REPUBLIKA HRVATSKA
URED VIJEĆA ZA NACIONALNU SIGURNOST
NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini

Zagreb, 14. lipnja 2018.

SAŽETAK

Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini izradilo je Nacionalno vijeće za kibernetičku sigurnost za potrebe Koordinacije za sustav domovinske sigurnosti i na temelju prethodno izrađenog i povezanog dokumenta: Analiza potreba i sposobnosti kibernetičkog djelovanja na razini RH.

Kao primarne reference za izradu ovog dokumenta korišteni su Zakon o informacijskoj sigurnosti, Nacionalna strategija kibernetičke sigurnosti te budući Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kao i niz procesa i inicijativa povezanih s ovim aktima, koje su u proteklom razdoblju pokrenute u okviru procesa uređenja hrvatskog kibernetičkog prostora i uvođenja upravljanja kibernetičkom sigurnošću na nacionalnoj razini.

Ovakav pristup organizacijskom i ustrojbenom položaju tijela za kibernetičko djelovanje na nacionalnoj razini, rezultirao je uspješnim odgovorima na nacionalne i međunarodne izazove Republike Hrvatske u pitanjima kibernetičke sigurnosti, prvenstveno u smislu zahtjeva koje pred države članice postavljaju EU i NATO te se u tom smislu može smatrati prihvatljivim pristupom i za primjenu u najširem nacionalnom konceptu sustava domovinske sigurnosti, u kojem kibernetička sigurnost predstavlja jedan od niza elemenata ovog sustava. Dodatno je aktualni hrvatski pristup upravljanju kibernetičkom sigurnošću uspješno testiran i u slučaju globalnog kibernetičkog napada malicioznim ucjenjivačkim kripto kodom WannaCry u svibnju 2017. godine.

Sadržaj:

1. OPSEG I OKVIRI DOKUMENTA

1.1. SUDIONICI IZRADE DOKUMENTA

Predmetni dokument s opisom organizacijskog i ustrojbenog položaja tijela za kibernetičko djelovanje na nacionalnoj razini izrađuje se temeljem Godišnjeg plana rada Koordinacije za sustav domovinske sigurnosti za 2018. godinu, a vezano za odabrani specifični cilj 6. „Razvitak sposobnosti kibernetičkog djelovanja u okviru sustava domovinske sigurnosti“ i zadanu aktivnost „Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini“. Nositelj ove aktivnosti je Ured Vijeća za nacionalnu sigurnost (UVNS), u svojstvu predsjedatelja Nacionalnog vijeća za kibernetičku sigurnost, a u provedbi surađuju Sigurnosno-obavještajna agencija (SOA), Vojna sigurnosno-obavještajna agencija (VSOA), Zavod za sigurnost informacijskih sustava (ZSIS), Glavni stožer Oružanih snaga RH (GS OS RH) i nadležna tijela državne uprave.

Prijedlog teksta analize dostavljen je, na razmatranje, svim članovima Vijeća, a Vijeće je tekst analize usvojilo u lipnju 2018. godine. U ovaj proces bili su uključeni predstavnici svih 18 institucija uključenih u rad Vijeća te je na ovaj način zadovoljena obveza uključenja nadležnih tijela državne uprave u proces izrade organizacijskog i ustrojbenog položaja tijela za kibernetičko djelovanje na nacionalnoj razini. Time su ujedno u rad uključeni predstavnici svih relevantnih institucija za područje kibernetičke sigurnosti u RH.

Kako bi se zadovoljilo zahtjev Godišnjeg plana rada Koordinacije za domovinsku sigurnost, u smislu njime definiranih tijela koja surađuju u izradi predmetnog dokumenta (SOA, VSOA, ZSIS, GS OS RH), u okviru pripreme i usvajanja ovog teksta od strane Vijeća, Vijeće je zatražilo od članova i zamjenika članova Vijeća iz SOA-e, ZSIS-a i MORH-a, da se kroz unutarnji dogovor u tim institucijama povežu s odgovarajućim predstavnicima ovih institucija u Koordinaciji za domovinsku sigurnost, a vezano za provedbu ove aktivnosti.

1.2. KORIŠTENE REFERENCE

Kao primarne reference za izradu ovog dokumenta korišteni su Zakon o informacijskoj sigurnosti („Narodne novine“ broj: 79/07), Nacionalna strategija kibernetičke sigurnosti („Narodne novine“ broj: 108/15) te Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (lipanj 2018., Zakon u drugom čitanju u Hrvatskom Saboru, http://www.sabor.hr/prijedlog-zakona-o-kibernetickoj-sigurnosti-operat, a pripadna podzakonska Uredba Vlade je u procesu javnog e-savjetovanja na https://esavjetovanja.gov.hr/Econ/MainScreen?EntityId=7489), kao i niz povezanih Odluka Vlade o osnivanju nacionalnih međuresornih tijela za kibernetičku sigurnost („Narodne novine“ broj: 61/16i 28/18) te Rješenja o imenovanju predsjednika i članova Nacionalnog

vijeća za kibernetičku sigurnost.. Spomenuti i povezani materijali iz područja kibernetičke sigurnosti dostupni su javno na web poveznici UVNS-a http://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost, pod naslovom *Kibernetička sigurnost*.

1.3. METODOLOGIJA PRISTUPA

Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini analizira se i prikazuje na temelju više povezanih regulativnih okvira u RH, primarno onih koji su uređeni zakonima korištenim kao primarne reference ovog dokumenta. Dodatno se koriste i neki drugi povezani regulativni okviri u usko povezanim područjima kao što su javne elektroničke komunikacije ili kazneni postupak. Većina ostalih potrebnih sektorskih regulativnih okvira uvodi se kroz Zakon o informacijskoj sigurnosti za državni sektor te Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga za ostale gospodarske sektore povezane kibernetičkim prostorom.

Radi jasnije vizualizacije organizacijskog i ustrojbenog položaja tijela, razrada je napravljena prateći logički povezane nacionalne i sektorske funkcionalnosti važne iz kuta kibernetičke sigurnosti te dodatnim povezivanjem uloge pojedinih tijela preko korištenja kataloga sigurnosnih rizika kao dijela plana rada Koordinacije za sustav domovinske sigurnosti.

Daje se također i osvrt na stanje kibernetičkog prostora kao i kratki prikaz razvoja postojećih kapaciteta kibernetičke sigurnosti u RH realiziranih u posljednjih desetak godina.

2. KRATKI PREGLED DOSADAŠNJEG RAZVOJA KIBERNETIČKE SIGURNOSTI U REPUBLICI HRVATSKOJ

Temeljni koncepti suvremene sigurnosne politike Republike Hrvatske postavljeni su u Nacionalnom programu informacijske sigurnosti koji je donesen 2005. godine u okviru priprema za pristup NATO-u (https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-04-110.pdf). Nacionalni program pratile su zakonodavne promjene, među kojima je bilo i donošenje Zakona o informacijskoj sigurnosti. Već tada je u RH prepoznata potreba i propisane su osnovne sposobnosti koje se trebaju razviti u RH, kroz uspostavu Zavoda za sigurnost informacijskih sustava (https://www.zsis.hr/), sa zadaćama koje su, između ostalog, vezane za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u okviru državnog sektora te kroz uspostavu Nacionalnog CERT-a (https://www.cert.hr/) u okviru Hrvatske akademske i istraživačke mreže (CARNET), sa zadaćama vezanim za prevenciju i zaštitu od računalnih ugroza sigurnosti svih javnih informacijskih sustava u Republici Hrvatskoj. Upravo ove dvije institucije, deset godina nakon ustrojavanja njihovih temeljnih CERT-ovskih sposobnosti, u Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga predstavljaju CSIRT[1] tijela sa sličnim zadaćama prevencije i odgovora na ugroze sigurnosti informacijskih sustava. Ovim Zakonom provodi se i daljnje uređenje područja prevencije i zaštite od ugroza sigurnosti informacijskih sustava kroz usmjeravanje mjera zaštite na Zakonom utvrđene sektore ključnih usluga i davatelja digitalnih usluga kako ih propisuje EU[2] te na dodatni sektor ključnih usluga od interesa za RH[3]. Pri tome se provodi uravnoteženje obveza i odgovornosti korisnika informacijskih sustava s jedne strane te načina obavješćivanja i međusobne pomoći u rješavanju incidenata na sektorskoj, nacionalnoj i EU razini, s druge strane.

Sa spomenutim Zakonom povezan je i niz drugih inicijativa u RH, koje su mu prethodile u prijašnjim godinama, primjerice procjena ključnih ugroza u telekomunikacijskom sustavu RH provedena 2010. godine u koordinaciji UVNS-a, koja je rezultirala nizom mjera, od kojih je

[1] CSIRT je kratica za Computer Security Incident Response Team, odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u RH koristi i kratica istog značenja CERT (Computer Emergency Response Team).

[2] NIS direktiva utvrđuje obvezu država članica uvesti mjere za visoku razinu zaštite kibernetičke sigurnosti u sljedećim sektorima ključnih usluga: energetika – električna energija, nafta, plin; prijevoz – zračni, željeznički, vodni, cestovni; bankarstvo; infrastrukture financijskog tržišta; zdravstveni sektor; opskrba vodom za piće i njezina distribucija; digitalna infrastruktura – razmjena internetskog prometa, usluge naziva domena i kontrola vršne nacionalne domene. NIS direktiva također utvrđuje obavezu za davatelje digitalnih usluga na razini jedinstvenog digitalnog tržišta EU u području usluga: internetsko tržište, internetske tražilice i usluge računalstva u oblaku.

[3] RH u okviru Zakona uvodi dodatni sektor: poslovne usluge za državna tijela, koji se sastoji od dva podsektora: usluge u sustavu e–Građani, poslovne usluge za korisnike državnog proračuna.

jedna provedena u koordinaciji sa Sveučilišnim računskim centrom Sveučilišta u Zagrebu (Srce), s ciljem uspostavljanja organizacijskih i sigurnosnih mjera za direktnu i neposrednu razmjenu internetskog prometa između davatelja internetskih usluga u RH (Croatian Internet Exchange – CIX, http://www.srce.unizg.hr/croatian-internet-exchange-cix), a što danas predstavlja jedan od zahtjeva NIS direktive za sve države članice EU-a.

