analizira proces nabave u bolnicama, a predstavljene su i dobre prakse. Napominje se da bi trebalo uključiti IT odjel u nabavu prvenstveno iz razloga uvida u eventualne propuste u prostoru kibernetičke sigurnosti te implementirati proces identifikacije ranjivosti sustava i upravljanja istim (ENISA, 2020s: 29). Treba razviti unutarnju politiku ažuriranja

hardvera i softvera i poraditi na sigurnosti bežičnih komunikacija unutar bolnice, prije svega WiFi mreži (ENISA, 2020s: 30). Također, napominje se potreba za uspostavljanjem sustava za sigurnosno testiranje pojedinih uređaja i sustava u bolnici (ENISA, 2020s: 31). Nadalje, u slučaju pada sustava trebaju biti uspostavljeni planovi koji će osigurati kontinuitet poslovanja (ENISA, 2020s: 32). U slučaju uvođenja novijih komponenti informacijske tehnologije treba uzeti u obzir potencijalne sigurnosne praznine prilikom rada sa starijim komponentama sustava (ENISA, 2020s: 32). Treba omogućiti prikupljanje i spremanje podataka iz sustava, kako bi se u slučaju napada moglo lakše otkriti uzrok propusta (ENISA, 2020s: 33) i savjetuje se enkripcija osjetljivih osobnih podataka (ENISA, 2020s: 34). Postoje još pojedini prijedlozi tehničkog i menadžerskog karaktera, ali se nadovezuju na već spomenute.

Na razini EU-a luke se smatraju važnima prilikom omogućavanja funkcioniranja domaćeg i međunarodnog lanca dobave, a u EU luke igraju važnu ulogu te podržavaju 90% izvoza EU-a i dodatnih 43% unutarnje tržišne razmjene (ENISA, 2020t: 8). U pravilu, preporuke za luke se mogu svesti na 4 faze upravljanja rizicima u sferi kibernetičke sigurnosti. Identifikacija imovine i usluga koje su povezane s kibernetičkim rizicima, identifikacija i evaluacija kibernetičkih rizika, identifikacija sigurnosnih mjera tehničkog i strateškog, normativnog karaktera i naposljetku, procjena zrelosti kibernetičke sigurnosti s obzirom na provedene mjere (ENISA, 2020t: 53).

Zadnja komponenta kritične infrastrukture obrađena u izvješćima ENISA-e je željeznica. Željeznički sektor omogućava prijenos ljudi i dobara te je ključan za razvoj EU-a (ENISA, 2020u: 8). Prilikom implementacije NIS direktive, velika većina EU zemalja, između njih i RH, je identificirala bitne usluge željezničkog sektora poput upravljanja i održavanja infrastrukture, omogućavanje prijevoza putnika i dobara i ostalo (ENISA, 2020u: 21). Naravno, kao i za ostale sektore tako i za željeznice iz NIS direktive proizlaze politike zaštite ove komponente kritične infrastrukture.

Na kraju ovog poglavlja može se reći koji su to strateški i normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture. Oni su: Strategija nacionalne sigurnosti Republike Hrvatske (Hrvatski sabor, 2017), Nacionalna strategija kibernetičke sigurnosti (Vlada RH, 2015), Zakon o kritičnim infrastrukturama (Hrvatski sabor, 2013), Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Hrvatski sabor, 2018) i Opća uredba o zaštiti podataka (Europski parlament i Vijeće, 2016). Dakle, RH legislativa, koja se tiče zaštite kritične

infrastrukture, prati EU legislativu. Međutim, postoje određene manjkavosti po pitanju provođenja određenih zakonskih akata na razini RH poput Zakona o kritičnim infrastrukturama (Hrvatski sabor, 2013). S druge strane, na razini EU, odnosno ENISA-e postoje mnoge analize koje detaljnije proučavaju politike zaštite pojedinih komponenti kritičnih infrastruktura. To dovodi do zaključka da bi takve analize mogli provesti, u najmanju ruku, na razini RH te naknadnom sintezom sprovesti određene zaključke u formu službenih ili savjetodavnih akata.

4. Javno-privatna partnerstva u kibernetičkom prostoru

U ovom poglavlju se razrađuje pojam javno-privatnih partnerstava (JPP) u kibernetičkoj sferi te se odgovara na treće pitanje: Koji su uvjeti potrebni te čime su isti definirani u slučaju sklapanja javno privatnih partnerstava u kibernetičkoj sferi u RH? Kao temelj za traženje odgovora na ovo istraživačko pitanje analizirani su strateški i normativni akti RH. Naknadno, analizirani su dokumenti ENISA-e koji se tiču JPP-a u kibernetičkoj sferi te tisak u RH koji razrađuje ovakve i slične tematike. Uz sve to, u sklopu pisanja ovog poglavlja provedena je anketa na koju je odgovorilo pet privatnih pravnih osoba. Naime, anketa je bila namijenjena isključivo privatnim tvrtkama koje pružaju usluge ili proizvode kibernetičke sigurnosti, a djeluju između ostalog unutar okvira RH.

