IZVJEŠĆE O OSNIVANJU I POČETKU RADA

NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST

I

OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST

Sadržaj:

1. UVOD

1.1. IZRADA NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA

Nacionalnu strategiju kibernetičke sigurnosti izradilo je međuresorno povjerenstvo za izradu nacrta prijedloga Strategije, u razdoblju od travnja 2014. godine do listopada 2015. godine. Povjerenstvo je bilo sastavljeno od predstavnika iz 19 institucija, a nositelj izrade bio je Ured Vijeća za nacionalnu sigurnost (UVNS). Povjerenstvo je u okviru radnih grupa formiranih za analizu odabranih pet područja kibernetičke sigurnosti[1] i četiri poveznice područja kibernetičke sigurnosti[2], uključilo u radne skupine i predstavnike iz niza drugih institucija, čime je ukupno u izradu Strategije bilo uključeno gotovo 40 različitih državnih tijela, akademskih institucija te regulatornih tijela u gospodarskim sektorima ključnim za problematiku stvaranja sigurnijeg nacionalnog kibernetičkog prostora.

Metodologija pristupa, razrađena za potrebe izrade Strategije, uključivala je i izradu Akcijskog plana za provedbu Strategije te su oba dokumenta međusobno usko povezana i usklađena. Strategija i Akcijski plan međusobno su povezani pomoću odabranih općih ciljeva Strategije, za koje su definirani posebni ciljevi svakog od područja i poveznica područja, a za svaki od ovih posebnih ciljeva definirane su odgovarajuće mjere za njegovo postizanje u okviru provedbe Akcijskog plana. Time je dobiven koherentan i sveobuhvatan sustav međusobno povezanih ciljeva i mjera. Svaka mjera, koja je razrađena u Akcijskom planu u svrhu postizanja nekog posebnog cilja u jednom od područja ili poveznica područja, doprinosi postizanju općih ciljeva Strategije iz kojih su izvedeni svi posebni ciljevi. Tako je za 8 općih ciljeva Strategije, razrađeno 35 posebnih ciljeva u okviru 5 područja kibernetičke sigurnosti i 4 poveznice područja, čija je daljnja razrada rezultirala s ukupno 77 mjera razrađenih u Akcijskom planu. Svaka od ovih 77 mjera u Akcijskom planu ima određene nositelje i sunositelje te definiranu osnovnu metriku rokova i pokazatelja provedbe.

Nakon usuglašavanja tekstova Strategije i Akcijskog plana, na razini institucija čiji su predstavnici bili uključeni u rad Povjerenstva, provedena je javna rasprava o Strategiji i Akcijskom planu putem Internetskog portala e-savjetovanje te je održano više javnih okruglih stolova na kojima su predstavljeni rezultati izrade Strategije u okviru stručne, ali i najšire javnosti u RH, kao i u okviru više povezanih aktualnih inicijativa EU-a (npr. EU GENVAL proces procjene sposobnosti država članica u području kibernetičkog kriminala, ili EU NIS

[1] Elektronička komunikacijska i informacijska infrastruktura i usluge (A. Javne elektroničke komunikacije, B. Elektronička uprava, C. Financijske elektroničke usluge), D. Kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama, E. Kibernetički kriminal

[2] 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

direktiva za provedbu EU strategije kibernetičke sigurnosti[3]) i NATO-a (npr. aktualna procjena sposobnosti zemalja članica NATO-a s obzirom na utvrđivanje kibernetičkog prostora kao domene vojnog djelovanja). Pristup RH prezentiran je i u zemljama uže regije kao referentan model, primjerice u Republici Sloveniji za predstavnike državnih tijela koji su bili u sličnom procesu izrade strategije kibernetičke sigurnosti, ali koji je započeo nešto kasnije u odnosu na hrvatski proces izrade Strategije. Nadalje, pristup RH u području kibernetičke sigurnosti prezentiran je kroz 6S inicijativu regionalnih NSA[4] tijela, nastalu na temeljima političke inicijative Hrvatske i Slovenije u procesu Brdo-Brijuni, kao i kroz niz aktivnosti financiranih putem TAIEX programa Europske Komisije u svrhu predpristupne pomoći zemljama hrvatskog susjedstva (Bosna i Hercegovina, Crna Gora, Makedonija, Srbija).

