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

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2018. GODINI

Zagreb, 16. svibnja 2019.

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 2018. godini prikazanim u Godišnjem izvješću o radu Vijeća u 2018. godini[2]. Godišnje izvješće o radu Vijeća uključuje i kratki osvrt na stanje kibernetičkog prostora u 2018. godini[3].

Izvješće o provedbi Akcijskog plana u 2018. godini temelji se na ciljevima Nacionalne strategije kibernetičke sigurnosti[4] (u daljnjem tekstu: Strategija), koji su razrađeni u obliku mjera pripadnog Akcijskog plana[5] („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 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
E. Kibernetički kriminalitet – 5 mjera

[1] Odluka o osnivanu Vijeća objavljena je u Narodnim novinama broj: 61/2016, 28/2018, 110/2018
[2] https://www.uvns.hr/hr/aktualnosti-i-obavijesti/godisnje-izvjesce-o-radu-nacionalnog-vijeca-za-kiberneticku-sigurnost-i-operativno-tehnicke-koordinacije-za-kiberneticku-sigurnost-za-2018-godinu
[3] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Godišnje%20izvješće%20o%20radu%20NVKS%20i%20OTKKS%20za%202018.%20godinu.pdf
[4] https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kiberneticke%20sigurnosti%20(2015.).pdf
[5] https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20(2015.).pdf

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera
G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata – 5 mjera
H. Međunarodna suradnja – 6 mjera
I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru – 27 mjera

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

Za sustavno praćenje i koordiniranje provedbe Strategije zaduženo je Vijeće, koje u tu svrhu provodi horizontalnu koordinaciju prema svim institucijama - nositeljima mjera, kako bi se moglo procijeniti jesu li željeni rezultati pojedinih područja ili mjera ostvareni, ili je potrebno redefinirati pristup pojedinim područjima u skladu s novim potrebama.

Pri tome je Vijeće i samo nositelj većine mjera u području *D. Kritična komunikacijska i informacijska infrastruktura*, području koje je u visokoj mjeri regulirano upravo kroz inicijativu i rad Vijeća tijekom 2017. i 2018. godine te je rezultiralo donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[6] i pripadne Uredbe[7].

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. Državna uprava za zaštitu i spašavanje (DUZS) odnosno Ravnateljstvo civilne zaštite Ministarstva unutarnjih poslova
5. Hrvatska akademska i istraživačka mreža (CARNET)
6. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)
7. Hrvatska narodna banka (HNB)
8. Ministarstvo gospodarstva, poduzetništva i obrta (MGPO)
9. Ministarstvo obrane (MORH)
10. Ministarstvo pravosuđa (MP)

[6] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Zakon%20o%20kibernetičkoj%20sigurnosti%20operatora%20ključnih%20usluga.pdf
[7] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Uredba%20o%20kibernetičkoj%20sigurnost%20operatora%20ključnih%20usluga.pdf

11. Ministarstvo unutarnjih poslova (MUP)
12. Ministarstvo uprave (MU)
13. Ministarstvo vanjskih i europskih poslova (MVEP)
14. Ministarstvo znanosti i obrazovanja (MZO)
15. Nacionalni CERT / CARNET
16. Operativno-tehnički centar za nadzor telekomunikacija (OTC)
17. Operativno-tehnička koordinacija za kibernetičku sigurnost (Koordinacija)
18. Pravosudna akademija (PA)
19. Sigurnosno-obavještajna agencija (SOA)
20. Sveučilišni računski centar (SRCE)
21. Ured Vijeća za nacionalnu sigurnost (UVNS)
22. Vojna sigurnosno-obavještajna agencija (VSOA)
23. Zavod za sigurnost informacijskih sustava (ZSIS)

Mjere Akcijskog plana uključuju i niz drugih tijela koja su bila sunositelji ili su opisno definirana i koordinirana u procesu provedbe mjera (npr. središnja tijela državne uprave u suradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor kritične infrastrukture). U svim mjerama koje uključuju više nositelja/sunositelja Vijeće je usmjeravalo nositelje i sunositelje na koordinirano djelovanje, kako bi se postigao sinergijski učinak njihovog rada. U tu svrhu Vijeće je koncipiralo i pripremilo elektronički adresar s preko stotinu osoba, neposrednih koordinatora pojedinih mjera u okviru svih spomenutih institucija. Elektronički adresar uključuje i osnovne podatke o nadležnostima pojedinih institucija te o povezanim odgovornim osobama kao što su članovi i zamjenici članova u Vijeću i Koordinaciji, nadležne ustrojbene cjeline tih institucija i odgovorni rukovoditelji. U provedbi mjera institucije nositelji uključivale su prema potrebi druge organizacije i stručnjake.

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 tijekom ožujka i travnja 2019. 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 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 znatnoj mjeri, ali su potrebne dodatne aktivnosti***. U domeni računalno sigurnosnih incidenata potrebna je izmjena Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga[8] u cilju kontrole računalno-sigurnosnih incidenata prema nacionalnoj taksonomiji donesenoj 2018. godine[9]. HAKOM je odgovorno tijelo za usklađivanje ovog Pravilnika, a provedba ovog usklađivanja u segmentu prilagodbe korištene taksonomije, kao i osiguravanja uvjeta za obavljanje poslova nadležnog sektorskog CERT ili CSIRT tijela od visokog je značenja u 2019. godini. Razlog tome je da je sektor javnih elektroničkih komunikacija uređen zasebnim regulativnim okvirom i nije obuhvaćen novim Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Stoga **HAKOM u 2019. godini, kroz prilagodbu ovog Pravilnika, treba osigurati nacionalno usklađeni pristup kibernetičkoj sigurnosti u sektoru svoje odgovornosti**.

[8] https://www.hakom.hr/UserDocsImages/2016/propisi/VL-KU-PR-INTS-Pravilnik%20o%20sigurnosti-neslu%C5%BEbeni%20pro%C4%8Di%C5%A1%C4%87eni%20tekst.pdf
[9] https://www.cert.hr/wp-content/uploads/2019/04/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf

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. Zasebno planirane aktivnosti u cilju provođenja ove mjere nisu do sada planirane ili provođene, a **uočen je još uvijek nedovoljno razvijen pristup području zaštite poslovne tajne**. Premda poslovna tajna koncepcijski pripada području zaštite intelektualnog vlasništva, ona ima sve veću važnost u suradnji državnog i privatnog sektora, ali i u području kibernetičkog prostora kroz povezane i rastuće prijetnje industrijske špijunaže.

