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

IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2017. GODINI

Zagreb, 12. srpnja 2018.

Osvrt na recentno razdoblje izvješćivanja

Godina 2017. u mnogim je elementima bila godina prekretnice u globalnom kibernetičkom prostoru. To se prvenstveno odražava na puno jasnije globalno prepoznavanje sve veće ovisnosti društva o novim tehnološkim konceptima od kojih su u 2017. godini u velikoj mjeri dominirale društvene mreže, računalstvo u oblaku i Internet stvari (Internet of Things - IoT). Svijest o tehnološkoj ovisnosti i prepoznavanje tehnoloških koncepata o kojima društvo postaje sve više zavisno, dovodi i do šire globalne svijesti o izloženosti suvremenog društva novim ugrozama koje neumitno prate sve tehnološke razvoje.

Brigu o utjecaju javnog mnijenja putem komunikacijskih kanala različitih globalno rasprostranjenih društvenih mreža vidimo kroz sve veću zabrinutost država za procese političkih izbora, inicirane posljednjim predsjedničkim izborima u SAD-u, što je nakon „zabrinutosti" za nacionalne izborne procese, primjerice u Njemačkoj ili Nizozemskoj, danas već poprimilo prve oblike formalnih postupaka o kojima i Europska unija (u daljnjem tekstu: EU) razmišlja u susret idućim izborima za EU parlament[1].

Sve značajniji izazov predstavljaju novi globalni kanali utjecaja koji paralelno s tradicionalnim javnim medijima postaju sve više i formalni predmet sigurnosne politike u smislu prepoznavanja, prevencije i suzbijanja dijela tzv. hibridnih prijetnji. Unatoč javno prisutnom jednostavnom shvaćanju hibridnog kao sučeljavanja fizičkog i kibernetičkog prostora, hibridne prijetnje se moraju tretirati bitno sustavnije[2] *kako bi se shvatili njihovi stvarni uzroci i dosezi, koji su puno dublji od odabranog korištenja nekog od vektora napada. Iako vektori napada danas u mnogo slučajeva predstavljaju kibernetičke napade, poput hakiranja računa e-pošte nekog političkog dužnosnika*[3]*, ili NonPetya*[4] *malicioznog napada, oni u slučajevima hibridnih prijetnji predstavljaju samo jedan od načina ostvarenja viših ciljeva*

[1] http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614650/EPRS_IDA(2018)614650_EN.pdf

[2] Hibridne prijetnje u svojoj osnovi predstavljaju način utjecaja na elemente državne organizacije, te je u većini slučajeva (SAD, EU) zastupljen tzv. DIMEFIL način praćenja domena hibridnih prijetnji (DIMEFIL = Diplomacy, Information, Military, Economy, Financial, Intelligence, Law Enforcement/Legal). Ovisno o metodi pristupa koriste se različiti indikatori intenziteta i međusobnog utjecaja, odnosno zahvaćenosti više domena od interesa.

[3] https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html?rref=collection%2Fnewseventcollection%2FRussian%20Hacking%20in%20the%20U.S.%20Election

[4] Za razliku od malicioznog koda *Petya* koji je ucjenjivački kripto- kod, *NonPetya* je na prvi pogled sličan ucjenjivačkom kripto- kodu, ali za koji se ustanovilo da ne omogućava napadnutom korisniku dekriptiranje podataka, odnosno, otkup ključa. Stoga cilj *NonPetya* napada nije zaraditi nego uništiti podatke na računalu koje je napao, iako je temeljena na istoj ranjivosti koja je korištena i u ranijim *Petya* i u *WannaCry* napadima. U ovom slučaju je Velika Britanija izašla s prvom formalnom atribucijom napada na Rusiju i vojno-obavještajne organizacije, koristeći upravo popratna svojstva samog tehničkog vektora napada i prepoznavši tako hibridni napad na sustave kritične infrastrukture u Ukrajini koji se zbog korištenja neselektivne ranjivosti proširio globalno kao i drugi spomenuti napadi (https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks)

puno ozbiljnijeg napadača, koji u pojedinim slučajevima samo koristi „usluge" hakerskih grupa ili pojedinaca, a koji toga čak i ne moraju biti svjesni.

Računalstvo u oblaku na prijelazu godine ulazi sve više i na velika vrata u prihvatljive koncepte tehnološke platforme te i u međunarodne organizacije poput Organizacije Sjevernoatlantskog ugovora (u daljnjem tekstu: NATO) i EU, ali i sve zemlje članice, koje su do sada već uvele procese koje se, u većoj ili manjoj mjeri, oslanjaju na ovaj tehnološki koncept. Računalstvo u oblaku ušlo je na mala vrata u EU[5] znatno prije aktualne EU GDPR[6] regulative, no u skladu s konceptima koje će u 2018. primijeniti sve zemlje obveznice GDPR-a. Rješenja za državni sektor su također u pripremi u mnogim zemljama[7], a međunarodne organizacije poput MISWG-a[8] pripremaju rješenja koja bi u određenim uvjetima mogla biti prihvatljiva i za problematiku vezanu za sigurnost poslovne suradnje i klasificirane ugovore. Sličan tehnološki prodor sve učestalijeg korištenja[9] prisutan je u području Interneta stvari (IoT), počevši od automatizacije i povezanosti aparata i usluga na razini obiteljskih kućanstava, pa sve do kompleksnih proizvodnih procesa u nizu industrijskih grana.

Svi ovi tehnološki i društveni procesi imaju i svoju snažnu gospodarsku dimenziju koja je već postala vidljiva u pristupu Europske komisije digitalnom gospodarstvu. Jedinstveno EU digitalno tržište je na najvišem mjestu prioriteta političke i razvojne agende EU-a i rezultira nizom povezanih aktivnosti koje imaju za cilj osiguravanje razvoja i održivosti digitalnog gospodarstva. Digitalna transformacija organizacija i državne uprave, revizija koncepta obrazovanja i šira svijest o potrebi cjeloživotnog obrazovanja samo su neki od sustavnih aktivnosti koje EU i zemlje članice provode. Kibernetička sigurnost u ovakvom pristupu mora biti duboko ugrađena u sve segmente društva, državne uprave i ekonomije i u tom smislu je koncipirana i Nacionalna strategija kibernetičke sigurnosti Republike Hrvatske kao i rad Nacionalnog vijeća za kibernetičku sigurnost u njegovoj prvoj godini postojanja.

