REPUBLIKA HRVATSKA

URED VIJEĆA ZA NACIONALNU SIGURNOST

NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2022. GODINI

Zagreb, lipanj 2023.

SADRŽAJ:

I. UVOD

Izvješće o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (u daljnjem tekstu: Akcijski plan) izrađeno je u okviru rada **Nacionalnog vijeća za kibernetičku sigurnost** (u daljnjem tekstu: Vijeće[1]) te je sadržajno usko povezano s aktivnostima Vijeća u 2022. godini prikazanim u Godišnjem izvješću o radu Vijeća i Koordinacije u 2022. godini[2].

Izvješće o provedbi Akcijskog plana u 2022. godini temelji se na ciljevima Nacionalne strategije kibernetičke sigurnosti[3] (u daljnjem tekstu: Strategija), čije je ostvarenje razrađeno kroz mjere pripadnog Akcijskog plana[4] („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

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

[2] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI%20o%20radu%20Vije%C4%87a%20i%20Koordinacije%20u%202022.pdf

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

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

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

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 Vijeće koje u tu svrhu provodi 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.

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, osim samog Vijeća, su:

1. Agencija za odgoj i obrazovanje (AZOO)
2. Agencija za strukovno obrazovanje i obrazovanje odraslih (ASOOO)
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)
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 predstavnik predsjedava Vijećem i koje osigurava 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 svibnja 2023. 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 te 1 s rokom provedbe od 12 mjeseci (od donošenja Strategije).

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, koje su operatori obvezni dostavljati na godišnjoj razini te analizira nalaze revizije njihovih informacijskih sustava.

U 2022. sigurnosne politike i reviziju informacijskih sustava dostavilo je 5 operatora, te je HAKOM proveo 2 inspekcijska nadzora u kojim su utvrđeni određeni nedostaci zbog kojih je inspektor propisao mjere za njihovo uklanjanje.

HAKOM je u 2022. 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.

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).

U 2022. godini nastavlja se **kontinuirana suradnja između relevantnih tijela iz područja kibernetičke sigurnosti**. Povećan je intenzitet komunikacije i suradnje zahvaljujući Vijeću i Koordinaciji. Sastanci navedenih tijela održavaju se na mjesečnoj razini, osim u slučaju potrebe za sazivanjem izvanredne sjednice. Osim toga, u sklopu projekta Grow2CERT, NCERT je u prvoj polovini 2022. godine organizirao i održavao sastanke radne skupine za razvoj, promociju i stalno poboljšanje Platforme za razmjenu informacija o incidentima i prijetnjama PiXi. Tijekom 2022. godine održano je pet sastanaka radne skupine i jedno završno događanje u lipnju povodom završetka projekta Grow2CERT. Članovi radne skupine su predstavnici nositelja provedbe mjera iz Akcijskog plana Nacionalne strategije kibernetičke sigurnosti, regulatornih agencija, nadležnih sektorskih tijela prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/18; dalje ZoKS), akademske zajednice i Hrvatske udruge banaka. Radna skupina se sastoji od predstavnika ukupno 13 institucija i organizacija. U 2022. nastavljena je edukacija korisnika iz pojedinih sektora ključnih usluga prema ZoKS-u. Edukaciju je prošao ukupno 221 korisnik iz entiteta uključenih u provedbu ZoKS-a (operatori ključnih usluga, davatelji digitalnih usluga, nadležna sektorska tijela, nadležni CSIRT-ovi) i telekomunikacijske tvrtke.

SOA je usklađivala standardne operativne procedure upravljanja kibernetičkim krizama na nacionalnoj razini i s EU CyCLONe organizacijom. U prosincu 2022. su započele i intenzivne pripreme za transpoziciju NIS2 direktive[5], koja je objavljena u prosincu 2022., i uvođenje novog modela upravljanja kibernetičkom sigurnošću u RH, čime će se postaviti nacionalni okvir za višu i centraliziranu razinu koordinacije različitih aktivnosti u području kibernetičke sigurnosti, a zakonski će se propisati i područja upravljanja u krizama.

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***

[5] DIREKTIVA (EU) 2022/2555 EUROPSKOG PARLAMENTA I VIJEĆA od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/ 2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148

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.)

(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 jedna, a tri 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 nije započela 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[6] 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[7]

Napravljena je **periodična procjena organizacijskih i tehničkih zahtjeva** za povezivanje na državnu informacijsku infrastrukturu, uvjeta i aktivnosti nužnih za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostale elemente neophodne 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 (Europsko nadzorno tijelo za bankarstvo) objavila u ožujku

[6] NN 92/14
[7] NN 60/17

2015. Na radionicama su sudjelovali predstavnici svih banaka koje posluju u RH, kao i predstavnici najznačajnijih institucija za elektronički novac.

U svibnju 2015. svim bankama upućen je dopis odnosno okružnica u vezi primjene *Smjernica o sigurnosti internetskih plaćanja* koje su objavljene i na internetskim stranicama HNB-a čija primjena je započela 1. kolovoza 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 2018. *Smjernice o sigurnosti internetskih plaćanja* zamijenile su *Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju Direktive (EU) 2015/2366 (Direktiva PSD2).*

Europsko nadzorno tijelo za bankarstvo (EBA) nije objavilo Smjernice o sigurnosti mobilnih plaćanja. EBA niti neće objaviti navedene smjernice s obzirom da su mobilna plaćanja (odnosno plaćanja koja se zadaju putem mobilnih telefonskih uređaja) obuhvaćena Direktivom o platnim uslugama (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 Direktive (EU) 2015/2366 (Direktiva PSD2)

Sukladno navedenom, mjera nije provedena niti će se provoditi, ali su ciljevi ostvareni provedbom alternativnih mjera.

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,
- o 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 i

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.

Temeljem čl. 20. ZoKS-a, Vlada RH donijela je Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[8]. Nastavno na navedenu regulativu, NCERT je objavio Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom koje određuju način dostave obavijesti i sadrže obrasce za obvezno obavještavanje o incidentima sa znatnim učinkom.

Zakon, uredba i navedene 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.

U rujnu 2021. HNB i banke identificirane kao operatori ključne usluge prema ZoKS-u, te ostale zainteresirane banke, sudjelovale su na radionici o korištenju PiXi platforme za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima.

Također, HNB se u 2021. pridružila radu međuresorne radne skupine za izradu standardnih operativnih procedura za upravljanje kibernetičkim krizama u RH. Cilj radne skupine je definiranje usklađenih procedura i tehničkih rješenja za sigurnu i jednostavnu razmjenu informacija pri upravljanju kibernetičkim krizama u pojedinom sektoru, odnosno na nacionalnoj razini.

U 2022. godini HNB u sklopu međuresorne radne skupine za upravljanje kibernetičkim krizama razmjenjuje kvartalna situacijska izvješća.

Smjernice o *sigurnosti internetskih plaćanja* su izrađene još 2015. g. te prezentirane širem krugu institucija bankarskog sektora, platnog prometa i najznačajnijih institucija odgovornih za elektronički novac. Smjernice definiraju vrste incidenata koje je potrebno prijavljivati HNB, kao i informacije koje je potrebno dostaviti.

2. veljače 2018. svim kreditnim institucijama upućen je dopis u vezi primjene Smjernica o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 koje su objavljene i na internetskim stranicama HNB-a, a čija primjena počinje od dana stupanja na snagu novog Zakona o platnom prometu[9] kojim se u zakonodavstvo RH prenosi Direktiva (EU) 2015/2366.

U 2018. organizirana je i radionica o sadržaju i primjeni Smjernica na kojoj su sudjelovale sve kreditne institucije, institucije za platni promet te institucije za elektronički novac u RH.

U 2019. i 2020. u više navrata je s kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac u RH komunicirano o obavezama tih institucija vezano uz izvješćivanje HNB-a o incidentima.

[8] NN 68/18
[9] NN 66/18

U lipnju 2021. Europsko nadzorno tijelo za bankarstvo (*engl. European Banking Authority – EBA*) objavilo je revidirane Smjernice o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 koje stupaju na snagu 1. siječnja 2022. godine. U srpnju 2021. HNB je održala radionicu o izmjenama sadržaja i primjeni revidiranih Smjernica, na kojoj su sudjelovale sve kreditne institucije, institucije za platni promet te institucije za elektronički novac u RH. U prosincu 2021. na internetskim stranicama HNB-a objavljene su Revidirane smjernice o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2 te obrasci za izvješćivanje čija primjena počinje od 1. siječnja 2022.

Od 1. siječnja 2022. godine na snagu su stupile Revidirane smjernice o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2 te je svim kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac u RH komunicirano o njihovim obvezama vezano uz izvješćivanje HNB-a o nastalim incidentima. Revidirane smjernice, između ostalog, definiraju nove kriterije za provedbu sigurnosti mrežnih ili informacijskih sustava te je uvedena detaljnija kategorizacija temeljnog uzroka nastalog incidenta.

(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. ZoKS u tom smislu je najdetaljnije uređivao odnose i obveze državnih tijela i pravnih osoba u uspostavljanju otpornosti informacijskih sustava. U tijeku je proces transpozicije NIS2 direktive, koja uvodi nove sektore i nove obveze iz domene kibernetičke sigurnosti. Uspostavit će se i horizontalna poveznica i na CER direktivu[10] te usklađeno riješiti 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.

[10] 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

U skladu sa Zakonom o kritičnim infrastrukturama (NN 56/13) Ministarstvo unutarnjih poslova, Ravnateljstvo civilne zaštite kao tijelo državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja, koordiniralo je postupak **identifikacije nacionalnih kritičnih** infrastruktura (KI). Kritične infrastrukture u RH se identificiraju temeljem Zakona o kritičnim infrastrukturama i „Odluke o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura“ (NN 108/2013), gdje je sektor „Komunikacijska i informacijska tehnologija“ (sa podsektorima: elektroničke komunikacije, prijenos podataka, informacijski sustavi te pružanje audio i audio-vizualnih medijskih usluga) naveden kao jedan od jedanaest sektora za određivanje KI. Nadležna sektorska tijela su postupak identifikacije provodila kroz primjenu kriterija za identifikaciju KI (propisani „Pravilnikom o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura“ (NN 47/2016)) 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 i koji uključuje i komunikacijsko – informacijsku infrastrukturu. Nakon što Odlukom Vlada potvrdi predloženu nacionalnu KI, odrediti će se posebne mjere zaštite i jačanja otpornosti za takve infrastrukture koje će operatori biti obvezani primjenjivati.

Obvezujuće sigurnosne mjere i upravljanje rizicima koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture su definirane Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. ZoKS-om je predviđen i nadzorni mehanizam. ZoKS-om su dodijeljene potrebne nadležnosti za njegovo provođenje te je uveden poseban institut „ocjene sukladnosti“, za koji su ZoKS-om zadužena nacionalna tehnička tijela s najviše stručnih znanja i iskustava u tim pitanjima[11], sve u cilju olakšavanja provedbe obveza iz Zakona i prateće Uredbe njihovim obveznicima i nadležnim sektorskim tijelima koji su dužni provoditi nadzor nad primjenom Zakona i Uredbe. Za sektore u kojima postoji regulirani sektorski mehanizam revizije poslovanja operatora ostavljena je mogućnost koordiniranog proširenja postojećeg opsega revizije poslovanja na način koji će uključiti spomenutu ocjenu sukladnosti prema zahtjevima ZoKS-a.

ZoKS-om te pripadnom Uredbom utvrđena je obveza izvješćivanja o sigurnosnim incidentima, kriteriji za utvrđivanje učinka incidenta, sadržaj obavijesti i način dostave te informiranje javnosti. Sukladno tome, uspostavljena je **platforma za razmjenu informacija** bitnih za ostvarenje zajedničkog cilja svih uključenih dionika – uspostava visoke razine sigurnosti komunikacijskih (mrežnih) i informacijskih sustava ključnih za društvene i gospodarske aktivnosti - čime se smatra da se ova mjera provodi u potpunosti.

Na prijedlog SOA-e, Vijeće i Koordinacija za sustav domovinske sigurnosti su se 2020. godine usuglasile o potrebi uspostave novog nacionalnog pristupa **upravljanju kibernetičkim krizama**, za koji je SOA određena kao koordinator. Daljnju obavezu oko predmetnog područja i izrade standardnih procedura za nacionalno upravljanje kibernetičkim krizama je preuzela SOA koja je u tu svrhu osnovala međuresornu radnu skupinu za upravljanje kibernetičkim

[11] Zavod za sigurnost informacijskih sustava i Nacionalni CERT - ujedno i CSIRT tijela iz Zakona.

krizama. SOA je također razradila nacionalni koncept upravljanja kibernetičkim krizama te ga uskladila s aktualnim pristupom EU-a i NATO-a. Na temelju prijedloga Vijeća, SOA je određena nadležnim tijelom koje predstavlja RH u području upravljanja kibernetičkim krizama te je od proljeća 2020. godine uključena u rad EU CyCLONe-a, organizacije za upravljanje kibernetičkim krizama na EU razini.

Nacionalni SOP razradio je kriterije, pojmove i taksonomije opisa te načine rada nadležnih tijela pri čemu je obuhvaćen cjeloživotni ciklus upravljanja kibernetičkim krizama (redoviti, upozoravajući i krizni način rada), kao i potrebne procedure i kriteriji za eskalaciju načina rada te drugi elementi.

(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 2022. 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 2022. godini redovno sudjelovali u radu Odbora Vijeća Europe za praćenje primjene Konvencije o kibernetičkom kriminalitetu (T-CY Odbor)..

Vijeće EU-a 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.

Nakon usvajanja Općeg pristupa u odnosu na Prijedlog uredbe Europskog parlamenta i Vijeća o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u

kaznenim stvarima u prosincu 2018. na Vijeću ministara JHA i Općeg pristupa u odnosu na Prijedlog direktive o utvrđivanju usklađenih pravila za imenovanje pravnih zastupnika za potrebe prikupljanja dokaza u kaznenim postupcima u ožujku 2019., Europski parlament (LIBE Odbor) je u prosincu 2020. usvojio Izvješća u odnosu na Prijedloge gore navedene uredbe i direktive, čime su ispunjeni svi preduvjeti za pokretanje postupka trijaloga u dosjeu unutarnjeg zakonodavnog paketa e-dokaza. Trijalog s Europskim parlamentom vezano uz spomenuti paket traje od početka 2021. godine. Predstavnici MPU sudjeluju na svim sastancima radne skupine COPEN na temu unutarnjeg zakonodavnog paketa e-dokaza, te podržavaju inicijative i korake koji mogu dovesti do bržeg usvajanja kompromisnog rješenja.

COREPER II je početkom 2023. godine odobrio konačni kompromisni tekst paketa o e-dokazima (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, intenzivirat će se 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 je donijelo 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.

Služba kibernetičke sigurnosti (ustrojena unutar Kriminalističko-obavještajnog sektora, Uprave kriminalističke policije, kontakt kroz cyber.crime@mup.hr) prijavljena je kao kontakt točka prema Europskoj komisiji, organizaciji G 7 (koju čine sedam najrazvijenijih zemalja svijeta) i Interpolu. 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.

Tijekom 2022. godine Ministarstvo unutarnjih poslova redovno šalje zahtjeve prema drugim državama te prima zahtjeve drugih država, te nema poteškoća u provedbi.

NCERT ostvaruje međunarodnu suradnju 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 direktive o mrežnoj i informacijskoj sigurnosti (NIS direktiva).

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 kampanje (Advanced Persistent Threat – napredna ustrajna prijetnja). Međunarodna razmjena u području kibernetičke sigurnosti posebno se razvija u segmentima razmjene indikatora kompromitacije (Indicators of Compromise – IoC) i taktika, tehnika i procedura kibernetičkih napada (Tactics, technics and procedures – TTP).

U DORH je, u okviru međunarodne pravne pomoći i pravosudne suradnje vezano za kibernetički kriminalitet kao kontakt točka za mrežu "Cybercrime Eurojust", određen zamjenik ravnateljice Ureda za suzbijanje korupcije i organiziranog kriminala.

Stalna kontakt točka u Odsjeku za međunarodnu pravnu pomoć i suradnju Ureda Glavnog državnog odvjetnika RH je zamjenica općinskog državnog odvjetnika u Općinskom državnom odvjetništvu u Zagrebu, koja u predmetima kibernetičkog kriminaliteta kao nacionalni predstavnik RH u Europskoj pravosudnoj mreži žurno prosljeđuje zamolbe za međunarodnu pravnu pomoć i suradnju prema zemljama članicama EU i drugim zemljama u svrhu brze razmjene informacija.

MUP je tijekom 2021. godine ostvarivao suradnju na konkretnim slučajevima istraživanja kibernetičkog kriminaliteta sa ZSIS-om i Nacionalnim CERT-om. MUP i NCERT potpisali su sporazum o suradnji, te se navedeni sporazum uspješno provodi. Suradnja sa Zavodom za sigurnost informacijskih sustava 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. NCERT sudjeluje u sastancima Operativno-tehničke koordinacije kibernetičke sigurnosti koji se održavaju na mjesečnoj razini.

SOA je kroz sudjelovanje u radu Vijeća i Koordinacije te suradnju 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, APT 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) nakon izrade i usuglašavanja Nacionalnih standardnih operativnih procedura za upravljanje kibernetičkim krizama započela rad međuresorne radne skupine u redovitom stanju te održavanje periodičkih kvartalnih sastanaka i poticanje kibernetičke operativne suradnje na nacionalnoj razini u skladu sa zahtjevima EU-a.

Sukladno Uredbi o izmjenama i dopunama uredbe o unutarnjem ustrojstvu MUP-a (NN 97/2020.) 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 Ministarstva, 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 2019. godine ustrojena su radna mjesta policijskih službenika za kibernetičku sigurnost i digitalnu forenziku na nacionalnoj razini i na razini svih 20 policijskih uprava u RH.
U tijeku je dovršetak provedba projekta, koji se u iznosu od 90% financira sredstvima EU: „Jačanje kapaciteta MUP-a u borbi protiv svih oblika kibernetičkog kriminaliteta; Fond za unutarnju sigurnost – Instrument za financijsku potporu u području policijske suradnje, sprečavanja i suzbijanja kriminaliteta i upravljanje krizama“
Cilj projekta: Povećanje kibernetičke sigurnosti na području RH i EU razvijanjem i unapređivanjem sustava prikupljanja, korištenja i analize digitalnih dokaza, edukacijama za policijske službenike o metodama istraživanja kaznenih djela protiv računalnih sustava, programa i podataka.
Ukupni predviđeni proračun je 995.000,00 EUR s PDV-om, a postotak EU sufinanciranja iznosi 90%.
Projekt se sastoji od 2 komponente:

- Opremanje ustrojstvenih jedinica MUP-a potrebnim softverskim i hardverskim komponentama. U sklopu projekta nabavit će se potrebna oprema i računalni programi koji će omogućiti efikasno izvršavanje naloga sudova za pretragom nositelja elektroničkih dokaza poput računala, tableta, tvrdih diskova i mobilnih telefona. Pretrage će se obavljati na način tako što će se putem specijaliziranog forenzičkog softvera i hardvera izraditi forenzičke kopije sadržaja memorije predmeta koji se pretražuju, navedene kopije pohranit će se na poslužiteljima, nakon čega će se obavljati analiza sadržaja. Projektom se planira financirati nabava svih postojećih licenci za forenzičke softvere, koje su do sada svake godine financirane proračunskim sredstvima MUP-a, te nabava licenci, koje MUP do sada nije posjedovao, a neophodne su obavljanje poslova digitalne forenzike.
- Provođenje edukacijskih modula na temu digitalnih dokaza i forenzičkih metoda i procedura za 31 policijskog službenika.

SOA kontinuirano brine o jačanju ljudskih potencijala te razvoju i nadogradnji alata i sustava za kibernetičku zaštitu. U tom cilju SOA, u suradnji sa ZSIS-om, provodi projekt SK@UT koji obuhvaća 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 2022. godine na sektora ključnih usluga i pravne osobe od posebnog interesa za RH, daje se 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, SOA je uspostavila Centar za kibernetičku sigurnost te je preuzela koordinaciju nacionalnog procesa transpozicije EU NIS2 direktive, kao i nacionalnu koordinaciju EU horizontalne skupine za suradnju u kibernetičkim pitanjima. U cilju daljnjeg unaprjeđenja sigurnosnog stanja nacionalnog kibernetičkog prostora, tijekom 2022. godine proširen je način organizacije SOA-inog Centra za kibernetičku sigurnost, u kojem sada djeluje združeni

kibernetički tim SOA-e, Zavoda za sigurnost informacijskih sustava (ZSIS), i Vojne sigurnosno-obavještajne agencije (VSOA).

Predstavnici Službe kibernetičke sigurnosti Ministarstva unutarnjih poslova 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**[12], 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

[12] NN 30/18

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.

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 ZoKS-a 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 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.

Zavod za sigurnost informacijskih sustava i Hrvatska akademska i istraživačka mreža - 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 se trenutno sastoji od 13 institucija i organizacija: FER, HAKOM, HANFA, HNB, HUB, MINGOR, MORH, MUP, NCERT, SDURDD, MIZ, MMPI i ZSIS. Radna skupina je aktivna od 2017. godine do danas te je izradila je i objavila Nacionalnu taksonomiju računalno-sigurnosnih incidenata koja je u ožujku 2019. godine bila i ažurirana zbog pojave novih vrsta incidenata i zbog zahtjeva iz ZoKS-a. Najnovija inačica Nacionalne taksonomije u primjeni je od 1. siječnja 2022., izmjene i dopune napravljene su zbog pojave novih vrsta računalno-sigurnosnih incidenata koje se nisu mogle svrstati u postojeću inačicu taksonomije, a dostupna je na sljedećoj poveznici: https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf

Radna skupina sudjelovala je u daljnjem razvoju, promociji i uključivanju korisnika (predstavnika operatora ključnih usluga i davatelja digitalnih usluga) u korisničku edukaciju za korištenje PiXi platforme. Na PiXi platformi je aktivirano ukupno 235 korisničkih računa. Prema rječniku Nacionalne taksonomije klasificirane su vrste incidenata i prijetnji na Platformi PiXi.

Sektorski nadležna tijela prikupljaju podatke o incidentima te se može smatrati da se mjera primjenjuje u potpunosti. NCERT statistički vodi evidenciju o sektorskim incidentima za tri sektora: bankarstvo, davatelje Internet usluga i sektorske incidente koji su prijavljeni sukladno ZoKS-u. 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 vezanim 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 prijavit prema:

- Revidiranim smjernicama o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 (PSD2);
- ZoKS-u; ili
- Odluci o primjerenom upravljanju informacijskim sustavom[13].

NCERT od kreditnih institucija koje su obveznici primjene ZoKS-a informacije o incidentima zaprima sukladno Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom 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).

HNB objedinjuje podatke o svim značajnim incidentima i razmjenjuje anonimizirane podatke o prikupljanim incidentima s institucijama koje sudjeluju u radu Koordinacije.

HNB je proteklih godina poduzimala i aktivnosti usmjerene ne prevenciju incidenata te je u suradnji s Europskom središnjom bankom (ESB) 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 slanjem kvartalnih situacijskih izvješća razmjenjuje anonimizirane podatke o prikupljenim incidentima s institucijama koje sudjeluju u radu Međuresorne radne skupine za upravljanje kibernetičkim krizama.

U 2021. godini se izmijenio Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga te su time operatori obvezni prijavljivati računalne incidente putem PiXi platforme. Na sastancima Koordinacije izvještava se o incidentima iz prethodnog razdoblja, te Koordinacije obavještava Vijeće. Osim toga, NCERT šalje mjesečni izvještaj o sigurnosnim incidentima zainteresiranim tijelima. Izvještavanje zainteresiranih dionika NCERT provodi i kroz unos statističkih podataka o obrađenim incidentima kroz PiXi platformu.

[13] NN 37/10

NCERT je kao nositelj mjere u 2022. godini izdao 11 upozorenja putem web sjedišta www.cert.hr, Facebook stranice CERT.hr i Twitter računa HRCERT. Na usluzi CERT Epsilon koja korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava u 2022. godini bile su aktivne 162 pretplate, a ukupan broj posjeta stranici 3241. 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/

HNB je kao sunositelj navedene mjere u 2022. godini izdala 10 objava svim kreditnim institucijama o uočenim sigurnosnim prijetnjama i ranjivostima te preporuke za daljnje postupanje. Osim obavijesti o otkrivenim sigurnosnim prijetnjama i ranjivostima HNB je zadnjem kvartalu 2022. godine svim financijskim institucijama dostavila i "Preporuke za prilagodbu IT sustava KI za pripremu konverzije" koje su sadržavale preporuke vezane uz pripreme za konverziju, kontigencijske planove te održavanje primjerene razine sigurnosti.

ZSIS je kao sunositelj mjere tijekom 2022. godine obavljao redovne aktivnosti u sklopu svoje nadležnosti.

HAKOM je kao sunositelj mjere izdao u 2022. godini 23 upozorenja/preporuka putem društvenih mreža od kojih su minimalno 2 podijeljena s CERT.hr Facebook stranice i dvije objave koje su vodile na CERT.hr internetske stranice.

Policijski službenici Službe kibernetičke sigurnosti MUP-a su tijekom 2022. 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 Koordinacije 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 kampanija te drugih kibernetičkih ugroza, tijekom 2022. otvorila je mogućnost puno dublje suradnje u okviru preko 60 institucija koje su pristupile sustavu SK@UT, a uključujući državna tijela i operatore ključne infrastrukture, kao i pravne osobe od posebnog interesa za RH. Dodatna razmjena iskustva i znanja intenzivno se provodila tijekom 2022. godine kroz rad Međuresorne radne skupine za upravljanje kibernetičkim krizama, a u kojoj sudjeluju predstavnici 7 institucija koje koordinira SOA. Zaključkom Vlade RH iz rujna 2022. godine SOA je određena za nacionalnog stručnog nositelja Horizontalne radne skupine za kibernetička pitanja na kojoj se raspravlja niz pitanja od interesa za tijela kaznenog progona i sigurnosno-obavještajni sustav.

(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 Vijeća 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 elektroničkom) komunikacijom unutar samog Vijeća. Trend rasta broja relevantnih međunarodnih aktivnosti se nastavlja, a u kontekstu smiraja globalne pandemije COVID-19 pojačala se i dinamika fizičkih sastanaka. MVEP je redovno distribuirao informacije o međunarodnim kibernetičkim aktivnostima uključujući distribuciju dokumenata i informacija putem zajedničke email adrese Vijeća, s ciljem rasprave i donošenja potrebnih odluka Vijeća. Krajem godine uspostavljena je komunikacija sa Republikom Slovenijom i dogovorene široke bilateralne konzultacije tijekom 2023. godine.

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. Tijekom 2022. godine naglasak s općih političkih i organizacijskih aspekata pripreme rada *Ad hoc* odbora postupno je prešao u supstantivnu raspravu i razradu prijedloga.

Nastavljeni su sastanci tzv. EU mreže kibernetičkih veleposlanika. Sve češće bilježe se i veći koordinativni sastanci koji uključuju i novu dimenziju tzv. mreže digitalnih veleposlanika.

Vezano za ključne globalne aktivnosti, RH je svoj doprinos pružala kroz zajedničke napore EU, dakle ponajprije putem SPRH pri EU u formatu Horizontalne radne skupine za kibernetička pitanja (HRS CYBER). HRS je pripremala i stajališta EU-a za UN procese u sklopu Prvog (OEWG) i Trećeg odbora (AHC).

Također, kroz HRS nastavljen je rad i u kontekstu provedbe odnosno unaprjeđenja EU kibernetičkog okvira, uključujući i sankcijskog režima. 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 2022. godine RH je nastavila sudjelovati (uglavnom putem MVEP-a) 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). Uočene poteškoće u provedbi i dalje su bile uzrokovane vanjskim čimbenicima (načinu organizacije kao i konačnoj strukturi OESS CBM vježbi te uslijed rezultata drugih članica OESS-a) na koje RH nije mogla utjecati.

U organizaciji OSRH pravovremeno su provedene planske konferencije i druge pripremne aktivnosti za potrebe NATO „*Cyber Coalition* 2022“ vježbe, uključujući i suradnja s drugim tijelima te stručnjacima iz sfere akademske zajednice i privatnog sektora. Vježba je obuhvaćala obranu od zlonamjernog sadržaja, hibridne izazove, testiranje operativnih i pravnih procedura. CARNET je imao ulogu IPoC-a (Industrial Point of Contact) čime je koordinirao sudjelovanje privatnog sektora i akademske zajednice. Zamjetan je nastavak jačanja nacionalnih sposobnosti, ne samo u tehničkom, već i u dijelu vježbe o pravnim aspektima kibernetičkog djelovanja. Dok se u pojedinim aspektima može zaključiti da RH ispunjava svoje međunarodne obveze, a ponegdje i nadilazi očekivanja (suradnja sa SAD-om), ostaje prostor za napredak posebice u smislu realizacije nacionalne vježbe iz područja kibernetičke sigurnosti na visokoj i tehničkoj razini. Nacionalni CERT je u lipnju 2022. godine sudjelovao u vježbi „*Cyber Europe“* u organizaciji ENISA-e. Cilj vježbe bio je poboljšanje suradnje i komunikacije između CSIRT-ova EU te jačanje nacionalne suradnje sa zdravstvenim sektorom.

Aktivnosti usmjerene na jačanje suradnje u području ***upravljanja rizicima europskih kritičnih infrastruktura*** su se provodile u okviru ZoKS-a.

(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.

Vezano uz mjere uvrštavanja predmetnih i međupredmetnih sadržaja vezanih uz kibernetičku sigurnost u osnovnoškolske i srednjoškolske programe donesene su Odluka o donošenju kurikuluma za nastavni predmet Informatike za osnovne škole i gimnazije u RH (22/2018) i Odluka o donošenju kurikuluma za međupredmetnu temu Uporaba informacijske i komunikacijske tehnologije za osnovne i srednje škole u RH (7/2019).

Temeljem Nacionalnog programa otpornosti i oporavka, u sklopu projekta e-Sveučilišta kojim se provodi modernizacija visokog obrazovanja, dogovorene su aktivnosti vezane uz kibernetičku sigurnost. Studente će se upoznati sa sadržajima vezanima uz kibernetičku sigurnost u sklopu edukacija čiji je cilj podizanje svijesti o kibernetičkoj sigurnosti, prevenciji kibernetičkih prijetnji i napada te povećanje interesa studenata za karijeru u području kibernetičke sigurnosti.

Sveučilišta, visoka učilišta i njihova tijela samostalno odlučuju o uspostavljanju i izvođenju diplomskih, doktorskih i specijalističkih studijskih programa, u skladu sa zakonom te ih se Strategijom ne može obvezati na uključivanje određenih sadržaja osim što se kod donošenja novih te izmjena i dopuna postojećih studijskih programa od visokih učilišta očekuje da programi obuhvaćaju ishode učenja koji su usklađeni s potrebama tržišta rada i aktualnim dostignućima u području u kojem se izvode.

ASOO je u sklopu ESF projekta Modernizacija sustava stručnog usavršavanja nastavnika strukovnih predmeta nakon revizije donesenog Koncepta novog modela stručnog usavršavanja nastavnika strukovnih predmeta, objavila njegovu revidiranu verzija Novi model stručnog usavršavanja nastavnika strukovnih predmeta te su donesene i Preporuke za osiguravanje kvalitete novog koncepta i provedbe otvorenog programa. Prema novom konceptu stručno usavršavanje nastavnika provodi se kroz temeljne i izborne module. Unutar donesenog koncepta razvijen je i modul MI12 (S3) Kibernetička sigurnost.

Cilj 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.

Modul uključuje: Uvod u sigurnost, upravljanje pristupom i sigurnost razvoja softvera; Planiranje kontinuiteta poslovanja i oporavka od katastrofe; Upravljanje informacijskom sigurnošću i upravljanje rizikom; Pravne propise i usklađenost; Kriptografiju; Sigurnosnu arhitekturu i dizajn; Telekomunikacije i sigurnost mreže.

Nakon uspješno završenog modula polaznik može:

- Raspraviti o ključnim konceptima kibernetičke sigurnosti i načelu njihova rada
- Nabrojiti korake za izradu sustava upravljanja pristupom
- Opisati životni ciklus razvoja softvera
- Razlikovati uloge i odgovornosti povezane s kibernetičkom sigurnosti
- Opisati razlike između oporavka od katastrofe i kontinuiteta poslovanja nakon katastrofe
- Opisati najbolje prakse koje olakšavaju implementaciju oporavka od katastrofe
- Objasniti osnove kriptografije te suvremene tehnike enkripcije podataka
- Analizirati hardver, softver, komponente mreže i njihove međusobne odnose s ciljem postizanja sigurnosti sustava
- Opisati različite sigurnosne modele te rješenja za umrežavanje i otklanjanje sigurnosnih problema

Dodatnu podršku u provedbi ove mjere ASOO pružaju i srednje strukovne škole na području cijele RH koje na školskoj razini provode stručna usavršavanja za nastavno i nenastavno osoblje na teme vezane uz kibernetičku sigurnost. Cilj ovih edukacija je razvoj kompetencija sigurnog korištenja interneta kod nastavnog i nenastavnog osoblja a time i kod učenika.

Uvidom u službenu evidenciju o studijskim programima u RH koja se vodi sukladno Zakonu o visokom obrazovanju i znanstvenoj djelatnosti (Narodne novine, broj: 119/22) utvrđeno je da su u 2022. godini u Upisnik studijskih programa upisana 2 nova studijska programa u području Tehničkih znanosti, polje Računarstvo:

- sveučilišni diplomski studij *Primijenjeno/poslovno računarstvo* na engleskom jeziku i na hrvatskom jeziku Sveučilište u Dubrovniku *(33 studenta)*
- izmjene i dopune sveučilišnog diplomskog studija *Elektrotehnika (159 studenta) uvođenje nova tri smjera: Elektroenergetika (2studenta), Automatizacija industrijskih sustava (nema podataka) i Informacijske i komunikacijske tehnologije (4 studenta)*

U dijelu poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja raspisivan je natječaj za dodjelu bespovratnih sredstava projektima udruga u području izvaninstitucionalnoga odgoja i obrazovanja djece i mladih.

Financirano je ukupno 11 projekata prijavljenih na natječaj MZO-a za dodjelu bespovratnih sredstava u području izvaninstitucionalnog odgoja i obrazovanja.

U sklopu ESF projekta Promocija učeničkih kompetencija i strukovnog obrazovanja kroz strukovna natjecanja i smotre održano je državno natjecanje (*WorldSkills Croatia*) u sljedećim disciplinama a koje uključuju elemente kibernetičke sigurnosti :

1. Administracije IT sustava
2. Izrada programskih rješenja
3. Robotika

Disciplina Administracija IT sustava uključuje pružanje širokog spektra usluga, uključujući korisničku podršku, dizajn, rješavanje problema te instaliranje, konfiguriranje i ažuriranje operativnih sustava i mrežnih uređaja. Bez IT sustava bismo teško mogli zamisliti sadašnjost, a posebno je važan za budućnost i razvoj koji nam ona donosi.

Disciplina je povezana sa sljedećim nastavnim planovima i programima ili strukovnim kurikulumima:

- Programer/programerka računalnih primjena
- Administrator/administratorica područne računalne mreže (LAN)
- Računalni tehničar/računalna tehničarka
- Tehničari/tehničarke za razvoj računalnih mreža i sustava
- Tehničar/tehničarka za telekomunikacije
- Tehničar/tehničarka za računalstvo
- Elektrotehničar/Elektrotehničarka
- Tehničar/tehničarka za elektroniku
- Tehničar/tehničarka za mehatroniku

Zanimanje tehničar za računalstvo obuhvaća praktična znanja i vještine potrebne za obavljanje poslova iz područja ljudskih djelatnosti povezanih s projektiranjem, izradbom i održavanjem manje složenih baza podataka i računalnih programa, nadziranjem i dijagnosticiranjem te evidentiranjem i otklanjanjem sklopovskih i programskih problema, educiranjem i pomaganjem korisnicima u rješavanju njihovih problema, konfiguriranjem i održavanjem računala, lokalne računalne mreže, računalnih i informacijskih sustava. Središnja i integrirajuća kompetencija ovog zanimanja objedinjuje poslove: rada na računalu, pripreme i obrade podataka, kontrole pripreme i obrade podataka, jednostavnijeg oblikovanja baza podataka, jednostavnije zadatke unutar administracije baza podataka, sudjelovanja u dijelu projektiranja informacijskih sustava, operatera na vanjskoj računalnoj opremi, sistemskog tehničara, uključujući administraciju operacijskih sustava i računalnih mreža, kontrole kvalitete i učinkovitosti rada, komunikacije s krajnjim korisnicima, edukacije krajnjih korisnika, komunikacije i suradnje u timu i na projektnim zadatcima, poduzetništva, marketinga i prodaje u području IKT-a i druge srodne poslove.

Izrada programskih rješenja obuhvaća praktična znanja i vještine koja se stječu kroz obrazovanje za zanimanje tehničar za računalstvo: obavljanje poslova iz područja ljudskih djelatnosti povezanih s projektiranjem, izradom i održavanjem manje složenih relacijskih baza podataka i računalnih programa namijenjenih za web i/ili mobilne platforme; nadziranjem i dijagnosticiranjem te evidentiranjem i otklanjanjem hardverskih i softverskih problema; educiranjem i pomaganjem korisnicima u rješavanju njihovih problema; pripremanju razvojne, tehnološke i operativne dokumentacije proizvodnje.

Disciplina je povezana sa nastavnim planovima i programima ili strukovnim kurikulumima za tehničara za računalstvo. Rade se poslovi na pripremanju razvojne, tehnološke i operativne dokumentacije proizvodnje, ispitivanju elektroničkih komponenti i sklopova, montiranju i ispitivanju elektroničkih uređaja i opreme, njihovu posluživanju i održavanju, tehničko-administrativni poslovi, obavljanje poslova sudjelovanja u projektiranju, pripremi i vođenju proizvodnje te operativnom vođenju i održavanju telekomunikacijskih sustava i mreža.

Robotika je brzo razvijajuća industrija, orijentirana na ishođenje rješenja. Roboti igraju sve veću ulogu u našim životima i radnim mjestima u svim područjima, a pogotovo u proizvodnji, poljoprivredi, zrakoplovstvu, rudarstvu i medicini.

Obuhvaća rad u uredima, proizvodnim pogonima ili laboratorijima; dizajn, održavanje, razvijanje novih aplikacija i provođenje istraživanja.

Stvaranje robota počinje dizajnom, a zatim prototipom koji mora biti programiran i testiran.

Stručnjak u ovom području mora biti upoznat s logikom, mikroprocesorima i računalnim programiranjem te pripremiti specifikacije za sposobnosti robota koje se odnose na određenu radnu okolinu.

Disciplina je povezana sa sljedećim nastavnim planovima i programima ili strukovnim kurikulumima:

- EiR:
- Tehničar za elektroniku NPP
- Tehničar za računalstvo NPP
- Tehničar za mehatroniku NPP
- Elektrotehničar
- SBM:
- Strojarski tehničar
- Strojarski računalni tehničar
- Računalni tehničar za strojarstvo
- Tehničar za energetiku
- Tehničar za mehatroniku
- Tehničar za finomehaniku
- Tehničar za obrađivačke tehnike
- Tehničar za strojeve i uređaje
- Brodograđevni tehničar
- Tehnički crtač

Obuhvaća rad u uredima, proizvodnim pogonima ili laboratorijima; dizajn, održavanje, razvijanje novih aplikacija i provođenje istraživanja. Stvaranje robota počinje dizajnom, a zatim prototipom koji mora biti programiran i testiran. Stručnjak u ovom području mora biti upoznat s logikom, mikroprocesorima i računalnim programiranjem te pripremiti specifikacije za sposobnosti robota koje se odnose na određenu radnu okolinu.

Nastavilo se s provedbom mjere sustavne izobrazbe državnih službenika. Jedan dio izobrazbe je već obuhvaćen državnim ispitom u posebnom dijelu stručnog ispita i to ne u cijelosti već samo postupanje s klasificiranim podacima.

Sustavna izobrazba državnih službenika provodi se i prilikom imenovanja savjetnika za informacijsku sigurnost u državnim tijelima. UVNS u suradnji s Državnom školom za javnu

upravu kontinuirano provodi edukaciju državnih službenika iz područja informacijske sigurnosti te je tako u 2022. proveo 8 edukacija.

U MUP-u su tijekom 2022. godine, u organizaciji PA i Uprave kriminalističke policije održana slijedeća stručna usavršavanja:

- jedan modul treninga „Napredne forenzičke metode i postupci“ u trajanju od 3 dana,
- 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.
- jedan modul 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
- 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 od kolovoza 2019. do kraja 2022. godine provodila projekt „Unaprjeđenje programa edukacija u borbi protiv kibernetičkog kriminala”. Cilj projekta bio je unaprijediti kapacitet i funkcioniranje pravosuđa za borbu protiv kibernetičkog kriminala te ojačati kapacitete pravosudnih dužnosnika i službenika za utvrđivanje i procesuiranje kaznenih djela povezanih s kibernetičkim kriminalom.

U 2022. godini održana su tri specijalistička seminara na teme „Zabranjeni sadržaji“, „Zlouporaba računalnih sustava“ i „Napadi na računalne sustave“. Ukupno je sudjelovalo 67 polaznika.

Provedena su i dva e-tečaja na teme „Kibernetički kriminal – osnovni modul“ i „Kibernetički kriminal – napredni modul“. Ukupno je sudjelovalo 60 polaznika.

Ciljnu skupinu u ovim aktivnostima su činili suci, državni odvjetnici, savjetnici u pravosudnim tijelima i službenici u pravosuđu, kao i vježbenici.

U okviru projekta organiziran je i studijski posjet EUROPOL-u, EUROJUST-u i pravosudnim tijelima u Nizozemskoj. U posjetu su sudjelovali voditelji educirani kroz projekt, članovi radne skupine zaduženi za izradu obrazovnih materijala u ovom projektu te predstavnici PA. U 2022. je u okviru ovog projekta izrađena i testirana nova Moodle platforma PA za e-učenje koja će omogućiti i digitalizaciju dijela poslovnih procesa PA.

U okviru međunarodne suradnje PA hrvatski pravosudni dužnosnici sudjelovali su na sljedećim seminarima u organizaciji Europske mreže za pravosudno osposobljavanje (EJTN):

- Seminar „Razumijevanje bitcoina i tehnologija kriptovaluta“, 1 polaznik,

- Seminar „Novi izazovi u kibernetičkom prostoru“, 2 polaznika.

U suradnji s Veleposlanstvom Sjedinjenih Američkih Država u RH je organiziran mrežni seminar “Kibernetički kriminal i digitalni dokazi” za 32 polaznika iz RH te napredna obuka o digitalnim dokazima na kojoj je sudjelovala jedna sutkinja iz RH.

U suradnji s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu raspisana su potrebna predznanja za rad u CERT timovima po slijedećim ulogama:

- upravljanje incidentima,
- osnovna forenzika,
- napredna forenzika,
- penetracijsko testiranje,
- analiza koda i
- voditelj.

Napravljena je matrica stručnih certifikata s kojima se stječu stručna znanja za pojedinu ulogu u CERT timovima.

ZSIS svake godine donosi plan školovanja u kojemu su na godišnjoj razini definirane potrebne izobrazbe i načine stjecanja tih znanja.

MORH je definirao potrebne izobrazbe i načini stjecanja znanja za svoje zaposlenike i ustrojstvene cjeline pod nadležnošću i u potpori CERT-a MORH-a i OS 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).

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 2022. godini osam djelatnika odslušalo je edukaciju odnosno pripremu za certifikat Certified Ethical Hacker – CEH. Troje djelatnika je certificirano ISO27001 Lead Auditor certifikatom. Osim toga, pohađane su edukacije za javne nastupe i kriznu komunikaciju, CSIRT sposobnosti, tehničke vještine za obradu incidenata, penetracijsko testiranje te provjeru ranjivosti, kibernetičko ratovanje, povećanje kapaciteta u kibernetičkoj sigurnosti te prikupljanja podataka iz otvorenih izvora (OSINT). Zbog jačanja internih kapaciteta u NCERT-u postoji stalno obnavljan repozitorij knjiga, stručnih časopisa, mrežnih tečajeva i digitalnih knjiga i priručnika.

Svake godine ZSIS donosi plan školovanja sukladno kojem se provodi izobrazba. ZSIS provodi i specijalističku izobrazbu drugih tijela.

MORH je organizirao edukaciju za svoje djelatnike te su tako:

- 4 djelatnika sudjelovala na Tehničkom veleučilištu Zagreb na stručnom specijalističkom diplomskom studiju informacijske sigurnosti i digitalne forenzike za školske godine 2020/2021 i 2021/2022.

- 2 djelatnika sudjelovala u SAD na tečaju Cyber Security Fundamentals and Defence
- 1 djelatnik sudjelovao u SAD na tečaju Cyber Law and Hybrid Warfare, NewPort, Rhode Island
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Critical Information Infrastructure Protection Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Operational Cyber Threat Intelligence Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Infrastructury Digital Protection Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Cyber Defence Monitoring Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Malware and Exsploit Essentials Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na IT Systems Attack and Defence Course
- 1 djelatnik sudjelovao u Estoniji u CCDCOE na Reverse Enginnering Malware Course
- 1 djelatnik sudjelovao u Njemačkoj na tečaju Iregular Warfare and Hybrid Threats
- 12 djelatnika sudjelovalo na Malom Lošinju na Radionici razvoja kibernetičkih sposobnosti tehničke razine (eng. Tehnical Cyber Workshop)
- 18 djelatnika je prošlo obuku Mandinat ThretaSpace uz potporu stručnjaka tvrtke Mandiant,
- 3 djelatnika su sudjelovala na online tečaju CompTIA Security Plus
- 7 djelatnika je započelo s korištenjem on-line tečajeva Network Security

U 2022. 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 2022. HAKOM je obilježio Dan sigurnijeg interneta sudjelovanjem na konferenciji „Potraga za boljim internetom″ čiji organizatori bili su Udruga Suradnici u učenju, CARNET i NCERT s partnerima, među kojima je i HAKOM, na kojoj su osim edukativnih materijala istaknute obveze operatora prilikom pružanja usluga u elektroničkim komunikacijama u odnosu na djecu. 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. Isto tako, predstavljeno je i veliko HAKOM-ovo ispitivanje o navikama i iskustvima korisnika interneta u RH, koje je provedeno u prosincu 2021. i u kojemu je sudjelovalo 1003 ispitanika u dobi od 18 do 65 godina. Nadalje, HAKO je gostovao u radijskim emisijama koje obrađuju teme o zaštiti potrošača i objavljen je članak u tisku „24 sata“ na temu „Jeste li zaštitili svoje dijete“ u kojem su istaknuti digitalni tragovi i sigurna uporaba interneta.

HAKOM je izradio i zanimljiv videozapis namijenjen najmlađima koji sadrži praktične i korisne savjete o zaštiti na internetu te je isti objavljen na YouTube kanalu i društvenim mrežama.

U 2022. HAKOM je izvršio nadogradnju postojećih funkcionalnosti i ažuriranje aplikacije "Kalkulatora privatnosti" dodavanje novih scenarija prema zastupljenosti prevara u hrvatskom internetskom prostoru te Kviz o sigurnosti na internetu.

U svim razredima osnovne i srednje škole u kojima se provodi bilo redovna bilo izborna/fakultativna nastava informatike i računalstva, obrađuju se nastavni sadržaji iz područja kibernetičke sigurnosti.

Kurikulum međupredmetne teme Uporaba informacijsko komunikacijske tehnologije također pokriva teme iz kibernetičke sigurnosti.

Na satovima razrednog odjela često se razgovara o sigurnosti, odgovornosti i oprezu pri korištenju internetskih usluga i digitalnih uređaja.

Stručni suradnici provode radionice s učenicima na temu 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 za javno i komercijalno dostupne bežične mreže (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 2022. godini HNB je izdala 10 objava svim kreditnim institucijama o uočenim sigurnosnim ranjivostima te preporuke za daljnje postupanje. Značajnije objave upućene su i institucijama za platni promet te institucije za elektronički novac.

Osim obavijesti o otkrivenim sigurnosnim prijetnjama i ranjivostima HNB je u zadnjem kvartalu 2022. svim financijskim institucijama dostavila i „Preporuke za prilagodbu IT sustava KI za pripremu konverzije“ koje su sadržavale preporuke vezano uz pripremu za konverziju, kontigencijske planove te održavanje primjerene razine sigurnosti.

HNB je 17.5.2022. održala radionicu vezanu uz nacrt Odluke o primjerenom upravljanju informacijskim sustavom. Održana radionica imala je za cilj banke upoznati s novim obvezama koje proizlaze iz Odluke te im odgovoriti na nejasnoće prije javnog savjetovanja.

Nadalje, u 2022. godini nadziranim institucijama upućeno je 87 dopisa i 20 okružnica te je održano 113 sastanaka s temama vezanim 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.

U 2022. godini NCERT je nastavio s aktivnostima podizanja svijesti građana o važnosti kibernetičke sigurnosti objavljivanjem aktualnih novosti iz svijeta kibernetičke sigurnosti i IKT tehnologije te sigurnosnih preporuka. Tijekom 2022. nastavljena je suradnja sa FER-om u pogledu pisanja i izdavanja stručnih dokumenata (objavljena su tri 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 2022. godini proveo niz aktivnosti vezanih uz jubilarni deseti 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 “Razmisli prije nego klikneš!” 10-ti ECSM se bavio temama phishing i ransomware napada.

NCERT je aktivan i na društvenim mrežama:

- https://www.facebook.com/CERT.hr/
- https://twitter.com/HRCERT

Tijekom 2022. NCERT je objavio ukupno 161 novost na web sjedištu i društvenim mrežama.

Broj posjetitelja web sjedišta www.cert.hr je 177.533

Broj pratitelja Facebook stranice 2038

Broj pratitelja Twitter stranice 1435

U listopadu 2022. godine provedeno je treće CTF natjecanje Hacknite za srednje škole na kojem je sudjelovao ukupno 54 srednjoškolskih timova s 270 učenika iz 33 srednje škole.

2022. godine pokrenuta je i 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 prvi put sudjelovala na European Cyber Security Challenge-u (ECSC) s nacionalnim timom sastavljenim od pet srednjoškolaca i pet studenata Fakulteta elektrotehnike i računarstva.

U listopadu 2022. izrađena je i tiskana brošura pod nazivom Sigurna knjižica https://www.cert.hr/wp-content/uploads/2022/11/Sigurna-knjizica.pdf koja donosi osnovne informacije o temama iz kibernetičke sigurnosti za opću populaciju poput: važnost sigurnosne kopije, phishinga i ransomware napada, prepoznavanja i zaštite, sigurnom surfanju, snažnim lozinkama, važnosti ažuriranja, kriptografiji, steganografiji i digitalnoj forenzici.

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

HAKOM je u 2022. godini nastavio aktivnosti podizanja svijesti o važnosti kibernetičke sigurnosti. Od 2015. godine provodi se program koji uključuje podizanje svijesti učenika i roditelja o temi sigurnosti na internetu, a edukativni materijali dostupni su svima. Osim predavanja učenicima ili roditeljima po pozivu škola, svake godine se osvježi i revidira brošura *„Kako se zaštititi u svijetu interneta i mobilnih telefona“,* koja se otisne u 50.000 primjeraka i dostavi u sve osnovne škole uoči svjetskog obilježavanja Dana sigurnijeg interneta (DSI) u veljači svake godine, što je i učinjeno 2022. godine. Zadnja revizija brošure obavljena je krajem 2022. za tisak brošure u siječnju 2023., a objavljena je na internetskoj stranici HAKOM-a. Promocija najnovije brošure uslijedila je u sklopu DSI2023. Tijekom godine redovito su se dijelili savjeti ili upozorenja oko kibernetičke sigurnosti na društvenim mrežama.

Nastavljena je analiza načina 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 raznih edukativnih materijala i preporuka na internetskim stranicama ZSIS-a.

Zbog utjecaja pandemije Covida 19 na prethodno uobičajeni način života građana, izrađeni su promotivni materijali pod nazivima: Sigurnost u domu i Siguran rad od kuće, sa savjetima o sigurnosti na internetu te su isti u više navrata distribuirani medijima.

Tijekom 2021. godine i dalje je veliki broj građana bio oštećen različitim oblicima internetskih prijevara. Temeljem navedenog, a u suradnji s Europolom, MUP je proveo javnu kampanju #CyberScams kao dio programa European Cyber Security Month. U svrhu te kampanje izrađen je i korišten promotivni materijal o 7 najčešće korištenih financijskih online prijevara i kako ih izbjeći.

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

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

U slučaju nastanka računalnih sigurnosnih incidenata koji se mogu multiplicirati i pogoditi veliki broj korisnika, javnost će obavijestiti nadležno državno odvjetništvo preko nadležnog državnog odvjetnika ili određenog zamjenika koji zaprimi informaciju ili kaznenu prijavu, odnosno Državno odvjetništvo RH odgovarajućim priopćenjem, vodeći pri tome računa o zaštiti probitaka kriminalističkog istraživanja ili istrage u predmetima kibernetičkog kriminaliteta, a prema potrebi će davati upute radi sprječavanja daljnjih prijetnji i umanjenja štetnih posljedica incidenata.

Za koordinatora opisanih aktivnosti na razini državnoodvjetničke organizacije određena je zamjenica Glavne državne odvjetnice RH.

U 2022. godini Hrvatska zaklada za znanost financirala je šest projekata povezanih s područjem informacijske i komunikacijske tehnologije s naglaskom na informacijskoj sigurnosti:

- „Korisniku orijentiran (re)dizajn procesa i modeliranje informacijskih sustava na primjeru smart city usluga“, Sveučilište u Splitu, Ekonomski fakultet
- „Okvir za kontrolu i nadzor bespilotnih letjelica“, Sveučilište u Zagrebu, Fakultet organizacije i informatike
- „Pametne usluge usmjerene čovjeku u interoperabilnim i decentraliziranim okolinama Interneta stvari“, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva
- „Pouzdani i sigurni kompleksni softverski sustavi: Od empirijskih principa prema teoretskim modelima iz perspektive industrijske primjene“, Sveučilište Jurja Dobrile u Puli
- „Višeslojni okvir za karakterizaciju širenja informacija putem društvenih medija tijekom krize COVID-19“, Sveučilište u Rijeci, Odjel za informatiku
- „Učinak digitalizacije interne komunikacije na zadovoljstvo internom komunikacijom, angažiranost zaposlenika i, posljedično, percipirano zadovoljstvo životom“, Sveučilište u Zagrebu, Ekonomski fakultet u Zagrebu

U 2022. godini javna visoka učilišta i organizacije civilnog društva prijavila su sedam znanstvenih ili znanstvenostručnih skupova koji su povezani s područjem informacijske i komunikacijske tehnologije, a koji su financirani od MZO-a:

- Skup „MOTSP2022 (Management of Technology - Step to Sustainable Production), organizator Fakultet strojarstva i brodogradnje, Zagreb
- Skup „CECIIS 2022 (Central European Conference on Information and Intelligent Systems)“, organizator Fakultet organizacije i informatike, Varaždin
- Skup „7. međunarodna konferencija o pametnim i održivim tehnologijama“, organizator Fakultet elektrotehnike, strojarstva i brodogradnje u Splitu
- Skup „Technology, Innovation and Stability: New Directions in Finance“, organizator Ekonomski fakultet, Zagreb

- Skup „IEEE 2022 International Conference on Smart Grid Synchronized Measurements and Analytics – IEEE SGSMA 2022“, organizator Fakultet elektrotehnike i računarstva, Zagreb
- Skup „45. Jubilarni međunarodni ICT skup MIPRO 2022“, organizator Hrvatska udruga za informacijsku, komunikacijsku i elektroničku tehnologiju – MIPRO
- Skup „The 8th ENTerprise REsearch InNOVAtion Conference – ENTRENOVA 2022“, organizator Udruga za promicanje inovacija i istraživanja u ekonomiji „IRENET“

IV. ZAKLJUČAK

Kako se tijekom 2022. smanjio utjecaj pandemije na normalno funkcioniranje tijela povećao se broj i opseg koordinativnih aktivnosti. Dodatan značajniji čimbenik povećane koordinacije je rat u Ukrajini koji ima svoju refleksiju i u kibernetičkom prostoru.

Tijekom 2022. godine je donesena i vrlo značajna NIS2 direktiva koja između ostalog propisuje elemente koje nacionalne strategije kibernetičke sigurnosti moraju sadržavati kao i obavezne mjere za kritične i ključne operatore u nizu sektora. Slijedom toga pripreme provedene u 2022. na izmjenama Nacionalne strategije kibernetičke sigurnosti i Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga bi trebale rezultirati izmjenama ova dva akta kao i donošenjem novih podzakonskih akata u 2023./2024.

Postojeća Strategija je najvećim dijelom provedena i ujedno prva koja je obuhvatila područje kibernetičke sigurnosti. Temeljila se na postojećim sposobnostima tijela, postojećoj regulativi i vrlo skromnim financijskim sredstvima osiguravanim najvećim dijelom iz redovnog proračuna dionika provedbe. Strategija se fokusirala na prioritete koje je trebalo provesti u što kraćem razdoblju, i nije imala ambiciju provesti značajne promjene u nadležnostima tijela. Tijekom provedbe Strategije utjecaj EU-a na pitanje uređenja kibernetičke sigurnosti, kako u ostalim članicama tako i u RH, je jačao i u regulatornom dijelu i u financijskim mehanizmima potpore.

Vrlo značajan rezultat provedbe Strategije je povećana svijest državnih tijela, različitih drugih organizacija, poslovnih subjekata i građana te uspostava mehanizama koordinacije i suradnje. U dijelu mjera koje nisu provedene iz različitih objektivnih okolnosti i razloga bit će potrebno u novoj Strategiji pronaći drukčije mehanizme provedbe ciljeva.