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

GODIŠNJE IZVJEŠĆE O RADU

NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST

I

OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST

ZA 2020. GODINU

SADRŽAJ

1. SAŽETAK

I u normalnim okolnostima svakodnevice izuzetno je izazovno nositi se s prijetnjama u kibernetičkom prostoru i na njih pravovremeno reagirati i odgovarajuće odgovoriti, a tijekom nesigurne i nepredvidive 2020. to je postalo još izazovnije, dinamičnije i složenije. Potpuno je ispravno zaključiti kako nema mirne godine kad je kibernetička sigurnost u pitanju, kao i da su neke godine u pitanjima kibernetičke sigurnosti teže od drugih, što 2020. može s punim pravom potvrditi. Kad su prve informacije o SARS-COV-2 virusu obišle svijet, nitko zapravo nije mogao niti naslutiti njegove razmjere i dugotrajnost, a niti razmjere štete i ograničenja koja će nametnuti. Kako se virus sve brže širio, postajalo je sve jasnije da njegov utjecaj neće ostati nezamijećen. U takvim je okolnostima, kad je kibernetička sigurnost u pitanju, možda i najveći izazov tijekom 2020. bila organizacija rada od kuće, što je diljem svijeta, pa i u RH, povećalo udio onih kibernetičkih prijetnji i rizika koji mogu nanijeti najviše štete. A to je u svakom pogledu postavilo nove zadaće pred naše IT i sigurnosno osoblje, čime se 2020. može nazvati godinom transformacije u kibernetičkom svijetu.

Kibernetička pitanja od važnosti za državu i globalno okruženje predstavljaju puno šire područje od područja kibernetičke sigurnosti kojim se bavi Nacionalno vijeće za kibernetičku sigurnost i usko su povezana s nizom tradicionalnih resora državne uprave, dok kibernetička sigurnost u tim pitanjima predstavlja samo podlogu za njihov nesmetani razvoj u virtualnoj dimenziji suvremenog društva.

Kibernetička sigurnost dio je svih procesa državne uprave s obzirom da se svi procesi oslanjaju na ispravno funkcioniranje komunikacijsko-informacijskih sustava, bilo izravno, kroz obradu, pohranu i prijenos podataka, bilo posredno kroz upravljanje temeljnim uslugama (npr. distribucijom električne energije, promet itd.).

S obzirom na veliku raspršenost odgovornosti državnih tijela u kibernetičkom prostoru, uspostavom Nacionalnog vijeća za kibernetičku sigurnost uspostavljen je mehanizam dijeljenja informacija i usklađivanja postupanja državne uprave na stručnoj i političkoj/upravnoj razini.

1. UVOD

Nacionalno vijeće za kibernetičku sigurnost (dalje: Vijeće) započinje sa svojim radom 16. ožujka 2017. godine održavanjem prve konstituirajuće sjednice, slijedom Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Vijeća, a koje je donijela Vlada RH na sjednici održanoj 16. veljače 2017. godine. Odlukom Vlade RH od 22. ožujka 2018. godine proširen je sastav Vijeća s dva tijela – Ministarstvom mora, prometa i infrastrukture i Središnjim državnim uredom za razvoj digitalnog društva. Pripajanjem Državne uprave za zaštitu i spašavanje Ministarstvu unutarnjih poslova od 1. siječnja 2019. – sukladno Zaključku Vlade RH o smanjenju broja agencija, zavoda, fondova, trgovačkih društava, instituta, zaklada i drugih pravnih osoba s javnim ovlastima od 2. kolovoza 2018. – broj tijela u Vijeću čini njih 17, u kojem sastavu i danas djeluje („Narodne novine“, brojevi: 61/16, 28/18, 110/18, 79/19 i 136/20). Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u **Operativno-tehničkoj koordinaciji za kibernetičku sigurnost** (dalje: Koordinacija), koja započinje s radom 23. ožujka 2017. održavanjem prve sjednice[1].

Konstituiranjem Vijeća i Koordinacije otvoren je put za ostvarenje ciljeva Nacionalne strategije kibernetičke sigurnosti i punu provedbu mjera Akcijskog plana za njezinu provedbu („Narodne novine“, broj: 108/15 – dalje: **Strategija i Akcijski plan**).

Vijeće je međuresorno tijelo za koordinaciju horizontalnih nacionalnih inicijativa u području kibernetičke sigurnosti. Vijeće se primarno bavi ciljevima Strategije i mjerama Akcijskog plana te inicira rasprave i donosi preporuke i zaključke o svim aktualnim pitanjima povezanim s kibernetičkom sigurnošću. Vijeće djeluje kroz nominalne nadležnosti tijela i institucija čiji su predstavnici imenovani u rad Vijeća (prvenstveno državni sektor). Daljnjim radom nastojat će se dodatno unaprijediti i osnažiti uspostavljena formalna međusektorska koordinacija između državnog, akademskog, gospodarskog i javnog sektora, temeljeno na nastavku aktivnosti koje je Vijeće u proteklom razdoblju poduzelo kroz svoje aktivnosti i aktivnosti tijela koja sudjeluju u radu Vijeća.

Koordinacija je operativno međuresorno tijelo, uspostavljeno radi učinkovitije koordinacije aktivnosti prevencije i reakcije na ugroze kibernetičke sigurnosti. Koordinacija djeluje primarno u smislu komplementarnog pristupa tijela i institucija čiji su predstavnici imenovani u rad Koordinacije (prvenstveno državni sektor) u prevenciji i rješavanju sigurnosnih incidenata. Time se istovremeno usklađuje razvoj nacionalnih sposobnosti u kibernetičkom prostoru. Rad Koordinacije usmjerava Vijeće, a koordinira Ministarstvo unutarnjih poslova.

[1] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf;
https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

2. IZVJEŠĆE O RADU NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST U 2020. GODINI

2.1. SJEDNICE 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. Nakon nekoliko izmjena i dopuna Odluke o osnivanju Vijeća i Koordinacije, Vijeće čine predstavnici sljedećih 16 tijela:

1. Ured Vijeća za nacionalnu sigurnost (UVNS) (predsjednik),
2. Ministarstvo unutarnjih poslova (MUP) (član),
3. Ministarstvo vanjskih i europskih poslova (MVEP) (član),
4. Ministarstvo obrane (MORH) (član),
5. Ministarstvo pravosuđa i uprave (MPU) (član),
6. Ministarstvo gospodarstva i održivog razvoja (MGOR) (član),
7. Ministarstvo znanosti i obrazovanja (MZO) (član),
8. Ministarstvo mora, prometa i infrastrukture (MMPI) (član),
9. Središnji državni ured za razvoj digitalnog društva (SDURDD) (član),
10. Sigurnosno-obavještajna agencija (SOA) (član),
11. Zavod za sigurnost informacijskih sustava (ZSIS) (član),
12. Operativno-tehnički centar za nadzor telekomunikacija (OTC) (član),
13. Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (NCERT) (član),
14. Hrvatska regulatorna agencija za mrežne djelatnosti – HAKOM (član),
15. Hrvatska narodna banka (HNB) (član),
16. Agencija za zaštitu osobnih podataka (AZOP) (član).

Kako bi se osiguralo da sjednice Vijeća imaju dostatnu prisutnost članova potrebnu za donošenje zaključaka i odluka, sva navedena tijela i pravne osobe imenovala su i zamjenika člana Vijeća. Ministarstava koja su ustrojena za više upravnih područja povezanih s pitanjima kibernetičke sigurnosti mogu imenovati dva zamjenika člana, što su Ministarstvo unutarnjih poslova, Ministarstvo pravosuđa i uprave i Ministarstvo gospodarstva i održivog razvoja i učinili. U svrhu potpore opsežnim administrativnim i tehničkim poslovima koji proizlaze iz aktivnosti Vijeća, UVNS je, uz predsjednika i zamjenika predsjednika, odredio dodatne osobe koje sudjeluju u radu tj. administrativno-tehničkoj potpori radu Vijeća.

Tijekom 2020. godine Vijeće je održalo 8 sjednica, od kojih je šest održano u virtualnom/elektroničkom formatu. Tradicionalno održavanje sjednica nije bilo moguće uslijed pandemije uzrokovane SARS-COV-2 virusom, odnosno radi odgovarajućeg održavanja preporučenih protupandemijskih mjera, a potom i zbog posljedica potresa koji je u ožujku zadesio Zagreb. U mjesecima u kojima sjednice nisu održane (travanj, kolovoz, rujan i listopad), članovi Vijeća su razmjenjivali informacije iz područja kibernetičke sigurnosti, kako

bi svi relevantni dionici bili upoznati s trenutnim aktivnostima. ZSIS je, s ciljem povećanja sigurnosne svijesti korisnika i administratora sustava u okruženju rada od kuće i podešavanja informacijskih sustava za takav rad, izradio i distribuirao dva dokumenta: *Preporuke za siguran rad iz kućnog okruženja za korisnike* i *Preporuke za siguran rad iz kućnog okruženja za administratore*, kako bi svi bili upoznati s preporukama za zaštitu informacijskih sustava, kao i kako bi se osigurao kontinuitet poslovanja. Radi daljnjeg podizanja svijesti korisnika, UVNS i ZSIS su izradili brošuru *Savjeti za zaštitu osobnih uređaja od kibernetičkih napada* koja se odnosi na postupanje s osobnim uređajima (računala, dlanovnici, pametni telefoni, pametni satovi i sl.), a u cilju smanjenja rizika od kibernetičkih napada na takve uređaje koji imaju mogućnost povezivanja s internetom.

Sjednice su se održavale sredinom mjeseca, a elektroničke u trajanju od dva-tri dana. Na svim održanim sjednicama Vijeće je imalo kvorum. Svi zapisnici, dnevni redovi i zaključci sa sjednica Vijeća usvojeni su jednoglasno te dostavljeni svim članovima i zamjenicima članova radi planiranja i provedbe daljnjih/usuglašenih aktivnosti u vlastitim institucijama.