Sve veća izloženost informacijskih tehnologija zlonamjernim aktivnostima raznih interesnih skupina ili pojedinaca pokazuje kako je sustavan i koordiniran angažman država u podizanju svojih sposobnosti u području kibernetičke sigurnosti ključan za izgradnju sigurnog društva u kibernetičkom prostoru. U vrijeme izrade Nacionalne strategije kibernetičke sigurnosti (2014. – 2015.) odvijao se niz malicioznih kampanja s masovnim slanjem lažne e-pošte (phishing), koja je tekstualno prilagođenim sadržajem ciljala na krađu važnih i osobnih podataka brojnih hrvatskih korisnika različitih elektroničkih usluga (najčešće e-pošte i e-bankarstva). U to vrijeme Hrvatsku je pogodio i veliki ciljani kibernetički napad na pravne osobe, korisnike

[5] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[6] http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr
[7] https://ukcloud.com/wp-content/uploads/2017/05/Whitepaper-Bringing-clarity-to-the-cloud1.pdf
[8] *Multinational Industrial Security Working Group* - MISWG
[9] https://www.forbes.com/sites/louiscolumbus/2017/11/12/2017-internet-of-things-iot-intelligence-update/#3194a9ce7f31

usluga e-bankarstva te smo bili suočeni i s tzv. naprednim ustrajnim prijetnjama (APT), kojima je cilj bio uspostaviti vanjsku kontrolu i upravljanje korisničkim računalima u svrhu krađe novca s računa korisnika e-bankarstva. Sličan, ali još sofisticiraniji način napada špijunskim malicioznim kodom pogodio je tijekom prošlih nekoliko godina niz državnih institucija u više zemalja članica EU-a, uključujući i Republiku Hrvatsku (u daljnjem tekstu: RH), a napose institucije koje su koncentratori političkih informacija i poželjna meta za ovakve napade aktera sponzoriranih politikama nekih država.

RH nije bila ciljem velikih napada na kritičnu infrastrukturu za razliku od brojnih drugih država, uključujući i članice EU, ali takav napad u bliskoj budućnosti se ne može isključiti. Niz napada u Ukrajini (uključujući spomenuti NonPetya maliciozni kod), koji je u prošloj godini pogodio energetske objekte, državne institucije i tvrtke, još jednom je pokazao visoku ovisnost država o informacijskoj tehnologiji te razornu moć ovakvih tehnološko sofisticiranih napada, koji napadom na informacijske resurse onemogućavaju rad određene vitalne infrastrukture društva i paraliziraju cijele društvene sektore.

Zamjetan je stalni porast broja kaznenih dijela u EU, a i u RH, u području kibernetičkog kriminaliteta, posebno u dijelu računalnih prijevara. U europskim državama broj kaznenih dijela iz područja kibernetičkog kriminaliteta doseže i do 20% u ukupnom broju kaznenih dijela i može se očekivati da će u budućnosti to biti dominantno područje kriminaliteta. Kriminal i ovdje samo prati gospodarski rast digitalne ekonomije. Poučene ovakvim iskustvom, mnoge europske države kibernetičku sigurnost postavljaju kao prioritetno područje nacionalne sigurnosti.

Posljednji globalni kibernetički napad ucjenjivačkim malicioznim kodom u okviru kampanje WannaCry u svibnju 2017. godine, pokazao je visok stupanj ovisnosti niza industrijskih sektora o suvremenoj informacijskoj tehnologiji, a osobito je pokazao moguće devastirajuće posljedice u zdravstvenom sektoru Ujedinjene Kraljevine. Upravo u ovom globalnom napadu hrvatska međuresorna tijela, Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost, iako tek konstituirana, uspješno su reagirala i uspostavila pravovremenu i učinkovitu koordinaciju i kriznu komunikaciju na najširoj horizontalnoj razini hrvatskog društva i svih njegovih sektora, osiguravajući time i minimalnu štetu po hrvatsko društvo u cjelini.

Kibernetički napadi doveli su do značajne promjene u percepciji važnosti kibernetičkog prostora za suvremeno društvo, a slijedno tome i do promjene pristupa kibernetičkoj sigurnosti, kako na razini međunarodnih organizacija tako i na razini država članica. NATO 2016. godine uvodi kibernetički prostor kao novu dimenziju vojnog djelovanja, uz tradicionalna područja kopna, zraka i mora, odnosno svemira. EU 2016. godine, na temelju svojeg kibernetičkog strateškog okvira iz 2013. godine, donosi Direktivu o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS Direktiva).

Vlada Republike Hrvatske u ovom razdoblju donosi Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu, Odluku o osnivanju međuresornih tijela za upravljanje provedbom Strategije[10], te početkom 2017. godine osigurava i puno pokretanje rada međuresornih upravljačkih tijela Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost. Tijekom 2017. pokrenuta je i nacionalna transpozicija EU NIS direktive koja će se dovršiti tijekom prve polovine 2018. godine. Sve ovo preduvjet je uspješnog razvoja hrvatskog društva i konkurentnosti na jedinstvenom digitalnom tržištu EU.

[10] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016, 28/2018)

SADRŽAJ

I. UVOD

Nacionalna strategija kibernetičke sigurnosti (u daljnjem u tekstu: Strategija) donesena je na sjednici Vlade Republike Hrvatske održanoj 7. listopada 2015. godine.

Strategijom su definirani ciljevi za 5 područja kibernetičke sigurnosti, koja ujedno predstavljaju segmente društva procijenjene kao sigurnosno najvažnije za RH u odnosu na stupanj razvoja informacijskog društva.

Radi osiguranja koordiniranog planiranja svih zajedničkih aktivnosti i resursa u odabranim područjima kibernetičke sigurnosti, Strategija prepoznaje i 4 poveznice područja kibernetičke sigurnosti, za koje, također kroz definiranje posebnih ciljeva, opisuje rezultate koji se kroz provođenje strateškog okvira žele postići.