Primjer postignuća RH na razvoju sposobnosti u području kibernetičke sigurnosti u prošlom razdoblju predstavlja i suradnja Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM) i Nacionalnog CERT-a, provedena 2012. godine pod okriljem UVNS-a, koja je rezultirala izradom Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga[4] (Narodne novine, broj 109/12, 33/13, 126/13 i 67/16). Time su u RH uvedene obveze provedbe sigurnosnih mjera za operatore javnih komunikacijskih mreža u RH, u obliku minimalnih sigurnosnih mjera u skladu s međunarodnom normom ISO 27001, kao i koordinacija rješavanja sigurnosnih incidenata između operatora i Nacionalnog CERT-a. Važno je uočiti da za razliku od ovog primjera u kojem se primarno adresira kriterij raspoloživosti infrastrukture davatelja javnih komunikacijskih mreža u RH, spomenutim Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga se uvode širi zahtjevi i adresiraju se sva tri temeljna sigurnosna kriterija (povjerljivost, cjelovitost i raspoloživost), uključujući i svojstvo autentičnosti digitalnih vjerodajnica, za mrežne i informacijske sustave kojima se upravlja ključnim i digitalnim uslugama koje su u opsegu ovog Zakona.

Jedno od postignuća iz ovog prethodnog razdoblja RH predstavlja i sustav SRU@HR – Nacionalni sustav ranog upozoravanja na sigurnosne ugroze na Internetu, koji je u koordinaciji s UVNS-om uspostavio CARNET-ov Nacionalni CERT 2011. godine (https://www.cert.hr/sru/) i koji široj javnosti u RH danas omogućava uvid u stanje kibernetičkog prostora u RH i globalno.

NIS direktiva koja se u RH prenosi donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i njegovog podzakonskog akta, dio je široke aktualne digitalne inicijative EU–a, kojom se svijest o nužnosti razvoja digitalnog gospodarstva širi kroz niz segmenata suvremenog društva, počevši od procesa stvaranja jedinstvenog digitalnog tržišta EU–a, preko niza inicijativa za jačanje sigurnosne svijesti građanstva o kibernetičkom prostoru, do poticanja razvoja javno–privatnog partnerstva i elektroničkih usluga u državnoj upravi i gospodarstvu. Pri tome NIS direktiva stvara primjerene okvire prevencije i zaštite društva od kibernetičkih ugroza zajedničkim pristupom svih država članica koje osiguravaju usklađene vertikalne sektorske pristupe u nacionalnom okruženju, dok nova EU regulativa zaštite osobnih podataka (GDPR) sličan pristup osigurava

[4] Neslužbeni pročišćeni tekst: https://www.hakom.hr/UserDocsImages/2016/propisi/VL-KU-PR-INTS-Pravilnik%20o%20sigurnosti-neslu%C5%BEbeni%20pro%C4%8Di%C5%A1%C4%87eni%20tekst.pdf

horizontalnim funkcionalnim pristupom kroz sve segmente društva u cjelini. Potrebno je uočiti da se aktualna problematika zlouporabe osobnih podataka u kibernetičkom prostoru primarno adresira kroz GDPR regulativu, dok NIS direktiva primarno adresira problem sigurnosti infrastrukture koja služi za ključne i digitalne usluge društva i gospodarstva.

Sustavno povezivanje opisanog niza aktivnosti i inicijativa u RH, koje su provođene u razdoblju od 2005. do 2014. godine, provedeno je u okviru izrade Nacionalne strategije kibernetičke sigurnosti, koja je zajedno s detaljnim Akcijskim planom provedbe donesena 2015. godine. Pristup uveden u RH u Nacionalnoj strategiji kibernetičke sigurnosti, iako dovršen prije objave EU NIS direktive, u potpunosti je sukladan sa zahtjevima NIS direktive. Tako je Nacionalnom strategijom RH uvedeno i jedno od pet nacionalnih područja kibernetičke sigurnosti: kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama, koje u potpunosti pretpostavlja provedbu mjera iz predmetnog Zakona te će provedba Zakona u najvećoj mogućoj mjeri predstavljati i istovremenu provedbu mjera Nacionalne strategije kibernetičke sigurnosti RH u spomenutom području. Nadalje, kako bi se omogućilo učinkovito praćenje provedbe Nacionalne strategije kibernetičke sigurnosti, ali i osiguralo potrebnu međuresornu povezanost nadležnih institucija državnog i javnog sektora, 2016. godine uspostavljena su strateška i operativna međuresorna nacionalna tijela za upravljanje provedbom Nacionalne strategije kibernetičke sigurnosti i rješavanje svih bitnih nacionalnih pitanja u području kibernetičke sigurnosti - Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost.

Nacionalno vijeće za kibernetičku sigurnost[5] (u daljnjem tekstu: Vijeće) konstituirano je 16. ožujka 2017. godine, slijedom Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, koje je donijela Vlada Republike Hrvatske na sjednici održanoj 16. veljače 2017. godine. Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u Operativno-tehničkoj koordinaciji za kibernetičku sigurnost (u daljnjem tekstu: Koordinacija), koja 23. ožujka 2017. započinje sa svojim radom. Konstituiranjem Vijeća i Koordinacije otvoren je put za punu provedbu mjera Akcijskog plana i ostvarenje ciljeva Nacionalne strategije kibernetičke sigurnosti u RH.

Vijeće predstavlja strateško međuresorno tijelo sastavljeno od predstavnika 18 institucija s ciljem uspostave i upravljanja svim potrebnim horizontalnim inicijativama u području kibernetičke sigurnosti RH, kako u državnom sektoru, tako i međusektorski, odnosno u društvu u cjelini. Rad Vijeća koordinira UVNS. Koordinacija predstavlja međuresorno operativno tijelo sastavljeno od predstavnika 8 institucija s odgovarajućim operativnim nadležnostima i resursima, putem kojeg se žele učinkovitije koordinirati i provoditi potrebne

[5] http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf

aktivnosti prevencije i reakcije na ugroze kibernetičke sigurnosti, primarno u smislu komplementarnog pristupa u prevenciji i rješavanju sigurnosnih incidenata, a time i usklađenog razvoja nacionalnih sposobnosti u kibernetičkom prostoru. Rad Koordinacije koordinira Ministarstvo unutarnjih poslova (MUP), a usmjerava Vijeće.

UVNS na svojoj mrežnoj stranici redovito objavljuje godišnja izvješća o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti na kraju drugog kvartala tekuće godine za prošlu godinu[6], kao i Godišnja izvješća o radu Vijeća i Koordinacije[7].

[6] Izvješće o provedbi Akcijskog plana za 2016. godinu: http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvjesce%20o%20provedbi%20Akcijskog%20plana%20za%20provedbu%20NSKS%20u%202016.pdf

[7] http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

3. OSVRT NA AKTUALNO STANJE KIBERNETIČKOG PROSTORA

Godina 2017. u mnogim je elementima bila godina prekretnice u globalnom kibernetičkom prostoru. To se prvenstveno odražava na puno jasnije globalno prepoznavanje sve veće ovisnosti društva o novim tehnološkim konceptima od kojih su u 2017. godini u velikoj mjeri dominirale društvene mreže, računalstvo u oblaku i Internet stvari (Internet of Things - IoT). Svijest o tehnološkoj ovisnosti i prepoznavanje tehnoloških koncepata o kojima društvo postaje sve više ovisno, dovodi i do šire globalne svijesti o izloženosti suvremenog društva novim ugrozama koje neumitno prate sve tehnološke razvoje.

Brigu o utjecaju javnog mnijenja putem komunikacijskih kanala različitih globalno rasprostranjenih društvenih mreža vidimo kroz sve veću zabrinutost država za procese političkih izbora, inicirane posljednjim predsjedničkim izborima u SAD-u, što je nakon „zabrinutosti“ za nacionalne izborne procese, primjerice u Njemačkoj ili Nizozemskoj, danas već poprimilo prve oblike formalnih postupaka o kojima i EU razmišlja približavajući se idućim izborima za EU parlament[8].

Problem novih globalnih kanala utjecaja koji se stvara paralelno s tradicionalnim javnim medijima postaje sve više predmet formalnih procesa sigurnosne politike u smislu prepoznavanja, prevencije i suzbijanja tzv. ***hibridnih prijetnji***. Unatoč javno prisutnom jednostavnom shvaćanju hibridnog kao sučeljavanja fizičkog i kibernetičkog prostora, hibridne prijetnje se moraju tretirati bitno sustavnije[9] kako bi se shvatili njihovi stvarni uzroci i dosezi, koji su puno dublji od odabranog korištenja nekog od vektora napada. Iako vektori napada danas u mnogo slučajeva predstavljaju kibernetičke napade, poput hakiranja računa e-pošte nekog političkog dužnosnika[10], ili *NonPetya*[11] malicioznog napada, oni u slučajevima

[8] http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614650/EPRS_IDA(2018)614650_EN.pdf

[9] Hibridne prijetnje u svojoj osnovi predstavljaju način utjecaja na elemente državne organizacije te je u većini slučajeva (SAD, EU) zastupljen tzv. DIMEFIL način praćenja domena hibridnih prijetnji (DIMEFIL = Diplomacy, Information, Military, Economy, Financial, Intelligence, Law Enforcement/Legal). Ovisno o metodi pristupa koriste se različiti indikatori intenziteta i međusobnog utjecaja, odnosno zahvaćenosti više domena od interesa.

[10] https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html?rref=collection%2Fnewseventcollection%2FRussian%20Hacking%20in%20the%20U.S.%20Election

[11] Za razliku od malicioznog koda *Petya* koji je ucjenjivački kripto kod, *NonPetya* je na prvi pogled sličan ucjenjivačkom kripto kodu, ali za koji se ustanovilo da ne omogućava napadnutom korisniku dekriptiranje podataka, odnosno, otkup ključa. Stoga cilj *NonPetya* napada nije zaraditi nego uništiti podatke na računalu koje je napao, iako je temeljena na istoj ranjivosti koja je korištena i u *Petya* i u *WannCry* napadima. U ovom slučaju je Velika Britanija izašla s prvom formalnom atribucijom napada na Rusiju i vojno-obavještajne organizacije, koristeći upravo popratna svojstva samog tehničkog vektora napada i prepoznavši tako hibridni napad na sustave kritične infrastrukture u Ukrajini koji se zbog korištenja neselektivne ranjivosti proširio globalno kao i drugi spomenuti napadi (https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks)

hibridnih prijetnji predstavljaju samo način ostvarenja viših ciljeva puno ozbiljnijeg napadača, koji u nekim slučajevima samo koristi „usluge“ hakerskih grupa ili pojedinaca.