Potrebno je posebno naglasiti da cilj ove prve Strategije nije bio riješiti sve probleme u kibernetičkom prostoru, već pokrenuti sustavan i usklađen pristup ovom području. Stoga je Strategija oblikovana na način da bude provediva u okviru postojećih sposobnosti tijela, u okviru postojećih financijskih sredstava te u okviru postojećeg zakonodavnog okvira i ovlasti. Strategija je stoga primarno adresirala prioritete koji se realno mogu provesti, i koje je nužno provesti što prije.

1.2. POSTUPAK DONOŠENJA STRATEGIJE

Nakon provedene javne rasprave i završnog usuglašavanja tekstova Strategije i Akcijskog plana s institucijama čiji su predstavnici sudjelovali u radu Povjerenstva za izradu nacrta prijedloga Strategije, Vlada Republike Hrvatske donijela je na sjednici održanoj 7. listopada 2015. godine, Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njezinu provedbu (*„Narodne novine“, broj: 108/2015*).

S ciljem osiguravanja upravljanja složenim procesom kibernetičke sigurnosti i provedbom mjera Akcijskog plana, koje obuhvaćaju kibernetički prostor tretiran sveobuhvatno kao virtualna dimenzija suvremenog društva, Strategijom je predviđena uspostava sustava kontinuiranog praćenja ostvarivanja ciljeva Strategije i provedbe mjera Akcijskog plana, a koji ujedno predstavlja i upravljački mehanizam horizontalnog koordiniranja čitavog niza nadležnih institucija u kreiranju odgovarajućih nacionalnih i sektorskih politika i odgovora na prijetnje u nacionalnom kibernetičkom prostoru. Stoga je Vlada Republike Hrvatske u tu svrhu donijela na sjednici održanoj 8. lipnja 2016. godine, Odluku o osnivanju Nacionalnog

[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7.2.2013, JOIN(2013)1 final

[4] National Security Authority (NSA) – središnja državna tijela za politiku informacijske sigurnosti, u RH ovu ulogu obnaša Ured Vijeća za nacionalnu sigurnost (UVNS)

vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (*„Narodne novine“, broj: 61/2016*).

Kako bi se omogućilo pokretanje rada nacionalnih međuresornih tijela za kibernetičku sigurnost, Vlada Republike Hrvatske je na sjednici održanoj 16. veljače 2017. godine, donijela Rješenje o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, čime je otvoren put za punu provedbu mjera Akcijskog plana i ciljeva Strategije te upravljanje horizontalnim inicijativama, kako u državnom sektoru, tako i međusektorski, u društvu u cjelini.

1.3. CILJEVI STRATEGIJE

Nacionalna strategija kibernetičke sigurnosti Republike Hrvatske utemeljena je na pristupu koji kibernetički prostor tretira kao virtualnu dimenziju društva te ravnopravno razmatra potrebe društva u cjelini, odnosno potiče stvaranje partnerstva i uključenje svih sektora društva kao dionika u provedbi Strategije. Donošenjem strateških i provedbenih akata Nacionalne strategije kibernetičke sigurnosti, Republika Hrvatska započela je s uvođenjem sustavnog i sveobuhvatnog pristupa području kibernetičke sigurnosti kojim se želi postići niz ciljeva koji su od iznimne važnosti za budući razvoj hrvatskog društva, a napose:

- sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, virtualna dimenzija društva (kibernetički prostor);
- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora u okvirima nacionalne odgovornosti RH;
- uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru;
- jačanje svijesti o potrebi sigurnosti svih korisnika kibernetičkog prostora;
- poticanje razvoja usklađenih obrazovnih programa s ciljem podizanja tehnološke osviještenosti građana i podizanja stupnja digitalne higijene društva u cjelini;
- poticanje razvoja elektroničkih usluga kroz razvoj povjerenja svih korisnika;
- poticanje istraživanja i razvoja, u svrhu aktiviranja hrvatskih potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora;
- sustavni pristup međunarodnoj suradnji u području kibernetičke sigurnosti kroz doprinos i aktivnu suradnju RH s akterima u međunarodnoj zajednici i punu svijest o nacionalnoj odgovornosti za globalnu sigurnost kibernetičkog prostora.

2. NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

2.1. USTROJAVANJE I SASTAV VIJEĆA

Nakon donošenja Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, na sjednici Vlade Republike Hrvatske održanoj 16. veljače 2017. godine, UVNS je pripremio materijale i sazvao prvu konstituirajuću sjednicu Vijeća za 16. ožujka 2017. Na konstituirajućoj sjednici ukratko je prezentiran proces razrade Strategije i Akcijskog plana te je usuglašen sadržaj poslovnika o radu Vijeća i okvirni plan rada Vijeća u drugom kvartalu 2017. godine, a UVNS je odredio tajništvo za obavljanje administrativnih i tehničkih poslova za potrebe rada Vijeća.

