REPUBLIKA HRVATSKA
URED VIJEĆA ZA NACIONALNU SIGURNOST
NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2020. GODINI

Zagreb, rujan 2021.

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 povezano s aktivnostima Vijeća u 2020. godini prikazanim u Godišnjem izvješću o radu Vijeća u 2020. godini[2].

Izvješće o provedbi Akcijskog plana u 2020. 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 postići.

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

Područja kibernetičke sigurnosti:

A. Javne elektroničke komunikacije – 3 mjere
B. Elektronička uprava – 8 mjera
C. Elektroničke financijske usluge – 4 mjere
D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama – 13 mjera
E. Kibernetički kriminalitet – 5 mjera

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera
G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata – 5 mjera

[1] Odluka o osnivanu Vijeća objavljena je u Narodnim novinama broj: 61/2016, 28/2018, 110/2018, 79/19, 136/20
[2] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Godi%C5%A1nje%20izvje%C5%A1%C4%87e%20o%20radu%20Vije%C4%87a%20i%20Koordinacije%20u%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

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 samo nositelj većine mjera u području *D. Kritična komunikacijska i informacijska infrastruktura*.

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

1. Agencija za odgoj i obrazovanje (AZOO)
2. Agencija za strukovno obrazovanje i obrazovanje odraslih (ASOOO)
3. Agencija za zaštitu osobnih podataka (AZOP)
4. Hrvatska akademska i istraživačka mreža (CARNET)
5. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)
6. Hrvatska narodna banka (HNB)
7. Ministarstvo gospodarstva i održivog razvoja (MinGOR)
8. Ministarstvo obrane (MORH)
9. Ministarstvo pravosuđa i uprave (MPU)
10. Ministarstvo unutarnjih poslova (MUP)
11. Ministarstvo vanjskih i europskih poslova (MVEP)
12. Ministarstvo znanosti i obrazovanja (MZO)
13. Nacionalni CERT / CARNET
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 (SDU RDD)
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)

U 2020. g. pandemija COVID-19 uzrokovala je odstupanja u provedbi Strategije. Strategija se primarno oslanja na koordinaciju i usklađeno postupanje državnih tijela. Primjenom epidemioloških mjera značajno su se otežale sve zajedničke aktivnosti (vježbe, konferencije, koordinacije) stoga je izostala primjena pojedinih mjera ili su one provođene u manjem opsegu. 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, prikupljena su na standardiziranim obrascima od tijela koja su prema Akcijskom planu odgovorna kao nositelji provedbe predviđenih mjera.

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 je u ponudi 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 i 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 svim provedenim analizama u 2020. utvrđena je sukladnost s propisanim obvezama.

Nadalje, temeljem nacionalne procjene sigurnosnih rizika koji utječu na uvođenje 5G mreže, sukladno obvezi iz Preporuke o kibernetičkoj sigurnosti 5G mreža (EU) 2019/534 od 26. ožujka 2019. (radna skupina MMPI, MVEP, CARNET, UVNS, SOA, OTC, ZSIS, SDU RDD, HAKOM), te u konačnici 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., u 2020. analizirane su mjere koje je na nacionalnoj razini potrebno implementirati kako bi se doprinijelo sigurnosti 5G mreža. Utvrđeno je kako je većinu tehničkih mjera iz zbirke alata za ublažavanje mjera i podupirućih radnji (5G Toolboxa) potrebno implementirati u Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga koji donosi HAKOM, slijedom čega je u 2020. pokrenut postupak izrade nacrta novog Pravilnika.

Vezano uz obveze tajnog nadzora elektroničkih mreža i usluga, HAKOM je u 2020. nastavio suradnju s operativno-tehničkim tijelom nadležnim za aktivaciju i upravljanje mjerom tajnog nadzora elektroničkih komunikacija.

Nadalje, HAKOM provodi i inspekcijske nadzore vezane uz zaštitu privatnosti u elektroničkim komunikacijama što, između ostalog, obuhvaća nadzor nad operatorima u pogledu primijenjenih mjera zaštite osobnih podataka u elektroničkim komunikacijama, postupanja u slučaju eventualnih povreda osobnih podataka, povrede tajnosti elektroničkih komunikacija, postupanja s prometnim podacima te slanja neželjenih komunikacija. Nastavno, HAKOM je u 2020. proveo jedan inspekcijski nadzor vezan uz primjenu mjera zaštite osobnih podataka u elektroničkim komunikacijama te izdao mjeru u skladu sa svojim propisima.

Tehnička koordinacija regulatornog tijela za područje javnih elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti prije svega se **provodi u okviru rada Vijeća,** ali se provodi i u drugim sektorskim i međunarodnim okvirima. Tijela su sudjelovala u radnoj skupini za razvoj Projekta „Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti“, u dijelu prikupljanja i razmjene informacija o računalno-sigurnosnim incidentima i prijetnjama putem PiXi platforme. Podaci se razmjenjuju u i okviru Operativno-tehničke koordinacije za kibernetičku sigurnost, Koordinacije za sustav domovinske sigurnosti, u krugu tijela obveznika provedbe Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kao i s međunarodnim tijelima iz područja informacijske i kibernetičke sigurnosti.

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 utvrđenom Akcijskim planom. Dodatno, poduzete su i daljnje aktivnosti, u cilju upoznavanja ciljanih korisnika o dostupnosti ove usluge te podizanja svijesti o važnosti usvajanja danih preporuka. U okviru izvještajnog postupka iskazana je i usmjerenost na daljnje unaprjeđenje stanja te krajnju realizaciju u vidu sve većeg broja korisnika CIX-a.

(B) Elektronička uprava

Komunikacija državnih tijela s građanima sve više se odvija elektroničkim putem, stoga je daljnji razvoj elektroničke uprave - kojom se osigurava brza, transparentna i sigurna usluga svim građanima putem kibernetičkog prostora - strateški cilj RH.

Da bi se navedeno postiglo, nužno je uspostaviti 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 dvije – definirani su organizacijski i tehnički zahtjevi za povezivanje na državnu informacijsku infrastrukturu te je provedena analiza mogućnosti povezivanja državnih tijela klasificiranom mrežom i izrađen plan povezivanja koji se provodi u fazama**. Napravljen je i sljedeći korak te je u 2020. započela operativna uporaba klasificirane mreže.

Analiza postojećeg stanja u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora nije provedena, zbog relativno učestalih značajnih ustrojstvenih i kadrovskih promjena u strukturi relevantnih državnih tijela, kao niti utvrđivanje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica. **Iz istog razloga nije provedena analiza u svrhu donošenja kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica,** kojom će se obuhvatiti i kako procjena mogućnosti korištenja buduće elektroničke osobne iskaznice građana za potrebe elektroničke uprave i drugih javnih i financijskih usluga, tako i drugi aspekti povezani s nacionalnim mogućnostima za uspostavu odgovarajućih akreditacijskih i certifikacijskih sposobnosti u području kvalificiranih elektroničkih potpisa, sukladno EU zahtjevima.

Operator NIAS-a još nije započeo s izradom smjernica za primjenu sustava NIAS i odgovarajućih normi zbog postavljenih prioriteta u projektima „e-Poslovanje“ i „e-Pristojbe“. Uspostavljena je Radna skupina za analizu, standardizaciju i sigurnost mreža, kojoj je jedna od zadaća bila analizirati potrebe i mogućnosti povezivanja na državnu informacijsku infrastrukturu šireg kruga tijela javnog sektora te u skladu s rezultatima analize, izraditi preporuke za povezivanje na državnu informacijsku infrastrukturu ili uvođenje dodatnih mjera zaštite za informacijske sustave onih tijela javnog sektora koja nisu povezana na državnu informacijsku infrastrukturu. Bilo je potrebno definirati organizacijske i tehničke zahtjeve za povezivanje na državnu informacijsku infrastrukturu, uvjete i aktivnosti nužne za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostale elemente neophodne za rad državne informacijske infrastrukture, slijedom čega je donesena Uredba o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu (NN 60/17).

Izrada periodične procjene 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 u ovisnosti je o provedbi projekta povezivanja na Državnu informacijsku infrastrukturu, te se planira provesti u narednom razdoblju.

(C) Elektroničke financijske usluge

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

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

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

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

Smjernice o sigurnosti internetskih plaćanja izrađene su još 2015. g. te prezentirane širem krugu institucija bankarskog sektora, platnog prometa i najznačajnijih institucija odgovornih za elektronički novac. Provjera usklađenosti rada relevantnih institucija s odredbama Smjernica se provodi kroz supervizije i nadzorne mjere HNB-a. *Smjernice o sigurnosti internetskog plaćanja* zamijenile su *Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama* na temelju DirektiVe 8EU) 2015/2366 (Direktiva PSD2).

