REPUBLIKA HRVATSKA

UREDVIJEĆA ZA NACIONALNU SIGURNOST

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2023. GODINI

Zagreb, kolovoz 2024.

SADRŽAJ:

I. UVOD 3
II. ANALIZA PROVEDBE MJERA PO PODRUČJIMA KIBERNETIČKE SIGURNOSTI 6
(A) Javne elektroničke komunikacije 6
(B) Elektronička uprava 9
(C) Elektroničke financijske usluge 10
(D) Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama 12
(E) Kibernetički kriminalitet 14
III. ANALIZA PROVEDBE MJERA PO POVEZNICAMA PODRUČJA KIBERNETIČKE SIGURNOSTI 24
(F) Zaštita podataka 24
(G) Tehnička koordinacija u obradi računalnih sigurnosnih incidenata 26
(H) Međunarodna suradnja 29
(I) Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru 32
IV. ZAKLJUČAK 41

I. UVOD

Izvješće o provedbi Akcijskog plana u 2023. godini temelji se na ciljevima Nacionalne strategije kibernetičke sigurnosti[1] (u daljnjem tekstu: Strategija), čije je ostvarenje razrađeno kroz mjere pripadnog Akcijskog plana[2] („Narodne novine“, broj: 108/2015). Strategijom su definirani ciljevi za pet područja kibernetičke sigurnosti koja predstavljaju segmente društva procijenjene kao sigurnosno najvažnije za Republiku Hrvatsku (RH) u odnosu na stupanj razvoja informacijskog društva u vrijeme donošenja Strategije. Radi osiguranja koordiniranog planiranja svih zajedničkih aktivnosti i resursa u odabranim područjima kibernetičke sigurnosti, Strategija definira dodatne četiri poveznice spomenutih pet područja kibernetičke sigurnosti za koje se, kroz definiranje posebnih ciljeva, opisuju rezultati koje se provedbom strateškog okvira želi posti.

Svi ciljevi definirani Strategijom po područjima i poveznicama područja kibernetičke sigurnosti razrađeni su Akcijskim planom. Pri tome svaka mjera, razrađena Akcijskim planom radi postizanja nekog posebnog cilja u jednom od područja ili poveznici područja, doprinosi postizanju općih ciljeva Strategije za RH u cjelini. Tako je za osam općih ciljeva Strategije razrađeno 35 posebnih ciljeva u okviru pet područja kibernetičke sigurnosti i četiri poveznice područja čija je daljnja razrada rezultirala s ukupno 77 mjera razrađenih Akcijskim planom, 33 mjere u područjima kibernetičke sigurnosti te 44 mjere u poveznicama područja kibernetičke sigurnosti.

Područja kibernetičke sigurnosti:

A. Javne elektroničke komunikacije – 3 mjere

B. Elektronička uprava – 8 mjera

C. Elektroničke financijske usluge – 4 mjere

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama – 13 mjera

E. Kibernetički kriminalitet – 5 mjera

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata – 5 mjera

H. Međunarodna suradnja – 6 mjera

I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru – 27 mjera

[1] https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kiberneticke%20sigurnosti%20(2015.).pdf

[2] https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20(2015.).pdf

Akcijskim planom definirani su nositelji i sunositelji provedbe mjera, a uvođenjem sustava obveznog izvješćivanja o provedbi mjera Akcijskog plana, Strategija je dala alat za sustavan nadzor njezine provedbe. Ovaj kontrolni mehanizam služi procjeni razine provedenosti i svrhovitosti pojedinih mjera, osobito u kontekstu vremena i brzog razvoja informacijskog društva i kibernetičkog prostora.

Za sustavno praćenje i koordiniranje provedbe Strategije zaduženo je bilo Nacionalno vijeće za kibernetičku sigurnost (dalje u tekstu Vijeće[3]). koje je u tu svrhu provodilo horizontalnu koordinaciju prema svim institucijama - nositeljima mjera - kako bi se moglo procijeniti jesu li željeni rezultati pojedinih područja ili mjera ostvareni, ili je potrebno redefinirati pristup pojedinim područjima u skladu s novim potrebama. Donošenjem Zakona o kibernetičkoj sigurnosti[4] Vijeće je prestalo sa radom.

Vijeće je nositelj većine mjera u području *D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama*.

Većina institucija, ključnih nositelja i sunositelja u provedbi mjera, poimence je nabrojana u Akcijskom planu, dok se za manji broj institucija obveza provođenja mjera utvrđuje kroz proces provedbe nekih predradnji (npr. određivanje vlasnika/upravitelja kritične informacijske infrastrukture). Nositelji mjera koji su izravno identificirani Akcijskim planom i čija su izvješća korištena u pripremi ovog objedinjenog nacionalnog izvješća su:

1. Agencija za odgoj i obrazovanje (AZOO)
2. Agencija za strukovno obrazovanje i obrazovanje odraslih (ASOO)
3. Agencija za zaštitu osobnih podataka (AZOP)
4. Hrvatska akademska i istraživačka mreža (CARNET)
5. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)
6. Hrvatska narodna banka (HNB)
7. Ministarstvo gospodarstva i održivog razvoja (MinGOR)
8. Ministarstvo obrane (MORH)
9. Ministarstvo pravosuđa i uprave (MPU)
10. Ministarstvo unutarnjih poslova (MUP)
11. Ministarstvo vanjskih i europskih poslova (MVEP)
12. Ministarstvo znanosti i obrazovanja (MZO)
13. Nacionalni CERT / CARNET (NCERT)
14. Operativno-tehnički centar za nadzor telekomunikacija (OTC)
15. Operativno-tehnička koordinacija za kibernetičku sigurnost (Koordinacija)
16. Pravosudna akademija (PA)
17. Sigurnosno-obavještajna agencija (SOA)
18. Središnji državni ured za razvoj digitalnog društva (SDURDD)
19. Sveučilišni računski centar (SRCE)
20. Ured Vijeća za nacionalnu sigurnost (UVNS)

[3] Odluka o osnivanu Vijeća i Koordinacije objavljena je u Narodnim novinama broj: 61/2016, 28/2018, 110/2018, 79/2019, 136/2020

[4] Zakon o kibernetičkoj sigurnosti je objavljen u Narodnim novinama broj: 14/2024

21. Vojna sigurnosno-obavještajna agencija (VSOA)
22. Zavod za sigurnost informacijskih sustava (ZSIS)

Ovo Izvješće izrađeno je na temelju podataka koje je zaključkom Vijeća prikupio UVNS, kao tijelo čiji je predstavnik predsjedavao Vijećem i koje je osiguravalo administrativno-tehničku podršku radu Vijeća. Izvješća institucija, koja su prema Akcijskom planu odgovorna kao nositelji provedbe predviđenih mjera, prikupljena su na standardiziranim obrascima u razdoblju od siječnja do lipnja 2024. godine.

II. ANALIZA PROVEDBE MJERA PO PODRUČJIMA KIBERNETIČKE SIGURNOSTI

(A) Javne elektroničke komunikacije

S obzirom na značaj javnih elektroničkih komunikacija za sve veći broj korisnika, kojima se nudi sve veći broj raznovrsnih usluga, javne elektroničke komunikacije odabrane su kao jedno od 5 prioritetnih područja kibernetičke sigurnosti za koje je potrebno voditi brigu na strateškoj razini.

Uvažavajući pravne, regulatorne i tehničke odredbe koje se već provode u praksi, u svrhu daljnjeg unaprjeđenja bitnih pretpostavki za postizanje veće razine sigurnosti u ovom području, **Strategija određuje 3 cilja**:

- provođenje nadzora tehničkih i ustrojstvenih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga te usmjeravanje operatora u cilju osiguranja visoke razine sigurnosti i dostupnosti javnih komunikacijskih mreža i usluga;
- uspostavu neposredne tehničke koordinacije regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti;
- poticanje korištenja nacionalnog čvora za međusobnu razmjenu internetskog prometa pružatelja javnih komunikacijskih mreža i/ili usluga za davanje usluga korisnicima u RH.

Akcijskim planom utvrđene su 3 mjere za provedbu opisanih ciljeva: 2 mjere kontinuiranog trajanja, koje se u potpunosti provode, te 1 s rokom provedbe od 12 mjeseci (od donošenja Strategije) koja je u potpunosti provedena.

Nadzor tehničkih i ustrojstvenih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga ***provodi se u potpunosti***.

HAKOM nadzire primjenu mjera sigurnosti elektroničkih komunikacijskih mreža i usluga na način da prikuplja sigurnosne politike, planove tretiranja rizika te planove uklanjanja uočenih nedostataka koje su operatori obvezni dostavljati na godišnjoj razini te analizira nalaze revizije njihovih ISMS[5]-ova.

U 2023. sigurnosne politike i reviziju informacijskih sustava dostavilo je 4 operatora, te je HAKOM proveo 4 inspekcijska nadzora u kojim su kod pojedinih operatora utvrđeni određeni nedostaci zbog kojih je inspektor propisao mjere za uklanjanje istih.

Temeljem zaključka s 29. sjednice Vijeća, od 16. svibnja 2019. HAKOM je i u 2023. godini koordinirao rad radne skupine Vijeća za 5G, u kojoj su sudjelovali MVEP, MMPI, UVNS,

[5] Information Security Management System – skup pravila i procedura za sustavno upravljanje osjetljivim podacima

SOA, OTC, ZSIS, NCERT, CARNET i SDURDD. Unutar radne skupine distribuirane su sve aktualnosti vezane za 5G i izvješća koja je pripremala NIS Grupa [6]za suradnju kao i BEREC[7].

HAKOM je u 2023. nastavio suradnju s operativno-tehničkim tijelom nadležnim za aktivaciju i upravljanje mjerom tajnog nadzora elektroničkih komunikacija, a vezano uz obveze tajnog nadzora elektroničkih mreža i usluga. U travnju 2023. potpisan je sporazum o suradnji OTC-HAKOM.

Nadalje, HAKOM provodi i inspekcijske nadzore vezane uz zaštitu privatnosti u elektroničkim komunikacijama što, između ostalog, obuhvaća nadzor nad operatorima u pogledu primijenjenih mjera zaštite osobnih podataka u elektroničkim komunikacijama, postupanja u slučaju eventualnih povreda osobnih podataka, povrede tajnosti elektroničkih komunikacija, postupanja s prometnim podacima te slanja neželjenih komunikacija.

AZOP kontinuirano, sukladno svojoj nadležnosti i ovlastima u području zaštite osobnih podataka, provodi nadzorna postupanja u odnosu na voditelje obrade koji su operatori javnih komunikacijskih mreža i/ili usluga (po zahtjevima ispitanika/korisnika usluga i po primljenim Izvješćima o povredi osobnih podataka prema članku 33. Opće uredbe o zaštiti podataka[8]).

U 2023. godini nastavlja se **kontinuirana suradnja između relevantnih tijela iz područja kibernetičke sigurnosti**. Komunikacija i suradnja je ostvarivana unutar Vijeća i Koordinacije ali i u izravnoj suradnji tijela. Sastanci su se održavali na mjesečnoj razini, osim u slučaju potrebe za sazivanjem izvanredne sjednice. Nastavljena je suradnja Nacionalnog CERT-a s bankarskim sektorom kroz sudjelovanje na sastancima Odbora za sigurnost HUB-a. Aktivna je suradnja s ostalim dionicima iz područja kibernetičke sigurnosti kroz međuresornu radnu skupinu za upravljanje kibernetičkim krizama.

Kroz suradnju s nacionalnim institucijama, privatnim sektorom i međunarodnim partnerima, te kroz aktivnu razmjenu informacija, SOA je kontinuirano povećavala mjere i standarde kibernetičke sigurnosti koji pomažu većoj sigurnosti kibernetičkog prostora RH s naglaskom na prevenciju i brzi oporavak, kao i odgovor u slučaju ugroze kibernetičkog prostora. Nakon 2020. godine, kada je SOA pokrenula novu aktivnost upravljanja nacionalnim kibernetičkim krizama i ustrojila međuresornu radnu skupinu s drugim tijelima, tijekom 2021. završena je izrada nacionalnog dokumenta sa standardnim operativnim procedurama za upravljanje kibernetičkim krizama. Ovaj proces, kao i rezultirajući prijedlog standardnih operativnih procedura, SOA kontinuirano usklađuje s EU-CyCLONe[9] organizacijom, u kojoj SOA predstavlja RH. U prosincu 2022. godine započete su i u RH intenzivne pripreme za nacionalnu

[6] NIS Grupa za suradnju (NIS Cooperation Group) je uspostavljena NIS direktivom i sastoji se od predstavnika država članica EU, Europske komisije i ENISA-e

[7] BEREC - The Body of European Regulators for Electronic Communications

[8] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

[9] EU-CyCLONe je uspostavljen kako bi podržao koordinirano upravljanje kibernetičkim sigurnosnim incidentima i krizama velikih razmjera na operativnoj razini i osigurao redovitu razmjenu relevantnih informacija među državama članicama i institucijama, tijelima, uredima i agencijama Unije.

transpoziciju EU NIS2[10] direktive i uvođenje novog modela upravljanja kibernetičkom sigurnošću u RH, čime će se poboljšati nacionalni okvir za upravljanje kibernetičkim krizama u cilju provedbe puno zahtjevnijih odredbi NIS2 direktive. Konačni tekst EU NIS2 direktive objavljen je u prosincu 2022. godine, a stupio je na snagu u siječnju 2023. godine, s rokom transpozicije za države članice od 21 mjesec (do 17.10.2024.). Odredbe navedene direktive uvode EU CyCLONe mrežu kao ključnog operativnog čimbenika na razini EU te pri tome obvezuju države članice na zakonsko propisivanje sukladnih organizacijskih modela upravljanja kibernetičkim krizama, uključujući obvezu donošenja nacionalnog plana upravljanja kibernetičkim krizama.