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 stoga sastavljeno od 16 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),
- 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).

Kako bi se osiguralo da sjednice Vijeća imaju stalnu prisutnost članova, potrebnu za donošenje zaključaka i odluka, sva navedena tijela i pravne osobe predložila su i imenovanja zamjenika članova Vijeća. U svrhu obavljanja opsežnih administrativnih i tehničkih poslova

UVNS je, uz predsjednika i zamjenika predsjednika, utvrdio dodatne osobe koje sudjeluju u radu Vijeća u svojstvu tajništva.

2.2. NADLEŽNOSTI VIJEĆA

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.

Slijedom potreba opisanih u području upravljanja u kibernetičkim krizama, Vijeću su Strategijom dodijeljene i dodatne zadaće, kojima je Vijeće zaduženo:

- razmatrati pitanja bitna za upravljanje u kibernetičkim krizama i predlagati mjere za veću učinkovitost;
- razmatrati izvješća o stanju sigurnosti koje mu dostavlja Operativno-tehnička koordinacija za kibernetičku sigurnost;
- izrađivati periodične procjene o stanju sigurnosti;
- utvrđivati planove postupanja u kibernetičkim krizama;
- izrađivati programe i planove aktivnosti Operativno-tehničke koordinacije za kibernetičku sigurnost i usmjeravati njezin rad.

Nacionalno Vijeće za kibernetičku sigurnost podnosi Vladi Republike Hrvatske godišnje izvješće o svom radu i radu Operativno-tehničke koordinacije za kibernetičku sigurnost (dalje: Koordinacija), najkasnije do kraja prvog kvartala tekuće godine, za prethodnu godinu. Vijeće podnosi Vladi RH i izvješće o provedbi Akcijskog plana za provedbu Strategije, najkasnije do kraja drugog kvartala tekuće godine, za prethodnu godinu.

2.3. POČETAK RADA VIJEĆA, USVAJANJE POSLOVNIKA O RADU I DEFINIRANJE OKVIRNIH PROGRAMA RADA VIJEĆA

Cilj uspostave Nacionalnog Vijeća za kibernetičku sigurnost kao međuresornog tijela s predstavnicima iz 16 relevantnih institucija, nadležnog na nacionalnoj razini za kibernetičku sigurnost, jest upravljati strategijskim planiranjem u ovom složenom i iznimno važnom području za razvoj suvremenog društva te u sklopu toga upravljati akcijskim provedbenim planovima, inicirati i nadzirati provedbu mjera u pojedinim područjima, odnosno davati rješenja za potrebna usklađivanja politika postupanja na nacionalnoj i različitim sektorskim razinama te za relevantno zastupanje Republike Hrvatske u okviru EU-a i NATO-a, kao i u drugim relevantnim međunarodnim procesima u području kibernetičke sigurnosti. Uspostavom i usmjeravanjem djelovanja Koordinacije, kao međuresornog tijela s predstavnicima iz 8 relevantnih institucija s potrebnim nadležnostima i operativno-tehničkim sposobnostima, Vijeće upotpunjava spektar potrebnih instrumenata za pokrivanje strateške, taktičke i operativne razine u području sigurnosti virtualne dimenzije društva – kibernetičkog prostora.

UVNS je po dostavi Rješenja Vlade RH o imenovanju članova Vijeća pripremio teme i prijedloge prvih akata za konstituirajuću sjednicu Vijeća sazvanu za 16. ožujka 2017. Jedna od početnih aktivnosti Vijeća provedena je odmah nakon zaprimanja rješenja o imenovanju predsjednika Vijeća kada je putem UVNS-a, kao tijela nositelja rada Vijeća, zatraženo od osam institucija predviđenih Odlukom Vlade RH, da obavijeste predsjednika Vijeća o imenovanju svojeg predstavnika i zamjenika predstavnika u Koordinaciju. Po zaprimanju imenovanja predstavnika i zamjenika predstavnika iz svih nadležnih tijela, predsjednik Vijeća je imenovanja putem UVNS-a proslijedio MUP-u, kao tijelu nadležnom za rad Koordinacije i obavljanje administrativnih i tehničkih poslova za potrebe Koordinacije.

