REPUBLIKA HRVATSKA

URED VIJEĆA ZA NACIONALNU SIGURNOST

NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2021. GODINI

Zagreb, srpanj 2022.

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 2021. godini prikazanim u Godišnjem izvješću o radu Vijeća u 2021. godini[2].

Izvješće o provedbi Akcijskog plana u 2021. godini temelji se na ciljevima Nacionalne strategije kibernetičke sigurnosti[3] (u daljnjem tekstu: Strategija), koji su razrađeni u obliku mjera 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 Republiku Hrvatsku 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

[1] Odluka o osnivanu Vijeća 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/Godi%C5%A1nje%20izvje%C5%A1%C4%87e%20o%20radu%20Nacionalnog%20vije%C4%87a%20za%20kiberneti%C4%8Dku%20sigurnost%20i%20Operativno-tehni%C4%8Dke%20koordinacije%20za%20kiberneti%C4%8Dku%20sigurnost%20za%202021.%20godinu%20(o%C5%BEujak%202020.).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

E. Kibernetički kriminalitet – 5 mjera

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera

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

H. Međunarodna suradnja – 6 mjera

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

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 obnovljivog 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 lipnja 2022. 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 u okviru svojih redovnih ovlasti nadzora primjene mjera sigurnosti elektroničkih komunikacijskih mreža i usluga prikuplja i analizira sigurnosne politike koje su operatori obvezni dostavljati na godišnjoj osnovi, kao i nalaze revizije njihovih informacijskih sustava.

U 2021. sigurnosne politike i reviziju informacijskih sustava dostavilo je 5 operatora, a HAKOM je dokumente analizirao i zaključio da su sukladni propisanim obvezama.

Nadalje, temeljem zahtjeva iz 5G Toolbox-a, odnosno zbirke alata za ublažavanje mjera i podupirućih radnji (Cybersecurity of 5G networks EU Toolbox of risk mitigating measures) iz siječnja 2020., HAKOM je u 2021. donio novi Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga[5] u kojem je implementirana većina tehničkih mjera zbirke alata za ublažavanje mjera i podupirućih radnji (5G Toolbox).

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

[5] NN 112/21

slučaju eventualnih povreda osobnih podataka, povrede tajnosti elektroničkih komunikacija, postupanja s predmetnim 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[6]).

Tehnička koordinacija regulatornog tijela za područje javnih elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti provodi se u potpunosti prije svega u okviru Koordinacije, ali i kroz druge oblike suradnje. U 2021. godini se izmijenio Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga te su operatori obvezni prijavljivati računalne incidente putem PiXi platforme. Kroz suradnju s nacionalnim institucijama, privatnim sektorom i međunarodnim partnerima te aktivnu razmjenu informacija, SOA kontinuirano povećava mjere i standarde informacijske sigurnosti koji pomažu većoj sigurnosti kibernetičkog prostora Republike Hrvatske s naglaskom na prevenciji i brzom oporavku kao i odgovoru u slučaju ugroze tog prostora što doprinosi boljoj zaštiti podataka. Nakon 2020. godine, kada je SOA pokrenula novu aktivnost upravljanja nacionalnim kibernetičkim krizama i ustrojila međuresornu radnu skupinu s drugim tijelima, tijekom 2021. završena je izrada nacionalnog dokumenta sa standardnim operativnim procedurama za upravljanje kibernetičkim krizama. Ovaj proces, kao i rezultirajući prijedlog standardnih operativnih procedura, SOA usklađuje s EU CyCLONe organizacijom za upravljanje kibernetičkim krizama na EU razini, a u kojoj SOA predstavlja RH. Sastanci Vijeća i Koordinacije održavaju se na mjesečnoj razini, osim u slučaju potrebe za sazivanjem izvanredne sjednice. Osim toga, u sklopu projekta Grow2CERT, NCERT organizira i održava sastanke radne skupine za razvoj, promociju i stalno poboljšanje platforme za razmjenu informacija o incidentima i prijetnjama PiXi koja se sastaje jednom mjesečno i tijekom godine održano je osam sastanaka. Članovi radne skupine su predstavnici nositelja provedbe mjera iz Akcijskog plana Nacionalne strategije kibernetičke sigurnosti, regulatornih agencija, akademske zajednice i Hrvatske udruge banaka. Radna skupina se sastoji od predstavnika ukupno 12 institucija i organizacija. U travnju 2021. započela je edukacija korisnika iz pojedinih sektora ključnih usluga prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[7] (dalje u tekstu ZoKS). Edukaciju su prošli operatori ključnih usluga iz sektora energetike, bankarstva, infrastrukture financijskog tržišta, opskrbe vodom za piće i njezina distribucija, digitalne infrastrukture i dijela poslovnih usluga za državna tijela te davatelji digitalnih usluga i telekomunikacijske tvrtke. Platforma PiXi puštena je u punu produkciju 3. svibnja. 2021.

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

[7] NN 64/18

Nakon donošenja ZoKS-a uspostavljen je novi okvir sektorske i međusektorske suradnje s nadležnim tijelima te je proširena uloga ZSIS-a i NCERT-a s funkcijom CSIRT-a za određene sektore u RH pa je na taj način proširena i funkcija međusobne razmjene podataka.

OTC, koji je temeljem Zakona o elektroničkim komunikacijama[8], nadležan za propisivanje i nadzor mjera i standarda informacijske sigurnosti kod operatora elektroničkih komunikacija po pitanju funkcije tajnog nadzora, provodi kontinuiranu koordinaciju s regulatornim tijelom za područje tržišta elektroničkih komunikacija i središnjim državnim tijelom za informacijsku sigurnost kako bi osigurao usklađivanje propisanih i implementiranih mjera i standarda informacijske sigurnosti kod operatora s novonastalim regulatornim zahtjevima, s ciljem zadržavanja postignute razine informacijske sigurnosti ili mogućeg unaprjeđenja iste.

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

(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 tri – definirani su **organizacijski i tehnički zahtjevi** za povezivanje na državnu informacijsku infrastrukturu, provedena je

[8] NN 73/08, 90/11, 133/12, 80/13, 71/14, 72/17

analiza mogućnosti povezivanja državnih tijela klasificiranom mrežom te je izrađen **plan povezivanja** koji se provodi u fazama. Planom je u prvoj fazi predviđeno uvezivanje tijela sigurnosno-obavještajnoga sustava, ključnih ministarstava, Vlade RH, Hrvatskoga sabora i Ureda Predsjednika, a u drugoj fazi uvezivanje ostalih državnih tijela sukladno ispunjenju potrebnih preduvjeta.