Provedba nacionalnih aktivnosti u području **sigurnosti mobilnih plaćanja**, u obliku opisanom Akcijskim planom, nije provedena jer je ovisila o postupcima Europske središnje banke i Europskog nadzornog tijela za bankarstvo, ali je sadržajno cilj mjere ispunjen kroz usvajanje i primjenu Delegirane Uredbe 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 i Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju Direktive (EU) 2015/2366 (Direktiva PSD2), koji na zadovoljavajući način adresiraju relevantno područje.

Druge dvije mjere Akcijskog plana, koje su odnose na **unapređenje razmjene i ustupanja podataka o nastalim računalnim sigurnosnim incidentima vezanima uz informacijske sustave te izvješćivanje o incidentima u cijelosti su provedene u 2018. godini**. Donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, tijekom 2018. godine dodatno je usklađen sektorski pristup i u području bankarstva s

nacionalnim pristupom kibernetičkoj sigurnosti. Pri tome je osigurana sukladnost bankarstva kao sektora ključnih usluga i s EU zahtjevima iz NIS Direktive i sa sektorskom regulativom bankarskog sektora. Osigurana je i potrebna suradnja institucija u sektoru bankarstva, u razmjeni podataka o sigurnosnim incidentima i koordinaciji nacionalnog rješavanja i odgovaranja na kibernetičke prijetnje. Ostvaren je i cjelokupni sustav povezivanja nacionalno nadležnih tijela za kibernetičku sigurnost s tijelima drugih EU država članica i nadležnim službama Europske komisije (EK), usklađujući se pri tome sa sektorskim regulativnim obvezama sektora bankarstva u RH i HNB-a u odnosu na zahtjeve i obveze prema Europskom nadzornom tijelu za bankarstvo (EBA)[5].

(D) Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

Sigurnost kritične komunikacijske i informacijske infrastrukture predstavlja jedno od pet prioritetnih područja Strategije. Vrlo teško je izdvojiti usluge koje ne ovise o potpori informacijskih sustava, a kada se radi o kritičnim uslugama nefunkcioniranje može dovesti do gubitka života, narušavanja zdravlja, ogromnih financijskih šteta i urušavanja državne uprave.

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.)
- 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.).

Transpozicijom NIS direktive u hrvatsko zakonodavstvo, odnosno donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18), ciljevi D.1 – D.3, u regulatornom smislu, kroz prepoznavanje nadležnih entiteta i mjera koje su dužni provesti, u velikoj mjeri su ispunjeni. Izmjenama Zakona o kritičnim infrastrukturama planira se kritičnu komunikacijsko-informacijsku infrastrukturu definirati kao horizontalnu komponentu nacionalne kritične infrastrukture, čime se otvara mogućnost usklađenog pristupa sigurnosti informacijskih sustava.

Sredinom 2020. godine prezentiran je novi koncept upravljanja kibernetičkim krizama. Isti je usuglašen na Vijeću i usvojen i na Koordinaciji za domovinsku sigurnost te je uključen u Plan

[5] https://www.hnb.hr/documents/20182/2220984/h-smjernice-izvjescivanje-o-incidentima-direktiva-2018-2366_PSD2.pdf

rada Operativno – tehničke koordinacije za 2020. godinu. Daljnju obavezu oko predmetnog područja i izrade standardnih procedura za nacionalno upravljanje kibernetičkim krizama je preuzela SOA, koja je u tu svrhu osnovala radnu skupinu za upravljanje kibernetičkim krizama. SOA je također razradila nacionalni koncept upravljanja kibernetičkim krizama te ga uskladila s aktualnim pristupom EU-a i NATO-a, a na temelju suglasnosti Vijeća SOA se kao nadležno tijelo RH u proljeće 2020. uključila u EU CyCLONe organizaciju za upravljanje kibernetičkim krizama. U svrhu usuglašavanja i razrade predloženog nacionalnog koncepta upravljanja kibernetičkim krizama, SOA je u listopadu 2020. formirala međuresornu stručnu radnu skupinu u koju su pozvani predstavnici ključnih tijela za predmetno područje (MORH/VSOA, MUP, ZSIS, NCERT, HAKOM i HNB).

(E) Kibernetički kriminalitet

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

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

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

Dostavljena izvješća o provedbi mjera pokazuju da su se **sve mjere u 2020. godini** (unaprjeđenje nacionalnog zakonodavnog okvira, unaprjeđenje i poticanje međunarodne suradnje, unaprjeđenje međuinstitucionalne suradnje radi brze razmjene informacija, jačanje ljudskih potencijala, poticanje i stalni razvoj suradnje s gospodarskim sektorom) **provodile u potpunosti ili većoj mjeri, kako je to utvrđeno Akcijskim planom**.

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

Predstavnici RH su u 2020. redovno sudjelovali u radu Odbora Vijeća Europe za praćenje primjene Konvencije o kibernetičkom kriminalitetu (T-CY Odbor). U 2020. predstavnik

DORH-a je sudjelovao na plenarnom sastanku Odbora Konvencije (T-CY) i dva plenarna sastanka za izradu (drugog) protokola uz Konvenciju (Protocol Drafting Plenary).

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. Tijekom 2020. predstavnici MPU zajedno sa SPRH, u okviru hrvatskog predsjedanja Vijećem EU, ulagali su napore pri nastojanjima da EP usvoji neophodno Izvješće kako bi se s trijalogom moglo započeti čim prije (stupanje u neformalne kontakte s Europskom komisijom (EK), *like-minded* skupinom unutar Vijeća i LIBE Odborom; formalno pismo u ime HRPRES2020 upućeno je izvjestiteljici LIBE Odbora). Predstavnici MPU i po završetku HRPRES2020 sudjeluju na svim sastancima radne skupine COPEN na temu unutarnjeg zakonodavnog paketa e-dokaza.

EK je u siječnju 2020. organizirala završnu konferenciju EXEC-a (01.02.2018.–01.02.2020.) pod nazivom „Digitalna prekogranična suradnja u kaznenom pravosuđu (‘Digital Cross-Border Cooperation in Criminal Justice’ Conference), kojoj je cilj bio okupiti dionike koji aktivno rade na poslovima koji uključuju elektroničku prekograničnu pravosudnu suradnju u kaznenim stvarima te kako bi upoznala širu zainteresiranu zajednicu s razvojem uspostave sigurne internetske platforme za razmjenu e-dokaza. Predstavnici MPU sudjelovali su i na navedenoj konferenciji održali prezentaciju o svojim postignućima u okviru projekta EXEC (Elektronička razmjena e-dokaza korištenjem tehničkih komponenti e-Codexa), te iskoristili priliku pozvati koordinatora projekta EXEC (AT) i predstavnike EK da na sastanku CATS-a u veljači 2020. za vrijeme HRPRES2020 predstave projekt i ishod spomenute konferencije. Nadalje, MPU se, nakon uspostavljanja nacionalnog konektora koji je neophodan za elektroničko povezivanje s pravosudnim tijelima drugih država članica EU preko zajedničke platforme u svrhu razmjene e-dokaza, uključio u projekt EXEC II (trajanje: 24 mjeseca počev od 01.10.2020.) kojim se nastavlja s radom i aktivnostima potrebnim za uspješnu integraciju nacionalnih sustava e-Spis i CTS s e-EDES-om (e-Evidence Digital Exchange System).

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

- Kontakt točke uspostavljene odredbom čl. 13. Direktive 2013/40/EU o napadima na informacijske sustave. Uredbom Vlade RH o preuzimanju Direktive 2013/40/EU o napadima na informacijske sustave te direktive 2014/62/EU o kaznenopravnoj zaštiti eura i drugih valuta od krivotvorenja određena je ustrojstvena jedinica MUP-a za suzbijanje kibernetičkog kriminaliteta kao operativna nacionalna kontakt točka za razmjenu informacija o kaznenim djelima protiv računalnih sustava, programa i podataka. Imenik kontakt točki vodi EK, kojoj su dostavljeni slijedeći podaci o hrvatskoj kontakt točki:

Služba kibernetičke sigurnosti, Kriminalističko-obavještajni sektor, Uprava kriminalističke policije.

- Kontakt točku G7 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 2020. godine MUP redovno šalje zahtjeve prema drugim državama te prima zahtjeve drugih država, te nema poteškoća u provedbi, dok SOA kroz uspostavljenu međunarodnu suradnju aktivno razmjenjuje informacije s ciljem prevencije, brzog oporavka i odgovora u slučaju ugroze kibernetičkog prostora RH usmjeravajući se pri tome primarno na državno sponzorirane kibernetičke napade i APT kampanje. 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. Također, odlukom Vlade RH iz rujna 2019., ZSIS je određen Nacionalnim tijelom za kibernetičku sigurnosnu certifikaciju te od tada daje predstavnika Republike Hrvatske u Europskoj skupini za kibernetičku sigurnosnu certifikaciju („ECCG“) s pravom glasa.

Međunarodna suradnja Nacionalnog CERT-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 Nacionalni CERT akreditirani član, te članstvom u Mreži CSIRT-ova (CSIRT Network) koja je nastala temeljem direktive o mrežnoj i informacijskoj sigurnosti (NIS direktiva). U 2020. godini, za vrijeme predsjedavanja RH Vijećem EU, sastanak CSIRT mreže trebao se održati u Zagrebu, no zbog pandemije COVID-19 sastanak se po prvi puta održao virtualno. Hrvatska je bila uspješna u održavanju virtualnog sastanka te se taj trend nastavio i dalje.

U DORH je, **u okviru međunarodne pravne pomoći i pravosudne suradnje vezano za kibernetički kriminalitet** kao kontakt točka za mrežu "Cybercrime Eurojust", određen je 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 općinskom državnom odvjetništvu u Zagrebu, upućena na rad u državno odvjetništvo RH te u predmetima kibernetičkog kriminaliteta kao nacionalni predstavnik RH u Europskoj

pravosudnoj mreži usmjerava i žurno prosljeđuje zamolbe za međunarodnu pravnu pomoć i suradnju prema zemljama članicama Europske unije i drugim zemljama.

Osim kontakt točaka uspostavljenih u okviru međunarodne suradnje, uspostavljen je i nacionalni sustav koordinatora, sa svrhom prevencije i efikasnijeg rješavanja incidenta na nacionalnom nivou. U MUP-u kontakt točka za razmjenu informacija i koordinaciju postupanja s drugim nacionalnim tijelima je Služba kibernetičke sigurnosti. Tijekom 2020. godine ostvarena je suradnja na konkretnim slučajevima istraživanja kibernetičkog kriminaliteta sa ZSIS-om i Nacionalnim CERT-om. MUP i Nacionalni CERT 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.
Suradnja tijela se odvija i u okviru Koordinacije koja je u 2020. godini održala 10 sastanaka.
U DORH-u je stalna kontakt točka zamjenik Glavne državne odvjetnice RH, Ured glavne Državne odvjetnice RH radi preveniranja i učinkovitog rješavanja incidenata na nacionalnoj razini.

Sukladno Uredbi o izmjenama i dopunama uredbe o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 129/2017), **Služba kibernetičke sigurnosti u MUP-u sudjeluje u primjeni i razvoju nacionalnog zakonodavnog okvira kibernetičke sigurnosti**; sudjeluje u aktivnostima i mjerama u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora; sudjeluje u uspostavi učinkovitih mehanizama razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru; aktivno djeluje na jačanju svijesti o sigurnosti svih korisnika kibernetičkog prostora; 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) te predlaže rješenja na planu podizanja 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 Ministarstva, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada; sudjeluje u planiranju i izradi programa obuke i specijalizacije policijskih službenika 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.

U odnosu na ciljeve i mjere, 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: *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 iznosi 995.000,00 EUR s PDV-om, dok postotak EU sufinanciranja iznosi 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 tako što će se putem specijaliziranog forenzičkog softvera i hardvera izraditi forenzičke kopije sadržaja memorije predmeta koji se pretražuju, navedene kopije pohranit će se na poslužiteljima, nakon čega će se obavljati analiza sadržaja. Projektom se planira financirati nabava svih postojećih licenci za forenzičke softvere, koje su do sada svake godine financirane proračunskim sredstvima MUP-a, te nabava licenci, koje MUP do sada nije posjedovao, a neophodne su obavljanje poslova digitalne forenzike.
2. *Provođenje edukacijskih modula na temu digitalnih dokaza i forenzičkih metoda i procedura za 31 policijskog službenika*
   Edukacija policijskih službenika odvijala se krajem 2019. i početkom 2020. godine, a obuhvatila slijedeće teme:
   1. Osnove napada i zaštite informacijskih sustava i informacijska sigurnost
   2. Arhitektura, modeli, mehanizmi i načela informacijske tehnologije
   3. Digitalni tragovi, dokazi i forenzika
   4. Prevencija, nadzor i specijalizirana područja kibernetičkih napada

SOA kontinuirano brine o jačanju ljudskih potencijala te razvoju i nadogradnji forenzičkih alata i sustava, kao i sustava za tajni nadzor elektroničkih mreža i usluga. U tom cilju SOA, **u suradnji sa ZSIS-om, provodi projekt SK@UT** koji obuhvaća izgradnju sustava za ranu detekciju, praćenje i zaštitu od državno sponzoriranih kibernetičkih napada i APT kampanja putem distribuirane mreže senzora u ključnim državnim tijelima. Implementacijom sustava SK@UT u državnim tijelima, daje se dodatni poticaj ovim tijelima kao korisnicima sustava SK@UT, za razvoj kompetencija svojih kapaciteta u području

kibernetičke sigurnosti. Tijekom 2020. godine napravljene su pripreme za daljnje proširenje opsega sustava SK@UT i time vidljivosti nacionalnog kibernetičkog prostora.

Unaprjeđene su postojeće i razvijene nove tehničke mogućnosti sustava za provođenje posebnih dokaznih radnji propisanih Zakonom o kaznenom postupku, koje su primjenjive i za kaznena djela iz domene računalnog kriminaliteta.

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.

U ožujku 2019. godine u sklopu projekta GrowCERT Nacionalni CERT održao je dvije radionice za gospodarski sektor. Teme pokrivene radionicama su bile zakonski i institucionalni okviri, vrste kibernetičkih napada i njihove posljedice, mjere zaštite, svijest o kibernetičkoj sigurnosti te poslovni aspekti sigurnosti. Osim toga, u sklopu navedenog projekta izrađeni su edukacijski materijali (brošure, letci i digitalni materijali i sadržaji) koji su podijeljeni na HUB, HGK, Admiral Casino, HEP, HPB i ostalim zainteresiranim gospodarskim subjektima.

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 (NN 30/2018 dalje: ZZNITV), u nadležnosti Državnog zavoda za intelektualno vlasništvo, **zaštita poslovne tajne** kao značajnog ekonomsko-pravnog instituta usklađena je sa zakonodavstvom EU (Direktiva EU 2016/943 Europskog parlamenta i Vijeća od 08. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija poslovne tajne od nezakonitog pribavljanja, korištenja i otkrivanja i Direktiva 2004/48/EZ Europskog parlamenta i Vijeća od 29. travnja 2004. o provedbi prava intelektualnog vlasništva). Definicija poslovne tajne, sukladno navedenom, je jasnije i šire definirana, dok se sama poslovna tajna počinje tretirati kao jedan oblik intelektualnog vlasništva nositelja poslovne tajne.

U odnosu na mjeru **uspostave redovitih koordinacijskih aktivnosti nacionalnih tijela nadležnih za pojedine skupine zaštićenih podataka, radi razmjene iskustava, detektiranja problema i/ili potencijalne neujednačenosti u primjeni propisa, te izrade analize i preporuka za njihovo rješavanje**, AZOP je angažiran u aktivnostima praćenja i provedbe primjene Opće uredbe o zaštiti podataka (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) posebice u dijelu aktivnosti usmjerenih na provođenje istraga o primjeni Opće uredbe o zaštiti podataka kao i kontinuiteta osvješćivanja i edukacije voditelja i izvršitelja obrade osobnih podataka kao i samih ispitanika tj. građana (budući da se predmetna Uredba izravno i obvezujuće primjenjuje u državama članicama od 25.05.2018. godine), dok Ured Vijeća za nacionalnu sigurnost, uvažavajući sve specifičnosti tijela u odnosu na štićene podatke (klasificirane i neklasificirane-službene), održava redovite bilateralne konzultacije i koordinacijske aktivnosti.

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 Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga dio usluga koje se nude i podliježu zaštiti odnosno procesima nadzora definiranim u Uredbi o kibernetičkoj sigurnosti i operatora ključnih usluga i davatelja digitalnih usluga.

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 tijekom 2020. godine proveden je u znatnoj mjeri te su izrađeni predlošci za svaku zaštićenu kategoriju podataka te određene skupine klasificiranih i neklasificiranih podataka, koji bi trebali dati odgovarajuću podlogu za kvalitetniji i sigurniji rad/postupanje te ih olakšati i ujednačiti kao i u samoj provedbi kod obveznika primjene.

U ZSIS-u je **završena interna analiza iskustava u korištenju palete normi HRN ISO/IEC 27000** kroz iskustva i aktivnosti ZSIS-a u korištenju ove palete normi u postupku sigurnosnih akreditacija informacijskih sustava.

Uz navedeno, ZSIS je prepoznao potrebu uvezivanja ove zadaće s cjelokupnim legislativnim okvirom (nacionalnim i EU) koji je donesen ili se planira donošenje.

ZSIS je 31. prosinca 2020. donio „Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava“ koji se temelji na normi HRN ISO/IEC 27001.

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.

Mjera Akcijskog plana u okviru čije realizacije je potrebno ***definirati taksonomije, pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostaviti platformu ili tehnologiju za razmjenu podataka*** provedena je u potpunosti.

U cilju provedbe Mjere osnovana je radna skupina čiji su članovi, uz nositelje, naknadno dodana tijela sukladno potrebi za razvoj platforme PiXi. Radna skupina trenutno se sastoji od 11 tijela a to su FER, HAKOM, HANFA, HNB, HUB, MINGOR, MORH, MUP, NCERT, SDURDD i ZSIS. Radna skupina koja je aktivna od 2017. godine do danas, izradila je i objavila Nacionalnu taksonomiju računalno-sigurnosnih incidenata[6] koja je u ožujku 2019. godine bila i ažurirana zbog pojave novih vrsta incidenata i zbog zahtjeva iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.
Mjera u okviru koje sektorski nadležna tijela **prikupljaju podatke o incidentima** od dionika, poput regulatora i drugih CERT-ova iz njihove sektorske nadležnosti **uz objedinjavanje na**

[6] https://www.cert.hr/wp-content/uploads/2019/04/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf

sektorskoj razini te razmjenu anonimiziranih podataka o incidentima provodi se u znatnoj mjeri.

Nositelji mjere prikupljaju podatke u okviru svojih sektora nadležnosti, uspostavljena je razmjena podataka između sektorski nadležnih tijela sukladno dogovorenoj taksonomiji i protokolu iz mjere G.1.1.[7] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga dodatno i precizno utvrđuje sektorske obaveze u sektorima koji su od ključnog interesa za područje kritične informacijske i komunikacijske infrastrukture.

HNB je 1. travnja 2020. (a uzimajući u obzir pandemiju COVID-19, ali i posljedice potresa u Zagrebu), uspostavila privremeni mehanizam izvješćivanja o problemima odnosno poteškoćama u pružanju usluga koje se klijentima izravno pružaju elektroničkim kanalima. Navedene usluge obuhvaćaju bankomate, EFTPOS uređaje, internetsko bankarstvo, mobilno bankarstvo, e-commerce i PSD2 sučelja. Tim mehanizmom kreditne institucije trebaju HNB izvješćivati o problemima vezanima uz funkcionalnost, dostupnost ili sigurnost navedenih usluga/sučelja. Pri tome bi izvješćivanjem trebalo obuhvatiti i manje probleme u radu, o kakvima kreditne institucije inače ne bi izvješćivale HNB u skladu s propisanim uvjetima izvješćivanja o incidentima. Cilj uspostavljenog privremenog mehanizma izvješćivanja jest osiguravanje primjerene i pravovremene informiranosti supervizora.
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.

Na sastancima Koordinacije izvještava se o incidentima iz prethodnog razdoblja, te Koordinacija obavještava Vijeće. Osim toga, Nacionalni CERT periodično šalje mjesečni izvještaj o sigurnosnim incidentima zainteresiranim tijelima.
HNB na temelju informacija o računalno sigurnosnim incidentima koje zaprimi kroz suradnju s drugim nacionalnim i EU tijelima dostavlja informacije relevantnim dionicima unutar sektora. HNB redovito ažurira listu institucionalnih primatelja.

Aktivnosti u provedbi mjere usmjerene na **izdavanje upozorenja o uočenim sigurnosnim ugrozama i trendovima** te odgovarajućih preporuka za postupanje, **provode se u potpunosti**. Nadležna tijela izdavala su upozorenja i preporuke, a intenzivirana je i suradnja u okviru Koordinacije.

[7] Definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka.

Nacionalni CERT je kao nositelj mjere u 2019. godini izdao četiri upozorenja, a u 2020. godini 12 upozorenja putem web sjedišta www.cert.hr, Facebook stranice CERT.hr i Twitter računa HRCERT. U 2019. godini izdano je 2999, a u 2020. 3682 sigurnosnih preporuka.
HNB kao sunositelj navedene mjere u 2019. godini izdao je 7 objava svim kreditnim institucijama o uočenim sigurnosnim ranjivostima te preporuke za daljnje postupanje. U 2020. godini HNB je izdao 24 objave svim kreditnim institucijama o uočenim sigurnosnim ranjivostima te preporuke za daljnje postupanje.
ZSIS je kao sunositelj mjere u 2019. godini izdao 4 javna upozorenja putem web sjedišta www.zsis.hr, dok ih je tijekom 2020. izdao 8 te je 86 puta izdao preporuke rješavajući sigurnosne incidente na neklasificiranim sustavima državnih tijela tijekom 2019. dok je u 2020. zabilježeno 113 preporuka.
HAKOM kao sunositelj mjere izdao je 5 upozorenja/preporuka za postupanje putem društvenih mreža (od kojih je jedno podijeljeno s CERT.hr Facebook stranice) u 2019. godini, a u 2020. 25 upozorenja/preporuka za postupanje (CERT.hr - 6). Na web sjedištu je tijekom 2020. objavljeno jedno upozorenje s preporukom.

Uspostava i održavanje periodičkih (ili po potrebi češćih) koordinacija vezano uz **razmjenu iskustava i znanja te informacija o sigurnosti kibernetičkog prostora RH** do kojeg su došla tijela kaznenog progona i sigurnosno obavještajnog sustava, mjera je Akcijskog plana koja se **provodi u potpunosti**. Provođenje ove mjere vidljivo je kroz smanjenja vremena potrebnog za otkrivanje računalno-sigurnosnih incidenata te u vremenu odziva na incident i otklanjanja ugroze, kao i u preventivnom djelovanju.

Policijski službenici Službe kibernetičke sigurnosti MUP-a su tijekom 2020. godine u dva navrata tijekom složenih kriminalističkih istraživanja surađivali sa SOA-om, ZSIS-om i Nacionalnim CERT-om, čiji su djelatnici pružali stručnu i tehničku pomoć prilikom obavljanja forenzičkih analiza digitalnih dokaza.

(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.

Provedba mjera koje su trebale rezultirati uspostavom ***koordinacije za jačanje i širenje međunarodne suradnje u području kibernetičke sigurnosti***, povećanju broja sudjelovanja u i organiziranja međunarodnih aktivnosti vezanih uz ***razvoj međunarodnog pravnog okvira kibernetičke sigurnosti,*** tijekom 2020. godine uključivala je minimalno informiranost na strateškoj razini.

Zbog obveza koje su proizlazile iz predsjedanja RH Vijećem Europske Unije tijekom prve polovine 2020. godine kao i zbog posebnih otegotnih okolnosti izazvanih pandemijom COVID-19, a potom i potresa, Stalna radna skupina za međunarodne aktivnosti nije održavala fizičke sastanke te je većina potrebnih aktivnosti svedena na redovnu (i pretežito elektroničku) komunikaciju bilo kroz djelovanje samog Vijeća, slanjem informacija elektroničkom poštom ali i organizacijom virtualnih brifinga, kao što je i bilo inicijalno planirano.
I bez navedenih otegotnih okolnosti, poseban izazov u radu predstavljalo je značajno povećanje dinamike aktivnosti na međunarodnom planu pri čemu nije došlo do značajnijih pomaka zbog relativno limitiranih kadrovskih kapaciteta institucija.

MVEP je nastojao što redovnije informirati o aktivnostima na kojima se **razvija međunarodni pravni okvir kibernetičke sigurnosti**. Kao i ranije, u tom smislu posebno aktivno bilo je Stalno predstavništvo RH u Bruxellesu i radu na jačanju relevantnog EU *acquisa* (nova EU Strategija kibernetičke sigurnosti te prijedlog revidirane NIS 2.0 direktive, Uredba o centrima kompetencije u području kibernetičke sigurnosti itd.), uključujući i Stalne misije RH pri UN u New Yorku (pitanja s dnevnog reda Prvog i Trećeg odbora, te rada UNGGE i OEWG radnih skupina kao i priprema za početak rada posebne *Ad hoc* Radne skupine UN-a za izradu novog međunarodnopravnog instrumenta na području kibernetičkog kriminala.
Tijekom HRPRES2020 po prvi puta je pokrenut sankcijski režim EU vezan za maliciozne kibernetičke aktivnosti, čime je konačno zaokružen Okvir za zajednički diplomatski odgovor na zlonamjerne kibernetičke aktivnosti („*diplomatic toolbox*“).
Pored navedenog, RH je sudjelovala (preko ŽDORH, MPU i MUP) i u radu nadležnog Odbora Vijeća Europe (T-CY) na izradi Drugog protokola na Budimpeštansku konvenciju o kibernetičkom kriminalu.

Početkom 2020. u organizaciji UVNS-a u Zagrebu, **s ciljem poticanja o pomaganja bilateralne i multilateralne suradnje u okviru postojećih i budućih sporazuma**, održane su bilateralne konzultacije s delegacijama Crne Gore i SAD-a. Tijekom HRPRES2020 dodatno su valorizirani visokokvalitetni odnosi s drugim državama članicama EU te je RH sve češće pozivana sudjelovati u neformalnim konzultacijama i drugim tipovima sastanaka po pojedinim pitanjima kibernetičke sigurnosti. **Istovremeno, kroz cijelu 2020. godinu RH aktivno sudjeluje u raspravama i dogovorima oko zajedničkih pozicija država članica EU** i partnera u kontekstu aktualnih zbivanja, a osobito u kontekstu rada Ujedinjenih naroda, gdje je RH također postala dijelom PoA inicijative koja zagovara objedinjavanje dvaju (UNGGE i OEWG) procesa.

Aktivnosti usmjerene na jačanje suradnje u području **upravljanja rizicima europskih kritičnih infrastruktura** u ovisnosti su od procesa koji se u RH provodi u području zaštite kritične infrastrukture, gdje još nije završena identifikacija kritične infrastrukture. Ovo je pitanje djelomično riješeno (u 7 sektora) donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te pripadajućom Uredbom, ali u manje sektora nego što ih je Zakonom o kritičnim infrastrukturama identificirano (11) i samo u području kritične informacijske i komunikacijske infrastrukture. Do potpune identifikacije kritične infrastrukture neće biti moguće provoditi aktivnosti u svim identificiranim sektorima predviđene Akcijskim planom u okviru opisane mjere.

Sudjelovanje RH (ponajprije putem MVEP-a) u aktivnostima OESS-ovih *Comm-check* vježbi za provedbu mjera za izgradnju povjerenja (CBMs), a u kojima je RH i tijekom 2020. 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). Time je **sudjelovanje u diplomatskim aktivnostima u okviru međunarodnih organizacija i drugih foruma radi davanja doprinosa RH aktivnostima usmjerenima na izgradnju povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija,** provedena u znatnoj mjeri.

Sudjelovanje i organizacija međunarodnih civilnih i vojnih vježbi i drugih stručnih programa tijekom 2020. u značajnoj je mjeri odstupala od planiranog, primarno zbog posljedica i restrikcija uzrokovanih pandemijom COVID-19 virusa. U međunarodnoj NATO vježbi "Cyber Coalition 2020" sudjelovali su sudjelovali predstavnici MORH-a, MUP-a, NCERT-a, ZSIS-a, SOA-e, VSOA-e i HAKOM-a.
Vježba je obuhvaćala obranu od zlonamjernog sadržaja (eng. malware) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom, a čiji je koordinator bio CARNET.

Predstavnici Nacionalnog CERT-a po prvi su puta sudjelovali u International CyberEx-u, CTF natjecanju u organizaciji OAS-a (Organization of American States), INCIBE (Spanish National Cybersecurity Institute) i CNPIC-a (Spanish National Centre for Infrastructure and Cybersecurity), čiji je cilj jačanje sposobnosti odgovora na računalno-sigurnosne incidente. Natjecanje, „CTF jeopardy", se održalo 10. rujna 2020. godine. Za natjecanje su se smjeli prijaviti isključivo nacionalni CERT-ovi i CSIRT zajednice, te su organizatori odabrali 81 tim koji se natjecao. Tim iz Nacionalnog CERT-a osvojio je 11. mjesto. Zadaci su bili iz područja kriptografije, digitalne forenzike, reverznog inženjerstva, web sigurnosti i sličnih područja.

(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 se 22 mjere trebaju provoditi kontinuirano.

U aktivnostima za provedbu mjere kojom **u programe ranog i predškolskog odgoja treba uvrstiti sadržaje vezane uz kibernetičku sigurnost** provodi se u potpunosti.

Mjere, u okviru kojih je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije **potrebno uvrstiti sadržaje vezane uz kibernetičku sigurnost u osnovnoškolske i srednjoškolske programe obrazovanja** u cijelosti su provedene. Među odgojno-obrazovnim ciljevima učenja i poučavanja aktivnosti su se provodile unutar sljedećih kurikuluma: Priroda i društvo za osnovne škole, Talijanski jezik za osnovne i srednje škole, Likovna kultura za osnovne škole, Srpski jezik za osnovne i srednje škole, Informatike za osnovne škole i gimnazije, Francuski jezik za osnovne škole i gimnazije, Latinski jezik za osnovne škole i gimnazije i Katolički vjeronauk za osnovne i gimnazije.

Sadržaji su uvršteni i u međupredmetne teme: *Osobni i socijalni razvoj* za osnovne i srednje škole, *Uporaba informacijske i komunikacijske tehnologije* za osnovne i srednje škole, *Zdravlje* za osnovne i srednje škole i *Održivi razvoj* za osnovne i srednje škole.

Vezano uz **programe na visokoškolskoj razini uvrstiti sadržaje vezane uz kibernetičku sigurnost**, provedba nije započela, uvažavajući članak 4. Zakona o znanstvenoj djelatnosti i visokom obrazovanju (Narodne novine, broj: 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15, 131/17), kojim su akademskoj zajednici zajamčene akademske slobode koje uključuju i samostalno utvrđivanje i provođenje obrazovnih, znanstvenih, umjetničkih i stručnih programa. Dakle, kreiranje i donošenje kurikuluma u visokom obrazovanju u isključivoj je nadležnosti visokih učilišta koja samostalno odlučuju o sadržajima i ishodima učenja koje će uključiti u svoje studijske programe te ih MZO ne može obvezati na implementaciju određenih sadržaja, pa tako i sadržaja vezanih uz kibernetičku sigurnost.

S**adržaji vezani uz kibernetičku sigurnost uvršteni su u kolegije na studijima tehničkih fakulteta ili u jednom dijelu studija drugih visokih učilišta** kroz kolegije vezane uz

informacijsku sigurnost. Međutim, i nadalje najveći dio visokih učilišta u svojim studijskim programima **nema** uvršten sadržaj vezan uz kibernetičku sigurnost. Broj kolegija vezanih uz kibernetičku sigurnost ovisi, između ostalog, i o interesu šire društvene zajednice te poslodavaca koji traže specifična znanja vezana uz kibernetičku sigurnost. S obzirom na autonomiju sveučilišta i visokih učilišta, ***potrebno je u narednom razdoblju uložiti dodatne napore radi poticanja sveučilišta i visokih učilišta da u svoje studijske programe uvrste ove tematske sadržaje***, ističući dobre primjere sveučilišta i fakulteta koji to čine i planiraju provesti, uz istovremeno osvješćivanje društvene zajednice o važnosti kibernetičke sigurnosti, kao i poslodavaca o važnosti ovih specifičnih znanja.

Aktivnosti u provedbi mjere kojima se osigurava ***sustavno obrazovanje učitelja, nastavnika, ravnatelja i stručnih suradnika, kao i djelatnika visokih učilišta***, osobito onih koji rade na predmetima s uključenim sadržajima kibernetičke sigurnosti **provode se u potpunosti**. MZO je organiziralo savjetničke posjete za učitelje, nastavnike, stručne suradnike i ravnatelje te Webinare edukacije učitelja kako bi se upoznali sa svim mogućnostima korištenja informacijsko - komunikacijske tehnologije i u suradnji s AZOO nastavlja pružati podršku svim odgojno-obrazovnim djelatnicima.

Poticanje uspostavljanja i izvođenja diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti provodi se u znatnoj mjeri. U razdoblju od 2018. do 2020. g. uspostavljeno je 5 novih studijskih programa s ishodima učenja u području kibernetičke sigurnosti na visokim učilištima u Republici Hrvatskoj: specijalistički diplomski stručni studij *Informacijska sigurnost i digitalna forenzika* na Tehničkom veleučilištu u Zagrebu (2018.) – 75 polaznika, preddiplomski stručni studij *Računarstvo* na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija Sveučilišta u Osijeku (2018.) – 175 polaznika, preddiplomski sveučilišni studij *Računarstvo* na Sveučilištu Jurja Dobrile u Puli (2018.) – 76 polaznika, poslijediplomski sveučilišni specijalistički studij *Domovinska sigurnost* na Sveučilištu u Zagrebu (2020.), te preddiplomski sveučilišni studij *Cyber komunikacije i znanosti o mreži* na Sveučilištu VERN (2020.) – 17 polaznika.

Poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja provodi se u potpunosti. Svi učenici razredne nastave mogu odabrati izbornu informatiku. Za nastavu izborne informatike predviđeno je 70 sati nastave godišnje. Za tu namjenu u 2019. godini utrošeno je za dodatno opremanje 1.137 područnih škola 15.334.000 kuna. Sredstva su se namjenski dodijelila matičnim osnovnim školama koje su samostalno provodile nabavu hibridnih računala za područne škole.

Aktivnosti u provedbi mjere **poticanje organiziranja natjecanja u području informacijske sigurnosti provode se u znatnoj mjeri**. Održano je i državno natjecanje (WorldSkills Hrvatska) iz područja administracije IT sustava koja uključuje elemente kibernetičke sigurnosti (sudjelovalo je 8 učenika iz 8 srednjih strukovnih škola RH na Zagrebačkom velesajmu).

Mjera **uvrštavanje teme informacijske sigurnosti u programe sveučilišta kroz programske ugovore** nije provedena. Odlukom Vlade RH o programskom financiranju javnih visokih

učilišta u Republici Hrvatskoj u ak. g. 2018./2019. - 2021./2022. (Narodne novine, broj 87/2018.) utvrđen je četverogodišnji način i iznos sredstava za programsko financiranje javnih visokih učilišta. Mjera će biti uključena u cjelovito, potpuno programsko financiranje koje će obuhvatiti sve aktivnosti i troškove javnih sveučilišta, veleučilišta i visokih škola od akademske godine 2022./2023.

Uspostava sustava izobrazbe i provjere znanja iz područja informacijske sigurnosti je započela i provodi se u manjoj mjeri, kroz odgovarajuće stručne i državne ispite za državne službenike i namještenike, te će se periodično izvoditi za rukovodno osoblje, tehničko osoblje i ostale korisnike informacijskih sustava u tijelima državne uprave. Sustavna izobrazba nije uspostavljena, ali je obuhvaćeno državnim stručnim ispitom, u posebnom dijelu stručnog ispita, i to ne u cijelosti, već samo postupanje s klasificiranim podacima. Jedina sustavna izobrazba državnih službenika provodi se ciljano, prilikom imenovanja savjetnika za informacijsku sigurnost u državnim tijelima.
Temeljem prijedloga UVNS-a o uspostavljanju sustava izobrazbe, Državna škola za javnu upravu ponudila je organiziranje jednodnevnog stručnog seminara u 2019. godini na temu „Informacijska i kibernetička sigurnost“ koju bi zajednički proveli djelatnici UVNS-a, ZSIS-a i CARNet-a. Edukacije se redovno održavaju u DŠJU, a naziv programa je „Sigurni u kibernetičkom prostoru“.

Stalno **stručno usavršavanje policijskih službenika u području informacijske sigurnosti i kibernetičkog kriminaliteta provodi se u potpunosti**.
U MUP-u su tijekom 2020. godine, u organizaciji Policijske akademije i Uprave kriminalističke policije održana slijedeća stručna usavršavanja:

- dva modula treninga „Postupanje s digitalnim dokazima na mjestu događaja“ 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.

U sklopu projekta „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“, održana je u siječnju i veljači 2020. edukacija 31 policijskog službenika u trajanju od 160 nastavnih sati sa slijedećim temama:

1. Osnove napada i zaštite informacijskih sustava i informacijska sigurnost
2. Arhitektura, modeli, mehanizmi i načela informacijske tehnologije
3. Digitalni tragovi, dokazi i forenzika
4. Prevencija, nadzor i specijalizirana područja kibernetičkih napada

Policijski službenici Službe kibernetičke sigurnosti, policijski službenici regionalnih službi Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta te

policijski službenici policijskih uprava tijekom 2020. godine sudjelovali su na različitim on-line radionicama, seminarima i edukacijama u organizaciji Europola i CEPOL-a.
ZSIS sudjeluje u navedenim aktivnostima sukladno traženju nositelja mjere i ostalih dionika.

Mjeru stalnog stručnog usavršavanja državnih odvjetnika i sudaca u području informacijske sigurnosti i kibernetičkog kriminaliteta u znatnom opsegu provodi Pravosudna akademija, koja od 2019. provodi projekt „Unaprjeđenje programa edukacija u borbi protiv kibernetičkog kriminala“. Cilj projekta je unaprijediti kapacitet i funkcioniranje pravosuđa u borbi protiv kibernetičkog kriminala te ojačati kapacitete pravosudnih dužnosnika i službenika za utvrđivanje i procesiranje kaznenih djela povezanih s kibernetičkom sigurnošću. U 2020. g. su razvijeni programi obuke za osnovni i naprednu razinu te za pet specijalističkih tema. Organizirane su dvije radionice za obuku budućih voditelja te radionica o vještinama poučavanja za 10 polaznika. U lipnju/srpnju 2020. kroz projekt je nabavljena i oprema za kvalitetniju provedbu edukacije u Pravosudnoj akademiji. U 2021. Pravosudna akademija planira provesti osnovne, napredne te specijalističke module edukacije na temu kibernetičkog kriminaliteta u koje je planirano uključiti suce, državne odvjetnike, savjetnike u pravosudnim tijelima i službenike u pravosuđu, uključujući i vježbenike.
Planirano je i studijsko putovanje u neku od država članica EU-a, kao i pokretanje otvorenog postupka javne nabave vezanog uz digitalizaciju Pravosudne akademije (izrada nove baze korisnika te unaprjeđenje sustava za e-učenje). Također se planira i provedba e-tečaja o kibernetičkom kriminalu.

U skladu s mjerom I.1.13, kojom au tijela koja imaju CERT funkcionalnost trebala **definirati svoje zaposlenike, na godišnjoj razini potrebna područja ekspertize te potrebne izobrazbe, mjeru provode u znatnom opsegu te su utvrdila potrebna predznanja za rad u CERT timovima**. NCERT je u suradnji s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu definirao predznanja za rad u CERT timovima po slijedećim ulogama:

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

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

ZSIS donosi godišnji plan školovanja u kojemu su na godišnjoj razini definirane potrebne stručne i specijalističke izobrazbe i načini stjecanja tih znanja.

MORH je definirao katalog potrebnih tečajeva za djelatnike CERT-a MORH-a:
- IMET
- ITIL v.3 Foundation

- CEH, Certified Ethical Hacker
- COMPTIA Network+
- COMPTIA Security+
- C4ISR Orientation Course for Officers (1 polaznik)
- IT Essentials
- MCSA Windows Server 2012
- Red Hat System Administration I
- Cyber Defence NATO CIS Security Officer (INFOSEC version 2.0)
- Network Security Fundamentals and Defence Course
- Network Vulnerability Assessment Risk Mitigation Course

EU projekti su omogućili edukacije djelatnika, odnosno **specijalističke izobrazbe za potrebe CERT funkcionalnosti,** za vrijeme trajanja projekta. U 2020. godini u NCERT-u su tri djelatnika položila su certifikat za Certified Ethical Hacker – CEH i jedan djelatnik za Certified Devops engineer.

U 2020. godini nastavilo se s aktivnostima **sigurnosnog osvješćivanja i obrazovnih kampanja usmjerenih na najširi krug korisnika postojećih i svih budućih elektroničkih usluga**. Objavljivane su aktualne novosti vezane uz kibernetičku sigurnost putem društvenih mreža i internetskih stranica tijela, a neke od tema u nastupima na radiju i televiziji bavile su se i sigurnošću korisnika u elektroničkim komunikacijama/na internetu. Početkom 2020. HAKOM je bio suorganizator obilježavanja „Dana sigurnijeg interneta“ pod sloganom *„Zajedno za bolji internet“* kojom prilikom je promoviran i edukativni HAKOM-ov animirani video za roditelje *„Kako zaštititi djecu na Internetu?“.* Također, HAKOM od 2015. godine provodi program podizanja svijesti učenika i roditelja o temi sigurnosti na internetu. Osim predavanja učenicima ili roditeljima, svake godine se osvježi i revidira brošura *„Kako se zaštititi u svijetu interneta i mobilnih telefona“,* koja se otisne i dostavi u sve osnovne škole u RH za jednu generaciju učenika. Zadnja revizija učinjena je krajem 2020., objavljena je na web sjedištu HAKOM-a, a otisnuti primjerci poslani su u škole za obilježavanje Dana sigurnijeg interneta u 2021. godini. Također, prilikom obilježavanja „Dana sigurnijeg interneta“, 2018. godine HAKOM, tri mobilna operatora i Centar za sigurniji Internet potpisali su Povelju o sigurnosti djece na internetu u Hrvatskoj, a 2020. pokrenuta je web-platforma SINI - Sigurni na internetu koja na jednom mjestu nudi pomoć djeci, mladima, roditeljima i stručnjacima u obrazovnom sustavu oko tema sigurnosti i ponašanja na internetu.
U 2020. godini Nacionalni CERT 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 i 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 kojem je predstavljena tema „Odgovorna zabava na internetu“, te je organiziran i interaktivni webinar “Na digitalnom tragu” na kojem je prisustvovalo 500 osoba.

Mjera **informiranja i produbljivanja svijesti djece i mladih uključenih u sve razine formalnog obrazovanja, o potrebi brige o sigurnosti podataka te odgovornom korištenju**

informacijskih i komunikacijskih tehnologija provodi se u cijelosti. Temeljem kurikularnih dokumenata donijetih 2018. i 2019. godine, učenike se podučava o potrebi brige o sigurnosti podataka te odgovornom korištenju informacijskih i komunikacijskih tehnologija. U svim razredima osnovne i srednje škole u kojima se provodi bilo redovna bilo izborna/fakultativna nastava informatike i računalstva obrađuju se nastavni sati iz područja kibernetičke sigurnosti. Kurikulum međupredmetne teme Uporaba informacijsko komunikacijskih tehnologija također pokriva teme iz kibernetičke sigurnosti. Na satovima razrednih odjela često se razgovara o sigurnosti odgovornosti i oprezu pri korištenju internetskih usluga i digitalnih uređaja. Stručne službe provode radionice s učenicima na temu sigurnosti na Internetu.

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

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

Mjera, kojom se kreditne institucije, institucije za platni promet te institucije za **elektronički novac kontinuirano informiraju o aktualnim i potencijalnim sigurnosnim prijetnjama**, kao i odgovornostima vezanima uz njihov djelokrug rada, **provodi se u potpunosti**.

U 2020. godini HNB je izdao 24 objave 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 ožujku 2020. HNB je – nastavno na promjene koje je COVID-19 pandemija unijela u poslovanje kreditnih institucija – ukazala na povezane rizike te dala preporuke za daljnje postupanje, vezano uz sljedeća područja:

- nužnost osiguravanja primjerene zamjenjivosti kritičnih osoba,
- mogućnosti i rizici rada na daljinu,
- potrebe povećanja i održavanja odgovarajućih kapaciteta izravnih elektroničkih distribucijskih kanala

Nadalje, HNB je u 2020. godini nadziranim institucijama uputio 102 dopisa i 7 okružnica te je održao 25 sastanaka s, temama vezanima uz rizike korištenja informacijskih sustava.

Mjera osmišljavanja i provođenja usklađenih kampanja o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u RH o značaju kibernetičke sigurnosti je provođena u znatnoj mjeri.

U 2019. i 2020. godini Nacionalni je CERT 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 2019. i 2020. nastavljena je suradnja sa FER-om u pogledu pisanja i izdavanja stručnih dokumenata (objavljeno ukupno 15 recenzija alata i 16 dokumenata). Također, Nacionalni je CERT 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, Nacionalni je CERT u 2019. godini proveo kampanju za podizanje svijesti o važnosti kibernetičke sigurnosti u sklopu projekta GrowCERT. U 2019. godini Nacionalni CERT je u okviru provedbe aktivnosti GrowCERT projekta proveo četiri radionice s ciljem podizanja svijesti o kibernetičkoj sigurnosti za akademsku zajednicu i poslovni sektor.

Kampanja pod nazivom „Veliki hrvatski naivci“ provedena je u periodu od veljače do travnja 2019. godine i u njoj su uz dva TV spota, objavljene tri digitalne i jedna tiskana brošura o temama kibernetičke sigurnosti, dva letka za opću javnost i poslovnu javnost. Zbog velikog interesa inozemne publike iz CSIRT zajednice izradili smo video materijale i s engleskim prijevodom.

Nacionalni CERT je aktivan i na društvenim mrežama: https://www.facebook.com/CERT.hr/ https://twitter.com/HRCERT

Tijekom 2019. Nacionalni CERT je objavio ukupno 94 novosti na web sjedištu i društvenim mrežama.

U 2019. godini objavljeno je ukupno 109 novosti.

Broj posjetitelja web sjedišta www.cert.hr je 289.947

Broj posjetitelja web sjedišta www.naivci.hr je 28.600

Broj pratitelja Facebook stranice 1356

Broj pratitelja Twitter stranice 969

Povodom Dana sigurnijeg interneta 2020. organiziran je interaktivni webinar „Na digitalnom tragu“ na kojem je sudjelovalo 500 ljudi.

U listopadu 2020. godine provedeno je prvo CTF natjecanje za srednje škole na kojem je sudjelovalo 23 škole iz 16 hrvatskih gradova pod nazivom Hacknite. Od 2020. CERT je preuzeo ulogu nacionalne koordinacije provedbe aktivnosti na europskoj razini tijekom Europskog mjeseca kibernetičke sigurnosti. Objavljeni su brojni sadržaji – dva najavna spota za animirane filmove, dva kratka animirana filma o Internet prevarama i digitalnim kompetencijama, tri infografike – zaštita od Internet prevara, digitalne kompetencije i digitalni trag. Na službenim stranicama zajedničke europske inicijative uređena je stranica posvećena hrvatskoj publici https://cybersecuritymonth.eu/countries/croatia. Javna prisutnost Nacionalnog CERT-a je u stalnom porastu – brojna gostovanja na televiziji, radiju, tiskanim i digitalnim medijima.

U 2020. godini objavljeno je ukupno 104 novosti.

Broj posjetitelja web sjedišta je 137.224

Broj pratitelja Facebook stranice 1739

Broj pratitelja Twitter stranice 1142

Osmišljavanje i provođenje usklađene kampanje o podizanju svijesti o značaju kibernetičke sigurnosti za državna tijela i pravne osobe s javnim ovlastima, provođeno je u znatnoj mjeri.

Nastavljena je analiza načina na koji bi se provele odgovarajuće kampanje o podizanju svijesti o značaju kibernetičke sigurnosti za državna tijela i pravne osobe s javnim ovlastima.

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

ZSIS redovito širi svijest o važnosti kibernetičke sigurnosti na stručnim konferencijama, skupovima kao i objavama raznih edukativnih materijala i preporuka na internetskim stranicama ZSIS-a.

Aktivnosti **pravodobnog obavješćivanja javnosti putem javnih medija, u slučaju nastanka računalnih sigurnosnih incidenata koji se mogu lako multiplicirati i pogoditi veliki broj korisnika u kibernetičkom prostoru, provode se kontinuirano**.

Tijekom 2020. godine zabilježen je kibernetički napad većih razmjera na štetu trgovačkog društva, koje je dijelom u državnom vlasništvu, tako što je organizirana skupina iz inozemstva putem cryptolocker ransomwarea šifrirala i onemogućila pristup podacima neophodnima za funkcioniranje trgovačkog društva. O navedenom je pravovremeno informirana javnost.

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 u više navrata distribuirani medijima.

Tijekom 2020. godine i dalje je veliki broj građana oštećen različitim oblicima internetskih prijevara. Temeljem navedenog, a u suradnji s Europolom MUP je proveo je javnu kampanja #CyberScams kao dio programa European Cyber Security Month.

Najučinkovitija obrana od društvenog inženjeringa je obrazovanje potencijalnih žrtava - to može biti svatko od nas kada izađe na internet. Podizanje svijesti u društvu kako identificirati takve prijevarne tehnike učinit će sigurnim same korisnike kao i njihove financije.

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 pokrenulo 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[8].

Nacionalni CERT je u 2020. godini objavio 12 upozorenja putem web sjedišta www.cert.hr, Facebook stranice CERT.hr i Twitter računa HRCERT. U 2020. godini izdano je 3682 sigurnosne preporuke.

[8] 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 koje zaprimi informaciju ili kaznenu prijavu, odnosno Državno odvjetništvo RH odgovarajućim priopćenjem, vodeći pri tome računa o zaštiti interesa kriminalističkog istraživanja ili istrage u predmetima kibernetičkog kriminaliteta, a prema potrebi davati upute radi sprječavanja daljnjih prijetnji i umanjenja štetnih posljedica incidenata.
Za koordinatora opisanih aktivnosti na razini državnoodvjetničke organizacije određen je zamjenik Glavne državnog odvjetnice RH.

U 2020. godini **provođene su u manjoj mjeri aktivnosti usmjerene na poticanje i podupiranje znanstvenih istraživanja u području informacijske i komunikacijske tehnologije** s posebnim naglaskom na informacijsku sigurnost i područja poput kriptologije, sustavskih rizika, privatnosti u internetskom okruženju.
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 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 2020. godini Hrvatska zaklada za znanost financirala je pet projekata povezana s područjem informacijske i komunikacijske tehnologije s naglaskom na informacijskoj sigurnosti:

- „Korisniku orijentiran (re)dizajn procesa i modeliranje informacijskih sustava na primjeru smart city usluga“, voditeljica Maja Ćukušić, Sveučilište u Splitu, Ekonomski fakultet
- „Okvir za kontrolu i nadzor bespilotnih letjelica“, voditelj Neven Vrček, Sveučilište u Zagrebu, Fakultet organizacije i informatike
- „Pametne usluge usmjerene čovjeku u interoperabilnim i decentraliziranim okolinama Interneta stvari“, voditeljica Ivana Podnar Žarko, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva
- „Pouzdani i sigurni kompleksni softverski sustavi: Od empirijskih principa prema teoretskim modelima iz perspektive industrijske primjene“, voditeljica Tihana Galinac Grbac, Sveučilište Jurja Dobrile u Puli

„Višeslojni okvir za karakterizaciju širenja informacija putem društvenih medija tijekom krize COVID-19“, voditeljica Ana Meštrović, Sveučilište u Rijeci, Odjel za informatiku

Također su **provođene aktivnosti, u manjoj mjeri, u cilju osiguranja aktivnog poticanja organizacije redovitih znanstvenih i stručnih skupova** te drugih oblika razmjene znanja i iskustva i homogeniziranja stručne zajednice radi bolje interakcije u incidentnim situacijama.
U 2020. godini javna visoka učilišta i organizacije civilnog društva prijavila su tri znanstvena ili znanstvenostručna skupa koji su povezani s područjem informacijske i komunikacijske tehnologije, a financirani su od strane MZO:

- Skup „43. Međunarodni skup MIPRO 2020“, organizator Hrvatska udruga za informacijsku, komunikacijsku i elektroničku tehnologiju – MIPRO,
- Skup „International Conference on Smart Systems and Technologies 2020 (SST 2020)“, organizator Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek,
- Skup „CECIIS 2020“, organizator Fakultet organizacije i informatike, Varaždin.

Provedba mjere **poticanja znanstvenog istraživanja u području kibernetičke sigurnosti za razvoj novih proizvoda i usluga za tržište te poticanja razvoja tehnološke infrastrukture** i provedba mjere **poticanje razvoja novih proizvoda i usluga iz područja kibernetičke sigurnosti za unutarnje tržište EU i svjetsko tržište, otvaranjem novih mogućnosti za RH kroz poticanje nacionalne normizacije i organizacije koja može osigurati odgovarajuće akreditirane, certificirane i evaluirane domaće proizvođače i proizvode za svjetsko tržište su provođene u znatnoj mjeri.**
Posredstvom CEF Telekoma - financijskog instrumenta EU, otvorena mogućnost sufinanciranja digitalnih projekata gospodarskim subjektima i javnoj/državnoj upravi te je za projekte digitalizacije poslovnih procesa iz EU sredstava za razdoblje 2014.-2021. bilo namijenjeno milijardu eura, a za razdoblje 2021.-2027. godine namijenjene su 3 milijarde eura.

Hrvatski gospodarski subjekti, državna i javna uprava te MinGOR uspješno su aplicirali za CEF sredstava. Najviše sredstava dobili su upravo projekti kibernetičke sigurnosti - Cybersecurity HR Projects, vrijednost do 2019 - 3,516,420 EU - (pregled projekata nalazi se u tablici), kako slijedi:

2019-HR-IA-0086	Improving cybersecurity capabilities of "Sestre milosrdnice Univ.Hospital Center" to meet national and EU requirements
2018-HR-IA-0121	Consolidation/Upgrade of the Process Network Infrastructure and Implementation of the SIEM system
2018-HR-IA-0124	NIS Compliance Upgrade of Plinacro Corporate Network
2018-HR-IA-0109	Increasing maturity of National CERT for stronger cooperation in cybersecurity community (Grow2CERT)
2018-HR-IA-0120	Increasing cybersecurity of SCADA and Information System for Capacity Management
2019-HR-IA-0090	Improvement of cybersecurity for safe and reliable gas distribution
2016-HR-IA-0085	Increase of National CERT capacities and enhancement of cooperation on national and European level – GrowCERT
2017-EU-IA-0118	CyberExchange
2019-HR-IA-0054	System for Prevention and Analysis of HOPS's communication networks security incidents
2018-HR-IA-0147	Increase of ViK Split capacities to improve compliance with cyber security requirements on national and European level
2019-HR-IA-0069	Increasing cybersecurity capacity and NIS Directive compliance in CHC

2019-HR-IA-0143	Increasing Cyber Security Capacity of MZLZ - Zagreb Airport Operator

Također, 2020. godine odabrano je nekoliko HR CyberSecurity projekata za sufinanciranje, a čije ugovaranje je u tijeku; MZLZ - Međunarodna zračna luka Zagreb, HOPS, Hrvatska akreditacijska agencija, Zagrebački holding, Gradska plinara Zagreb, Opća bolnica Varaždin, Reiffeisen banka.

Na marginama javnih predstavljanja CEF projekata, organizirano je nekoliko sastanaka s tematikom kibernetičke sigurnosti, na kojim su aktivno sudjelovali i tijela državne uprave i hrvatski gospodarstvenici/poduzetnici sve s ciljem poticanja primjene domicilnih rješenja kibernetičke sigurnosti.

U 2020. godini aktivnosti u provedbi mjere **poticanja potencijala RH u području kibernetičke sigurnosti za vlastitu proizvodnju u segmentima u kojima postoje potencijali za proizvode i usluge te gdje bi poticanje primjene domaćih rješenja, naročito kod korisnika državnog proračuna, javnih ustanova i drugih gospodarskih subjekata moglo donijeti određene gospodarske i/ili sigurnosne prednosti nisu provođene u dostatnoj mjeri**.

IV. ZAKLJUČAK

Nastavak provedbe Akcijskog plana tijekom 2020. godine rezultirao je daljnjim povećanjem sigurnosne svijesti na nacionalnoj razini i aktiviranjem mjera koje su kasnile u odnosu na planiranu dinamiku provedbe Akcijskog plana prethodnih godina. Važnost kibernetičke sigurnosti kao preduvjeta digitalne transformacije društva sada je puno bolje prihvaćena, kako unutar državnog sektora, tako i unutar gospodarstva i građanstva. Na rizike iz kibernetičkog prostora se sve manje gleda kao na potencijalna, malo vjerojatna događanja, a sve više na nešto što je neminovno i za što treba biti spreman. Institucije koje su dionici Strategije i provode mjere iz Akcijskog plana sve bolje međusobno surađuju i usklađuju postupanja.

Strategija je, uza sva pravna, financijska, organizacijska i kadrovska ograničenja i poteškoće, od svog donošenja do danas bila uspješna. Novi zahtjevi, kako realni, životni, uslijed primjene novih tehnologija i time posljedično novih rizika, tako i zbog potrebe usklađivanja s međunarodnim savezima i preuzetim obvezama neminovno zahtijevaju daljnje prilagodbe Strategije i viziju nacionalnih potreba u sljedećem vremenskom razdoblju. Rad na novoj Nacionalnoj strategiji kibernetičke sigurnosti je već započeo. Dok je prva Strategija pokušala adresirati prioritete, nova bi Strategija trebala stvoriti ambicioznije organizacijske, pravne, financijske i ljudske preduvjete za sigurno digitalno društvo budućnosti.