Prve zajedničke aktivnosti Vijeća provedene su na konstituirajućoj sjednici 16. ožujka 2017., a bile su usmjerene na uređivanje organizacije i načina rada Vijeća te utvrđivanje okvirnog programa rada Vijeća u narednom razdoblju. Poslovnik o radu Vijeća usuglašen je na konstituirajućoj sjednici Vijeća u ožujku, a usvojen na drugoj sjednici Vijeća 11. travnja 2017. Na konstituirajućoj sjednici članovi i zamjenici članova Vijeća informirani su o prethodnom tijeku izrade Strategije i Akcijskog plana, međusobnoj povezanosti ciljeva i mjera Akcijskog plana, a UVNS je odredio tajništvo za obavljanje administrativnih i tehničkih poslova za potrebe rada Vijeća. Na konstituirajućoj sjednici donesen je i okvirni plan rada Vijeća za II. tromjesečje 2017. godine (travanj – lipanj), koji je uključivao i datume predviđenih redovnih mjesečnih sjednica te ključne teme za rad Vijeća u ovom razdoblju.

2.4. PODUZETE AKTIVNOSTI I DONESENE ODLUKE VIJEĆA

Vijeće je u razdoblju od ožujka do lipnja održalo četiri redovite mjesečne sjednice te radilo na nizu pitanja koja su procijenjena prioritetnim u ovom razdoblju. Jedno od razmatranih pitanja je problematika pripreme izvješća o provedbi Akcijskog plana u 2016. godini. Na konstituirajućoj sjednici Vijeće je odlučilo o potrebi izrade i slanja obrasca za prikupljanje izvješća nositelja o mjerama Akcijskog plana, za što je zadužen UVNS. Izvješća o provedbi mjera Akcijskog plana u 2016. godini prikupljena su u razdoblju do kraja svibnja 2017. od 21 institucije koje su zadužene kao nositelji pojedinih mjera u Akcijskom planu. S obzirom da je Vijeće kao međuresorno tijelo osnovano tek 2017. godine, provedba Akcijskog plana u 2016. godini počivala je na mogućnostima i inicijativama institucija nositelja pojedinih mjera. Nedostatak međuresornog tijela očekivano se najviše osjećao u nizu horizontalno povezanih mjera s više nositelja iz različitih resora/sektora, u kojima se Akcijskim planom želio postići sinergijski učinak njihovog koordiniranog rada.

Na prvoj sjednici Vijeća, 16. ožujka 2017., predsjednik Vijeća informirao je Vijeće da su s danom 14. ožujka 2017. godine dostavljene obavijesti o imenovanjima predstavnika svih tijela i pravnih osoba koje sudjeluju u radu Koordinacije, o čemu je obaviješteno Ministarstvo unutarnjih poslova, kao koordinirajuće tijelo i tijelo nadležno za pružanje administrativne i tehničke podrške Operativno-tehničkoj koordinaciji. Predstavnik MUP-a u Vijeću, potvrdio je zaprimanje popisa članova Koordinacije i izvijestio o pripremi za sazivanje prve sjednice Koordinacije. Tako je Vijeće već na prvoj, konstituirajućoj sjednici, konstatiralo da je Operativno-tehnička koordinacija uspostavljena te da može započeti s radom. Zaključkom Vijeća utvrđeni su prvi zadaci za Koordinaciju vezani za dostavu inicijalnog izvješća o stanju kibernetičke sigurnosti, sa sadržajem koji je potrebno usmjeriti prema analizi raspoloživih kapaciteta za postupanje u kibernetičkim incidentima i krizama, temeljeno na nadležnostima i načinu postupanja osam tijela i pravnih osoba uključenih u rad Koordinacije te njihovim dosadašnjim iskustvima u slučajevima incidenata kibernetičke sigurnosti.

Na drugoj sjednici Vijeća odabran je i pripremljen pregled niza nacionalnih i međunarodnih tema od značaja za rad Vijeća, za koje su članovi Vijeća iz nadležnih tijela pripremili kratko izvješće i održali prezentacije Vijeću, s posebnim osvrtom na poveznice i mogući značaj ovih odabranih tema za rad Vijeća:

- EU NIS Direktiva[5] i rad NIS odbora i stručne radne grupe (UVNS);
- EU NIS Direktiva i rad CSIRT Network stručne radne grupe (ZSIS i NCERT);
- EU GENVAL Cyber Crime[6] inspekcijsko izvješće za RH (MUP, MP);

[5] 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

[6] http://www.consilium.europa.eu/en/meetings/mpo/2015/10/wp-on-general-matters-including-evaluation-(242565)/

- EU GDPR regulativa[7] (AZOP);
- NATO Cyber Defence Assesment[8] i NATO vježba CMX17 (MORH);
- Strategija pametne specijalizacije RH[9] (MGPO);
- Strategija eHR 2020[10] (MU).