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. 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. **Visoka uređenost ovog područja, koju je u prethodnim godinama ostvarilo SRCE kao nadležno tijelo, rezultirala je 2018. godine ugradnjom ove važne funkcionalnosti u Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.** Time je nacionalno razvijena funkcionalnost CIX-a, zadovoljila sve zahtjeve prepoznate i na razini EU-a 2016. godine u okviru NIS Direktive[10] i nacionalno transponirane spomenutim Zakonom.

(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, 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.

[10] https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L1148&from=EN

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. Tri mjere provode se u manjem opsegu, mjere vezano za donošenje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica, kojom će se obuhvatiti i drugi aspekti povezani s nacionalnim mogućnostima za uspostavu odgovarajućih akreditacijskih i certifikacijskih sposobnosti u području kvalificiranih elektroničkih potpisa, a sukladno zahtjevima Europske unije[11] (EU). U tijeku je izrada smjernica za primjenu sustava NIAS i odgovarajućih normi kao i analiza stanja u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora. Provedba u slučaju posljednje tri mjere se nastavlja ili se planira slijedom ostvarenih rezultata prethodno spomenutih mjera, a intenzivirat će se uspostavljanjem radne skupne za analizu, standardizaciju i sigurnost mreža državnih tijela.

Značajan dio opsega aktivnosti iz ovih mjera uređen je 2018. godine, u okviru donošenja ranije spomenutog Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Tako je ovim Zakonom utvrđen sektor ključnih usluga koji obuhvaća poslovne usluge za državna tijela, napose usluge u sustavu e-Građani i poslovne usluge za korisnike državnog proračuna. Uvođenjem ovog sektora poslovnih usluga za državna tijela kao sektora ključnih usluga, cjelokupni okvir mjera kibernetičke sigurnosti razrađen Zakonom i pripadnom Uredbom te smjernicama nadležnih tijela, od srpnja 2018. godine, sustavno obvezuje niz subjekata koji sudjeluju u realizaciji većine usluga elektroničke uprave te će se pojedine funkcionalnosti provoditi u Zakonom propisanim rokovima u razdoblju od 2018. do 2020. godine. Za ovo područje elektroničke uprave, posebno je **važna inicijativa Vijeća za nacionalnu sigurnost**, donesena krajem 2018. godine, temeljem analize stanja informacijske sigurnosti u RH koju je tijekom 2018. godine proveo UVNS u koordinaciji s tijelima sigurnosno-obavještajnog sustava. **Zaključci Vijeća za nacionalnu sigurnost i odgovarajuće smjernice dostavljene su nadležnim državnim tijelima na provedbu u 2019. godini**.

(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;

[11] https://www.mingo.hr/page/uredba-o-elektronickoj-identifikaciji-za-uspostavljanje-jedinstvenog-eu-digitalnog-trzista-1

- 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*** su izrađene 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.

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 drugih akata 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 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 Europskoj središnjoj banci[12].

(D) Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

Sigurnost kritične komunikacijske i informacijske infrastrukture predstavlja jedno od pet prioritetnih područja Strategije.

Takvim pozicioniranjem ovog područja na strateškoj razini RH je pokazala visoki stupanj svijesti o važnosti kritične komunikacijske i informacijske infrastrukture za društvo u cjelini. Dodatno, Strategijom i Akcijskim planom definirani su ciljevi i aktivnosti kojima je RH

[12] https://www.hnb.hr/documents/20182/2220984/h-smjernice-izvjescivanje-o-incidentima-direktiva-2018-2366_PSD2.pdf/403ca3a8-e45f-4868-bb5e-adff39a19950

pokazala da je odabrala smjer postupanja u ovom području koji 2016. godine i EU uvodi kao obligatoran za sve države članice donošenjem ranije spomenute NIS Direktive.

Naime, 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.).

Provedba ciljeva u ovom području, a time i same aktivnosti koje su definirane Akcijskim planom za njezinu provedbu[13] temeljene su na nacionalnom zakonodavnom okviru koji je postojao u vrijeme donošenja Strategije – Zakonu o kritičnim infrastrukturama („Narodne novine“, broj: 56/13).

Rezultati provedbe Akcijskog plana već u 2016. godini pokazali su poteškoće u provedbi planiranih aktivnosti u ovom segmentu, budući da provedba Zakona o kritičnim infrastrukturama do tada nije zaživjela u opsegu kakav je bio nužan za željeni napredak. Dodatno, Zakon o kritičnim infrastrukturama ne razmatra kritične sektore iz kuta ovisnosti o komunikacijskoj i informacijskoj tehnologiji, već komunikacijsku i informacijsku tehnologiju tretira zasebno kao jedan od kritičnih sektora te ne daje detaljnije smjernice za postizanje njihove zaštite. Međutim, već u 2017. godini započinje se s potpuno novim nacionalnim pristupom kritičnoj informacijskoj i komunikacijskoj infrastrukturi, neovisnim o provedbi Zakona o kritičnim infrastrukturama, koje su, sukladno najavama i očekivanjima opisanim u Izvješću o provedbi Strategije i Akcijskog plana u 2017. godini, u 2018. godini donijele željene rezultate.

U ljeto 2018. godine donesen je Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kojima je u nacionalno zakonodavstvo prenesena EU NIS direktiva, čime je ujedno ostvaren prvi cilj zadan Strategijom u ovom području **(cilj D.1.)**.

Naime, ovim Zakonom su kroz definirani Popis ključnih usluga[14] (i svim elementima koje Popis sadrži) te uvođenje i propisivanje postupka identifikacije operatora ključnih usluga postavljeni temelji za prepoznavanje kritične komunikacijske i informacijske infrastrukture, što je već u prvim mjesecima njegove provedbe **rezultiralo utvrđivanjem stotinjak**

[13] Ukupno 13 mjera.
[14] Ukupno 52 ključne usluge u 8 sektora i 7 podsektora.

operatora ključnih usluga[15] čiji mrežni i informacijski sustavi predstavljaju komunikacijsku i informacijsku infrastrukturu ključnu za društvene i gospodarske aktivnosti u Zakonom definiranim sektorima[16]. Također, sukladno zahtjevima NIS direktive, kao ključnom komunikacijskom i informacijskom infrastrukturom, Zakonom su određeni oni mrežni i informacijski sustavi koji su u potpori pružanju slijedećih digitalnih usluga: internetsko tržište, internetske tražilice i usluge računalstva u oblaku. U odnosu na mrežne i informacijske sustave, za operatore ključnih usluga i davatelje digitalnih usluga, Zakonom se postavljaju daljnje obveze – **primjena sigurnosnih mjera i obveza izvješćivanja o incidentima na tim sustavima.**

Sigurnosne mjere, način njihove provedbe, kriteriji za određivanje incidenata za koje postoji obveza izvješćivanja i sam postupak dostave obavijesti, uključujući sadržaj koji su o incidentu dužni prijaviti, detaljnije su razrađene uredbom[17] donesenom temeljem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.