Ciljevi definirani Strategijom kibernetičke sigurnosti po područjima i poveznicama područja kibernetičke sigurnosti razrađeni su Akcijskim planom za provedbu nacionalne strategije kibernetičke sigurnosti11 (dalje u tekstu: Akcijski plan).

Svaka mjera, koja je razrađena u Akcijskom planu u svrhu postizanja nekog posebnog cilja u jednom od područja ili poveznica područja, doprinosi postizanju općih ciljeva Strategije iz kojih su izvedeni svi posebni ciljevi. Tako je za 8 općih ciljeva Strategije, razrađeno 35 posebnih ciljeva u okviru 5 područja kibernetičke sigurnosti i 4 poveznica područja, čija je daljnja razrada rezultirala s ukupno 77 mjera razrađenih u Akcijskom planu. Akcijski plan obuhvaća ovih 77 mjera, 33 mjere u područjima kibernetičke sigurnosti te 44 mjere u poveznicama područja kibernetičke sigurnosti:

Područja kibernetičke sigurnosti:

A. Javne elektroničke komunikacije – 3 mjere

B. Elektronička uprava – 8 mjera

C. Elektroničke financijske usluge – 4 mjere

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

E. Kibernetički kriminalitet – 5 mjera

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera

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

H. Međunarodna suradnja – 6 mjera

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

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

[11] Strategija i Akcijski plan doneseni Odlukom Vlade RH objavljene u „Narodnim novinama“, broj: 108/2015 i čine njezin sastavni dio.

nadzor njezine provedbe te uvela kontrolni mehanizam pomoću kojeg će se moći vidjeti je li određena mjera provedena u potpunosti i je li polučila željeni rezultat ili ju je potrebno redefinirati u skladu s novim potrebama.

Za sustavno praćenje i koordiniranje provedbe Strategije zaduženo je Nacionalno vijeće za kibernetičku sigurnost12 (u daljnjem tekstu: Vijeće), koje u tu svrhu provodi horizontalnu koordinaciju prema nositeljima mjera.

Većina ključnih obveznika provođenja mjera poimence je nabrojena u Akcijskom planu, dok će za manji broj institucija obveza provođenja biti utvrđena nakon provedbe nekih predradnji (npr. vlasnici/upravitelji kritične infrastrukture kada se ta infrastruktura definira). Nositelji mjera koji su izravno identificirani su:

- Agencija za odgoj i obrazovanje
- Agencija za strukovno obrazovanje i obrazovanje odraslih
- Agencija za zaštitu osobnih podataka
- CARNET
- Državna uprava za zaštitu i spašavanje
- HAKOM
- Hrvatska narodna banka
- Ministarstvo gospodarstva, poduzetništva i obrta
- Ministarstvo obrane
- Ministarstvo pravosuđa
- Ministarstvo unutarnjih poslova
- Ministarstvo uprave
- Ministarstvo vanjskih i europskih poslova
- Ministarstvo znanosti i obrazovanja
- Nacionalni CERT
- Nacionalno vijeće za kibernetičku sigurnost
- Operativno-tehnički centar za nadzor telekomunikacija
- Pravosudna akademija
- Sigurnosno-obavještajna agencija
- Sveučilišni računski centar
- Ured Vijeća za nacionalnu sigurnost
- Vojna sigurnosno-obavještajna agencija
- Zavod za sigurnost informacijskih sustava

Mjere Akcijskog plana uključuju i niz drugih tijela koja su funkcionalno definirana (npr. središnja tijela državne uprave u suradnji s regulatornim agencijama i strukovnim udruženjima

[12] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016).

za svaki pojedini sektor kritične infrastrukture). U svim mjerama koje uključuju više nositelja/sunositelja nužno je koordinirano djelovanje, kako bi se postigao sinergijski učinak njihovog rada. U provedbu mjera nositelji mogu uključiti i druge organizacije i stručnjake kada to ocijene potrebnim.

Ovo Izvješće izrađeno je na temelju podataka koje je odlukom Nacionalnog vijeća za kibernetičku sigurnost prikupio Ured Vijeća za nacionalnu sigurnost, kao tijelo koje predsjedava Nacionalnim vijećem za kibernetičku sigurnost i osigurava administrativno-tehničku podršku radu Vijeća. Izvješća od tijela koja su, prema Akcijskom planu, odgovorna kao nositelji provedbe predviđenih mjera prikupljena su na standardiziranim obrascima tijekom travnja i svibnja 2018. godine.

II. ANALIZA PROVEDBE MJERA PO PODRUČJIMA KIBERNETIČKE SIGURNOSTI

Javne elektroničke komunikacije (A)

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).

Od 1.1.2017. su u primjeni novi akti kojim se uređuju minimalne sigurnosne mjere, opisani sigurnosni incidenti i kriteriji za izvješćivanje o tim sigurnosnim incidentima, te je uvedena obveza provedbe godišnje revizije informacijskih sustava, kao i obveza obavješćivanja o određenim pojavnostima koje mogu negativno utjecati na obavljanje djelatnosti javnih komunikacijskih mreža i/ili usluga. Nadležno tijelo je na taj način ***provelo mjeru provedbe nadzora.*** Preporuča se daljnje praćenje provedbe mjere, te donošenje konačne ocjene uspješnosti u sklopu postupka izvještavanja za sljedeće izvještajno razdoblje (2017. godinu).

Tehnička koordinacija regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti prije svega se ***provodi u okviru Operativno-tehničke koordinacije za kibernetičku sigurnost***[13]. Zasebno planirane aktivnosti u cilju provođenja ove mjere nisu planirane ili provođene.

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

[13] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016).

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.

Elektronička uprava (B)

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 **ciljeve (ukupno 3)** usmjerene na stvaranje pretpostavki za postizanje više razine sigurnosti uspostavljenog sustava, kroz:

- **Poticanje na povezivanje informacijskih sustava tijela javnog sektora međusobno i na javni 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 dijelu međusobno slijednih i ovisnih, s opisanim konkretnim pokazateljima provedbe, te jasno određenim rokovima. **Od 8 utvrđenih mjera provedena je samo jedna - definirani su organizacijski i tehnički zahtjevi za povezivanje na državnu informacijsku infrastrukturu**.