Nastavno na pripremljene materijale i diskusiju Vijeća, na trećoj sjednici Vijeća prihvaćen je prijedlog UVNS-a za uspostavu stručne radne skupine Vijeća za provedbu obveza RH u području EU NIS direktive, s prijedlogom institucija koje bi imenovale članove te planom i rokovima provedbe njezinih aktivnosti. Ova aktivnost ima visoki prioritet zbog rokova prilagodbe nacionalnih propisa do svibnja 2018. godine, kao i rokova izvješća o nacionalnoj provedbi ovih propisa do studenog 2018. godine.

Vijeće je provelo analizu zaprimljenih izvješća nositelja mjera Akcijskog plana te pripremilo prijedlog izvješća o provedbi mjera Akcijskog plana u 2016. godini, koje će sadržavati i smjernice za provedbu Akcijskog plana u 2017. godini. Cilj smjernica je uvođenje novih inicijativa u provedbu mjera Akcijskog plana putem jačeg horizontalnog povezivanja različitih resora/sektora i postizanja sinergijskog učinka. Prijedlog izvješća Vijeća se u lipnju upućuje na mišljenje nositeljima mjera Akcijskog plana te će se nakon završnog usklađivanja dostaviti Vladi, na prihvaćanje.

Vijeće je na trećoj sjednici raspravljalo o dostavljenom inicijalnom izvješću Koordinacije o stanju kibernetičke sigurnosti, sa sadržajem koji je usmjeren prema analizi raspoloživih kapaciteta za postupanje u kibernetičkim krizama, temeljeno na nadležnostima i načinu postupanja osam tijela i pravnih osoba uključenih u rad Koordinacije te njihovim dosadašnjim iskustvima u slučajevima incidenata kibernetičke sigurnosti. Izvješće je Vijeću predstavio koordinator iz MUP-a ispred Koordinacije.

Vijeće, odnosno predsjednik Vijeća, uključeni su u svibnju u rad Koordinacije vezano za *WannaCry* globalnu kampanju malicioznog koda, 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 su istupi koordinirani s Uredom Vlade za odnose s javnošću. Vijeće je zatražilo od Koordinacije dodatnu precizniju analizu kako bi se dala točnija procjena štete i naučene lekcije te dalo tematsko priopćenje za javnost. Zaključak je da su i Vijeće i Koordinacija, iako su tek osnovani, već u ovoj prvoj globalnoj kibernetičkoj prijetnji pokazali potrebu horizontalnog međuresornog i međusektorskog pristupa, ali i

[7] http://www.eugdpr.org/
[8] https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html, http://www.nato.int/cps/en/natohq/official_texts_133169.htm
[9] http://www.mingo.hr/page/vlada-usvojila-strategiju-pametne-specijalizacije-rh-za-razdoblje-2016-2020
[10] https://uprava.gov.hr/vijesti/ek-prihvatila-strategiju-e-hrvatska-2020/14408 , https://uprava.gov.hr/UserDocsImages//e-Hrvatska//e-Croatia%202020%20Strategy%20(20.01.2016.).pdf

dokazali učinkovitost i uspješnost po svim aspektima djelovanja na sigurnosni incident, od uzbunjivanja, međusobnog izvještavanja, distribucije uputa i najboljih praksi postupanja, pa sve do komunikacije s javnosti.

Na četvrtoj sjednici Vijeća u lipnju usvojen je program aktivnosti Koordinacije te plan aktivnosti za drugu polovinu 2017. godine. Usvojena su i izvješća o osnivanju i početku rada Vijeća i Koordinacije te Izvješće o provedbi Akcijskog plana u 2016. godini.

Vezano za javna priopćenja, Vijeće je 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 za svibanj i lipanj su odabrane tematske objave informacija o odluci Vijeća o uspostavi stručne radne skupine Vijeća za provedbu obveza RH u području EU NIS direktive te vezano za zaključno izvješće Koordinacije o malicioznoj kampanji *WannaCry*. Planira se i izvješćivanje o provedbi Akcijskog plana, o čemu će se donijeti zaključak na sjednici Vijeća na kojoj se utvrdi da je izvješće za 2016. godinu usuglašeno i prihvaćeno.