Računalstvo u oblaku na prijelazu godine ulazi sve više i na velika vrata u prihvatljive koncepte tehnološke platforme te se i međunarodne organizacije poput NATO-a i EU-a, ali i sve zemlje članice, koje su do sada već uvele procese koji se, u većoj ili manjoj mjeri, oslanjaju na ovaj tehnološki koncept. Računalstvo u oblaku ušlo je u na mala vrata u EU[12] znatno prije aktualne EU GDPR[13] regulative, no u skladu s konceptima koje će u 2018. primijeniti sve zemlje obveznice GDPR-a. Rješenja za državni sektor su također u pripremi u mnogim zemljama[14], a međunarodne organizacije poput MISWG-a[15] pripremaju rješenja koja bi u određenim uvjetima mogla biti prihvatljiva i za problematiku vezanu za sigurnost poslovne suradnje i klasificirane ugovore. Republika Hrvatska prepoznala je ovaj problem koji je obuhvaćen Zakonom o državnoj informacijskoj infrastrukturi i pratećoj Uredbi Vlade RH o sigurnosnim i tehničkim standardima za spajanje na državnu informacijsku infrastrukturu. Sličan tehnološki prodor korištenja[16] prisutan je u području **Interneta stvari (IoT)**, počevši od automatizacije kuća i stanova, preko niza industrijskih grana.

Svi ovi tehnološki i društveni procesi imaju i svoju ***gospodarsku dimenziju*** koja je vidljiva u pristupu Europske komisije digitalnom gospodarstvu. Jedinstveno EU digitalno tržište je na najvišem mjestu prioriteta političke agende EU-a i rezultira nizom povezanih aktivnosti koje imaju za cilj osiguravanje razvoja i održivosti digitalnog gospodarstva. Digitalna transformacija organizacija i državne uprave, revizija koncepta obrazovanja i šira svijest o potrebi cjeloživotnog obrazovanja samo su neki od sustavnih aktivnosti koje EU i zemlje članice provode. Kibernetička sigurnost u ovakvom pristupu mora biti duboko ugrađena u sve segmente društva, državne uprave i ekonomije i u tom smislu je koncipirana i hrvatska strategija kibernetičke sigurnosti kao i rad Vijeća u njegovoj prvoj godini postojanja.

Sve veća izloženost informacijskih tehnologija zlonamjernim aktivnostima raznih interesnih skupina ili pojedinaca pokazuje kako je sustavan i koordiniran angažman država u podizanju svojih sposobnosti u području kibernetičke sigurnosti ključan za izgradnju sigurnog društva u kibernetičkom prostoru. U doba izrade hrvatske strategije kibernetičke sigurnosti odvijalo se niz kampanja s masovnim slanjem maliciozne e-pošte (phishing), koja je tekstualno prilagođenim sadržajem masovno dostavljana hrvatskim korisnicima e-pošte. U to vrijeme Hrvatsku je pogodio i veliki ciljani kibernetički napad na pravne osobe, korisnike usluga e-bankarstva te smo bili suočeni i s tzv. naprednim ustrajnim prijetnjama (APT), kojima je cilj

[12] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[13] http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr
[14] https://ukcloud.com/wp-content/uploads/2017/05/Whitepaper-Bringing-clarity-to-the-cloud1.pdf
[15] Multinational Industrial Security Working Group - MISWG
[16] https://www.forbes.com/sites/louiscolumbus/2017/11/12/2017-internet-of-things-iot-intelligence-update/#3194a9ce7f31

bio uspostaviti vanjsku kontrolu i upravljanje korisničkim računalima u svrhu krađe novca s računa korisnika e-bankarstva. Sličan, ali još sofisticiraniji način napada špijunskim malicioznim kodom pogodio je tijekom prošlih nekoliko godina niz državnih institucija u više zemalja članica EU-a, napose ministarstva vanjskih poslova koji su koncentratori političkih informacija i poželjna meta za ovakve napade aktera sponzoriranih politikama nekih država. Napad ove vrste rješavan je prošle godine i u MVEP RH.

Hrvatska nije bila ciljem velikih napada na kritičnu infrastrukturu za razliku od brojnih drugih država, uključujući i članice EU, ali takav napad u bliskoj budućnosti se ne može isključiti. Niz napada u Ukrajini (uključujući spomenuti *NonPetya* maliciozni kod), koji je u prošloj godini pogodio energetske objekte, državne institucije i tvrtke, još jednom je pokazao visoku ovisnost država o informacijskoj tehnologiji te razornu moć ovakvih hibridnih napada, koji napadom na informacijske resurse onemogućavaju rad određene vitalne infrastrukture društva i paraliziraju cijele društvene sektore.

Zamjetan je stalni porast broja kaznenih dijela u EU, a i u RH, u području kibernetičkog kriminaliteta, posebno u dijelu računalnih prijevara. U europskim državama broj kaznenih dijela iz područja kibernetičkog kriminaliteta doseže i do 20% u ukupnom broju kaznenih dijela i može se očekivati da će u budućnosti to biti dominantno područje kriminaliteta. Kriminal prati gospodarski rast digitalne ekonomije. Poučene ovakvim iskustvom, mnoge europske države kibernetičku sigurnost postavljaju kao prioritetno područje nacionalne sigurnosti.

Posljednji globalni kibernetički napad ucjenjivačkim malicioznim kodom u okviru kampanje ***WannaCry*** u svibnju 2017. godine, pokazao je visok stupanj ovisnosti niza industrijskih sektora o suvremenoj informacijskoj tehnologiji, a osobito je pokazao moguće devastirajuće posljedice na primjeru zdravstvenog sektora Velike Britanije. Upravo u ovom globalnom napadu hrvatska međuresorna tijela, Vijeće i Koordinacija, iako tek konstituirana, uspješno su reagirala i uspostavila pravovremenu i učinkovitu koordinaciju i kriznu komunikaciju na najširoj horizontalnoj razini hrvatskog društva i svih njegovih sektora, osiguravajući time i minimalnu štetu po hrvatsko društvo u cjelini.

Kibernetički napadi doveli su do značajne promjene u percepciji važnosti kibernetičkog prostora za suvremeno društvo, a slijedno tome i do promjene pristupa kibernetičkoj sigurnosti, kako na razini međunarodnih organizacija tako i na razini država članica. NATO 2016. godine uvodi kibernetički prostor kao novu dimenziju vojnog djelovanja, uz tradicionalna područja kopna, zraka i mora, odnosno svemira. EU 2016. godine, na temelju strategije iz 2013. godine, donosi NIS Direktivu.

Vlada RH u ovom razdoblju donosi Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu, Odluku o osnivanju međuresornih tijela za upravljanje provedbom

Strategije[17] te početkom 2017. godine osigurava i puno pokretanje rada već spomenutih međuresornih upravljačkih tijela - Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost. Tijekom 2017. pokrenuta je i nacionalna transpozicija NIS direktive. Sve ovo preduvjet je uspješnog razvoja hrvatskog društva i konkurentnosti na jedinstvenom digitalnom tržištu EU.

3.1. GLOBALNI KIBERNETIČKI NAPAD *WANNACRY* U SVIBNJU 2017. GODINE

Sredinom svibnja 2017., zloćudni ucjenjivački kripto kod *WannaCry*, koristeći ranjivost *Windows* operativnih sustava, napao je računala širom svijeta uključujući i Republiku Hrvatsku.

S obzirom na potencijalnu opasnost za hrvatski kibernetički prostor, 13. svibnja 2017. žurno se sastala Koordinacija te su dogovorene aktivnosti za prevladavanje ove ugroze. Vijeće i predsjednik Vijeća uključili su se u rad Koordinacije, osobito u aspekte analize štete i naučenih lekcija na nacionalnoj razini, kao i u poslove obavještavanja javnosti te davanja relevantnih informacija u cilju smanjivanja štete na nacionalnoj razini i smanjivanja mogućnosti za stvaranje panike u javnosti. Javni nastupi predsjednika Vijeća koordinirani s Uredom Vlade za odnose s javnošću.

Koordinirane informacije i preporuke za korisnike objavljene su na web stranici MUP-a[18], kao i na web stranicama ZSIS-a i Nacionalnog CERT-a. Najširа javnost je informirana putem medijskih kuća, a sektorska tijela su informirala i organizacije u svojim sektorima. Istovremeno, sva raspoloživa stručna tijela su poduzimala aktivnosti na detektiranju zaraženih računala i blokadi prometa s kompromitiranih uređaja. Vijeće je zatražilo od Koordinacije dodatnu precizniju analizu kako bi se utvrdila točnija procjena štete, naučene lekcije i pripremilo odgovarajuće tematsko priopćenje za javnost.

Mjesec dana nakon napada zaključeno je kako WannaCry nije nanio znatniju štetu u Hrvatskoj. Prema dostupnim podacima, ukupno je bilo zaraženo 205 računala. U nekim slučajevima je bilo potrebno ponoviti instalaciju računala, ali u većini slučajeva je zaraza uklonjena i bez toga.

Potpunu sigurnost na Internetu nije moguće postići. Nove ranjivosti operacijskih sustava i aplikacija će se i dalje otkrivati, a bit će i onih koji će te ranjivosti željeti zlouporabiti radi financijske ili neke druge koristi. Državna tijela provode u međuresornoj usklađenoj koordinaciji sve što je u njihovoj nadležnosti kako bi se zaštitio kibernetički prostor RH, međutim, potrebna je i budnost krajnjih korisnika u svim društvenim sektorima. Korisnici bi

[17] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016)
[18] https://www.mup.hr/novosti/628/wcry-ransomware-kampanja

trebali voditi računa da njihova računala imaju posljednje verzije programskih zakrpa, da imaju instalirane i omogućene odgovarajuće sigurnosne alate te da se ponašaju odgovorno u korištenju društvenih mreža i drugih oblika elektroničke komunikacije[19].

Zaključak je da su i Vijeće i Koordinacija, iako su u doba *WannaCry* napada tek osnovani, već u ovoj prvoj globalnoj kibernetičkoj prijetnji pokazali nužnost i potrebu horizontalnog međuresornog i međusektorskog pristupa, ali i dokazali učinkovitost i uspješnost po svim aspektima djelovanja na sigurnosni incident, od uzbunjivanja, međusobnog izvještavanja, distribucije uputa i najboljih praksi postupanja u rješavanju incidenta, pa sve do učinkovite komunikacije s javnosti, kojom se ubrzalo provedbu zaštite i spriječila panika.

Vezano za javna priopćenja, Vijeće je na temelju ovog iskustva zaključilo kako će pojedina tijela koja participiraju u radu Vijeća i dalje izvještavati javnost o aktivnostima iz svoje nadležnosti, dok će Vijeće odlučiti o slučajevima kada će se javnost upoznati o pojedinim tematskim aktivnostima Vijeća. U tom smislu su na web mjestu UVNS-a tijekom godine odabrane tematske objave Vijeća o odluci Vijeća o uspostavi stručne radne skupine Vijeća za provedbu obveza RH u području EU NIS direktive, o zaključnom izvješću Koordinacije o malicioznoj kampanji *WannaCry*, prihvaćanju Izvješća o osnivanju Vijeća i Koordinacije na Vladi te Izvješća o provedbi Akcijskog plana za 2016. godinu.