S obzirom na predstojeće aktivnosti u digitalizaciji javne uprave, u narednom razdoblju potrebno je podići svijest o važnosti uloge nadležnog tijela u ostvarenju gore opisanih ciljeva, odrediti koordinatore za pojedine mjere, te pokrenuti mjere.

Elektroničke financijske usluge (C)

Sigurnosni zahtjevi koji se provode u području elektroničkih financijskih usluga osiguravaju visoku razinu sigurnosti za njezine korisnike.

Poticanje razvoja elektroničkih 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.**
- **Unapređenje 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.

Dostavljena izvješća pokazuju da su ***mjere provođene, ali ne i ostvarene u potpunosti.***

Smjernice o ***sigurnosti internetskih plaćanja*** su izrađene još 2015. g., te prezentirane širem krugu institucija bankarskog sektora, platnog prometa i najznačajnijih institucija za elektronički novac. Provjera usklađenosti relevantnih institucija s odredbama Smjernica bit će te provedena u narednom razdoblju, kroz supervizije i nadzorne mjere središnje nacionalne banke.

Provedba nacionalnih aktivnosti u domeni ***sigurnosti mobilnih plaćanja***, prema Akcijskom planu, ovisi o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europske agencije za bankarstvo (EBA).

Iz dostavljenih podataka proizlazi da ti postupci moguće neće uslijediti, te da je daljnje aktivnosti na nacionalnoj razini potrebno planirati u ovisnosti od normativnog postupka koji se na nivou EU provodi u domeni platnih usluga, u okviru kojeg bi trebale uslijediti i regulatorni tehnički standardi i smjernice.

Stoga se svakako preporuča daljnje praćenje ove problematike, koje će uključivati i prikupljanje podataka o provedbi mjere Akcijskog plana koja se na nju odnosi i za sljedeće izvještajno razdoblje.

Druge dvije mjere Akcijskog plana trebaju rezultirati unapređenjem ***razmjene i ustupanja podataka o nastalim računalnim sigurnosnim incidentima*** između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela.

Izvješće s procjenom zakonskih mogućnosti, ograničenja te poželjnih mehanizama razmjene informacija o incidentima vezanima uz informacijske sustave kreditnih institucija s relevantnim institucijama u RH je izrađeno. Provedba je usko vezana uz postupke i rokove za implementaciju koje je definirala Europska centralna banka (ECB) i Europsko nadzorno tijelo za bankarstvo (EBA). EBA je objavila Smjernice za izvješćivanje o incidentima u veljači 2018. te se rezultati mjere mogu očekivati tijekom 2018. Stoga se svakako preporuča daljnje praćenje provedbe mjere.

Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama (D)

Prema Strategiji, kritičnu komunikacijsku i informacijsku infrastrukturu predstavljaju oni komunikacijski i informacijski sustavi koji upravljaju kritičnom infrastrukturom ili su bitni za njezino funkcioniranje, neovisno o kojem sektoru kritične infrastrukture je riječ. Sustav upravljanja kibernetičkim krizama, pri tome ima za cilj osigurati pravovremenu i učinkovitu reakciju/odgovor na prijetnju i osigurati oporavak infrastrukture ili usluge od naročitog sigurnosnog interesa za RH.

Sustav upravljanja u kibernetičkim krizama u RH potrebno je uspostaviti u skladu sa sljedećim zahtjevima:

1. usklađenost s nacionalnim rješenjima upravljanja u krizama,

2. obuhvaćanje zaštite kritične nacionalne komunikacijske i informacijske infrastrukture,
3. usklađenost s međunarodnim sustavima upravljanja u kibernetičkim krizama EU-a i NATO-a,
4. usklađenost s nacionalnim nadležnostima tijela zakonom zaduženih za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

U cilju zaštite procesa koji su ključni za funkcioniranje države i gospodarstva, kao i uspostave učinkovitog odgovora na moguće krize, Strategijom je definirano **5 ciljeva** usmjerenih na:

- **utvrđivanje kriterija za prepoznavanje kritične komunikacijske i informacijske infrastrukture;**
- **utvrđivanje obvezujućih sigurnosnih mjera koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture;**
- **jačanje prevencije i zaštite kroz upravljanje rizikom;**
- **jačanje javno-privatnog partnerstva i tehničke koordinacije u obradi računalnih sigurnosnih incidenata;**
- **uspostava kapaciteta za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu.**

Za ostvarivanje ovih ciljeva Akcijskim planom je predviđeno provođenje 13 mjera. Preduvjet za provođenje ovih mjera je identifikacija nacionalnih kritičnih infrastruktura. ***Vlada je*** svojom Odlukom[14] ***definirala kritične nacionalne sektore***, ali je ***izostala identifikacija konkretnih infrastruktura u tim sektorima*** te samim tim i određivanje dodatnih sigurnosnih zahtjeva prema istima.

Vijeće je na temelju rezultata provedbe Akcijskog plana u 2016. godini zaključilo kako postoji ključni problem u ***nedovoljnom stupnju provedbe Zakona o kritičnim infrastrukturama*** („Narodne novine“, broj: 56/13), ali i ***dodatni problem pristupa kritičnim sektorima*** koji se u ovom Zakonu ne razmatraju iz kuta ovisnosti o komunikacijskoj i informacijskoj tehnologiji već se komunikacijska i informacijska tehnologija tretira kao jedan od kritičnih sektora.