Vijeće je u lipnju prihvatilo i okvirni plan rada Vijeća za treći kvartal 2017. godine (srpanj – rujan) sa sljedećim prioritetnim aktivnostima:

- izvješće Vladi RH o osnivanju i pokretanju rada te postignutim početnim rezultatima međuresornih tijela, Vijeća i Koordinacije;
- izrada godišnjeg izvješća za Vladu RH o provedbi Akcijskog plana za 2016.g. uz prethodnu verifikaciju svih nositelja mjera Akcijskog plana;
- slanje godišnjeg izvješća o provedbi Akcijskog plana za 2016.g. svim nositeljima provedbe Akcijskog plana, s uključenim smjernicama provedbe Akcijskog plana za drugu polovinu 2017.g.;
- verifikacija početnih mjesečnih izvješća Koordinacije o sigurnosnim incidentima i prijetnjama i prijedloga metodologije za sveobuhvatnu procjenu stanja kibernetičke sigurnosti;
- analiza mogućnosti i priprema pokretanja rada na mjerama Akcijskog plana koje su u nadležnosti Vijeća (upravljanje kibernetičkim krizama), s obzirom na izvješća o provedbi povezanih mjera Akcijskog plana i napretku NIS radne skupine Vijeća u povezanim segmentima nacionalne i sektorskih razina.

3. OPERATIVNO-TEHNIČKA KOORDINACIJA ZA KIBERNETIČKU SIGURNOST

3.1. USTROJAVANJE I SASTAV KOORDINACIJE

Nakon donošenja Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, na sjednici Vlade Republike Hrvatske održanoj 16. veljače 2017. godine, UVNS je kao tijelo nositelj rada Vijeća, zatražio od osam institucija predviđenih Odlukom Vlade RH, da obavijeste predsjednika Vijeća o imenovanju svojeg predstavnika i zamjenika predstavnika u Operativno-tehničkoj koordinaciji za kibernetičku sigurnost (Koordinacija). Po zaprimanju imenovanja predstavnika i zamjenika predstavnika iz svih nadležnih tijela, predsjednik Vijeća je imenovanja putem UVNS-a proslijedio MUP-u, kao tijelu nadležnom za rad Koordinacije i obavljanje administrativnih i tehničkih poslova za potrebe Koordinacije.

Koordinacija okuplja predstavnike institucija u okviru čijih se nadležnosti nalaze operativni postupci djelovanja na sigurnosne incidente u kibernetičkom prostoru i tehnički resursi koji omogućavaju takvo djelovanje u okviru odgovarajućih sektorski utvrđenih nadležnosti. Sukladno Odluci o osnivanju, Koordinacija je stoga 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).

Kako bi se osiguralo da sjednice Koordinacije imaju stalnu prisutnost predstavnika potrebnu za međusobno operativno-tehničko usklađivanje postupaka, sva navedena tijela i pravne osobe imenovale su i zamjenike članova Koordinacije. MUP je određen nositeljem administrativnih i tehničkih poslova za potporu rada Koordinacije.

3.2. NADLEŽNOSTI KOORDINACIJE

Radi osiguravanja podrške radu Nacionalnog Vijeća za kibernetičku sigurnost, Strategija predviđa osnivanje Operativno-tehničke koordinaciju za kibernetičku sigurnost, čije su zadaće:

- 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 obavlja zadaće prema programima i planovima aktivnosti te smjernicama Nacionalnog vijeća za kibernetičku sigurnost, a o svom radu podnosi Vijeću izvješće, najkasnije do 31. siječnja tekuće godine, za prethodnu godinu.

3.3. POČETAK RADA KOORDINACIJE, USVAJANJE PROGRAMA I PLANA AKTIVNOSTI

Cilj uspostave Operativno-tehničke koordinacije za kibernetičku sigurnost, kao međuresornog tijela s predstavnicima iz 8 relevantnih institucija, nadležnog na nacionalnoj razini za usklađeno operativno postupanje tijela s različitim nadležnostima u kibernetičkom prostoru, jest rješavanje incidenata kibernetičke sigurnosti, a napose u onim slučajevima koji bi mogli prerasti u kibernetičku krizu. Usklađeno djelovanje institucija s operativno-tehničkim nadležnostima u različitim sektorima društva, učinkovita i pravovremena razmjena, ustupanje i pristup podacima o sigurnosnim incidentima te zajedničko djelovanje s ciljem sinergijskog učinka u okviru operativne i taktičke razine postupanja, ključni je razlog uspostave Koordinacije.