Temeljem iskustava Vijeća i Koordinacije iz svibnja 2017., tijekom maliciozne kampanje WannaCry, razmotrena je problematika komunikacije Vijeća s javnošću vezano za kibernetičke krize. Zaključeno je kako je web mjesto MUP-a bilo najvažnije za komunikaciju s najširom javnošću te da postoje dobre predispozicije za komunikaciju s javnosti i u CARNET-u, odnosno Nacionalnom CERT-u i njihovom web mjestu, ali usmjereno užem krugu stručne javnosti. Stoga je odlučeno kako je u tom smislu najprimjerenije kriznu komunikaciju s javnošću provoditi putem MUP-a, koji vodi Koordinacija putem koje ima dostup do svih potrebnih operativnih informacija tijekom potencijalne kibernetičke krize. Pri tome bi voditelj/zamjenik koordinatora iz MUP-a, odnosno član i zamjenik člana Vijeća iz MUP-a trebali na odgovarajući način koordinirati i planirati krizno komuniciranje s predsjednikom i predstavnicima Vijeća, kao što je to u slučaju iz svibnja 2017. godine i bilo napravljeno.

3.1.1. DETALJNIJI PRIKAZ PODUZETIH AKTIVNOSTI U RH U GLOBALNOM KIBERNETIČKOM NAPADU WANNACRY

Globalna kampanja malicioznog koda *WannaCry* prve je velike štete nanijela u sustavu zdravstva Velike Britanije, a izvješća o štetama u svijetu počela su se objavljivati u petak 12. svibnja 2017. Maliciozni kod bio je usmjeren na Windows računalne platforme i koristio je

[19] https://www.sigurnostnainternetu.hr/

ranjivosti prisutne u različitim verzijama ovog operativnog sustava, što je osobito problematično bilo u slučajevima ranijih verzija Windows operativnog sustava, koje je Microsoft već prije stavio na popis proizvoda s ograničenim modalitetima održavanja (npr. Windows XP). Dodatni utjecaj na brzo širenje predstavljao je vektor napada koji je koristio internu ranjivost operativnog sustava za autonomno širenje malicioznog koda bez potrebe ikakve interakcije s korisnikom računala (računalni crv). Korisnici Windows 10 operativnog sustava nisu bili izloženi napadu zbog ranije provedene automatske sigurnosne zakrpe Microsofta, ali su neke od prethodnih verzija Windowsa, koje su izvan programa održavanja Microsofta, dobile mogućnost korištenja sigurnosne zakrpe tek na dan masovnog širenja malicioznog koda.

Na inicijativu ZSIS-a, Koordinacija je već na prvi dan masovnog širenja malicioznog koda započela s radom, što je u prvom redu obuhvatilo objavu javnih upozorenja i načina zaštite od malicioznog koda putem sigurnosnih zakrpa koje je distribuirao Microsoft, zatim dodatnim obavještavanjem sektorskih tijela i administratora računalnih sustava u tijelima u državnom sektoru, telekomunikacijskom sektoru, sektoru bankarstva itd. Objave upozorenja i upute za sprječavanje širenja malicioznog koda odgovarajućim sigurnosnim zakrpama, objavljene su u razdoblju između 12. i 14. svibnja 2017. Objave su davane na nizu web stranica različitih tijela koja sudjeluju u radu Koordinacije, a objave na stranicama MUP-a pokazale su se najučinkovitije i najposjećenije za široki krug korisnika u ovakvim slučajevima globalnog i neselektivnog kibernetičkog napada koji je usmjeren na sve instalacije Windows operativnog sustava, od državnog sektora, preko gospodarstva, do građanstva u cjelini. Microsoft Hrvatska je vrlo brzo reagirao i također dostavio promptne upute za daljnje prosljeđivanje svim korisnicima, za što su korištene adrese kontakt osoba u Vijeću, Koordinaciji, UVNS-u, ZSIS-u, HNB-u, HAKOM-u i drugim institucijama uključenim u rad Vijeća i Koordinacije.

Na sastanku Koordinacije održanom 13. svibnja 2017., na kojem je sudjelovao i predsjednik Vijeća, donesen je zaključak o potrebi koordiniranih istupa prema javnosti u RH, zbog alarmantnih vijesti koje stižu iz svijeta i mogućnosti nastanka panike u domaćoj javnosti. Stoga su sve objave na mrežnim stranicama tijela s predstavnicima u Koordinaciji koordinirano prenijela upozorenja i upute o postupanju, a dogovorene su osnovne naznake za usmene javne istupe predstavnika iz pojedinih tijela koja su preko vikenda dobivala upite hrvatskih medija. Posredstvom Ureda Vlade RH za odnose s javnošću, predsjednik Vijeća odgovorio je na pitanja redakcija televizijskih kuća HRT i Nova TV, u okviru večernjeg dnevnika u subotu 13. svibnja 2017. godine, što je dalje preneseno i putem mrežnih internetskih portala. Procjene koje su napravljene tijekom vikenda s 13. na 14. svibnja 2017. godine, pokazale su se dobrima, jer je šteta maliciozne kampanje *WannaCry* u RH bila minimalna i nije ugrozila nacionalnu sigurnost, čime se ujedno dobila i potvrda učinkovitosti i opravdanosti novog modela međuresorne organizacije i koordinacije rada tijela za kibernetičku sigurnost u Hrvatskoj, odnosno Vijeća i Koordinacije.

4. ORGANIZACIJSKI I USTROJBENI POLOŽAJ TIJELA ZA KIBERNETIČKO DJELOVANJE NA NACIONALNOJ RAZINI

4.1. UVOD

Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini nužno prati stanje i problematiku suvremenog kibernetičkog prostora i sveobuhvatno se obrađuje u nacionalnim strategijama koje se bave područjem kibernetičke sigurnosti. Zbog sve veće tehnološke ovisnosti svih segmenata društva i sve veće izloženosti različitih informacija u javnom Internet prostoru, značaj kibernetičkog prostora za suvremeno društvo postaje sve veći. Stoga su i inicijative povezane s kibernetičkom sigurnošću sve brojnije i sve šire usmjerene na društvene i gospodarske sektore suvremenog društva, a ne samo na državni, odnosno javni sektor.

Na Slici 1. prikazani su ključni procesi bitni za kibernetičku sigurnost. S jedne strane to su mjere i standardi informacijske sigurnosti primijenjeni u različitim sektorima društva, a s druge strane to je problematika kritične komunikacijske i informacijske infrastrukture koja prožima čitav niz gospodarskih i društvenih sektora. Pored toga, potrebno je uočiti važnost skupina zakonom zaštićenih podataka (klasificirani, neklasificirani, osobni, intelektualno vlasništvo) koji u današnje vrijeme predstavljaju ne samo vertikalnu sektorsku problematiku, primjerice državnog sektora u slučaju klasificiranih i neklasificiranih podataka, već i horizontalnu problematiku društva u cjelini u slučaju osobnih podataka ili intelektualnog vlasništva. Posvemašnja globalizacija i međusobna komunikacija u globalnom kibernetičkom prostoru upućuje na nužnost odgovarajućeg tretiranja zaštićenih skupina podataka u svim sektorima društva.

Važnu specifičnost kibernetičkog prostora čine i tzv. osjetljivi podaci koji mogu nastajati u kibernetičkom prostoru (npr. osobni podaci o sklonostima potrošača nastali korištenje Internet usluga), ili se mogu kumulirati u svrhu ostvarivanja e-usluga (npr. indeksni registri matičnog broja građana kao preduvjet pristupu uslugama elektroničke uprave), pri čemu takvi osjetljivi podaci mogu predstavljati društvene ranjivosti velikih razmjera, kako je to pojašnjeno na primjerima u poglavlju 3. s osvrtom na stanje kibernetičkog prostora. Upravo stoga, sveukupna digitalna higijena društva u cjelini nema alternativu u daljnjem razvoju suvremenog društva.

Na Slici 1. naznačena je i povezanost kibernetičkog prostora s puno širim konceptom kritične nacionalne infrastrukture, pri čemu se problematika kibernetičke sigurnosti razrađuje u okviru užeg koncepta kritične komunikacijske i informacijske infrastrukture, odnosno pristupa

sektorima ključnih i digitalnih usluga kako će to u Hrvatskoj biti utvrđeno Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.

Slika 1. – *Povezanost kibernetičkog prostora i kritične nacionalne infrastrukture te najvažniji elementi kibernetičke sigurnosti koji su u fokusu Nacionalne strategije kibernetičke sigurnosti i rada Nacionalnog vijeća za kibernetičku sigurnost*

Na sličan način kako je komunikacijska i informacijska kritična infrastruktura podskup šireg koncepta nacionalne kritične infrastrukture, jednako tako je i koncept kibernetičkog kriznog upravljanja i komuniciranja u slučajevima kibernetičkih napada većih razmjera, podskup nacionalnog kriznog upravljanja.

Svi opisani elementi predstavljaju sadržaj Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za njenu provedbu, a za praćenje provedbe zaduženo je međuresorno tijelo - Nacionalno vijeće za kibernetičku sigurnost, sastavljeno od predstavnika 18 institucija s odgovarajućim nadležnostima, odnosno organizacijskim i ustrojbenim položajem.

4.2. Pregled po sektorima – prevencija i zaštita mrežnih i informacijskih sustava od ugroza sigurnosti

4.2.1. Sektor politike informacijske sigurnosti u državnim tijelima

Područje kibernetičke sigurnosti po prvi puta je zakonski regulirano u domeni potreba državnog sektora u sklopu propisivanja suvremene nacionalne sigurnosne politike Zakonom o informacijskoj sigurnosti 2007. godine. Na temelju uvođenja i reguliranja područja neklasificiranih podataka, kao podataka koji mogu biti označeni s ciljem ograničenja korištenja samo u službene svrhe, započeto je reguliranje pripadnih mjera i standarda koje su se referirale na zahtjeve zaštite osobnih podataka i međunarodnu normu ISO 27001. UVNS je

temeljem ovoga Zakona postao NSA tijelo (National Security Authority), zaduženo za usklađivanje nacionalnih, EU i NATO mjera i standarda za zaštitu klasificiranih i neklasificiranih podataka državnog sektora. Sustav mjera i standarda informacijske sigurnosti predviđen je za klasificirane i neklasificirane podatke i obvezujući je za sve korisnike takvih podataka, a kontrolira se nadzorima UVNS-a, odnosno certifikacijskim i akreditacijskim postupcima koje obavljaju UVNS i ZSIS.