Implementacija propisanih sigurnosnih mjera je u tijeku, a rok za njihovu punu provedbu do kraja 2019. godine, dok je obveza obavješćivanja o incidentima na snazi već od studenoga 2018. godine.

Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga predviđen je i nadzorni mehanizam. Zakonom su dodijeljene potrebne nadležnosti za njegovo provođenje te je uveden poseban institut „ocjene sukladnosti“, za koji su Zakonom zadužena nacionalna tehnička tijela s najviše stručnih znanja i iskustava u tim pitanjima[18], sve u cilju olakšavanja provedbe obveza iz Zakona i prateće Uredbe, kako njihovim obveznicima, tako i nadležnim sektorskim tijelima koji su dužni provoditi nadzor nad primjenom Zakona i Uredbe. Za sektore u kojima postoji (ili će se u perspektivi uvesti) 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 **(cilj D.2.)**.

Upravljanju rizicima posvećeno je poglavlje II. Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kojim je postavljen normativni okvir za uvođenje sustava upravljanja rizicima te su definirani elementi o kojima se mora voditi računa prilikom izrade procjene rizika. Dodatno, poseban naglasak stavljen je na važnost uvažavanja rezultata

[15] Ukupan broj identificiranih operatora mijenja se sukladno dinamici procesa identifikacije operatora. Na dan podnošenja ovog Izvješća ukupno su bila identificirana 92 subjekta (tijela i pravne osobe), koji pružaju neku od 50 definiranih ključnih usluga iz Popisa ključnih usluga, pri čemu ova 92 subjekta pružaju ukupno 124 ključne usluge u RH, jer su neki od ovih subjekata višestruki operatori koji pružaju više ključnih usluga.

[16] Energetika – Električna energija, Nafta, Plin; Prijevoz – Zračni, Željeznički, Vodni, Cestovni; Bankarstvo; Infrastrukture financijskog tržišta; Zdravstvo; Opskrba vodom za piće i njezina distribucija; Digitalna infrastruktura; Poslovne usluge za državna tijela.

[17] Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Narodne novine, broj: 68/18).

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

provedenih procjena ne samo prilikom izgradnje, već i nadogradnje i održavanja mrežnih i informacijskih sustava na koje se Uredba odnosi **(cilj D.3.)**.

Također, Zakonom i Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga uspostavljena je **platforma za razmjenu informacija** bitnih za ostvarenje zajedničkog cilja svih uključenih dionika – uspostave visoke razine sigurnosti komunikacijskih (mrežnih) i informacijskih sustava ključnih za društvene i gospodarske aktivnosti **(cilj D.4.)**.

Uvažavajući sve gore izneseno, a kada se uzmu u obzir i planirane izmjene Zakona o kritičnim infrastrukturama upravo kako bi se primjena odredbi Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga proširila i na objekte, mreže i sustave obuhvaćene Zakonom o kritičnim infrastrukturama, ocjenjuje se da su donošenjem Zakona i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga ostvareni i ciljevi Strategije u području kritične komunikacijske i informacijske infrastrukture (**D.2., D.3. i D.4.).**

Vezano uz provedbu aktivnosti povezanih s ciljem **uspostave kapaciteta za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu** (D.5.), važno je ponovno spomenuti donošenje ***Odluke Vijeća o komuniciranju u situacijama kibernetičkih kriza***, kojom je u lipnju 2017. Vijeće utvrdilo način djelovanja temeljen na iskustvu stečenom pri rješavanju globalnog kibernetičkog napada ucjenjivačkim malicioznim kodom WannaCry. Tako je donesen protokol Vijeća i Koordinacije u svrhu kriznog komuniciranja s javnošću u području kibernetičke sigurnosti, odnosno u slučajevima kibernetičkih kriza, kojim je ova odgovornost stavljena u zadatak predstavnicima MUP-a, uz obavezu odgovarajuće suradnje i koordinacije s Vijećem[19].

Također, važno je ponovno istaći da je sudjelovanje Vijeća u aktivnostima Koordinacije za sustav domovinske sigurnosti, rezultiralo ***izradom analize potreba i sposobnosti kibernetičkog djelovanja na razini RH[20],*** *kao i dokumentima u kojima je opisan* ***organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini[21]*** odnosno definiran sadržaj ***registra sigurnosnih rizika od kibernetičkih napada (Tablica 1.),*** čime su u znatnoj mjeri provedene dvije od tri aktivnosti opisane Akcijskim planom u okviru cilja D.5.

[19] Godišnje izvješće o radu Vijeća u 2017. godini, str. 13., https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

[20] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Analiza%20potreba%20i%20sposobnosti%20kiberneti%C4%8Dkog%20djelovanja%20na%20razini%20RH.pdf

[21] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Organizacijski%20i%20ustrojbeni%20polo%C5%BEaj%20tijela%20za%20kiberneti%C4%8Dko%20djelovanje.pdf

Tablica 1.: MATRICA RIZIKA

Matrica rizika kibernetičkih napada preporučena je i dana kao prilog Vijeća za razradu šireg registra sigurnosnih rizika čija je izrada u nadležnosti MUP-a, a izrađuje se u okviru plana rada Koordinacije za sustav domovinske sigurnosti.

Opis rizika	Prijetnja	Ranjivost	Utjecaj	Vjerojatnost	KOORDINATOR	Uključivanje drugih tijela državne uprave
Kibernetički napad	**VISOKA RAZINA** - globalni napad koji uzrokuje potencijalno dugotrajni i široko rasprostranjeni prekid ključnih usluga ili ugrožava nacionalnu sigurnost RH	**VISOKA RAZINA** - ranjivosti prisutne u široko korištenoj informacijskoj tehnologiji, nepoznate, nove ili povezane s upotrebom starijih informacijskih tehnologija koje su izvan roka održavanja proizvođača	**VISOKA RAZINA** - teške ekonomske ili društvene posljedice na najširoj nacionalnoj razini ili gubitak života	**SREDNJA RAZINA** - zbog brzog trenda digitalizacije društva, gospodarskih sektora i uspostave niza javno dostupnih informacijskih resursa s visokom kumulacijom podataka	**MUP / Operativno-tehnička koordinacija za kibernetičku sigurnost**	**UVNS / Nacionalno vijeće za kibernetičku sigurnost** **Nadležna tijela iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga**
	SREDNJA RAZINA - napad na velike organizacije ili dijelove državne i lokalne vlasti ili pojedine gospodarske sektore s ključnim uslugama	**SREDNJA RAZINA** - ranjivosti vezane uz ljudski faktor pri korištenju tehnologije, što uključuje krajnje korisnike, tehničko osoblje za održavanje informacijskih sustava te rukovodno osoblje u različitim vrstama organizacija	**SREDNJA RAZINA** - ozbiljne posljedice za velike organizacije ili dijelove državne i lokalne vlasti ili pojedine sektore gospodarstva s ključnim uslugama te posljedične štete za građanstvo na užoj razini određen regije	**VISOKA RAZINA** - zbog nedovoljno razvijene sigurnosne svijesti i projekata digitalizacije koji se brzo uvode bez odgovarajuće procjene i upravljanja rizicima	**Nacionalni CERT (CARNet)** **ZSIS**	**Izvještavati i prema potrebi uključiti:** **MUP / Operativno-tehnička koordinacija za kibernetičku sigurnost** **Nadležna tijela iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga** **UVNS / Nacionalno vijeće za kibernetičku sigurnost**