2.2. PREGLED AKTIVNOSTI VIJEĆA U 2020. GODINI

Vijeće je u 2020. godini nastavilo usmjeravati svoj rad prema Strategijom postavljenim ciljevima kibernetičke sigurnosti, prvenstveno kroz daljnji razvoj i poboljšavanje horizontalne komunikacije među tijelima koja sudjeluju u radu Vijeća ili su dionici provedbe Akcijskog plana. Uključenjem u rad Vijeća predstavnika MMPI-ja i SDURDD-a 2018. upotpunjena je zastupljenost svih državnih tijela s nadležnostima koje su vezane uz informacijsku i komunikacijsku domenu što se pokazalo dobrim iskorakom poglavito u provođenju aktivnosti povezanih s Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibernetičku sigurnost) te o kibernetičkoj sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibernetičkoj sigurnosti) te omogućavanje korištenja rezultata rada Vijeća u drugim međuresornim inicijativama, poput Koordinacije za sustav domovinske sigurnosti.

Zaključkom Vlade RH od 7. veljače 2019. o zaduženjima središnjih tijela državne uprave i drugih tijela za sudjelovanje u radu radnih skupina i odbora Vijeća EU-a, SDURDD je određen nositeljem Horizontalne radne skupine za kibernetička pitanja. Određena su i tri sloja unutar područja rada Horizontalne radne skupine za kibernetička pitanja po kojima će se kibernetička pitanja dalje razdjeljivati ovisno o tematici: za područje jedinstvenog digitalnog tržišta nositelj je SDURDD uz suradnju MGOR-a, za sigurnosnu uniju nositelj je MUP, a za digitalnu ekonomiju i društvo nositelj je MGOR uz suradnju sa SDURDD-om. Kibernetička pitanja, koja su predmet rada ove Horizontalne radne skupine, puno su šira od područja kibernetičke sigurnosti, ali se i na njih reflektiraju sigurnosni zahtjevi te su stoga od interesa za Vijeće, slijedom čega je jedna od stalnih točaka dnevnog reda sjednica Vijeća i informiranje Vijeća o aktualnim aktivnostima, nacionalnim i međunarodnim, u kibernetičkim pitanjima. Sva tijela iz Vijeća koja su nadležna za ova pitanja izvješćuju Vijeće o svojim aktivnostima te se time, osim

bolje međusobne obaviještenosti, doprinosi i boljoj i bržoj međusobnoj koordinaciji te nužnoj sinergiji u užem području rada Vijeća.

Akcijski plan za 5G strateška je inicijativa na razini Europske komisije koja se odnosi na sve dionike, privatne i javne, male i velike, u svim državama članicama, kako bi se odgovorilo na izazov da 5G do kraja 2020. godine postane stvarnost za sve građane, organizacije i tvrtke, tj. društvo u cjelini. U pitanjima provedbe sigurnosti 5G mreža u RH, HAKOM je nositelj i koordinator radne skupine Vijeća u kojoj sudjeluju MMPI, MVEP, SDURDD, UVNS, SOA, ZSIS, CARNet i OTC, a prema potrebi se mogu uključivati i predstavnici drugih tijela ili pojedine osobe s potrebnim ekspertizama. Višemjesečni intenzivan rad radne skupine u pitanjima sigurnosti 5G mreža kroz sudjelovanje u redovnim koordinacijskim sastancima na razini Europske komisije te s drugim državama članicama rezultirao je usvajanjem *paketa alata za 5G* (tzv. *Toolbox*) tijekom hrvatskog predsjedanja Vijećem EU-a u siječnju 2020. Ovim paketom alata utvrđen je mogući zajednički skup mjera te smjernice za njihov odabir vezano uz ublažavanje glavnih rizika za sigurnost 5G mreža, a s ciljem osiguranja odgovarajuće razine kibernetičke sigurnosti 5G mreža diljem EU-a te koordiniranog pristupa među državama članicama. Očekuje se da će u državama članicama 5G Toolbox biti implementiran do polovine 2021. godine. Radna skupina Vijeća za 5G, predvođena HAKOM-om, pripremila je inicijalnu analizu i razmatrala način implementacije tehničkih mjera iz Toolbox-a kroz pravilnik koji donosi Vijeće HAKOM-a. Ostaje još otvoreno pitanje implementacije dvije strateške mjere (osigurati raznovrsnost dobavljača i izbjegavanje ovisnosti o visoko rizičnim dobavljačima; jačanje otpornosti na nacionalnoj razini). Radna skupina će morati što ranije razmotriti i potvrditi prijedlog implementacije tehničkih i strateških mjera, odnosno njihovu primjenu, kako bi dionici na tržištu bili upoznati s prijedlogom pravila prije dodjele novih frekvencija za 5G.

U odnosu na američku inicijativu prema RH za potpisivanje bilateralnog MoU-a u vezi 5G [U.S.-Republic of Croatia Memorandum of Understanding [or Declaration] on 5G Security], Radna skupina Vijeća održala je u kolovozu 2020. sastanak te je zaključeno da RH prepoznaje rizik za zajednički način rješavanja pitanja sigurnosti 5G mreža u EU, a koji bi mogao proizaći iz potpisivanja spomenutog MoU-a. Zauzet je stav kako RH svakako treba pratiti i podržati zajednički nastup EU-a prema trećim zemljama.

Zaključcima Vijeća EU o promicanju uzajamnog priznavanja jačanjem uzajamnog povjerenja od 7. prosinca 2018., države članice i Komisija su pozvane prioritizirati uspostavu digitalnog sustava razmjene e-dokaza kao sigurnog načina slanja europskih istražnih naloga te zahtjeva i odgovora za uzajamnu pravnu pomoć. Europska komisija izrađuje sustav, odnosno aplikaciju za elektroničku razmjenu obrazaca europskih istražnih naloga iz Direktive 2014/41/EU Europskog parlamenta i Vijeća od 3. travnja 2014. o europskom istražnom nalogu u kaznenim stvarima, te zamolnicu za međunarodnu pravnu pomoć u svrhu pribavljanja odnosno razmjene elektroničkih dokaza (*e-Evidence Digital Exchange System*, skraćeno: e-EDES). Europska komisija razvoj e-EDES-a smatra jednim od apsolutnih prioriteta u području razvoja informacijskih tehnologija u pravosuđu, a o dosegnutom razvoju aplikacije izvješćuje na sastancima projektnog tima za uspostavu sustava razmjene elektroničkih dokaza (*Expert Group*

on the e-Evidence Digital Exchange system). Republika Hrvatska je, putem Ministarstva pravosuđe i uprave, sudjelovala u projektu EXEC (*Electronic Xchange of e-Evidences with e-CODEX,* 01.02.2018.-31.01.2020.), koji je omogućio pripremu nacionalnog informacijskog sustava (nadogradnjom tehničkih komponenti) za priključivanje e-EDES-u.

Od 1. siječnja 2019. do 30. lipnja 2020. godine Hrvatska je, uz Rumunjsku i Finsku, bila dijelom predsjedavajuće trojke Vijeća EU-a, pa tako i CSIRT mreže[2] i NIS Grupe za suradnju[3]. Za vrijeme hrvatskog presjedanja Vijećem EU-a, sastanci NIS Grupe za suradnju i sastanak CSIRT mreže, kojima su predsjedali UVNS i NCERT (uz zajednički blok za razmjenu informacija, iskustava i očekivanja), na kojima se očekivalo sudjelovanje oko 160 sudionika, trebao se održati u Zagrebu. No, zbog pandemije, sastanci su održani virtualnim putem.

Za vrijeme HR PRES-a funkciju predsjedanja HRS CYBER-om odradilo je Stalno predstavništvo RH pri EU, a HRS CYBER je započela s radom već 8. siječnja te je do kraja lipnja održala 23 sastanka (od toga 5 VTC), što je jedan više nego je prvotno bilo predviđeno programom. Što se tiče zakonodavnih akata, HR PRES je krajem siječnja predstavilo svoj kompromisni Prijedlog Uredbe o osnivanju Europskog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i Mreže nacionalnih koordinacijskih centara, a koji je jako dobro prihvaćen od strane DČ i EK.

Tijekom fizičkih sastanaka, a potom i pisanih konzultacija (u vrijeme COVID-19 krize), uspješno je okončana procedura usuglašavanja teksta revidiranog mandata za trijaloge te je isti potom jednoglasno usvojen na COREPER-u. Zahvaljujući dobrim kontaktima s EP i EK, RH je uspjela organizirati i prvi trijalog o novom revidiranom mandatu (ukupno treći u cijelom procesu), a koji je održan 25. lipnja 2020.

Drugi prominentni dosje tiče se 5G-a gdje je u siječnju 2020. prvo usvojen set alata za kibernetičku sigurnost 5G mreža (5G toolbox) u sklopu NIS Grupe za suradnju (također pod HR PRES-om). Potom je na razini NIS podgrupe za 5G (pod HR PRES-om) počelo praćenje provedbe implementacije mjera od strane DČ (sastanci su održavani i tijekom COVID-19) te je sukladno prvotnom planu izrađeno i izvješće o provedbi, a koje je predstavljeno na posljednjem sastanku Podgrupe za 5G pod HR PRES-om 30. lipnja. Nastavljen je i angažman oko WHOIS reforme te praćenje aktivnosti ICANN-a.

[2] CSIRT Network (CSIRT NW) osnovan je Direktivom o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). CSIRT NW se sastoji od imenovanih nacionalnih CSIRT-ova (CERT) tijela država članica, radi suradnje, izgradnje povjerenja i razmjene informacija u području rješavanje kibernetičkih incidenata; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[3] NIS Grupa za suradnju osnovana je Direktivom (EU) 2016/1148 radi osiguranja strateške suradnje i razmjene informacija između država članica.