Slijedno tome je utvrđena potreba te su istim Zakonom propisane i ostale temeljne sposobnosti koje se trebaju razviti u RH - Zavodu za sigurnost informacijskih sustava (https://www.zsis.hr/) dodijeljene su zadaće koje su, između ostalog, vezane za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u okviru državnog sektora te je uspostavljen Nacionalni CERT (https://www.cert.hr/), u okviru Hrvatske akademske i istraživačke mreže (CARNET), sa zadaćama vezanim za prevenciju i zaštitu od računalnih ugroza sigurnosti svih javnih informacijskih sustava u Republici Hrvatskoj.

Spomenute institucije, UVNS, ZSIS i Nacionalni CERT, 2018. godine, kroz Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga dobivaju dodatne nacionalne funkcionalnosti. UVNS postaje jedinstvena nacionalna kontaktna točka (Single Point of Contact – SPOC), a ZSIS i Nacionalni CERT postaju nacionalna CSIRT[20] tijela sa sličnim zadaćama prevencije i odgovora na ugroze sigurnosti informacijskih sustava. Ovim Zakonom provodi se daljnje uređenje područja prevencije i zaštite od ugroza sigurnosti mrežnih i informacijskih sustava kroz usmjeravanje mjera na Zakonom utvrđene sektore ključnih usluga i davatelja digitalnih usluga kako ih propisuje EU[21] te na dodatni sektor ključnih usluga od interesa za RH[22]. Pri tome se provodi uravnoteženje obveza i odgovornosti korisnika informacijskih sustava s jedne strane i načina obavješćivanja i međusobne pomoći u rješavanju incidenata na sektorskoj, nacionalnoj i EU razini, s druge strane.

Na ovaj način je, nakon pristupa u Zakonu o informacijskoj sigurnosti koji je primarno rješavao problematiku informacijske sigurnosti državnog sektora i uspostavio osnove prevencije računalne sigurnosti u javnom Internet prostoru, napravljen prikladni iskorak i

[20] CSIRT je kratica za Computer Security Incident Response Team, odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u RH koristi i kratica istog značenja CERT (Computer Emergency Response Team).

[21] NIS direktiva utvrđuje obvezu država članica uvesti mjere za visoku razinu zaštite kibernetičke sigurnosti u sljedećim sektorima ključnih usluga: energetika – električna energija, nafta, plin; prijevoz – zračni, željeznički, vodni, cestovni; bankarstvo; infrastrukture financijskog tržišta; zdravstveni sektor; opskrba vodom za piće i njezina distribucija; digitalna infrastruktura – razmjena internetskog prometa, usluge naziva domena i kontrola vršne nacionalne domene. NIS direktiva također utvrđuje obavezu za davatelje digitalnih usluga na razini jedinstvenog digitalnog tržišta EU u području usluga: internetsko tržište, internetske tražilice i usluge računalstva u oblaku.

[22] RH u okviru Zakona uvodi dodatno sektor: poslovne usluge za tijela, koji se sastoji od dva podsektora: usluge u sustavu e–Građani, poslovne usluge za korisnike državnog proračuna.

proširenje uloge državnih institucija u Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, prema puno širim ciljevima društvenih i gospodarskih sektora društva u cjelini.

Iznimno važan segment rada državne uprave predstavlja međunarodna suradnja koja danas u svijetu sve više uključuje i kibernetičke aspekte, što se prati i razvija osobito u koordinaciji s MVEP-om.

4.2.2. SEKTOR SIGURNOSNO-OBAVJEŠTAJNOG DJELOVANJA

Područje sigurnosno-obavještajnog djelovanja definirano je Zakonom o sigurnosno-obavještajnom sustavu (ZSOS). Aktivnosti sigurnosno-obavještajnih agencija obuhvaćaju sigurnosno, obavještajno i operativno djelovanje u kibernetičkom prostoru.

Temeljem ZSOS-a, djelovanje SOA-e u području kibernetičke sigurnosti usmjereno je na sprječavanje:

- neovlaštenog ulaska u zaštićene informacijske i komunikacijske sustave državnih tijela,
- odavanja klasificiranih podataka od čelnika i zaposlenika državnih tijela, znanstvenih institucija i pravnih osoba s javnih ovlastima,
- drugih aktivnosti usmjerenih na ugrožavanje nacionalne sigurnosti.

U državno sponzoriranim kibernetičkim napadima koriste se napredni maliciozni alati, koji napadaču omogućavaju visoku razinu prikrivenosti u dužem vremenskom razdoblju, te imaju za cilj prikupiti podatke ili na neki drugi način direktno ili indirektno ugroziti nacionalnu sigurnost. U slučaju prikupljanja podataka cilj su podaci o hrvatskim sigurnosnim, političkim, diplomatskim, gospodarskim i drugim procesima te podaci i dokumenti euroatlantskih asocijacija kojih je Republika Hrvatska članica.

Tijekom 2016. godine detektirano je više od 7 kibernetičkih napada te vrste na zaštićene informacijske i komunikacijske sustave državnih tijela Republike Hrvatske, što je i objavljeno u Javnom izvješću SOA-e za 2017. godinu[23].

Sukladno tome, sigurnosno-obavještajne agencije aktivno sudjeluju u otkrivanju, suzbijanju i sprječavanju državno sponzoriranih kibernetičkih napada.

Zbog međusobne povezanosti i ovisnosti informacijskih i komunikacijskih sustava i globalno raširene Internet mreže, kibernetički prostor nema klasičnih granica, a pokretanje novog napada, odnosno odabir novog cilja moguće je napraviti u vrlo kratkom vremenskom roku. Sigurnosno-obavještajne agencije aktivno surađuju s međunarodnim partnerima, što je ključno za uspješan odgovor na izazove u području kibernetičke sigurnosti te prepoznavanje RH kao pouzdanog i kvalitetnog međunarodnog partnera.

[23] https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/

4.2.3. SEKTOR OBRAMBENOG PLANIRANJA

Ključno tijelo u području obrambenog planiranja je Ministarstvo obrane koje je zaduženo za poslove kibernetičke obrane kao dijela obrambenog planiranja i koje je također ustrojilo resurs CERT-a MORH-a. Područje kibernetičke obrane predstavlja dio strategije obrane i ono je predmet zasebne obrade i rješavanja, pri čemu se koriste svi potrebni elementi i resursi koji proizlaze iz Nacionalne strategije kibernetičke sigurnosti.

Najvažniji element predstavlja transformacija obrambenog planiranja koju su prihvatile sve države članice NATO-a u okviru NATO sastanka na vrhu u Varšavi u srpnju 2016. godine, a kojom se kibernetički prostor uvodi kao nova domena ratovanja NATO-a i svih država članica NATO-a, uz tradicionalne domene kopna, mora, zraka i svemira. U narednim godinama obrambeni sektori NATO država članica trebaju isplanirati ovu transformaciju.

Važan proces predstavlja i NATO procjena kibernetičke obrane, kojom NATO procjenjuje zrelost nacionalnih strategija kibernetičke sigurnosti, kao i sposobnosti koje se razvijaju u okviru obrambenog sektora i povezanih nacionalnih resursa država članica. Ovaj proces je tijekom 2017. i 2018. godine, u velikoj mjeri u Hrvatskoj usklađen s ciljevima Nacionalne strategije kibernetičke sigurnosti i mjerama Akcijskog plana za provedbu Strategije. MORH u svojstvu nadležnog tijela provodi redovitu godišnju procjenu i usklađuje mjere za razvoj potrebnih područja s dionicima nacionalnog Akcijskog plana i tijelima koja imaju predstavnike u Nacionalnom vijeću za kibernetičku sigurnost, koristeći Vijeće kao platformu za horizontalnu koordinaciju svih nacionalnih dionika ovog opsežnog programa.

S obzirom na važnu ulogu MORH-a u Sustavu domovinske sigurnosti, MORH ima istaknutu ulogu i u planiranju i pripremanju različitih vrsta nacionalnih i međunarodnih vježbi, kao što su vježbe u području kriznog upravljanja te strateške i taktičke vježbe iz područja kibernetičke sigurnosti.

4.2.4. SEKTOR ISTRAŽNOG I KAZNENOG POSTUPANJA

Ključna tijela u segmentu istražnog i kaznenog postupanja predstavljaju Ministarstvo unutarnjih poslova (MUP) i Državno odvjetništvo (DORH), kao provedbena tijela, odnosno Ministarstvo pravosuđa (MP) kao nadležno tijelo za planiranje sektorskog zakonodavstva, u dijelu kibernetičkog kriminaliteta koji je od interesa za predmetnu analizu. MP i MUP sudjeluju u radu Vijeća, a MUP dodatno koordinira rad Koordinacije te je ovlašten i za krizno komuniciranje u slučajevima nacionalnih kibernetičkih kriza.

Za tehničku provedbu implementacije zakonskih rješenja potrebnih u istražnim postupcima OTC permanentno provodi razvoj, nadogradnju i održavanje funkcionalnih sposobnosti

sustava pribavljanja podataka od pravnih i fizičkih osoba koji su registrirani u RH za pružanje telekomunikacijskih usluga.

Postoji dugogodišnja suradnja između MUP-a i Nacionalnog CERT-a u segmentu obuke i pomoći u istražnim i forenzičkim postupcima, koja se razvija od samih početaka rada Nacionalnog CERT-a te danas uključuje i suradnju sa ZSIS-om. Također, kroz nadzor informacijske sigurnosti UVNS-a u MUP-u, već niz godina se potiče i uspješno razvija sve bolja unutarnja organizacija MUP-a u povezanom segmentu visokotehnološkog kriminaliteta i forenzičkih sposobnosti. Postoji također uspješna suradnja između UVNS-a i DORH-a u segmentu informacijske sigurnosti, koja se dodatno kroz Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti tijekom 2018. godine operacionalizira kroz novi program Pravosudne akademije za stručnu izobrazbu u segmentu kibernetičke sigurnosti.

4.2.5. SEKTOR JAVNIH ELEKTRONIČKIH KOMUNIKACIJA

Kako je napomenuto u pregledu dosadašnjeg razvoja, postoji već niz godina uspostavljena suradnja između nadležnog Ministarstva mora, prometa i infrastrukture (MMPI) kao središnjeg sektorskog tijela, Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM) kao sektorskog regulatora, odnosno UVNS-a kao središnjeg tijela nadležnog za informacijsku sigurnost i Nacionalnog CERT-a u domeni prevencije i zaštite od računalnih ugroza sigurnosti za najširi skup korisnika javnih elektroničkih usluga, kao i koordinacija rješavanja sigurnosnih incidenata između operatora javnih elektroničkih usluga i Nacionalnog CERT-a.