Opis rizika	Prijetnja	Ranjivost	Utjecaj	Vjerojatnost	KOORDINATOR	Uključivanje drugih tijela državne uprave
Kibernetički napad	**NISKA RAZINA** - razne vrste zlonamjernih programskih kodova u opticaju na javnim mrežama koje pogađaju pojedine manje organizacije u gospodarstvu ili pojedino državno ili lokalno tijelo vlasti, građane ili skupine građana koji su korisnici nekih usluga	**NISKA RAZINA** - ranjivosti vezane uz lošu praksu primjena zakrpa i nadogradnji programske podrške ili kontrolu konfiguracije informacijskih sustava	**NISKA RAZINA** - manje posljedice po pojedine organizacije i građane	**VISOKA RAZINA** - još uvijek nedovoljna digitalna higijena društva u cjelini, iako je većinom prisutna svijest u široj javnosti o nužnosti korištenja programskih alata u svrhu suzbijanja zlonamjernih kodova	**Organizacije/građani koji su vlasnici napadnute informacijske infrastrukture** **i** **Davatelji elektroničke usluge**	**Izvještavati i prema potrebi uključiti:** **Nacionalni CERT (CARNet)** **ZSIS**

Opis tablice:

Kibernetički napadi (1. stupac), sukladno zadanoj metodologiji razvoja registra sigurnosnih rizika za koji je nositelj MUP ispred Koordinacije za sustav domovinske sigurnosti, opisani su sa tri razine prijetnje (2. stupac) u koje su za ilustraciju pridružene tipične prijetnje svake razine kibernetičkih napada. U sljedećem 3. stupcu prikazane su tipične ranjivosti na isti način podijeljene i ilustrirane kroz tri odabrane razine. U 4. stupcu je opisan procijenjeni utjecaj također na tri odabrane razine. U 5. stupcu je dana procjena vjerojatnosti događanja kibernetičkih napada, također na tri razine i s pojašnjenjem temeljnih razloga zbog kojih napadi uspijevaju. Pri tome u svim kolonama zelena boja označava nisku razinu, narančasta srednju, a crvena visoku razinu.

U 6. i 7. stupcu prikazani su tipični načini eskalacije odgovora na kibernetičke napade za odabrane tri razine kibernetičkih napada. Pri tome 6. stupac opisuje nadležna koordinacijska tijela, a 7. stupac tipični proces eskalacije kojim se uključuju druga tijela povezanih nadležnosti.

Iako pojednostavljen, ovakav prikaz u velikoj mjeri odgovara i procesu propisanom Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kako na sektorskoj, tako i na nacionalnoj, odnosno EU razini. Također, ovakav proces eskalacije primijenjen je i u slučaju WannaCry kibernetičkog napada kriptografskim malicioznim kodom u svibnju 2017. godine (visoka razina)[22].

[22] Godišnje izvješće o radu Vijeća u 2017. godini, str. 16., https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

Nadalje, napominje se kako od 2018. godine RH ima i **Nacionalnu taksonomiju računalno-sigurnosnih incidenata[23],** koja, između ostalog, daje okvirnu definiciju pojma kibernetičke krize.

No, za naredno razdoblje ostaje još za izraditi detaljnije planove i procedure postupanja u kibenetičkim krizama. Uvažavajući definirane zadaće Vijeća i Koordinacije u tom pitanju, kao i najavljene planove daljnjeg djelovanja Koordinacije domovinske sigurnosti u vidu izrade standardnih operativnih postupaka i priručnika za upravljanje u izvanrednim i kriznim stanjima, može se očekivati da će, kako kroz samostalne aktivnosti Vijeća i Koordinacije planirane u 2019. godini, tako i uz daljnje sudjelovanje Vijeća u aktivnostima Koordinacije za sustav domovinske sigurnosti povezanim s pitanjima kibernetičke zaštite i upravljanja u krizama, i posljednja mjera povezana s ciljem D.5. biti provedena tijekom 2019. godine.

(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 ***sve mjere u 2018. godini provodile u potpunosti ili većoj mjeri, kako je to utvrđeno Akcijskim planom***.

Provedena je revizija transpozicije Direktive 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave (SL L 218/8, 14.8. 2013), na potrebu koje je ukazala EK u svom evaluacijskom Izvješću iz 2017. godine. Izviješće EK je pokazalo potrebu za izmjenom tri kaznena djela iz Glave kaznenih djela protiv računalnih sustava, programa i podataka, i to: neovlašteni pristup (članak 266. Kaznenog zakona), oštećenje računalnih podataka (članak 268. Kaznenog zakona) i zlouporaba naprava (članak 272.

[23] https://www.cert.hr/wp-content/uploads/2018/06/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf

Kaznenog zakona). Slijedom navedenog, u 2018. je izmjenama i dopunama Kaznenog zakona provedena prilagodba navedenih kaznenih djela, čime je ***unaprijeđen zakonodavni okvir u domeni kaznenog prava***. Predstavnici nadležnih tijela aktivno sudjeluju u radu međunarodnih tijela relevantnih za pitanja kibernetičkog kriminaliteta te se vodi računa o potrebama predlaganja izmjena i dopuna kaznenog zakonodavstva. Pokrenut je **projekt elektroničke razmjene e-dokaza**, povodom inicijative EK za uspostavljanjem sustava razmjene e-dokaza u svim državama članicama. Aktivnosti tijela treba nadalje provoditi u forumu kakav trenutno i jeste uspostavljen, kako po pitanju nacionalnih predstavnika, tako i međunarodnih tijela u čijem radu oni sudjeluju. Međutim, Akcijski plan je u utvrđenim mjerama, osim međunarodnog okvira, usmjeren i na nacionalne prilike (poput, primjerice, dosadašnje prakse u primjeni kaznenopravnog zakonodavstva, analize novih modaliteta počinjenja djela i sl.), a koje je također potrebno uzimati u obzir u kontekstu procjene potreba za izmjenama i dopunama u svrhu njegova unaprjeđenja.