Osim što je pod HR PRES-om održano dosad najviše sastanaka radne skupine u odnosu na sva dosadašnja Predsjedništva, u prvih šest mjeseci 2020. godine usvojeno je i više stajališta EU-a i Lines to take nego u protekloj godini, prvenstveno za procese u sklopu Prvog i Trećeg odbora Opće skupštine UN-a.

Prije i nakon sastanaka UN GGE-a organizirani su brifinzi predstavnika DČ iz glavnih gradova koji sudjeluju u radu tog odbora. Procesi u UN-u kao i kibernetičke restriktivne mjere bile su dominantne teme na području kibernetičke diplomacije, a objavljene su i dvije Deklaracije Visokog predstavnika u ime EU-a, prva u veljači kao odgovor na kibernetički napad na Gruziju, a u travnju druga kojom se osuđuju maliciozne kibernetičke aktivnosti u vrijeme pandemije korona virusa (obje su, uz velik trud HR PRES-a zbog zadrške nekih DČ dogovorene na razini HRS CYBER-a te jednoglasno usvojene na COREPER-u). Usprkos ograničenjima, uspješno je okončana i rasprava o prvim listiranjima u sklopu kibernetičkog sankcijskog režima. Na inicijativu HR PRES-a održan je i prvi ikad tematski sastanak HRS CYBER-a posvećen jednoj regiji, a koji je, s obzirom na prioritet HR PRES-a, bio posvećen kibernetičkoj sigurnosti na Zapadnom Balkanu.

Tijekom predsjedanja RH Vijećem EU-a, AZOP je bio nositelj provedbe tematske konferencije o zaštiti osobnih podataka koja je u siječnju održana u Zagrebu povodom europskog dana zaštite osobnih podataka te međunarodne konferencije „SPRING“ na kojoj su sudjelovala različita tijela država EU-a i pridruženih država kojima je djelatnost vezana uz zaštitu osobnih podataka.

SDURDD je, u koordinaciji s Europskom komisijom, organizirao Digitalnu skupštinu, online konferenciju za razmjenu mišljenja i najboljih praksi koje podupiru digitalnu transformaciju, potiču inovacije i suradnju u različitim javnim upravama, uključujući Europsku komisiju.

Europska komisija je trebala provesti u svim državama članicama, pa tako i (početkom travnja) u RH, informativni nadzor/konzultacije s ciljem sagledavanja statusa implementacije NIS Direktive (prenesene u nacionalno zakonodavstvo *Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*, „Narodne novine“, broj: 64/18) te održati zasebne sastanke s operatorima ključnih usluga iz svakog sektora[4], nadležnim sektorskim tijelima[5], CSIRT tijelima[6] te jedinstvenom nacionalnom kontaktnom točkom[7] u prostorima Europske komisije u Zagrebu. No, zbog ograničenja koja je nametnuo COVID, isto je provedeno online putem (web sastanci). Ukupan dojam i rezultat za RH po provedenim konzultacijama nije poznat jer o istom Europska komisija države članice nije povratno izvještavala, već su joj takva iskustva i razina provedbe poslužila kao početni temelj za reviziju NIS direktive s ciljem poboljšanja i jasnijeg definiranja odredbi i zahtjeva.

[4] Energetika (podsektori Električna energija, Nafta, Plin), Prijevoz (podsektori Zračni prijevoz, Željeznički promet, Vodni prijevoz, Cestovni promet), Bankarstvo, Infrastrukture financijskog tržišta, Zdravstveni sektor, Opskrba vodom za piće i njezina distribucija, Digitalna infrastruktura, Poslovne usluge za državna tijela
[5] MGOR, MMPI, HNB, HANFA, MZ, SDURDD
[6] NCERT, ZSIS
[7] UVNS

Tijela u Vijeću provode aktivnosti sukladno svojem djelokrugu i samostalno pa je tako SDURDD nositelj preuzimanja *Akta o kibernetičkoj sigurnosti*. Obveze iz Uredbe bi u nacionalnom zakonodavstvu trebale biti reflektirane u prvoj polovini 2021. godine. S tim povezano, ZSIS je sudjelovao, kao redovni član, na sastancima Europske grupe za kibernetičko sigurnosno certificiranje (ECCG). Europska komisija je pripremila prijedlog prve sheme za kibernetičku sigurnosnu certifikaciju (EUCC) te provedbeni akt koji ima pravnu snagu zakona na razini EU te će se sva certificiranja IKT proizvoda nadalje provoditi prema toj shemi.

U praćenje i rad na Prijedlogu uredbe Europskog parlamenta i Vijeća EU o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) aktivno je uključen AZOP. Europska komisija je usvojila prijedlog, predviđen Strategijom jedinstvenog digitalnog tržišta za jačanje povjerenja i sigurnosti na jedinstvenom digitalnom tržištu, čiji je cilj osigurati zaštitu temeljnih prava i sloboda, posebno prava na poštivanje privatnog života i komunikacija te zaštitu osobnih podataka u sektoru elektroničkih komunikacija. Prijedlog sadrži odredbe koje osiguravaju povjerljivost elektroničkih komunikacija, uključujući odredbe koje se odnose na zaštitu terminalne opreme korisnika, kao i odredbe o kontroli krajnjih korisnika nad njihovim elektroničkim komunikacijama. Dogovor nije postignut, pa je predsjedavajući Portugal predložio kompromisno rješenje kojeg je RH, uz većinu država članica, podržala.

MGOR je nacionalna točka za prijavu projekata po raspisanim natječajima u okviru CEF[8] Telecom Cybersecurity, a u okviru kojih je koordinirao prijave za nacionalne projekte. Samo je na posljednji natječaj u 2020. prijavljeno čak 19 hrvatskih projekata čime se, posredstvom aktivnosti Ministarstva, izravno doprinijelo podizanju razine svijesti problematike kibernetičke sigurnosti i sposobnosti za odgovor na kibernetičke prijetnje sa strane hrvatskih pravnih subjekata. Republika Hrvatska najuspješnija je baš u projektima kibernetičke sigurnosti. Slijedeće mogućnosti financiranja rješenja u području kibernetičke sigurnosti očekuju se kroz Digital Europe Programme[9] u narednom financijskom razdoblju.

MORH je, kao nositelj i nacionalni koordinator, krajem godine pokrenuo naredni ciklus izrade Samoprocjene sposobnosti iz obveza u području kibernetičke obrane kao dio obveza RH prema NATO-u (Cyber Defence Pledge), a kako bi se osiguralo pravovremeno i ravnopravno sudjelovanje svih nadležnih tijela. MORH je, nadalje, ispred RH pristupio Memorandumu o snagama za brze odgovore na kibernetičke napade (tzv. Cyber Rapid Reaction Response Teams) u sklopu PESCO (Permanent Structured Cooperation – Stalna strukturirana suradnja)

[8] CEF – Connecting Euope Facility, financijski instrument osnovan za dodatna ulaganja u izgradnju nove te unaprjeđenje postojeće prometne, energetske i telekomunikacijske infrastrukture, iz kojeg države članice, osim iz postojećih Strukturnih i Kohezijskog fondova, mogu financirati svoje projekte. Područja financiranja: Transport, Energija i Telekomunikacije.

[9] Program Europske komisije usmjeren na izgradnju strateških digitalnih kapaciteta EU-a i na olakšavanje široke primjene digitalnih tehnologija. S ukupnim proračunom od preko 8 mlrd eura, oblikovat će i podržati digitalnu transformaciju europskog društva i gospodarstva

projekta. PESCO je uspostavljen odlukom Vijeća EU-a krajem 2017., u području sigurnosne i obrambene politike, a nudi okvir za zajedničko planiranje, razvoj i ulaganje u projekte zajedničkih sposobnosti te poboljšanje operativne spremnosti oružanih snaga. Nakon potpisivanja Memorandum of Understanding (MoU) među članicama projekta (Hrvatska, Poljska, Litva, Rumunjska, Estonia, Nizozemska) u tijeku je usuglašavanje zemalja članica u drugom dijelu projekta (Mutual Assistance) povezano sa sadržajem Memoranduma u odnosu na CERT-EU[10].

ENISA, Europska agencija za kibernetičku sigurnost, svake godine provodi na razini EU-a i država članica kampanju podizanja svijesti o kibernetičkoj sigurnosti. Za te je potrebe bilo potrebno odrediti nacionalnu kontaktnu točku. S obzirom da se u ovim pitanjima prije svega radi o poslovima koje u svojem osnovnom opsegu poslova provode CERT tijela u državama članicama, ovu je ulogu preuzeo NCERT koji već niz godina provodi kampanje ovakvoga tipa u RH.

NIS Grupa za suradnju (NIS CG - NIS Cooperation Group) uspostavila je više radnih skupina koje se bave različitim pitanjima (primjerice, radnu skupinu za jačanje sposobnosti, digitalnu infrastrukturu, izvještavanje o incidentima, suradnju u prekograničnoj ovisnosti, itd), pa tako i Radnu skupinu za kibernetičke krize i incidente velikih razmjera (Working Stream 7 - WS7). Na temelju suglasnosti članova Vijeća i prethodno predloženih područja za novu Strategiju te plana rada Koordinacije za sustav domovinske sigurnosti, SOA je preuzela koordinaciju područja kibernetičkih kriza kao nadležno tijelo ispred RH slijedom čega je predstavnik SOA-e sudjelovao na (online) sastancima NIS CG radne skupine WS7 u okviru koje se do kraja drugog kvartala 2020. uspostavila nezavisna CyCLONe (Cyber Crisis Liaison Organisation Network) radna skupina za upravljanje kibernetičkim krizama na taktičkoj razini EU-a. CyCLONe organizacija predstavlja operativnu razinu upravljanja EU kibernetičkim krizama uspostavljenu s ciljem praćenja i koordinacije tehničke razine upravljanja kibernetičkim krizama (CERT/CSIRT tijela) te u svrhu boljeg razumijevanja i prevođenja složene tehničke problematike u operativni utjecaj i situacijsko stanje razumljivo za političko-stratešku razinu odlučivanja (EU IPCR – Integrated Political Crisis Response). Radi izrade i usuglašavanja nacionalnog koncepta upravljanja kibernetičkim krizama, SOA je u listopadu 2020. formirala međuresornu stručnu radnu skupinu (MORH, MUP, ZSIS, NCERT, HAKOM i HNB) na kojoj je prezentiran prijedlog nacionalnog pristupa upravljanju kibernetičkim krizama.

