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 2023. GODINU

SADRŽAJ

1. SAŽETAK

Nacionalno vijeće za kibernetičku sigurnost (Vijeće) osnovano je 2017., prošireno je 2018., te je i tijekom 2023. godine u njegov rad bilo uključeno 16 tijela. Fokusira se na koordinaciju nacionalnih inicijativa u kibernetičkoj sigurnosti, vođeno ciljevima Nacionalne strategije kibernetičke sigurnosti (Strategija) i Akcijskog plana za njeno provođenje („Narodne novine", br. 105/2015). Paralelno s Vijećem, formirana je i Operativno-tehnička koordinacija za kibernetičku sigurnost (Koordinacija), usmjeravana od Vijeća, a u koordinaciji Ministarstva unutarnjih poslova.

Tijekom 2023. godine, Vijeće je redovito održavalo sjednice na kojima su se raspravljala pitanja iz područja kibernetičke sigurnosti. Glavna aktivnost Vijeća bila je transpozicija nove Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS2 direktiva zamjenjuje prethodnu NIS direktivu i modernizira pravni okvir za kibernetičku sigurnost). Odlučeno je uspostaviti Nacionalni centar za kibernetičku sigurnost unutar Sigurnosno-obavještajne agencije kako bi se poboljšala koordinacija postupanja tijela u kibernetičkim pitanjima i podrška ključnim sektorima te osiguralo koordinirano centralizirano upravljanje sigurnošću kibernetičkog prostora Republike Hrvatske.

Tijela uključena u Vijeće sudjelovala su tijekom godine u nizu nacionalnih i međunarodnih aktivnosti vezanih uz kibernetičku sigurnost, uključujući radne skupine, vježbe, suradnju s drugim državama te inicijative za koordinaciju i podršku u području kibernetičke sigurnosti. Posebne aktivnosti bilježe se u sektorima obrazovanja, elektroničkih komunikacija, vanjskih poslova, gospodarstva, obrambenog sektora, ali i drugima.

2. UVOD

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 Republike Hrvatske na sjednici održanoj 16. veljače 2017. godine. Odlukom Vlade Republike Hrvatske 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 djeluje kroz 16 tijela. Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u **Koordinaciju**, koja započinje s radom 23. ožujka 2017. održavanjem prve sjednice[1].
Konstituiranjem Vijeća i Koordinacije otvoren je put za ostvarenje ciljeva Strategije i punu provedbu mjera Akcijskog plana za njezinu provedbu („Narodne novine", broj: 108/15).

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). Kroz svoje djelovanje, Vijeće je dodatno unaprjeđivalo i snažilo uspostavljenu formalnu međusektorska koordinaciju 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 ZA 2023. GODINU

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 imenovala su 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 2023. godine Vijeće je održalo 12 sjednica. Na svim, osim jednoj, od održanih sjednica je ostvaren kvorum za donošenje odluka. 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 2023. GODINI

Ključna aktivnost Vijeća u 2023. godini je bila transpozicija nove Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS2 direktiva). NIS2[2] direktiva je stupila na snagu 16. siječnja 2023., a rok za njenu transpoziciju je 17. listopada 2024. NIS2 direktiva zamjenjuje NIS[3] direktivu iz 2016. godine i modernizira postojeći pravni okvir kako bi se održao korak s povećanom digitalizacijom i promjenjivim okruženjem prijetnji kibernetičkoj sigurnosti. Proširenjem područja primjene pravila o kibernetičkoj sigurnosti na nove sektore i subjekte dodatno se poboljšava otpornost i kapaciteti za odgovor na incidente javnih i privatnih subjekata, nadležnih tijela i EU-a u cjelini.

Usko povezani akti s NIS2 direktivom, DORA[4] i CER[5] također su stupili na snagu 16. siječnja 2023., ali za razliku od NIS2 direktive iste se neće transponirati kroz radne skupine Vijeća, već u okviru redovnih aktivnosti nadležnih tijela.

Iskustva u implementaciji i provedbi NIS direktive kroz donošenje Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", br. 64/2018) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", br. 68/2018.), te provođenje identifikacije operatora, radionica, nadzora i izvješćivanja pokazala su da najveći dio nadležnih sektorskih tijela ima vrlo ograničene mogućnosti aktivne potpore kibernetičkoj sigurnosti subjektima u svojim sektorima. Povećani zahtjevi NIS2 direktive bi dodatno povećali jaz između zakonodavnih i stvarnih potreba potpore kibernetičkoj sigurnosti ključnih društvenih i gospodarskih sektora i s druge strane usluga i mogućnosti nadležnih sektorskih tijela te je ocijenjeno kako je nužno uspostaviti nacionalno tijelo, Nacionalni centar za kibernetičku sigurnost u okviru Sigurnosno-obavještajne agencije, koji bi, uz odgovarajuće zakonske ovlasti i nadogradnju vlastitih sposobnosti, postao središnje državno tijelo za kibernetičku sigurnost.