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga[24], uveo je obveze provedbe sigurnosnih mjera za operatore javnih komunikacijskih mreža u RH, u obliku minimalnih sigurnosnih mjera u skladu s međunarodnom normom ISO 27001. HAKOM, kao nadležno regulatorno tijelo, kontrolira provedbu mjera nadzorom operatora javnih elektroničkih usluga.

Na prijedlog MMPI, HAKOM imenuje svog predstavnika u Upravni odbor EU agencije ENISA-e. Na nacionalnom međuresornom planu i MMPI i HAKOM sudjeluju u radu Vijeća, dok HAKOM sudjeluje i u radu Koordinacije.

4.2.6. SEKTOR GOSPODARSTVA I JAVNO-PRIVATNO PARTNERSTVO

Procesi povezani s razvojem digitalnog gospodarstva i javno-privatnog partnerstva razvijaju se u okviru nadležnog Ministarstva gospodarstva, poduzetništva i obrta (MGPO) te Hrvatske gospodarske komore (HGK). Kao važne inicijative u predmetnom području potrebno je

[24] Neslužbeni pročišćeni tekst: https://www.hakom.hr/UserDocsImages/2016/propisi/VL-KU-PR-INTS-Pravilnik%20o%20sigurnosti-neslu%C5%BEbeni%20pro%C4%8Di%C5%A1%C4%87eni%20tekst.pdf

navesti Strategiju pametne specijalizacije („Narodne novine“, broj: 32/16), koja otvara mogućnosti sufinanciranja razvoja proizvoda i usluga hrvatskih tvrtki u definiranim područjima, od kojih je jedno područje sigurnosti, u kojem je uključena i kibernetička sigurnost. Postoji suradnja i poticanje hrvatskih tvrtki u okviru Centra za industrijski razvoj HGK, u suradnji sa Svjetskom bankom i nizom tvrtki raspoređenih u tematske klastere organizirane pri HGK.

Važan doprinos u ovom sektoru je lokalizacija i promocija Vodiča Međunarodne trgovačke komore za informacijsku sigurnost u poslovanju[25] koji je izrađen pod vodstvom Hrvatske gospodarske komore i u suradnji s nacionalnim partnerima poput NCERT-a, MUP-a, UVNS-a i ZSIS-a. Ovaj Vodič na pristupačan način pojašnjava osnove informacijske sigurnosti u poslovanju, upozorava na sigurnosne ugroze i rizike poslovanja na Internetu te nudi praktična rješenja za učinkovitije upravljanje rizikom. Namijenjen je poduzećima svih veličina i iz svih sektora gospodarstva, vlasnicima poduzeća, menadžmentu i zaposlenicima i nije ograničen samo na IT službe.

Transpozicijom EU NIS direktive kroz Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, otvaraju se dodatne mogućnosti korištenja EU financiranja putem CEF fonda, kako za nadležna državna tijela, tako i za privatne tvrtke koje će, sukladno Zakonu, biti identificirane kao operatori ključnih usluga ili davatelji digitalnih usluga.

Dobrom koordinacijom ključnih sektora društva: državnog, gospodarskog i akademskog, mogu se ostvariti potencijali za jaču inicijativu razvoja gospodarstva u segmentu digitalnog tržišta. Uloga državnog sektora potrebna je u smislu razrade odgovarajućih politika koje prate razvoj područja digitalnog gospodarstva te u smislu poticanja i otvaranja mogućnosti za primjenu hrvatskih proizvoda i usluga u nadležnim tijelima i drugim obveznicima Zakona. Uloga gospodarskog sektora važna je u smislu interesa potencijalnih ponuditelja koji bi mogli razvijati povezane usluge i proizvode. Akademski sektor predstavlja poveznicu koja svojim sudjelovanjem može uvelike pomoći i ubrzati nacionalne procese razvoja proizvoda i usluga, ali i dugoročno ostvariti prilagodbe svojih istraživačkih potencijala prema ciljanom i perspektivnom tržišnom segmentu koji se otvara kroz EU razvoj digitalnog gospodarstva.

Važnost tržišnog segmenta digitalnog gospodarstva najbolje se vidi kroz široku digitalnu inicijativu EK, koja, osim područja NIS direktive, uključuje tijekom posljednjih nekoliko godina i čitav niz povezanih i gospodarski iskoristivih pristupa kao što su GDPR tj. regulativa o zaštiti osobnih podataka (https://www.eugdpr.org/), odnosno eIDAS direktiva o elektroničkoj identifikaciji i uslugama povjerenja u elektroničkim transakcijama

[25] https://www.hgk.hr/documents/vodic-icc-a-za-informacijsku-sigurnost-u-poslovanju5a97cb153fceb.pdf

(https://www.mingo.hr/page/uredba-o-elektronickoj-identifikaciji-za-uspostavljanje-jedinstvenog-eu-digitalnog-trzista-1), kao i uspostava jedinstvenog digitalnog tržišta EU-a.

4.2.7. SEKTOR OBRAZOVANJA

Sektor obrazovanja je iznimno značajan za područje kibernetičke sigurnosti. Nacionalna strategija kibernetičke sigurnosti oko 40% mjera Akcijskog plana projicira na ciljeve vezane u širem smislu na sektor obrazovanja kroz više segmenata počevši od formalnih obrazovnih programa (osnovno, srednje i visoko obrazovanje), preko specijalističkog obrazovanja u okviru postojećih sektorskih akademija kao što su u pravosudnom sektoru, sektoru unutarnjih poslova, obrane, vanjskih poslova, odnosno državne uprave, do problematike razvoja sigurnosne svijesti i cjeloživotnog obrazovanja. Istovremeno se u ovom sektoru adresira i problem istraživanja i razvoja, usko povezan s konceptom javno-privatnog partnerstva.

Ministarstvo znanosti i obrazovanja s pripadnim strukovnim agencijama za obrazovanje i spomenute sektorske akademije dionici su provedbe mjera iz Akcijskog plana, dok se programi razvoja sigurnosne svijesti nastoje dodatno koordinirati kroz rad Vijeća i usklađivanje ovih obveza koje postoje za sve nositelje sigurnosnih politika u različitim sektorima.

Ključni problem na kojem je potrebno raditi jest potreba puno veće konzistentnosti obrazovnih programa kibernetičke sigurnosti te bolje osposobljenosti i informiranosti predavača na različitim razinama i vrstama obrazovanja. Aktualno stanje još uvijek ukazuje na nizak stupanj konzistentnosti programa i nedovoljnu osposobljenost predavača, a samim time i na upitne rezultate edukacijskih programa kibernetičke sigurnosti koji se provode u RH.

Razrada kibernetičke sigurnosti u okviru Strategije i Akcijskog plana morale bi biti okvir za izradu svih nacionalnih edukacijskih programa u ovom području, a Vijeće je potrebno u odgovarajućoj mjeri uključiti u savjetodavni proces nadležnih ministarstva i drugih tijela povezanih s unaprjeđenjem svih vrsta i razina obrazovanja u RH.

Ministarstvo znanosti i obrazovanja, Ministarstvo uprave, Ministarstvo unutarnjih poslova i Ministarstvo obrane, kao primarni nositelji spomenutih obrazovnih programa sudjeluju u radu Vijeća, a Vijeće je započelo s dogovorima za tematske sjednice u svrhu poticanja različitih nacionalno važnih inicijativa, od kojih je jedna i obrazovna inicijativa te je načelno dogovorena jesenska tematska sjednica Vijeća u Ministarstvu znanosti i obrazovanja koja bi se fokusirala na potrebe kibernetičke sigurnosti u okviru različitih obrazovnih programa.

Iako se mjere razvoja sigurnosne svijesti i provedbe edukacijskih kampanja u okviru najšire javnosti provode, još uvijek nije uspostavljena dovoljno učinkovita horizontalna koordinacija, već se aktivnosti u razvijanju ovih programa usmjerenih na najširi krug korisnika, provode na

razini sektorskih nositelja u okvirima njihovih redovitih aktivnosti. U narednom je razdoblju potrebno uspostaviti jaču horizontalnu koordinaciju ovih aktivnosti i tema koje se obuhvaćaju ovakvim aktivnostima na nacionalnoj razini.

4.2.8. SEKTORI KRITIČNE KOMUNIKACIJSKE I INFORMACIJSKE INFRASTRUKTURE

Prema Nacionalnoj strategiji kibernetičke sigurnosti, 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. Sustav upravljanja kibernetičkim krizama, pri tome ima za cilj osigurati pravovremenu i učinkovitu reakciju/odgovor na prijetnju i osigurati oporavak infrastrukture ili usluge od naročitog sigurnosnog interesa za RH. Pri tome je sustav upravljanja u kibernetičkim krizama u RH potrebno uspostaviti u skladu sa sljedećim zahtjevima:

1. usklađenost s nacionalnim rješenjima upravljanja u krizama,
2. obuhvaćanje zaštite kritične nacionalne komunikacijske i informacijske infrastrukture,
3. usklađenost s međunarodnim sustavima upravljanja u kibernetičkim krizama EU-a i NATO-a,
4. usklađenost s nacionalnim nadležnostima tijela zakonom zaduženih za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

U cilju zaštite procesa koji su ključni za funkcioniranje države i gospodarstva, kao i uspostave učinkovitog odgovora na moguće krize, Strategijom je definirano pet ciljeva usmjerenih na:

- utvrđivanje kriterija za prepoznavanje kritične komunikacijske i informacijske infrastrukture;
- utvrđivanje obvezujućih sigurnosnih mjera koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture;
- jačanje prevencije i zaštite kroz upravljanje rizikom;
- jačanje javno-privatnog partnerstva i tehničke koordinacije u obradi računalnih sigurnosnih incidenata;
- uspostava kapaciteta za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu.

Za ostvarivanje ovih ciljeva Akcijskim planom je predviđeno provođenje 13 mjera. Preduvjet za provođenje ovih mjera je identifikacija nacionalnih kritičnih infrastruktura.

Vlada je svojom Odlukom[26] definirala kritične nacionalne sektore, ali je izostalo definiranje konkretnih infrastruktura u tim sektorima te samim tim i dodatnih sigurnosnih zahtjeva prema

[26] Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura („Narodne novine“, broj: 108/13).

istima. Vijeće je na temelju rezultata provedbe Akcijskog plana u 2016. godini zaključilo kako postoji ključni problem u nedovoljnom stupnju provedbe Zakona o kritičnim infrastrukturama („Narodne novine“, broj: 56/13) gledajući iz kuta kibernetičkog prostora, ali i dodatni problem pristupa kritičnim sektorima koji se u ovom Zakonu ne razmatraju iz kuta ovisnosti o komunikacijskoj i informacijskoj tehnologiji već se komunikacijska i informacijska tehnologija tretira kao jedan od kritičnih sektora.