S obzirom na nedostatno stanje provedbe u segmentu kritičnih nacionalnih sektora te na obavezu RH za provedbu EU NIS Direktive[15] u 2018. godini, Vijeće je u svibnju 2017. godine odlučilo uspostaviti radnu skupinu Vijeća za pripremu provedbe NIS direktive, čiji rad koordinira Ured Vijeća za nacionalnu sigurnost. Ovaj proces pokrenut je na temelju visokog stupnja korelacije između EU strategije kibernetičke sigurnosti i NIS direktive te Nacionalne strategije kibernetičke sigurnosti RH, odnosno ***Odluke Vlade RH o uspostavi međuresornih tijela, Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost***, kao i formata za suradnju predviđenih u NIS direktivi, NIS skupine za stratešku suradnju i CSIRT mreže za operativno-tehničku suradnju. Dodatno, pristup koji se koristi u NIS direktivi u potpunosti je primjeren kibernetičkom prostoru jer promatra ovisnosti

[14] Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura („Narodne novine“, broj: 108/13).
[15] Direktiva (EU) 2016/1148 EP i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije od 6. srpnja 2016. (Network and Information Security Directive), https://ec.europa.eu/digital-single-market/en/cybersecurity

definiranih sektora i podsektora u odnosu na mrežnu i informacijsku infrastrukturu te omogućava dodatna proširenja izbora sektora i podsektora na nacionalnoj razini.

Radna skupina Vijeća za transpoziciju NIS direktive započela je rad u lipnju 2017. te je izradila **NIS transpozicijski plan koji je predvidio donošenje nacionalnog Zakona o kibernetičkoj sigurnosti operatora ključnih usluga[16] i davatelja digitalnih usluga[17]** te ***podzakonsku Uredbu*** Vlade RH istog naziva. Do kraja 2017. godine NIS radna skupina pripremila je tekst Nacrta Zakona za proces javnog savjetovanja i određen je opseg razrade podzakonske Uredbe.

NIS transpozicijski plan i izrađeni Nacrt Zakona u potpunosti zadovoljavaju pet ciljeva područja Kritične komunikacijske i informacijske infrastrukture i upravljanja u kibernetičkim krizama, kako su određeni Nacionalnom strategijom kibernetičke sigurnosti i ovdje citirani, a u potpunosti zadovoljavaju i četiri zahtjeva postavljena u Strategiji za sustav upravljanja krizama kibernetičke sigurnosti u RH. S obzirom na sve izneseno, Vijeće planira tijekom 2018. godine pratiti i prema potrebi usmjeravati proces implementacije Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te podzakonske Uredbe te u okviru ovog procesa i dodatnih aktivnosti Vijeća i Koordinacije, osigurati puno postizanje svih postavljenih ciljeva i zahtjeva Strategije u području kibernetičke sigurnosti D.

Primjer dodatnih aktivnosti Vijeća u ovom području predstavlja i ***Odluka Vijeća o komuniciranju u situacijama kibernetičkih kriza***, kojom je Vijeće u lipnju 2017. utvrdilo način djelovanja međuresornih tijela Vijeća i Koordinacije, i u koju su ugrađena iskustva nastala pri rješavanju globalnog kibernetičkog napada ucjenjivačkim malicioznim kodom WannaCry.

Drugi primjer dodatnih aktivnosti Vijeća u osiguravanju zahtjeva za usklađenosti upravljanja u kibernetičkim krizama s nacionalnim sustavom upravljanja u krizama, jest ***sudjelovanje Vijeća u aktivnostima Koordinacije za sustav domovinske sigurnosti, kroz izradu dokumenata i analiza mogućnosti djelovanja RH u području kibernetičke sigurnosti, organizacijskih nadležnosti tijela, odnosno registra sigurnosnih rizika od kibernetičkih napada.***

Slijedom ovih procesa, svih 13 mjera iz Akcijskog plana za provođenje spomenutih pet ciljeva Nacionalne strategije kibernetičke sigurnosti u predmetnom području D prilagodit će se tijekom 2018. godine novom Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i opisanim dodatnim aktivnostima Vijeća, s ciljem dovršenja ovih mjera iz ovog dijela Akcijskog plana u 2019. godini. Pri tome će se rješenja tražiti kroz procese identifikacije operatora ključnih usluga, davatelje digitalnih usluga, primjenu odgovarajućih zahtjeva kibernetičke sigurnosti, odnosno obavješćivanje o incidentima sa znatnim učinkom na pružanje ključnih usluga i njihovo rješavanje, kao i Zakonom uspostavljena nadležna tijela i njihove odgovornosti, međusobnu koordinaciju i trajno praćenje stanja kibernetičke sigurnosti u nizu Zakonom propisanih sektora.

[16] Operators of Essential Services – OES (treba ih nacionalno definirati/identificirati svaka DČ prema kriterijima iz NIS direktive i pomoćnih akata koji će se uskladiti te u okviru 7 traženih EU sektora: energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura)

[17] Digital Service Providers – DSP (Online marketplace - Internetsko trgovanje, Online search engine - Internetske tražilice, Cloud computing services - računalstvo u oblaku)

Kibernetički kriminalitet (E)

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,**
- **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 2017. godini provodile u potpunosti ili većoj mjeri, no, ne na sustavan način kako je to predviđeno Akcijskim planom***, osobito ako se učinkovitost poduzetih aktivnosti promatra u svjetlu pokazatelja provedbe utvrđenih za svaku pojedinu mjeru, koja u pravilu nisu ostvarena ili aktivnosti koje su poduzete u okviru mjere nisu na odgovarajući način praćene, evidentirane i obrađivani njihovi rezultati.

Kazneno zakonodavstvo u 2017. godini nije mijenjano u dijelu koji bi se odnosio na kibernetički kriminalitet. 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, kojih tijekom 2017. nije bilo. U pitanju su u biti redovne aktivnosti tijela, koje se svakako podržava i nadalje provoditi u forumu kakav on trenutno i egzistira, kako po pitanju nacionalnih predstavnika, tako i međunarodnih tijela u čijem radu oni sudjeluju. Međutim, Akcijski plan je u svojoj mjeri, 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 u razmjeni učinkovite razmjene informacija na međunarodnoj razini je uspostavljena, po svim relevantnim linijama rada. Komunikacije na nacionalnoj razini u 2017. godini primarno su ostvarivane kroz sudjelovanje u radu Operativno-tehničke koordinacije za kibernetičku sigurnost.

Kontinuirana briga o ***jačanju ljudskih potencijala te razvoju i nadogradnji forenzičkih alata i sustava*** postoji, no, nužno je u narednom razdoblju i dalje voditi računa o potrebama osiguranju potrebne financijske potpore za daljnje jačanje i razvoj.