Do stupanja na snagu novog Zakona o kibernetičkoj sigurnosti („Narodne novine", br. 14/2024), kojim se mijenja i dosadašnji način nacionalne koordinacije u području kibernetičke sigurnosti, Vijeće je nastavilo redovito održavati sjednice i razmjenjivati informacije o svim aktivnosti poveznim s kibernetičkom sigurnošću. Temeljem usklađenih stavova, tijela u Vijeću su provodila aktivnosti samostalno, sukladno nominalnim nadležnostima propisanim *Zakonom*

[2] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS2) (SL L 333/80, 27.12.2022.)

[3] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije

[4] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj 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

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

o ustrojstvu i djelokrugu tijela državne uprave („Narodne novine“, broj: 85/20) i drugim zakonskim, podzakonskim aktima te odlukama Vlade Republike Hrvatske.

U 2023. je nastavljeno dogovaranje o uspostavi Nacionalnog koordinacijskog središta za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti (slijedom ***Uredbe o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i Mreže nacionalnih koordinacijskih centara***[6]), te je Nacionalni koordinacijski centar uspostavljen unutar CARNET-a s upravljačkim odborom kojeg čine predstavnici Središnjeg državnog ureda za razvoj digitalnog društva, Ministarstva znanosti i obrazovanja, Ministarstva gospodarstva i održivog razvoja, Ministarstva unutarnjih poslova, Ministarstva obrane, Ministarstva mora, prometa i infrastrukture, Ureda predsjednika Vlade Republike Hrvatske, Sigurnosno-obavještajne agencije te ravnatelj CARNET-a, ali bez prava glasa.

Radna skupina Vijeća za 5G je tijekom godine održala više sastanaka na kojima su raspravljena različita pitanja vezana uz implementaciju mjera za sigurnost elektroničkih komunikacija, poput sigurnosti povodnih komunikacijskih kabela, implementacije EU toolboxa za sigurnost 5G mreža i sigurnosne procjene temeljem Poziva iz Nevera.

Radne skupine Vijeća su radile na izradi nove Nacionalne strategije kibernetičke sigurnosti.
Članovi Vijeća su održali sastanak s *Uradom Vlade Republike Slovenije za informacijsku varnost* na temu suradnje u području kibernetičke sigurnosti.

Inicijativa Vijeća vezana uz korištenje prefiksoida *„kiber“* u inačicama EU propisa na hrvatskom jeziku rezultirala je u travnju 2023. godine dogovorom o budućem korištenju pridjeva „kibernetički“ umjesto prefikosida *„kiber“* u svim novim EU zakonodavnim aktima..

Tijela uključena u Vijeće su sudjelovala u mnogobrojnim nacionalnim i međunarodnim aktivnostima povezanim s kibernetičkom sigurnošću, pri čemu se redovito provodila koordinacija unutar Vijeća, ovdje izdvojene:

NCERT je uspostavio platformu hacknite.hr sa zadacima iz hakerskih natjecanja, sudjelovao na sastancima GEANT-a[7], sudjelovao u radu CSIRT[8] mreže, sudjelovao u vježbi Cyber Coalition 2023 i Cyber SOPEx, pripremama za vježbu Cyber Europe, sudjelovao u projektu „Dan sigurnijeg interneta“ i radnoj skupini Europski mjesec kibernetičke sigurnosti, radionici ENISA-e[9] o otkrivanju ranjivosti, e-Biz konferenciji, predavanjima za policijske službenike,

[6] 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
7 Europska multi-gigabitna akademska računalna mreža - https://geant.org/
8 CSIRT – Computer Security Incident Team - stručni tim koji obrađuje računalne sigurnosne incidente
CSIRT Network – EU mreža nadležnih CSIRT-ova država članica i CERT-EU
9 ENISA – European Union Agency for Cybersecurity

konferenciji za CARNET korisnike, Panelu o kibernetičkoj otpornosti u povezanom svijetu, te informirao javnost o ugrozama kibernetičke sigurnosti na svojim mrežnim stranicama.

MVEP je sudjelovao u sastancima na temu zajedničke sigurnosne i obrambene politike EU, sastancima vezanim uz Konvenciju o kibernetičkom kriminalitetu, sastancima vezanim uz Cyber Diplomacy Toolbox[10], sastancima vezanim uz Inicijativu o kibernetičkom iznuđivanju.