S obzirom na nedostatno stanje provedbe u segmentu kritičnih nacionalnih sektora te na obavezu RH za provedbu EU NIS Direktive[27] u 2018. godini, Vijeće za je u svibnju 2017. godine odlučilo uspostaviti radnu skupinu Vijeća za pripremu provedbe NIS direktive, čiji rad koordinira UVNS. Ovaj proces pokrenut je na temelju visokog stupnja korelacije između EU strategije kibernetičke sigurnosti i NIS direktive te Nacionalne strategije kibernetičke sigurnosti RH, odnosno Odluke Vlade RH o uspostavi Vijeća i Koordinacije, kao i formata za suradnju predviđenih u NIS direktivi, NIS skupina za stratešku suradnju i CSIRT mreža za operativno-tehničku suradnju. Dodatno, pristup koji se koristi u NIS direktivi u potpunosti je primjeren kibernetičkom prostoru jer promatra ovisnosti definiranih sektora i podsektora u odnosu na mrežnu i informacijsku infrastrukturu te omogućava dodatna proširenja izbora sektora i podsektora na nacionalnoj razini.

Radna skupina Vijeća za transpoziciju NIS direktive započela je rad u lipnju 2017. te je izradila NIS transpozicijski plan koji je predvidio donošenje Zakona o kibernetičkoj sigurnosti operatora ključnih usluga[28] i davatelja digitalnih usluga[29] te podzakonsku Uredbu Vlade RH istog naziva. Zakon u lipnju ide u drugo čitanje u Hrvatski sabor[30], a Uredba je u svibnju upućena u savjetovanje sa zainteresiranom javnošću (e-savjetovanje[31]).

NIS transpozicijski plan i izrađeni Nacrt Zakona u potpunosti zadovoljavaju pet ciljeva područja Kritične komunikacijske i informacijske infrastrukture i upravljanja u kibernetičkim krizama, kako su određeni Nacionalnom strategijom kibernetičke sigurnosti i ovdje citirani, a u potpunosti zadovoljavaju i četiri zahtjeva postavljena u Strategiji za sustav upravljanja krizama kibernetičke sigurnosti u RH. S obzirom na sve izneseno, Vijeće planira tijekom 2018. godine pratiti i prema potrebi dodatno usmjeravati proces implementacije Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te podzakonske

[27] Direktiva (EU) 2016/1148 EP i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije od 6. srpnja 2016. (Network and Information Security Directive), https://ec.europa.eu/digital-single-market/en/cybersecurity

[28] Operators of Essential Services – OES (treba ih nacionalno definirati/identificirati svaka DČ prema kriterijima iz NIS direktive i pomoćnih akata koji će se uskladiti te u okviru 7 traženih EU sektora: energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura)

[29] Digital Service Providers – DSP (Online marketplace - Internetsko trgovanje, Online search engine - Internetske tražilice, Cloud computing services - računalstvo u oblaku)

[30] http://www.sabor.hr/prijedlog-zakona-o-kibernetickoj-sigurnosti-operat

[31] https://esavjetovanja.gov.hr/Econ/MainScreen?EntityId=7489

Uredbe te u okviru ovog procesa i dodatnih aktivnosti Vijeća i Koordinacije, osigurati puno postizanje postavljenih ciljeva i zahtjeva Strategije u području kritične komunikacijske i informacijske infrastrukture.

4.2.8.1. NADLEŽNA TIJELA U SEKTORIMA KRITIČNE KOMUNIKACIJSKE I INFORMACIJSKE INFRASTRUKTURE

Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost

Sektor ključnih usluga	**Nadležno sektorsko tijelo**	**CSIRT**	**Tehničko tijelo za ocjenu sukladnosti**
Energetika	tijelo državne uprave nadležno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	tijelo državne uprave nadležno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	–
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	–
Zdravstveni sektor	tijelo državne uprave nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	tijelo državne uprave nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNET
Poslovne usluge za državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

Davatelji digitalnih usluga	**Nadležno sektorsko tijelo**	**CSIRT**	**Tehničko tijelo za ocjenu sukladnosti**
	tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava

*Napomena: Nadležni CSIRT za sektor Poslovne usluge za središnja državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (Srce) ili CARNET-a, za koje je nadležni CSIRT Nacionalni CERT.

**Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Poslovne usluge za središnja državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili Hrvatske akademske i istraživačke mreže – CARNET-a, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNET.

4.3. MEĐURESORNI PRISTUP U PODRUČJU KIBERNETIČKE SIGURNOSTI

Sve prethodno spomenute sektorske nadležnosti pojedinih institucija povezane su u međuresorni pristup kojim se omogućava učinkovitija i brža suradnja te osigurava protok i razdioba informacija svim dionicima u području kibernetičke sigurnosti. Nacionalne strategije pri tome predstavljaju ključne dokumente kojima se promoviraju i potiču inicijative na najširoj nacionalnoj razini. U tom cilju je izrađena i hrvatska Nacionalna strategija kibernetičke sigurnosti i pripadni Akcijski plan za njezinu provedbu. Osnovana međuresorna nacionalna tijela (Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost) pružaju neophodan nacionalni okvir za pokretanje, ali i za trajno održavanje potrebnih aktivnosti u okviru svih segmenata kibernetičke sigurnosti i svih sektora društva u cjelini.

Nacionalna strategija kibernetičke sigurnosti (u daljnjem u tekstu: Strategija) predstavlja prvi strateški dokument u području kibernetičke sigurnosti u RH, koji je usmjeren na stvaranje organizacijskih preduvjeta potrebnih za uvođenje trajne i sustavne brige za virtualnu dimenziju našeg društva.

Strategijom su definirani ciljevi za pet područja kibernetičke sigurnosti, koja ujedno predstavljaju segmente društva procijenjene kao sigurnosno najvažnije za RH u odnosu na stupanj razvoja informacijskog društva. Radi osiguranja koordiniranog planiranja svih zajedničkih aktivnosti i resursa u odabranim područjima kibernetičke sigurnosti, Strategija prepoznaje i četiri poveznice područja kibernetičke sigurnosti, za koje, također kroz definiranje posebnih ciljeva, opisuje rezultate koji se kroz provođenje strateškog okvira žele postići.

Područja kibernetičke sigurnosti:

A. Javne elektroničke komunikacije

B. Elektronička uprava

C. Elektroničke financijske usluge

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

E. Kibernetički kriminalitet

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata

H. Međunarodna suradnja

I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru

4.3.1. VERTIKALNA KOORDINACIJA NA NACIONALNOJ RAZINI

Strategijom je određeno da će, radi razmatranja i unaprjeđenja provođenja Strategije i Akcijskog plana za njezinu provedbu, Vlada Republike Hrvatske osnovati Nacionalno vijeće za kibernetičku sigurnost, koje će:

- sustavno pratiti i koordinirati provedbu Strategije te raspravljati o svim pitanjima od važnosti za kibernetičku sigurnost;
- predlagati mjere za unaprjeđenje provođenja Strategije i Akcijskog plana za provedbu Strategije;
- predlagati organiziranje nacionalnih vježbi iz područja kibernetičke sigurnosti;
- izrađivati preporuke, mišljenja, izvješća i smjernice u vezi s provedbom Strategije i Akcijskog plana te
- predlagati izmjene i dopune Strategije i Akcijskog plana, odnosno donošenje nove Strategije i akcijskih planova, u skladu s novim potrebama.

Vrlo široka i složena problematika na koju se odnosi Strategija, potreba za usklađivanjem zajedničkog rada niza različitih dionika koji sudjeluju u provedbi Strategije i mjera koje su u tu svrhu definirane Akcijskim planom, odrazile su se i na utvrđivanje sastava Vijeća. Sukladno Odluci o osnivanju, Vijeće je sastavljeno od 18 članova koje čine predstavnici sljedećih institucija:

- Ured Vijeća za nacionalnu sigurnost (predsjednik),
- Ministarstvo unutarnjih poslova (član),
- Ministarstvo vanjskih i europskih poslova (član),
- Ministarstvo uprave (član),
- Ministarstvo gospodarstva, poduzetništva i obrta (član),
- Ministarstvo znanosti i obrazovanja (član),
- Ministarstvo obrane (član),
- Ministarstvo pravosuđa (član),
- Ministarstvo mora, prometa i infrastrukture (član),
- Središnji državni ured za razvoj digitalnog društva (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Državna uprava za zaštitu i spašavanje (član),
- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član),

- Agencija za zaštitu osobnih podataka (član).

Vijeće je ujedno i nositelj triju mjera Akcijskog plana iz dijela upravljanja u kibernetičkim krizama, kao dijela nacionalnog sustava upravljanja u krizama.

Vijeće podnosi Vladi i izvješće o provedbi Akcijskog plana za provedbu Strategije, najkasnije do kraja drugog kvartala tekuće godine, za prethodnu godinu.

Strategija je nadalje predvidjela i osnivanje Operativno-tehničke koordinaciju za kibernetičku sigurnost, radi osiguravanja operativne podrške radu Vijeća. Koordinacija ima zadaću:

- pratiti stanje sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu;
- izrađivati izvješća o stanju kibernetičke sigurnosti;
- predlagati planove postupanja u kibernetičkim krizama;
- obavljati druge poslove prema utvrđenim programima i planovima aktivnosti.

Koordinacija je sastavljena od 8 članova koje čine predstavnici sljedećih institucija:

- Ministarstvo unutarnjih poslova (koordinator),
- Ministarstvo obrane (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član).

Koordinacija obavlja zadaće prema programima i planovima aktivnosti te smjernicama Vijeća, a o svom radu podnosi Vijeću izvješće, najkasnije do 31. siječnja tekuće godine, za prethodnu godinu. U spomenutim mjerama Akcijskog plana u kojima je Vijeće nositelj provedbe, Koordinacija je sunositelj.

Vijeće podnosi Vladi RH godišnje izvješće o svom radu i radu Koordinacije najkasnije do kraja prvog kvartala tekuće godine, za prethodnu godinu.