Suradnja i učinkovita razmjena informacija na međunarodnoj razini je uspostavljena po svim relevantnim linijama rada. Uspostavljena je ***kvalitetna međuinstitucionalnu suradnju u svrhu učinkovite razmjene informacija na nacionalnoj razini***, a u koju svrhu su nadležna tijela odredila kontakt točke. Nadležna tijela su neposredno komunicirajući uspješno surađivala na konkretnim slučajevima istraživanja kibernetičkog kriminaliteta, a također je suradnja uspješno ostvarivana kroz rad Koordinacije.

Kontinuirana briga o ***jačanju ljudskih potencijala te razvoju i nadogradnji forenzičkih alata i sustava*** postoji te su unaprijeđene postojeće i razvijene nove tehničke mogućnosti sustava za provođenje dokaznih radnji. Nužno je u narednom razdoblju nadalje voditi računa o potrebama osiguranja adekvatne financijske potpore za daljnje jačanje i razvoj.

Također, nastavljena je uspostavljena ***suradnja s gospodarskim sektorom***, no, u mjeri koja još uvijek nije na zadovoljavajućoj razini. U narednom razdoblju nužno je povećati broj predstavnika iz različitih sektora gospodarstva s kojima će se uspostaviti partnerski odnos u razmjeni podataka o zabilježenim incidentima, uz praćenje rezultata uspostavljene suradnje. Novi **Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga** u svakom slučaju će potaknuti ovu suradnju u velikom broju gospodarskih sektora koji su njime regulirani u pitanjima kibernetičke sigurnosti.

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.

U odnosu na potrebu **unaprjeđenja nacionalne regulative u području poslovne tajne**, nije bilo moguće doraditi nacionalnu regulativu, budući da ista gotovo i ne postoji, dok je Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti usmjeren na građansko-pravnu zaštitu poslovnih tajni, čime preciznije i sveobuhvatnije propisivanje sigurnosnih zahtjeva u području zaštite podataka koji predstavljaju poslovnu tajnu i nadalje nije na odgovarajući način riješeno[24]. ***Kako se nositelj određen Akcijskim planom ne smatra nadležnim za rješavanje ovog pitanja, tako provedba mjere nije niti započela, stoga će prilikom revizije Strategije i Akcijskog plana biti potrebno sagledati mogućnosti određivanja drugog nositelja provedbe ove mjere.***

Osigurane zakonske pretpostavke za nastavak provedbe mjera donošenjem Zakona o zaštiti neobjavljenih informacija s tržišnom vrijednosti („Narodne novine“, broj: 30/18). i ***Zakon o provedbi Opće uredbe o zaštiti podataka*** („Narodne novine“, broj: 42/18), nadležna tijela su iskoristila i uspostavila redovitu suradnju u razmjeni iskustava, iznošenju i analiziranju detektiranih problema i/ili uočenih potencijalnih neujednačenosti u primjeni propisa te izmjenjivanju preporuka za njihovo rješavanje, s posebnim naglaskom na donesene promjene zakonskih propisa čije odredbe određuju postupanje sa zaštićenim podacima, **čime se ova mjera provodi u znatnom opsegu**.

Također, učinjena je i operativna analiza u odnosu na promjene glede primjene GDPR-a (Opće uredbe o zaštiti podatka) i procjena potreba usklađivanja nacionalnog zakonodavstva koje iz istog proizlazi.

Provedba aktivnosti usmjerenih na ustrojavanje, obveze i odgovornosti nadležnih tijela, zaštitu i sva druga pitanja bitna za nacionalne elektroničke registre podataka, do sada je u pravilu izostala, osim 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

[24] Djelomično regulirano – glava VIII. Zakona o zaštiti tajnosti podataka („Narodne novine“, broj: 108/96)

se nude i podliježu zaštiti odnosno procesima nadzora definiranim u Uredbi o kibernetičkoj sigurnosti i operatora ključnih usluga i davatelja digitalnih usluga. Nadalje, na 20. sjednici Nacionalnog vijeća za kibernetičku sigurnost prihvaćen je dogovor između MU i Središnjeg državnog ureda za razvoj digitalnog društva (SDURDD) u pogledu promjene nositelja ove mjere te je nositeljem daljnje provedbe ove mjere određen SDURDD.

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 2018. 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. I nadalje se planira praćenje razvoja i primjene novih tehnologija (elektroničke usluge, računalstvo u oblaku i dr.) radi eventualne dopune/modifikacije te dodatne prilagodbe glede primjene Opće uredbe o zaštiti podataka.

Također, u narednom razdoblju ***potrebno je intenzivirati mjere čije su aktivnosti usmjerene na ustrojavanje, obveze i odgovornosti nadležnih tijela, zaštitu i sva druga pitanja bitna za nacionalne registre podataka***, a čija provedba je do sada u pravilu izostala kako zbog kašnjenja u provedbi definiranih mjera, tako i zbog povezanosti s terminskim planom provedbe i rezultatima naprijed spomenutih zakonodavnih procesa.

Tijekom 2018. godine završena je 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. Nastavno na navedeno, ZSIS je prepoznao potrebu uvezivanja naprijed navedenog s novim zakonodavnim okvirom, Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te Općom uredbom o zaštiti podatka, a čija će se primjena moći analizirati u narednom razdoblju.

(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 izradom i službenom objavom Nacionalne taksonomije računalno-sigurnosnih incidenata u 2018. godini. U narednom razdoblju potrebno je pratiti korištenje i primjenu iste te po isteku godine dana od dana primjene provesti analizu potrebe za ažuriranjem taksonomije.

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 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.[25] Novi **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 te će dodatno pospješiti i olakšati nastavak aktivnosti u ovom području.

Aktivnosti ***izvješćivanja dionika unutar sektora o računalnim sigurnosnim incidentima i periodično izvješćivanje Vijeća o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja***, provode se u manjoj mjeri jer nije u potpunosti provedena prethodna mjera prikupljanja podataka o incidentima (u ovisnosti od provedbe mjere G.1.2.[26]). Izvješćivanje se provodi u okviru rada Koordinacije, a u narednoj fazi se očekuje korištenje tih izvješća u svrhu analize trendova.

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. Dodatni poticaj za provedbu ove mjere daje i primjena Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga.

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

[25] Definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka.
[26] Sektorski nadležna tijela prikupljaju podatke o incidentima od dionika, poput regulatora i drugih CERT-ova iz njihove sektorske nadležnosti te objedinjavaju na sektorskoj

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. U narednom je razdoblju potrebno dalje unaprjeđivati suradnju i koordinaciju kroz rad Koordinacije.