SDU RDD je sudjelovao u aktivnostima povezanim s Programom politike za digitalno desetljeće do 2030., Deklaracijom o digitalnim pravima i načelima, Lisnicom europskog digitalnog identiteta.

ZSIS je sudjelovao u radu upravljačkog odbora ENISA-e i u radu ECCG-a[11], a **UVNS** u radu NIS Grupe za suradnju Europske komisije.

MORH je održao radionicu s timom iz SAD-a o uvođenju kibernetičkog područja u vojnu doktrinu, sudjelovao u vježbi Cyber Coalition, sudjelovao u razgovorima na temu kibernetičke sigurnosti u okviru Američko-jadranske povelje, započeo s uspostavom Operativnog centra za kibernetičku sigurnost.

AZOP je sudjelovao u radu EU odbora za zaštitu podataka i u njegovoj radnoj skupini vezano uz korištenje umjetne inteligencije.

HAKOM je sudjelovao u radu BEREC-ove[12] radne skupine za kibernetičku sigurnost i u radu podskupine za 5G/Telecom NIS Grupe za suradnju, **MPU** je održalo regionalnu konferenciju o kibernetičkom kriminalitetu, **OTC** na sastanku EUROPOL-a, a **HNB** je sudjelovao u implementaciji DORA-e.

SOA je sudjelovala u radu EU-CyCLONe[13] mreže, HWPCI (Horizontalne radne skupine za kibernetička pitanja). U okviru Pilot projekta Europske komisije, ENISA-e i EU-CyCLONe mreže provedena je nominacija za 2023. godinu za 18 usluga za Republiku Hrvatsku pri čemu je osigurano 1,7 milijuna EUR-a kroz 100% financiranje EU.

O svim bitnim pitanjima iz navedenih aktivnosti informirano je Vijeće, koje je dalje raspravljalo i usmjeravalo nacionalnu koordinaciju i aktivnosti u pitanjima bitnim za sigurnost kibernetičkog prostora Republike Hrvatske.

[10] EU Cyber Diplomacy Toolbox - zajednički EU diplomatski odgovor na zloćudne kibernetičke aktivnosti
[11] ECCG - European Cybersecurity Certification Group
[12] BEREC - Body of European Regulators for Electronic Communications
[13] EU-CyCLONe Network - The European cyber crisis liaison organisation network

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

NIS2 direktiva, između ostalog, utvrđuje obvezne elemente koje nacionalne strategije kibernetičke sigurnosti država članica EU moraju sadržavati. Početkom 2023. nastavljen je rad radnih skupina Vijeća na izradi nove Nacionalne strategije kibernetičke sigurnosti, međutim, kako je napredovao rad na novom Zakonu o kibernetičkoj sigurnosti, zaključeno je kako je potrebno prvo dovršiti rad na zakonu i pripadajućoj uredbi kako bi se bolje uskladili zakonski i podzakonski akti sa strategijom te je u skladu s tim i dinamika rada radnih skupina revidirana.

Člankom 55. Zakona o kibernetičkoj sigurnosti i njegovim Prilogom IV. prenesene su u nacionalno zakonodavstvo odredbe NIS2 direktive koje se odnose na obveze država članica u pogledu strateškog planiranja u području kibernetičke sigurnosti.

Model koji predviđa Zakon o kibernetičkoj sigurnost vezano uz buduće akte strateškog planiranja iz područja kibernetičke sigurnosti usklađen je s općim propisom koji uređuje područje strateškog planiranja i upravljanja razvojem Republike Hrvatske, te isti uključuje i izradu akcijskog plana za provedbu akta strateškog planiranja.

Prvi akt strateškog planiranja iz članka 55. Zakona o kibernetičkoj sigurnosti bit će donesen u roku od 24 mjeseca od dana stupanja tog Zakona na snagu odnosno najkasnije do 15. veljače 2026. godine.

4. IZVJEŠĆE O RADU OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST ZA 2023. GODINU

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 2023. godine planirano je i održano 12 sjednica Koordinacije. Sve su sjednice Operativno – tehničke koordinacije, osim jedne, održane kao virtualne sjednice.

4.2. PREGLED AKTIVNOSTI OPERATIVNO-TEHNIČKE KOORDINACIJE U 2023.

Planom aktivnosti Operativno – tehničke koordinacije za 2023. 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 2023. 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 2023. godini
   rok: kvartalno – ožujak, lipanj, rujan, prosinac 2023. godine

4. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2023. godinu
   rok: siječanj 2024. godine

5. Procjena stanja kibernetičke sigurnosti u Republici Hrvatskoj na temelju podatka dobivenih provedbom dokumenta Metodologija procjene stanja kibernetičke sigurnosti Republike Hrvatske
   rok: prosinac 2023. godine

6. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj
   rok: prosinac 2023. godine

Operativno – tehnička koordinacija je tijekom 2023. 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-a i CARNET-a – NCERT-a.
   Tijekom 2023. 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, najčešće su prijavljivani phishing (504 prijave), phishing URL (190), scam (173), zaraze pojedinačnih računala malicioznim kodom (157) i pogađanje zaporki (153).