VSOA u okviru predmetne mjere kroz raspoložive komunikacijske kanale razmjenjuje podatke iz područja tehničke koordinacije i to prvenstveno između tijela koja su zadužena za područja sigurnosti informacijskih sustava u RH. Na mjesečnim sastancima u sklopu Koordinacije razmjenjuju se podaci o trendovima i pojavnostima kibernetičkih ugroza. VSOA kontinuirano razmjenjuje zaprimljene podatke o kibernetičkim ugrozama od strane partnera sa svim relevantnim tijelima. Isto tako VSOA je uključena u rad međuresorne radne skupine za upravljanje kibernetičkim krizama u RH. Nadalje, unutar MORH-a razmjenjuju se podaci vezani uz područja kibernetičke i informacijske sigurnosti i politike zaštite podataka koji se zaprimaju iz NATO i EU asocijacija, odnosno njihovih članica.

OTC, koji je temeljem Zakona o elektroničkim komunikacijama nadležan za propisivanje i nadzor mjera i standarda informacijske sigurnosti kod operatora elektroničkih komunikacija po pitanju funkcije tajnog nadzora, provodi kontinuiranu koordinaciju s regulatornim tijelom za područje tržišta elektroničkih komunikacija i središnjim državnim tijelom za informacijsku sigurnost, kako bi osigurao usklađivanje propisanih i implementiranih mjera i standarda informacijske sigurnosti kod operatora s novonastalim regulatornim zahtjevima, s ciljem zadržavanja postignute razine informacijske sigurnosti ili mogućeg unaprjeđenja iste.

Pokazatelji provedbe mjere utvrđene u svrhu poticanja ***korištenja nacionalnog čvora za međusobnu razmjenu internetskog prometa*** (CIX, Croatian Internet eXchange) ***ostvareni su u potpunosti*** – preporuke su donesene u roku utvrđenim Akcijskim planom - izrađene su i javno objavljene preporuke (https://www.cix.hr/files/cix/docs/nsks_cix_preporuka_v1.0_20160921.pdf, rujan 2016.), napravljena je promocija preporuka na Savjetovanju o sigurnosti informacijskih sustava u organizaciji ZSIS-a (prosinac 2016.) i promocija preporuka na konferenciji KOM 2016 (studeni 2016.).

[10] 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

(B) Elektronička uprava

RH razvija i unaprjeđuje elektroničku komunikaciju s građanima već duži niz godina. Daljnji razvoj elektroničke uprave kojim se osigurava brza, transparentna i sigurna usluga svim građanima putem kibernetičkog prostora strateški je cilj RH.

Da bi se navedeno postiglo, uspostavlja se sustav javnih registara kojim se upravlja kroz jasno definirana prava, obveze i odgovornosti nadležnih tijela javnog sektora. **Strategija definira 3 cilja** usmjerena na stvaranje pretpostavki za postizanje više razine sigurnosti sustava elektroničke uprave, kroz:

- poticanje na povezivanje informacijskih sustava tijela javnog sektora međusobno i na Internet kroz državnu informacijsku infrastrukturu;
- podizanje razine sigurnosti informacijskih sustava javnog sektora;
- donošenje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica.

Za ostvarenje ovih ciljeva, Akcijskim planom razrađeno je ukupno 8 mjera, u određenom dijelu međusobno slijednih i ovisnih, s opisanim konkretnim pokazateljima provedbe te jasno određenim rokovima.

Od osam utvrđenih mjera u potpunosti su provedene četiri, djelomično dvije, a dvije su zastale u provedbi jer potrebne pretpostavke još nisu u cijelosti ispunjene.

Uspostavljena je Radna skupina za analizu, standardizaciju i sigurnost mreža, izrađena **analiza potreba i mogućnosti povezivanja na državnu informacijsku infrastrukturu,** a daljnja razrada mjere je predviđena kroz projekt predviđen za financiranje kroz NPOO, s provedbom do 2026.

Analiza mogućnosti povezivanja državnih tijela klasificiranom mrežom je izrađena kao i Plan povezivanja koji se provodi u fazama, te se može konstatirati kako je ova mjera provedena.

Izrada **analize postojećeg stanja** u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora provodi se u manjoj mjeri zbog neodgovarajućih nadležnosti SDURDD-a.

Izrada **smjernica za primjenu sustava NIAS** i odgovarajućih normi (ISO 27001 i sl.) je zastala jer se čekaju najavljena zakonska i podzakonska rješenja koja trebaju urediti zakonodavni okvir sustava NIAS (Izmjene Zakona o državnoj informacijskoj infrastrukturi[11] i podzakonskih akata).

Mjera **definiranja organizacijskih i tehničkih zahtjeva za povezivanje na državnu informacijsku infrastrukturu** je provedena te je donesena Uredba o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu[12]

Napravljena je **periodična procjena organizacijskih i tehničkih zahtjeva** za povezivanje na državnu informacijsku infrastrukturu, uvjeta i aktivnosti nužnih za pokretanje, implementaciju,

[11] NN 92/14
[12] NN 60/17

razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostale elemente neophodne za rad državne informacijske infrastrukture. Procjena je rezultirala smjernicama u postupku izrade prijedloga izmjena/novog Zakona o državnoj informacijskoj infrastrukturi, u sklopu kojeg će se redefinirati organizacijski i tehnički zahtjevi za povezivanje na državnu informacijsku infrastrukturu, uvjeti i aktivnosti nužni za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostali elementi neophodni za rad državne informacijske infrastrukture.

Analiza u svrhu donošenja kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica kojom će se obuhvatiti i procjena mogućnosti korištenja buduće elektroničke osobne iskaznice građana za potrebe elektroničke uprave i drugih javnih i financijskih usluga, a i drugi aspekti povezani s nacionalnim mogućnostima za uspostavu odgovarajućih akreditacijskih i certifikacijskih sposobnosti u području kvalificiranih elektroničkih potpisa, sukladno EU zahtjevima – provodi se u manjoj mjeri zbog izostanka podrške svih dionika.

Provođenje slijedne mjere **utvrđivanja kriterija za korištenje pojedinih razina autentifikacije** kod davatelja usluga elektroničke uprave i davatelja vjerodajnica je zbog prethodno navedenoga odgođeno.

(C) Elektroničke financijske usluge

Sigurnosni zahtjevi koji se provode u području elektroničkih financijskih usluga osiguravaju visoku razinu sigurnosti za cjelokupno građanstvo te poslovni i državni sektor.

Poticanje razvoja elektroničkih financijskih usluga i neprekidna briga o zaštiti njihovih korisnika cilj je svake suvremene države. Stoga je i RH utvrdila okvir daljnjeg djelovanja u ovom području kroz definiranje sljedeća **2 strateška cilja**:

- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, a s ciljem poticanja razvoja elektroničkih financijskih usluga;
- unaprjeđenje razmjene i ustupanja podataka o nastalim računalnim sigurnosnim incidentima između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela.

Oba strateška cilja su ostvarena. Akcijskim planom utvrđene su 4 mjere u ovom području, s opisanim konkretnim pokazateljima provedbe te rokovima.

U lipnju 2015. u HNB-u su održane cjelodnevne prezentacije Smjernica o sigurnosti internetskih plaćanja koje je EBA[13] objavila u ožujku 2015. Na radionicama su sudjelovali predstavnici svih banaka koje posluju u RH, kao i predstavnici najznačajnijih institucija za elektronički novac.

[13] Europsko nadzorno tijelo za bankarstvo

U svibnju 2015. svim bankama upućen je dopis odnosno okružnica u svezi primjene Smjernica o sigurnosti internetskih plaćanja koje su objavljene i na internetskim stranicama HNB-a čija primjena je započela s 1. kolovozom 2015. a koje je izdala EBA.

U 2016. vanjski revizori svih kreditnih institucija ocijenili su usklađenost sa svim (pojedinačnim) odredbama Smjernica o sigurnosti internetskih plaćanja te svoju procjenu dostavili HNB-u.

U 2018. Smjernice o sigurnosti internetskih plaćanja zamijenile su Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju PSD2[14].

EBA nije i neće objaviti Smjernice o sigurnosti mobilnih plaćanja, obzirom da su mobilna plaćanja (odnosno plaćanja koja se zadaju putem mobilnih telefonskih uređaja) obuhvaćena PSD2 i proizlazećim regulatornim tehničkim standardima i smjernicama. Odnosno, sadržajno, preporuke o sigurnosti mobilnih plaćanja uključene su u sljedeće dokumente:

a) DELEGIRANA UREDBA KOMISIJE (EU) o dopuni Direktive 2015/2366 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda za pouzdanu autentifikaciju klijenta i zajedničke i sigurne otvorene standarde komunikacije
b) Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju PSD2

Cilj procjene zakonskih mogućnosti i ograničenja vezanih uz razmjenu informacija o incidentima vezanima uz informacijske sustave kreditnih institucija s relevantnim institucijama u RH bio je osigurati uvjete za provedbu učinkovite razmjene i ustupanja podataka čime bi se unaprijedilo rješavanje nastalih sigurnosnih incidenata te ujedno osiguralo sprječavanje nastanka ili ograničavanje učinka takvih incidenata u budućnosti.

Inicijalno provedena procjena mogućnosti razmjene informacija o incidentima pokazala je da HNB podatke o incidentima vezanima uz informacijske sustave kreditnih institucija može dostavljati relevantnim institucijama u RH isključivo u anonimiziranom obliku iz kojeg nije moguće utvrditi:

- osobne ili poslovne podatke o klijentu,
- podatke koji predstavljaju poslovnu tajnu,
- kojoj kreditnoj instituciji je riječ.

Neka relevantna tijela u RH s kojima bi se, ovisno o karakteristikama incidenta (ili incidenata) i procjeni HNB-a mogli dostavljati podaci su: HANFA, HAKOM, NCERT, ZSIS, MUP, SOA. Dodatno, ovisno o karakteristikama incidenta, HNB prilikom procjene potrebe i optimalnog načina dijeljenja podataka može identificirati i druga relevantna tijela.

Podatke bi s relevantnim tijelima trebalo dijeliti koristeći sigurne načine (tj. protokole) razmjene koji su jednostavni za korištenje.

[14] DIREKTIVA (EU) 2015/2366 EUROPSKOG PARLAMENTA I VIJEĆA od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ

NCERT je objavio Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom određuju način dostave obavijesti i sadrže obrasce za obvezno obavještavanje o incidentima sa znatnim učinkom.

Smjernice dodatno uređuju zakonske mogućnosti, ograničenja te mehanizme razmjene informacija o incidentima vezanima uz informacijske sustave kreditnih institucija (koje su ujedno i operatori ključnih usluga) s relevantnim institucijama u RH.

(D) Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

Sigurnost kritične komunikacijske i informacijske infrastrukture predstavlja jedno od pet prioritetnih područja Strategije. U njemu se preklapaju i nadopunjuju zahtjevi različitih nacionalnih, EU i NATO propisa. Novi Zakon o kibernetičkoj sigurnosti[15] uređuje odnose i obveze državnih tijela i pravnih osoba u uspostavljanju otpornosti informacijskih sustava. U tijeku je proces transpozicije CER direktive[16] te će se na usklađen način rješavati pitanje sigurnosti kritične infrastrukture i kritičnih sektora.

U cilju podizanja veće sigurnosti komunikacijskih i informacijskih sustava koji su ključni za funkcioniranje države i gospodarstva, **Strategijom je definirano pet ciljeva**:

- utvrditi kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture;
- utvrditi obvezujuće sigurnosne mjere koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture;
- ojačati prevenciju i zaštitu kroz upravljanje rizikom;
- ojačati javno-privatno partnerstvo i tehničku koordinaciju u obradi računalnih sigurnosnih incidenata;
- uspostaviti kapacitete za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu.

Uvažavajući model korišten u Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga Ravnateljstvo civilne zaštite MUP-a kao središnjeg tijela državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja, koordiniralo je postupak identifikacije nacionalnih kritičnih infrastruktura (KI). Navedeno se provodilo kroz primjenu kriterija za identifikaciju KI u dijelovima na koje se oni odnose te je u suradnji s nadležnim tijelima državne uprave izrađen prvi prijedlog Popisa nacionalne KI, koji je u procesu potvrđivanja posebnom odlukom čije je donošenje u nadležnosti Vlade RH.

[15] NN 14/2024
[16] Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekta i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ

Postojeći Zakon o KI stupio je na snagu 1.1.2023. u kojem je komunikacijska i informacijska tehnologija definirana kao horizontalna komponenta nacionalne KI.

Međutim, trenutno je u fokusu implementacija u nacionalna zakonodavstva nove CER direktive. Direktiva donesena u prosincu 2022. godine usmjerena je na jačanje otpornosti ključnih kritičnih subjekata i ključnih usluga u odnosu na rizike povezane s ozbiljnim incidentima. Direktiva potiče suradnju između država članica EU-a kako bi se osigurao koordinirani pristup identifikaciji, procjeni rizika i upravljanju krizama koji bi mogli utjecati na kritične sektore.

Kako bi se mogla provesti analiza kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza prethodno je potrebno napraviti procjenu stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora.

U cilju procjene stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora, Koordinacija je izradila Metodologiju za procjenu stanja kibernetičke sigurnosti u nacionalnom kibernetičkom prostoru RH.

Ravnateljstvo policije izradilo je 2022. godine Nacrt standardnih operativnih procedura o postupanju policije u slučaju kibernetičkih napada velikih razmjera. Navedene procedure biti će usvojene nakon što se usvoje Nacionalne standardne procedure o upravljanju kibernetičkim krizama u RH.

U Zakonu o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga, te Uredbi definiran je incident koji ima znatan učinak na kontinuitet usluge (nije definirana kibernetička kriza). U Nacionalnoj taksonomiji računalno-sigurnosnih incidenata definiran je općeniti pojam kibernetička kriza, ali nije definirano točno kako se utvrđuje, kada ona nastaje i koji su kriteriji.

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

SOA je također razradila nacionalni koncept upravljanja kibernetičkim krizama te ga uskladila s aktualnim pristupom EU-a i NATO-a, a na temelju suglasnosti NVKS-a, SOA se kao nadležno tijelo RH u proljeće 2020. uključila u EU CyCLONe organizaciju za upravljanje kibernetičkim krizama. U svrhu usuglašavanja i razrade predloženog nacionalnog koncepta upravljanja kibernetičkim krizama, SOA je u listopadu 2020. formirala međuresornu stručnu radnu skupinu u koju su pozvani predstavnici ključnih tijela za predmetno područje (MORH, MUP, ZSIS, NCERT, HAKOM i HNB).

(E) Kibernetički kriminalitet

U cilju uspostave učinkovitih mjera za kvalitetnije i uspješnije suzbijanje kibernetičkog kriminaliteta **Strategijom je utvrđeno 5 ciljeva** usmjerenih na:

- unaprjeđivanje nacionalnog zakonodavnog okvira u domeni kaznenog prava, vodeći računa o međunarodnim obvezama;
- uspostavljanje kvalitetne suradnje nadležnih tijela u svrhu učinkovite razmjene informacija, kako na međunarodnoj, tako i na nacionalnoj razini;
- uspostavljanje kvalitetne međuinstitucionalne suradnje u svrhu učinkovite razmjene informacija na nacionalnoj razini, a posebno u slučaju računalnog sigurnosnog incidenta;
- jačanje ljudskih potencijala i razvoj tehničkih mogućnosti državnih tijela nadležnih za otkrivanje, kriminalističko istraživanje i procesiranje kaznenih djela iz domene računalnog kriminaliteta; te
- razvoj suradnje s gospodarskim sektorom.

Za ostvarenje tih ciljeva, Akcijskim planom predviđeno je ukupno 5 mjera, koje je, s obzirom na njihov karakter, ***potrebno kontinuirano provoditi***.

Dostavljena izvješća o provedbi mjera pokazuju da su se ***sve mjere u 2023. godini provodile u potpunosti ili većoj mjeri, kako je i utvrđeno Akcijskim planom***.

MPU, MUP i DORH imaju svoje predstavnike u svim relevantnim međunarodnim tijelima te redovno sudjeluju u radu istih i prate međunarodne aktivnosti i razvoj međunarodnih instrumenata.

Predstavnici RH su u 2023. godini redovno sudjelovali u radu Odbora Vijeća Europe za praćenje primjene Konvencije o kibernetičkom kriminalitetu (T-CY Odbor). Datumi plenarnih sastanaka su bili slijedeći:

- redovni plenarni sastanak T-CY, dana 27.-28. lipnja 2023.
- redovni plenarni sastanak T-CY, dana 11.-12. prosinca 2023.

Vijeće EU je u veljači 2023. donijelo odluku o ovlašćivanju država članica da u interesu EU-a ratificiraju Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu te se u RH trenutno poduzimaju mjere u svrhu ratifikacije.

U 2023. godini usvojene su Uredba o europskom nalogu za dostavljanje i europskom nalogu za čuvanje e-dokaza, s prilozima, te Direktiva o imenovanju pravnih zastupnika za prikupljanje dokaza. Nastavno na navedeno, nastavljaju se intenzivni pregovori sa Sjedinjenim Američkim Državama o olakšavanju prekograničnog pristupa e-dokazima za potrebe pravosudne suradnje u kaznenim stvarima, a koji su započeli u rujnu 2019.

MPU se, radi uspostavljanja nacionalnog konektora koji je neophodan za elektroničko povezivanje s pravosudnim tijelima drugih država članica EU preko zajedničke platforme u

svrhu razmjene e-dokaza, uključio u projekt EXEC II (trajanje: 24 mjeseca počev od 01.10.2020.) kojim se nastavilo s radom i aktivnostima potrebnim za uspješnu integraciju nacionalnih sustava e-Spis i CTS s e-EDES-om (e-Evidence Digital Exchange System). Taj projekt je završen krajem 2022. godine. Vezano uz gore navedenu prekograničnu razmjenu e-dokaza, u cilju lakšeg identificiranja nadležnog tijela u drugim državama članicama, Europska komisija će uspostaviti bazu podataka o nadležnim tijelima (sudovima i državnim odvjetništvima) u kaznenim stvarima. Slijedom toga, MPU se uključilo u EU projekt „Criminal Court Database“ (CCDB) u cilju financiranja uspostave nacionalne baze kaznenih pravosudnih tijela te njezinog povezivanja s EU platformom. Projekt CCDB je započeo s realizacijom 1. veljače 2021. godine i završen je 31. siječnja 2023. godine. Ažuriranje baze kaznenih sudova zahtijevat će dodatan i stalni angažman, te je stoga zamišljeno da u sklopu ovog novog projekta projektni partneri analiziraju i odrede strukturu podataka koja će se prikazivati na zajedničkom referencijalnom portalu, a sve radi bržeg i točnijeg identificiranja nadležnih tijela za postupanje po europskom istražnom nalogu, a u kasnijoj fazi i za postupanje temeljem drugih EU instrumenata u području kaznenog zakonodavstva.

U cilju usklađenja nacionalnog zakonodavstva s EU izvorima prava, MPU donijelo je Zakon o provedbi Uredbe 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu. Predmetni Zakon stupio je na snagu 7. lipnja 2022. godine te se njime osigurava potpuna i pravovremena provedba Uredbe (EU) 2021/784 kojom se uvodi izravna obveza u pogledu radnji koje pružatelji usluga smještaja na poslužitelju i nadležna tijela država članica EU poduzimaju radi borbe protiv širenja terorističkog sadržaja na internetu.

MUP na međunarodnoj razini koristi tri kontakt točke za razmjenu informacija o kaznenim djelima kibernetičkog kriminaliteta.

- Kontakt točke uspostavljene odredbom čl. 13. Direktive 2013/40/EU o napadima na informacijske sustave. Uredbom Vlade RH o preuzimanju Direktive 2013/40/EU o napadima na informacijske sustave te direktive 2014/62/EU o kaznenopravnoj zaštiti eura i drugih valuta od krivotvorenja određena je ustrojstvena jedinica MUP-a za suzbijanje kibernetičkog kriminaliteta kao operativna nacionalna kontakt točka za razmjenu informacija o kaznenim djelima protiv računalnih sustava, programa i podataka. Imenik kontakt točki vodi Europska komisija, kojoj su dostavljeni slijedeći podaci o hrvatskoj kontakt točki: Služba kibernetičke sigurnosti, Kriminalističko-obavještajni sektor, Uprava kriminalističke policije.
- Kontakt točka G 7, koju je uspostavila je organizacija sedam najrazvijenijih zemalja svijeta. Kontakt točkom administrira Ministarstvo pravosuđa SAD-a. Hrvatska kontakt točka je Služba kibernetičke sigurnosti.
- Kontakt točke Interpola za razmjenu informacija o kibernetičkom kriminalitetu Hrvatska kontakt točka je Služba kibernetičke sigurnosti. Hrvatska kontakt točka dostupna je putem adrese elektroničke pošte cyber.crime@mup.hr te je u posjedu kontakt podataka o svim ostalim kontakt točkama u svijetu. Kontakt točke služe za

zadržavanje podataka i elektroničkih dokaza za čije je pribavljanje potrebna međunarodna pravna pomoć ili za izravno pribavljanje obavijesti za koje nije potreban zahtjev pravosudnog tijela.

MUP redovno šalje zahtjeve prema drugim državama te prima zahtjeve drugih država, te nema poteškoća u provedbi.

Preko CSIRTs Netvvork zajednice Nacionalni CERT surađuje se s LEA (law enforcement agencies) diljem EU, sudjelujemo na sastancima za jačanje suradnje CERT timova i policije. U sklopu navedene suradnje, NCERT je aktivno uključen u „digital skimming" radnu skupinu kod koje prati informacije o incidentima ove kategorije u svojoj nadležnosti te vrši analizu malicioznog koda po potrebi.

SOA uspostavljenu međunarodnu suradnju kontinuirano razvija u području kibernetičke sigurnosti te aktivno razmjenjuje informacije s partnerskim agencijama u cilju prevencije, brzog oporavka i odgovora u slučajevima ugroze kibernetičkog prostora RH. U ovom procesu SOA se prvenstveno usmjerava na svoje uže područje nadležnosti, odnosno na državno-sponzorirane kibernetičke napade i APT (Advanced Persistent Threat – napredna ustrajna prijetnja) kampanje. Međunarodna razmjena u području kibernetičke sigurnosti posebno se razvija u segmentima razmjene indikatora kompromitacije (Indicators of Compromise – IoC) i taktika, tehnika i procedura kibernetičkih napadača (Tactics, Technics and Procedures – TTP).

MVEP je tijekom 2023. godine kontinuirano i pravovremeno izvještavalo Vijeće, a po potrebi i MUP, o međunarodnim aktivnostima vezanim za kibernetičku sigurnost i kibernetički kriminal. Također je i koordiniralo aktivnosti i sudjelovanje na sastancima u okviru međunarodne Inicijative protiv kibernetičkog iznuđivanja.

European Judicial Cybercrime Network (EJCN) (Europska mreža za borbu protiv kibernetičkog/računalnog kriminaliteta ustanovljena je krajem 2016. kad su se u organizaciji EUROJUST-u okupili pravni stručnjaci (državni odvjetnici i manjim dijelom suci) poslani od strane njihovi matičnih tijela, bilo da se radi o praktičarima koji su radili na kaznenim predmetima iz područja suzbijanja kibernetičkog kriminaliteta ili su zainteresirani za to područje. RH sudjeluje u radu EJCN-a od njezina osnivanja te ima svoju kontakt točku, a to je zamjenik ravnatelja USKOK-a. Kako je kibernetički kriminalitet u pravilu često povezan s potrebom korištenja međunarodne pravne pomoći cilj uspostavljanja EJCN-a je bio uspostaviti mrežu osoba u svakoj od država članica Europske unije koji će služiti kao kontakt točke radi ubrzavanja i olakšavanja razmjene informacija. Od osnivanja EJCN-a mreža se proširila tako da danas u mreži postoje kontakt točke iz Sjedinjenih Američkih Država, Švicarske konfederacije, Kraljevine Norveške, Republike Srbije, Japana, a nakon Odlaska Ujedinjenog Kraljevstva iz EU isto trenutno nema svoju kontakt točku. 2 Mreža funkcionira u vidu o neformalne razmjene informacija između kolega o nekim konkretnim problemima ili novim pojavnostima u području kibernetičkog kriminaliteta. Cilj razmjene tih informacija je upoznati kolege iz drugih država s novim pojavnostima kako bi mogli djelovati preventivno (koliko je to moguće), a prvenstveno olakšati kolegama (ne samo kontakt

točkama već i njihovim kolegama u njihovim državama koji rade na konkretnim predmetima) postupanje u konkretnim predmetima, na koji se način da im se savjetuje od kojeg tijela ili pravne osobe se može dobiti određeni podatak radi eventualnog daljnjeg korištenja istog kao dokaza u kaznenom postupku ili razmjene iskustava iz prakse. Mreža svake godine organizira dva plenarna sastanka koji se održavaju u prostorijama EUROJUST-a, a kojim predsjeda rotirajuće predsjedništvo po uzoru na predsjedništvo Vijeća Europe u to vrijeme. Osim kontakt točaka na te se sastanke (njihov otvoreni dio) redovito pozivaju i predstavnici drugih tijela posebice EUROJUST-a, Europske komisije i njezinih odbora, Europola, kao i predstavnici trgovačkih društava koja imaju poveznicu s kibernetičkim kriminalitetom, primjerice kriptomjenjačnice, predstavnici velikih internetskih servisa i sl. Na tim se sastancima razmatraju nove pojavnosti u sferi kibernetičkog kriminaliteta kao i problemi koji se pojavljuju u praksi, a vezani su za otkrivanje i progon počinitelja kaznenih djela kibernetičkog kriminaliteta. Tijekom 2023. zamjenik ravnatelja USKOK-a sudjelovao je na oba plenarna sastanka kao kontakt točka RH, a osim toga tijekom prošle godine unutar mreže zaprimljeni su desetci upita od drugih članova EJCN-a u svezi konkretne problematike iz područja kibernetičkog kriminaliteta. Ti se upiti u većinom slučajeva upućuju na sve kontakt točke bilo da se radi o upitima o susretu s nekim novim oblikom računalnog kriminaliteta, novom kriptovalutom i problemom pribavljanja podatka od kriptomjenjačnica ili pružatelja usluga iz određene države. U radu EJCN-a uvijek su aktualne teme razmjena informacija i pribavljanje dokaza sukladno Budimpeštanskoj konvenciji, tema elektroničkih dokaza, tema kripto valuta te tema zadržavanja podataka. Radi toga unutar mreže su osnovane i podgrupe koje se bave radom na konkretnim temama (Data Retention, Electronic Evidence, Virtual Currencies, Case Building i Training), a zamjenik ravnatelja USKOK-a osobno sudjeluje u grupi koja se bavi problematikom *data retention* (zadržavanja podataka) i pitanja njihove zakonitosti u kontekstu odluka europskih sudova koje su ukinule europsku legislativu u tom području. Kako je u tijeku izrada nove legislative Europske unije kojom bi se reguliralo pitanje zadržavanja podataka EJCN je od strane tijela Europske unije prepoznat kao tijelo koje, s obzirom na poznavanje problematike iz prakse, može aktivno doprinijeti kvalitetnijem radu odnosno izradi kvalitetnije legislative. EJCN sa svojim znanjima i informacijama koje su prikupljene također sudjeluje u izradi izvješća EUROJUST-a u svezi kibernetičkog kriminaliteta (Cybercrime Judicial 3 Monitor). U tu svrhu se od članova redovito traže izvješća kao i statistički podaci o kibernetičkom kriminalitetu, zakonodavnom okviru, novim zakonodavnim rješenjima/propisima iz njihovih matičnih država. U konačnici EJCN služi i kao platforma putem koje se dobivaju informacije o organiziranju raznih stručnih skupova, seminara, webinara na temu borbe protiv kibernetičkog kriminaliteta u kojima mogu sudjelovati kako EJCN kontakt točke, no isto tako te informacije kontakt točke mogu proslijediti kolegama u svojim matičnim državama. Što se tiče međunarodne pravne pomoći stalna "kontakt točka" u Odsjeku za međunarodnu pravnu pomoć i suradnju Ureda Glavnog državnog odvjetnika RH je zamjenica općinskog državnog odvjetnika koja u predmetima kibernetičkog kriminaliteta kao nacionalni predstavnik RH u Europskoj pravosudnoj mreži, usmjerava i žurno prosljeđuje zamolbe za međunarodnu pravnu pomoć i suradnju prema zemljama članicama Europske unije i drugim zemljama.

U 2023. kontaktne točke Europske pravosudne mreže u kaznenim stvarima u RH prijavile su 213 aktivnosti. Samo 6 slučajeva od ukupno prijavljenih aktivnosti odnosilo se na slučajeve kibernetičkog kriminala. Treba naglasiti da se 21 slučaj odnosio na prijevaru (prijevara uključuje i računalne prijevare) tako da je obujam slučajeva pravosudne suradnje/MLA kibernetičkog kriminala veći nego što je izraženo u statističkim podacima. Europska pravosudna mreža koristi se u svrhu pripreme zahtjeva za međunarodnu pravnu pomoć/instrumenata pravosudne suradnje, požurivanja njihovog izvršenja kao i dobivanja informacija o nadležnom pravosudnom tijelu i mjerodavnom pravu u državi izvršiteljici. Napominjemo da se većina slučajeva međunarodne pravne pomoći Državnog odvjetništva odnosi na pravosudnu suradnju sa SAD-om zbog činjenice da Facebook (Meta) i Google imaju sjedišta u SAD-u. Pravosudna suradnja temelji se na Europskoj konvenciji o kibernetičkom kriminalu potpisanoj 2001. Mora se naglasiti da učinkovitost ove suradnje ovisi o učinkovitoj policijskoj suradnji (kontaktne točke 24/7) i pravovremenom čuvanju podataka, kao i o visokim dokaznim standardima zakona i prakse SAD-a (osobito kada se zahtjevi za međunarodnu pravnu pomoć odnose na podatke o transakciji i sadržaju) koji često otežavaju dobivanje traženih dokaza.

U tablici su prikazane aktivnosti EJCN kontaktne točke RH u 2023.:

Total reported activities	213
Extracts from criminal records	
Directive 2014/41/EU on the European investigation Order in criminal matters	3
Other	1
Total	4
e-Evidence	
Convention on Cybercrime (Budapest, 2001)	2
Total	2
Hearings standard procedure	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	8
Directive 2014/41/EU on the European Investigation Order in criminal matters	12
European Convention on Mutual Assistance in Criminal Matters 1 (Strasbourg, 1959)	1
Bilateral agreement	2
Other	1
Total	24
Hearings by videoconference	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	3
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Total	4
Hearings by videoconference	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	3
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Total	4
Summoning and Service of documents	

Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	3
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Total	4
Other MLA / EIO measures	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	6
Directive 2014/41/EU on the European Investigation Order in criminal matters	10
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	3
Bilateral agreement	2
Total	21
Freezing/sequestration of assets	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	2
Framework Decision 2003/577/JHA on Freezing Orders	3
Regulation 2018/1805 on Freezing and Confiscation	1
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Total	7
Confiscation	
Framework Decision 2006/783/JHA on mutual recognition of Confiscation Orders	1
Regulation 2018/1805 on Freezing and Confiscation	1
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Total	3
European Arrest Warrant / Extradition	
Framework Decision 2002/584/JHA on European arrest warrant and the surrender procedures between Member States	53
European Convention on Extradition (Paris, 1957)	5
Total	58
Enforcement of a Financial Penalty	
Framework Decision 2005/214/JHA on mutual recognition of Financial Penalties	15
Total	15
Enforcement of a Custodial Sentence / Transfer of sentenced persons	
Framework Decision 2008/909/JHA on the mutual recognition of Custodial Sentences	5
Total	5
Probation measures	
Framework Decision 2008/947/JHA on mutual recognition of Probation decisions	5
Total	5
Transfer of proceedings	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	1
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	5
Bilateral agreement	1
Total	7
Measure not known	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	1
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	1
Other	2
Total	4

Other	
Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union	7
Directive 2014/41/EU on the European Investigation Order in criminal matters	3
European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959)	4
Bilateral agreement	2
Other	9
Total	25
Incoming and outgoing activities	
Incoming	88
Outgoing	125
Type of assistance given	
Facilitating establishing direct contacts between the issuing (requesting) and the executing (requested) judicial authorities, including providing information on competent authorities	47
Providing legal and practical information to enable the judicial authorities to prepare an effective request for judicial cooperation	44
Providing legal and practical information or other type of support to facilitate/speeding-up the execution of request for judicial cooperation	52
Provide assistance in case of delay of execution of requests	7
Provide information on law	25
Provide information about the status of criminal cases	45
Other	17
Countries reported *	
Austria	13
Belgium	5
Bulgaria	2
Croatia	1
Cyprus	2
Czech Republic	5
Denmark	4
Estonia	1
Finland	2
France	4
Germany	39
Hungary	4
Ireland	2
Italy	23
Malta	1
Netherlands	15
Romania	1
Slovenia	29
Spain	13
Sweden	6
Albania	1
North Macedonia	2
Serbia	3
Ukraine	2
Norway	1

Switzerland	5
Bosnia and Herzegovina	3
Canada	1
Kosovo	1
Panama	1
Russia	1
Uganda	1
United Kingdom	3
United States of America	2
Other third countries incoming	16
Other third countries outgoing	11
Category of crime involved	
Corruption	9
Crimes against children	4
Cybercrime	6
Drug trafficking	23
Environmental crimes	1
Financial crimes	5
Forgery	11
Fraud, including that affecting the financial interests of the EU	21
Illegal migrant smuggling	10
Money laundering	12
Motor vehicle crime	10
Murder, bodily injury and other crimes against the person	10
Organized crime	6
Property crimes, including theft	18
Tax crime, including VAT fraud	7
Terrorism	1
Trafficking in human beings	1
Not known	25
Category of crime involved	
Other	44
Organizations, partner networks and other actors involved	
Liaison magistrate	11
Europol	1
Interpol	4
Other	23
Cooperation with Eurojust	
Request received at Eurojust, redirected to an EJN Contact Point	28
Request received by an EJN Contact Point, redirected to Eurojust	4
Not applicable or not known	111
Channel of contact	
E-mail	188
Face to face/participation in meeting/hearings	5
Fax	1
Regular mail	13
Other	1
Activities reported per month *	
January	29

February	14
March	12
April	12
May	23
June	13
July	10
August	11
September	17
October	13
November	11
December	48

U MUP-u kontakt točka za razmjenu informacija i koordinaciju postupanja s drugim nacionalnim tijelima je Služba kibernetičke sigurnosti. Tijekom 2023. godine ostvarena je suradnja na konkretnim slučajevima istraživanja kibernetičkog kriminaliteta sa SOA-om, ZSIS-om i NCERT-om. MUP i NCERT potpisali su sporazum o suradnji, te se navedeni sporazum uspješno provodi. Suradnja sa ZSIS-om odvija se bez potpisanog sporazuma te je na sastanku glavnog ravnatelja policije i ravnatelja ZSIS-a zaključeno da, zbog izvrsne suradnje, nema potrebe za izradom posebnog sporazuma o suradnji.

SOA je kroz sudjelovanje u radu Vijeća i Koordinacije s nacionalnim institucijama u okviru svoje nadležnosti, uspostavila kontakt točke sa svrhom prevencije i efikasnijeg rješavanja kibernetičkih incidenata i to primarno kroz razvoj i implementaciju sustava SK@UT, sustava za otkrivanje, rano upozorenje i zaštitu od državno-sponzoriranih kibernetičkih napada, ATP kampanja te drugih kibernetičkih ugroza. SOA je također, kao nadležno nacionalno tijelo, uspostavila stalne nacionalne kontakt točke u okviru EU-CyCLONe mreže za upravljanje kibernetičkim krizama na razini EU-a. Za potrebe nacionalnog upravljanja kibernetičkim krizama, SOA je kroz koordinaciju međuresorne radne skupine nadležnih institucija (SOA, MUP, MORH, VSOA, ZSIS, NCERT, HAKOM i HNB), koristeći usuglašene Nacionalne standardne procedure za upravljanje kibernetičkim krizama, u 2023. godini nastavila koordinirati rad međuresorne radne skupine u redovitom stanju te je organizirala održavanje periodičkih kvartalnih sastanaka i provodila poticanje kibernetičke operativne suradnje različitih sektorskih nadležnih tijela na nacionalnoj razini, u skladu sa zahtjevima EU.

U svrhu prevencije i efikasnijeg rješavanja incidenata na nacionalnom nivou u DORH-u je osnovana Specijalizirana gruba za suzbijanje računalnog kriminaliteta gdje su članovi te grupe određeni kao kontakt točke za tijela izvan državnoodvjetničkog sustava dok su u svim općinskim i županijskim državnim odvjetništvima imenovane osobe koje isključivo rade na predmetima računalnog kriminaliteta, a te osobe su ujedno i kontakt točke za svako pojedino niže državno odvjetništvo. Specijalizirana grupa za suzbijanje računalnog kriminaliteta pri Državnom odvjetništvu RH je osnovana s ciljem savjetovanja i pružanja stručne pomoći za postupanje nižih državnih odvjetništva u konkretnim predmetima računalnog kriminaliteta i računalno potpomognutog kriminaliteta, koordiniranju rada na ovim predmetima te vođenja evidencije i nadzora o ovim predmetima za područje cijele RH.

Sukladno Uredbi izmjenama i dopunama uredbe o unutarnjem ustrojstvu Ministarstva unutarnjih poslova[17] Služba kibernetičke sigurnosti u MUP-u sudjeluje u primjeni i razvoju nacionalnog zakonodavnog okvira kibernetičke sigurnosti; sudjeluje u aktivnostima i mjerama u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora; sudjeluje u uspostavi učinkovitih mehanizama razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru; aktivno djeluje na jačanju svijesti o sigurnosti svih korisnika kibernetičkog prostora; razvija usklađene obrazovne programe; potiče istraživanja i razvoj; radi na sustavnom pristupu međunarodnoj suradnji u području kibernetičke sigurnosti; sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetičkog kriminaliteta (kaznena djela protiv računalnih sustava, programa i podataka, kaznena djela protiv intelektualnog vlasništva, te kaznena djela iskorištavanja djece za pornografiju) te predlaže rješenja na planu podizanja razine učinkovitosti rada u suzbijanju kibernetičkog kriminaliteta; neposredno provodi složena kriminalistička istraživanja; obavlja poslove digitalne forenzike koji uključuju osiguranje, prikupljanje, obradu i analizu digitalnih dokaza, pruža specijaliziranu potporu drugim policijskim jedinicama; surađuje s drugim ustrojstvenim jedinicama MUP-a, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada; sudjeluje u planiranju i izradi programa obuke i specijalizacije policijskih službenika; sudjeluje u izradi normativnih akata, izvješća i drugih stručnih materijala iz domene kibernetičkog kriminaliteta te obavlja i druge poslove iz svoga djelokruga.

MUP posjeduje forenzičke alate za izradu forenzičkih kopija nositelja elektroničkih dokaza te za analizu elektroničkih dokaza koji se nalaze na mobilnim telefonima, računalima i drugim nositeljima elektroničkih dokaza. U odnosu na forenzičke alate svake godine raspisuje se javna nabava te se obnavljaju licence. Tijekom 2023. godine nabavljen je i koristi se alat za dekripciju/otključavanje zaključanih pametnih telefona.

U okviru Nacionalnog programa oporavka i otpornosti Služba kibernetičke sigurnosti provodi projekt „C2.3. R3-I2 Jačanje kapaciteta policije za suzbijanje kibernetičkog kriminaliteta“. Cilj projekta je povećanje razine kibernetičke sigurnosti na području RH i EU-a, razvijanjem i unaprjeđenjem sustava prikupljanja, korištenja i analize digitalnih dokaza, organiziranjem i provođenjem specijaliziranih edukativnih programa o metodama istraživanja kaznenih djela protiv računalnih sustava, programa i podataka, namijenjenih policijskim službenicima te organiziranjem edukacija za šire građanstvo u svrhu podizanja svijesti o važnosti kibernetičke sigurnosti. U svrhu osnaživanja kapaciteta MUP-a za borbu protiv kibernetičkih prijetnji i kriminaliteta, tijekom 2023. godine provedene su sljedeće aktivnosti: Nabava kompleta i sustava za istraživanje kibernetičkog kriminaliteta, pretraživanje otvorenih izvora na internetu i digitalnu računalnu forenziku; Nabava istražiteljskih analitičkih računalnih setova za analizu digitalnih dokaza; Provedba preventivne kampanje za šire građanstvo i privatni sektor.

SOA kontinuirano brine o jačanju ljudskih potencijala te razvoju i nadogradnji alata i sustava za kibernetičku zaštitu. U tom cilju SOA je nastavila provoditi projekt SK@UT koji obuhvaća

[17] NN97/2020

izgradnju sustava za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza putem distribuirane mreže senzora u ključnim državnim tijelima i pravnim osobama. Implementacijom sustava SK@UT u državnim tijelima, kao i proširenjem opsega sustava tijekom 2023. godine na sektora ključnih usluga u području energetike, transporta i distribucije pitke vode te na pravne osobe od posebnog interesa za RH. Time se daje dodatni poticaj tijelima i pravnim osobama koji su korisnici sustava SK@UT, za razvoj kompetencija svojih zaposlenika te za bolje uređenje svojih kapaciteta i sposobnosti u području kibernetičke sigurnosti. U cilju sustavnog uređenja složenih poslovnih procesa koje SOA obavlja u području kibernetičke sigurnosti, na temelju Zakona o kibernetičkoj sigurnosti (NN 14/2024) započele su pripreme za transformaciju postojećeg Centra za kibernetičku sigurnost SOA-e u Nacionalni centar za kibernetičku sigurnost (NCSC-HR). U tom smislu nastavljena je i provedba nacionalnog procesa transpozicije EU NIS2 direktive kroz pripremu podzakonskih akata. Također je nastavljena i nacionalna koordinacija EU horizontalne skupine za suradnju u kibernetičkim pitanjima., s obzirom na novi niz akata iz područja kibernetičke sigurnosti koji su u pripremi na EU razini.

Predstavnici Službe kibernetičke sigurnosti MUP članovi su Odbora za sigurnost Hrvatske udruge banaka koji se bavi suradnjom na području kibernetičkih napada na bankarski sektor, te Povjerenstva za sigurnost Hrvatske udruge banaka koje se bavi suradnjom na području suzbijanja kartičnih prijevara.

NCERT svakodnevno surađuje s gospodarskim sektorom obradom računalno-sigurnosnih incidenata. Potiče se i suradnja kroz korištenje PiXi platforme za razmjenu informacija o incidentima i prijetnjama. Provode se aktivnosti podizanja svijesti korisnika o ugrozama koje dolaze s interneta što uključuje i gospodarski sektor.

III. ANALIZA PROVEDBE MJERA PO POVEZNICAMA PODRUČJA KIBERNETIČKE SIGURNOSTI

(F) Zaštita podataka

Za sigurnost i nesmetanu razmjenu i ustupanje zaštićenih (kategorija) podataka među različitim dionicima kibernetičke sigurnosti, **Strategijom je utvrđeno 5 ciljeva** koji su usmjereni na:

- unaprjeđenje nacionalne regulative u području poslovne tajne;
- poticanje kontinuirane suradnje između tijela nadležnih za posebne skupine zaštićenih podataka u nacionalnom okruženju u svrhu postizanja usklađenosti u provedbi relevantnih propisa;
- određivanje kriterija za prepoznavanje nacionalnih elektroničkih registara koji su kritični informacijski resursi te nositelja odgovornosti za njihovu zaštitu;

- unaprjeđenje postupanja sa zaštićenim podacima kod nositelja odgovornosti za zaštićene podatke, izvršitelja obrade zaštićenih podataka i ovlaštenih korisnika zaštićenih podataka;
- jednoobraznost korištenja palete normi informacijske sigurnosti HRN ISO/IEC 27000.

Radi ostvarenja ovih ciljeva, Akcijskim planom predviđeno je 6 mjera, pri čemu se jedna mjera provodi kontinuirano, za 4 mjere utvrđeni su rokovi provedbe od 12 mjeseci, odnosno 24 mjeseca od donošenja Strategije ili početka provedbe mjere, dok je provedba jedne mjere ovisila o donošenju EU direktive.

Stupanjem na snagu **Zakona o zaštiti neobjavljenih informacija s tržišnom vrijednosti**[18], u nadležnosti Državnog zavoda za intelektualno vlasništvo, zaštita poslovne tajne kao značajnog ekonomsko-pravnog instituta usklađena je sa zakonodavstvom EU-a (Direktiva EU 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija **poslovne tajne** od nezakonitog pribavljanja, korištenja i otkrivanja i Direktiva 2004/48/EZ Europskog parlamenta i Vijeća od 29. travnja 2004. o provedbi prava intelektualnog vlasništva). Definicija poslovne tajne, sukladno navedenom, sada je jasnije i šire definirana, dok se sama poslovna tajna počinje tretirati kao jedan oblik intelektualnog vlasništva nositelja poslovne tajne te se može smatrati da je mjera u cijelosti provedena.

Redovite koordinacijske aktivnosti nacionalnih tijela nadležnih za pojedine skupine zaštićenih podataka su se provodile primarno u okviru rada Vijeća, radi razmjene iskustava, detektiranja problema i/ili potencijalne neujednačenosti u primjeni propisa. Kontinuirana potreba praćenja i prilagodbe unutar specifičnih uvjeta postupanja akceptirajući posebnosti i promjene (primjenjive tehnologije i primjenjivi posebni propisi) različitih područja u kojima se primjenjuje zaštita osobnih podataka te posljedično dodatno zahtjevna angažiranost stručnih resursa AZOP-a u aktivnostima praćenja i provedbe primjene Opće uredbe o zaštiti podataka posebice u dijelu aktivnosti usmjerenih na provođenje istraga o primjeni Opće uredbe o zaštiti podataka kao i kontinuiteta osvješćivanja i edukacije voditelja i izvršitelja obrade osobnih podataka kao i samih ispitanika tj. građana (budući da se predmetna Uredba izravno i obvezujuće primjenjuje u državama članicama od 25.05.2018. godine) vezano i za adekvatnu i konzistentnu primjenu donesenih Smjernica EDPB-a (European Data Protection Board).

Provedba aktivnosti usmjerenih na ustrojavanje, obveze i odgovornosti nadležnih tijela, zaštitu i sva druga pitanja bitna za **nacionalne elektroničke registre podataka** realizirana je u okviru onih registara koji podliježu NIS direktivi te su na temelju Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga dio usluga koje se nude i podliježu zaštiti odnosno procesima nadzora definiranim u Uredbi o kibernetičkoj sigurnosti i operatora ključnih usluga i davatelja digitalnih usluga. Uspostavljena je radna skupina te se razmatraju dodatni zahtjevi za zaštitu nacionalnih elektroničkih registara, na lokacijama tijela i u oblaku, kroz izmjenu propisa o državnoj informacijskoj infrastrukturi.

Provedba mjere za unaprjeđenje **postupanja sa zaštićenim podacima** kod nositelja odgovornosti za zaštićene podatke, izvršitelja obrade zaštićenih podataka i ovlaštenih korisnika

[18] NN 30/18

zaštićenih podataka kroz izradu predložaka sadržaja dijelova ugovora (prilozi, aneksi, klauzule) kojim bi se obveznici primjene zakonskih propisa usmjeravali na detalje provedbe svih onih obveza koje su od visoke važnosti za zaštićene kategorije podataka provedena je još tijekom 2020. godine u znatnoj mjeri te su izrađeni predlošci za svaku zaštićenu kategoriju podataka i određene skupine klasificiranih i neklasificiranih podataka, a koji bi trebali dati odgovarajuću podlogu za kvalitetniji i sigurniji rad/postupanje te olakšati i ujednačiti samu provedbu kod obveznika primjene.

U ZSIS-u je završena interna analiza iskustava u korištenju palete normi HRN ISO/IEC 27000 kroz iskustva i aktivnosti ZSIS-a u korištenju ove palete normi u postupku sigurnosnih akreditacija informacijskih sustava. Uz navedeno ZSIS je prepoznao potrebu uvezivanja ove zadaće s cjelokupnim legislativnim okvirom (nacionalnim i EU) koji je donesen ili se planira donošenje. Slijedom toga je ZSIS 31. prosinca 2020. donio „Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava“ koji se temelji na normi HRN ISO/IEC 27001.

ZSIS i CARNET izradili su u listopadu 2019. dokument "Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti" koji se također temelji na normi HRN ISO/IEC 27001.

(G) Tehnička koordinacija u obradi računalnih sigurnosnih incidenata

Unaprjeđenje međusektorske organiziranosti te razmjena i ustupanje informacija o računalnim sigurnosnim incidentima nužni je uvjet učinkovitosti tehničke koordinacije u obradi računalnih sigurnosnih incidenata za čije su ostvarenje **Strategijom utvrđena 3 cilja**, usmjerena na:

- kontinuirano unaprjeđivanje postojećih sustava za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te skrb o ažurnosti drugih podataka ključnih za brzu i učinkovitu obradu takvih incidenata;
- redovito provođenje mjera za poboljšanje sigurnosti kroz izdavanje upozorenja i preporuka;
- uspostavu stalne razmjene informacija o računalnim sigurnosnim incidentima te relevantnih podataka i ekspertnih znanja u rješavanju specifičnih slučajeva kibernetičkog kriminaliteta.

Akcijskim je planom za ostvarenje ovih ciljeva predviđeno 5 mjera od kojih se jedna mjera treba provesti 12 mjeseci od donošenja Strategije, dok se preostale trebaju provoditi kontinuirano. Sve mjere se provode u cijelosti ili većim dijelom.

U cilju **kontinuiranog unaprjeđivanja postojećih sustava za prikupljanje, analizu i pohranu podataka** osnovana je radna skupina čiji su članovi, uz nositelje, naknadno dodani ovisno o razvoju platforme PiXi. Radna skupina prestala je s radom u 2022. godini nakon završetka projekta Grow2CERT, te je rad na platformi PiXi nastavljen u NCERT-u. Nastavlja se daljnji razvoj, promocija i uključivanju korisnika (predstavnika operatora ključnih usluga i davatelja digitalnih usluga) u PiXi platformu, te je edukacija nastavljena putem snimljenih

video materijala i korisničkih uputa. Na PiXi platformi je aktivirano ukupno 276 korisničkih računa. Prema rječniku Nacionalne taksonomije klasificirane su vrste incidenata i prijetnji na Platformi PiXi. U ožujku 2023. godine, nakon uključivanja predstavnika svih identificiranih operatora ključnih usluga i davatelja digitalnih usluga u rad Platforme PiXi, izmijenjene su Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga na način da se prijave takvih incidenata izvršavaju kroz PiXi platformu.
Najnovija inačica taksonomije u primjeni je od 1. siječnja 2022., a dostupna je na sljedećoj poveznici:
https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf

NCERT statistički vodi evidenciju o sektorskim incidentima za tri sektora: bankarstvo, davatelje Internet usluga i sektorske incidente koji su prijavljeni sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Sektorska razmjena informacija moguća je kroz platformu PiXi na kojoj prijavitelj sam bira razinu dijeljenja: bez dijeljenja (ostaje unutar organizacije), sektorsko dijeljenje (informacija se dijeli svim dionicima iz sektora u kojem je prijavitelj), nacionalno (informacija se dijeli svim korisnicima PiXi platforme na nacionalnoj razini) i dijeljenje na EU razini.

HNB prikuplja podatke o značajnim incidentima vezanima uz informacijske sustave institucija nad kojima provodi nadzor (kreditne institucije, institucije za elektronički novac, institucije za platni promet, pružatelji usluga agregiranja informacija o računu), a koje su obavezne takve incidente prijaviti prema:

- Revidiranim smjernicama o izvješćivanju o značajnim incidentima u skladu s PSD2
- Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga ili
- Odluci o primjerenom upravljanju informacijskim sustavom[19]

NCERT od kreditnih institucija, koje su obveznici primjene Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, informacije o incidentima zaprima sukladno Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom koje određuju način dostave obavijesti i sadrže obrasce za obvezno obavještavanje o incidentima sa znatnim učinkom te ih dostavlja HNB-u.

HNB je 9. srpnja 2021. ukinula obvezu svih kreditnih institucija za izvješćivanje o problemima u pružanju usluga putem izravnih distribucijskih kanala (bankomati, EFTPOS, internetsko bankarstvo, mobilno bankarstvo, e-commerce i PSD2 sučelja). Mehanizam je uspostavljen u travnju 2020. zbog posebnog fokusa na usluge koje se izravno pružaju elektroničkim kanalima, kao posljedica izvanrednih vanjskih okolnosti (COVID-19 pandemija i potresi).

[19] NN 110/2022

HNB je proteklih godina poduzimala i aktivnosti usmjerene ne prevenciju incidenata te je u suradnji s Europskom središnjom bankom implementirala instancu MISP (engl. Malware Information Sharing Platform) sustava. Od kraja 2018. i početka 2019. svim kreditnim institucijama omogućen je pristup toj platformi. MISP je platforma za pohranjivanje, povezivanje, korištenje i dijeljenje indikatora kompromitacije (tzv. IoC – engl. Indicator of Compromise) kibernetičkih napada, u zajednici pouzdanih sudionika. Pri tome instanca MISP sustava uspostavljena u HNB-u prvenstveno sadrži IoC-e kibernetičkih napada relevantnih za financijske institucije.

HNB je u 2023. godini slanjem kvartalnih situacijskih izvješća razmjenjivala anonimizirane podatke o prikupljanim incidentima s institucijama koje sudjeluju u radu Međuresorne radne skupine za upravljanje kibernetičkim krizama.

NCERT je u 2023. godini izdao 11 upozorenja putem web sjedišta www.cert.hr, Facebook stranice CERT.hr i Twitter računa HRCERT. Na usluzi CERT CVE (prije CERT Epsilon) koja korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava u 2023. godini bile su aktivne 184 pretplate, a ukupan broj posjeta stranici 6553. Usluga je namijenjena svim korisnicima, a posebno onima koji rade u području kibernetičke sigurnosti te im je potrebna sažeta informacija o poznatim ranjivostima proizvođača i proizvoda koje su sami odabrali u obliku personalizirane poruke elektroničke pošte. Usluga je dostupna na poveznici https://cve.cert.hr/

Hrvatska narodna banka (HNB) je u 2023. godini izdala četiri objave svim kreditnim institucijama o uočenim sigurnosnim prijetnjama i ranjivostima te preporuke za daljnje postupanje.

HAKOM je izdao u 2023. godini 36 upozorenja / preporuka putem društvenih mreža.

Policijski službenici Službe kibernetičke sigurnosti MUP su tijekom 2023. godine u više navrata tijekom složenih kriminalističkih istraživanja surađivali sa SOA-om, ZSIS-om i NCERT-om, čiji su djelatnici pružali stručnu i tehničku pomoć prilikom obavljanja poslova forenzičkih analiza digitalnih dokaza i mrežne forenzike, te se između navedenih tijela redovito razmjenjuju informacije od značaja za kibernetičku sigurnost i održavaju tematski radni sastanci.

SOA je kroz suradnju s nacionalnim institucijama te kroz sudjelovanje u radu Operativno-tehničke koordinacije za kibernetičku sigurnost ubrzala razmjenu podataka te poboljšala razmjenu znanja i iskustva. Izgradnja i širenje sustava SK@UT za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza. Tijekom 2023. godine otvorila se mogućnost puno dublje suradnje u okvirima sustava SK@UT za preko 70 institucija koje su pristupile sustavu SK@UT, a koja uključuju i državna tijela i operatore ključne infrastrukture, kao i pravne osobe od posebnog interesa za RH. Dodatna razmjena iskustva i znanja intenzivno se provodila tijekom 2023. godine kroz rad međuresorne radne skupine za upravljanje kibernetičkim krizama, u kojoj je sudjeluju predstavnici sedam institucija koje koordinira SOA. Zaključkom Vlade RH iz rujna 2022. godine SOA je određena za nacionalnog stručnog nositelja Horizontalne radne skupine za

kibernetička pitanja, te je sukladno tome tijekom 2023. godine ispred RH koordinirala niz novih akata iz područja kibernetičke sigurnosti koje predlaže Europska Komisija (npr. Cyber Resiliency Act i Cyber Solidarity Act ili amandmani na Cyber Security Act iz 2019. godine).

(H) Međunarodna suradnja

Strategijom je kao prioritet RH u području kibernetičke sigurnosti na međunarodnom planu **utvrđeno 6 ciljeva** koji su usmjereni na:

- jačanje suradnje na područjima vanjske i sigurnosne politike s partnerskim državama;
- učinkovito sudjelovanje RH u razvoju međunarodnog pravnog okvira i adekvatno usklađivanje i razvoj nacionalnog pravnog okvira u ovom području;
- nastavak i razvijanje bilateralne i multilateralne suradnje;
- promicanje koncepta izgradnje mjera povjerenja u kibernetičkoj sigurnosti;
- razvoj i jačanje sposobnosti koordiniranog nacionalnog i međunarodnog odgovora na prijetnje kibernetičke sigurnosti, kroz sudjelovanje i organizaciju međunarodnih civilnih i vojnih vježbi i drugih stručnih programa; te
- jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.

Radi ostvarenja ovih ciljeva, Akcijskim planom predviđeno je 6 mjera za koje je određena kontinuirana provedba. Sve mjere su provođene u **potpunosti ili većim dijelom**.

Formalno **uspostavljanje koordinacije ispunjeno je u cijelosti** usvajanjem Zaključka NVKS sredinom 2018. godine. Zbog spleta logističkih, kadrovskih i drugih otegotnih okolnosti, Stalna radna skupina za međunarodne aktivnosti nije održavala formalne sastanke te je većina potrebnih aktivnosti odrađena redovnom (fizičkom i elektronskom) komunikacijom unutar samog Vijeća. Uspjeh provedbe mjere se očitovao kroz:

- Uspješno prenošenje informacija o ključnim kibernetičkim pitanjima iz okvira djelovanja EU i međunarodnih organizacija i inicijativa;
- suradnja u provedbi OESS-ovih tzv. *Comm-check* vježbi kao provedbe Mjera za izgradnju povjerenja (CBMs) na području kibernetičke sigurnosti;
- sudjelovanje RH na trećem samitu međunarodne inicijative protiv kibernetičkog iznuđivanja (*ransomware*) održanog krajem 2023. u Washingtonu, SAD;
- periodično praćenje online stručnih evenata u organizaciji EU CyberNet;
- aktivno sudjelovanje u grupi država istomišljenica koje podupiru prijedlog uspostave tzv. Programa akcije (PoA) za pitanja kibernetičke sigurnosti u okviru Ujedinjenih naroda;
- održavanje međuresornih konzultacija s predstavnicima nadležnih institucija Republike Slovenije

Međunarodna suradnja postoji kroz nekoliko članstva u međunarodnim udruženjima CERT-ova kao što su FIRST (Forum od Incident Response and Security Teams) i TI (Trusted Introducer) čiji je NCERT akreditirani član, te članstvom u Mreži CSIRT-ova (CSIRT Network) koja je nastala temeljem NIS direktive.

Uz značajne napore, u prvom redu MVEP-a te stalnih misija odnosno predstavništava RH pri EU i UN, veći dio aktivnosti vezan uz **sudjelovanje RH u razvoju međunarodnog pravnog okvira** i adekvatno usklađivanje i razvoj nacionalnog pravnog okvira u ovom području bio je pokriven diplomatskim putem. Nakon prvih, poglavito organizacijskih sjednica, UN-ov *Ad hoc* Odbor za izradu sveobuhvatne međunarodne konvencije o suzbijanju korištenja informacijskih i komunikacijskih tehnologija za kriminalne svrhe počeo je sa supstantivnim raspravama i razradama prijedloga buduće konvencije oko čega je koordinaciju izrade stajališta i nastupa preuzela EK. Daljnje praćenje procesa odvijalo se kroz izvještavanje stalnih predstavništava RH u New Yorku, Beču te posebice u Bruxellesu.

U ključnim međunarodnim aktivnostima na području kibernetičke sigurnosti RH aktivno sudjeluje u konzultacijama s drugim državama istomišljenicama, kako u sklopu EU tako i u pojedinim međunarodnim organizacijama te globalnim inicijativama. U izvještajnom razdoblju nastavljeni su i pojačani sastanci tzv. EU mreže kibernetičkih veleposlanika (i u fizičkom i u online formatu). Učestalije su organizirani i zajednički koordinativni sastanci koji su uključili i novu dimenziju tzv. mreže digitalnih veleposlanika. Prenesene su informacije i o konzultacijama (tada budućeg) BE PRES, s ciljem unaprjeđenja rada i institucionalnog okvira po digitalnim pitanjima, kao i komplementarnosti s postojećim *cyber* i telekom aktivnostima unutar Vijeća EU - što otvara pitanje ustrojavanja nacionalne međuresorne koordinacije za digitalna pitanja.

U okviru rada samog Vijeća, 12. srpnja 2023. održane su bilateralne multiresorne konzultacije s predstavnicima slovenskih institucija predvođenih Uredom Vlade Slovenije za informacijsku sigurnost. Razmijenjene su informacije i stajališta o temama od zajedničkog interesa, uključujući ekosustave kibernetičke sigurnosti u SI/HR (strategije, zakoni); procese upravljanja kibernetičkim incidentima u SI/HR (krizno upravljanje); općenito o aktivnostima CERT-ova; izazovima novih tehnologija (5G); komunikacijskim strategijama o kibernetičkim incidentima; pitanjima atribucije (tehnički, pravni, politički te međunarodni aspekti) te druga relevantna pitanja. S hrvatske strane sudjelovali su UVNS, MVEP, MORH, SOA, ZSIS, CARNET i AZOP. Kroz direktan bilateralni kontakt sredinom studenog potvrđen je i dalje visoki interes UK za jačanjem suradnje s RH. Tijekom godine u direktnoj bilateralnoj suradnji s međunarodnim partnerima prevladavale su teme međunarodnopravnog okvira za kibernetičku sigurnost, shema kibernetičke sigurnosne certifikacije za oblačno računarstvo, *end-to-end* enkripcije, 5G tehnologije, suzbijanja kibernetičkog iznuđivanja, malicioznog kibernetičkog uplitanja u izborne procese i sl. Međutim, do kraja godine se posebno profilirala kao teme od posebnog interesa iz različitih kutova razmatranja – umjetna inteligencija.

Čak je i Vijeće sigurnosti UN-a 18. srpnja po prvi put održalo tematsku raspravu o umjetnoj inteligenciji i njenom utjecaju na međunarodni mir i sigurnost. U tom smislu MVEP je predložilo da se, po uzoru na radnu skupinu za 5G, u okviru međuresorne suradnje pokrene i skupina za pitanja UI i sigurnosti, te uspostavi suradnja s Hrvatskom udrugom za umjetnu inteligenciju. U međuvremenu, RH pridružila se Političkoj deklaraciji o odgovornoj vojnoj uporabi umjetne inteligencije i autonomije, koja pruža normativni okvir koji se bavi uporabom ovih sposobnosti u vojnoj domeni.

U okviru EU aktivnosti, MVEP je detaljno prenio i situaciju vezanu uz problematiku neadekvatnog prijevoda prefiksa „*cyber*“ i poduzetih diplomatskih aktivnosti u tom smislu.

Također, tijekom godine nastavljen je rad na reviziji instrumentarija *Cyber Diplomacy Toolbox* i njegove provedbe, odnosno unaprjeđenja EU kibernetičkog okvira, uključujući i proširenjem na sektorske sankcije.

Krajem 2023. godine hrvatsko izaslanstvo sudjelovalo je na 3. Summitu Inicijative za borbu protiv kibernetičkog iznuđivanja (CRI) na kojemu je sudjelovalo 50 članica Inicijative (48 država + EU + INTERPOL), što je 13 više nego 2022. godine. Raspravljalo se o budućoj zajedničkoj platformi za koordinaciju. Veliki naglasak i dalje je bio na izgradnji kapaciteta. Po završetku je usvojena zajednička izjava kojom se pozivaju svi dionici na suzdržavanje od plaćanja otkupnina. Stoga se može konstatirati kako mjera **poticanja i potpomaganja bilateralne i multilateralne suradnje** u okviru postojećih i budućih sporazuma s međunarodnim asocijacijama provodila u potpunosti.

U okviru aktivnosti OESS-a tijekom 2023. godine RH je nastavila sudjelovati (uglavnom putem MVEP) u redovnim, ali nenajavljenim Comm-check vježbama za provedbu **mjera za izgradnju povjerenja** (CBMs). Pitanja izgradnje povjerenja radi smanjenja mogućih rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija pojavljuju se sve učestalije i u radu UN-a (OEWG, a posredno i UNGGE), što je dovelo do inicijative za kreiranjem i globalnog direktorija nacionalnih CBMs političkih i tehničkih kontakt-točaka na razini UN-a, a po uzoru na postojeći mehanizam OESS-a. U okviru obje organizacije MVEP (politički) i SOA (tehnički) predstavljaju nacionalne kontakt točke za mjere izgradnje povjerenja u području kibernetičke sigurnosti.

Nacionalni CERT je u studenom 2023. godine sudjelovao u vježbi Cyber SOPEx u organizaciji ENISA-e. Cilj vježbe je poboljšanje suradnje i komunikacije između CSIRT-ova Europske unije te poboljšanje standardnih operativnih procedura. U organizaciji NATO-a 2023. godine održana je vježba Cyber Coalition a obuhvaćala je obranu od zlonamjernog sadržaja, hibridne izazove, testiranje operativnih i pravnih procedura te suradnju s privatnim sektorom i akademskom zajednicom. CARNET je imao ulogu IPoC (Inudstrial Point of Contact) čime je koordinirao sudjelovanje privatnog sektora i akademske zajednice. Nacionalni CERT i CARNET su sudjelovali u tehničkoj obučnoj skupini, pravnoj obučnoj skupini, obučnoj skupini za kriznu komunikaciju te u role-play skupini.

Aktivnosti usmjerene na jačanje suradnje u području ***upravljanja rizicima europskih kritičnih infrastruktura*** su se provodile u značajnoj mjeri. U organizaciji OSRH pravovremeno su provođeni planski sastanci i druge pripremne aktivnosti za potrebe NATO „*Cyber Coalition* 2023“ vježbe, uključujući i suradnja s drugim TDU te stručnjacima iz sfere akademske zajednice i privatnog sektora. Pored jačanja nacionalnih operativno-tehničkih sposobnosti, važno je zadržati i unaprijediti sposobnosti ključne za upravljanje operacijama i donošenje kvalitetnih odluka, a koje se odnose na pravne aspekte kibernetičkog djelovanja, dakle pravila postupanja (*rules of engagement*) u scenarijima odnosno situacijama koje nerijetko nisu nedvojbeno međunarodnopravno regulirane.

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

U svrhu izgradnje razvijenog suvremenog društva te iskorištavanja tržišnog potencijala informacijske sigurnosti i informacijskog društva u cjelini, kroz sustavan pristup podizanju razine kompetencija cjelokupnog društva u području kibernetičke sigurnosti, **Strategija definira 3 cilja** usmjerena na **razvoj i jačanje**:

- ljudskih potencijala u području sigurnosti komunikacijsko-informacijskih tehnologija;
- svijesti o sigurnosti u kibernetičkom prostoru;
- nacionalnih sposobnosti, istraživanje i poticanje gospodarstva.

Akcijskim je planom, radi ostvarenja ciljeva, utvrđeno 27 mjera od čega je za tri mjere rok provedbe 2017. - 2020., za dvije mjere 6 mjeseci, odnosno 12 mjeseci po donošenju Strategije, dok se ostale 22 mjere trebaju provoditi kontinuirano.

Donošenjem Nacionalnog kurikuluma za rani i predškolski odgoj i obrazovanje 2015. godine stvoreni su uvjeti za poticanje razvoja osobnog identiteta djeteta te osnaživanje u izgrađivanju osjećaja sigurnosti u susretu iskustvima u užem i širem socijalnom okruženju. U Kurikulumu je navedeno osam ključnih kompetencija za cjeloživotno obrazovanje, u koje je uključena i Digitalna kompetencija u kojoj se dijete, između ostaloga, osnažuje u uporabi informacijsko-komunikacijske tehnologije.

Donesene su Odluka o donošenju kurikuluma za nastavni predmet Informatike za osnovne škole i gimnazije u RH[20] i Odluka o donošenju kurikuluma za međupredmetnu temu Uporaba informacijske i komunikacijske tehnologije za osnovne i srednje škole u RH[21] u cilju ostvarivanja mjere uvrštavanja predmetnih i međupredmetnih sadržaja vezanih uz kibernetičku sigurnost u osnovnoškolske i srednjoškolske programe.

U sklopu Eksperimentalnog programa „Osnovna škola kao cjelodnevna škola - uravnotežen, pravedan, učinkovit i održiv sustav odgoja i obrazovanja" u 2023./2024. školskoj godini uveden je Nastavni predmet Informacijske i digitalne kompetencije koji se uči i poučava u svih osam razreda osnovne škole. Izrađeni su udžbenici i radne bilježnice za predmet Informacijske i digitalne kompetencije za 1. i 5. razrede OS. Satnica nastavnoga predmeta iznosi 35 sati godišnje. Domena Komunikacija, suradnja i sigurnost usmjerena je na razvoj kompetencija potrebnih za učinkovitu i sigurnu komunikaciju u digitalnome okruženju. Teme kao što su područje sigurnosti na mreži, zaštita podataka, elektroničko nasilje i briga o svojoj digitalnoj dobrobiti razvijaju potrebne vještine i stavove nužne za odgovorne, kompetentne, kreativne i pouzdane sudionike digitalnoga društva. Objavljivanje te dijeljenje podataka, sadržaja i izvora uz poštivanje svih etičkih načela, omogućuje širemu broju ljudi stvaranje

[20] NN 22/2018
[21] NN 7/2019

novih znanja i vrijednosti. Istraživanje poslova i područja u kojima se koristi digitalnom tehnologijom pridonosi budućoj profesionalnoj orijentaciji i razvoju mlade osobe.

ASOO odraslih je kroz ESF projekt „Modernizacija sustava strukovnog obrazovanja i osposobljavanja" izradila 132 nova strukovna kurikuluma te će se teme vezane uz kibernetičku sigurnost poučavati kroz sadržaje iz informacijsko komunikacijskih tehnologija.

Novi kurikulumi izrađeni su za obrazovne sektore:

- Ekonomija i trgovina (izrađeno je 9 novih strukovnih kurikuluma)
- Pravo, politologija, sociologija, državna uprava i javni poslovi (izrađena su 4 nova strukovna kurikuluma)
- Graditeljstvo i geodezija (izrađeno je 13 novih strukovnih kurikuluma)
- Strojarstvo, brodogradnja i metalurgija (izrađeno je 11 novih strukovnih kurikuluma)
- Turizam i ugostiteljstvo (izrađeno je 6 novih strukovnih kurikuluma)
- Osobne, usluge zaštite i druge usluge (izrađena su 4 nova strukovna kurikuluma)
- Grafička tehnologija i audiovizualne tehnologije (izrađeno je 10 novih strukovnih kurikuluma)
- Geologija, rudarstvo, nafta i kemijska tehnologija (izrađena su 3 nova strukovna kurikuluma)
- Zdravstvo (izrađena su 2 nova strukovna kurikuluma)
- Psihologija, edukacijska rehabilitacija, logopedija i socijalne djelatnosti (izrađena su 2 nova strukovna kurikuluma)
- Poljoprivreda, prehrana i veterina (izrađeno je 16 novih strukovnih kurikuluma)
- Promet i logistika (izrađeno je 14 novih strukovnih kurikuluma)
- Elektrotehnika i računarstvo (izrađeno je 16 novih strukovnih kurikuluma)
- Moda, tekstil i koža (izrađeno je 12 novih strukovnih kurikuluma)
- Šumarstvo, prerada i obrada drva (izrađeno je 10 novih strukovnih kurikuluma)

Kroz ostvarene aktivnosti ovog ESF projekta koji se je provodio posljednje tri godine uspješno je započeta sveobuhvatna kurikularna reforma strukovnog obrazovanja u RH.

MZO je u 2023. godini provelo upis u Upisnik studijskih programa 2 studijska programa u području Tehničkih znanosti:

- sveučilišni diplomski studij Mehatronika i robotika Fakulteta strojarstva i brodogradnje Sveučilišta u Zagrebu (polje Strojarstvo)
- stručni prijediplomski studij Računarstvo Tehničkog veleučilišta u Zagrebu (do sada se izvodio kao modul studija Politehnika, a od akademske godine 2023./24. upisan je u Upisnik kao zaseban studij (polje Računarstvo).

Nastavno na ciljeve digitalne preobrazbe visokih učilišta, ulaganjem u projekt „e-Sveučilišta" kroz NPOO[22] unaprijedit će se digitalna preobrazba visokog obrazovanja za 90% javnih visokih učilišta. Projekt je podijeljen u elemente: mrežna i računalna infrastruktura, oprema i povezani servisi, unaprjeđenje postojećeg informatičkog sustava i povezivanje evidencija u visokom obrazovanju, edukacijska podrška i obrazovni programi osnaživanja kompetencija nastavnog osoblja za učenje i poučavanje u digitalnom okruženju, podrška i profesionalni razvoj stručnog osoblja te horizontalne aktivnosti kibernetičke sigurnosti. Provedba projekta započela je 21. ožujka 2022. s planiranim završetkom 31. prosinca 2025.

Poboljšanje sigurnosti informacijskih sustava visokih učilišta i učinkovitosti reagiranja na incidentne situacije te početak razvoja sadržaja i provedbe obrazovanja visokih učilišta u vezi istog, dio je aktivnosti kibernetičke sigurnosti koja se provlači horizontalno kroz cijeli projekt te čini nezaobilazni dio aktivnosti u okviru modernizacije visokih učilišta, prilikom planiranih ulaganja u digitalnu tranziciju visokog obrazovanja.

ASOO provodi stručna usavršavanja nastavnika strukovnih predmeta u srednjim strukovnim školama te obrazovnog osoblja u ustanovama za obrazovanje odraslih prema Konceptu novog modela stručnog usavršavanja unutar kojeg je razvijen i modul MI 12 (S3) Kibernetička sigurnost.

Cilj navedenog modula je stjecanje znanja o sigurnosnim politikama (povjerljivost, integritet, dostupnost), ključnim pojmovima i konceptima povezanim sa zakonodavstvom u području kibernetičke sigurnosti, o kriptografiji i suvremenim tehnikama enkripcije te razmatranje pristupa za upravljanje rizicima i zaštiti poslovanja, osobnih podataka, uređaja i okoline. ASOO i Span Centar kibernetičke sigurnosti održali su u prosincu 2023. god. vrlo važnu edukaciju na temu „Osnove kibernetičke sigurnosti" . Cilj edukacije bio je da se zbog sve učestalijih kibernetičkih napada, svakodnevne primjene računala, mobitela i interneta, nastavnici moraju svladati osnovna načela sigurnosti kako bi isto znanje mogli prenijeti svojim učenicima i kako bi mogli prepoznati potencijalne prijetnje s kojima se suočavaju učenici.

Edukaciju nastavnicima koji u školi ne predaju samo i isključivo informatiku nego i ostale predmete držao je Zoran Kežman, Spanov stručnjak za cyber sigurnost koji im je prenio znanja za bolje razumijevanje ozbiljnosti prijetnji u kibernetičkom svijetu. Ovo usavršavanje bilo je namijenjeno primamo profesorima i nastavnicima strukovnih škola koji žele biti sigurniji u korištenju računala, mobilnih uređaja i interneta, bez obzira na njihovo informatičko predznanje.

U sklopu ove edukacije 35 nastavnika iz više od 20 škola imalo je priliku naučiti više o sigurnijem korištenju računala, interneta, društvenih mreža i elektroničke pošte. Neke od ključnih točaka edukacije bile su usmjerene na postavljanje sigurnijih lozinki i bolju zaštitu korisničkih računa, zatim na izbjegavanje zlonamjernih softvera, sigurnije rukovanje

[22] Nacionalni plan oporavka i otpornosti 2021.-2026.

dokumentima te siguran rad izvan ureda, a posebna je pozornost posvećena edukaciji o opasnostima na društvenim mrežama.

Nadalje, kako bi se dodatno osiguralo sustavno obrazovanje učitelja, nastavnika, ravnatelja i stručnih suradnika u srednjim strukovnim školama, Osim usavršavanja koje provodi ASOO dodatnu podršku nastavnom i nenastavnom osoblju pružaju i srednje strukovne škole na području cijele RH koje na školskoj, županijskoj i međužupanijsko razini organiziraju usavršavanja na teme vezane uz kibernetičku sigurnost.

Tako su na županijskoj razini tijekom 2023. u Obrazovnom sektoru ekonomije, trgovine i poslovne administracije provedena sljedeća usavršavanja nastavnika na temu kibernetičke sigurnosti:

- Medijska pismenost - Kristina Vukošić Popov, dr.sc. dipl. oec, nastavnica Ekonomska škola Šibenik, ishodi: procijeniti sigurnost podataka na internetu; ocijeniti važnost zaštite podataka na internetu,19 sudionika,
- Digitalni marketing i izazovi digitalnog poslovanja - Mario KOS, Kosinus, obrt za usluge, Koprivnica, ishod: identificirati načine povećanja sigurnosti u on line okruženju, 25 sudionika, Utjecaj digitalnih medija na ponašanje mladih - Anita Grgić, mr.sc. i Ivana Cikeš, dipl. oec., Ekonomska i upravna škola Split, ishod: Prepoznati rizike i opasnosti koje nose virtualni odnosi, 43 sudionika i
- Sigurnosne ugroze u digitalnom okruženju - mr.sc.Miljenko Vrbanec, viši predavač na Međimurskom veleučilištu u Čakovcu, ishodi: dati primjer sigurnosnih ugroza u digitalnom okruženju; objasniti načine zaštite od digitalnih prijetnji i sigurnosnih ugroza; koristiti sigurniji način rada u digitalnom okruženju, 25 sudionika.

Poticanje uključivanja mladih u vodene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja je provedeno kroz financiranje 8 projekata prijavljenih na natječaj MZO-a za dodjelu bespovratnih sredstava u području izvaninstitucionalnog odgoja i obrazovanja.

ASOO je od 10. do 12. svibnja 2023. godine u Zagrebu organizirala:

- Državno natjecanje učenika strukovnih škola — „WorldSkills Croatia 2023“
- Croatia 2023., najveći događaj u obrazovanju u RH i najveće natjecanje u ovomu dijelu Europe. Na natjecanju je sudjelovalo 400 najboljih učenika strukovnih škola uz pratnju i podršku njihovih nastavnika, natjecali su se u 46 strukovnih disciplina — od onih tradicionalnih struka, kao što su frizerstvo, zidarstvo, pekarstvo i cvjećarstvo, pa do suvremenih disciplina poput administracije IT sustava, CNC i CAD-CAM tehnologija ili interdisciplinarne discipline poput robotike. Jedna od natjecateljskih disciplina koja je uključivala elemente kibernetičke sigurnosti bila je Administracija IT u kojoj se je natjecalo osam (8) učenika koji se školuju u sljedećim zanimanjima:
    - Tehničar telekomunikacije
    - Tehničar za računalstvo

- Tehničar za elektroniku

Učenici su pokazali vrlo dobru razinu znanja u rješavanju zadataka koji su uključivali elemente kibernetičke sigurnosti.

U MUP-u su tijekom 2023. godine, u organizaciji PA i Uprave kriminalističke policije održana slijedeća stručna usavršavanja:

- jedan modul treninga „Istraživanje seksualnih kaznenih djela na štetu djece putem Interneta“ u trajanju od 5 dana,
- jedan modul treninga „Praktična iskustva u predmetima istraživanja kibernetičkog kriminaliteta“ u trajanju od 4 dana.
- dva modula treninga „Istraživanje otvorenih izvora na internetu (OSINT)“.

Policijski službenici za kibernetičku sigurnost i digitalnu forenziku sudjelovali su na sljedećim radionicama i seminarima u organizaciji CEPOL-a (Europske Policijske Akademije):

- Advanced Windows File System Forensics
- Mobile Foresics
- Apple Forensics
- First responders and cyber-forensics
- Cyber Intelligence
- Cross-border Exchange of e-Evidence
- Open-Source Intelligence (OSINT)
- Open-Source Intelligence (OSINT) and IT Solutions

PA je u 2023. godini održala tri jednodnevne radionice na teme „Kibernetički kriminalitet“ za kaznene suce i sudske savjetnike općinskih i županijskih sudova te zamjenike državnih odvjetnika i državnoodvjetničke savjetnike općinske i županijske razine. Ukupno su sudjelovala 32 polaznika.

U okviru međunarodne suradnje PA troje hrvatskih pravosudnih dužnosnika je sudjelovalo na HELP-ovom e-tečaju Vijeća Europe o suzbijanju kibernetičkog kriminala.

U 2023. godini izrađen je popis znanja, kompetencija i vještina iz područja kibernetičke sigurnosti za operativno-tehničke uloge i voditeljske uloge u NCERT-u. Popis je izrađen na osnovu ENISA ECSF – European Cybersecurity Skills Framework: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Zahvaljujući sudjelovanju u EU projektima mogućnosti edukacije za djelatnike i suradnike NCERT-a su znatno povećane, ali na kratki rok – trajanje projekta. Ovisno o potrebama, edukacije za neke zaposlenike su obavezne, zaposlenik ima mogućnost samostalnog biranja edukacije, dok su vanjski suradnici uglavnom obavezni proći unaprijed definirane online edukacije. Edukacije se odnose na sve djelatnike i suradnike u NCERT-u. U 2023. godini šest

djelatnika sudjelovalo je na tehničkom ili operativnom treningu LETRA u organizaciji ENISA-e: Defending Against Adversary Actions, Zero Trust Arhitecture te Cyber Awareness Program Development. Pohađani su treninzi za Splunk SIEM sustav u organizaciji tvrtke INFIGO IS i Linux akademija u organizaciji SRCE-a. Tvrtka Infigo IS je za zaposlenike NCERT-a održala dvije edukacije na teme penetracijskog testiranja web aplikacija i sigurnosti Windows AD-a. Osim toga, zaposlenici su u 2023. godini sudjelovali u školovanjima u sklopu CARNET-ovog projekta e-Škole: DevSecOps, aplikacije u kontejnerima (osnovni i napredni modul), upravljanje projektima, upravljanje IT uslugama, vođenje sastanaka, komunikacijske, pregovaračke, prezentacijske i voditeljske vještine i izgradnja timova. Jedan zaposlenik se školovao u *online bootcampu* pod nazivom *„Red Team Ops with Powershell Empire“* gdje je predstavljen okvir za post-eksploataciju. Zaposlenica je sudjelovala u radionica u organizaciji MORH-a pod nazivom *„Primjena prava u kibernetičkom prostoru"*. NCERT je sudjelovao na nekoliko konferencija i susreta vezanih uz teme EU legislativa, umjetne inteligencije, razvoja aplikacija, OSINT-a, cryptojacking, ransomware napada i druge. Zbog jačanja internih kapaciteta u NCERT-u postoji stalno obnavljan repozitorij knjiga, stručnih časopisa, mrežnih tečajeva i digitalnih knjiga i priručnika.

Definirane su potrebne izobrazbe i načini stjecanja znanja za zaposlenike i ustrojstvene cjeline pod nadležnošću i u potpori CERT-a Ministarstva obrane i Oružanih snaga RH. (Stručni specijalistički diplomski studij informacijske sigurnosti i digitalne forenzike (TVZ), tečajevi iz domene kibernetičke sigurnosti (obrazovne institucije u RH, suradnja s partnerima, tečajevi putem udaljenog pristupa, tečajevi na Kibernetičkom poligonu).

Djelatnici MORH su sudjelovali u sljedećim edukacijama iz područja kibernetičke sigurnosti:

- Tehničko veleučilište Zagreb (Ugovor o suradnji): Stručni specijalistički diplomski studij informacijske sigurnosti i digitalne forenzike 2022/2023
- Tehničko veleučilište Zagreb (Ugovor o suradnji): Stručni specijalistički diplomski studij informacijske sigurnosti i digitalne forenzike 2023/2024
- Školovanja u SAD:
    - IMET, Napredna časnička izobrazba, SAD
    - „Cyber Security Fundamentals and Defense Certificate“, Naval Postgraduate School, Monterey, California
- Školovanja u CCDCOE, Estonija:
    - Exoloitation Advance Course
    - Introduction Digital Forensic Course
    - Cyber Defence Monitoring Course
    - Cyber Defence Monitoring Course: Large Scale Packet Capture Analysis
- Organizirana obuka Mandiant ThretaSpace uz potporu stručnjaka tvrtke Mandiant
- Tečajevi u sklopu Središta za obuku Zapovjedništva za kibernetički prostor:

    - CompTIA Security Plus
    - Tečajevi na kibernetičkom poligonu.
- Ostali tečajevi:
    - Kontinuirano korištenja on-line tečajeva Offensive Security

U 2023. HAKOM je nastavio s aktivnostima podizanja svijesti o važnosti kibernetičke sigurnosti objavljivanjem aktualnih novosti vezane uz kibernetičku sigurnost putem društvenih mreža i svoje internetske stranice.

U veljači 2023. obilježen je Dan sigurnijeg interneta prigodnim događajem organiziranim u suradnji sa osnovnom školom Rapska te sudjelovanjem na konferenciji „Potraga za boljim internetom″ na organiziranom od strane Udruge Suradnici u učenju, CARNET-a i NCERT-a, a s koje je poslana poruka o potrebi snažnije prevencije elektroničkog nasilja, zaštite osobnih podataka djece, stvaranja sigurnog virtualnog okružja te dostupnosti kvalitetnih internetskih sadržaja za djecu i mlade. Jedan od najvažnijih dana u kalendaru internetske sigurnosti okupio je brojne relevantne sugovornike, ali i nastavnike i učenike obrazovnih ustanova diljem RH kako bi se ukazalo na svakodnevnu potrebu zaštite djece i mladih. Predstavljena je i nova, redizajnirana HAKOM-ova brošura pod naslovom „Kako se zaštititi u svijetu interneta i mobilnih uređaja“ koja sadrži praktične i korisne savjete o opasnostima i sigurnosti na internetu, zaštiti privatnosti i osobnih podataka, načinu ponašanja i odgovornoj uporabi društvenih mreža, a dio je HAKOM-ovog programa informiranja djece i roditelja koji se od 2016. provodi u suradnji s MZO-om.

U 2023. nadopunjena je i ažurirana aplikacija "Kalkulator privatnosti" dodavanjem novih scenarija prema zastupljenosti prijevara u hrvatskom internetskom prostoru te Kviz o sigurnosti na internetu.

Aktivnosti usmjerene na izradu i publiciranje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike usluga udomljavanja različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi), s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva, provode se u potpunosti. U 2018. godini je izdana brošura „Sigurnost bežičnih mreža“ te je dostupna u digitalnom obliku, a također je tiskana i dijeljena na raznim događanjima.

Mjera čijom provedbom pružatelji e-usluga trebaju ostvariti blisku suradnju s nadležnim tijelima za koordinaciju prevencije i odgovara na ugroze informacijskih sustava provodi se u manjoj mjeri. SDURDD provodi projekt redizajna sustava e-Građani. Također, radi se i na projektu standardiziranja elektroničkih usluga koji definira standardizirani proces upravljanja i razvoja elektroničkih usluga koje će se spajati na državnu informacijsku infrastrukturu. Ujedno, sve usluge unutar sustava e-Građani dužne su imati upute za korištenje, a za pojedine usluge su izrađene i video upute.

HNB na temelju informacija o računalno sigurnosnim prijetnjama koje zaprimi kroz suradnju s drugim nacionalnim i EU tijelima diseminira informacije relevantnim dionicima unutar sektora.

U 2023. godini HNB je izdala četiri objave svim kreditnim institucijama o uočenim sigurnosnim prijetnjama i ranjivostima te preporuke za daljnje postupanje. Značajnije objave upućene su i institucijama za platni promet te institucijama za elektronički novac.

U drugom kvartalu 2023. godine, u suradnji s HANFA-om, održana je radionica za financijske institucije o nacrtima podzakonskih akata proizašlih iz DORA Uredbe[23]. Cilj radionice bio je upoznati predstavnike financijskih institucija s Uredbom DORA, međuovisnosti DORA Uredbe i povezanih akata EU o kibernetičkoj sigurnosti, opsegom primjene DORA Uredbe, procesom javnog savjetovanja o tehničkim standardima i sadržajem tehničkih standarda (Upravljanje IKT rizikom, Upravljanje incidentima i prijetnjama, Testiranje digitalne operativne otpornosti, Upravljanje trećim stranama i Nadzor IKT pružatelja usluga trećih strana).

Nadalje, u 2023. godini nadziranim institucijama upućeno je 19 dopisa i 4 okružnica te je održano 47 sastanaka s temama vezanima uz rizike korištenja informacijskih sustava.

HNB je proteklih godina poduzimala i aktivnosti usmjerene na prevenciju incidenata te je u suradnji s Europskom središnjom bankom implementirala instancu MISP sustava. Od kraja 2018. i početka 2019. svim kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac omogućen je pristup toj platformi. MISP je platforma za pohranjivanje, povezivanje, korištenje i dijeljenje indikatora kompromitacije kibernetičkih napada, u zajednici pouzdanih sudionika. Pri tome instanca MISP sustava uspostavljena u HNB-u prvenstveno sadrži IoC-e kibernetičkih napada relevantnih za financijske institucije. MISP platforma funkcionirala je i u 2023. godini.

U 2023. godini NCERT je nastavio s aktivnostima podizanja svijesti cjelokupne populacije o važnosti kibernetičke sigurnosti objavljivanjem aktualnih novosti iz svijeta kibernetičke sigurnosti i IKT tehnologije te sigurnosnih preporuka. Tijekom 2023. nastavljena je suradnja sa FER-om u pogledu pisanja i izdavanja stručnih dokumenata (objavljena su dva stručna dokumenta iz područja kibernetičke sigurnosti). NCERT je sudjelovao na više konferencija te je tijekom godine obavio veći broj predavanja, radionica, prezentacija te webinara za obrazovni, akademski te poslovni sektor. Uz navedene djelatnosti, NCERT je u listopadu 2023. godini proveo niz aktivnosti vezanih uz Europski mjesec kibernetičke sigurnosti. NCERT je imao ulogu nacionalnog koordinatora za provedbu europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti. Na službenim stranicama zajedničke europske inicijative uređena je stranica posvećena hrvatskoj publici https://cybersecuritymonth.eu/countries/croatia.

Pod sloganom “Be smarter than a hacker!” ECSM se bavio temama socijalnog inženjeringa koji podrazumijeva manipulaciju žrtve kako bi se od nje ostvarila neka korist.

NCERT je aktivan i na društvenim mrežama: https://www.facebook.com/CERT.hr/

https://twitter.com/HRCERT

[23] 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

Tijekom 2023. NCERT je objavio ukupno 193 novosti na web sjedištu i društvenim mrežama.

Broj posjetitelja web sjedišta www.cert.hr je 185.536

Broj pratitelja Facebook stranice 2212

Broj pratitelja Twitter stranice 1485

U listopadu 2023. godine provedeno je četvrto CTF natjecanje Hacknite za srednje škole na kojem je sudjelovao ukupno 63 srednjoškolskih timova s 315 učenika iz 40 srednjih škola.

2022. godine pokrenuta je, a u 2023. godini nastavljena Hacknite CTF platforma https://platforma.hacknite.hr/ na kojoj se učenici, nakon registracije svojim @skole.hr računom, mogu pripremati za buduća Hacknite natjecanja. Platforma sadrži zadatke sa svih dosadašnjih natjecanja, a učenici mogu pratiti i svoj rank na tablici rezultata.

RH je po drugi put sudjelovala na European Cyber Security Challenge-u (ECSC) s nacionalnim timom sastavljenim od pet juniora i pet seniora.

U 2023. godini u sklopu IVLP Impact Awards programa (program financiran od strane Vlade SAD-a (U.S Department of State, Bureau od Educational and Cultural Affairs te koordiniran od strane Meridian International) proveden je projekt Cybersecurity Ninja kojim je educirano 384 učenika, nastavnika i roditelja iz područja zaštite djece na internetu. Izrađena je i tiskana brošura pod nazivom Cybersecurity Ninja https://www.cert.hr/wp-content/uploads/2023/10/Cybersecurity_Ninja.pdf koja donosi osnovne informacije o temama iz kibernetičke sigurnosti za djecu i roditelje poput: vrste zlonamjernog sadržaja, socijalni inženjering, prijetnje na društvenim mrežama, pravila kibernetičke sigurnosti, savjeti za dobru lozinku, digitalni trag, sigurnost školskog računala te vodič za roditelje i učitelje.

Javna prisutnost NCERT-a je u stalnom porastu – brojna gostovanja na televiziji, radiju, tiskanim i digitalnim medijima.

U 2023. godini nastavljene su aktivnosti podizanja svijesti o važnosti kibernetičke sigurnosti, koje se kao program provode od 2015. Tako se svake godine podiže svijest učenika i roditelja o temi sigurnosti na internetu, a edukativni materijali svima su na raspolaganju u elektroničkom obliku. Osim predavanja učenicima ili roditeljima po pozivu škola, svake godine osvježi se i revidira brošura „Vodič za siguran Internet i nepromišljene surfere - Kako se zaštititi u svijetu interneta i mobilnih telefona“. Osvježena brošura tiska se u 50.000 primjeraka i dostavlja u sve osnovne škole uoči svjetskog obilježavanja Dana sigurnijeg interneta (DSI) u veljači svake godine. Zadnja revizija brošure obavljena je krajem 2023. i objavljena je na internetskoj stranici HAKOM-a. Promocija najnovije brošure uslijedila je u sklopu DSI2024. Tijekom godine redovito su se dijelili savjeti ili upozorenja oko kibernetičke sigurnosti na društvenim mrežama.

ZSIS stalno analizira nove načine na koji bi se provele odgovarajuće kampanje o podizanju svijesti o značaju kibernetičke sigurnosti za državna tijela i pravne osobe s javnim ovlastima.

Osim rješenja za e-učenje razmatrane su i pokrenute suradnje s pojedinim učilištima poput HVU, Policijske akademije, PA te Diplomatske akademije u smislu držanja predavanja i osmišljavanja programa koji bi pokrili ovu temu.

ZSIS redovito širi svijest o važnosti kibernetičke sigurnosti na stručnim konferencijama, skupovima kao i objavama.

Veći broj fizičkih i pravnih osoba u RH oštećen je cryptolocker ransomwareima, zbog čega je MUP u suradnji s Europolom pokrenulo i redovito održava web mjesto https://www.nomoreransom.org/cro/index.html sa savjetima za građane i dostupnim alatima za dekripciju zaključanih datoteka.

Tijekom 2023. godine provodila se kampanja osvještavanja javnosti pod nazivom „Web heroj: Ulovimo lika s weba koji tvoje eure vreba“. Izrađena je internetska domena https://webheroj.hr/ koja sadrži savjete za građane i tvrtke i interaktivnu kartu RH o mogućnostima prijave kaznenih djela policiji.

Savjeti za građane redovito se objavljuju na Twitter računu MUP-a https://twitter.com/mup_rh i YouTube kanalu MUP-a https://www.youtube.com/channel/UCfEIxm5sLeVt6mCx02gUCqA

NCERT širu javnost redovito obavještava o računalno-sigurnosnim incidentima i ranjivostima putem web sjedišta www.cert.hr , Facebook stranice, Twitter računa te putem raznih mailing lista, televizijskih medija i novinskih članaka, Ovisno o incidentu daju se upute za postupanje i korisnike se poziva na dodatan oprez. U 2023. godini objavljeno je 11 upozorenja za širu javnost.

Državna odvjetništva na web stranici DORH-a objavljuju informacije o poduzetom kaznenom progonu za pojedina kaznena djela pa tako i kaznena djela vezana za računalni kriminalitet.

Hrvatska zaklada za znanost raspisuje godišnje natječaje za financiranje znanstvenih projekata, uključujući i projekte povezane s ovim područjem, s obzirom na to da projekti nisu specijalizirani za pojedina područja. Tijekom provedbe ovih projekata provedene su uobičajene redovne aktivnosti koje kao dio praćenja provedbe projekta provodi Hrvatska zaklada za znanost.

IV. ZAKLJUČAK

Strategija i Akcijski plan za njeno provođenje i nakon 9 godina od njihovog donošenja i dalje imaju snažan utjecaj na pristup kibernetičkoj sigurnosti u RH.

Postojeća Strategija je najvećim dijelom provedena i potrebno je izraditi novu, usklađenu sa zahtjevima novih zakonodavnih akata EU, NIS2 direktivom, DORA direktivnom, CRA uredbom, CSA+ uredbom te drugim aktima koji se izravno ili posredno oslanjaju na kibernetičku sigurnost. Osim EU zahtjeva koji su primarno usmjereni na zaštitu zajedničkog tržišta, potrebno je novom strategijom adresirati i pitanja koja su u isključivoj nadležnosti RH, kao što su pitanje nacionalne sigurnosti, kriznog upravljanja, razvoja sposobnosti i kapaciteta.

Novi Zakon o kibernetičkoj sigurnosti u to smislu već je pridijelio nove nadležnosti i odgovornosti koje će se razrađivati podzakonskim aktima. Ono što je nesporno je nužnost suradnje kako na međunarodnoj razini unutar saveza kojima RH pripada, tako i na nacionalnoj razini povezujući sposobnosti državnih tijela, akademske zajednice i gospodarstva. Kao što svi

dijelimo teritorij RH, tako svi dijelimo i isti kibernetički prostor i izloženi smo rizicima koji iz njega proizlaze. Alternativa razvoju novih usluga i sve većoj povezanosti putem kibernetičkog prostora ne postoji.