(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 2018. godine uključivala je minimalno informiranost na strateškoj razini, prvenstveno u sklopu rada Vijeća, gdje su nositelji aktivnosti izvješćivali Vijeće o aktivnostima u području međunarodne suradnje iz područja kibernetičke sigurnosti.

Mehanizam kontinuiranog izvješćivanja i koordinacije i dalje nije uspostavljen, ali bi tijekom 2019. godine trebao biti uspostavljen kroz nedavno uspostavljenu **Stalnu radnu skupinu za međunarodnu suradnju Vijeća, čijim radom upravlja MVEP.** Uz praćenje međunarodnih aktivnosti još uvijek nedostaje inicijativa za pokretanje vlastitih, kao i ciljana i usklađena koordinacija državnih tijela u smislu promoviranja nacionalnih interesa. Određena poboljšana postignuta u ovom području tijekom 2018. godine, trebaju se iskoristiti u pripremi hrvatskog predsjedavanja Vijećem EU-a 2020. godine, kada se očekuje niz EU aktivnosti u kojima će se moći i trebati pokazati inicijativa nadležnih institucija. Unaprjeđenje provedbe mjere moguće je dodatno ostvariti kroz povezivanje aktivnosti državnih tijela s akademskom zajednicom i gospodarstvom, kroz oblike javno-privatnog partnerstva, na čemu je Vijeće tijekom 2018. godine počelo intenzivnije raditi.

Aktivnosti usmjerene za ***jačom bilateralnom i multilateralnom suradnjom u okviru međunarodnih sporazuma u kojima RH sudjeluje*** tijekom 2018. godine provodile su se u

manjoj mjeri, u okviru raspoloživih financijskih i ljudskih resursa, sudjelovanjem u bilateralnim i multilateralnim aktivnostima kroz redovne nadležnosti nositelja. Također, aktivnosti su poduzimane u okviru implementacije NIS direktive, kroz sastanke odbora i radnih skupina. U narednom razdoblju potrebno je definirati tematska događanja koja je bitno pratiti na međunarodnoj razini, odrediti predstavnike (tijela) koji će biti zaduženi za praćenje pojedine problematike te uvesti koordinirani način razmjene relevantnih informacija prije i poslije sastanaka.

Aktivnosti usmjerene na ***sudjelovanje u diplomatskim aktivnostima u okviru međunarodnih organizacija i drugih foruma radi izgradnje povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija***, provode se u okviru redovnih aktivnosti nositelja u znatnoj mjeri, jednako kao i sudjelovanje i organizacija ***međunarodnih civilnih i vojnih vježbi i drugih stručnih programa*** (kroz NATO vježbu Cyber Coalition 2018, EU vježbu EU Cyber Europe, Kibernetički štit 18, Simpozij „Kibernetička obrana 2018“, NAICS Paintball, Cyber SOPEx, ITU Cyber Drill - ALERT i druge). U narednom razdoblju potrebno je poticati daljnji angažman relevantnih institucija RH u tim aktivnostima, kao i osnažiti međuresornu suradnju.

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.

(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.-2018., za dvije mjere 6 mjeseci, odnosno 12 mjeseci po donošenju Strategije, dok se ostale 22 mjere trebaju provoditi kontinuirano.

U aktivnostima za provedbu mjere kojom ***u programe ranog i predškolskog odgoja treba uvrstiti sadržaje vezane uz kibernetičku sigurnost*** nema pomaka, jer se predstojećim restrukturiranjem osnovnog obrazovanja s osmogodišnjeg na devetogodišnje planira obuhvatiti i predškolski dio obrazovanja.

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. Od školske godine 2018./2019. obavezan predmet *Informatika* uveden je u 5. i 6. razrede osnovne škole, također od školske godine 2017./2018. primjenjuju se novi kurikulum nastave informatike u osnovnim školama i gimnazijama u Republici Hrvatskoj. Kurikulumom su utvrđene domene kojima se realiziraju ciljevi predmeta Informatika: e-Društvo, Digitalna pismenost i komunikacija, Računalno razmišljanje i programiranje te Informacije i digitalna tehnologija. Osim u predmetu Informatika, ove teme obrađuju se i kao međupredmetna tema Uporaba informacijske i komunikacijske tehnologije te također kroz povezanost s ostalim predmetima (medijska pismenost, digitalno stvaralaštvo). Tijekom 2018. godine organizirana je ***edukacija nastavnika*** informatike s ciljem podizanja kompetencija kako bi mogli pripremati aktivnosti i sadržaje za nastavu prema ishodima učenja iz novih kurikuluma. Napravljena je analiza stanja po školama i sukladno iskazanim potrebama škola odlučeno je na temelju podataka o raspoloživoj opremi i starosti opreme te broju učenika da će se osnovne škole opremiti računalnom opremom, što se i provodi u fazama.

Kao i 2017. godine, u 2018. **sadržaji 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 znatnoj mjeri**. U sklopu edukacije učitelja i nastavnika organizirana je 81 virtualna radionica u kojima je sudjelovalo 42724 sudionika. Održano je također i 1092 sati edukacije uživo, a 984 učitelja i nastavnika Informatike prisustvovalo je usavršavanjima. Usprkos postignutom napretku, u narednom je razdoblju ***potrebno nastaviti intenzivno provoditi aktivnosti u ovim mjerama***, posebno usmjerene na poticanje obrazovnog kadra na sudjelovanje na stručnim skupovima i specijalističkim tečajevima s temama kibernetičke sigurnosti.

U aktivnostima mjere ***poticanja uspostavljanja i izvođenja diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti*** nije bilo bitnog pomaka u odnosu na 2017. godinu. Osim minimalnog i nedovoljnog broja studijskih programa usko vezanih uz kibernetičku sigurnost, prethodno uspostavljenih na ***javnim visokim učilištima u RH*,** **nije bilo napretka u provedbi mjere.** U odnosu na izvođenje kolegija iz područja informacijske sigurnosti na javnim visokim učilištima nije evidentiran napredak u 2018. godini. Potrebno je ***u idućim godinama poticati planiranje novih studijskih programa koji u sebi uključuju veći broj kolegija vezano uz informacijsku sigurnost***. Ministarstvo znanosti i obrazovanja ne može utjecati na povećanje broja sadržaja vezanih uz kibernetičku sigurnost na visokim učilištima u Republici Hrvatskoj, jer visoka učilišta imaju zajamčenu autonomiju u skladu s odredbama Zakona o znanstvenoj djelatnosti i visokom obrazovanju te će se o tome trebati voditi računa prilikom revizije Strategije.

U provedbi mjere ***poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja*** **nije evidentiran napredak** u odnosu na 2017. godinu, jer se provedba mjere **naslanja na provedbu kurikularne reforme**.