Također, uspostavljena je ***suradnja s gospodarskim sektorom***, no, u mjeri koja još uvijek nije zadovoljavajuća. U narednom razdoblju nužno je povećati broj predstavnika iz različitih gospodarskih sektora, s kojima će se uspostaviti partnerski odnos u razmjeni podataka o zabilježenim incidentima, uz praćenje rezultata uspostavljene suradnje.

III. ANALIZA PROVEDBE MJERA PO POVEZNICAMA PODRUČJIMA KIBERNETIČKE SIGURNOSTI

Zaštita podataka (F)

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.

Provedba aktivnosti u okviru ove poveznice kibernetičke sigurnosti ***u uskoj je vezi sa zakonodavnim postupcima koji su provođeni tijekom 2017. godine*** radi:

- prijenosa Direktive (EU) 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja u nacionalno zakonodavstvo,

- osiguranja provedbe 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).

Direktiva (EU) 2016/943 prenesena je u nacionalno zakonodavstvo ***Zakonom o zaštiti neobjavljenih informacija s tržišnom vrijednosti***, koji je Hrvatski sabor donio na sjednici 23. ožujka 2018. („Narodne novine“, broj: 30/18).

Zakon o provedbi Opće uredbe o zaštiti podataka donesen je na sjednici Hrvatskog sabora održanoj 27. travnja 2018. godine („Narodne novine“, broj: 42/18).

Donošenjem navedenih Zakona osigurane su zakonodavne pretpostavke za nastavak provedbe mjera u vidu uspostave redovite suradnje i provedbe potrebnih koordinacijskih aktivnosti nadležnih tijela potrebnih za potpuno ostvarenje ciljeva definiranih Strategijom u svrhu postizanja veće razine sigurnosti zaštićenih kategorija podataka te stvaranja potrebnih preduvjeta za njihovu nesmetanu razmjenu i ustupanje.

U odnosu na potrebu unaprjeđenja nacionalne regulative u području poslovne tajne ukazuje se kako je Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti usmjeren na građansko pravnu zaštitu poslovnih tajni, dok preciznije i sveobuhvatnije propisivanje sigurnosnih zahtjeva u području zaštite podataka koji predstavljaju poslovnu tajnu i nadalje nije na odgovarajući način riješeno[18].

Stoga se ***ocjenjuje potrebnim u narednom razdoblju poduzeti daljnje aktivnosti usmjerene na izradu analize i prijedloga poboljšanih kriterija za zaštitu tajnosti poslovne tajne***, u cilju preciznije normativne razrade mjera i standarda zaštite takvih podataka (prava pristupa, označavanje, fizička sigurnost itd.).

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 sa terminskim planom provedbe i rezultatima naprijed spomenutih zakonodavnih procesa.

Tijekom 2017. godine izrađena je analiza dosadašnjih iskustava u ***korištenju palete normi HRN ISO/IEC 27000*** u postupku sigurnosnih akreditacija informacijskih sustava u nadležnosti Zavoda za sigurnost informacijskih sustava. U narednom razdoblju potrebno je nastaviti s provedbom ove aktivnosti, uz njezino uvezivanje sa novim nacionalnim zakonodavnim okvirom u području kibernetičke sigurnosti te zaštite osobnih podataka.

Tehnička koordinacija u obradi računalnih sigurnosnih incidenata (G)

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,**

[18] Djelomično regulirano i to Zakonom o zaštiti tajnosti podataka koji datira još iz 1996. godine („Narodne novine“, broj: 108/96, glava VIII.).

- **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.

Provedba mjere, u okviru kojih aktivnosti 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, nije započela, odnosno može započeti tek po provedenoj mjeri Akcijskog plana u okviru čije je realizacije ***potrebno definirati taksonomije***, uključujući pojam značajnog incidenta, protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostaviti platformu za razmjenu podataka sektorski nadležnih tijela uz korištenje definirane taksonomije i protokola. Mjeru definiranja taksonomija i protokola, na kojoj radi radna skupina, potrebno je u narednom razdoblju dovršiti, kako bi se moglo započeti s provedbom ostalih mjera, čiji početak provedbe ovisi o završetku njezine provedbe.

Aktivnosti izvješćivanja dionika unutar sektora o računalnim sigurnosnim incidentima i periodično izvješćivanje Vijeća o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja, koje se trebaju provoditi kontinuirano, započet će po ispunjenju preduvjeta – donošenju taksonomija, definicija i protokola.

Aktivnosti u provedbi mjere usmjerene na ***izdavanje upozorenja o uočenim sigurnosnim ugrozama i trendovima*** te odgovarajućih preporuka za postupanje, provodi se u manjoj mjeri, prvenstveno zbog nedostatne (kvalitetne) međusektorske razmjene informacija o incidentima i ugrozama, kao i nedovoljne razine svijesti da se incidenti prijavljuju nadležnim tijelima, koja sigurnosne preporuke i upozorenja objavljuju preko svojih portala i društvenih mreža. U proteklom razdoblju se u ovom segmentu intenzivirala suradnja u okviru Operativno-tehničke koordinacije za kibernetičku sigurnost. Dodatni poticaj za provedbu ove mjere će se ostvariti primjenom Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga.

Uspostava i održavanje periodičkih (ili po potrebi češćih) koordinacija vezano uz ***razmjenu iskustva i znanja te informacija o sigurnosti kibernetičkog prostora RH*** do kojeg su došla tijela kaznenog progona i sigurnosno obavještajnog sustava, mjera je Akcijskog plana provedena u većoj mjeri. Provođenje ove mjere je rezultiralo i otkrivanjem počinitelja većih broja kaznenih dijela u ovom području. U narednom je razdoblju potrebno dalje unaprjeđivati suradnju i koordinaciju kroz Operativno-tehnički koordinaciju za kibernetičku sigurnost.

Međunarodna suradnja (H)

Strategijom su kao prioriteti 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 te**
- **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.**

Radi ostvarenje ovih ciljeva, Akcijskim planom predviđeno je 6 mjera, za koje je određena kontinuirana provedba.