Ministarstvo pravosuđa i uprave, nadležno za državnu informacijsku infrastrukturu i ključne projekte, nadležno je za koordinaciju elektroničkih usluga koje razvijaju tijela javnog sektora korištenjem državne informacijske infrastrukture, odnosno njenih komponenti. Uz projekt e-Poslovanje, koji će omogućiti jedinstveni pristup elektroničkim uslugama za poslovne korisnike, razvija se projekt kao što je e-Pristojbe – projekt kojim će se povećati dostupnost javnih usluga na način da će se uvesti elektronička naplata upravnih pristojbi i naknada u

[10] Tim za brzi odgovor na računalne incidente za institucije, tijela i agencije EU-a, sastavljen od eksperata iz vodećih EU institucija. Surađuje s drugim CERT timovima država članica, kao i specijaliziranim tvrtkama za IT sigurnost, kako bi pravodobno odgovorio na sve kibernetičke prijetnje i incidente

postupcima i procedurama za koje je propisana njihova naplata što će omogućiti daljnji razvoj složenijih elektroničkih usluga u sustavima e-Građani i e-Poslovanje. Započelo se i s implementacijom projekta e/m-Potpis i e/m-Pečat kojom će se bitno olakšati poslovanje u javnoj upravi. Projektom će se razviti i uspostaviti platforma s elektroničkim uslugama za proces elektroničkog i mobilnog potpisivanja, elektroničkog i mobilnog pečatiranja te provjeru valjanosti elektroničkog potpisa odnosno pečata, koji će se koristiti u elektroničkim javnim uslugama i biti dostupni sudionicima u okviru elektroničkog poslovanja tijela državne i javne uprave.

Osim postojeće kompleksne usluge e-Novorođenče, razvija se i podrška odnosu roditelj/skrbnik-dijete te e-Ovlaštenja koja će, ustvari, biti nadogradnja NIAS-a (Nacionalni identifikacijski i autentifikacijski sustav) u okviru e-Poslovanja i kojom će biti podržane punomoći i zastupanja. S obzirom na važnost i značajan potencijal u broju korisnika elektroničkih usluga u sustavu obrazovanja, također se radi i na razvoju složene e-usluge e-Upisi u odgojne i obrazovne ustanove itd.

Uspostavom Centra dijeljenih usluga (CDU), kao strateškim projektom Vlade RH, vrijednim ukupno 361 milijun kuna, koji se u iznosu do 85% sufinancira iz Europskog fonda za regionalni razvoj preko Operativnog programa Konkurentnost i kohezija, uspostavlja se državni oblak, koji predstavlja informacijski servis namijenjen tijelima državne uprave i institucijama javnih službi. CDU tijelima državne uprave nudi usluge infrastrukture, platforme i aplikacija u modelima: Iaas (infrastruktura kao servis), PaaS (platforma kao servis), SaaS (softver kao servis). Država će kroz CDU dobiti brži pristup najnovijim tehnologijama koje su osnova za pružanje većeg broja digitalnih usluga javne uprave na što efikasniji način i u što kraćem roku. Do sada je više od 30 tijela započelo s korištenjem CDU-a. Ne radi se tu samo o migraciji postojećih usluga, već i o uspostavi virtualne infrastrukture u CDU-u koja na taj način postaje dijelom lokalne mreže korisnika čime korisnik dobiva u potpunosti sigurnu i georeduntantno zaštićenu infrastrukturu. Pojedina tijela su u CDU-u tako uspostavila više usluga od kojih su migrirane neke postojeće ili uspostavljene potpuno nove. Ovdje nije riječ samo o ministarstvima, već je izrazit interes zdravstvenog sektora gdje pojedine bolnice uspostavljaju nove sustave u sklopu CDU.

MPU povelo je zajedno s nadležnim institucijama projekt kreiranja digitalnog pomoćnika koji je dostupan na https://andrija.ai. Riječ je o računalnom programu koji automatizira komunikaciju s građanima oko pojedinih pitanja borbe protiv koronavirusa te može dovoljno brzo i učinkovito građanima pružiti aktualne informacije i preporuke. Na kreiranju rješenja radio je tim stručnjaka predvođen epidemiologom prof. dr. sc. Brankom Kolarićem, uz tehničku i informatičku podršku udruženih domaćih tvrtki Mindsmiths, Neos i Oracle Hrvatska, a koje su uz Infobip, članice Hrvatske udruge za umjetnu inteligenciju CroAI.

RH je potpisom deklaracije 29. studenoga 2019. pristupila inicijativi za stvaranje nove generacije komunikacijske mreže znatno povećane sigurnosti EuroQCI (European Quantum Communication Infrastructure). Temeljem zahtjeva EK, svaka od 24 uključene države je

morala, najkasnije do 1. lipnja 2020., u svoj tim imenovati i predstavnika iz sektora nacionalne sigurnosti. S tim u vezi, a na traženje predstavnika RH za EuroQCI (Institut Ruđer Bošković), u hrvatski tim je, u ovoj fazi, imenovan predstavnik UVNS-a. Sukladno razvojnim fazama, u inicijativu će se uključivati i druge sastavnice nacionalne sigurnosti. U inicijativu je također uključen i predstavnik CARNET-a - NCERT-a.

Situaciju nastalu SARS-COV-2 virusom značajnije su obilježile inače konstantno prisutne phishing kampanje, vrlo često lokalizirane na hrvatski jezik, koje lažnim prikazivanjem svrhe pokušavaju putem elektroničke pošte prikupiti osobne podatke građana i/ili podatke o njihovom elektroničkom identitetu s pripadajućim lozinkama. Registrirane su brojne nove internetske domene, poput internetske domene www.samoizolacija.hr, s ciljem prikupljanja osobnih podataka građana, a navodno u svrhu zaprimanja dojava građana o osobama koje postupaju protivno određenim posebnim mjerama samoizolacije, odnosno protuepidemijskim mjerama. Registrirani su deseci lažnih web-shopova na *.hr* domeni koji nude obuću i odjeću poznatih modnih *brand*-ova u cilju prijevare kupaca i prikupljanja osobnih podataka građana. U svim je takvim situacijama, kao što to i redovno čini, MUP putem Službe za odnose s javnošću izdavao medijska priopćenja u kojima se građane upozorava na prijetnje te ih se upućuje kako se samozaštitno ponašati.

Značajniji incidenti za vrijeme prvog vala COVID-a, koje je CARNET-NCERT detektirao, su DDoS napadi na e-learning infrastrukturu u trenutku prelaska na učenje od kuće, prekid u radu kod pružatelja internetskih usluga (ISP) radi požara uzrokovanog potresom, širenje malicioznih privitaka putem COVID-19 tematskih mailova, spam poruke (prodaja maski, dezinficijensa itd.). U odnosu na brzu intervenciju i rješavanje incidenata, ocjenjuje se da napadi u ovim okolnostima nisu imali velik utjecaj na krajnje korisnike pod nadležnošću Nacionalnog CERT-a, koji redovito izdaje preporuke i upozorenja na svojim stranicama i društvenim mrežama za zainteresiranu javnost.

Tijela u Vijeću sad već tradicionalno sudjeluju u međunarodnim kibernetičkim vježbama, no tijekom 2020. značajan broj planiranih vježbi nije održan (primjerice, na razini EU-a *CyberEurope* i *SOPEx* ili nacionalna *Kibernetički štit*), već je odgođen za 2021. godinu. Tijekom 2020. godine tijela su sudjelovala u NATO vježbi *Cyber Coalition 2020,* koja je imala za cilj uvježbati koordinaciju između nacionalnih i NATO-ovih tijela prilikom odgovora na zajedničke kibernetičke prijetnje i incidente u kibernetičkom prostoru članica NATO saveza; potom u vježbi *Blue OLEx 2020* u području upravljanja kibernetičkim krizama. Dvije ključne teme vježbe bile su službeno pokretanje EU CyCLONe organizacije i plan EK o osnivanju Joint Cyber Unita (JCU). NCERT po prvi je puta sudjelovao u International CyberEx-u, CTF (Capture the Flag) natjecanju u organizaciji OAS-a (*Organization of American States*), INCIBE-a (*Spanish National Cybersecurity Institute*) i CNPIC-a (*Spanish National Centre for Infrastructure and Cybersecurity*), čiji je cilj jačanje sposobnosti odgovora na računalno-sigurnosne incidente. Vježba je obuhvatila područja kriptografije, digitalne forenzike, reverznog inženjerstva, web sigurnosti i srodnih područja.

Suradnja s Koordinacijom za sustav domovinske sigurnosti odvijala se putem predstavnika tijela u Vijeću. U skladu s Godišnjim planom rada Koordinacije za sustav domovinske sigurnosti za 2020. godinu, ZSIS je u okviru Specifičnog cilja 6., „*Razvitak sposobnosti kibernetičkog djelovanja u okviru sustava domovinske sigurnosti*“ proveo sve postavljene zadaće, a pojedini segmenti su prepoznati kao osnova za daljnje inicijative i projekte podizanja sigurnosti kibernetičkog prostora RH.

Na inicijativu i u organizaciji MVEP-a i SPRHEU-a održavani su neformalni virtualni brifinzi o statusu pripreme Kibernetičkog paketa.

Tijekom 2020. Vijeće je pratilo i aktualne teme država članica i institucija EU-a u kibernetičkim pitanjima, a naglasak je stavljen na podizanje svijesti državnih tijela o njihovim izvornim nadležnostima koje je nužno primijeniti i na kibernetički prostor.

2.3. NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI I AKCIJSKI PLAN ZA NJEZINU PROVEDBU

Odmah po donošenju Zaključka Vlade RH od 22. kolovoza 2019. kojim se Vijeće zadužuje do kraja 2019. godine dostaviti Vladi RH prijedlog nove Strategije i pripadnog Akcijskog plana, Vijeće je pristupilo izradi izmjena i dopuna Strategije. Za te su potrebe izrađene i distribuirane *Smjernice za provedbu ažuriranja Strategije i Akcijskog plana*, s naznakom dionika procesa ažuriranja, rokova provedbe, uz opis potrebnih ažuriranja u odnosu na status ispunjenja pojedinih mjera i nove pojave i trendove sigurnosnih rizika u kibernetičkom prostoru te obavezno sagledavanje razvoja informacijske i komunikacijske tehnologije.

Nakon procesa ažuriranja u koji su bili uključeni svi relevantni dionici, Vladi RH je u veljači 2020. dostavljen prijedlog ažurirane Strategije i Akcijskog plana radi ishođenja suglasnosti za provođenje prethodnog postupka sa zainteresiranom javnosti. U međuvremenu su, a prije kraja godine, Europska komisija i Visoki predstavnik Unije za zajedničke vanjske poslove i sigurnosnu politiku predstavili Kibernetički paket (The Cyber Package) – novu Strategiju kibernetičke sigurnosti EU, prijedlog revidirane NIS Direktive i Direktivu o otpornosti kritičnih subjekata. Strategijom se želi ojačati europska kolektivna otpornost na kibernetičke prijetnje i osigurati da svi građani i poslovni subjekti mogu u punom opsegu imati koristi od pouzdanih i digitalnih alata. Bilo da se radi o povezanim uređajima, električnoj mreži ili bankama, avionima, javnim upravama i bolnicama, Europljanima koji to često koriste mora se dati jamstvo da će to koristiti zaštićeni od kibernetičkih prijetnji. Komisija nadalje daje prijedloge kojima se adresiraju i kibernetička i fizička otpornost kritičnih subjekata i mreža u okviru revizije NIS Direktive (Directive on measures for high common level of cybersecurity across the Union – ‘NIS 2') i nove Directive on the resilience of critical entities (Direktiva o otpornosti kritičnih subjekata) koje obuhvaćaju širok spektar sektora i usmjerene su na buduće online i offline rizike, od kibernetičkih napada do kriminala i prirodnih katastrofa, na koherentan i komplementaran način.

Kako do predstavljanja Kibernetičkog paketa još uvijek nije bio pokrenut postupak savjetovanja sa zainteresiranom javnošću, Vijeće je na sjednici u prosincu 2020. donijelo jednoglasan zaključak da se prijedlog teksta nove Strategije povuče iz postupka te se, s obzirom na novu EU kibernetičku strategiju i reviziju NIS Direktive, prijedlog teksta Strategije i Akcijskog plana dodatno ažurira.
Slijedom toga se odmah pristupilo dodatnom ažuriranju Strategije, slijedeći ciljeve Strategije kibernetičke sigurnosti EU-a, za koje su procese pripremljene i distribuirane smjernice za reviziju prema poglavljima Strategije, odnosno nositeljima pojedinih područja koja se Strategijom obuhvaćaju (primjerice, MVEP za vanjske poslove, MUP za kibernetički kriminalitet, MZO za obrazovanje, itd.).

Kao jedan od temeljnih dokumenata, pored Strategije kibernetičke sigurnosti EU-a koja se koristi u procesu revizije, je i dokument ENISA-a, objavljen u prosincu 2020., *National Capabilities Assessment Framework* čija je primarna svrha usmjeravanje razvoja nacionalnih kapaciteta država članica za metodično organiziranje i provedbu samoprocjene zrelosti nacionalnih sposobnosti u području kibernetičke sigurnosti. Razrada metodologije temelji se na pretpostavci o postojanju zajedničkih, uobičajenih, strateških ciljeva koje države članice razrađuju u svojim nacionalnim strategijama kibernetičke sigurnosti. Svrha toga je jednoznačno, mjerljivo i komparabilno ocijeniti sposobnosti na razini EU-a. Pri raščlambi postojećih nacionalnih strategija utvrđeno je 15 zajedničkih strateških ciljeva s 49 užih ciljeva, na što su u konačnici dodana još 2 nova strateška cilja te je sve grupirano u 4 temeljna područja. Ovom revizijom se, pored usklađenja promišljanja s onima ostalih članica EU-a, usklađuju i nacionalni ciljevi međuresornom koordinacijom na način da će se nacionalni ciljevi i mjere mapirati na ovaj sada 51 cilj, a potom će se pristupiti drugom koraku u reviziji, a to je razrada preostalih ciljeva koji možebitno prethodno nisu bili dotaknuti.

Očekivani rezultat ažuriranja su nova Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njezinu provedbu koji se temelje na ovdje opisanoj metodologiji razrade strategije i korištenju elementima postojeće Strategije i Akcijskog plana te na strukturnim i sadržajnim promjenama koje je potrebno unijeti, uključujući i moguće otvaranje novih poglavlja u Strategiji.

3. IZVJEŠĆE O RADU OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST U 2020. GODINI

Vlada Republike Hrvatske je na sjednici održanoj 7. listopada 2015. godine donijela Odluku o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (Klasa: 022-03/15-07/81, Urbroj: 50301-09/09-15-5). Spomenuta Odluka, Strategija i Akcijski plan objavljeni su u Narodnim novinama, broj 108/2015 od 9. listopada 2015. godine.

U cilju provođenja Nacionalne strategije kibernetičke sigurnosti Vlada Republike Hrvatske je, temeljem članka 24. stavaka 1. i 3. Zakona o Vladi Republike Hrvatske (»Narodne novine«, br. 150/11 i 119/14), na sjednici održanoj 8. lipnja 2016. godine donijela Odluku o osnivanju Nacionalnog vijeća za kibernetičku sigurnost (u daljnjem tekstu: Nacionalno vijeće) i Operativno-tehničke koordinacije za kibernetičku sigurnost (u daljnjem tekstu: Operativno-tehnička koordinacija).

Prva, konstituirajuća sjednica Operativno-tehničke koordinacije održana je 23. 3. 2017. godine.

Zadaće Operativno-tehničke koordinacije propisane su člankom III. Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, kako slijedi:

- 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.

Administrativne i tehničke poslove za potrebe rada Operativno-tehničke koordinacije obavlja Ministarstvo unutarnjih poslova.

Sastav Operativno-tehničke koordinacije čine:

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

3.1. SJEDNICE OPERATIVNO-TEHNIČKE KOORDINACIJE

Tijekom 2020. godine bilo je planirano održavanje 12 sjednica Operativno-tehničke koordinacije, no dvije sjednice (ožujak i travanj) nisu održane zbog zbog pandemije virusa Covid-19. Tri su sjednice održane su kao virtualne sjednice putem Cisco Meeting aplikacije.

3.2. PREGLED AKTIVNOSTI OPERATIVNO-TEHNIČKE KOORDINACIJE U 2020.

Planom aktivnosti Operativno-tehničke koordinacije za 2020. godinu bilo je predviđeno provođenje slijedećih aktivnosti:

1. Praćenje stanja sigurnosti nacionalnog kibernetičkog prostora u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu, rok: tijekom 2020. godine
2. Predlaganje planova postupanja u kibernetičkim krizama, rok: tijekom 2020. godine
3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2020. godini, rok: kvartalno – ožujak, lipanj, rujan i prosinac 2020. godine
4. Izrada izvješća o provedbi mjera Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, rok: ožujak 2020. godine
5. Procjena stanja kibernetičke sigurnosti u Republici Hrvatskoj na temelju podatka dobivenih provedbom dokumenta Metodologija procjene stanja kibernetičke sigurnosti RH, rok: prosinac 2020. godine
6. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj, rok: prosinac 2020. godine
7. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2020. godinu, rok: siječanj 2021. godine.

Operativno – tehnička koordinacija je tijekom 2020. godine provela zadaće iz Plana aktivnosti, kako slijedi:

1. Praćenje stanja sigurnosti nacionalnog kibernetičkog prostora u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu.

   Operativno-tehnička koordinacija redovito prati stanje sigurnosti u svrhu otkrivanja prijetnji koje bi mogle imati za posljedicu kibernetičku krizu. U praćenju događaja u kibernetičkom prostoru Operativno-tehnička koordinacija se posebno oslanja na informacije CARNET-ovog NCERT-a i CERT-a ZSIS-a, a preporuke i upute za javnost za slučaj prijetnje objavljuju na službenim stranicama MUP i CARNET – NCERT.

   Tijekom 2020. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru Republike Hrvatske. Članovi Operativno-tehničke koordinacije tijekom redovnih sjednica najčešće su prijavljivali pojedinačne slučajeve slijedećih

incidenata: phishing, phishing URL, malware URL, web defacement, pogađanje zaporki, te zaraze pojedinačnih računala malicioznim kodom.

2. Predlaganje planova postupanja u kibernetičkim krizama.

   Tijekom nekoliko radnih sastanaka Operativno-tehničke koordinacije u prvoj polovini 2020. bila je razmatrana izrada planova postupanja u kibernetičkim krizama. Polovinom 2020. godine predstavnici SOA-e prezentirali su na sastanku Operativno-tehničke koordinacije novi koncept upravljanja kibernetičkim krizama. Ovaj prijedlog SOA-e prethodno je, krajem 2019. godine, usuglašen na NVKS-u i uključen u novi prijedlog NSKS-a. Dodatno je ovaj prijedlog SOA-e usvojen i na Koordinaciji za domovinsku sigurnost te je uključen u Plan rada Operativno – tehničke koordinacije za 2020. godinu, koji je u prosincu 2019. odobrilo i Vijeće za nacionalnu sigurnost. Na taj način je daljnju obavezu oko predmetnog područja i izrade standardnih procedura za nacionalno upravljanje kibernetičkim krizama preuzela SOA.

   SOA je u tu svrhu razradila nacionalni koncept upravljanja kibernetičkim krizama te ga uskladila s aktualnim pristupom EU-a i NATO-a, a na temelju suglasnosti NVKS-a, SOA se kao nadležno tijelo RH u proljeće 2020. uključila u EU CyCLONe organizaciju za upravljanje kibernetičkim krizama. U svrhu usuglašavanja i razrade predloženog nacionalnog koncepta upravljanja kibernetičkim krizama, SOA je u listopadu 2020. formirala međuresornu stručnu radnu skupinu u koju su pozvani predstavnici ključnih tijela za predmetno područje (MORH, MUP, ZSIS, NCERT, HAKOM i HNB). Na prvom sastanku ove međuresorne stručne radne skupine, održanom u studenom 2020. godine, SOA je prezentirala prijedlog nacionalnog pristupa upravljanju kibernetičkim krizama i Centar za kibernetičke tehnologije SOA-e. Na sastanku je usuglašen plan rada međuresorne radne skupine za 2021. godinu, a zaključci sastanka s prikazom usuglašenog pristupa i plana rada dostavljeni su polovinom studenog 2020. godine čelnicima i predstavnicima svih institucija uključenih u SOA-inu međuresornu stručnu radnu skupinu za upravljanje kibernetičkim krizama.

3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2020. godini.

   Izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske izrađuju se tromjesečno i redovito se dostavljaju Nacionalnom vijeću za kibernetičku sigurnost. Vijeću se dostavljaju i mjesečna izvješća o najznačajnijim incidentima i prijetnjama s prikazom trendova prijetnji.

4. Izrada izvješća o provedbi mjera Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti.

Tijekom 2019. godine započeto je ažuriranje Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti. Prijedlog ažurirane Nacionalne strategije i pripadnog Akcijskog plana je do kraja 2019. godine Nacionalno vijeće za kibernetičku sigurnost trebalo dostaviti Vladi Republike Hrvatske na usvajanje. Kako do sad Nacionalna strategija i pripadni Akcijski plan nisu usvojeni, ove godine nisu izrađena izvješća o provedbi mjera iz Akcijskog plana iz nadležnosti Koordinacije.

Niže su navedene mjere koje su bile u nadležnosti Operativno-tehničke koordinacije do ažuriranja Nacionalne strategije i pripadnog Akcijskog plana:

- Mjera D.5.1: *Provesti analizu kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza kao dijelu nacionalnog sustava upravljanja u krizama*

  Nisu definirana postupanja državnih tijela u slučajevima kibernetičkih kriza. U Zakonu o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga propisani su CSIRT-ovi za sektore ključnih usluga (što ne predstavlja popis i analizu kapaciteta) te jedinstvena nacionalna kontaktna točka.

- Mjera D.5.2: *Utvrditi kriterije za definiranje pojma kibernetičke krize u okviru šireg koncepta nacionalnog upravljanja u krizama, kao i kriterije za utvrđivanje/proglašavanje kibernetičke krize*

  U Zakonu o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga, te Uredbi definiran je incident koji ima znatan učinak na kontinuitet usluge (nije definirana kibernetička kriza). U Nacionalnoj taksonomiji računalno-sigurnosnih incidenata definiran je općeniti pojam kibernetička kriza, ali nije definirano točno kako se utvrđuje, kada ona nastaje i koji su kriteriji. Nije definiran pojam kibernetička kriza u okviru šireg koncepta nacionalnog upravljanja krizama. Nisu definirani kriteriji za proglašenje kibernetičke krize.

- Mjera D.5.3: *Izrada planova postupanja u kibernetičkim krizama i njihovo kontinuirano ažuriranje*

  Trenutačno ne postoje planovi postupanja u kiberentičkim krizama. Formirana je međuresorna radna skupina za upravljanje kibernetičkim krizama koja ima za zadaću u 2021. godini izraditi SOP za upravljanje kibernetičkim krizama.

5. Procjena stanja kibernetičke sigurnosti u Republici Hrvatskoj na temelju podatka dobivenih provedbom dokumenta Metodologija procjene stanja kibernetičke sigurnosti RH.

   Metodologija procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj dovršena je krajem prošle godine i usvojena je na Nacionalnom vijeću za kibernetičku sigurnost čime je omogućena procjena stanja kibernetičke sigurnosti u kibernetičkom prostoru Republike

Hrvatske. Vijeću je predložen model sustava samoprocjene u tijelima pojedinih sektora koji je i prihvaćen, te su u cilju procjene stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora procjenjena stanja kibernetičke sigurnosti po sektorima.

Planom Aktivnosti Operativno – tehničke koordinacije za kibernetičku sigurnost za razdoblje od 01.07.2020. do 31.12.2020. godine predviđeno je ažuriranje podataka koji su dobiveni u postupku procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj na temelju dokumenta Metodologija procjene stanja kibernetičke sigurnosti RH. Kako je proteklo relativno kratko vrijeme od posljednje procjene, koja je izvršena krajem siječnja 2020. godine, članovi OTKKS-a su zaključili da se zakonska regulativa nije i vjerojatno neće uskoro mijenjati, a ni prijetnje u kibernetičkom prostoru nisu se promijenile u dovoljnoj mjeri da bi isti mogli bitnije utjecati na prethodno procijenjeno stanje kibernetičke sigurnosti u kibernetičkom prostoru Republike Hrvatske.

6. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj.

   Ova zadaća je preuzeta iz Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, kao stalna zadaća Operativno-tehničke koordinacije. Posljednja procjena stanja kibernetičke sigurnosti i pripadno Izvješće napravljeni su temeljem Metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj početkom 2020 godine.

Jedna od odrednica 2020. godine svakako je globalno premještanje ključnih sigurnosnih procesa u kibernetički prostor, dijelom kao rezultat aktualne COVID-19 pandemije, ali ponajviše kao posljedica brzog tehnološkog razvoja. Stoga su globalni sigurnosni procesi i trendovi u velikom djelu danas uvjetovani razvojem novih tehnologija koje donose nove rizike i izazove. Takve nove tehnologije traže osposobljenost sigurnosnih institucija, a primjeri su računalstvo u oblaku (Cloud), mobilne 5G mreže, ili Internet stvari (Internet of Things – IoT), kao i čitav niz područja na koje ove disruptivne tehnologije izravno utječu, poput pametnih gradova ili autonomnih vozila.

Rezultat svih ovih promjena je da današnji kibernetički napadi imaju sve veći udio državno sponzoriranih napada, da postaju sve složeniji i učestaliji, a štete koje uzrokuju su sve veće. Ovakvi napadi imaju za cilj ne samo krađu podataka (državna i industrijska špijunaža), već i stvaranje štete na kritičnoj infrastrukturi, kao i financijske iznude i krađe, što je uvelike olakšano mogućnostima prikrivanja napadača i njihovom geografskom raspršenosti. COVID-19 pandemija poslužila je kao dodatni obrazac za kibernetičke napade u segmentu državno sponzoriranih kibernetičkih napada kroz prateću utrku u razvoju cjepiva, ali i kao novi instrument djelovanja organiziranog kriminala kroz financijske iznude i krađe. U konačnici to je tijekom 2020. donijelo i prve javne EU atribucije kibernetičkih napada državnih i drugih aktera iz Ruske Federacije, NR Kine i Sjeverne Koreje, praćenih EU gospodarskim sankcijama

niza atribuiranih entiteta (30.7.2020., Official Journal of the European Union, L 246/12 i 22.10.2020., Official Journal of the European Union, L 351 I).

Globalne kibernetičke prijetnje u stalnom su porastu, a sve veći broj sofisticiranih kibernetičkih napada, uz rastuću ovisnost suvremenog društva o kibernetičkoj tehnologiji, traži nove pristupe. Republika Hrvatska je, posebice kao članica NATO-a i EU-a, meta državno sponzoriranih kibernetičkih napada koji su temeljito planirani, napredni i ustrajni (APT - Advanced Persistent Threat) i koje obilježava visoka razina stručnosti i prikrivenosti počinitelja napada u dužem razdoblju. Zamjetan je i trend korištenja složenih taktika, tehnika i procedura APT napada u okviru organiziranih kriminalnih skupina koje kibernetički prostor koriste u cilju financijskih iznuda (ransomware) ili za malverzacije u financijskom sektoru.

Stoga je SOA, u suradnji s drugim nadležnim nacionalnim tijelima, započela opsežan proces prevencije i zaštite nacionalnog kibernetičkog prostora. U okviru ovog procesa, SOA je krajem 2019. godine uspostavila Centar za kibernetičke tehnologije[11]. Cilj uspostave Centra je zaštita nacionalnog kibernetičkog prostora od državno sponzoriranih kibernetičkih napada i APT kampanja pomoću mreže senzora smještenih u tijelima koja se štite. Time je omogućeno otkrivanje sofisticiranih kibernetičkih napada u najranijim fazama napada i u bilo kojem segmentu kibernetičkog prostora koji pokriva mreža senzora. Ovakav pristup povezuje najsloženije tehničke sustave za zaštitu kibernetičkog prostora i sigurnosno-obavještajne sposobnosti, s ciljem otkrivanja, sprječavanja i atribucije državno sponzoriranih kibernetičkih napada i APT kampanja usmjerenih protiv Republike Hrvatske, čime se bitno smanjuje rizik kompromitacije ključnih nacionalnih informacijskih resursa.

Kibernetički APT napadi usmjereni su na pažljivo odabrane i pomno proučene ciljeve, a provode ih organizirane hakerske skupine koje se povezuje s obavještajnim sustavima pojedinih država. Republika Hrvatska je posljednjih godina bila meta više desetaka kibernetičkih APT napada. SOA danas, nakon uspostave Centra za kibernetičke tehnologije, putem mreže senzora na dnevnoj bazi registrira nekoliko stotina tisuća sigurnosno indikativnih događaja, koji se rješavaju procesom trijaže u suradnji s više nacionalnih tijela koja imaju različite funkcionalne ili sektorske nadležnosti. Tako je tijekom 2019. godine detektirano i zaustavljeno više sofisticiranih državno sponzoriranih kibernetičkih APT napada, među kojima su bili i napadi na ministarstva vanjskih i europskih poslova te obrane. Trend kibernetičkih APT napada na Republiku Hrvatsku u 2020. godini bio je značajno intenzivniji od 2019. godine, a dodatno je pojačan različitim načinima iskorištavanja pandemije COVID-19 za provedbu kibernetičkih napada.

Kao i prošlih godina i dalje se bilježi uzlazni trend različitih kibernetičkih aktivnosti koje se svrstavaju u područje kibernetičkog kriminala. Pri tome je i globalni trend korištenja složenih taktika i tehnika APT napada za kibernetičke napade na poslovne sustave strateških i velikih

[11] https://www.soa.hr/files/file/Javno-izvjesce-2019.pdf

kompanija stigao u Republiku Hrvatsku kroz kibernetički napad na naftnu kompaniju INA-u u veljači 2020. Stoga je SOA-in Centar za kibernetičke tehnologije i projekt zaštite nacionalnog kibernetičkog prostora, iako primarno orijentiran na državni i javni sektor, otvoren i za druge sektore.

U cilju uvođenja sustavnog pristupa u području nacionalnog upravljanja kibernetičkim krizama, SOA je tijekom 2020. razradila nacionalni koncept upravljanja kibernetičkim krizama te ga uskladila s aktualnim pristupom EU-a i NATO-a. U svrhu usuglašavanja i razrade predloženog nacionalnog koncepta upravljanja kibernetičkim krizama, SOA je u listopadu 2020. formirala međuresornu stručnu radnu skupinu u koju su pozvani predstavnici ključnih tijela za predmetno područje (MORH, MUP, ZSIS, NCERT, HAKOM i HNB). Također, SOA se kao nadležno tijelo RH u proljeće 2020. uključila i u EU CyCLONe organizaciju koja predstavlja operativnu razinu upravljanja EU kibernetičkim krizama. CyCLONe je uspostavljen s ciljem praćenja i koordinacije tehničke razine upravljanja kibernetičkim krizama (CERT/CSIRT tijela) te u svrhu boljeg razumijevanja i odgovarajućeg prevođenja složene tehničke problematike kibernetičkih napada u opisni operativni utjecaj i situacijsko stanje razumljivo za političko-stratešku razinu odlučivanja. U okviru aktivnosti EU CyCLONe organizacije, predstavnici SOA-e sudjelovali su u rujnu 2020. na strateškoj simulacijskoj EU vježbi Blue OLEx 2020 (Blueprint Operational Level Exercise) u području upravljanja kibernetičkim krizama.

Temeljem podataka MUP-a, najveću prijetnju predstavljaju potencijalni kibernetički napadi većeg obujma na kritičnu infrastrukturu, no najveći je broj kibernetičkih napada manjeg opsega koji koriste dostupnije alate za napade, s obzirom da je tada i veća šansa da će takvi napadi polučiti uspjeh. Za kibernetičke napade koriste se malwarei, kojima se napadaju različiti ranjivi softveri, IoT (Internet of Things) uređaji, te korisnici i podaci koji koriste navedene softvere i uređaje. Prijetnju u budućem razdoblju predstavljaju i malwarei na mobilnim telefonima, iako do sada nije evidentiran njihov veći broj. Slijedeću veliku prijetnju predstavljali su DDoS napadi većih razmjera koji su izravna posljedica velikog broja slabo zaštićenih IoT uređaja. Najveći broj kibernetičkih napada i dalje se pojavljuju u obliku računalnih prijevara kojima prethode napadi na računala korisnika internetskog bankarstva, preuzimanje nadzora nad računalima oštećenika i neovlašteni prijenos novca na račune drugih osoba u inozemstvu.

Policija konstantno zaprima prijava građana i trgovačkih društava u kojima navode kako su njihovi privatni i poslovni podaci na računalima kriptirani te im više nisu u mogućnosti pristupiti, a na njihove adrese elektroničke pošte dostavljena je ucjenjivačka poruka kojom nepoznate osobe traže uplatu iznosa u virtualnim valutama u zamjenu za pomoć u otključavanju podataka. Radi se o pojavnim oblicima kibernetičkih napada koji uključuju tzv. Cryptolocker Ransomware - zarazu računala oštećenika malwareom (zloćudni računalni programi) koji kriptiraju sadržaje na računalima oštećenika, a zatim počinitelji traže isplatu novca (bitcoina), kako bi dekriptirali datoteke.

Ukoliko je oštećenicima računalo zaraženo zloćudnim računalnim programom koji je kriptiralo njihove datoteke i onemogućio pristup građani podacima, pomoć mogu potražiti na internetskoj

poveznici https://www.nomoreransom.org/cro/index.html na kojoj se nalazi alat pod nazivom KRIPTO ŠERIF, koji omogućuje na jednostavan način učitati kriptirane datoteke. To će omogućiti provjeru postoji li dostupno rješenje za dekripciju te, ukoliko postoji, oštećenici će dobiti upute o načinu na koji možete pristupiti vašim podacima. Navedeni alat izrađen je u suradnji s Europolom i redovito se ažurira.

Najveći broj zaprimljenih prijava građana i pravnih osoba odnosi se na internetske prijevare. S obzirom na način izvršenja, najčešće se pojavljuju sljedeće vrste internetskih prijevara:

1. Krađe identiteta (samostalno kazneno djelo ili pripremna radnja):
   Vishing – Krađa identiteta pozivom: Telefonska prijevara u kojoj počinitelji zovu i pokušavaju navesti sugovornika da otkrije svoje osobne, financijske ili sigurnosne podatke ili da im uplate novčana sredstva.
   Phishing – Mrežna krađa identiteta lažnim porukama e-pošte: Počinitelji šalju lažne poruke e-pošte kojima pokušavaju navesti primatelja na dijeljenje osobnih, financijskih ili sigurnosnih podataka.
   Smishing – Krađa identiteta SMS-om: Pokušaj je počinitelja da dođu do osobnih, financijskih ili sigurnosnih podataka putem tekstualne poruke.
   Krađa osobnih podataka kroz kanale društvenih mreža, poput Facebooka
2. CEO prijevara / direktorska prijevara: počinitelji se predstavljaju da su rukovoditelji ili nadređeni u organizaciji i prijevarom navode djelatnike da uplate novčani iznos na lažni račun ili da neovlašteno doznače novac s poslovnog računa.
3. BEC (Business Email Compromise) prijevara ili Prijevara s računima: počinitelji se predstavljaju da su klijenti/dobavljači i navode djelatnike trgovačkog društva da plate buduće račune na drugi bankovni račun.
4. Krivotvorene internetske stranice banaka: koristi se lažna e-pošta banke s poveznicom na krivotvorenu mrežnu stranicu. Jednom kada neka osoba klikne na poveznicu, koriste se razne metode prikupljanja financijskih i osobnih informacija. Stranica izgleda kao i prava mrežna stranica uz nekoliko malih razlika.
5. Romantične prijevare: počinitelji se pretvaraju da su zainteresirane za romantičnu vezu. One se obično događaju na mrežnim stranicama za upoznavanje, a varalice često koriste društvene medije ili e-poštu za uspostavljanje kontakta.
6. Investicijske prijevare i prijevare u online kupovini: počinitelji navode osobe da misle da su na tragu pametnog ulaganja, poput ulaganja u virtualne valute ili im daju „izvrsnu“ lažnu online ponudu za kupovinu nekog proizvoda.

   Tijekom 2020. godine zabilježene su tri veće računalne prijevare na štetu domaćih tvrtki u kojima je počinjena znatna imovinska šteta. Tijekom provođenja kriminalističkih istraživanja, osim utvrđivanja identiteta počinitelja kaznenih djela, nužno je utvrditi tijek novčanih transakcija koje su predmet kaznenih djela, radi zaustavljanja transakcija i/ili povrata novca oštećenima. Iz navedenog razloga od iznimne je važnosti žurno postupanje policije i državnog odvjetništva, te Ureda za sprječavanje pranja novca radi blokade sredstava. Ostvarena je iznimno dobra suradnja s Uredom za sprečavanje pranja novca u

cilju zaustavljanja transakcija i/ili povrata novca u vidu žurnog izvješćivanja po saznanju o počinjenom kaznenom djelu Računalne prijevare.

Služba kibernetičke sigurnosti MUP-a redovito surađuje s medijima putem priopćenja i javnih nastupa u kojima ukazuje na nove pojavne oblike kibernetičkih napada i računalnih prijevara, te se izdaju upozorenja za javnost prilikom pojave novih oblika računalnih prijevara. Savjeti za građane i tvrtke dostupni su na YouTube kanalu MUP-a i Twitter profilu MUP-a.

Tijekom 2020. godine Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenata i smanjenja šteta pri njihovom nastanku.
U 2020. godini zaprimljeno je i obrađeno ukupno 1710 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su phishing URL, phishing i pogađanje zaporki.
Najznačajnija promjena u odnosu na prošlu godinu je općenito velik broj prijavljenih incidenata. Korištenjem OSINT metoda (eng. Open Source Inteligence) za otkrivanje računalno-sigurnosnih incidenata na web sjedištima pod nadležnošću Nacionalnog CERT-a, ali i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta, u odnosu na 2019. godinu Nacionalni CERT je zaprimio i obradio 66% incidenata više. Što se tiče broja registriranih botova vidi se blagi pad, no broj botova po danu se najčešće kreće nešto ispod 2000 što ne predstavlja razliku u odnosu na prethodne godine.

Na bankarski sektor su u 2020. godini u velikoj mjeri utjecali COVID-19 i učinci potresa. Banke su se istovremeno susrele s izazovom organiziranja kontinuiranog udaljenog rada velikog broja svojih djelatnika uz istovremeni izraziti porast korištenja bankovnih posredstvom izravnih distribucijskih kanala te narušavanje fizičke infrastrukture kao posljedice potresa. Udaljeni rad i porast korištenja bankovnih usluga putem interneta utjecali su na porast inherentnog kibernetičkih rizika, kao i na potrebu pojačane pozornosti banaka na pojavu sigurnosnih incidenata. No, malen broj i vrlo ograničen učinak uočenih kibernetičkih incidenata pokazuju da su se hrvatske banke dobro prilagodile novonastaloj situaciji te uspješno organizirale svoje poslovanje i u ovim izvanrednim okolnostima.

OTC tijekom prošle godine nije zabilježio incidente u kibernetičkom prostoru. Naime, OTC je razmjerno nisko izložen javnom Internet prostoru, te sustav bilježi pokušaje neželjenih elektroničkih poruka (spam i hoax) koji se obrađuju i ne izazivaju incidente. Dodatno, OTC je u sustavu SCOUT, što možemo navesti kao pozitivnu i poželjnu karakteristiku borbe protiv kibernetičkih ugroza.

7. Izrada godišnjeg izvješća o radu Operativno-tehničke koordinacije za kibernetičku sigurnost za 2020. godinu.

Prijedlog godišnjeg Izvješća o radu Operativno-tehničke koordinacije za 2020. godinu dostavljen je na mišljenje svim članovima Operativno-tehničke koordinacije, te je usuglašena konačna verzija dokumenta koja je dostavljena Nacionalnom vijeću za kibernetičku sigurnost, koji je isto usvojio na elektroničkoj sjednici, održanoj od 16. do 18. veljače 2021. godine.

Tijela, članovi Operativno-tehničke koordinacije, bila su uključena u nekoliko aktivnosti na nacionalnoj i međunarodnoj razini od kojih su najznačajnije:

- NATO vježba „**Cyber Coalition 2020**.“ – 16.-20. studenoga 2020. godine u državama članicama NATO-a i partnerskim zemljama. Cilj vježbe bio je uvježbavanje koordinacije između nacionalnih i NATO-ovih tijela prilikom odgovora na zajedničke kibernetičke prijetnje i incidente u kibernetičkom prostoru članica NATO saveza.

- Vježba „**Blue OLEx 2020“** – predstavnici SOA-e sudjelovali su u strateškoj simulacijskoj EU vježbi „Blue OLEx 2020 (Blueprint Operational Level Exercise)“ u području upravljanja kibernetičkim krizama. Zbog COVID-19 pandemije vježba je održana u obliku video-konferencije, u organizaciji Nizozemske i uz podršku EK i ENISA-e. Dvije ključne teme vježbe bile su službeno pokretanje EU CyCLONe organizacije i plan EK o osnivanju Joint Cyber Unita (JCU).

- Mreža CSIRT-ova – mreža CSIRT-ova (eng. *CSIRTs Network*) nastala je temeljem Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva) koju je donijela Europska unija. Hrvatsku na sastancima zastupa delegacija koju čine stručnjaci iz CARNET-ovog odjela za Nacionalni CERT i CERT-a Zavoda za sigurnost informacijskih sustava (ZSIS). CSIRT mreža ima za cilj unaprjeđenje suradnje, komunikacije i razmjene informacija među CSIRT-ovima Europske unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a te razmjenu znanja i razvoj alata koji se koriste u CSIRT zajednici.

- DSI Governance Bord – Nacionalni CERT od 2018. godine aktivno sudjeluje u radu odbora CEF Cyber DSI Governance Board koji je uspostavljen unutar europskog CEF (eng. *Connecting European Facility)* programa sufinanciranja za projekte koji se provode u okviru implementacije Europske strategije kibernetičke sigurnosti. Nastavkom aktivnosti projekta Grow2CERT, Nacionalni CERT podržava i implementira usluge i servise nadogradnje i poboljšanja razmjene informacija o kibernetičkim prijetnjama i incidentima na europskoj razini te se pridružuje ostalim europskim projektima na zajedničkoj platformi MeliCERTes koja je ušla u drugu fazu razvoja s projektom SMART 2018/1024.

- DSI CTF International CyberEx 2020 – predstavnici CARNET-ovog Nacionalnog CERT-a po prvi su puta sudjelovali u International CyberEx-u, CTF natjecanju u

organizaciji OAS-a (*Organization of American States*), INCIBE (*Spanish National Cybersecurity Institute*) i CNPIC-a (*Spanish National Centre for Infrastructure and Cybersecurity*), čiji je cilj jačanje sposobnosti odgovora na računalno-sigurnosne incidente. Natjecanje se održalo 10. rujna 2020. godine. Zadaci su bili iz područja kriptografije, digitalne forenzike, reverznog inženjerstva, web sigurnosti i sličnih područja.

Više informacija o natjecanju dostupno je na poveznici:
https://www.incibe-cert.es/en/international-cyberex

4. ZAKLJUČAK

Do danas je većina tijela razvila značajnije vlastite sposobnosti u području kibernetičke sigurnosti, s jedne strane potaknuti ubrzanim razvojem informacijske i komunikacijske tehnologije koji ne trpi zaostajanje te s druge strane ulaganjem (ne samo financijskim) u razvoj vlastitih sposobnosti, što je preduvjet za daljnje unaprjeđenje kibernetičke sigurnosti na nacionalnoj razini i nošenje sa sve većim izazovima u kibernetičkom prostoru za što je nužna visoka razina i koncentracija stručnosti, kapaciteti dostatni za pokretanje i realizaciju vlastitih inicijativa te proaktivan pristup koji se u narednom razdoblju očekuje od svih tijela uključenih u rad Vijeća, ali i šire kroz provedbu Strategije te pokretanjem vlastitih inicijativa.

Velik broj aktivnosti prikazanih u ovom izvješću prikazan je kao pojedinačna postupanja tijela u okviru svojih nadležnosti, međutim, iza takvih postupanja stoji koordinacija i usmjeravanje Vijeća u cilju optimalnih korištenja nacionalnih kapaciteta u području kibernetičke sigurnosti.

Ubrzani razvoj informacijske i komunikacijske tehnologije svakodnevno stvara nove izazove. Čak i u najoptimističnijem scenariju, za neke od izazova s kojima se Republika Hrvatska suočava svakodnevno, bez obzira radi li se o složenosti, nadležnosti, organizaciji ili koordinaciji, zasigurno će trebati više godina da se riješe. U ovom trenutku Strategija, uz odgovarajuće podizanje sposobnosti pojedinih tijela, pruža dostatnu mogućnost za nužnu transformaciju upravljanja kibernetičkom sigurnošću i očuvanje napretka u digitalnom dobu, a za rješavanje i nošenje s nekim novim, budućim, brzorastućim izazovima radi zaštite kibernetičkog prostora RH bit će nužno uspostaviti centralizirano upravljanje kibernetičkom sigurnošću na svim razinama, u konačnici i kroz zakonodavni okvir.

Raspoloživi materijali povezani s radom Vijeća dostupni su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na mrežnim stranicama Ureda Vijeća za nacionalnu sigurnost[12].

[12] https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost

5. ČLANOVI VIJEĆA I OPERATIVNO-TEHNIČKE KOORDINACIJE

Tijekom 2017., 2018., 2019. i 2020. godine, na prijedlog nadležnih institucija došlo je do promjena pojedinih članova i zamjenika članova Vijeća i Koordinacije. U trenutku izrade i usvajanja ovog Izvješća, Vijeće i Koordinacija rade u sljedećem sastavu:

Članovi Vijeća:	**Zamjenici članova Vijeća:**
Suzana Galeković	Vinko Kuculo
dr. sc. Damir Trut	Marjan Vukušić, Davor Spevec
Mato Škrabalo	Tihomir Lulić
Nataša Mikuš Žigman	Maja Radišić Žuvanić, Davor Golenja
Goran Kolarić	Sandra Lukić
brg Bruno Bešker	bjn Nikola Bokulić
Vedrana Šimundža Nikolić	Ana Kordej, Zoran Luša
dr. sc. Ivan Matić	Mario Bušić
Dražen Ljubić	Krešimir Šipek
Mario Miljavac	mr. sc. Valentino Franjić
Tomislav Štivojević	mr. sc. Vlado Pribolšan
Tonko Obuljen	Zdravko Jukić
Mato Mihaljević	Davor Đeker
Tomislav Mihotić	Filip Matijaško
Bernard Gršić	Marin Ante Pivčević
Zdravko Vukić	Igor Vulje

Administrativna i tehnička potpora radu Vijeća:

Iva Jeličić	Andrej Milovac

Članovi Koordinacije	**Zamjenici članova Koordinacije**
Renato Grgurić, koordinator	Marjan Vukušić, zamjenik
Brg Darko Galinec	bjn Nikola Bokulić
Tomislav Kulčar	Stjepan Petrač
Mario Posavec	Ivan Koroša
Mirko Korajac	Marko Herceg
Vlatka Mišić	Zvonimir Bošnjak
Vesna Gašpar	Željka Kardum – Ban
dr. sc. Slaven Smojver	Mario Kozina