Aktivnosti u provedbi mjere ***poticanje organiziranja natjecanja u području informacijske sigurnosti*** **provode se u manjoj mjeri i nedostatno**. Poduzete aktivnosti uključuju povećanje broja pitanja iz kibernetičke sigurnosti na natjecanju iz informatike – Osnove informatike. U kurikulumima strukovnih nastavnih predmeta nema predmeta Informatika radi čega Agencija za strukovno obrazovanje i obrazovanje odraslih nije u mogućnosti organizirati natjecanja na temu informacijske sigurnosti. Uvođenjem novog modela natjecanja učenika srednjih strukovnih škola (*WorldSkills Croatia*), otvara se mogućnost za izradu Tehničkog opisa i Modela zadatka za natjecateljsku disciplinu Administracija IT sustava unutar kojih treba adresirati i pojmove kibernetičke sigurnosti.

Mjera ***uvrštavanje teme informacijske sigurnosti u programe sveučilišta kroz programske ugovore*** nije provedena te će istu biti potrebno koncepcijski revidirati prilikom revizije Strategije.

Započelo se s ***uspostavom sustava izobrazbe i provjere znanja iz područja informacijske sigurnosti, koji je ugrađen u odgovarajuće stručne i državne ispite***. Dio izobrazbe je već obuhvaćen državnim stručnim ispitom, u posebnom dijelu stručnog ispita. Sustavna izobrazba državnih službenika provodi se i prilikom imenovanja savjetnika za informacijsku sigurnost u državnim tijelima. U sklopu rada Vijeća nositelji aktivnosti izvješćuju Vijeće o aktivnostima oko uspostave sustava izobrazbe i provjere znanja iz područja informacijske sigurnosti. Državna škola za javnu upravu predvidjela je uvrštavanje programa za stručnu edukaciju državnih službenika iz područja informacijske sigurnosti u izvedbeni plan za 2019. godinu, s temama iz područja informacijske i kibernetičke sigurnosti te provedbu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, u suradnji s UVNS-om, ZSIS-om i NCERT-om.

Stalno ***stručno usavršavanje policijskih službenika*** u području informacijske sigurnosti i kibernetičkog kriminaliteta u organizaciji Policijske akademije i Uprave kriminalističke policije i organizaciji Europol-a i CEPOL-a, kao i ***osiguranje potrebnih ekspertiza i specijalističkih znanja potrebnih za CERT funkcionalnosti, kroz definiranje godišnjih lista izobrazbi, tečajeva, seminara i drugih oblika usavršavanja*** (Nacionalni CERT, ZSIS, MORH CERT) **provodi se u znatnoj mjeri i kontinuirano**.

Pravosudna akademija je u 2018. godini u provedbi ***mjere stalnog stručnog usavršavanja državnih odvjetnika i sudaca u području informacijske sigurnosti i kibernetičkog kriminaliteta*** organizirala dvije dvodnevne radionice na temu kibernetičkog kriminaliteta za suce i državne odvjetnike, a na istima su sudjelovali i predstavnici sudstva, državnog odvjetništva, UVNS-a, ZSIS-a, NCERT-a te MUP-a. Nastavno na provedenu radionicu, Pravosudna akademija u 2019. godini planira provesti specijalistički modul edukacije na temu kibernetičkog kriminaliteta u suradnji s nadležnim tijelima.

Iako se mjera ***sigurnosnog osvješćivanja i edukacijskih kampanja najšire javnosti*** **provodi kontinuirano**, još uvijek nije uspostavljena potpuno učinkovita horizontalna koordinacija, već se aktivnosti u razvijanju programa sigurnosnog osvješćivanja i obrazovnih kampanja usmjerenih na najširi krug korisnika postojećih i svih budućih elektroničkih usluga u RH te osiguranje ujednačene provedbe kroz usmjeravanje i obvezivanje različitih operatora i davatelja usluga u RH na provedbu odgovarajućih mjera prema svojim korisnicima, provodi na razini sektorskih nositelja u okvirima njihovih redovitih aktivnosti. U narednom je razdoblju potrebno dodatno poboljšati horizontalnu koordinaciju ovih aktivnosti i tema koje se obuhvaćaju na nacionalnoj razini.

Pojedinačne aktivnosti u provedbi mjere ***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*** provode se kontinuirano, putem programa i projekata Hrvatske akademske i istraživačke mreže - CARNET-a (informira i educira učenike, nastavnike, stručne suradnike te roditelje o odgovornom korištenju informacijskih i komunikacijskih tehnologija), Sveučilišnog računskog centra SRCE (programi namijenjeni akademskoj zajednici - studentima i zaposlenicima visokih učilišta) te Fakulteta organizacije i informatike Sveučilišta u Zagrebu (uključen u organiziranje konferencije o informacijskoj sigurnosti, organizira ljetne škole iz područja informacijske i kibernetičke sigurnosti). Međutim, izostaje cjelovita koordinirana provedba mjere na razini i kroz aktivnosti nositelja i sunositelja, jer se provedba mjere naslanja na provedbu kurikularme reforme.

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, kao što je CARNET-ova korisnička

konferencija CUC 2018. Tiskana brošura bit će dostupna i u 2019. godini kroz edukacije (radionice), vježbe, konferencije i druga događanja.

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**. Ministarstvo uprave RH provodi projekt redizajna sustava e-Građani. Također, radi se i na projektu standardiziranja elektroničkih usluga koji će definirati bitne standarde svake elektroničke usluge koja 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**. HNB je u svibnju 2018. održala radne sastanke sa sistemski važnim kreditnim institucijama vezano uz funkcionalnost i sigurnost informacijskih sustava. Provode se objave (elektroničkom poštom) svim kreditnim institucijama o uočenim sigurnosnim ranjivostima i preporukama za daljnje postupanje te objave o odgovornostima uz njihov djelokrug rada. HNB je u lipnju 2018. organizirala radionicu za sve kreditne institucije, institucije za platni promet te institucije za elektronički novac o sigurnosnim zahtjevima koji proizlaze iz Zakona o platnom prometu i dodatnim zahtjevima po posebnim propisima. Također je HNB organizirala radionicu za sve ostale sistemski važne kreditne institucije (operatori ključnih usluga) o Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te pripadajućoj Uredbi, kao i Smjernicama za prijavljivanje incidenata. Pored navedenog provode se kontinuirano i druge aktivnosti, kao i pojedinačna korespondencija s kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac o aktualnim i potencijalnim sigurnosnim prijetnjama.

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, iako je izostala formalna suradnja nositelja te su aktivnosti provođene samostalno. Provedene aktivnosti uključuju obilježavanje europskog mjeseca informacijske sigurnosti, Dana sigurnijeg interneta, izdavanje brošura o sigurnosti na Internetu, izradu aplikacija za bolje informiranje korisnika i kontinuirano gostovanje stručnjaka nositelja mjera u školama (HAKOM), kao i objavu aktualnih novosti u području kibernetičke sigurnosti i informacijsko – komunikacijske tehnologije te sigurnosnih preporuka. Održavana su predavanja, radionice, prezentacije te webinari za obrazovni, akademski i poslovni sektor i sudjelovanje na više konferencija. Nastavljena je suradnja s visokoškolskim i istraživačkim ustanovama u pogledu pisanja i izdavanja stručnih dokumenata. Ugovorena je usluga produkcije nacionalne kampanje za podizanje svijesti o važnosti kibernetičke sigurnosti u sklopu projekta GrowCERT. Prisutnost Nacionalnog CERT-a u javnosti se povećala otvaranjem stranice CERT.hr na društvenoj mreži Facebook. Potrebno je dalje nastaviti s aktivnostima u provedbi mjere te formalno uskladiti suradnju i provedbu aktivnosti između nositelja.

***Osmišljavanje i provođenje usklađene kampanje o podizanju svijesti o značaju kibernetičke sigurnosti za državna tijela i pravne osobe s javnim ovlastima*, provođeno je u manjoj 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 i Pravosudne akademije u smislu držanja predavanja i osmišljavanja programa koji bi pokrili ovu temu. Zavod za sigurnost informacijskih sustava je kao nositelj mjere redovno provodio aktivnosti na podizanju svijesti o važnosti kibernetičke sigurnosti na stručnim konferencijama i skupovima te je za predstavnike državnih tijela organizirao Konferenciju o sigurnosti informacijskih sustava. Provođena je edukacija državnih odvjetnika u organizaciji Pravosudne akademije.

Koordinaciji za sustav domovinske sigurnosti predložena je provedba aktivnosti simulacija kibernetičkih napada u svrhu jačanja sigurnosne svijesti i sigurnosne kulture, kao i izrada preporuka za povećanje sigurnosti komunikacije e-poštom, što je i usvojeno u Godišnjem planu rada Koordinacije za sustav domovinske sigurnosti za 2019. godinu. Sukladno navedenom, intenziviranje provedbe ove mjere očekuje se u 2019. godini.

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**, ali većinom sektorski. Provođene su kampanje te je izrađen promotivni materijal o najčešće korištenim financijskim internetskim prijevarama i kako ih izbjeći. Također se objavljuju informacije o ranjivostima koje se mogu multiplicirati s ciljem zaštite i sprječavanja mogućeg daljnjeg širenja računalno-sigurnosnih incidenata. U narednom je razdoblju potrebno suradnju i koordinaciju podići na višu razinu nacionalne usklađenosti.

U 2018. godini ***provođene su 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.

Također su ***provođene aktivnosti 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 narednom je razdoblju potrebno i nadalje poticati aktivniji pristup organizaciji ovakvih skupova i drugih sličnih oblika razmjene iskustava, znanja i najbolje prakse, kao i ukazivati znanstvenicima na važnost informacijske i kibernetičke sigurnosti i u tim ih okvirima poticati na istraživanja u ovim područjima.

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 **nisu sustavno započete**, jer nisu osigurana sredstva za provedbu tih mjera u okviru proračuna nositelja mjere. U okviru buduće revizije Strategije i mjera Akcijskog plana bit će u njihovu provedbu potrebno uključiti i druga relevantna tijela i institucije, odnosno poticati koncept javno-privatnog parnerstva.

U 2018. 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**. Intenziviranje aktivnosti u 2019. godine predviđeno je kroz tematsku sjednicu Vijeća na temu „digitalno gospodarstvo i kibernetička sigurnost“ i sastanke s gospodarskim subjektima koji se bave kibernetičkom sigurnošću.

IV. ZAKLJUČAK

Nastavak provedbe Akcijskog plana tijekom 2018. godine rezultirao je značajnim povećanjem sigurnosne svijesti na nacionalnoj razini i puno boljim razumijevanjem problematike kibernetičke sigurnosti u različitim institucijama i sektorima koji su uključeni u provedbu Akcijskog plana. Institucije koje su dionici Strategije i provode mjere iz Akcijskog plana sve bolje prepoznaju i povezuju aktivnosti iz svoje temeljne nadležnosti s tematski koncipiranim mjerama Akcijskog plana, ali još uvijek se uočava nedovoljna horizontalna suradnja s drugim nadležnim tijelima u provedbi mjera, osobito između institucija koje pripadaju različitim sektorima.

U području kritične komunikacijske i informacijske infrastrukture i upravljanju krizama napravljen je iznimno veliki iskorak 2018. godine donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i pripadajuće Uredbe, čijim su se donošenjem ujedno uskladile i obveze koje za RH proizlaze iz zahtjeva provedbe EU NIS direktive. Time se RH pozicionirala na mapi EU država članica u skupinu država koje imaju uspješno verificiranu nacionalnu strategiju kibernetičke sigurnosti i koje su uspješno pokrenule rješavanje iznimno složene problematike kritične komunikacijske i informacijske i infrastrukture.

Važno je naglasiti kako i područje obrazovanja i razvoja sigurnosne svijesti, koje je u vrijeme donošenja aktualne Strategije bilo u velikom zaostatku u odnosu na većinu drugih područja obuhvaćenih Strategijom, danas počinje uspješno dostizati korak s razvojem ostalih područja na koja se referira Akcijski plan.

Dosadašnje iskustvo s provedbom Akcijskog plana u razdoblju od 2016. godine do danas, jasno pokazuje potrebu aktivnog usmjeravanja provedbe mjera iz Akcijskog plana, jer su ključni rezultati u provedbi Akcijskog plana postignuti u 2017. i 2018. godini, odnosno nakon uspostavljanja i početka rada Vijeća, kao međuresornog tijela kojeg sada čine predstavnici 18 institucija.

Ažuriranje Strategije i pripadnog Akcijskog plana, koje se planira Vladi RH predložiti do kraja 2019. godine, temeljit će se na analizi niza uspješno provedenih ciljeva Strategije u proteklom razdoblju, na promjeni pristupa ciljevima koji nisu u potpunosti ostvareni ili njihovo ostvarenje sporije napreduje, kao i na uvođenju novih ciljeva koje diktira globalno okruženje i brzi razvoj informacijske i komunikacijske tehnologije. Jedno od tih područja koje treba posebno adresirati ažuriranjem Strategije, svakako je potreba učinkovitije i formalnije međusektorske koordinacije između državnog, akademskog i privatnog sektora.