Izrada **analize postojećeg stanja** u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora nije započela radi utvrđivanja odgovarajućih nadležnosti SDURDD.

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[9], Uredba o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu[10]).

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 je odgođena jer je procijenjeno da rok periodične procjene treba s 2 godine produljiti na 5 godina.

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 u sustavu kao i intenzivnom radu na redizajnu sustava e-Građani.

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**:

[9] NN 92/14
[10] NN 60/17

- 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 2015. Na radionicama su sudjelovali predstavnici svih banaka koje posluju u Republici Hrvatskoj , 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 Hrvatskoj narodnoj banci.

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 Republike Hrvatske donijela je Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[11]. 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 ZKS-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 Republici Hrvatskoj. 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.

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 Hrvatskoj narodnoj banci, 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

[11] NN 68/18

objavljene i na internetskim stranicama HNB-a, a čija primjena počinje od dana stupanja na snagu novog Zakona o platnom prometu[12] kojim se u zakonodavstvo Republike Hrvatske 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 Republici Hrvatskoj.
U 2019. i 2020. u više navrata je s kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac u Republici Hrvatskoj komunicirano o obavezama tih institucija vezano uz izvješćivanje HNB-a o incidentima.

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 Republici Hrvatskoj. 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.

(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 su procesi donošenja novih propisa na razini EU (prvenstveno NIS2 direktive) koji će utjecati na dimenzioniranje novih sektora i područja iz domene kibernetičke sigurnosti. Uskladit će se zakonski i podzakonski akti te na taj način napraviti razlika između pojmova kritične infrastrukture i kritične komunikacijsko-informacijske infrastrukture kako bi se dodatno podigla razina znanja o predmetnoj problematici i izbjegle sve nejasnoće, dvosmislenosti i nedoumice. Učinjena je prilagodba u izmjenama prijedloga Zakona o kritičnim infrastrukturama[13] uvođenjem glave „Kritična komunikacijsko-informacijska infrastruktura“, a koja istu definira kao horizontalnu komponentu nacionalne kritične infrastrukture.

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 (cilj D.1.);

[12] NN 66/18
[13] NN 56/13

- utvrditi obvezujuće sigurnosne mjere koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture (cilj D.2.);
- ojačati prevenciju i zaštitu kroz upravljanje rizikom (cilj D.3);
- ojačati javno-privatno partnerstvo i tehničku koordinaciju u obradi računalnih sigurnosnih incidenata (cilj D.4.);
- uspostaviti kapacitete za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu (cilj D.5.).

Kriteriji za prepoznavanje kritične komunikacijske i informacijske infrastrukture su definirani ZoKS-om. Primjenom navedenih kriterija identificirano je 100-tinjak operatora ključnih usluga.

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[14], 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 ovog Zakona

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 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,

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

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 2021. 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 2021. godini redovno sudjelovali u radu Odbora Vijeća Europe za praćenje primjene Konvencije o kibernetičkom kriminalitetu[15] (T-CY Odbor). U 2021. godini održano je nekoliko on-line sastanaka, te je usvojen nacrt Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu. Promjena u odnosu na prethodna razdoblja je i da su u radu T-CY-a sudjelovali i predstavnici MVEP.

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

[15] NN 9/02

COPEN na temu unutarnjeg zakonodavnog paketa e-dokaza te podržavaju inicijative i korake koji mogu dovesti do bržeg usvajanja kompromisnog rješenja.

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 1.10.2020.) kojim se nastavlja s radom i aktivnostima potrebnim za uspješnu integraciju nacionalnih sustava e-Spis i CTS s e-EDES-om (*e-Evidence Digital Exchange System*). 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 trajati će ukupno 24 mjeseca odnosno do 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.

Na području kaznenog materijalnog zakonodavstva, tijekom 2021. izvršene su izmjene i dopune Kaznenog zakona[16] kojima je u nacionalno zakonodavstvo transponirana Direktiva (EU) 2019/713 Europskog parlamenta i Vijeća od 17. travnja 2019. o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP. S tim u vezi, u Kazneni zakon unesena je definicija bezgotovinskog instrumenta plaćanja te su uvedena nova kaznena djela: nedozvoljeno posjedovanje bezgotovinskog instrumenta plaćanja (u članku 244.a Kaznenog zakona) te izrada, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za zlouporabu bezgotovinskih instrumenta plaćanja (u članku 331.a Kaznenog zakona). Također su izvršene dopune kaznenih djela krivotvorenja isprave (članak 278. Kaznenog zakona) i računalne prijevare (članak 271. Kaznenog zakona).

Spomenutim Zakonom o izmjenama i dopunama Kaznenog zakona provedeno je i daljnje usklađivanje kaznenog zakonodavstva s Direktivom (EU) 2017/541 Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni Odluke Vijeća 2005/671/PUP u dijelu članka 3. stavka 1. točke (i) predmetne Direktive, koji se poziva na Direktivu 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP.

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

[16] NN 84/21

- Kontakt točka uspostavljena 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[17] 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.
- Kontakt točku G 7 uspostavila je organizacija sedam najrazvijenijih zemalja svijeta. Kontakt točkom administrira Ministarstvo pravosuđa SAD-a. Hrvatska kontakt točka je Služba kibernetičke sigurnosti.
- Kontakt točke Interpola za razmjenu informacija o kibernetičkom kriminalitetu. Hrvatska kontakt točka je Služba kibernetičke sigurnosti. Hrvatska kontakt točka dostupna je putem adrese elektroničke pošte cyber.crime@mup.hr te je u posjedu kontakt podataka o svim ostalim kontakt točkama u svijetu. Kontakt točke služe za zadržavanje podataka i elektroničkih dokaza za čije je pribavljanje potrebna međunarodna pravna pomoć ili za izravno pribavljanje obavijesti za koje nije potreban zahtjev pravosudnog tijela.

Tijekom 2021. godine MUP je redovno slao zahtjeve prema drugim državama te primao zahtjeve drugih država te nema poteškoća u provedbi.

SOA uspostavljenu međunarodnu suradnju kontinuirano razvija i u području kibernetičke sigurnosti te aktivno razmjenjuje informacije s partnerskim agencijama u cilju prevencije, brzog oporavka i odgovora u slučajevima ugroze kibernetičkog prostora Republike Hrvatske. 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).

ZSIS sudjeluje u radu više tijela međunarodnih organizacija te u okviru toga po potrebi i upitima razmjenjuje informacije primarno tehničkog karaktera vezane uz kibernetičke prijetnje i računalno sigurnosne incidente te informacije vezane uz područja kriptografske zaštite podataka, zaštite od neželjenog elektromagnetskog istjecanja (TEMPEST) i provođenja sigurnosnih akreditacija informacijskih sustava međunarodnih asocijacija kojih je RH članica.

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

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 Republike Hrvatske je zamjenica općinskog državnog odvjetnika u

[17] NN 102/15

Općinskom državnom odvjetništvu u Zagrebu, koja u predmetima kibernetičkog kriminaliteta kao nacionalni predstavnik Republike Hrvatske u Europskoj pravosudnoj mreži, usmjerava i žurno prosljeđuje zamolbe za međunarodnu pravnu pomoć i suradnju prema zemljama članicama Europske unije i drugim zemljama.

U MUP-u kontakt točka za razmjenu informacija i koordinaciju postupanja s drugim nacionalnim tijelima je Služba kibernetičke sigurnosti. Tijekom 2021. godine ostvarena je suradnja na konkretnim slučajevima istraživanja kibernetičkog kriminaliteta sa ZSIS-om i NCERT-om. MUP i NCERT potpisali su sporazum o suradnji te se navedeni sporazum uspješno provodi. Suradnja sa ZSIS-om odvija se bez potpisanog sporazuma te je na sastanku glavnog ravnatelja policije i ravnatelja ZSIS-a zaključeno da zbog izvrsne suradnje nema potrebe za izradom posebnog sporazuma o suradnji.

U DORH-u je stalna kontakt točka zamjenica Glavne državne odvjetnice Republike Hrvatske, Ured Glavne državne odvjetnice Republike Hrvatske, a radi preveniranja i učinkovitog rješavanja incidenata na nacionalnoj razini. Do 31. kolovoza 2021. godine stalna kontakt točka bio je zamjenik Glavne državne odvjetnice Republike Hrvatske.

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 organizacije 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) izradila i usuglasila Nacionalne standardne operativne procedure za upravljanje kibernetičkim krizama te ih predložila za usvajanje na Vijeću za nacionalnu sigurnost.

Sukladno Uredbi o izmjenama i dopunama uredbe o unutarnjem ustrojstvu Ministarstva unutarnjih poslova[18], Služba kibernetičke sigurnosti u MUP-u sudjeluje u primjeni i razvoju nacionalnog zakonodavnog okvira kibernetičke sigurnosti, aktivnostima i mjerama u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, 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, potiče razvoj usklađenih obrazovnih programa, potiče istraživanja i razvoj, napose u području e-usluga, radi na sustavnom pristupu međunarodnoj suradnji u području kibernetičke sigurnosti, sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela visokotehnološkog kriminaliteta (kaznena djela protiv računalnih sustava, programa i podataka, kaznena djela protiv intelektualnog vlasništva, naročito počinjenog putem računalnih sustava ili mreža, kaznena djela počinjena zlouporabom sredstava plaćanja – kartični kriminalitet te kaznena djela iskorištavanja djece za pornografiju)

[18] NN 97/2020

te predlaže rješenja za podizanje razine učinkovitosti rada u suzbijanju visokotehnološkog kriminaliteta, neposredno provodi složena kriminalistička istraživanja u domeni kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža, kriminaliteta počinjenog zlouporabom sredstava plaćanja te iskorištavanja djece za pornografiju, obavlja forenzičku analizu digitalnih dokaza, pruža specijaliziranu potporu drugim policijskim jedinicama, surađuje s drugim ustrojstvenim jedinicama MUP-a, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada, sudjeluje u planiranju i izradi programa obuke i specijalizacije policijskih službenika u čijem je djelokrugu rada problematika visokotehnološkog kriminaliteta, sudjeluje u izradi normativnih akata, izvješća i drugih stručnih materijala iz domene visokotehnološkog 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 Republici Hrvatskoj.

U tijeku je 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 je 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: 90%.

Projekt se sastoji od 2 komponente:

1. 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 da će se putem specijaliziranog forenzičkog softvera i hardvera izraditi forenzičke kopije sadržaja memorije predmeta koji se pretražuju, navedene kopije pohranit će se na poslužiteljima, a nakon toga 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.

2. Provođenje edukacijskih modula na temu digitalnih dokaza i forenzičkih metoda i procedura za 31 policijskog službenika

Predstavnici Službe kibernetičke sigurnosti MUP-a 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.

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[19], u nadležnosti Državnog zavoda za intelektualno vlasništvo, zaštita poslovne tajne kao značajnog ekonomsko-pravnog instituta usklađena je sa zakonodavstvom EU-a (Direktiva EU 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija **poslovne tajne** od nezakonitog pribavljanja, korištenja i otkrivanja i Direktiva 2004/48/EZ Europskog parlamenta i Vijeća od 29. travnja 2004. o provedbi prava

[19] NN 30/18

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.

Uspostava **redovitih koordinacijskih aktivnosti** nacionalnih tijela nadležnih za pojedine skupine zaštićenih podataka se provodila u smanjenom obimu zbog okolnosti uzrokovanih pandemijom COVID-19 i drugih specifičnih obveza. AZOP je imao zahtjevnu angažiranost stručnih resursa u aktivnostima praćenja i provedbe primjene Opće uredbe o zaštiti podataka posebice u dijelu aktivnosti usmjerenih na provođenje istraga o primjeni Opće uredbe o zaštiti podataka kao i kontinuiteta osvješćivanja i edukacije voditelja i izvršitelja obrade osobnih podataka kao i samih ispitanika tj. građana (budući da se predmetna Uredba izravno i obvezujuće primjenjuje u državama članicama od 25.5.2018. godine).

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 EU 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.

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). ZSIS 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 **unaprjeđivanje postojećih sustava za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima** osnovana je radna skupina čiji su članovi, uz nositelje, naknadno dodani ovisno o razvoju platforme PiXi. Radna skupina trenutno se sastoji od 12 institucija i organizacija: FER, HAKOM, HANFA, HNB, HUB, MINGOR, MORH, MUP, NCERT, SDURDD, MIZ i ZSIS. Radna skupina koja je aktivna od 2017. godine do danas, 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. Krajem 2021. započeo je proces izmjena i dopuna Nacionalne taksonomije zbog pojave novih vrsta računalno-sigurnosnih incidenata koje se nisu mogle svrstati u postojeću inačicu taksonomije. Nova inačica Nacionalne taksonomije u primjeni je od 1. siječnja 2022., a dostupna je na sljedećoj poveznici:

https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf

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 112 korisničkih računa iz 42 različite organizacije i institucije. 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. HAKOM vodi evidenciju o računalnim incidentima za operatore te o istome obavještava i Koordinaciju na redovitim sastancima. U 2021. godini je izmijenjen Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga te su operatori postali obvezni prijavljivati računalne incidente putem PiXi platforme. HNB prikuplja podatke o značajnim incidentima vezanima uz informacijske sustave institucija nad kojima provodi nadzor (kreditne institucije, institucije za elektronički novac, institucije za platni promet, pružatelji usluga agregiranja informacija o računu), a koje su obavezne takve incidente prijaviti prema:

- Smjernicama o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 (PSD2);
- ZoKS-u; ili
- Odluci o primjerenom upravljanju informacijskim sustavom[20].

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 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.

NCERT je kao nositelj mjere u 2021. godini izdao pet upozorenja putem web sjedišta www.cert.hr, Facebook stranice CERT.hr i Twitter računa HRCERT. NCERT je ugasio uslugu izdavanja sigurnosnih preporuka čiju zadaću je u siječnju 2021. preuzela usluga CERT Epsilon koja korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava. Uz to usluga korisnicima omogućava brže pretraživanje poznatih ranjivosti prema specifičnim kriterijima kao što su proizvođač, CWE oznaka te ID oznaka. 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://epsilon.cert.hr/ . Prema pokazateljima korištenja usluge ukupan broj korisnika je 133, a ukupan broj posjeta stranici 1621.

HNB kao sunositelj navedene mjere u 2021. godini je izdao 11 objava svim kreditnim institucijama o uočenim sigurnosnim ranjivostima te preporuke za daljnje postupanje.

ZSIS je kao sunositelj mjere tijekom 2021. godine izdao 9 javnih upozorenja putem web sjedišta www.zsis.hr, 30 upozorenja putem elektroničke pošte te je dao 90 preporuka u okviru

[20] NN 37/10

rješavanja računalno-sigurnosnih incidenata na neklasificiranim informacijskim sustavima državnih tijela i institucija.

HAKOM je kao sunositelj mjere izdao u 2021. godini 19 upozorenja/preporuka putem društvenih mreža od kojih su minimalno 4 podijeljena s CERT.hr Facebook stranice. S web sjedišta HAKOM-a odaslana su u 2021. godini 2 upozorenja.

Policijski službenici Službe kibernetičke sigurnosti MUP-a su tijekom 2021. 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 kampanja te drugih kibernetičkih ugroza, otvorila je tijekom 2021. mogućnost puno dublje suradnje u okvirima preko 50 institucija koje su pristupile sustavu SK@UT, a uključuju i državna tijela i operatore ključne infrastrukture, kao i pravne osobe od posebnog interesa za RH. Dodatna razmjena iskustva i znanja intenzivno se provodila tijekom 2021. godine kroz rad međuresorne radne skupine za upravljanje kibernetičkim krizama, u kojoj sudjeluju predstavnici 7 institucija koje koordinira SOA.

(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**.

Koordinativne aktivnosti u 2021. u području međunarodne suradnje uvelike su bile oblikovane pandemijom. Dok su sastanci uživo najvećim dijelom izostali, broj on-line aktivnosti je jako porastao. Formalno **uspostavljanje koordinacije ispunjeno je u cijelosti** usvajanjem Zaključka NVKS sredinom 2018. godine. Redovno su se distribuirale informacije o međunarodnim kibernetičkim aktivnostima te su se inicirali virtualni radni sastanci (primjerice na temu nove Strategije kibernetičke sigurnosti EU) s ciljem rasprave i donošenja potrebnih odluka Vijeća, ali i u drugim formatima poput Radne skupine NVKS za 5G. Planirani sveobuhvatni pregled međunarodnih aktivnosti kao i Kalendar međunarodnih obveza i sastanaka nisu realizirani ponajprije zbog otegotnih pandemijskih uvjeta, izostanka softverskih rješenja i ograničenih kadrovskih kapaciteta.

Uz značajne napore, u prvom redu MVEP-a te stalnih misija odnosno predstavništava RH pri EU i UN, radilo se na općim političkim i organizacijskim aspektima pripreme rada Ad hoc Odbora za izradu sveobuhvatne **međunarodne konvencije** o suzbijanju korištenja informacijskih i komunikacijskih tehnologija za kriminalne svrhe. MVEP je redovno izvještavao NVKS o relevantnim međunarodnim aktivnostima i okolnostima u kontekstu napora izrade nove međunarodne konvencije. U svrhu preliminarne koordinacije za predstojeće obveze RH, na inicijativu MVEP i u organizaciji MPU, 22. srpnja 2021. godine održan je prvi neformalni sastanak na ovu temu s predstavnicima MUP-a i ŽDORH-a. Pored toga, MVEP je u izravnoj elektronskoj komunikaciji nastavio dijeliti informacije i tražiti mišljenja nadležnih tijela. Do kraja godine, i uz privolu RH, pripremljen je zajednički doprinos EU ovom procesu.

U rujnu, na marginama konferencija održanih pod SI PRES na Bledu, RH je sudjelovala na sastanku EU cyber diplomacije na kojem su razmijenjena stajališta i okvirno dogovorena postupanja oko ključnih aktualnih procesa u međunarodnim organizacijama. U tom kontekstu, postalo je vidljivo da je RH jedna od malobrojnih država u kojima su na vrijeme započele koordinacijske aktivnosti. Uz pojačani diplomatski angažman, u drugoj polovici godine RH se također uključila u američku inicijativu protiv tzv. ransomware-a te je poslala i svoj konkretan doprinos (kolekcijom prikupljenih vlastitih iskustava te primjera najbolje prakse kao i prijedloga djelovanja ove inicijative). Vezano za ključne globalne aktivnosti, RH je svoj doprinos pružala kroz zajedničke napore EU, dakle ponajprije putem Stalnog predstavništva RH pri EU (SPRH 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 EU kibernetičkog sankcijskog režima (koji je u svibnju produljen za još godinu dana). Na razini HRS usuglašeni su i nacrti izjave Visokog predstavnika kao odgovora u ime EU-a i država članica na kibernetičke incidente SolarWinds, Ghostwritter i Microsoft Exchange.

Sudjelovanje RH (ponajprije putem MVEP) u aktivnostima OESS-ovih Comm-check vježbi za provedbu **mjera za izgradnju povjerenja** (CBMs), RH je i tijekom 2021. godine (putem MVEP i u suradnji s pojedinim nadležnim institucijama) ispunila u najvećoj mogućoj mjeri sve zadaće i očekivanja. Dodatno, tematika izgradnje povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija jedna je od stožernih politika EU (i RH) u raspravama na globalnoj razini, a posebice u kontekstu rada

UN-a (OEWG, a posredno i UNGGE). U svibnju 2021. EU je organizirala prvu vježbu ikada s državama istomišljenicama vezano uz međusobno razumijevanje diplomatskih pristupa u prevenciji, onemogućavanju, obrani i odgovoru na zlonamjerne kibernetičke aktivnosti. U studenom je u okviru EU organizirana vježba za testiranje alata iz instrumentarija kibernetičke diplomacije (Cyber Diplomacy Toolbox), koja je bila doprinos promišljanjima o boljem načinu primjene toolboxa, kao i jačanju zajedničke situacijske svjesnosti. Po prvi put su sudjelovali i predstavnici CSIRT i CyCLONe mreže te predstavnik NATO-a kao promatrač.

U organizaciji OSRH pravovremeno su provedene planske konferencije i druge pripremne aktivnosti za potrebe Cyber Coalition 2021 **vježbe**, uključujući i suradnju s drugim TDU te stručnjacima iz sfere akademske zajednice i privatnog sektora. Vježba je provedena u Talinu uz sudjelovanje tima i u Zagrebu. U 2021. je provedena i međunarodna vojna vježba MWCKE Adriatic Thunder (Zagreb). NCERT je u listopadu 2021. godine sudjelovao u vježbi Cyber SOPEx u organizaciji ENISA-e, Agencije Europske unije za kibernetičku sigurnost. Cilj vježbe bio je poboljšanje suradnje i komunikacije između CSIRT-ova EU-a.

Aktivnosti usmjerene na jačanje suradnje u području ***upravljanja rizicima europskih kritičnih infrastruktura*** su se provodile u okviru Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.

(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.

U programe ranog i predškolskog odgoja uvršteni su sadržaji vezani uz kibernetičku sigurnost. Kurikulum za nastavni predmet Informatike za osnovne škole i gimnazije u Republici Hrvatskoj donijet je 2018., a kurikulum za međupredmetnu temu Uporaba informacijske i komunikacijske tehnologije 2019. te se spomenute teme kontinuirano provode u nastavnome procesu. Organizirani su i provedeni stručni skupovi u pripremi viših savjetnika AZOO, dijelom s glavnom temom sigurnosti u kibernetičkom prostoru, a dijelom su se skupovi u svom radu osvrnuli na sadržaje sigurnosti u kibernetičkom prostoru.

Online državni stručni skupovi u kojoj su bile sadržane teme vezane za kibernetičku sigurnost:

- ciklus 4 državna skupa online na temu Izvanrednih okolnosti, tijekom godine sa po 800 – 900 sudionika;
- nastavak ciklusa od 9 webinara: Informatika u razrednoj nastavi, tijekom godine sa po 700 – 900 sudionika;
- Informatika u obrazovanju 2021. - Info@Edu X., 930 sudionika;
- Financijska i mirovinska pismenost, 24. - 25. veljače 2021. godine (oko 470 sudionika, svi odgojno-obrazovni djelatnici);
- Financijska i mirovinska pismenost (ponovljeni), 29. – 30. lipnja 2021.godine (oko 900 sudionika, svi odgojno-obrazovni djelatnici);
- Međužupanijski stručni skup "Edukacija edukatora i osnaživanje za promjene " za stručne suradnike pedagoge u dječjim vrtićima, osnovnim i srednjim školama teme vezane za nasilje putem interneta;
- Organizacija rada škole i napredovanje u zvanjima za Voditelje županijskih stručnih vijeća ravnatelja OŠ: Uvođenje digitalnih tehnologija u osnovne škole - izazov za ravnatelje.

U sklopu ESF-ova projekta Modernizacija sustava stručnog usavršavanja nastavnika strukovnih predmeta, Jačanje pedagoških i specifičnih metodičkih kompetencija razvijen je 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 sadrži: Uvod u sigurnost, upravljanje pristupom i sigurnost razvoja softvera; Planiranje kontinuiteta poslovanja i oporavka od katastrofe; Upravljanje informacijskom sigurnošću i upravljanje rizikom; Pravni propisi i usklađenost; Kriptografija; Sigurnosna arhitektura i dizajn; Telekomunikacije i sigurnost mreže.

U 2021. godini upisana su u Upisnik studijskih programa 4 nova studijska programa u području Tehničkih znanosti, polje Računarstvo:

- stručni preddiplomski studij Računarstvo i informatika, Sveučilište Sjever *(u ak. god. 2021/22 na studiju ima 39 studenata, od toga 22 redovita);*
- stručni preddiplomski studij Računarstvo, Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija (*u ak. god. 2021/22 na studiju ima 240 redovitih studenata);*
- specijalistički diplomski studij Graduate study in Computer Science (studij na engleskom jeziku), Visoko učilište Algebra *(novi studij koji se još nije počeo izvoditi);*
- sveučilišni diplomski studij Računarstvo, Sveučilište Jurja Dobrile u Puli (novi studij koji se *još nije počeo izvoditi)*.

U okviru prioritetnog područja P3: Poticanje razvoja kompetencija u prirodoslovno-matematičkom području (podpodručja Odgoj i obrazovanje za financijsku, digitalnu i medijsku pismenost i Razvijanje vještina i kompetencija u području tehnike te informacijskih i komunikacijskih tehnologija) Natječaja za dodjelu bespovratnih sredstava projektima udruga u području izvaninstitucionalnoga odgoja i obrazovanja djece i mladih financirano je 7 projekata organizacija civilnog društva.

Održano je državno natjecanje (WorldSkills Hrvatska) iz područja administracije IT sustava koja uključuje elemente kibernetičke sigurnosti (sudjelovalo je sedam učenika iz sedam srednjih strukovnih škola RH na Zagrebačkom velesajmu).

Nastavilo se s provedbom mjere sustavne izobrazbe državnih službenika. Jedan dio izobrazbe je već obuhvaćen državnim stručnim 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.

U MUP-u su tijekom 2021. godine u organizaciji Policijske akademije 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.

Pravosudna akademija od 2019. godine provodi projekt „Unaprjeđenje programa edukacija u borbi protiv kibernetičkog kriminala”. Cilj projekta 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 2021. godini održano je šest mrežnih seminara za osnovni modul te je ukupno sudjelovalo 130 polaznika. Također je održano šest mrežnih seminara za napredni modul te je ukupno sudjelovalo 90 polaznika. Održana su i dva specijalistička seminara na teme „Pretrage i

vještačenja“ i „Dostupnost računalnih/elektroničkih podataka“. Ukupno je sudjelovalo 38 polaznika. Ciljna skupina su bili suci, državni odvjetnici, savjetnici u pravosudnim tijelima i službenici u pravosuđu, kao i vježbenici.

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

- Pravno-jezični seminar „Suradnja u području suzbijanja kibernetičkog kriminala“, 2 polaznika;
- Seminar „Kibernetički kriminal i digitalni dokazi“, 2 polaznika;
- Seminar „Kibernetički kriminal i digitalni dokazi – osnove“, 2 polaznika.

U suradnji s Veleposlanstvom Sjedinjenih Američkih Država u Hrvatskoj, Uredom za razvoj prekomorskih pravosudnih sustava (OPDAT) Ministarstva pravosuđa SAD-a i Programom za međunarodno računalno hakiranje i intelektualno vlasništvo (ICHIP), Pravosudna akademija je organizirala četiri aktivnosti tijekom 2021. godine.

Na dva mrežna seminara (Digitalni dokazi, Kriptovalute), koji su organizirani u okviru djelovanja Regionalnog centra za edukaciju pravosudnih dužnosnika o suzbijanju kibernetičkog kriminala pri Pravosudnoj akademiji, ukupno je sudjelovalo 327 polaznika iz 11 država, od čega 53 iz Hrvatske.

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.

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

Definirane su potrebne izobrazbe i načini stjecanja znanja za zaposlenike i ustrojstvene cjeline pod nadležnošću i u potpori CERT-a MO 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 i 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 2021. godini tri djelatnika položila su certifikat za Certified Ethical Hacker – CEH i jedan djelatnik za Certified Devops engineer.

Za potrebe MORH-a, na Tehničkom veleučilištu Zagreb temeljem Ugovora o suradnji je proveden stručni specijalistički diplomski studij informacijske sigurnosti i digitalne forenzike za 4 polaznika.

U SAD-u su provedena školovanja:

- Cyber Security Fundamentals and Defence tečaj u SAD-u od 14. prosinca 2020. godine do 17. lipnja 2021. godine – jedan djelatnik;
- Izobrazba „Cyber Law & Hybrid Warfire (CLHW) pri Defence Institut for Internationa Legal Studies, Newpore, Rhode Island u SAD od 28. lipnja do 31. srpnja 2021. godine – jedan djelatnik.

Provedeni su i online tečajevi:

- International Marshall centers program on Cyber Security Studies (Garmish Parten Kirchen) u vremenu od 29. studenog do 16. prosinca 2021. godine;
- „Defending the Perimeter from Cyber Attacks“ u organizaciji NCIA-e u vremenu od 4. – 7. svibnja 2021. godine.

U 2021. godini HAKOM je nastavio s aktivnostima podizanja svijesti o važnosti kibernetičke sigurnosti objavljivanjem aktualnih novosti vezanih uz kibernetičku sigurnost putem društvenih mreža i svoje internetske stranice.

U veljači 2021. HAKOM je obilježio Dan sigurnijeg interneta sudjelujući u dva organizacijska programa, u čije se aktivnosti uključilo preko 900 hrvatskih škola, institucija i ustanova. Virtualna događanja bila su usmjerena na sigurnost najranjivijih skupina društva, djece i mladih, a posebni edukativni programi bili su organizirani i za one koji o njima skrbe: roditelje, učitelje, nastavnike i odgajatelje. Uoči obilježavanja Dana sigurnijeg interneta, u ponedjeljak, 8. veljače, HAKOM-ovi su stručnjaci u sklopu građanskog odgoja za učitelje i profesore održali izlaganje na temu „Svijet elektroničkih komunikacija i kako se zaštititi u njemu“. U sklopu programa Centra za sigurniji internet održan je ZOOM webinar za djecu i mlade pod nazivom „Gdje si ti u digitalnoj džungli?“, na kojemu su sudjelovali poznati Youtuberi koji su govorili o svojim iskustvima na internetu i odgovarali na pitanja koja su postavljali djeca i mladi. S udrugom Suradnici u učenju HAKOM se uključio u konferenciju *"Potraga za boljim internetom",* u sklopu koje je održano izlaganje na temu *"Kako se zaštititi u svijetu elektroničkih komunikacija". Dan sigurnijeg interneta* obilježen je i pravom potragom za boljim internetom – interaktivnom igrom u kojoj su sudjelovali učenici i učitelji koji su tražili i kritički procjenjivati informacije na internetu, rješavali zagonetke i mozgalice, otkrivali tajne šifre i razotkrivali lažne vijesti, a najbolji su i nagrađeni prigodnim poklonima. Jedan od zadataka potrage bilo je i traženje HAKOM-ove ažurirane brošure pod naslovom „*Kako se zaštititi u svijetu interneta i mobilnih telefona“.* Brošura je tradicionalno poslana u osnovne škole koje

su je razdijelile djeci i njihovim roditeljima, a sadrži praktične i korisne savjete o opasnostima i sigurnosti na internetu, zaštiti privatnosti i osobnih podataka, načinu ponašanja i odgovornoj uporabi društvenih mreža. Brošura je dio HAKOM-ovog programa informiranja djece i roditelja koji se od 2016. provodi suradnji s MZO. Održane su radionice o zaštiti djece na internetu za učitelje, nastavnike, djecu i roditelje.

U 2021. godini NCERT je nastavio s aktivnostima podizanja svijesti o kibernetičkoj sigurnosti objavljivanjem novosti, infografika i dokumenata na svom web sjedištu i društvenim mrežama Facebook i Twitter. Povodom Dana sigurnijeg interneta u suorganizaciji s udrugom Suradnici u učenju organizirana je konferencija „Potraga za boljim i sigurnijim internetom“ https://ucitelji.hr/potraga-za-boljim-i-sigurnijim-internetom/ na kojoj je predstavljena tema „Odgovorna zabava na internetu“. Izrađeni su interaktivni sadržaji na portalu https://naivci.hr/#Aktivnosti o temama iz kibernetičke sigurnosti za širu populaciju: digitalni trag, kibernetička higijena, netiketa, dobre lozinke, zlonamjerni sadržaji i dobre sigurnosne prakse. Provedena je kampanja „Veliki hrvatski naivci“ u listopadu tijekom Europskog mjeseca kibernetičke sigurnosti u kojoj su na nacionalnoj televiziji emitirana dva nova kratka video spota o žrtvama internetskih prevara https://www.youtube.com/watch?v=p9R35L85Pw0 i https://www.youtube.com/watch?v=OktltftS6sQ.

Informiranje i produbljivanje svijesti djece i mladih uključenih u sve razine formalnog obrazovanja, o potrebi brige o sigurnosti podataka te odgovornom korištenju informacijskih i komunikacijskih tehnologija se provodi u potpunosti.

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 2021. godini HNB je izdao 11 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.

U 1. kvartalu 2021. godine zabilježen je neovlašteni pristup (od strane nepoznatih napadača) sustavu jednog pružatelja IT usluga koji pruža usluge većem broju banaka u Hrvatskoj. HNB je bila u konstantnoj komunikaciji s bankama koje koriste usluge spomenutog pružatelja kako bi bila svjesna trenutne situacije. Dodatno je HNB organizirala pojedinačne sastanke s bankama koje koriste uslugu spomenutog pružatelja IT usluga te je od banaka tražila informacije o:

- procjeni utjecaja incidenta na njihovu instituciju,
- poduzetim aktivnostima,
- aktivnostima koje se planiraju poduzeti.

Također, HNB je sudjelovala na zajedničkim sastancima s pružateljem IT usluga te podržala banke u provođenju zajedničkog nadzora pružatelja IT usluga za koji je angažiran nezavisni revizor.

U srpnju 2021. HNB je organizirala radionicu za sve kreditne institucije vezano uz njihove obveze o izvješćivanju HNB-a o IKT incidentima te je najavila objavu Revidiranih smjernica o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2 koje stupaju na snagu od 1. siječnja 2022.

U prosincu 2021. nakon saznanja o kritičnoj ranjivosti u Java biblioteci log4j (CVE-2021-44228) HNB je uz poslano upozorenje prema svim kreditnim institucijama zatražila i dodatne informacije o:

- procjeni utjecaja i rizika kojima je institucija izložena zbog otkrivene ranjivosti,
- provedenim i planiranim aktivnostima u cilju ovladavanja rizikom,
- dodatnim saznanjima o mitigacijskim i/ili korektivnim mjerama koja se mogu podijeliti s ostalim kreditnim institucijama.

Nakon prikupljanja podataka, HNB je organizirala prezentaciju za sve kreditne institucije na kojoj je prikazala rekapitulaciju prikupljenih informacija te dala sažeti pregled preventivnih, korektivnih i reaktivnih aktivnosti u cilju ovladavanja rizikom.

Nadalje, HNB je u 2021. godini nadziranim institucijama uputila 100 dopisa i 16 okružnica te je održala 82 sastanaka s temama vezanima uz rizike korištenja informacijskih sustava.

U 2021. godini je NCERT nastavio s aktivnostima podizanja svijesti cjelokupne populacije o važnosti kibernetičke sigurnosti objavljivanjem aktualnih novosti iz svijeta kibernetičke sigurnosti i IKT tehnologije te sigurnosnih preporuka. Tijekom 2021. nastavljena je suradnja sa FER-om u pogledu pisanja i izdavanja stručnih dokumenata (objavljene su dvije recenzije alata i tri dokumenta). 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 2021. godini proveo kampanju za podizanje svijesti o važnosti kibernetičke sigurnosti u sklopu projekta Grow2CERT.

Kampanja pod nazivom „Veliki hrvatski naivci 2“ provedena je u listopadu tijekom Europskog mjeseca kibernetičke sigurnosti te su prikazana dva TV spota – o Danielu, žrtvi prevare na društvenim mrežama https://www.youtube.com/watch?v=OktltftS6sQ i Ivani koja preuzima zlonamjerni sadržaj s interneta https://www.youtube.com/watch?v=p9R35L85Pw0

Uz video sadržaje na web sjedištu https://naivci.hr/#Aktivnosti objavljeno je 10 različitih interaktivnih sadržaja koji sadrže teme o digitalnom tragu, kibernetičkoj higijeni, netiketi, zlonamjernom sadržaju i zaštiti na internetu.

NCERT je aktivan i na društvenim mrežama:

https://www.facebook.com/CERT.hr/

https://twitter.com/HRCERT

Tijekom 2021. NCERT je objavio ukupno 128 novosti na web sjedištu i društvenim mrežama.

Broj posjetitelja web sjedišta www.cert.hr je bio 163.634.

Broj posjetitelja web sjedišta www.naivci.hr je bio 127.763.

Broj pratitelja Facebook stranice je bio 1873.

Broj pratitelja Twitter stranice je bio 1314.

U studenom je održana panel rasprava „Koliko smo podložni manipulaciji?“, na kojoj su sudjelovali predstavnici javnih institucija, privatnog i bankarskog sektora te akademske zajednice. Raspravilo se o temama socijalnog inženjeringa, kibernetičkoj higijeni, otkrivanju osobnih i bankovnih podataka, podizanju svijesti o kibernetičkoj sigurnosti te lakovjernosti korisnika interneta u Hrvatskoj.

Sudionici rasprave su naglasili važnost brige o kibernetičkoj higijeni svakog korisnika interneta – od vrtića do starije životne dobi.

U listopadu 2021. godine provedeno je drugo CTF natjecanje Hacknite za srednje škole na kojem je sudjelovao 51 srednjoškolski tim iz 18 gradova i 32 srednje škole.

Objavljeni su sadržaji nacionalne koordinacije provedbe aktivnosti na europskoj razini tijekom Europskog mjeseca kibernetičke sigurnosti: brojne infografike i videospotovi dostupni na web sjedištu i društvenim mrežama NCERT-a:

Video „Što učiniti ako su vam ukradeni bankovni podaci?“

Video „Što učiniti ako nam netko preuzme virtualni identitet?“

Video „Kako je lako postati žrtva hakiranja?“

Infografike:

„Savjeti za zaštitu računa na društvenim mrežama“

„Savjeti za zaštitu na internetu“

„Savjeti za zaštitu računa“

Na službenim stranicama zajedničke europske inicijative uređena je stranica posvećena hrvatskoj publici https://cybersecuritymonth.eu/countries/croatia. Javna prisutnost NCERT-a je u stalnom porastu – brojna gostovanja na televiziji, radiju, tiskanim i digitalnim medijima.

U 2021. godini nastavljeno je s aktivnostima podizanja svijesti o važnosti kibernetičke sigurnosti. Od 2015. godine provodi se program koji uključuje podizanje svijesti učenika i roditelja o temi sigurnosti na internetu. 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 2021. godine. Zadnja revizija brošure obavljena je krajem 2021. za tisak brošure u siječnju 2022., a objavljena je na internetskoj stranici HAKOM-a. Promocija najnovije brošure uslijedit će u sklopu DSI2022. Zajedno s nakladnikom 24 sata promovirana je tema sigurnosti na internetu objavom native članka i informacijama o internetskoj stranici sini.hr, koja je rezultat inicijative u koju su uz HAKOM bili uključeni Centar za sigurniji internet i mobilni operatori. Tijekom godine redovito su se dijelili savjeti ili upozorenja oko kibernetičke sigurnosti na društvenim mrežama.

U ZSIS-u je nastavljena 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, Pravosudne akademije 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 i 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 Republici Hrvatskoj 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 Republike Hrvatske 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 Republike Hrvatske.

Hrvatsku zakladu za znanost (u daljnjem tekstu: Zaklada) osnovao je Hrvatski sabor posebnim zakonom u prosincu 2001. godine. Izmjenama i dopunama Zakona o Hrvatskoj zakladi za znanost[21] 2012. godine, Zaklada je postala središnje mjesto za financiranje znanstvenih projekata te projekata razvoja karijera mladih istraživača u ranoj fazi razvoja njihovih karijera. Hrvatska zaklada za znanost raspisuje godišnje natječaje za financiranje znanstvenih projekata, međutim natječaji nisu specijalizirani po pojedinim područjima već se raspisuju za sva područja znanosti jednako te se sredstva dodjeljuju temeljem transparentnog, višerazinskog evaluacijskog postupka.

U 2021. godini javna visoka učilišta i organizacije civilnog društva prijavila su pet znanstvenih ili znanstvenostručnih skupova koji su povezani s područjem informacijske i komunikacijske tehnologije, a koji su financirani od strane MZO:

- Skup „CECIIS 2021 (Central European Conference on Information and Intelligent Systems)“, organizator Fakultet organizacije i informatike, Varaždin;
- Skup „44. Međunarodni skup MIPRO 2021“, organizator Hrvatska udruga za informacijsku, komunikacijsku i elektroničku tehnologiju – MIPRO;
- Skup „Međunarodna znanstvena konferencija Economics of Digital Transformation - Economics and business of the post COVID-19 world“, organizator Ekonomski fakultet, Rijeka;
- Skup „6. međunarodna konferencija o pametnim i održivim tehnologijama“, organizator Fakultet elektrotehnike, strojarstva i brodogradnje, Split;
- Skup „MOTSP2021 (Management of Technology - Step to Sustainable Production)“, organizator Fakultet strojarstva i brodogradnje, Zagreb.

MZO je u 2021. godini dao podršku znanstvenom istraživanju analize mehanizama obrane od *Phishing* napada koje se provodi u okviru poslijediplomskog doktorskog studija kandidata koji je zatražio podršku MZO-u u provedbi istraživanja. Istraživanje će se provesti, između ostalog, i među dionicima akademske zajednice, a rezultati istraživanja će biti korišteni kao podloga za unaprjeđenje politika iz područja kibernetičke sigurnosti u akademskoj zajednici.

Služba za digitalno gospodarstvo MinGOR-a je posredstvom CEF Telekoma - financijskog instrumenta EU, otvorila mogućnost sufinanciranja digitalnih projekata gospodarskim

[21] NN 117/01, 45/09, 92/10, 78/12

subjektima i javnoj/državnoj upravi. Za projekte digitalizacije i automatizacije poslovnih procesa iz CEG Telekom sredstava za razdoblje 2014.-2021. bilo je namijenjeno 1 milijardu eura. Hrvatski gospodarski subjekti, državna i javna uprava te MinGOR bili su uspješni u povlačenju CEF sredstava. Najviše sredstava dobili su upravo projekti kibernetičke sigurnosti: Cybersecurity HR Projects, vrijednost ugovorenih projekata do 2019. = 3,516,420 EUR.

IV. ZAKLJUČAK

Nastavak provedbe Akcijskog plana tijekom 2021. godine rezultirao je daljnjim povećanjem sigurnosne svijesti na nacionalnoj razini i boljim razumijevanjem problematike kibernetičke sigurnosti u različitim institucijama i sektorima koji su uključeni u provedbu Akcijskog plana.

U području kritične komunikacijske i informacijske infrastrukture i upravljanju krizama očekuju se daljnja unaprjeđenja nakon donošenja Zakona o kritičnim infrastrukturama te transpozicije NIS2 direktive koja bi se trebala provesti 2023. - 2024.

U području obrazovanja i razvoja sigurnosne svijesti ostvaren je u proteklom razdoblju značajan napredak.

Dosadašnje iskustvo s provedbom Akcijskog plana u razdoblju od 2016. godine do danas jasno pokazuje potrebu aktivnog praćenja provedbe mjera iz Akcijskog plana jer su ključni rezultati u provedbi Akcijskog plana postignuti pod usmjeravanjem Vijeća.

Uvažavajući zahtjeve NIS2 direktive, koja definira elemente koje novim generacijama nacionalnih strategija kibernetičke sigurnosti države članice moraju obuhvatiti, kao i uzimajući u obzir nove prijetnje i rizike koji svakodnevno dolaze iz kibernetičkog prostora, Nacionalno vijeće za kibernetičku sigurnost se na svojoj 51. sjednici suglasilo o potrebi donošenja u cijelosti nove nacionalne strategije kibernetičke sigurnosti. Prijedlog nove strategije, a koja će se temeljiti na prepoznatim rizicima i projekciji potreba povećanja kibernetičke sigurnosti za sljedećih (najviše) 5 godina digitalne dekade, uz uvažavanje svih zahtjeva postavljenih NIS2 direktivom, planira se Vladi RH predložiti do kraja 2022. godine.