Ministarstvo unutarnjih poslova, kao koordinirajuće tijelo i tijelo nadležno za pružanje administrativne i tehničke podrške Operativno-tehničkoj koordinaciji za kibernetičku sigurnost, organiziralo je prvi sastanak Koordinacije 23. ožujka 2017. godine. Tako je Koordinacija na prvoj sjednici započela pripremu inicijalnog izvješća o stanju kibernetičke sigurnosti, kroz koju je napravljena zajednička analiza nadležnosti institucija, raspoloživih tehničkih kapaciteta i načina postupanja te dosadašnjih iskustava u slučajevima incidenata kibernetičke sigurnosti. U okviru toga Koordinacija je dala i prijedloge za programe aktivnosti Koordinacije, kao i prijedlog plana aktivnosti Koordinacije u drugoj polovini 2017. godine, što je Vijeće nakon određenih dopuna i dorada donijelo u lipnju zaključkom o prihvaćanju.

3.4. PODUZETE AKTIVNOSTI KOORDINACIJE

Prve aktivnosti Koordinacije u razdoblju od ožujka do lipnja 2017. godine, bile su usmjerene na izradu inicijalnog izvješća i provedbu analize institucija koje čine Operativno-tehničku koordinaciju za kibernetičku sigurnost, u smislu njihovih nadležnosti, raspoloživih tehničkih kapaciteta i načina postupanja te dosadašnjih iskustava u slučajevima incidenata kibernetičke

sigurnosti. U okviru ovih aktivnosti izrađeni su i prijedlozi za programe aktivnosti Koordinacije, kao i prijedlozi plana aktivnosti Koordinacije u drugoj polovini 2017. godine.

Za vrijeme rada Koordinacije na spomenutim aktivnostima, započela je globalna kampanja malicioznog koda *WannaCry*, koja je prve 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 platforme i koristio je 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. 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 Zavoda za sigurnost informacijskih sustava (ZSIS), Koordinacija je već na prvi dan masovnog širenja malicioznog koda započela s radom, što je u prvom redu obuhvatilo objavu upozorenja i načina zaštite od malicioznog koda putem sigurnosnih zakrpa koje je distribuirao Microsoft, zatim dodatnim obavještavanjem sektorskih tijela i administratora 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 od 12. do 14. svibnja 2017. Objave su davane na nizu web stranica 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 masovnog 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, na koji je pozvan i predsjednik Vijeća zaključeno je 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 Nacionalnog vijeća za kibernetičku sigurnost

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, pokazale su se dobrima, jer je šteta maliciozne kampanje u RH bila minimalna i nije ugrozila nacionalnu sigurnost, čime se ujedno dobila i potvrda učinkovitosti, ali i potrebe novog modela organizacije međuresornih tijela za kibernetičku sigurnost u Hrvatskoj, odnosno Nacionalnog vijeća i Operativno-tehničke koordinacije za kibernetičku sigurnost.

4. ZAKLJUČAK

Kibernetički prostor na današnjem stupnju razvoja suvremenog društva, nužno je tretirati kao neodvojivu virtualnu dimenziju suvremenog društva. U ovoj virtualnoj dimenziji društva svi građani u velikoj mjeri žive svoje privatne i poslovne živote, njome se koristimo za razvoj kulture i obrazovanja, no sve više i za razvoj gospodarstva, bilo kroz specijalizirane tvrtke za kibernetičke proizvode i usluge, bilo kroz potporu ključnim granama hrvatskog gospodarstva kao što je turizam, ili kroz potporu ključnim državnim sektorima kao što je zdravstvo. Cilj kibernetičke sigurnosti stoga mora biti usmjeren ne samo na nametanje obveza društvenim sektorima već i na poticaj svih sektora društva za usklađeni nastup kroz javno-privatno partnerstvo i razvoj nacionalnih sposobnosti i proizvoda koji će biti konkurentne na međunarodnoj razini, primarno kroz tržište EU-a, ali i na široj globalnoj razini.

Aktualni pristup EU-a u području kibernetičke sigurnosti započet je EU strategijom kibernetičke sigurnosti donesenom u veljači 2013. godine, u vrijeme kada Hrvatska još nije bila članica EU, a nastavljen je donošenjem NIS direktive o visokoj razini mrežne i informacijske sigurnosti, koja je nakon mukotrpne tri godine usuglašavanja stupila na snagu u kolovozu prošle godine. EU time dodatno otvara put za Hrvatsku, ne samo za provedbu nacionalnih obaveza RH kao države članice EU, već visok stupanj sličnosti između EU i RH koncepata upravljanja kibernetičkom sigurnošću može u narednom razdoblju doprinijeti konkurentnosti hrvatskog gospodarstva u području kibernetičke sigurnosti i korištenja kibernetičkog prostora, u kojem je najveći broj zemalja na početku razvoja širih nacionalnih sposobnosti. Potvrda uspješnosti i konzistentnosti hrvatskog pristupa području kibernetičke sigurnosti tijekom svibnja 2017. uočena je i kroz diskusiju zemalja članica EU-a o reviziji EU strategije kibernetičke sigurnosti iz 2013. godine, nakon čega je zaprimljen poziv predstavnika Francuske za uključenje Hrvatske u inicijativu manjeg broja zemalja članica okupljenih oko Francuske, vezano za pripremu izmjena EU strategije u drugoj polovini 2017. godine.

Aktualni pristup NATO-a temeljem sastanka na vrhu u Varšavi 2016. godine, u kojem je kibernetički prostor utvrđen kao domena vojnog djelovanja, u punom je suglasju s Nacionalnom strategijom kibernetičke sigurnosti RH, koja domenu kibernetičke obrane tretira kao sub-strategiju i dio vojne doktrine koji se oslanja na nacionalne resurse. Tako je i na aktualnu procjenu stanja kibernetičke sigurnosti u RH kao članici NATO-a, uspješno odgovoreno upravo kroz instrumente predviđene i uspostavljene Strategijom i pratećim povezanim aktima i odlukama Vlade RH te nacionalnim međuresornim tijelima.

Ključni izazov za izuzetno dinamično područje kibernetičke sigurnosti, gdje se nove ugroze pojavljuju svakodnevno, jeste učinkovita suradnja državnih tijela, akademskih institucija, regulatornih agencija, pravnih osoba i građana. Nacionalno vijeće za kibernetičku sigurnost

već je u prvom tromjesečju rada opravdalo ustrojavanje i dalo dodatni poticaj u nizu inicijativa i pozicioniranju RH u užoj i široj regiji, a pored toga bit će aktivno uključeno u pokretanje inicijativa prema svim dionicima hrvatske strategije u provođenju mjera Akcijskog plana i prepoznavanju nadležnosti i odgovornosti u kibernetičkom prostoru te će poticati razvijanje novih suradnji i novog partnerstva između dionika strategije iz različitih društvenih sektora.

Cilj strateških inicijativa u području virtualne dimenzije društva je rad na razvoju povećane otpornosti društva i različite komunikacijske i informacijske infrastrukture na suvremene ugroze kibernetičke sigurnosti, na otvaranju mogućnosti hrvatskog gospodarstva u ovom, globalno iznimno propulzivnom području, na stvaranju tehnološki osviještenog građanstva svih generacija putem poboljšanja edukacijskih programa i programa razvoja sigurnosne svijesti, kao i na stalnom podizanju stupnja digitalne higijene društva primjereno potrebama suvremenog hrvatskog društva.

5. ČLANOVI NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST

Rješenjem Vlade Republike Hrvatske od 16. veljače 2017. imenovani su predsjednik, zamjenica predsjednika, članovi i zamjenici članova Vijeća[11]:

Članovi Vijeća:

dr. sc. Aleksandar Klaić, dipl. ing. (predsjednik)
Dario Hrebak
Siniša Jurić
Bernard Gršić
Bernard Topić
Ružica Vučić
dr. sc. Petar Mihatov
Vedrana Šimundža Nikolić
Valentino Franjić
Dražen Ljubić
Mario Miljavac
Petar Vitas
Tomislav Štivojević
dr. sc. Dražen Lučić
Mato Mihaljević
Anto Rajkovača

Zamjenici članova Vijeća:

Marija Portner Marinković, dipl. iur.
Ante Orlović
mr. sc. Amir Muharemi
Božo Zeba
Željko Zubak
Maja Šmit, prof.
brigadir, mr. sc. Stanko Ćavar
Ana Kordej
dr. sc. Ivan Matić
Zvonimir Grubišić
Mirko Korajac
Maja Matijaš Filipović
mr. sc. Vlado Pribolšan
mr. sc. Mario Weber
Davor Đeker
Igor Vulje

Tajništvo Vijeća:
Suzana Galeković

Vinko Kuculo

[11] detaljni popis članova Vijeća s kontakt podacima dostavlja se za potrebe Vlade Republike Hrvatske odvojeno od ovog izvješća