4.3.2. HORIZONTALNA KOORDINACIJA NA NACIONALNOJ RAZINI

Vijeće provodi horizontalnu koordinaciju prema nositeljima mjera iz Akcijskog plana, pri čemu UVNS obavlja administrativni dio poslova. Svaka pojedina mjera ima određenog barem jednog nositelja, a može biti i više nositelja i sunositelja. Većina ključnih obveznika provođenja mjera Akcijskog plana poimence je nabrojena, dok će za manji broj institucija

obveza provođenja biti utvrđena nakon provedbe nekih predradnji. Izravno je identificirano 23 nositelja mjera Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti:

- Agencija za odgoj i obrazovanje
- Agencija za strukovno obrazovanje i obrazovanje odraslih
- Agencija za zaštitu osobnih podataka
- CARNET
- Državna uprava za zaštitu i spašavanje
- HAKOM
- Hrvatska narodna banka
- Ministarstvo gospodarstva, poduzetništva i obrta
- Ministarstvo obrane
- Ministarstvo pravosuđa
- Ministarstvo unutarnjih poslova
- Ministarstvo uprave
- Ministarstvo vanjskih i europskih poslova
- Ministarstvo znanosti i obrazovanja
- Nacionalni CERT
- Nacionalno vijeće za kibernetičku sigurnost
- Operativno-tehnički centar za nadzor telekomunikacija
- Pravosudna akademija
- Sigurnosno-obavještajna agencija
- Sveučilišni računski centar
- Ured Vijeća za nacionalnu sigurnost
- Vojna sigurnosno-obavještajna agencija
- Zavod za sigurnost informacijskih sustava.

Mjere Akcijskog plana uključuju i niz drugih tijela koja su funkcionalno definirana (npr. središnja tijela državne uprave, regulatorne agencije i sl.). U svim mjerama koje uključuju više nositelja/sunositelja nužno je koordinirano djelovanje, kako bi se postigao sinergijski učinak njihovog rada, a u provedbu mjera nositelji mogu uključiti i druge organizacije i stručnjake kada to ocijene potrebnim.

U svrhu bolje učinkovitosti provedbe mjera Vijeće je donijelo smjernice za provedbu Akcijskog plana u 2017. godini, kojima se ukazuje na uočene ključne nedostatke u provedbi mjera iz Akcijskog plana u 2016. godini. Prvo izvještajno razdoblje ukazuje na nedostatnu horizontalnu komunikacije između uključenih institucija – dionika provedbe mjera Akcijskog plana, što je jedan od temelja za uspješnost provedbe Akcijskog plana za provedbu Nacionalne strategije za kibernetičku sigurnost. Također, dio dostavljenih izvješća o provedbi mjera oslanja se isključivo na rezultate redovnih aktivnosti institucije, što daje zaključiti da su se u prvom izvještajnom razdoblju rijetko provodile ciljane aktivnosti dionika, utemeljene na

opsegu i sadržaju pojedine mjere iz Akcijskog plana. Za prvu fazu provedbe u 2016. godini, već i samo prepoznavanje redovnih aktivnosti institucija i njihovo ispravno povezivanje s tematskim mjerama Akcijskog plana predstavlja zadovoljavajući nacionalni rezultat, napose uz činjenicu da u razdoblju tijekom 2016. godine nije bilo uspostavljeno Nacionalno vijeće za kibernetičku sigurnost koje bi poticalo koordinaciju na međuresornoj i međusektorskoj razini.

Nacionalno vijeće za kibernetičku sigurnost stoga je u 2017. godini dalo smjernice u cilju pokretanja koordinirane i ciljane provedbe mjera Akcijskog plana te u cilju poticanja svih dionika da dodatno razvijaju svoje temeljne sposobnosti i međusobno se povezuju i koordiniraju, stvarajući sinergijski učinak i na nacionalnoj i na sektorskim razinama. U tu svrhu Vijeće je pripremilo i poslalo svim nositeljima obrazac kojim se potiče u svim institucijama provesti analiza organizacije poslova povezanih s kibernetičkom sigurnošću, ciljano određivanje nositelja mjera i njihovo međusobno horizontalno povezivanje s nositeljima/sunositeljima u drugim institucijama. Spomenuta organizacija poslova odnosi se na redovne nadležnosti i operativno-tehničke resurse institucije koji su povezani s obavljanjem aktivnosti u domeni kibernetičke sigurnosti (npr. diplomacija, koordinacija, sigurnosna politika, zakonodavna aktivnost, istražne i operativne nadležnosti, tehnički resursi, edukacija, razvoj svijesti, predstavnici u povezanim EU/NATO odborima i tijelima, …).

5. TABLIČNI PRIKAZ SEKTORSKE NADLEŽNOSTI TIJELA

U tablici se daje pregledni prikaz ključnih institucija po sektorima bitnim za kibernetičku sigurnost i iz kuta bitnih nadležnosti povezanih s kibernetičkom sigurnošću:

Sektor politike informacijske sigurnosti u državnim tijelima	
Ured Vijeća za nacionalnu sigurnost (UVNS)	Središnje državno tijelo za informacijsku sigurnost (NSA) Nositelj rada Nacionalnog vijeća za kibernetičku sigurnost
Zavod za sigurnost informacijskih sustava (ZSIS)	Središnje državno tijelo za tehnička područja informacijske sigurnosti Koordinacija prevencije i odgovora na računalne ugroze sigurnosti u državnom sektoru
Nacionalni CERT u okviru CARNET-a	Prevencija i odgovor na računalne ugroze sigurnosti javnih informacijskih sustava
Ministarstvo vanjskih i europskih poslova (MVEP)	Međunarodna suradnja i kibernetička diplomacija
Sektor sigurnosno-obavještajnog djelovanja	
Sigurnosno-obavještajna agencija (SOA)	Sigurnosno, obavještajno i operativno djelovanje u kibernetičkom prostoru
Vojna sigurnosno-obavještajna agencija (VSOA)	Sigurnosno, obavještajno i operativno djelovanje u kibernetičkom prostoru
Sektor obrambenog planiranja	
Ministarstvo obrane (MORH)	Kibernetička obrana kao dio obrambenog planiranja MORH CERT funkcionalnost Nositelj i koordinator većine međunarodnih i

	nacionalnih vježbi Vojni studijski programi
Sektor istražnog i kaznenog postupanja	
Ministarstvo pravosuđa	Sektorsko zakonodavno planiranje Pravosudna akademija
Ministarstvo unutarnjih poslova (MUP)	Kriminalistički istražni i forenzički postupci u području visokotehnološkog kriminaliteta Nositelj rada Operativno-tehničke koordinacije za kibernetičku sigurnost Policijska akademija
Državno odvjetništvo (DORH)	Provedba kaznenog postupka u slučajevima kibernetičkog kriminaliteta
Sektor javnih elektroničkih komunikacija	
Ministarstvo mora, prometa i infrastrukture (MMPI)	Sektorsko zakonodavno planiranje
Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)	Sektorsko regulatorno tijelo Predstavlja RH članom u Upravi ENISA-e
Sektor gospodarstva i javno-privatno partnerstvo	
Ministarstvo gospodarstva, poduzetništva i obrta (MGPO)	Sektorsko zakonodavno planiranje Digitalno gospodarstvo Inicijative javno-privatnog partnerstva
Hrvatska gospodarska komora (HGK)	Provedba javno-privatnog partnerstva
Sektor obrazovanja	
Ministarstvo znanosti i obrazovanja (MZO)	Sektorsko zakonodavno planiranje

SEKTORI KRITIČNE KOMUNIKACIJSKE I INFORMACIJSKE INFRASTRUKTURE	
Državna uprava za zaštitu i spašavanje (DUZS)	Sektorsko zakonodavno planiranje u području zaštite kritične nacionalne infrastrukture
Ured Vijeća za nacionalnu sigurnost (UVNS)	Sektorsko zakonodavno planiranje u području ključnih i digitalnih usluga Jedinstvena nacionalna kontaktna točka
Sektor energetike – električna energija, nafta, plin	
Ministarstvo zaštite okoliša i energetike (MZOE)	Nadležno sektorsko tijelo
Zavod za sigurnost informacijskih sustava (ZSIS)	CSIRT tijelo Tehničko tijelo za ocjenu sukladnosti
Sektor prijevoza – zračni, željeznički, vodni, cestovni	
Ministarstvo mora, prometa i infrastruktura	Nadležno sektorsko tijelo
Zavod za sigurnost informacijskih sustava (ZSIS)	CSIRT tijelo Tehničko tijelo za ocjenu sukladnosti
Sektor bankarstva	
Ministarstvo financija	Sektorsko zakonodavno planiranje
Hrvatska narodna banka (HNB)	Nadležno sektorsko tijelo
Nacionalni CERT (CARNET)	CSIRT tijelo
Sektor infrastruktura financijskog tržišta	
Ministarstvo financija	Sektorsko zakonodavno planiranje
Hrvatska agencija za nadzor financijskih usluga (HANFA)	Nadležno sektorsko tijelo
Nacionalni CERT (CARNET)	CSIRT tijelo

Zdravstveni sektor	
Ministarstvo zdravstva	Nadležno sektorsko tijelo
Zavod za sigurnost informacijskih sustava (ZSIS)	CSIRT tijelo Tehničko tijelo za ocjenu sukladnosti
Opskrba vodom za piće i njezina distribucija	
Ministarstvo zaštite okoliša i energetike (MZOE)	Nadležno sektorsko tijelo
Zavod za sigurnost informacijskih sustava (ZSIS)	CSIRT tijelo Tehničko tijelo za ocjenu sukladnosti
Digitalna infrastruktura	
Središnji državni ured za razvoj digitalnog društva (SDU RDD)	Nadležno sektorsko tijelo
Nacionalni CERT (CARNET)	CSIRT tijelo Tehničko tijelo za ocjenu sukladnosti
Poslovne usluge za državna tijela	
Ministarstvo uprave	Sektorsko zakonodavno planiranje
Središnji državni ured za razvoj digitalnog društva (SDU RDD)	Nadležno sektorsko tijelo
Zavod za sigurnost informacijskih sustava ili Nacionalni CERT	CSIRT tijelo***** Tehničko tijelo za ocjenu sukladnosti******
Davatelji digitalnih usluga - internetsko tržište, internetska tražilica, usluge računalstva u oblaku	
Ministarstvo gospodarstva, poduzetništva i obrta (MGPO)	Nadležno sektorsko tijelo
Nacionalni CERT (CARNET)	CSIRT tijelo

Zavod za sigurnost informacijskih sustava (ZSIS)	Tehničko tijelo za ocjenu sukladnosti

[*] Napomena: Nadležni CSIRT za sektor Poslovne usluge za državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (Srce) ili CARNET-a, za koje je nadležni CSIRT Nacionalni CERT.

[**] Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Poslovne usluge za državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (Srce) ili Hrvatske akademske i istraživačke mreže – CARNET-a, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNET.