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

u 2022. GODINI

SADRŽAJ

1. SAŽETAK

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, prometom 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. No, unatoč tome, svako od tijela treba razvijati vlastite sposobnosti uočavanja i suočavanja s prijetnjama i rizicima koji svakodnevno dolaze iz kibernetičkog prostora, kako bi djelovali proaktivno.

Bližimo se polovini digitalnog desetljeća, u kojem se završetak digitalne transformacije društva i gospodarstva na razini EU-a očekuje do 2030., a sposobnosti u digitalnim vještinama, infrastrukturi i digitalizaciji poslovanja ne prate dovoljno brzo ritam potreba transformacije. U takvim okolnostima, u kojima se na razini EU-a donose uredbe galopirajućim tempom, a koje se u svim segmentima i tematikama dotiču kibernetičke sigurnosti, koja je u današnje vrijeme alat svega poslovanja, Vijeće je ispunilo svoju koordinativnu ulogu, no tijela moraju uložiti dodatne napore za razvoj svojih vlastitih sposobnosti i razvoj ljudskih potencijala, koji će moći adekvatno pratiti ovu ubrzanu dinamiku.

2. UVOD

Nacionalno vijeće za kibernetičku sigurnost (dalje: Vijeće) započinje s 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. Nakon nekoliko izmjena Odluke („Narodne novine“, brojevi: 61/16, 28/18, 110/18, 79/19 i 136/20; zbog pripajanja Državne uprave za zaštitu i spašavanje Ministarstvu unutarnjih poslova te spajanja Ministarstva pravosuđa i Ministarstva uprave), Vijeće danas djeluje kroz 16 tijela. Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u **Operativno-tehničku koordinaciju 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

3. IZVJEŠĆE O RADU NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST U 2022. GODINI

3.1. 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 te 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, odnosno pružaju administrativno-tehničku potporu radu Vijeća.

Tijekom 2022. godine Vijeće je održalo 12 sjednica. Sjednice su se održavale sredinom mjeseca, a one elektroničke su provedene kroz razmjenu informacija i koordinaciju elektroničkom poštom, u trajanju od dva-tri dana. Svi zapisnici, dnevni redovi i zaključci sa sjednica Vijeća usvojeni su jednoglasno te su dostavljeni svim članovima i zamjenicima članova radi planiranja i provedbe daljnjih/usuglašenih aktivnosti u vlastitim institucijama.

3.2. PREGLED AKTIVNOSTI VIJEĆA U 2022. GODINI

Vijeće je u 2022. 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.

Važno je napomenuti kako tijela u Vijeću provode aktivnosti samostalno, sukladno nadležnostima propisanim *Zakonom o ustrojstvu i djelokrugu tijela državne uprave* („Narodne novine“, broj: 85/20) i drugim podzakonskim aktima i odlukama Vlade, a Vijeće primarno služi kao platforma za razmjenu informacija te koordinaciju (uključujući i tematske radne skupine Vijeća) kada je potrebna suradnja više tijela u istim pitanjima. Ovakav način rada uspostavljen je zbog raspršenih nadležnosti nad pitanjima kibernetičke sigurnosti, odnosno nepostojanja središnjeg autoriteta nadležnog za sigurnost kibernetičkog prostora RH.

U 2022. je Vijeće raspravljalo o prikladnom državnom tijelu koje će preuzeti ulogu Nacionalnog koordinacijskog centra (slijedom ***Uredbe o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i Mreže nacionalnih koordinacijskih centara***[2]). Nacionalni koordinacijski centar trebao bi biti subjekt javnog sektora, ili subjekt s većinskim javnim udjelom, koji obavlja funkciju javne uprave na temelju nacionalnog prava, među ostalim i delegiranjem. Nacionalni koordinacijski centar bi mogao primati izravnu financijsku potporu EU, uključujući bespovratna sredstva, a trebao bi doprinijeti povećanju sigurnosti mrežnih i informacijskih sustava, uključujući internet i ostalu infrastrukturu ključnu za funkcioniranje društva, kao što su promet, zdravstvo, energetika, digitalna infrastruktura, voda, financijska tržišta i bankovni sustavi. Konačna usuglašena odluka o tijelu nadležnom za uspostavu Nacionalnog koordinacijskog centra nije donesena.

Daljnja značajna aktivnost oko koje je Vijeće bilo angažirano je donošenje nove Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije[3] (NIS direktiva). Dok je prva verzija direktive implementirana u hrvatsko zakonodavstvo donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i pripadajućom uredbom, potreba daljnjeg unaprjeđenja kibernetičke sigurnosti potaknula je Europsku komisiju na donošenje izmjena direktive. NIS direktiva je prvi dio

[2] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

[3] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/18, Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 68/18

zakona o kibernetičkoj sigurnosti na razini EU-a, a njezin je specifičan cilj bio postići visoku zajedničku razinu kibernetičke sigurnosti u državama članicama. Iako je povećala sposobnosti država članica za kibernetičku sigurnost, provedba se pokazala zahtjevnom, što je rezultiralo fragmentacijom na različitim razinama unutarnjeg tržišta. Kako bi odgovorila na rastuće prijetnje digitalizacije i porasta kibernetičkih napada, Komisija je podnijela prijedlog za izmjenu NIS direktive i na taj način ojačala sigurnosne zahtjeve, pozabavila se sigurnošću opskrbnih lanaca, pojednostavila obveze izvješćivanja i uvela strože nadzorne mjere i strože provedbene zahtjeve, uključujući usklađene sankcije u cijeloj EU. Predloženo proširenje opsega obuhvaćenog novom NIS direktivnom (tzv. NIS2 direktiva), efektivnim obvezivanjem više subjekata i sektora da poduzmu mjere, pomoglo bi dugoročnom povećanju razine kibernetičke sigurnosti u EU.

Nakon završetka postupka usuglašavanja NIS2 direktiva je stupila na snagu 16. siječnja 2023. Radna skupina Vijeća[4], uspostavljena da prati i priprema nacionalna stajališta, nastavit će svoj rad kroz transpoziciju direktive u nacionalno zakonodavstvo donošenjem u cijelosti novog zakona (kojim će se Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga staviti izvan snage). Rok za transpoziciju je 21 mjesec, odnosno najkasnije do 16. listopada 2024. NIS2 usko povezani akti DORA[5] i CER[6] također su stupili na snagu 16. siječnja 2023.

Direktive DORA i CER neće se, za razliku od NIS2 direktive, transponirati kroz radne skupine Vijeća, već u okviru redovnih aktivnosti nadležnih tijela.

DORA, kao *lex specialis,* adresira rizike komunikacijsko-informacijskih tehnologija u financijskom sektoru. Postojeći visoki stupanj međusobne povezanosti financijskih subjekata, financijskih tržišta i infrastruktura financijskog tržišta, a osobito međuovisnosti njihovih sustava IKT-a, predstavlja sistemsku ranjivost, jer bi se kibernetički incidenti mogli brzo proširiti s bilo kojeg od oko 22 000 financijskih subjekata u EU na cijeli financijski sustav, neovisno o zemljopisnim granicama, te kao za posljedicu imati pad likvidnosti i opći gubitak povjerenja i pouzdanja u financijska tržišta. DORA-om se nastoji jačati otpornost financijskog sektora EU, među ostalim i u operativnom smislu, kako bi se osigurali njegova tehnološka sigurnost u dobro funkcioniranje, brz oporavak od povreda i incidenata u području IKT-a, a time u konačnici omogućilo djelotvorno i neometano pružanje financijskih usluga u cijeloj EU, među ostalim i u stresnim okolnostima, uz istodobno očuvanje povjerenja potrošača i povjerenja u tržište.

CER uspostavlja pravni okvir čiji je cilj jačanje otpornosti kritičnih subjekata na unutarnjem tržištu utvrđivanjem usklađenih minimalnih pravila te pružanje pomoći tim subjektima koherentnim i namjenskim mjerama potpore i nadzora. Kritični subjekti trebali bi moći ojačati

[4] iz Vijeća HAKOM, CARNET, HNB, MGOR, MMPI, MPU, MUP, MVEP, SDURDD, UVNS, ZSIS te SOA kao voditelj radne skupine; izvan Vijeća Ministarstvo financija, HANFA, Ministarstvo poljoprivrede, Ministarstvo zdravstva

[5] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br.1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011

[6] Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i stavljanju izvan snage Direktive Vijeća 2008/114/EZ

svoju sposobnost sprečavanja incidenata koji mogu poremetiti pružanje ključnih usluga, zaštite od njih, odgovora na njih, odupiranja njima, njihova ublažavanja i apsorpcije, prilagodbe njima te oporavka od njih. Takvi subjekti bi trebali učiniti više za bolju opremu zbog dinamičkog okruženja prijetnji, koje uključuju hibridne i terorističke prijetnje koje se razvijaju, te sve veće međuovisnosti između infrastrukture i sektora. Osim toga, zbog prirodnih katastrofa i klimatskih promjena povećan je fizički rizik, što povećava učestalost i razmjere ekstremnih vremenskih pojava i dovodi do dugoročnih promjena u prosječnim klimatskim uvjetima koje mogu smanjiti kapacitet, učinkovitost i životni vijek određenih vrsta infrastrukture ako se ne uvedu mjere za prilagodbu klimatskim promjenama. Nacionalni stav po pitanju CER-a je Vijeće iskazivalo kroz nadležnu radnu skupinu Vijeća EU, Radnu skupinu za civilnu zaštitu (PROCIV).

Europska unija poduzela je niz mjera kako bi uredila odnose u kibernetičkom prostoru, povećavajući pri tome otpornost i pojačavajući svoju kibernetičku sigurnosnu pripravnost. Novom strategijom kibernetičke sigurnosti, donesene 2020., dodatno su (u odnosu na onu iz 2013., koje utvrđuje postizanje otpornosti, smanjenje kibernetičkog kriminaliteta, razvoj politike kibernetičke obrane i sposobnosti za kibernetičku obranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kibernetičkog prostora), naglašena tri područja – (1) otpornost, tehnološka suverenost i vodstvo, (2) izgradnja operativnih kapaciteta u svrhu sprječavanja, odvraćanja i uzvraćanja, (3) razvijanje globalnog i otvorenog kibernetičkog prostora. U cilju povećanja povjerenja i sigurnosti na Jedinstvenom digitalnom tržištu Unije (JDT) te s obzirom na brzo širenje povezanih uređaja (IoT – Internet of Things), bilo je potrebno uspostaviti okvir za sigurnosno certificiranje proizvoda, usluga i procesa informacijsko komunikacijske tehnologije (IKT), odnosno svih objekata kibernetičkog prostora. Kibernetičko sigurnosno certificiranje postaje posebno važno s obzirom na sve veću uporabu kibernetičkih tehnologija za namjene koje zahtijevaju visok stupanj pouzdanosti i sigurnosti te je u sve većem broju sektora primjetno povećanje ovisnosti o IKT proizvodima, uslugama i procesima, osobito u prometu (automatizirano upravljanje), u sustavima održavanja života i zdravlja (e-zdravstvo), u industriji (kontrolni sustavi za industrijsku automatizaciju – IACS) te u ostvarivanju ljudskih interesa i prava (e-građani). **Zakon o provedbi kibernetičke sigurnosne certifikacije, čiji je prijedlog koordiniralo Vijeće u užem sastavu, a Hrvatski sabor je proglasio na sjednici održanoj 27. svibnja 2022.**, u potpunosti regulira sustav nadležnih tijela na nacionalnoj razini, pri čemu je njihovo povezivanje s nadležnim tijelima EU i državama članicama (dalje: DČ) određeno samom Uredbom (EU) 2019/881. Time je provedeno harmoniziranje propisa i djelovanja RH na ovom području, te izgradnja i prilagodba nacionalnih sustava kibernetičke sigurnosne certifikacije zajedničkom certifikacijskom okviru.

Zavod za sigurnost informacijskih sustava, kao nositelj provedbe ovog Zakona, nastavlja sudjelovanje u radu ECCG-a (*European Cybersecurity Certification Group*), čije su zadaće, između ostalog, i savjetovati i pomagati Europsku komisiju u njezinu radu kako bi se osigurala dosljedna provedba i primjena Uredbe o ENISA-i te o kibernetičkoj sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (*The EU Cybersecurity Act*), savjetovati ju u pitanjima politike kibernetičkog sigurnosnog certificiranja i koordinaciji pristupa politikama i pripremi europskih shema kibernetičkog sigurnosnog certificiranja.

Radna skupina Vijeća za 5G je tijekom godine održala više sastanaka na kojima su raspravljena različita pitanja iz područja sigurnosti 5G tehnologija te je usuglašavan nacionalni stav po pitanju EU i bilateralnih inicijativa kao što je npr. podrška za Open RAN ili ograničenja korištenja opreme proizvođača iz rizičnih država u području telekomunikacija. Ovo je područje posebno osjetljivo zbog velikih prethodnih ulaganja operatera te regulatorna ograničenja bi mogla dovesti do znatnih troškova i smanjivanja investicija, a i države članice EU nisu u potpunosti usklađene u praktičnoj provedbi mjera. Regulatorni okvir za tehničke mjere u RH je implementiran, a operateri su dužni podatke o politikama i osjetljivim dijelovima sustava dostaviti do siječnja 2023., a do kraja svibnja 2023. moraju provesti revizije svojih mreža kako bi se utvrdilo jesu li sve potrebne sigurnosne mjere ostvarene.

U okviru upravljanja kibernetičkim krizama na razini EU-a u organizaciji CyCLONe[7], SOA je ne samo ispred Vijeća, već i RH, a u sklopu suradnje DČ u provođenju NIS direktive, kao nacionalni koordinator nastavila redovito pratiti CyCLONe aktivnosti te je tako sudjelovala u vježbi EU CyCLES (Cyber Crisis Linking Exercise) koju je organizirala Francuska u sklopu svog predsjedanja Vijećem EU, vježbi BlueOLEx 2022 te u strateškoj simulacijskoj table-top vježbi koju je organizirala Litva. Vježba se fokusirala na uvježbavanje procedura i odlučivanja na strateško-političkoj razini kroz Horizontalnu radnu skupinu za kibernetička pitanja (HWPCI) i COREPER. FAC (Foreign Affairs Council) je zbog drugih obveza izuzet dok se uloga IPCR-a (Integrated Political Crisis Response) simulirala.

NIS Grupa za suradnju (NIS CG – NIS Cooperation Group) održava nekoliko sastanaka godišnje na kojima ispred RH sudjeluje UVNS, dok u CSIRT mreži sudjeluju CARNET-NCERT i ZSIS. NIS Grupa je uspostavila više radnih skupina koje se bave različitim pitanjima (primjerice, radnu skupinu za jačanje sposobnosti, digitalnu infrastrukturu, izvještavanje o incidentima, suradnju u prekograničnoj ovisnosti, zdravstveni sektor, itd.), u kojima sudjeluju predstavnici hrvatskih institucija pa tako, primjerice Ministarstvo zdravstva sudjeluje u radnoj skupini za zdravstveni sektor.

Uslijed situacije u Ukrajini ZSIS i NCERT, kao članovi Mreže CERT-ova su bili pojačano angažirani u području praćenja stanja u kibernetičkom prostoru EU i međusobnoj razmjeni podataka. NCERT, ZSIS, SOA i MZO su sudjelovali i u vježbi Cyber Europe 22 koju je organizirala ENISA. Veći broj tijela i pravnih osoba iz RH je sudjelovao i u NATO vježbi Cyber Coalition. NCERT je sudjelovao u obilježavanju Europskog mjeseca kibernetičke sigurnosti.

Tijekom godine provedene su i brojne međunarodne koordinacije u kojima su predstavnici Vijeća sudjelovali: tako su MVEP i SOA sudjelovali u američkoj inicijativi za sprečavanje ransomwarea (Counter Ransomware Initiative), EU CyberNet sastanku na temu jačanja kibernetičkih kapaciteta u zapadnom Balkanu; MPU je sudjelovalo u radu na novoj Konvenciji o kibernetičkom kriminalitetu i provelo posjet SAD-u s temama kibernetički kriminalitet i e-dokazi; održan je sastanak s predstavnicima američkog veleposlanstva u RH, na njihov zahtjev,

[7] 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)

na temu prioriteta RH u području kibernetičke sigurnosti, gdje je RH ponuđena suradnja i pomoć; MORH je koordinirao nacionalni stav po pitanju Zavjeta kibernetičke obrane (Cyber Defence Pledge, preuzeta obveza NATO članica); HAKOM je koordinirao nacionalni stav po pitanja potpore Praškoj inicijativi (Prague Proposals on Telecommunications Supplier Diversity Proposals); NCERT je sudjelovao na konferenciji „Cybersecurity in Finance“, održao sastanak s predstavnicima američkog veleposlanstva po pitanju izravne suradnje s američkom Cybersecurity and Infrastructure Security Agency te održavao sastanke s CERT-ovima drugih država.

Provođene su aktivnosti podizanja svijesti. CARNET je sudjelovao u organizaciji konferencije pod nazivom „Potraga za boljim internetom“ na kojoj su predstavljene dvije teme „Zaštita virtualnog identiteta“ i „Educiranje kroz hakiranje“. Proveden je natječaj za osnovne škole u kojima su prijavljeni timovi crtali strip koji je obrađivao teme iz kibernetičke sigurnosti. Predstavljene su aktivnosti na HRT-u u emisiji „Dobro jutro Hrvatska“ povodom Dana sigurnijeg interneta. NCERT je također održao edukaciju za djelatnike HNB-a pod nazivom „Trag u (kibernetičkom) beskraju“, a na konferenciji CARNET-ovi korisnika (CUC) održano je i nekoliko predavanja na temu kibernetičke sigurnosti. HAKOM je održao konferenciju „5G dan“ za predstavnike industrije, znanstvene zajednice, gospodarstva i relevantnih državnih tijela. MORH je proveo tradicionalni simpozij kibernetičke obrane na kojem su sudjelovali i predstavnici NCERT-a, MUP-a i ZSIS-a. ZSIS je održao konferenciju o kibernetičkoj sigurnosti.

Tijekom 2022. Vijeće je pratilo i aktualne teme DČ i institucija EU-a u kibernetičkim pitanjima, a naglasak je stavljen na podizanje svijesti državnih tijela o njihovim izvornim nadležnostima koje je nužno primijeniti, jednako kao i u fizičkom okruženju i na kibernetički prostor.

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

Po donošenju novog kibernetičkog paketa na razini EU-a, među kojima se našla i NIS2 direktiva, Vijeće je donijelo zaključak o potrebi donošenja u cijelosti nove nacionalne strategije kibernetičke sigurnosti, uvažavajući zahtjeve NIS2 direktive o pojedinim elementima koje nove generacije nacionalnih strategija kibernetičke sigurnosti trebaju obuhvatiti. Slijedom toga, Vijeće je u 2022. g. nastavilo rad na izradi nove Nacionalne strategije kibernetičke sigurnosti te su uspostavljene 4 (tematske) radne skupine:

- Radna skupina za tehničku suradnju pod vodstvom SOA-e
- Radna skupina za netehničku suradnju pod vodstvom SOA-e
- Radna skupina za svijest i kompetencije pod vodstvom Nacionalnog CERT-a
- Radna skupina za istraživanje i razvoj pod vodstvom SDURDD-a.

Radne skupine su identificirale veći dio prioriteta koje treba ugraditi u novu Strategiju međutim, kako nova NIS2 direktiva izričito propisuje elemente koje nacionalne strategije kibernetičke

sigurnosti država članica moraju sadržavati, rad na Strategiji se privremeno obustavio do donošenja NIS2 direktive. U daljnjem radu radnih skupina biti će potrebno raščlaniti koje elemente NIS2 direktive treba ugraditi u Strategiju, a koje u novi zakon o kibernetičkoj sigurnosti kao implementacijski akt za NIS2 direktivu te koji bi trebao zamijeniti *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*.

Akcijski plan koji će biti pripadajući dio nove Strategije će sadržavati, kao i u prethodnoj, još uvijek važećoj strategiji, detaljnu razradu potrebnih aktivnosti koje je potrebno provesti s rokovima i nositeljima. Za razliku od postojeće strategije, za čije su provođenje sredstva osigurana gotovo u cijelosti iz postojećih proračuna uključenih tijela, za daljnje unaprjeđenje kibernetičke sigurnosti potrebno će biti osigurati dodatne izvore financiranja, pri čemu će se pokušati u najvećoj mjeri osloniti na EU fondove. Uvažavajući zahtjeve NIS2 direktive u odnosu na nacionalnu strategiju kibernetičke sigurnosti, proces transpozicije NIS2 direktive i izrade ove strategije morati će teći paralelno, a dovršetak rada na Strategiji očekuje se u prvoj polovini 2024.

4. IZVJEŠĆE O RADU OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST U 2022. GODINI

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.

4.1. SJEDNICE OPERATIVNO-TEHNIČKE KOORDINACIJE

Tijekom 2022. godine planirano je i održano 12 sjednica Operativno – tehničke koordinacije, a sve su sjednice Operativno – tehničke koordinacije održane kao virtualne sjednice.

4.2. PREGLED AKTIVNOSTI OPERATIVNO-TEHNIČKE KOORDINACIJE U 2022.

Planom aktivnosti Operativno – tehničke koordinacije za 2022. 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 2022. godine

2. Izrada i dostava podataka o trendovima i prijetnjama u kibernetičkoj sigurnosti na mjesečnoj razini.

   rok: mjesečno

3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2022. godini.

   rok: kvartalno – ožujak, lipanj, rujan, prosinac 2022. godine

4. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2022. godinu.

   rok: siječanj 2023. godine

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

   rok: prosinac 2022. godine

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

   rok: prosinac 2022. godine

Operativno – tehnička koordinacija je tijekom 2022. godine provela zadaće iz Plana aktivnosti:

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 posebno se 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 2022. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru Republike Hrvatske. Prema podacima iz kvartalnih Izvješća o incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske članovi Operativno – tehničke koordinacije najčešće su prijavljivali phishing (429 prijava), scam (197), phishing URL (186), pogađanje zaporki (133), incidenti bez kategorija – ostalo (86), web defacement (73), te malware URL (67) i zaraze pojedinačnih računala malicioznim kodom (67).

2. Izrada i dostava podataka o trendovima i prijetnjama u kibernetičkoj sigurnosti na mjesečnoj razini.

   Članovi Operativno – tehničke koordinacije na redovitim sjednicama iznose podatke o događajima, trendovima i prijetnjama u kibernetičkom prostoru Republike Hrvatske za sektore iz njihove nadležnosti, te se isti podaci unose u zapisnik sa sjednice Koordinacije.

   Nacionalnom vijeću za kibernetičku sigurnost redovito se dostavljaju zapisnici sa sjednica Operativno – tehničke koordinacije i mjesečna izvješća o trendovima i prijetnjama koja su bazirana na podacima iznesenim prilikom održavanja sjednica.

3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2022. godini.

   Izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske izrađuju se tromjesečno, krajem ožujka, lipnja, rujna i prosinca. Ista se redovito dostavljaju Nacionalnom vijeću za kibernetičku sigurnost.

4. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2022. godinu.

   Prijedlog godišnjeg Izvješća o radu Operativno – tehničke koordinacije za 2022. godinu dostavljen je na mišljenje svim članovima Operativno – tehničke koordinacije, te je usuglašena konačna verzija dokumenta. Ista se dostavlja Nacionalnom vijeću za kibernetičku sigurnost na daljnje postupanje.

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 2019. 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 procijenjena stanja kibernetičke sigurnosti po sektorima.

   Inicijalna procjena stanja kibernetičke sigurnosti u Republici Hrvatskoj napravljena je krajem siječnja i dostavljena Nacionalnom vijeću za kibernetičku sigurnost u ožujku 2020. godine.

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. Procjena stanja kibernetičke sigurnosti i pripadno Izvješće napravljeni su temeljem Metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj početkom 2020 godine. Sukladno raspravi na 70. sjednici Operativno – tehničke koordinacije, članovi Operativno – tehničke koordinacije smatraju da se sigurnosna situacija u kibernetičkom prostoru Republike Hrvatske nije bitnije promijenila, te da trenutno nema potrebe za novu procjenu stanja kibernetičke sigurnosti.

U nastavku su dodatni podaci članova Operativno – tehničke koordinacije vezani za sektore iz njihove nadležnosti.

MUP

Temeljem Strategije kibernetičke sigurnosti Europske unije za digitalnu dekadu, a kako bi se osiguralo da Hrvatska može iskoristiti društvene, ekonomske i političke prednosti interneta i korištenja novih tehnologija, policija je tijekom 2022. godine nastavila poduzimati aktivnosti s ciljem povećanja kibernetičke otpornosti i jačanja kapaciteta za istraživanja i kazneni progon kibernetičkog kriminala i odgovora na kibernetičke prijetnje.

Broj kibernetičkih napada raste, te su napadi sofisticiraniji nego ikada, dolaze iz širokog spektra izvora unutar i izvan Europske unije. Kibernetički rizici također su se pojavili kao značajna prijetnja financijskom sustavu. Materijalna šteta koja je izravna posljedica prijavljenih kibernetičkih napada iznosila je 8 milijuna EUR u 2022. godini.

Ključni trendovi ugrožavanja kibernetičke sigurnosti:

Cyber kriminalci su u najvećoj mjeri motivirani monetizacijom svojih aktivnosti, npr. korištenjem ransomware napada. Kriptovalute su i dalje najčešća metoda pribavljanja protupravne imovinske koristi.

Kibernetički napadi imaju za svoju metu i sve više utječu na kritičnu infrastrukturu.

Kompromitacije računalnih sustava putem „phishing“ e-pošte i „brute force“ napada na uslugama pristupa udaljenoj radnoj površini (RDP) i dalje predstavljaju dva najčešća vektora zaraze ransomwareom.

Fokus kriminalaca na poslovne modele tipa Ransomware kao usluge (eng. RaaS – Ransomware-as-a-Service) povećao se tijekom 2022. godine.

Poslovni kriminalni model Phishing-as-a-Service (PhaaS) sve je više prevladavajući.

Zlouporaba osobnih podataka u fokusu je kriminalaca i predstavlja pripremnu radnju za izvršenje različitih oblika prijevara. Internetske prijevare korištenjem bezgotovinskog plaćanja uzrokuju veliku materijalnu štetu, posebno za mala i srednja poduzeća i pod kontrolom su

kriminalnih organizacija iz inozemstva, te obuhvaćaju sve vrste prijevarnih radnji koje se koriste kod tradicionalnih metoda plaćanja i uključuju plaćanja s prisutnom karticom i bez prisutne kartice.

Najčešći oblici internetskih prijevara su:

• BEC prijevare (eng. Business Email Compromise), koje ciljaju na tvrtke i organizacije te se kriminalci pretvaraju da su njihovi klijenti/dobavljači i navode ih da plaćaju buduće račune na drugi bankovni račun koji se nalazi pod kontrolom kriminalnih organizacija.

• Zamjena SIM kartica (eng. SIM Swapping) i Smishing - pokušaj kriminalaca da dođu do osobnih, financijskih ili sigurnosnih podataka putem tekstualne poruke, koji predstavljaju značajan rizik za žrtve i njihove financije.

• Investicijske prijevare u vezi ulaganja u nepostojeće poslovne aktivnosti ili kriptovalute

Ovakvo sigurnosno okruženje snažan je poticaj za kontinuirano jačanje kapaciteta hrvatske policije za borbu protiv kibernetičkog kriminala. Policijski stručnjaci koji su na prvoj liniji borbe protiv cyber kriminalaca najvrjedniji su resurs.

Ulaganje u tehnologiju nužan je preduvjet za identifikaciju počinitelja kibernetičkih napada i pronalazak elektroničkih dokaza – u posljednje tri godine MUP je izravno uložio preko 1 000 000 EUR, a u tijeku je ulaganje od 1 600 000 EUR u okviru NPOO-a, te slijede i nova značajna ulaganja u 2023. godini pa nadalje.

16. prosinca 2022. godine predstavljena je na konferenciji za tisak u Ravnateljstvu policije kampanja osvještavanja javnosti o opasnostima na internetu „Web heroj: Ulovimo lika s weba, koji tvoje eure vreba.“, koja će trajati cijelu 2023. godinu, kako bi se smanjili rizici za hrvatske građana i trgovačka društva od različitih oblika kibernetičkih napada.

U cilju pružanja pomoći građanima i pravnim osobama, koje su oštećeni zloćudnim računalnim programima koji šifriraju podatke na njihovim računalima i serverima (Cryptolocker Ransomware), Služba kibernetičke sigurnosti zajedno s Europolom pruža pomoć i savjete te besplatne alate za dekripciju podataka na internetskoj adresi www.nomoreransom.org

Tijekom 2022. godine nastavljene su slijedeće aktivnosti koje će se dovršiti u narednom razdoblju:

„Cybercrime Classroom Project“ – u vrijednosti od 120.000,00 US$, kojim je Veleposlanstvo SAD-a u Zagrebu doniralo MUP-u opremu za učionicu na Policijskoj akademiji u Zagrebu za provođenje treninga policijskih službenika u području suzbijanja kibernetičkog kriminaliteta i digitalne forenzike i uključuje 25 računala, server i pametnu ploču.

„Održivost kapaciteta policije za suzbijanje kibernetičkog kriminaliteta“, koji se financira u okviru Nacionalnog programa oporavka i otpornosti u iznosu od 1 600 000 EUR, sa sljedećim aktivnostima:

Nabava kompleta i sustava za istraživanje kibernetičkog kriminaliteta, pretraživanje otvorenih izvora na internetu i digitalnu računalnu forenziku, a koja će se provesti u okviru procesa javne nabave– 130 računala za sve PU

Nabava istražiteljskih analitičkih računalnih setova za analizu digitalnih dokaza, a koja će se provesti u okviru procesa javne nabave – 130 računala za sve PU

Nabava modula za edukaciju policijskih službenika kojom je predviđena java nabava 11 modula edukacija za 65 policijskih službenika u ukupnom trajanju od 150 radnih dana.

Policijski službenici Službe kibernetičke sigurnosti provode konstantu obuku i edukaciju policijskih službenika na regionalnoj razini u području digitalne forenzike i istraživanja kibernetičkih napada i spolnog zlostavljanja djece putem interneta. U vezi s time 2022. godine provedeni su sljedeći treninzi za policijske službenike:

- „Postupanje s elektroničkim dokazima na mjestu događaja“,
- „Napredne metode i postupci u digitalnoj forenzici“,
- „Istraživanje kibernetičkih napada“,
- „Istraživanje dječje pornografije na internetu“
- „Istraživanje otvorenih izvora na internetu“.

NCERT

Nacionalni CERT je tijekom 2022. godine zaprimio i obradio ukupno 1296 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su phishing, scam i phishing URL.

Promjena u odnosu na prošlu godinu je veći broj korisničkih prijava računalno-sigurnosnih incidenata. Nacionalni CERT je u odnosu na 2021. godinu zaprimio i obradio 7% više incidenata. Rezultat je to veće vidljivosti Nacionalnog CERT-a u javnosti, ali i neprestanog usavršavanja alata za detekciju kompromitacija i dodavanje novih izvora informacija. Zbog velike ovisnosti o tehnologijama i sve sofisticiranijim metodama napadača i u narednim godinama očekujemo trend laganog povećanja ukupnog broja obrađenih incidenata.

Velika promjena odnosi se na rast broja incidenta koji su klasificirani kao scam koji je u 2022. godini došao na drugo mjesto. Razlog tome je povećan broj prijava takvih incidenata od strane građana uslijed objavljivanja upozorenja o scam i phishing kampanjama na mrežnim stranicama Nacionalnog CERT-a.

S obzirom na to da web defacement, phishing URL, malware URL i spam URL zapravo predstavljaju kompromitirana web sjedišta, ako se gleda sumarno, broj otkrivenih kompromitiranih web sjedišta smanjio se za 38,7% u odnosu na prethodnu godinu.

SOA

Nastavno na 2020. i 2021. godinu, kada je bilo uočljivo globalno premještanje ključnih sigurnosnih procesa u kibernetički prostor, dijelom kao rezultat aktualne COVID-19 pandemije, ali ponajviše kao posljedica brzog tehnološkog razvoja, 2021. godina, kao prva godina tzv. digitalne dekade, donijela je čitav niz globalnih kibernetičkih ugroza kakve do tada nisu viđene u globalnim razmjerima, a 2022. godina obilježena je nizom globalnih kriza uzrokovanih ruskom agresijom na Ukrajinu te daljnjim pogoršavanjem stanja sigurnosti globalnog kibernetičkog prostora.

Kibernetički napadi korištenjem lanca nabave kao što je bio Solarwinds na prijelazu u 2021. godinu, ili Kaseya sredinom 2021. godine, kroz masovne napade državno-sponzoriranih kibernetičkih APT grupa, kao i kroz napade organiziranih kibernetičkih kriminalnih skupina, pokazali su važnost podizanja razine kibernetičke sigurnosti ne samo u državnom sektoru, već u društvu u cjelini, a posebno u kritičnoj infrastrukturi. Tako je 2022. godinu obilježio ubrzani proces kibernetičke regulacije započet u EU NIS2 direktivom koja je objavljena 27.12.2022. godine te ulazi u proces transpozicije, zajedno s CER direktivom o kritičnoj infrastrukturi, te DORA uredbom za financijski sektor. Ova prva skupina akata nastavljena je CRA uredbom o kibernetičkoj otpornosti proizvoda koja je u prijedlogu od rujna 2022. i ulazi u proces usuglašavanja tijekom 2023. godine.

Ucjenjivački kibernetički napadi (*Ransomware*), primjerice kroz napad na Colonial Pipeline u svibnju 2021. postali su ogroman globalni problem usporediv s terorizmom, zbog čega su SAD započele okupljanje partnerskih država protiv ucjenjivačkih kibernetičkih napada kroz CRI inicijativu (*Counter Ransomware Initiative*).

Globalni sigurnosni procesi i trendovi u velikom djelu su i 2022. godine ostali uvjetovani razvojem novih tehnologija koje kontinuirano donose nove rizike i izazove. Takve nove tehnologije traže osposobljenost sigurnosnih institucija, ali i proizvođača i dobavljača 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.

Prema podacima Centra za kibernetičku sigurnost SOA-e broj kibernetičkih napada u 2022. godini u značajnoj mjeri se nastavio povećavati, upravo uslijed promjena koje su kibernetičkim napadačima omogućile masovna digitalizacija i sve bolja suradnja između različitih vrsta kibernetičkih napadača, ali i pod utjecajem ruskih državno-sponzoriranih kibernetičkih grupa koje su provodile niz aktivnosti u potpori ruske agresije na Ukrajinu. Rezultat svih ovih promjena je da današnji kibernetički napadi imaju i dalje rastući 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.

Nakon prvih javnih EU atribucija tijekom 2020. godine, za kibernetičke napade državnih i drugih aktera iz Ruske Federacije, NR Kine i Sjeverne Koreje, koje su bile praćene 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), 2021. godina donijela je u srpnju i prvu zajedničku atribuciju kineskih državno-sponzoriranih kibernetičkih napadača od strane EU-a i NATO-a. U 2022. godini koordinirane aktivnosti javnih atribucija su se nastavile te je i NATO i EU osudio kibernetičke napade na Crnu Goru i Albaniju tijekom ljeta 2022. godine. Time je započela snažna diplomatsko-politička kampanja za odgovorno ponašanje država u kibernetičkom prostoru, temeljena na UN-ovim normama odgovornog ponašanja država u kibernetičkom prostoru. Nastavljen je globalni trend korištenja složenih taktika i tehnika APT napada za kibernetičke napade na poslovne sustave strateških i velikih kompanija u svrhu ucjenjivačkih kibernetičkih napada (*Ransomware*).

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 država u osiguravanju društva i industrije. Republika Hrvatska je, posebice kao članica NATO-a i EU-a, i u 2022. godini bila 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. Centar za kibernetičku sigurnost SOA-e bilježi u 2022. godini porast od preko 35% u broju otkrivenih državno-sponzoriranih kibernetičkih napada na godišnjoj razini.

Stoga je SOA, u suradnji s drugim nadležnim nacionalnim tijelima, ubrzano nastavila opsežan proces prevencije i zaštite nacionalnog kibernetičkog prostora. U okviru ovog procesa, SOA je nastavila s profiliranjem svog Centra za kibernetičku sigurnost. Cilj uspostave Centra je zaštita nacionalnog kibernetičkog prostora od državno sponzoriranih kibernetičkih napada i APT kampanja pomoću sustava senzora smještenih u tijelima i pravnim osobama. 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. Tijekom 2022. godine, a na temelju Odluke Vlade od 01.04.2021. godine, opseg sustava SK@UT dodatno je proširen na više sektora ključnih usluga kao i na više pravnih osoba od posebne važnosti za RH te je do kraja 2022. godine preko 60 državnih tijela i pravnih osoba uključeno u ovaj tzv. „kibernetički kišobran“ RH.

U razdoblju od travnja do lipnja 2022. godine, temeljem suglasnosti Vlade RH i na prijedlog SAD-a, provedena je zajednička napredna kibernetička sigurnosna operacija pod nazivom Hunt Forward. Nositelj operacije ispred RH bila je SOA, a nositelj operacije ispred SAD-a bila je Kibernetička komanda SAD-a (USCYBERCOM). Cijela operacija odvijala se u okviru Centra za kibernetičku sigurnost SOA-e, gdje je bio smješten i kibernetički tim SAD-a.

U cilju uvođenja sustavnog pristupa u području nacionalnog upravljanja kibernetičkim krizama, SOA je tijekom 2022. godine nastavila rad na stvaranju nacionalnog koncepta upravljanja kibernetičkim krizama koji je usklađen s aktualnim pristupom EU-a te će biti nacionalno propisan sukladno zahtjevima NIS2 transpozicije. Međuresorna stručna radna skupina za

područje upravljanja kibernetičkim krizama (SOA, MUP, MORH, VSOA, ZSIS, NCERT, HAKOM i HNB) sastaje se na kvartalnoj razini i provodi testiranje aktivnosti propisanih nacionalnim standardnim operativnim procedurama za upravljanje kibernetičkim krizama.

U okviru projekta Europske komisije, ENISA-e i CyCLONe-a, SOA je kao nadležno nacionalno tijelo organizirala nacionalni pristup EU Pilot projektu potpore razvoja kibernetičke otpornosti EU država članica te provela nominacije za niz kibernetičkih usluga za državna tijela i pravne osobe koje će u cijelosti biti financirane bespovratnim EU sredstvima u iznosu od oko 1,5 miliona EUR-a tijekom razdoblja od 2023. – 2025. godine, pri čemu će sva EU sredstva za provedbu dobiti tri hrvatske tvrtke koje su izabrane na javnom natječaju EU-a.

Uz opisane aktivnosti izgradnje i širenja opsega sustava SK@UT, nacionalnih operativnih procedura upravljanja kibernetičkim krizama te kontinuirani analitički proces praćenja stanja u nacionalnom i globalnom kibernetičkom prostoru, u cilju daljnjeg unaprjeđenja sigurnosnog stanja nacionalnog kibernetičkog prostora, od 2022. godine u okviru Centra za kibernetičku sigurnost djeluje i združeni kibernetički tim SOA-e, VSOA-e i ZSIS-a.

Također je krajem 2022. godine Centar započeo pripreme za nacionalnu transpoziciju NIS2 direktive.

ZSIS

Zavod za sigurnost informacijskih sustava (ZSIS) je tijekom 2022. godine zaprimao prijave koje se mogu klasificirati kao računalno-sigurnosni incidenti (RSI). Prema važećoj Nacionalnoj taksonomiji računalno-sigurnosnih incidenata tri najzastupljenije vrste zabilježenih RSI spadaju u kategorije prijevara, uspješno ostvarene kompromitacije i probleme dostupnosti. Taj trend se u velikoj mjeri poklapa s trendom iz prethodne 2021. godine. Nadalje, sagledavajući kompleksnost pojedinih RSI može se istaknuti kako je tijekom 2022. godine bilo zabilježeno više RSI koji su bili sofisticirani i opsežni te je trebalo uložiti puno više napora u tehničkoj analizi, detekciji i oporavku informacijskih sustava.

Kroz 2022. godinu veliki dio raspoloživih resursa ZSIS je angažirao u poslovima vezanim uz preventivne aktivnosti te su provođene provjere ranjivosti sukladno dostavljenim zahtjevima. Nadalje, uspostavljen je produkcijski sustav SK@UT PDNS odnosno rekurzivni DNS poslužitelj koji korisnicima pruža uslugu filtriranja upita koji idu od korisnika prema malicioznim domenama. Svrha sustava je pružanje dodatne zaštite prvenstveno korisnicima iz državnih tijela i institucija, odnosno i drugih korisnika koji bi u budućnosti koristili sustav. Provedeno je uključenje nekoliko korisnika koji su dostavili zahtjeve, te su planirana i buduća proširenja. Slijedeći servis kroz koji je pružana podrška korisnicima je SK@UT Skener. Na temelju zahtjeva korisnika ZSIS provodi skeniranje javno dostupnih sučelja i servisa s ciljem detekcije poznatih ranjivosti te o pronalasku i potvrđivanju istih obavještava korisnike o potrebi uklanjanja istih.

U okviru međunarodne suradnje ZSIS je imao suradnju kroz različite radne skupine Europske agencije za kibernetičku sigurnost i institucije EU (ENISA MB, CSIRT Network, NLO, itd.),

suradnju s NATO institucijama te je sudjelovao u dvije velike međunarodne vježbe Cyber Europe 2022 i Cyber Coallition 2022.

Kroz međuresornu suradnju ZSIS je surađivao s državnim tijelima i institucijama sukladno potrebama i upitima koje je zaprimao, a posebno je bio aktivan u radu mješovitih timova u Centru za kibernetičku sigurnost SOA-e, Međuresorne radne skupine za upravljanje u kibernetičkim krizama, Nacionalnom vijeću za kibernetičku sigurnost, Operativno-tehničkoj koordinaciji za kibernetičku sigurnost, itd.

ZSIS je vršio i sve druge zadaće i poslove iz propisanih mjerodavnosti.

HAKOM

Pružatelji elektroničkih komunikacijskih usluga su obvezni najmanje jednom godišnje provoditi procjenu rizika te reviziju sigurnosti mreža i usluga kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti iz Dodatka 1 Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga koji je ažuriran u listopadu 2021. Nalaz revizije zajedno s planom uklanjanja uočenih nedostataka, pružatelji koji imaju više od 100 000 korisnika su obvezni dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu. Stoga, HAKOM je u 2022. godini nakon analize dostavljenih revizija i sigurnosnih politika uočio određene nedostatke te putem inspekcijskih postupaka odredio određene mjere za uklanjanje ovih nedostataka u svrhu sprječavanja i umanjenje utjecaja sigurnosnih i računalno-sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže ili za osiguranje cjelovitosti mreža i usluga. Značajnih incidenata kibernetičke prirode nije bilo u ovom sektoru tijekom 2022. pa to pokazuje dobru pripremljenost i sposobnost hrvatskih operatora za odgovor na kibernetičke prijetnje.

HNB

Financijske institucije česta su meta kibernetičkih napada pa je tako u 2022. godini zabilježeno 11 značajnih incidenata što je jednak broj kao i prethodne godine. Samo jedan incident može se klasificirati kao sigurnosni incident dok su ostali operativnog karaktera. Sigurnosni incident nastao kod jedne financijske institucije posljedica je uspješno izvedenog phishing napada na zaposlenike, nakon čega se s poslužitelja elektroničke pošte počeo slati veliki broj phishing poruka. Uz pomoć tvrtke specijalizirane za odgovor na incidente i forenzičku analizu provedene su korektivne aktivnosti te forenzička analiza informacijskog sustava. Izvršenom analizom nisu pronađeni pokazatelji da je sustav zaražen zlonamjernim kodom ili da je napadač i dalje prisutan u sustavu.

Uz ovaj incident, prvi i drugi kvartal obilježio je povećani broj DDoS napada. Zabilježeni DDoS napadi uglavnom su bili slabijeg intenziteta i kraćeg trajanja te nisu značajno utjecali na poslovanje, dok su intenzivniji napadi uglavnom spriječeni korištenjem anti-DDoS zaštite.

Protekla godina obilježena je pripremama i prilagodbama IT sustava financijskih institucija za zamjenu nacionalne valute eurom. Hrvatska narodna banka je kontinuirano pratila proces prilagodbe te je za te potrebe izradila i diseminirala "Preporuke za prilagodbu IT sustava KI za pripremu konverzije" u kojima se uz samu pripremu na konverziju osvrnula i na kontigencijske planove te preporuke za održavanje primjerene razine sigurnosti. Početkom prosinca uočena je povećana aktivnost sofisticiranih phishing napada u kojima je primijećeno i to da je napadač posebno aktivan i promptan na reakciju unutar regularnog radnog vremena što ukazuje na dobru pripremljenost i profesionalnost izvođenja napada.

Svi zabilježeni incidenti bili su vrlo ograničenog učinka na poslovanje financijskih institucija u Republici Hrvatskoj, što ukazuje na dobru pripremljenost i sposobnost za odgovor na kibernetičke prijetnje.

NCERT

NATO međunarodna vježba „Cyber Coalition 22“

Članice OTKKS-a sudjelovale su u NATO međunarodnoj vježbi „Cyber Coalition 22“. Cilj vježbe je osnažiti koordinaciju i suradnju između NATO Saveza i njegovih članica, te poboljšati mogućnosti odvraćanja, obrane i suzbijanja prijetnji u i kroz kibernetički prostor.

„Cyber Coalition 2022“ najveća je NATO vježba u području kibernetičke obrane. Organizirana je od strane Savezničkog zapovjedništva za transformacije (ACT), a održavala se od 29. studenog do 03. prosinca na više desetaka lokacija u zemljama sudionicama. U 14. izdanju vježba je okupila više od 1000 sudionika iz 34 zemalja članica NATO-a i partnerskih zemalja, akademske zajednice i industrije. Organizacija vježbe je po drugi put suočena sa specifičnim izazovima provedbe svih zapovijeđenih mjera suzbijanja epidemije SARS COV-2.

Scenariji na vježbi simulirali su ugroze iz stvarnog života kao što su napadi na električne mreže, programe i sredstva NATO-a i Saveznika tijekom vojnih operacija.

CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u pravnom scenariju te su koordinirali sudjelovanje igrača i igračica iz privatnog sektora i akademske zajednice.

Republika Hrvatska u vježbi sudjeluje od 2009. godine kao promatrač, a od 2013. kao aktivni sudionik vježbe. Od 2016. Zapovjedništvo za kibernetički prostor određeno je kao nacionalni nositelj vježbe.

Međunarodna vježba „Cyber Europe 22“

U organizaciji Agencije Europske unije za kibernetičku sigurnost (ENISA), 8. i 9. lipnja 2022. godine održana je vježba Cyber Europe. Paneuropska vježba obuhvatila je stručnjake iz 29 zemalja Europske unije i Europskog udruženja slobodne trgovine (EFTA) te agencije i institucije EU, ENISA-u, CERT institucija, tijela i agencija Europske unije (CERT-EU),

Europol i Europsku agenciju za lijekove (EMA). Vježbe Cyber Europe omogućavaju analizu naprednih incidenata u području kibernetičke sigurnosti te rješavanje složenih situacija u pogledu kontinuiteta poslovanja i upravljanja krizom. Ove godine, fiktivni scenarij obuhvatio je napad na infrastrukturu i usluge zdravstvenog sustava uz prijetnju objave osobnih medicinskih podataka u više zemalja Europske unije te kampanju dezinformiranja i diskreditiranja. Sukladno tome, u vježbi su ispred Republike Hrvatske u ulozi igrača sudjelovala i tijela zdravstvenog sektora povezana s opskrbom i logistikom, predstavnici malih i velikih bolnica – kao i predstavnici Ministarstva zdravstva u procesu organizacije i koordinacije.

Projekt Grow2CERT

Nacionalni CERT je u 2022. godini završio s provedbom projekta sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe (eng. CEF – Connecting Europe Facility) pod nazivom Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti (eng. Increasing maturity of National CERT for stronger cooperation in cybersecurity community).

Cilj projekta je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Jedna od najvećih aktivnosti projekta bila je integracija dodatnih komponenti na Nacionalnoj platformi za prijavu incidenata i prijetnji PiXi. Dodatne komponente odnose se na prijavu incidenata sa znatnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Osim PiXi jedna od većih aktivnosti je podizanje svijesti korisnika o kibernetičkoj sigurnosti.

EUROPSKI MJESEC KIBERNETIČKE SIGURNOSTI

Između ostalog, u 2022. godini obilježen je jubilarni deseti Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2022. godine proveden je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti. Nacionalni CERT je ponovno imao ulogu nacionalnog koordinatora za provedbu europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti tijekom listopada te je ažurirao sadržaj na stranici https://cybersecuritymonth.eu/countries/croatia.

U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je treće izdanje hrvatskog CTF natjecanja za srednjoškolce, provedeno od 14. do 16. listopada 2022. godine. Natjecanje je bilo organizirano u obliku CTF-a (Capture the Flag), a cilj mu je proširiti svijest o važnosti primjene sigurnosnih mjera te izbjegavanju i ispravljanju mogućih sigurnosnih propusta u programskom kôdu, postavkama ili nekoj drugoj komponenti računalnog sustava. Pravo sudjelovanja imali su svi učenici srednjih škola u Republici Hrvatskoj uz mentorstvo svojih profesora kao prijavitelja tima. U natjecanju je sudjelovao 270 učenika u 54 srednjoškolska tima iz 33 srednje škole.

MORH

NATO međunarodna vježba „Cyber Coalition 22“

Ministarstvo obrane Republike Hrvatske također je sudjelovalo u NATO međunarodnoj vježbi „Cyber Coalition 22“. Dva djelatnika su se nalazila u Tallinu, Estonija, dok je 145 djelatnika Oružanih snaga Republike Hrvatske, Ministarstva obrane Republike Hrvatske, državnih tijela, te akademske i industrijske zajednice sudjelovalo u Republici Hrvatskoj.

CAX MVV „CyberNet22“

Međunarodna vojna vježba „CyberNet 22“ je godišnja vježba PESCO CRRT tima koja se provodi u Kraljevini Nizozemskoj. Cilj vježbe Uvježbavanje međunarodnog tima za brzi odgovor u odgovoru na računalne prijetnje. 2022. godine na vježbi su sudjelovala 2 djelatnika Zapovjedništva za kibernetički prostor. Vježba se provela u vremenu od 16. do 19. svibnja 2022. godine.

CAX MVV „Amber Mist 22“

Međunarodna vojna vježba „Amber Mist 22“ je godišnja vježba PESCO CRRT tima koja se provodi u Republici Litvi. Cilj vježbe Uvježbavanje međunarodnog tima za brzi odgovor u odgovoru na računalne prijetnje. 2022. godine na vježbi su sudjelovala 2 djelatnika Zapovjedništva za kibernetički prostor. Vježba se provela u vremenu od 19. do 26. kolovoza 2022. godine.

5. ZAKLJUČAK

U prethodnoj godini nastavio se snažan angažman državnih tijela na unaprjeđenju sigurnosti hrvatskog kibernetičkog prostora. Istovremeno, izazovi su postali sve veći. Spomenimo samo agresiju na Ukrajinu i njezine refleksije na kibernetički prostor, kibernetički kriminal koji je sve sofisticiraniji, sve veću digitalizaciju i ovisnost o elektroničkim uslugama, nedostatak dovoljno stručnog osoblja.

Republika Hrvatska se s izazovima u području kibernetičke sigurnosti nosila kroz suradnju, razmjenu informacija, usklađivanje postupanja, kako između tijela tako i unutar asocijacija kojima pripada. Potrebno je ipak naglasiti kako su postupanja u području kibernetičke sigurnosti još uvijek najvećim dijelom u početnoj fazi: temelje se na dobrovoljnoj suradnji, adresiraju se kritični momenti, sredstva se osiguravaju iz postojećih proračuna državnih tijela uz financiranje iz EU fondova, ali još uvijek ne postoji vodeće nadležno tijelo koje bi imalo kapacitet realizirati složenije projekte.

Nova Nacionalna strategija kibernetičke sigurnosti i novi Zakon o kibernetičkoj sigurnosti bi trebali napraviti značajan iskorak i odgovarajuće se nositi i suprotstavljati rizicima čiji se rast očekuje u sljedećih 3-5 godina te pružiti sigurnost i povjerenje građanima i organizacijama.

Raspoloživi materijali povezani s radom Vijeća dostupni su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na mrežnim stranicama Ureda Vijeća za nacionalnu sigurnost[8].

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

6. ČLANOVI VIJEĆA

Tijekom godina rada Vijeća, na prijedlog nadležnih institucija došlo je do promjena pojedinih članova i zamjenika članova, a tijekom 2022. Vijeće radi u sljedećem sastavu:

Članovi Vijeća:	**Zamjenici članova Vijeća:**
Suzana Galeković	Andrej Milovac
dr. sc. Damir Trut	Marjan Vukušić, Davor Spevec
Sebastian Rogač	Tihomir Lulić
Nataša Mikuš Žigman	Maja Radišić Žuvanić, Davor Golenja
Goran Kolarić	Sandra Lukić
brg Eduard Špoljarić	bjn Nikola Bokulić
Vedrana Šimundža Nikolić	Ana Kordej, Bruno Ždero
dr. sc. Ivan Matić	Mario Bušić
Dražen Ljubić	Krešimir Šipek
Mario Miljavac	Mirko Korajac
Nataša Glavor	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

Administrativnu i tehničku potpora radu Vijeća pruža UVNS, gđa Iva Jeličić i g. Vinko Kuculo.

Administrativnu i tehničku potporu radu Koordinacije pruža MUP.