Suradnja javnog i privatnog sektora se opetovano pojavljuje u Strategiji nacionalne sigurnosti Republike Hrvatske iz 2017. godine (Hrvatski sabor, 2017). U tom dokumentu se nalaže važnost, između ostalog, jačanja otpornosti kritične infrastrukture na suvremene prijetnje te se istovremeno napominje potreba za suradnjom javnog i privatnog sektora, ponajviše sektora privatne zaštite. Nadalje, među ciljevima Nacionalne strategije kibernetičke sigurnosti (Vlada RH, 2015: 15) ističe se ojačavanje JPP-a i tehničke koordinacije u obradi računalnih sigurnosnih incidenata kako bi se osigurao nesmetani rad za one poslovne subjekte koji u svojem vlasništvu imaju kritičnu infrastrukturu. Također, u istoj Strategiji se navodi pod drugim ciljem kako će državna tijela kroz koordinirani pristup poticati JPP te povezivanje akademskog, javnog i gospodarskog sektora (Vlada RH, 2015: 26). Od normativnih akata postoji Zakon o kritičnim infrastrukturama (Hrvatski sabor, 2013) koji ne definira uspostavljanje JPP-a. Slično govori i Mikac u jednom od svojih intervjua gdje napominje da JPP nije definiran u zaštiti kritične infrastrukture te spominje važnost JPP-a: „JPP u jačanju otpornosti i zaštiti kritičnih infrastruktura predstavlja platformu suradnje i unapređenja zajedničkih potreba i interesa između vrlo različitih aktera u jednom društvu“ (Zaštita, 2021: 24). Naravno, za ovakvu nesinkroniziranost Zakona o kritičnim infrastrukturama i Nacionalne strategije kibernetičke sigurnosti razlog se može tražiti u vremenu nastajanja akta, a očito je da je Zakon donesen dvije godine prije Strategije. Zanimljiva je izjava trenutno čelnog čovjeka SOA-e Daniela Markića koja glasi: „Primijetili smo da i hrvatske institucije su pod konstantnim cyber napadima.

Stvorili smo novi cyber centar čija je zadaća štititi naše institucije. Odlukom Vlade tu ćemo mogućnost proširiti i privatnim tvrtkama. Već smo u kontaktu s tvrtkama koje žele surađivati s nama kako bismo ih probali štititi“ (tportal, 2021). Iz ove izjave se može zaključiti kako postoje težnje javnih i privatnih institucija u RH za suradnjom u prostoru pružanja usluga kibernetičke sigurnosti.

Na europskoj razini podrobne analize za problematiku funkcioniranja JPP-a u prostoru kibernetičke sigurnosti kritične infrastrukture nudi ENISA. Definicija JPP-a glasi: „Organizirani odnos između javnih i privatnih organizacija, koja uspostavlja zajedničko područje i ciljeve, te koristi definirane uloge i radnu metodologiju za postizanje zajedničkih ciljeva“ (ENISA, 2011: 12). Kako bi se što bolje definiralo JPP, treba odgovoriti na pitanja zašto, tko, kako, što i kad nastaju ovakve vrste suradnje. Razlozi za ulazak u JPP iz perspektive javnog i privatnog sektora mogu biti često različiti, stoga, treba jasno definirati vrijednosti za oba sektora kada odlučuju biti dijelom JPP-a (ENISA, 2011: 18). Primjerice, za javni sektor jedan od razloga ulaska u JPP može biti provedba nacionalne strategije za čiju provedbu nema dovoljno resursa, a za privatnu tvrtku može biti potreba usklađivanja s pojedinim regulativama (ENISA, 2011: 18). Na pitanje tko je dionik JPP-a postoje različite vrste odgovora. Naime, postoji podjela s obzirom na geografski položaj JPP-a, a on može biti nacionalni, europski ili međunarodni te podjela može biti s obzirom na fokus JPP-a, a tada JPP može biti geografski, sektorski, međusektorski i tematski (ENISA, 2011: 23). Dakako, u svakom JPP-u postoji problem podjele posla i kako će se podijeliti odgovornost. Drugim riječima, postavlja se pitanje kako upravljati JPP-om? JPP se može podijeliti s obzirom na svrhu i vrijeme trajanja projekta, pa postoje sljedeće vrste: dugoročna zajednica, radna skupina, grupa za brze odgovore, grupa za miješane aktivnosti te sveobuhvatna strateška i savjetodavna grupa (ENISA, 2011: 28). Također, postoji podjela s obzirom na način vođenja JPP-a: vodi jedan entitet unutar JPP-a, vodi koordinirani entitet te demokratski vođen JPP (cikličko vodstvo) (ENISA, 2011: 29). Nadalje, pitanje što se odnosi na usluge i poticaje koji se nude sudjelovanjem u JPP-u. Neke od usluga su istraživanje, zajedničke vježbe, podizanje svijesti o kibernetičkim rizicima, analiza rizika i ostalo (ENISA, 2011: 36). Na drugoj strani istog pitanja se nalaze poticaji koje nudi JPP, a jedan od primjera toga mogu biti manji troškovi prilikom zajedničkog rješavanja kritičnog problema (ENISA, 2011: 37). Zadnje preostalo pitanje je kada nastaje JPP te odgovor na ovo pitanje nudi kontekst

kako je došlo do nekog JPP-a. Način nastanka od gore prema dolje (*Top down*) nalaže da postoji neka vladina direktiva na temelju koje nastaje JPP i način nastanka JPP-a od dolje prema gore (*Bottom up*) gdje zajednica prepoznaje potrebu za nastankom JPP-a (ENISA, 2011: 39). Ostali načini se izvode iz ova dva osnovna koncepta (ENISA, 2011: 39). Nakon uvida u temelje odgovora na pet pitanja koja se vežu za JPP, zanimljivo je napomenuti temeljne razloge kojima se vode dionici JPP-a prilikom sklapanja istih, a oni su redom: ekonomski interesi, regulatorni zahtjevi, odnosi s javnošću, ostalo i naposljetku društveni interesi (ENISA, 2017: 12).