Mjere 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*** te ***jačom bilateralnom i multilateralnom suradnjom u okviru sporazuma s međunarodnim asocijacijama***, u 2017. godini provođene su u manjoj mjeri. Posljedica je to prije svega ograničenih financijskih i kadrovskih kapaciteta. 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 ***izgradnju povjerenja s ciljem smanjenja rizika od sukoba*** uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija, kao i sudjelovanje i organizacija ***međunarodnih civilnih i vojnih vježbi i drugih stručnih programa***, provodile su se u znatnoj mjeri. U narednom razdoblju potrebno je poticati daljnji angažman relevantnih institucija RH u tim aktivnostima.

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. Do tada neće biti moguće provoditi značajnije aktivnosti predviđene Akcijskim planom u okviru uvodno opisane mjere.

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

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.

Provedba mjera, u okviru kojih je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije potrebno ***uvrstiti sadržaje vezane uz kibernetičku sigurnost u programe ranog i predškolskog odgoja, osnovnoškolske i srednjoškolske programe obrazovanja djelomično je započeta*** u pojedinim segmentima.

U provedbi cjelovite kurikularne reforme, u cilju unaprjeđivanja digitalnih kompetencija, započete su aktivnosti na:

- uvođenju Informatike kao obveznog predmeta u V. i VI. razredu osnovne škole od školske godine 2018./2019. U tu svrhu nabavljena je informatička oprema za 210 osnovnih škola u iznosu od 10.500.000,00 kn.
- moderniziranju kurikuluma Informatike u srednjoškolskom odgoju i obrazovanju.

Dodatno, Ministarstvo znanosti i obrazovanja posebnu pažnju posvetilo je provedbi preventivnih aktivnosti vezanih za sigurnost djece i mladeži na Internetu, mrežnim tehnologijama i mobilnim telefonima u suradnji s Agencijom za odgoj i obrazovanje, Hrvatskom akademskom i istraživačkom mrežom (CARNET), Ravnateljstvom policije i civilnim inicijativama.

U narednom razdoblju ***planira se dalje unaprjeđivati i osuvremenjivati predmetne kurikulume***, prvenstveno Informatike, i međupredmetnog pristupa vezanih za problematiku kibernetičke sigurnosti.

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. Ipak, ***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 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 posebice onih kojima IKT nije primarna djelatnost.

Aktivnosti u provedbi mjere kojima bi se trebalo osigurati ***sustavno obrazovanje učitelja, nastavnika, ravnatelja i stručnih suradnika, kao i djelatnika visokih učilišta***, osobito onih koji rade na predmetima s uključenim sadržajima kibernetičke sigurnosti te poticati uspostavljanje i izvođenje diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti, ***provode se u manjoj mjeri***. U narednom je razdoblju ***potrebno intenzivirati aktivnosti u ovim mjerama***, posebno usmjerene na poticanje obrazovnog kadra na sudjelovanje na stručnim skupovima i specijalističkim tečajevima s temama kibernetičke sigurnosti. Tijekom 2017. godine MOOC tečaju *Digitalne kompetencije za nastavnike* pridružilo se dodatno 19 nastavnika, a samo tri su uspješno završila tečaj – većina nije odradila sve module tako ni modul Sigurnost. Agencija za odgoj i obrazovanje je tijekom 2017. provodila stručno usavršavanje učitelja, nastavnika i stručnih suradnika kroz predavanja te s kontinuiranim stručnim usavršavanjem nastavila kroz cijelu 2017./2018. školsku godinu.

Na ***javnim visokim učilištima u RH*** trenutno se izvode 2 studijska programa usko vezana uz kibernetičku sigurnost. Kako na trenutno uspostavljenim studijima nisu popunjene upisne kvote, ***povećanje broja studijskih programa izostalo je u 2017. godini***, dok se u skorije vrijeme može očekivati uspostavljanje samo još jednog studijskog programa vezanog uz kibernetičku sigurnost.

No, s druge strane, na javnim visokim učilištima izvodi se ukupno 48 kolegija iz područja informacijske sigurnosti te se ***u idućim godinama planiraju novi studijski programi koji u sebi uključuju veći broj kolegija vezano uz informacijsku sigurnost***.

U školskoj godini 2017./2018. Ministarstvo znanosti i obrazovanja financiralo je ***projekte povezane s područjem informacijske i komunikacijske tehnologije u okviru Natječaja za dodjelu bespovratnih sredstava projektima udruga*** u području izvaninstitucionalnoga odgoja i obrazovanja djece i mladih u školskoj godini 2017./2018. Također planira provesti Natječaj za dodjelu bespovratnih sredstava projektima udruga koje djeluju u području izvaninstitucionalnog odgoja i obrazovanja i Poziva na dostavu projektnih prijedloga UP.03.2.2.03 „Unaprjeđenje pismenosti - temelj cjeloživotnog učenja". Navedene aktivnosti provode se u cilju ***poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja.*** U školskoj godini 2017./2018. provedeno je natjecanje učenika osnovnih i srednjih škola u kojem se kroz natjecanje iz Osnova informatike povećao broj pitanja iz područja informacijske sigurnosti.

Stalno ***stručno usavršavanje*** policijskih službenika u području informacijske sigurnosti provodi se kontinuirano. Osiguranje potrebnih ekspertiza i specijalističkih znanja potrebnih za CERT funkcionalnosti (Nacionalni CERT, ZSIS, MORH CERT) provodi se kontinuirano u vrlo zahtjevnim okvirima u kojim su inženjeri kibernetičke sigurnosti u deficitu na cijelom tržištu rada, a posebno kada je riječ o zapošljavanju u državni sektor koji nije ujednačen sa realnim sektorom u pogledu plaća. Iz navedenog razloga neujednačenost plaća s realnim sektorom i izrazitim potrebama za sigurnosnim stručnjacima, često se nakon osigurane potrebne ekspertize i specijalističkih znanja stručnjaci odlučuju za prelazak u realni sektor.

Pravosudna akademija je započela u 2017. godini s planiranjem radionica za pravosudne dužnosnike na temu informacijske sigurnosti i kibernetičkog kriminaliteta u suradnji s Uredom Vijeća za nacionalnu sigurnost, Zavodom za sigurnost informacijskih sustava, Nacionalnim CERT-om, Službom kibernetičke sigurnosti pri Ravnateljstvu policije te predstavnicima sudaca i državnih odvjetnika. S održavanjem radionica planira se započeti u zadnjem kvartalu 2018. godine.