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 2023. 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 2023. godinu

Prijedlog godišnjeg Izvješća o radu Operativno – tehničke koordinacije za 2023. 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, odnosno integracije u cjelovito izvješće o radu Vijeća i Koordinacije u 2023.

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

Metodologija procjene stanja kibernetičke sigurnosti Republike Hrvatske 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.

Poslije inicijalne procjene, procjena stanja kibernetičke sigurnosti uporabom Metodologije procjene stanja kibernetičke sigurnosti Republike Hrvatske nije rađena, ali se stanje u kibernetičkom prostoru Republike Hrvatske kontinuirano pratilo i o primijećenim incidentima i prijetnjama redovito se raspravljalo na sjednicama OTKKS-a.

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 Republike Hrvatske početkom 2020 godine. Koordinacija smatra 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 Republika Hrvatska može iskoristiti društvene, ekonomske i političke prednosti interneta i korištenja novih tehnologija, policija je tijekom 2023. 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.

U 2023. godini policija je ukupno obradila 1 688 kaznenih djela koja predstavljaju najrazličitije oblike kibernetičkih napada. Materijalna šteta koja je izravna posljedica prijavljenih kibernetičkih napada iznosila je 10,5 milijuna EUR.

Ključni trendovi ugrožavanja kibernetičke sigurnosti:

Počinitelji kibernetičkih kaznenih djela su u najvećoj mjeri motivirani monetizacijom svojih aktivnosti, npr. korištenjem ransomware napada radi pribavljanja protupravne imovinske koristi. Kriptovalute su i dalje najčešća metoda pribavljanja protupravne imovinske koristi.
Kibernetički napadi imaju za svoju metu i sve više utječu na kritičnu infrastrukturu.
Poslovni kriminalni model Phishing-as-a-Service (PhaaS) i dalje je prevladavajući.
Zlouporaba osobnih podataka u fokusu je počinitelja kaznenih djela 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:

• Bankarske prijevare, koje ciljaju na tvrtke i građane, a kriminalci se lažno predstavljaju kao djelatnici hrvatskih poslovnih banaka te navode oštećenike da identifikacijske i verifikacijske podatke za pristup internetskom bankarstvu upisuju na lažnim stranicama banaka, čime kriminalcima omogućuju pristup računima, nakon čega sredstva na računima oštećenika neovlašteno prebacuju na druge bankovne račune koji se nalazi pod kontrolom kriminalnih organizacija.

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

Izazovi u otkrivanju počinitelja kaznenih djela povezani su s okolnošću da se najveći broj počinitelja nalazi u inozemstvu, te korištenjem tehnologija koje omogućuju anonimnost na internetu, kao što su VoIP tehnologija , VPN servisi i Tor mreže.

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 kibernetičkih kriminalaca najvrjedniji su resurs.

Ulaganje u tehnologiju nužan je preduvjet za identifikaciju počinitelja kibernetičkih napada i pronalazak elektroničkih dokaza – u posljednjih pet godina MUP je izravno uložio preko 1 000 000 EUR, a u tijeku je ulaganje od 1 600 000 EUR u okviru Nacionalnog programa oporavka i otpornosti, te 2 650 000 EUR u okviru Fonda za unutarnju sigurnost Europske unije. Navedenim ulaganjima nabavljaju se radne stanice za analizu digitalnih dokaza i istraživanje otvorenih izvora na interentu. Također se nabavljaju licence za obavljanje poslova forenzike digitalnih dokaza, te računalni programi za analizu transakcija kriptovaluta.

Tijekom 2023. godine započela je provedba kampanje osvještavanja javnosti o opasnostima na internetu „Web heroj: Ulovimo lika s weba, koji tvoje eure vreba.“, koja će se nastaviti u 2024. godini, kako bismo smanjili rizike za hrvatske građane i trgovačka društva od različitih oblika kibernetičkih napada. U okviru kampanje izrađena je internetska domena https://webheroj.hr/ koja sadrži savjete za građane i tvrtke i podatke o mogućnostima prijave kaznenih djela policiji.

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 Ravnateljstva policije zajedno s Europolom pruža pomoć i savjete te besplatne alate za dekripciju podataka na internetskoj adresi www.nomoreransom.org.

Policijski službenici Službe kibernetičke sigurnosti provode kontinuiranu obuku i edukaciju policijskih službenika na nacionalnoj i regionalnoj razini u području digitalne forenzike i istraživanja kibernetičkih napada. U vezi s time 2023. godine provedeni su sljedeći treninzi za policijske službenike:

- „Istraživanje kibernetičkih napada“,
- „Istraživanje dječje pornografije na internetu“
- „Istraživanje otvorenih izvora na internetu“.

NCERT

Tijekom 2023. godine zaprimljeno je i obrađeno ukupno 1236 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a.

Vodeći tipovi incidenata su phishing, phishing URL i scam.

Promjena u odnosu na prošlu godinu je smanjenje broja računalno-sigurnosnih incidenata od ukupno 4,63% u usporedbi s 2022. godinom. Razlog tome je velik broj zabilježenih phishing kampanja u kojima je izvor računalno-sigurnosnih incidenata bio isti, te su tretirani kao jedan incident.

Velika promjena odnosi se na porast broja incidenata koji su klasificirani kao Sustav zaražen zlonamjernim kôdom, u usporedbi s prošlom godinom ovaj tip incidenta je porastao za 263% odnosno s 54 incidenta na 142. Razlog ovom porastu je povećan broj vanjskih prijava te prijave zaprimljene kroz suradnju s CSIRT zajednicom.

Također je zabilježen i porast broja incidenata koji su klasificirani kao phishing i phishing URL, u usporedbi s prošlom godinom. Ukupan broj incidenata s ovom klasifikacijom porastao je za 53, što označava uvećanje od 9,52%, čime incidenti tipa phishing čine 49% svih incidenata.

Razlog tome je povećan broj takvih incidenata prijavljenih od građana za koji se pretpostavlja da se dogodio uslijed objavljivanja upozorenja o phishing kampanjama na mrežnim i društvenim stranicama, kao i veće javne vidljivosti Nacionalnog CERT-a. Isto tako zabilježene su phishing kampanje u kojima napadači imitiraju legitimne servise koje koriste velik broj građanstva.

SOA

Tijekom 2023. godine Europska unija je, kao i niz partnerskih zemalja, poduzela značajne aktivnosti u pripremi nove i sveobuhvatne regulative kibernetičke sigurnosti. Niz donošenja novih EU akata u ovom području započet je donošenjem NIS2 direktive, DORA uredbe za financijski sektor i CER direktive za kritičnu infrastrukturu, a nastavljen je radom na pripremi Akta o kibernetičkoj otpornosti (Cyber Resilience Act – CRA[14]), Akt o kibernetičkoj solidarnosti (Cyber Solidarity Act – CSoA[15]), kao i izmjene pravnog okvira kibernetičke sigurnosne certifikacije u području upravljanih IKT i upravljanih IKT sigurnosnih usluga kroz izmjene Akta o kibernetičkoj sigurnosti iz 2019. godine[16] (Cyber Security Act Amendments – CSA+).

Broj kibernetičkih napada u 2023. 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 snažno 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 geografskom raspršenosti. Ucjenjivački kibernetički napadi (Ransomware), primjerice kroz poznati napad na američki naftovod Colonial Pipeline u svibnju 2021., također su rezultirali naučenim lekcijama i mobilizirali međunarodnu zajednicu u borbi protiv ovog kriminala. Najuspješniju i najveću inicijativu ove vrste otvorile su SAD kroz međunarodnu Inicijativu o kibernetičkom iznuđivanju (Counter Ransomware Initiative), u kojoj Republika Hrvatska aktivno sudjeluje.

Republika Hrvatska je, posebice kao članica NATO-a i EU-a, i u 2023. 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 u 2023. godini bilježi do

[14] Prijedlog uredbe Europskog parlamenta i Vijeća o horizontalnim zahtjevima kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020 i Direktive EU) 2020/1828 – u donošenju

[15] Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje prijetnji kibernetičkoj sigurnosti i incidenata, pripremu za njih i odgovor na njih – u donošenju

[16] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibernetičkoj 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)

sada najveći godišnji porast broja otkrivenih državno-sponzoriranih kibernetičkih napada na godišnjoj razini od preko 60%.

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 i izgradnje sustava SK@UT. Cilj uspostave sustava SK@UT je zaštita nacionalnog kibernetičkog prostora od državno-sponzoriranih kibernetičkih napada i APT kampanja pomoću sustava senzora smještenih u državnim 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 2023. 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 Republiku Hrvatsku te je do kraja 2023. godine preko 70 državnih tijela i pravnih osoba uključeno u ovaj tzv. „kibernetički kišobran" Republike Hrvatske. U lipnju 2023. godine je održana Prva SK@UT konferencija u organizaciji Sigurnosno-obavještajne agencije i Zavoda za sigurnost informacijskih sustava. Konferenciju su svojim izlaganjima otvorili ravnatelj SOA-e Daniel Markić i predsjednik Vlade Republike Hrvatske Andrej Plenković. Konferencija je okupila oko 200 sudionika, predstavnika državnih tijela i pravnih osoba uključenih u SK@UT, a razmatrane teme su obuhvaćale sigurnost nacionalnog kibernetičkog prostora, dijeljenje najboljih iskustava i praksi sustava SK@UT, izazove i potrebe transpozicije EU NIS2 direktive u nacionalno zakonodavstvo, kao i pitanja vezana uz ustrojavanje nacionalnog centra za kibernetičku sigurnost.

U cilju uvođenja sustavnog pristupa u području nacionalnog upravljanja kibernetičkim krizama, SOA je tijekom 2023. godine nastavila rad na stvaranju nacionalnog koncepta upravljanja kibernetičkim krizama koji je usklađen s aktualnim pristupom EU-a te je postao dio nacionalne transpozicije NIS2 direktive. Međuresorna stručna radna skupina za područje upravljanja kibernetičkim krizama (SOA, MUP, MORH, VSOA, ZSIS, NCERT, HAKOM i HNB) tijekom 2023. godine sastajala se na kvartalnoj razini, a izrađena kvartalna izvješća razmjenjivala su se koristeći nacionalnu platformu PiXi. Početkom 2023. godine napravljeno je prvo godišnje izvješće međuresorne radne skupine za upravljanje kibernetičkim krizama za 2022. godinu, koje je dostavljeno državnom vrhu.

U okviru Pilot projekta Europske komisije, ENISA-e i EU-CyCLONe-a potpore razvoja kibernetičke otpornosti EU država, Centar za kibernetičku sigurnost SOA-e je usmjeravao provedbu ovog Projekta te je na razini Republike Hrvatske koordinirao nominacije za niz kibernetičkih usluga za državna tijela i pravne osobe, koje su u cijelosti bile financirane bespovratnim EU sredstvima. Na temelju učinkovite koordinacije Pilot projekta osigurano je 40% povećanje EU sredstava za Republiku Hrvatsku u 2023. godini, pri čemu je ukupan trogodišnji iznos sredstava povećan na oko 1,7 milijuna EUR-a tijekom razdoblja od 2023. –

2025. godine. Projekt za korisnike iz Republike Hrvatske provode prema pravilima ENISA-e tri hrvatske tvrtke koje su izabrane na javnom natječaju EU-a.
Tijekom 2023. godine SOA je koordinirala radnu skupinu Nacionalnog vijeća za kibernetičku sigurnost za izradu NIS2 transpozicijskog Zakona o kibernetičkoj sigurnosti (ZKS). Tako je u 2023. godini provedeno e-Savjetovanje za ZKS, u okviru kojeg je odgovoreno na brojna pitanja i nejasnoće u javnosti i medijima. Predstavnici Centra za kibernetičku sigurnost SOA-e su također tijekom jeseni sudjelovali na brojnim stručnim konferencijama na kojima se raspravljalo o ZKS-u i njegovoj budućoj provedbi, a u cilju upoznavanja stručne javnosti s konceptima ZKS-a. Dana 13. prosinca Vlada je uputila Konačni prijedlog ZKS-a na drugo čitanje u Sabor, koje se očekuje početkom 2024. godine.

ZSIS

Zavod za sigurnost informacijskih sustava (ZSIS) je tijekom 2023. 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 uspješno ostvarene kompromitacije (37%), prijevare (31%) i probleme dostupnosti (14%). Taj trend se u velikoj mjeri poklapa s trendom iz prethodne 2022. godine, uz vidljivo povećanje trenda uspješno ostvarenih kompromitacija. Sagledavajući kompleksnost pojedinih RSI možemo istaknuti kako je tijekom 2023. 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.
Aktivnosti ZSIS-a tijekom 2023. godine su uglavnom bile istog intenziteta kao i tijekom 2022. godine u poslovima koordinacije, prevencije i odgovora na računalno-sigurnosne incidente, dok je zabilježena veća aktivnost u odnosu na 2022. godinu u području provođenja ranjivosti informacijskih sustava. Kroz 2023. godinu ZSIS je aktivno sudjelovao u radu na transpoziciji NIS2 direktive u nacionalno zakonodavstvo Republike Hrvatske. U lipnju 2023. godine održana je SK@UT konferencija u zajedničkoj organizaciji SOA-e i ZSIS-a na kojoj je primarno SK@UT zajednici korisnika prezentiran sustav, njegovi noviteti te su podijeljeni primjeri dobrih praksi kako bi se i dalje poticala svijest o važnosti kibernetičke sigurnosti.
Aktivno je nadograđivan produkcijski sustav SK@UT PDNS odnosno rekurzivni DNS poslužitelj koji korisnicima pruža uslugu filtriranja upita koji idu od korisnika prema malicioznim domenama. Provedena su dodatna uključenja zainteresiranih korisnika koji su dostavili zahtjeve. Sljedeći 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. Tijekom 2023. godine pokrenut je proces unaprjeđenja sustava kako bi se prvenstveno dobile nove funkcionalnosti koje bi trebale olakšati pretraživanje, dohvaćanje i administraciju.
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, MESSEU itd.), suradnju s NATO institucijama te je sudjelovao u međunarodnoj vježbi Cyber Coalition 2023. Također ZSIS je 2023. godine sudjelovao u procesu usuglašavanja i

koordinacije sudionika za vježbu Cyber Europe Exercise 2024 (CE24) uz suradnju NCERT-a te provodio usuglašavanje za vježbu i scenarije za vježbu koja će se održati u 2024. godini
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 („Narodne novine“, br. 52/2023, dalje: Pravilnik). 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 2023. godini nakon analize dostavljenih revizija i sigurnosnih politika uočio određene nedostatke te putem inspekcijskih postupaka (stručni nadzori 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. Ove godine prvi put su provedene i procjene rizika za 5G mreže operatora te su sva tri operatora implementirali propisane mjere u skladu s Pravilnikom.
Također, HAKOM je u 2023. proveo 4 inspekcijska nadzora unutar kojih su se provjeravala pojedina područja informacijske sigurnosti u mreži 4 najveća operatora. Time je ove godine ispunjen plan o minimalno 3 inspekcijska nadzora kod 3 velika operatora. Nadalje, HAKOM je sa 4 zaposlenika sudjelovao u NATO međunarodnoj vježbi „Cyber Coalition 23“.
Značajnih incidenata kibernetičke prirode nije bilo u ovom sektoru tijekom 2023. pa to pokazuje dobru pripremljenost i sposobnost hrvatskih operatora za odgovor na kibernetičke prijetnje.

HNB

Hrvatska narodna banka je u 2023. godini u sektoru bankarstva zabilježila četiri značajna incidenata što ukazuje na pad broja zabilježenih incidenata u odnosu na prethodnu godinu. Svi zabilježeni incidenti operativnog su karaktera, nisu narušili sigurnost informacijskih sustava banaka, imali su su vrlo ograničen učinak na poslovanje banaka te su za posljedicu imali kratkotrajnu nedostupnost usluga za krajnje korisnike.
Protekla godina u bankarskom sektoru obilježena je i nizom dobro pripremljenih i sofisticiranih napada tehnikama socijalnog inženjeringa. U pripremljenim kampanjama napadači su se osim slanja uobičajenih phishing poruka putem elektroničke pošte koristili i slanjem lažiranih SMS poruka (engl. *smishing*) te upućivanjem telefonskih poziva (engl. *vishing/voice phishing*) u kojima su se predstavljali kao zaposlenici korisničkih službi financijskih institucija.
Sve navedeno ukazuje na dobru pripremljenost i sposobnost hrvatskih banaka za odgovor na kibernetičke prijetnje.

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

NCERT

NATO međunarodna vježba „Cyber Coalition 23"

Članice OTKKS-a sudjelovale su u NATO međunarodnoj vježbi „Cyber Coalition 2023". 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" najveća je NATO vježba u području kibernetičke obrane. Organizirana je od strane Savezničkog zapovjedništva za transformacije (ACT), a održavala se od 27. studenog do 01. prosinca na više desetaka lokacija u zemljama sudionicama. U 16. izdanju vježba je okupila više od 1300 sudionika iz 35 zemalja članica NATO-a i partnerskih zemalja, akademske zajednice i industrije. Sudionici su uključivali najnovijeg saveznika Finsku, zemlje partnere Švedsku, Gruziju, Irsku, Japan, Južnu Koreju, Švicarsku, Ukrajinu, kao i Europsku uniju.
Scenariji na vježbi simulirali su ugroze iz stvarnog života kao što su napadi na prometnu infrastrukturu i financijski sektor, programe i sredstva NATO-a i Saveznika tijekom vojnih operacija.
CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u tehničkom dijelu, pravnom scenariju i kriznoj komunikaciji 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 2015. godine vježbi su se pridružili i predstavnici iz privatnog sektora i akademske zajednice.

HACKNITE

Organizirano je četvrto izdanje hrvatskog CTF natjecanja za srednjoškolce, provedeno od 13. do 15. listopada 2023. godine. Natjecanju su mogli pristupiti samo prijavljeni timovi (ukupno šest osoba – prijavitelj i pet članova tima) s dobivenim korisničkim podacima za pristup natjecanju. Pravo sudjelovanja imali su svi učenici srednjih škola u Republici Hrvatskoj uz mentorstvo svojih profesora kao prijavitelja tima.
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.
U natjecanju je sudjelovalo 615 učenika u 63 srednjoškolska tima iz 40 srednjih škola.

Europski mjesec kibernetičke sigurnosti

CARNET-ov Nacionalni CERT aktivno je obilježio još jedan Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2023. godine proveden je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti.
Nacionalni CERT je 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

Za temu ECSM 2023. odabrana je tema socijalnog inženjeringa, prijetnje koja podrazumijeva manipulaciju žrtvom kako bi se od nje ostvarila neka korist. U socijalni inženjering spada i phishing, a budući da u statistici naših obrađenih incidenata on čini 49% svih incidenata, vidimo kolika je važnost upoznavanja građana s ovom prijetnjom i načinima zaštite od nje.
Osim suradnje s ENISA-om, u sklopu ECSM-a CARNET je surađivao i na izradi i provedbi GÉANT-ove (Multi-Gigabit European Academic Network) "Become a Cyber Hero" kampajne. U sklopu GÉANT kampanje snimljen je i animirani serijal "Cybercrime for Newbies" u kojem Grany Smith opisuje svoj pokušaj napada izvršen pomoću socijalnog inženjeringa i pretraživanja javno dostupnih podataka.
Za vrijeme ECSM kampanje, objavljeni su brojni savjeti za prepoznavanje i zaštitu od socijanog inženjeringa te su održana predavanja i webinari na teme kiberneitčke sigurnosti.

MORH

CAX MVV „CyberNet 23"
Međunarodna vojna vježba „CyberNet 23" je godišnja kibernetička vježba u organizaciji OS Kraljevine Nizozemske. U vježbi su sudjelovali djelatnici OS RH kao članovi PESCO CRRT tima.

CAX MVV „Cyber Unity 23"
Međunarodna vojna vježba „Cyber Unity 23" je godišnja kibernetička vježba u organizaciji US EUCOM-a, provedena u Kraljevini Luksemburg. U vježbi su sudjelovali i djelatnici OS RH.

CAX MVV „Amber Mist 23"
Međunarodna vojna vježba „Amber Mist 23" je godišnja kibernetička vježba u organizaciji OS Republike Litve. U vježbi su sudjelovali djelatnici OS RH kao članovi PESCO CRRT tima.

NATO MVV „Cyber Coalition 23"
„Cyber Coalition 23" je NATO vođena vježba koja obuhvaća sudjelovanje nacionalnih timova za kibernetičku obranu zemalja članica NATO-a i partnerskih zemalja. U vježbi su sudjelovali kibernetički stručnjaci iz MO i OS RH, TDU, akademske zajednice i privatnog sektora.

5. ZAKLJUČAK

Tijekom 2023. godine nastavljen je kontinuirani angažman tijela uključenih u rad Vijeća na unaprjeđenju sigurnosti hrvatskog kibernetičkog prostora uzimajući u obzir sve globalne izazove koji su imali refleksiju na kibernetički prostor, razvoj disruptivnih tehnologija, kibernetički kriminal koji je sve sofisticiraniji, kao i sve veću digitalizaciju i ovisnost o elektroničkim uslugama te 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.

Radilo se na izradi nove Nacionalne strategije kibernetičke sigurnosti i transpoziciji NIS2 direktive koji bi trebali unaprijediti i ujednačiti postupanje država u području kibernetičke sigurnosti te napraviti značajan iskorak i odgovarajuće se nositi i suprotstavljati rizicima čiji se rast očekuje u sljedećih 3-5 godina, kao i pružiti sigurnost građanima i organizacijama, osigurati njihovo povjerenje te optimalno koristiti financijska sredstva.

Raspoloživi materijali povezani s radom Vijeća dostupni su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na mrežnim stranicama Ureda Vijeća za nacionalnu sigurnost[17].

[17] 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 2023. 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
Hrvoje Bujanović	Antonio Pavlečić, 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	Tomislav Malarić
Zdravko Vukić	Igor Vulje

Administrativnu i tehničku potpora radu Vijeća pruža UVNS, gđa Iva Jeličić, g. Vinko Kuculo i g. Željko Jurić.
Administrativnu i tehničku potporu radu Koordinacije pruža MUP.