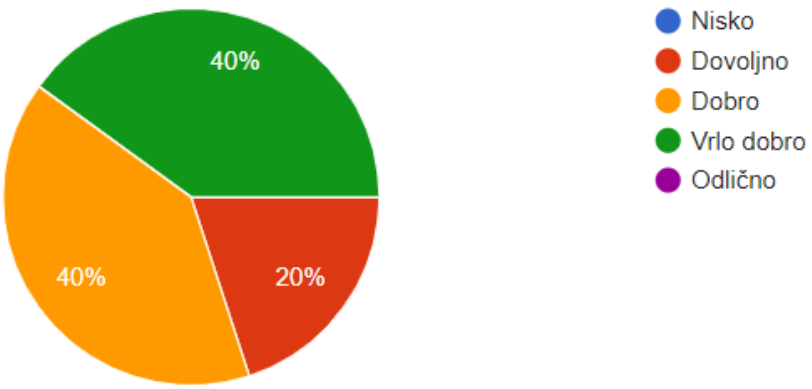
Idući dio ovog poglavlja zauzima predstavljanje i obrada rezultata ankete koja je provedena u sklopu izrade ovog rada. Cilj ankete je bio uvidjeti stanje trenutne suradnje između javnog i privatnog sektora u području kibernetičke sigurnosti iz perspektive privatnih tvrtki. Anketa se sastoji od 18 pitanja otvorenog i zatvorenog tipa te su na dotična pitanja mogli odgovarati isključivo dionici privatnih tvrtki koje nude usluge ili proizvode kibernetičke sigurnosti. Na anketu je odgovorilo pet ispitanika, odnosno dionici pet različitih privatnih tvrtki. Prije sadržajne analize rezultata, važno je napomenuti da su anketi pristupile tvrtke koje imaju broj zaposlenika u rasponu od manje od 10 zaposlenih pa sve do par stotina zaposlenika što ujedno predstavlja veliki raspon, a samim time ukazuje na šarolikost tvrtki iz perspektive broja zaposlenika. Naime, od pet tvrtki koje su pristupile anketi, njih dvije čine mala poduzeća i tri tvrtke čine srednja poduzeća. Također, u daljnjem tekstu, svaku pojedinu tvrtku će se oslovljavati s nazivom Tvrtka te će se tom nazivu pridijeliti broj. Svaka tvrtka će imati vlastiti jedinstveni broj. Ovakvim pristupom se postiže anonimnost ispitanika, a u drugu ruku i njegova jedinstvenost.

Nadalje, od svih tvrtki koje su odgovorile na anketu, jedino se Tvrtka 5 isključivo bavi pružanjem usluga kibernetičke sigurnosti, a to je ujedno i najmanja tvrtka koja je pristupila ovoj anketi. Ostale tvrtke nude još neke usluge ili proizvode uz kibernetičku sigurnost. Primjerice, Tvrtka 1 pruža zaštitu implementirane opreme i aplikacija, Tvrtka 2 u svojoj ponudi ima edukacije i treninge, Tvrtka 3 pruža usluge savjetovanja, implementaciju i održavanje rješenja u području kibernetičke sigurnosti te pruža usluge sigurnosne analitike. Tvrtka 4 nudi konzultantske usluge i trenutno su u procesu razvoja digitalne platforme za uspostavu sustava zaštite kritičnih infrastruktura u pametnim industrijama. Tvrtka 5 provodi penetracijske testove, specijalizirane edukacije za djelatnike, upravlja sigurnosnim rizicima, drži radionice osvještavanja o

problematici kibernetičke sigurnosti, upravlja incidentima te posjeduje sigurnosno-operativni centar (SOC). Ovdje je još važno za istaknuti da navedene tvrtke pružaju slične, pa i iste usluge i proizvode svojim klijentima u privatnom i javnom sektoru. Iz toga očito proizlazi zaključak da se dionici privatnog i javnog sektora susreću s gotovo istim izazovima u kibernetičkom prostoru.

Pošto JPP nije jedini oblik partnerstva u kojem mogu sudjelovati privatne tvrtke poput anketiranih, u anketi je, pod brojem pet postavljeno pitanje: „U kojim područjima djeluju tvrtke iz privatnog sektora s kojima Vaša tvrtka surađuje na području kibernetičke sigurnosti“. Primjerice, Tvrtka 1 surađuje s tvrtkama iz IT sektora, Tvrtka 2 surađuje s financijskim sektorom te tvrtkama koje pokrivaju ostale komponente kritične infrastrukture. Tvrtka 3 posluje s bankarskim sektorom, tvrtkama koje se bave osiguranjem i distribucijom. Tvrtka 4 je u anketi izjavila da surađuje s tvrtkama koje pod svojom ingerencijom imaju kritičnu infrastrukturu, ali nije napomenuto koja konkretno. Tvrtka 5 posluje s tvrtkama koje se bave telekomunikacijama, financijama te proizvodnjom, prodajom i razvojem softvera. Od poslova na kojima surađuju s tvrtkama partnerima ističe se Tvrtka 4 koja nudi rješenja u blockchainu te za SCADA sustave.

U sedmom pitanju se tražila procjena razine znanja o kibernetičkim rizicima u tvrtkama s kojima surađuju anketirane tvrtke. Percepcija znanja o kibernetičkim rizicima u privatnim tvrtkama s kojima posluju je moguće vidjeti na Slici 1.



Slika 1: Znanje o kibernetičkim rizicima u privatnom sektoru

Može se lako uvidjeti da je mišljenje podijeljeno, ali u pravilu ni jedan ispitanik nije ocijenio znanje o kibernetičkim rizicima u privatnom sektoru s krajnjim ocjenama poput nedovoljnog ili odličnog.

Kibernetički rizici s kojima su se anketirane tvrtke najčešće susrele su *malware*, odnosno *ransomware* te *phishing,* a u odgovorima su se našli i rizici poput *DDoS-a*, *APT-a* i iskorištavanje ranjivosti nultog dana (*Zero day exploit*). Također, u ovoj anketi se pridaje više pažnje informacijskoj komponenti kibernetičke sigurnosti te se tražilo mišljenje o provođenju standarda upravljanja sustavom informacijske sigurnosti ISO 27001 među tvrtkama s kojima posluju anketirani. Mišljenja su i u ovom slučaju bila podijeljena na način da su dvije tvrtke rekle da se navedeni standard u dotičnim sektorima provodi na zadovoljavajućoj razini, dvije tvrtke su napomenule da se standard provodi ispod zadovoljavajuće razine te je jedna napomenula da se standard uopće ne provodi.

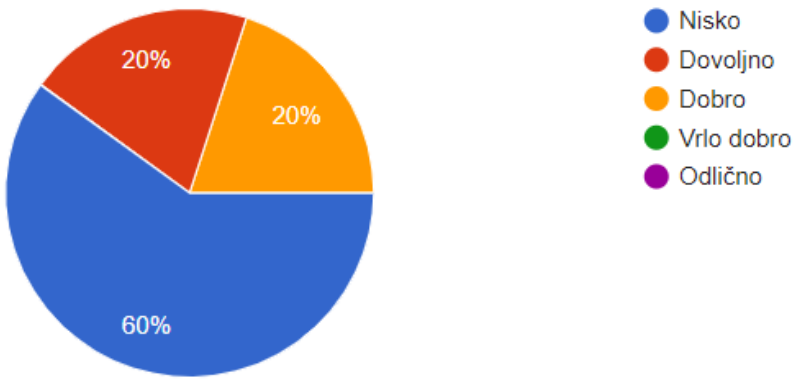
Nadalje, pod brojem deset postavljeno je pitanje o učestalosti nadgledanja i/ili upravljanja nekom vrstom kritične informacijske infrastrukture. Tvrtke 1 i 2 odgovaraju da njihovi partneri provode dotične aktivnosti često, odnosno svakodnevno. Tvrtka 3 navodi da većina njezinih partnera u nekoj mjeri upravlja i nadgleda, ali uglavnom nemaju dovoljno ljudi za to, nedovoljno su razvijeni procesi te rješenja nisu adekvatna ili nisu dovoljno dobro posložena. Tvrtka 4 i 5 napominju da partneri to rade rijetko, u slučaju sumnjivih radnji, ali da postoje primjeri partnera koji tome posvećuju kako dolikuje, odnosno svakodnevno. Inače, partneri o kojima anketirane tvrtke odgovaraju u dotičnom pitanju, dolaze iz energetskog, zdravstvenog, financijskog i prometnog sektora, a još se spominju i osobni podaci te intelektualno vlasništvo kao dio kritične informacijske infrastrukture kojom se upravlja. Lako se može uočiti da u slučaju nadgledanja kritične informacijske infrastrukture postoji veliki prostor za buduće dorade i poboljšanja.

Drugi dio ankete se koncentrira više na suradnju anketiranih tvrtki i tvrtki iz javnog sektora ili javnog sektora općenito. Naime, drugi dio ankete započinje pitanjem pod brojem dvanaest o suradnji ispitanika i javnog sektora. Zabilježena su četiri odgovora od kojih dvije tvrtke tvrde da surađuju rijetko s javnim sektorom (25% od ukupnog broja projekata), a druge dvije tvrtke surađuju vrlo često s javnim sektorom (75% od ukupnog broja projekata). Ostala tri ponuđena odgovora nije odabrao niti jedan ispitanik, a ponuđeni odgovori su bili sljedeći: uopće ne surađujemo, surađujemo često (50% od ukupnog broja projekata) i surađujemo gotovo stalno (90% i više od ukupnog broja projekata). Tvrtka 5 nije odgovorila na ovo pitanje. Poslovi, tj. usluge i proizvodi kibernetičke sigurnosti koje anketirane tvrtke pružaju tvrtkama iz javnog sektora su u

pravilu podjednaka onim uslugama i proizvodima koje pružaju privatnim tvrtkama partnerima što je već navedeno u gornjem dijelu poglavlja. Prilikom odgovaranja na ovo pitanje, Tvrtka 1 je bila konkretna te izjavila da je dobavljač rješenja za digitalizaciju poslovnih procesa javnopravnih tijela.

Nakon toga, pod pitanjem broj četrnaest, tražilo se mišljenje ispitanika o budućim trendovima kibernetičkih rizika u javnom sektoru u RH. Ovdje je važno napomenuti da su svi ispitanici odgovorili da će kibernetički rizici u javnom sektoru u RH rasti. Ovi odgovori se mogu iskoristiti kao empirijski dokaz za potvrđivanje zaključaka iz drugog poglavlja gdje se također prognozira rast pojave kibernetičkih rizika na razini EU i RH. Kao dodatak, iz priloženog se može zaključiti da će trend kibernetičkih prijetnji rasti i u privatnom sektoru s obzirom na podjednake usluge i proizvode te gotovo identične kibernetičke prijetnje s kojima se susreću javni i privatni sektor u RH.

U drugom dijelu ankete je, pod pitanjem broj petnaest, također postavljeno pitanje o razini znanja o kibernetičkim rizicima u javnom sektoru. Zanimljivo je uvidjeti, da su čak tri ispitanika procijenila znanje o kibernetičkim rizicima u javnom sektoru niskim. Jedan ispitanik je ocijenio znanje u javnom sektoru dovoljnim i jedan dobrim. Može se zaključiti da je percepcija znanja o kibernetičkim rizicima u javnom sektoru puno manja od percepcije znanja u privatnom sektoru. Naime, od ispitanika, nitko nije procijenio znanje o kibernetičkim rizicima u privatnom sektoru niskim, a za javni sektor je takvim procijenilo čak troje ispitanika. Rezultati ovog odgovora su vidljivi na Slici 2.



Slika 2: Znanje o kibernetičkim rizicima u javnom sektoru

Najčešći kibernetički rizici s kojima se susreću ispitanici u javnom sektoru su podjednaki, gotovo identični onima u privatnom sektoru, tako da u ovom segmentu nema značajnijih razlika između javnog i privatnog sektora iz perspektive ispitanika.

Također, ispitanici su odgovorili jednoliko i na osamnaesto pitanje koje propituje provođenje standarda upravljanja sustavom informacijske sigurnosti ISO 27001. Naime, kao i kod privatnog sektora dva su ispitanika odgovorila da se provodi ispod zadovoljavajuće razine, dva ispitanika su odgovorila da se provodi na zadovoljavajućoj razini te jedan da se ne provodi uopće.

I za kraj, ostalo je za razložiti sedamnaesto pitanje koje propituje problematiku sklapanja javno privatnih partnerstava vezanih za kibernetički sigurnost u RH. Ovdje Tvrtka 1 odgovara da je nužno mijenjati regulatorni okvir, koji za sada, to predviđa samo za projekte koji uključuju gradnju te je potrebno definirati standarde i uvidjeti dobre prakse kao nit vodilju. Tvrtka 3 nalaže kao ključni faktor (ne)povjerenje između privatnog i javnog sektora. Tvrtka 4 tvrdi da ima previše nepoznanica, nepostojanje jasnog okvira i uputa za takva partnerstva. Nadalje, Tvrtka 4 nadodaje da je za sada sve prepušteno tijelima državne uprave da javnim nabavama nabavljaju rješenja i usluge koje smatraju potrebnima. Tvrtka 5 vidi u birokraciji ključni problem. Tvrtka 2 nije odgovorila na ovo pitanje. Može se zaključiti na temelju odgovora na ovo pitanje da su ključni problemi nepostojanje normativnog, jasnog okvira za postizanje ovakvog tipa partnerstava te načelno nepovjerenje između javnog i privatnog sektora.

U ovom poglavlju, predstavljene su perspektive privatnog i javnog sektora na JPP. Privatni sektor kao jedan od osnovnih razloga ulaska u JPP vidi u potencijalnoj zaradi, dok javni sektor prvenstveno pokušava pružiti građanima bolju i sigurniju uslugu, a glavni izazov je kako uskladiti ova dva temeljna interesa. U ovom poglavlju je obrazložena provedena anketa među privatnim tvrtkama koje nude usluge ili proizvode kibernetičke sigurnosti. Iz ankete se može uvidjeti podosta toga. Primjerice, zanimljiva je usporedba ocjena znanja o kibernetičkim rizicima u javnom i privatnom sektoru iz perspektive privatnog sektora, gdje tri od pet tvrtki ocjenjuje znanje u javnom sektoru niskim, dok znanje ovog tipa za privatni sektor nitko nije ocijenio niskim. Glavni uvjeti za sklapanje budućih učinkovitih JPP-ova jesu jasna i definirana legislativa te izgradnja povjerenja između javnog i privatnog sektora. Na kraju, može se zaključiti da trenutni oblik javno privatne suradnje pospješuje ukupnu kvalitetu kibernetičke sigurnosti u RH, ali ne postoje još mogućnosti za ostvarivanje dugoročnih, strateških partnerstava u ovom području.

5. Zaključak

Sve učestalije korištenje digitalnih usluga javnih institucija, digitalizacija javne uprave i širenje IT sektora na razini RH i EU ima za posljedicu izloženost kibernetičkim ugrozama. Istovremeno, zaštita od kibernetičkih ugroza zahtjeva vještine, znanja i iskustvo pomoću kojih se omogućava obrana i sigurnost od navedenih prijetnji. Iako određene javne institucije pružaju uslugu kibernetičke sigurnosti javnim, državnim i akademskim institucijama, definitivno ona nije uvijek dostatna te se pojavljuje potreba za suradnjom s privatnim sektorom koji također nudi određene usluge i proizvode kibernetičke sigurnosti. Praksu suradnje javnog i privatnog sektora u kibernetičkom prostoru treba dobro definirati kako ne bi bilo propusta koji će imati implikacije na nacionalnu sigurnost. Zato su u ovom radu ponuđeni odgovori na tri istraživačka pitanja. Prvo pitanje glasi: Kakvi su trendovi kibernetičkih prijetnji i koje vrste prijetnji su zastupljene na razini EU i RH? U drugom poglavlju su imenovane sve značajnije kibernetičke prijetnje na razini EU i na razini RH, te se moglo uvidjeti i zaključiti da su učestalosti pojedinih kibernetičkih prijetnji gotovo identične na obje razine. Primjerice, *phishing* se u RH nalazi u samom vrhu, dok je na razini EU treći po redu. Isto tako, *cryptojacking* se u RH nalazi na začelju, baš kao i na razini EU. Stoga se ubuduće iz trendova na razini RH mogu uobličiti trendovi na razini EU, te obrnuto. Dakako, u anketi koja je provedena u ovom istraživanju svi ispitanici su se nedvosmisleno složili oko toga da će kibernetički rizici u javnom sektoru rasti. Privatni sektor u ovom slučaju zasigurno neće izbjeći dotične trendove. Drugo pitanje je glasilo: Koji su to strateški i normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture u RH? U trećem poglavlju su predstavljeni i obrađeni normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture. Oni su: Strategija nacionalne sigurnosti Republike Hrvatske (Hrvatski sabor, 2017), Nacionalna strategija kibernetičke sigurnosti (Vlada RH, 2015), Zakon o kritičnim infrastrukturama (Hrvatski sabor, 2013), Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Hrvatski sabor, 2018) i Opća uredba o zaštiti podataka (Europski parlament i Vijeće, 2016). Treba napomenuti da RH u potpunosti prati trendove zaštite kritične infrastrukture iz perspektive legislativnih akata, međutim, kao što napominju pojedini stručnjaci za nacionalnu sigurnost u RH, određeni zakoni ne žive u praksi kao što je slučaj sa Zakonom o kritičnim infrastrukturama. Za buduća istraživanja u ovom području potencijal leži u dubljem propitivanju politika zaštite svake pojedine

komponente kritične infrastrukture dok su u trećem poglavlju pokrivene osnovne karakteristike svake od tih politika. I treće pitanje je bilo: Koji su uvjeti potrebni te čime su isti definirani u slučaju sklapanja javno privatnih partnerstava u kibernetičkoj sferi u RH? U predzadnjem poglavlju, predstavljene su temeljne perspektive privatnog i javnog sektora na JPP. Privatni sektor kao jedan od osnovnih razloga ulaska u JPP vidi u potencijalnoj zaradi, dok javni sektor prvenstveno pokušava pružiti građanima bolju i sigurniju uslugu, a glavni izazov je kako uskladiti ova dva temeljna interesa. Kao što je već navedeno prije, provedena je anketa među privatnim tvrtkama koje nude usluge ili proizvode kibernetičke sigurnosti. Iz ankete, kao glavni razlozi zašto nema učinkovitih JPP-ova, proizlaze iz nedostatno definirane zakonske regulative koja bi isto područje definirala te nepovjerenje između javnog i privatnog sektora. Na kraju, uvidom u sva dostupna saznanja u ovom radu može se tvrditi da oblici javno privatne suradnje u kibernetičkom prostoru doprinose pozitivno kvaliteti kibernetičke sigurnosti u RH, što u konačnici potvrđuje početnu hipotezu. Isto tako, važno je još napomenuti da u RH ne postoji još legislativni okvir koji bi omogućavao ovakav vid javno privatne suradnje na dugoročnoj, strateškoj razini, već dionici ovakve suradnje improviziraju s postojećim zakonodavnim okvirom.

Literatura

- Akrap G., Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. Strategos : Znanstveni časopis Hrvatskog vojnog učilišta "Dr. Franjo Tuđman", Vol. 3 No. 2 2019.
- CERT (2020), Godišnji izvještaj 2020. Web stranica: https://www.cert.hr/GINC2020
- CERT, Web stranica: https://www.cert.hr/onama/, pristupljeno 14.09.2021.
- D. Su. (Kolovoz, 2021), Šef SOA-e otkrio: Pregovaramo s privatnim tvrtkama, štitit ćemo ih od cyber napada, tportal, Web stranica: https://www.tportal.hr/vijesti/clanak/sef-soa-e-otkrio-pregovaramo-s-privatnim-tvrtkama-stitit-cemo-ih-od-cyber-napada-foto-20210826 (pristupljeno 20.12.2021.).
- ENISA (2011), Cooperative models for effective public private partnerships. Web stranica: https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperative-models-for-effective-ppps
- ENISA (2012), Smart Grid Security. Web stranica: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations
- ENISA (2015), Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors. Web stranica: https://www.enisa.europa.eu/publications/maturity-levels
- ENISA (2017), Public private partnerships. Web stranica: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
- ENISA (2019), 7 Steps to Shore up BGP. Web stranica: https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp
- ENISA (2020a), List of Top 15 Threats. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats
- ENISA (2020b), Malware. Web stranica: https://www.enisa.europa.eu/publications/malware

- ENISA (2020c), Web-based attack. Web stranica: https://www.enisa.europa.eu/publications/web-based-attacks
- ENISA (2020d), Phishing. Web stranica: https://www.enisa.europa.eu/publications/phishing
- ENISA (2020e), Web application attacks. Web stranica: https://www.enisa.europa.eu/publications/web-application-attacks
- ENISA (2020f), Spam. Web stranica: https://www.enisa.europa.eu/publications/spam
- ENISA (2020g), Distributed denial of service. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service
- ENISA (2020h), Identity theft. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft
- ENISA (2020i), Data breach. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach
- ENISA (2020j), Insider threat. Web stranica: https://www.enisa.europa.eu/publications/insider-threat
- ENISA (2020k), Botnet. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-botnet
- ENISA (2020l), Physical manipulation, damage, theft, loss. Web stranica: https://www.enisa.europa.eu/publications/physical-manipulation-damage-theft-loss
- ENISA (2020m), Information Leakage. Web stranica: https://www.enisa.europa.eu/publications/information-leakage
- ENISA (2020n), Ransomware. Web stranica: https://www.enisa.europa.eu/publications/ransomware
- ENISA (2020o), Cyber espionage. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

- ENISA (2020p), Cryptojacking. Web stranica: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking
- ENISA (2020q), Sectoral threat analysis. Web stranica: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis
- ENISA (2020r), Emerging trends. Web stranica: https://www.enisa.europa.eu/publications/emerging-trends
- ENISA (2020s), Procurement guidelines for cybersecurity in hospitals. Web stranica: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
- ENISA (2020t), Cyber risk management for ports. Web stranica: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports
- ENISA (2020u), Railway cybersecurity. Web stranica: https://www.enisa.europa.eu/publications/railway-cybersecurity
- ENISA (2021a), Assessment of EU Telecom Security Legislation. Web stranica: https://www.enisa.europa.eu/publications/assessment-of-eu-telecom-security-legislation
- ENISA (2021b), EU cybersecurity initiatives in the finance sector. Web stranica: https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector
- Europska komisija (2020), The EU's Cybersecurity Strategy for the Digital Decade. Web stranica: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN
- Europski parlament i Vijeće (2016), Opća uredba o zaštiti podataka.
- Hrvatski sabor, Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu. NN 9/2002. Web stranica: https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html
- Hrvatski sabor, Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske. NN 105/2006. Web stranica: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske

- Hrvatski sabor, Zakon o informacijskoj sigurnosti, NN 79/2007. Web stranica: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html
- Hrvatski sabor, Zakon o kritičnim infrastrukturama, NN 56/2013. Web stranica: https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama
- Hrvatski sabor, Strategija nacionalne sigurnosti Republike Hrvatske, NN 73/2017. Web stranica: https://narodne-novine.nn.hr/clanci/sluzbeni/2017_07_73_1772.html
- Hrvatski sabor, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/2018. Web stranica: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html
- Hrvatski sabor, Zakon o privatnoj zaštiti, NN 16/2020. Web stranica: https://www.zakon.hr/z/291/Zakon-o-privatnoj-za%C5%A1titi
- Kezerić A. M., Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture, Zagreb, 2017.
- Košutić D., 2012, 9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual. Zagreb, EPPS Services Ltd.
- Marietje Schaake (2020). The Lawless Realm. Foreign Affairs (Studeni, 2020). Web stranica: https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
- Mikac R., Mamić K., Žutić I., Cyberterrorism Threats to Critical Infrastructure: Coordination and Cooperation from Brussels to South- Eastern Europe and back, Ljubljana, 2020.
- SOA (2020), Javno izvješće 2019. Web stranica: https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/
- SOA (2020), Javno izvješće 2020. Web stranica: https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/
- Srce, broj 71, 2018.
- Statista, 2022, Number of Internet users worldwide from 2005 to 2021. Web stranica: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
- Vlada Republike Hrvatske, Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste

redoslijeda sektora kritičnih infrastruktura, NN 108/2013. Web stranica: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html

- Vlada Republike Hrvatske. Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti. NN 108/2015. Web stranica: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html
- Vojković G., Štambuk-Sunjić M., Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split, 2006.
- Vuković H., Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, Vol. 13 No. 3, 2012.
- Zaštita, broj 8, 2021.
- Zelenika R., (2000), Metodologija i tehnologija izrade znanstvenog i stručnog djela. Rijeka: Ekonomski fakultet.
- ZSIS, Web stranica: https://www.zsis.hr/

SAŽETAK

Sve učestalije korištenje digitalnih usluga javnih institucija, digitalizacija javne uprave ima za posljedicu izloženost kibernetičkim ugrozama. Istovremeno, zaštita od kibernetičkih ugroza zahtjeva vještine, znanja i iskustvo pomoću kojih se omogućava obrana i sigurnost od navedenih prijetnji. Iako određene javne institucije pružaju uslugu kibernetičke sigurnosti javnim, državnim i akademskim institucijama, definitivno ona nije uvijek dostatna te se pojavljuje potreba za suradnjom s privatnim sektorom koji također nudi određene usluge i proizvode kibernetičke sigurnosti. Praksu suradnje javnog i privatnog sektora u kibernetičkoj sferi treba dobro definirati kako ne bi bilo propusta koji će imati implikacije na nacionalnu sigurnost. U ovom radu su ponuđeni odgovori na tri istraživačka pitanja. Prvo pitanje glasi: Kakvi su trendovi kibernetičkih prijetnji i koje vrste prijetnji su zastupljene na razini EU i RH? Drugo pitanje glasi: Koji su to strateški i normativni akti koji definiraju sustav kibernetičke sigurnosti kritične infrastrukture u RH? I treće pitanje je: Koji su uvjeti potrebni te čime su isti definirani u slučaju sklapanja javno privatnih partnerstava u kibernetičkoj sferi u RH? Prilikom odgovaranja na ova tri istraživačka pitanja, koristi se više metoda istraživanja poput teorije sustava, induktivnom i deduktivnom metodom. Prilikom odgovaranja na treće istraživačko pitanje koristi se i metoda intervjua s pojedinim privatnim tvrtkama koje nude usluge ili proizvode u sferi zaštite kritične infrastrukture od kibernetičkih prijetnji. Na kraju želi se provjeriti početna hipoteza koja govori da javno privatna partnerstva u kibernetičkom prostoru doprinose kvaliteti kibernetičke sigurnosti u RH.

Ključne riječi: nacionalna sigurnost, kibernetička sigurnost, informacijska sigurnost, kritična infrastruktura, javno-privatno partnerstvo, kibernetičke prijetnje, kibernetički prostor

ABSTRACT

Increasingly frequent use of digital services of public institutions, digitalization of public administration results in exposure to cyber threats. At the same time, protection against cyber threats requires skills, knowledge and experience to enable defense and security against these threats. Although certain public institutions provide cybersecurity services to public, state and academic institutions, they are definitely not always sufficient and there is a need to cooperate with the private sector, which also offers certain cybersecurity services and products. The practice of cooperation between the public and private sectors in the cyber sphere should be well defined so that there are no gaps that will have implications for national security. This paper offers answers to three research questions. The first question is: What are the trends of cyber threats and what types of threats are represented at the EU and Croatian levels? The second question is: What are the strategic and normative acts that define the cyber security system of critical infrastructure in the Republic of Croatia? The third question is: What conditions are needed and how are they defined in the case of concluding public-private partnerships in the cyber sphere in the Republic of Croatia? In answering these three research questions, several research methods such as systems theory, inductive and deductive methods are used. When answering the third research question, the method of interviewing individual private companies that offer services or products in the field of protection of critical infrastructure from cyber threats is also used. Finally, we want to test the initial hypothesis that public-private partnerships in cyberspace contribute to the quality of cyber security in the Republic of Croatia.

Keywords: national security, cybersecurity, information security, critical infrastructure, public-private partnership, cyber threat, cyberspace

Anketa

1. Broj zaposlenih:

2. Vaša tvrtka je malo, srednje ili veliko poduzeće:

3. Tvrtka se isključivo bavi pružanjem usluga i/ili proizvoda kibernetičke sigurnosti:

- Da
- Ne

4. Koje usluge i/ili proizvode kibernetičke sigurnosti pruža Vaša tvrtka:

5. U kojim područjima djeluju tvrtke iz privatnog sektora s kojima Vaša tvrtka surađuje na području kibernetičke sigurnosti:

6. Na kojim poslovima surađuje Vaša tvrtka i tvrtke partnera:

7. Na kojoj je razini znanje o kibernetičkim rizicima u tvrtkama s kojima surađujete:

- Nisko
- Dovoljno
- Dobro
- Vrlo dobro
- Odlično

8. Koje su najčešće vrste kibernetičkih rizika s kojima ste se susreli:

9. Provodi li se standard ISO 27001 po Vama na zadovoljavajućoj razini u sektorima s kojima surađujete:

- Ne provodi se uopće
- Provodi se ispod zadovoljavajuće razine
- Provodi se na zadovoljavajućoj razini

10. Koliko često Vaši partneri upravljaju i/ili nadgledaju neku vrstu kritične informacijske infrastrukture:

11. S obzirom na prethodno pitanje, koja je to vrsta kritične informacijske infrastrukture:

12. Surađuje li Vaša tvrtka s javnim sektorom:

- Uopće ne surađujemo
- Surađujemo rijetko (25% od ukupnog broja projekata)
- Surađujemo često (50% od ukupnog broja projekata)
- Surađujemo vrlo često (75% od ukupnog broja projekata)
- Surađujemo gotovo stalno (90% i više od ukupnog broja projekata)

13. Na kojim poslovima surađuje Vaša tvrtka i tvrtka iz javnog sektora:

14. Hoće li trend kibernetičkih rizika za javni sektor u RH po Vama rasti ili padati:

15. Na kojoj je razini znanje o kibernetičkim rizicima u javnom sektoru:

- Nisko
- Dovoljno
- Dobro
- Vrlo dobro
- Odlično

16. Koje su najčešće vrste kibernetičkih rizika u javnom sektoru s kojima ste se susreli:

17. Koji su po Vama izazovi za sklapanje javno privatnih partnerstava vezanih za kibernetičku sigurnost u RH:

18. Provodi li se standard ISO 27001 po Vama na zadovoljavajućoj razini u javnom sektoru:

- Ne provodi se uopće
- Provodi se ispod zadovoljavajuće razine
- Provodi se na zadovoljavajućoj razini