Odgovarajući sustav izobrazbe i provjere znanja iz područja informacijske sigurnosti za državne službenike i namještenike i nadalje nije uspostavljen. Stoga je u narednom razdoblju potrebno intenzivirati aktivnosti u ovim pitanjima, koristeći pri tome raspoložive resurse, a podredno i uz osiguranje dodatnih financijskih sredstava namijenjenih za ovu svrhu.

Iako je ***mjera sigurnosnog osvješćivanja i edukacijskih kampanja*** najšire javnosti provedena u određenoj mjeri, još uvijek nije uspostavljena potrebna 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 uspostaviti horizontalnu koordinaciju ovih aktivnosti i tema koje se obuhvaćaju na nacionalnoj razini.

Informiranje i produbljivanje svijesti djece i mladih uključenih u sve razine formalnog obrazovanja, o potrebi brige o sigurnosti podataka te odgovornom korištenju informacijskih i komunikacijskih tehnologija provodi 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), Fakulteta organizacije i informatike Sveučilišta u Zagrebu (uključen u organiziranje konferencije o informacijskoj sigurnosti, organizira ljetne škole iz područja informacijske i kibernetičke sigurnosti te sudjeluje u kibernetičkim vježbama), te Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu (surađuje s CERT-ovima, organizira edukacije kroz Centar informacijske sigurnosti (cis.hr) te sudjeluje u kibernetičkim vježbama).

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 znatnoj mjeri. Tijekom provedbe aktivnosti uočene su poteškoće financijske naravi, stoga će se u narednom razdoblju intenzivirati aktivnosti da se preporuke objavljuju elektroničkim putem, a sredstva za tiskane materijale osigurana su u okviru raspoloživih EU fondova.

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, provedena je u potpunosti. Redovito se ažuriraju smjernice i preporuke za postupanje kako bi se minimizirao rizik pojave neautoriziranih platnih transakcija u cilju osiguranja primjerenog, pravovremenog i koordiniranog odgovora na moguće kibernetičke prijetnje. Hrvatska narodna banka nastavlja usko surađivati s kreditnim institucijama u cilju razmjene korisnih informacija o informacijskim sustavima i upravljanju istima te unaprjeđenja suradnje kreditnih institucija i Hrvatske narodne banke.

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 u znatnoj mjeri, ali većinom sektorski. Mjera se provodi kontinuirano, a u narednom je razdoblju potrebno suradnju i koordinaciju podići na višu razinu nacionalne usklađenosti, kako bi mjera bila provedena u potpunosti.

Osmišljavanje i provođenje usklađenih kampanja o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u RH o značaju kibernetičke sigurnosti, kao i za državna tijela i pravne osobe s javnim ovlastima, nositelji su provodili u okviru redovnog djelokruga, različitim intenzitetom.

U 2017. godini ***provođene su 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. Jednako su ***provođene i aktivnosti usmjerene na poticanje i podupiranje znanstvenih istraživanja u području informacijske i komunikacijske tehnologije*** s posebnim naglaskom na informacijsku sigurnost i područja poput kriptologije, identifikacije, metoda napada te metode zaštite informacijskih sustava. 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.

IV. ZAKLJUČAK

Sve institucije u svojstvu nositelja pojedinih mjera Akcijskog plana provele su svoju obavezu te dostavile Vijeću podatke potrebne za izradu ovog Izvješća.

U 2017. godini, nakon osnivanja Vijeća kao međuresornog tijela i početka njegovog rada u ožujku 2017. godine, pokrenut je niz procesa opisanih u godišnjem izvješću Vijeća[19], a koji su iznimno važni za provedbu Akcijskog plana. Između ostalog, u cilju poticanja provedbe smjernica Vijeća iz Izvješća o provedbi Akcijskog plana u 2016. godini, prikupljeni su podaci i izrađena je zbirna elektronička knjižica za sve dionike provedbe Akcijskog plana, u kojoj su naznačene osnovne nadležnosti svih dionika Strategije, njihove uloge u radu međuresornih tijela i provedbi mjera iz Akcijskog plana te kontakt podaci osoba zaduženih u institucijama za koordiniranje provedbe pojedine mjere.

Nastavak provedbe Akcijskog plana tijekom 2017. godine rezultirao je daljnjim povećanjem svijesti i razumijevanja problematike kibernetičke sigurnosti i to u vrlo 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. Određivanje koordinatora provedbe mjera Akcijskog plana u institucijama u velikom broju slučajeva utvrđeno je praćenjem najbliže nadležnosti u portfelju nadležnosti pojedine institucije.

U području kritične komunikacijske i informacijske infrastrukture i upravljanju krizama napravljen je veliki napredak koncipiranjem i prijedlogom novog Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, čije se usvajanje, u paketu s Uredbom, očekuje polovinom 2018. godine. Ovo je dodatno veliki korak u usklađivanju obaveza koje za RH proizlaze iz zahtjeva provedbe EU NIS direktive, a koji se ovim Zakonom u potpunosti preuzimaju.

Ključni problem na kojem i dalje treba raditi jeste potreba puno veće konzistentnosti obrazovnih programa u području kibernetičke sigurnosti te bolje osposobljenosti predavača na različitim razinama i vrstama obrazovanja. Aktualno stanje pokazuje početne pomake u dobrom smjeru, ali i dalje ukazuje na nizak stupanj konzistentnosti programa i nedovoljnu osposobljenost predavača, a samim time i na upitne rezultate edukacijskih programa kibernetičke sigurnosti koji se provode u RH. Razrada kibernetičke sigurnosti u okviru Strategije i Akcijskog plana morale bi biti okvir za izradu svih nacionalnih edukacijskih programa u ovom području, a međuresorno tijelo, Nacionalno vijeće za kibernetičku sigurnost, nastavit će inicijative prema nadležnim tijelima i dionicima provedbe Akcijskog plana s ciljem unaprjeđenja svih vrsta i razina obrazovanja u RH.

[19] http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf