# IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI U 2016. GODINI

# *Osvrt na recentno razdoblje izvješćivanja*

*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 doba izrade hrvatske strategije kibernetičke sigurnosti odvijalo se niz kampanja s masovnim slanjem maliciozne e-pošte (phishing), koje su tekstualno prilagođenim sadržajem masovno dostavljana hrvatskim korisnicima e-pošte. U to vrijeme Hrvatsku je pogodio i veliki ciljani kibernetički napad na pravne osobe, korisnike 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, napose ministarstva vanjskih poslova koji su koncentratori političkih informacija i poželjna meta za ovakve napade aktera sponzoriranih politikama nekih država. Napad ove vrste rješavan je prošle godine i u hrvatskom MVEP-u. Počevši s posljednjim izborima za predsjednika SAD-a, kao i nekim kasnijim političkim izbornim procesima u državama EU-a, postalo je razvidno kako je kibernetičke napade moguće koristiti i za utjecaj na društvene procese. Hrvatska 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, koji se u opisanom razdoblju dogodio na energetske objekte, državne institucije i tvrtke, još jednom je pokazao visoku ovisnost država o informacijskoj tehnologiji te razornu moć ovakvih hibridnih napada, koji napadom na informacijske resurse onemogućavaju rad određene vitalne infrastrukture društva. Zamjetan je stalni porast broja kaznenih dijela u EU, a i u Republici Hrvatskoj, 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. 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 Velike Britanije. Upravo u ovom globalnom napadu hrvatska međuresorna tijela, Nacionalno Vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost, uspješno su reagirala i, na temelju planiranja u prethodnom razdoblju, 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 strategije iz 2013. godine, donosi Direktivu o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS Direktiva). Hrvatska Vlada u ovom razdoblju donosi Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu, Odluku o osnivanju međuresornih tijela za upravljanje provedbom Strategije, te početkom 2017. godine osigurava i puno pokretanje rada međuresornih upravljačkih tijela.*

*Upravo je provedba mjera Akcijskog plana od iznimne važnosti za osiguravanje otpornosti društva na sigurnosne probleme u kibernetičkom prostoru, ali i za stvaranje pretpostavki za uspješan razvoj hrvatskog društva i konkurentnost Hrvatske na jedinstvenom digitalnom tržištu Europske Unije.*

# SADRŽAJ

# I. UVOD

Vlada Republike Hrvatske donijela je, na sjednici održanoj 7. listopada 2015. godine, Nacionalnu strategiju kibernetičke sigurnosti (dalje u tekstu: Strategija). U pitanju je prvi strateški dokument u području kibernetičke sigurnosti u Republici Hrvatskoj, usmjeren na stvaranje organizacijskih preduvjeta potrebnih za uvođenje trajne i sustavne brige za virtualnu dimenziju našeg društva.

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 sigurnosti[1] (dalje u tekstu: Akcijski plan), na način da su njime utvrđene provedbene mjere nužne za ostvarenje tih općih ciljeva. Strategija i Akcijski plan su na taj način međusobno povezani pomoću odabranih općih ciljeva Strategije, za koje su definirani posebni ciljevi svakog od područja i poveznica područja, a za svaki od ovih posebnih ciljeva definirane su odgovarajuće mjere za njegovo postizanje u okviru provedbe Akcijskog plana. Time je dobiven koherentan i sveobuhvatan sustav međusobno povezanih ciljeva i mjera. 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

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

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

Svaka od ovih 77 mjera u Akcijskom planu ima određene nositelje i sunositelje te definiranu osnovnu metriku rokova i pokazatelja provedbe. Uvođenjem sustava obveznog izvješćivanja o provedbi mjera Akcijskog plana, Strategija je dala alat za sustavan 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.

S ciljem osiguravanja upravljanja složenim procesom kibernetičke sigurnosti i provedbom mjera Akcijskog plana, koje obuhvaćaju kibernetički prostor tretiran sveobuhvatno kao virtualna dimenzija suvremenog društva, Strategijom je predviđena uspostava sustava kontinuiranog praćenja ostvarivanja ciljeva Strategije i provedbe mjera Akcijskog plana, a koji ujedno predstavlja i upravljački mehanizam horizontalnog koordiniranja čitavog niza nadležnih institucija u kreiranju odgovarajućih nacionalnih i sektorskih politika i odgovora na prijetnje u nacionalnom kibernetičkom prostoru. Stoga je Vlada Republike Hrvatske u tu svrhu, na sjednici održanoj 8. lipnja 2016. godine, donijela Odluku o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (*„Narodne novine“, broj: 61/2016*).

Kako bi se omogućilo pokretanje rada nacionalnih međuresornih tijela za kibernetičku sigurnost, Vlada Republike Hrvatske je na sjednici održanoj 16. veljače 2017. godine, donijela Rješenje o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, čime je otvoren put za punu provedbu mjera Akcijskog plana i ciljeva Strategije te upravljanje horizontalnim inicijativama, kako u državnom sektoru, tako i međusektorski, u društvu u cjelini.

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 svibnja 2017. godine.

# II. PROVEDBA STRATEGIJE I AKCIJSKOG PLANA

### a. Vertikalna koordinacija na nacionalnoj razini

Strategijom je određeno da će, radi razmatranja i unaprjeđenja provođenja Strategije i Akcijskog plana za njezinu provedbu, Vlada Republike Hrvatske osnovati Nacionalno vijeće za kibernetičku sigurnost, koje će:

- sustavno pratiti i koordinirati provedbu Strategije te raspravljati o svim pitanjima od važnosti za kibernetičku sigurnost;
- predlagati mjere za unaprjeđenje provođenja Strategije i Akcijskog plana za provedbu Strategije;
- predlagati organiziranje nacionalnih vježbi iz područja kibernetičke sigurnosti;
- izrađivati preporuke, mišljenja, izvješća i smjernice u vezi s provedbom Strategije i Akcijskog plana te
- predlagati izmjene i dopune Strategije i Akcijskog plana, odnosno donošenje nove Strategije i akcijskih planova, u skladu s novim potrebama.

Vrlo široka i složena problematika na koju se odnosi Strategija, potreba za usklađivanjem zajedničkog rada niza različitih dionika koji sudjeluju u provedbi Strategije i mjera koje su u tu svrhu definirane Akcijskim planom, odrazile su se i na utvrđivanje sastava Vijeća. Sukladno Odluci o osnivanju, Vijeće je sastavljeno od 16 članova koje čine predstavnici sljedećih institucija:

- Ured Vijeća za nacionalnu sigurnost (predsjednik),
- Ministarstvo unutarnjih poslova (član),
- Ministarstvo vanjskih i europskih poslova (član),
- Ministarstvo uprave (član),
- Ministarstvo gospodarstva, poduzetništva i obrta (član),
- Ministarstvo znanosti i obrazovanja (član),
- Ministarstvo obrane (član),
- Ministarstvo pravosuđa (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Državna uprava za zaštitu i spašavanje (član),

- Hrvatska akademska i istraživačka mreža – CARNet, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član),
- Agencija za zaštitu osobnih podataka (član).

Vijeće je ujedno i nositelj triju mjera Akcijskog plana iz dijela upravljanja u krizama.

Vijeće podnosi Vladi Republike Hrvatske godišnje izvješće o svom radu i radu Operativno-tehničke koordinacije za kibernetičku sigurnost, najkasnije do kraja prvog kvartala tekuće godine, za prethodnu godinu. Vijeće podnosi Vladi i izvješće o provedbi Akcijskog plana za provedbu Strategije, najkasnije do kraja drugog kvartala tekuće godine, za prethodnu godinu.

Strategija je nadalje predvidjela i osnivanje Operativno-tehničke koordinaciju za kibernetičku sigurnost, radi osiguravanja podrške radu Nacionalnog Vijeća za kibernetičku sigurnost. Koordinacija ima zadaću:

- pratiti stanje sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu;
- izrađivati izvješća o stanju kibernetičke sigurnosti;
- predlagati planove postupanja u kibernetičkim krizama;
- obavljati druge poslove prema utvrđenim programima i planovima aktivnosti.

Koordinacija je sastavljena od 8 članova koje čine predstavnici sljedećih institucija:

- Ministarstvo unutarnjih poslova (koordinator),
- Ministarstvo obrane (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Hrvatska akademska i istraživačka mreža – CARNet, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član).

Koordinacija obavlja zadaće prema programima i planovima aktivnosti te smjernicama Nacionalnog vijeća za kibernetičku sigurnost, a o svom radu podnosi Vijeću izvješće, najkasnije do 31. siječnja tekuće godine, za prethodnu godinu. U svim mjerama Akcijskog plana u kojima je Vijeće nositelj provedbe, Koordinacija je sunositelj.

### b. Horizontalna koordinacija s nositeljima provedbe mjera

Vijeće provodi horizontalnu koordinaciju prema nositeljima mjera pri čemu UVNS obavlja administrativni dio poslova. Svaka pojedina mjera ima određenog barem jednog nositelja, a može biti i više nositelja i sunositelja. Većina ključnih obveznika provođenja mjera Akcijskog

plana poimence je nabrojena, 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 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.

### c. Uvjeti za provedbu mjera Akcijskog plana u 2016. godini

Sukladno zaključcima Nacionalnog vijeća za kibernetičku sigurnost sa konstiruirajuće sjednice održane 16. ožujka 2017., nositelji provedbe mjera iz Akcijskog plana – obveznici izvještavanja dostavili su izvješća o provedbi mjera Uredu Vijeća za nacionalnu sigurnost,

kao tijelu koje predsjedava Nacionalnim vijećem za kibernetičku sigurnost i osigurava administrativno-tehničku podršku radu Vijeća.

Odluku[2] o osnivanju Nacionalnog vijeća za kibernetičku sigurnost Vlada RH donijela je na sjednici održanoj 08. lipnja 2016. godine. Vijeće je sa svojim radom počelo u ožujku 2017. godine, kada su se, po donošenju Rješenja Vlade Republike Hrvatske o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost (od 16.2.2017.), stekli uvjeti za održavanje prve, konstituirajuće sjednice Nacionalnog vijeća za kibernetičku sigurnost.

Uloga Nacionalnog vijeća za kibernetičku sigurnost, kao međuresornog tijela, jeste dodatno poticanje suradnje institucija i sektora te koordiniranja provedbe mjera iz Akcijskog plana, ali i provođenje medijacije u slučajevima gdje su potrebna tumačenja, usklađivanje različitog shvaćanja i stavova pojedinih dionika ili dodatna pojašnjenja u provedbi i nadležnostima, Zakašnjeli početak rada Vijeća, stoga je rezultirao i sporijim početkom provedbe mjera te općenito otežanom provedbom u mjerama koje se odnose na složeniju problematiku i veći broj institucija nositelja/sunositelja, a time se odrazio i na ukupnu kvalitetu i kvantitetu provedbe mjera iz Akcijskog plana u 2016. godini.

No, uključenost širokog kruga dionika u sam proces donošenja Strategije i Akcijskog plana, uključujući sve institucije koje su izravno (nositelji) ili neizravno (sunositelji i sudionici) uključene i u njihovu provedbu, kao i samim time postignuto dobro razumijevanje problematike i prepoznavanja aktivnosti iz svoje nadležnosti koje pripadaju pojedinim tematski koncipiranim mjerama Akcijskog plana, doprinijelo je tome da je početak provedbe Akcijskog plana u 2016. godini ipak dao rezultate u velikom broju od 30-tak zaduženih institucija raznorodnih profila.

[2] „Narodne novine“, broj: 61/16.

# III. ANALIZA PROVEDBE MJERA

Analiza je provedena temeljem izvješća nositelja pojedinih mjera putem Obrasca izvješća o provedbi mjere Akcijskog plana, kojeg je Vijeće donijelo na konstituirajućoj sjednici održanoj 16. ožujka 2017. godine. Sve mjere Akcijskog plana imaju definirane pokazatelje provedbe, a obrazac za izvještavanje omogućuje 4 stupnja očitovanja o statusu provedbe (potpuno provedeno/provodi se, provedeno/provodi se u većoj mjeri, provedeno/provodi se u manjoj mjeri, provedba nije započela).

## a. Područja 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 sektora javnih elektroničkih komunikacija, u svrhu daljnjeg unaprjeđenja bitnih pretpostavki za postizanje veće razine kibernetičke sigurnosti u ovom području, Strategija određuje 3 cilja:

- provođenje nadzora tehničkih i organizacijskih 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 (CIX) za međusobnu razmjenu internetskog prometa pružatelja javnih komunikacijskih mreža i/ili usluga za davanje usluga korisnicima u RH.

Akcijskim planom utvrđene su tri mjere za provedbu opisanih ciljeva, dvije s rokom provedbe od 12 mjeseci (od donošenja Strategije) te jedna mjera kontinuiranog trajanja.

Aktivnosti koje su u 2016. g. poduzete u svrhu definiranja načina provedbe nadzora operatora bile su normativnog karaktera te su rezultirale izmjenama podzakonskog akta iz ove domene, kojim su redefinirane minimalne sigurnosne mjere, opisani sigurnosni incidenti i kriteriji za izvješćivanje o tim sigurnosnim incidentima, 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. Uvedene izmjene su u primjeni od 1. siječnja 2017. godine, a praćenje njihove provedbe od strane nadzornog tijela nastupa u drugoj polovini godine, čime će se ostvariti potpuna provedba mjere. Preporuča se daljnje praćenje provedbe mjere te donošenje konačne ocjene uspješnosti u sklopu postupka izvještavanja za sljedeće izvještajno razdoblje (2017. godinu).

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.

Tehnička koordinacija regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti postoji, no, u pravilu su u pitanju međusektorski odnosi koji su uspostavljeni u okviru obavljanja redovnih aktivnosti uključenih tijela. Neposredna, ciljana i kontinuirana razmjena podataka predstavlja ključni cilj za usklađenu provedbu mjera informacijske sigurnosti i politike zaštite podataka. Budući da provedba mjere u 2016. g. nije polučila rezultatom opisanom u Akcijskom planu kao pokazatelj njezine provedbe, nužno je u narednom razdoblju potaknuti horizontalne inicijative i sinergijsko djelovanje uključenih tijela, dionika Strategije u ovom procesu.

## 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 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 za potrebu pristupa Internetu, 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 utvrđenim rokovima provedbe.

Već samo izvještavanje o provedbi mjera iz ovog područja u 2016. g. je izostalo, osim u jednom manjem dijelu, gdje se započelo s pripremnim aktivnostima, ali je nužan njihov nastavak. U narednom razdoblju potrebno je podići svijest o važnosti uloge nadležnog tijela u ostvarenju gore opisanih ciljeva te inicirati analizu stanja o provedbi mjera iz ovog područja i prije pripreme za sljedeći godišnji izvještaj o provedbi mjera. Ključni problem koji se uočava je nedovoljna povezanost tehnoloških razvojnih strategija i projekata u području informacijske tehnologije sa sigurnosnim strategijama i zahtjevima, što je nužno promijeniti u narednom razdoblju i usko povezati kako bi se moglo osigurati povjerenje korisnika u ove usluge i njihov učinkovit i uspješan daljnji razvoj.

## C. Elektroničke financijske usluge

Sigurnosni zahtjevi koji se provode u području elektroničkih financijskih usluga imaju dužu tradiciju od ostalih područja i već sada 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 dva 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 četiri mjere u ovom području, s opisanim konkretnim pokazateljima provedbe te rokovima koji su većinom već nastupili. Dostavljena izvješća pokazuju da se mjere provode, ali i da nisu ostvarene u potpunosti.

Smjernice o sigurnosti internetskih plaćanja su izrađene 2015. g. te su prezentirane širem krugu institucija bankarskog sektora, platnog prometa i najznačajnijih institucija za elektronički novac. Provjera usklađenosti relevantnih institucija s odredbama Smjernica bit će provedena u narednom razdoblju, kroz supervizije i nadzorne mjere središnje nacionalne banke. Stoga se preporuča daljnje praćenje provedbe mjere te donošenje konačne ocjene uspješnosti u sklopu postupka izvještavanja za sljedeće izvještajno razdoblje (2017. godinu).

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 Europska agencija 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, a u okviru kojeg bi trebali 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 izostala u drugom dijelu, jer smjernice za izvješćivanje o incidentima nisu još donesene. No, treba napomenuti da je i ta aktivnost usko vezana uz postupke i rokove za implementaciju koje će definirati Europska centralna banka (ECB) i Europska agencija za bankarstvo (EBA). EBA još nije objavila Smjernice za izvješćivanje o incidentima. Očekivani termin objave je kraj 2017. ili početak 2018. godine. Stoga se svakako preporuča daljnje praćenje provedbe mjere, uz obvezu izvještavanja o učinjenom već i za 2017. g.

## D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

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 ima za cilj osigurati pravovremenu i učinkovitu reakciju/odgovor na prijetnju i osigurati oporavak infrastrukture ili usluge od naročitog sigurnosnog interesa za RH.

U cilju zaštite procesa koji su ključni za funkcioniranje države i gospodarstva, kao i uspostave učinkovitog odgovora na moguće krize, Strategijom je definirano pet 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 Strategijom je predviđeno provođenje 13 mjera. Preduvjet za provođenje ovih mjera je identifikacija kritičnih infrastruktura. Vlada je svojom Odlukom[3] definirala kritične nacionalne sektore, ali je izostalo definiranje konkretnih infrastruktura u tim sektorima te samim tim dodatni sigurnosni zahtjevi prema istima. U cilju provedbe mjera iz ovog područja nužno je prethodno dovršiti provedbu aktivnosti, po potrebi uz promjenu zakonodavnog okvira u području nacionalnih kritičnih infrastruktura, kako bi se moglo pristupiti provođenju mjera u području kritičnih komunikacijskih i informacijskih sustava.

S obzirom na nedostatno stanje provedbe u segmentu kritičnih nacionalnih sektora te na kratke rokove (9. svibanj 2018.) koji obvezuju RH u provedbi EU NIS Direktive[4], Vijeće je odlučilo uspostaviti radnu skupinu Vijeća za provedbu NIS direktive. Ovaj proces proveden je na temelju visokog stupnja korelacije između EU NIS direktive i 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 te formata za suradnju predviđenih u NIS direktivi, NIS CG za stratešku suradnju i CSIRT Network za operativno-tehničku suradnju. U narednom razdoblju stoga će biti potrebno formalizirati i neke druge nacionalne funkcionalnosti.

[3] 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).
[4] 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

Ključni problem predstavljat će potreba provedbe zahtjeva za operatore ključnih usluga (OES) u okviru sektora kritične infrastrukture prema EU zahtjevu[5], kao i utvrđivanje i usklađivanje kriterija i uvjeta za davatelje digitalnih usluga[6]. Za ove funkcionalnosti predviđeno je utvrđivanje nacionalnih nadležnih tijela, tzv. Competent Authorities, za sedam EU sektora kritične infrastrukture predviđenih NIS direktivom. Pored toga, u svrhu koordinacije provedbe svih elemenata NIS direktive na nacionalnoj razini, trebat će u daljnjem postupku provedbe zahtjeva NIS direktive utvrditi jedinstvenu nacionalnu kontaktnu točku (Single Point of Contact) za pitanja i koordinaciju koja proizlazi iz cjelokupnog opsega NIS direktive.

Sukladno NIS direktivi, nacionalna nadležna tijela i CERT mreža morat će imati odgovarajuće sposobnosti i ovlasti kako bi se osigurala implementacija Direktive (obveza DČ koja proizlazi izravno uz Direktive). Potrebno će biti i uspostaviti registar pravnih osoba (OES), obveznika provedbe sigurnosnih mjera, uključujući i obvezu izvješćivanja u slučajevima značajnih incidenata.

U provedbi navedenih obveza RH koje proizlaze iz NIS direktive, radna skupina Vijeća za NIS direktivu koristit će raspoložive modele i preporuke Europske komisije, koji su razrađeni na temelju iskustava EU država članica koje su provele slične nacionalne procese. Provedbom ovih obveza RH iz NIS direktive očekuje se razvoj potrebnih sposobnosti koji će potaknuti i omogućiti paralelnu ili naknadnu provedbu u preostalim nacionalno predviđenim sektorima kritične infrastrukture.

## E. Kibernetički kriminalitet

U cilju uspostave učinkovitih mjera za kvalitetnije i uspješnije suzbijanje kibernetičkog kriminaliteta Strategijom je utvrđeno pet 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

[5] 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)

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

- razvoj suradnje s gospodarskim sektorom.

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

Dostavljena Izvješća o provedbi mjera pokazuju da su se sve mjere u 2016. godini provodile u većoj ili manjoj mjeri, ali ne i 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 obrađivane u smislu postavljene metrike rezultata mjera.

Kazneno zakonodavstvo u 2016. godini nije mijenjano. 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 2016. godine 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 podataka na međunarodnoj razini je uspostavljena po svim relevantnim linijama rada. No, primjećuje se nedostatak komunikacije na nacionalnoj razini u 2016. godini, koji bi ubuduće trebao biti nadomješten međusobnom užom suradnjom tijela 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 i nadasve o naprednijim organizacijskim i upravljačkim okvirima nadležnih tijela za istraživanje i procesuiranje kaznenih djela kibernetičkog kriminaliteta.

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.

# b. Poveznice područja kibernetičke sigurnosti

## F. Zaštita podataka

Za sigurnost i nesmetanu razmjenu i ustupanje zaštićenih (kategorija) podataka među različitim dionicima kibernetičke sigurnosti, Strategijom je utvrđeno pet 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 ovisna o donošenju EU Direktive.

Mjere koje su trebale rezultirati uspostavom redovite suradnje i razmjene iskustava uz periodičnu izradu analiza i preporuka za rješavanje utvrđenih problema i neujednačenosti u primjeni propisa, u 2016. godini provođene su različitim intenzitetom.

Za aktivnosti usmjerene na unaprjeđenje nacionalne regulative u području poslovne tajne te u tu svrhu osnivanje radne skupine za izradu analize i prijedloga poboljšanih kriterija za utvrđivanje i zaštitu poslovne tajne, utvrđeno je kako je umjesto nositelja mjere utvrđenog Akcijskim planom, Državni zavod za intelektualno vlasništvo, pri EU koordinaciji, utvrđen nositeljem transpozicije EU Direktiva 2016/943 i 2004/48/EZ u nacionalno zakonodavstvo, u okvirima kojih je osnovana radna skupina u te svrhe.

Aktivnosti usmjerene na uspostavu redovitih koordinacijskih aktivnosti nacionalnih tijela nadležnih za pojedine skupine zaštićenih podataka, radi razmjene iskustava, detektiranja problema i/ili potencijalne neujednačenosti u primjeni propisa te izrade analize i preporuka za

njihovo rješavanje, aktivnosti usmjerene na izradu sadržaja dijelova ugovora kojima će se obveznici primjene zakonskih propisa usmjeravati na detalje provedbe svih onih obveza koje su od visoke važnosti za zaštićene kategorije podataka, prilikom korištenja/ugovaranja elektroničkih usluga u kibernetičkom prostoru i računalne infrastrukture, platforme, ili aplikacije u računalnom oblaku te osnivanje radne skupine koja će izraditi kriterije za provedbu sektorskih analiza dosadašnjih iskustava u korištenju palete normi HRN ISO/IEC 27000, koordinirati provedbu sektorskih analiza, evaluirati analize i temeljem rezultata izraditi preporuke za poboljšanja u provedbi, u cilju unifikacije u korištenju ove palete normi, provedene su u manjoj mjeri. U svim ovim aktivnostima, potrebno je u narednom razdoblju inicirati i intenzivirati koordinacijske aktivnosti svih nositelja mjera.

Mjere, čije su aktivnosti usmjerene na analizu postojećeg stanja, uključujući pravni okvir koji se odnosi na ustrojavanje, obveze i odgovornosti nadležnih tijela, zaštitu i sva druga pitanja bitna za nacionalne registre podataka, temeljem čijih rezultata je potrebno izraditi kriterije po kojima se definiraju nacionalni elektronički registri koji predstavljaju kritične informacijske resurse i nositelje odgovornosti za njihovu zaštitu te aktivnosti koje su usmjerene na utvrđivanje dodatnih mjera zaštite za nacionalne elektroničke registre koji predstavljaju kritične informacijske resurse i obveze nositelja odgovornosti za njihovu provedbu, nisu provođene zbog kašnjenja i drugih poteškoća u provedbi nadležnih zakona.

## 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.

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 uspostavu platforme za razmjenu podataka sektorski nadležnih tijela koja bi koristila definiranu taksonomiju i protokole. Mjeru definiranja taksonomija i protokola, koja se provodi u većoj mjeri, potrebno je u narednom razdoblju intenzivirati s ciljem finalizacije taksonomija, definicija i protokola te izrade platforme radi razmjene podataka i nacionalne statistike, 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 Nacionalnog vijeća za kibernetičku sigurnost o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja, koje se trebaju provoditi kontinuirano, započet će po ispunjenju preduvjeta – donošenju taksonomija, definicija i protokola. U manjoj mjeri ovi poslovi se planiraju organizirati kroz mjesečno izvještavanje Koordinacije Vijeću, o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru.

Aktivnosti u provedbi mjere usmjerene na izdavanje upozorenja o uočenim sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje, provode se uglavnom na sektorskoj razini, prvenstveno zbog nedostatne međusektorske razmjene informacija o incidentima i ugrozama te još uvijek nedovoljne razine svijesti o potrebi prijavljivanja sigurnosnih incidenata nadležnim tijelima. Sektorski nadležna tijela sigurnosne preporuke i upozorenja objavljuju redovno preko svojih portala i društvenih mreža. U narednom je razdoblju u ovom segmentu potrebno intenzivirati suradnju u okviru Operativno-tehničke koordinacije za kibernetičku sigurnost.

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 koja je provedena u većoj mjeri. Dosadašnji rezultati provođenja mjere ukazuju na smanjenje vremena potrebnog za otkrivanje određenih računalno-sigurnosnih incidenata te vremena reakcije, odnosno odziva na incident i otklanjanje ugroze. U narednom je razdoblju potrebno dalje unaprjeđivati suradnju i koordinaciju sektorskih nositelja kroz Operativno-tehničku koordinaciju za kibernetičku sigurnost.

## H. Međunarodna suradnja

Strategijom je kao prioritet RH u području kibernetičke sigurnosti na međunarodnom planu utvrđeno šest 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;
- jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.

Radi ostvarenje ovih ciljeva, Akcijskim planom predviđeno je šest 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 2016. godini provođene su u manjoj mjeri. U narednom razdoblju potrebno je definirati tematska događanja koja je bitno pratiti na međunarodnoj razini, odrediti nadležne predstavnike (institucije) koji će biti zaduženi za praćenje pojedine problematike te uvesti koordinirani način međusobne razmjene relevantnih informacija prije i poslije sastanaka i drugih aktivnosti.

Aktivnosti usmjerene na izgradnju povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija i kibernetičkog prostora, 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 nacionalne 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.

# 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 kroz tri 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 u programe ranog i predškolskog odgoja potrebno uvrstiti sadržaje vezane uz kibernetičku sigurnost, u osnovnoškolske i srednjoškolske programe obrazovanja uvrstiti predmetne i međupredmetne sadržaje vezane uz kibernetičku sigurnost, nije započela, jer nisu stvoreni preduvjeti kroz kurikularne dokumente, odnosno planirano je provođenje mjera tijekom završetka kurikularnih dokumenata. Kako bi se što prije započela provedba ovih mjera, potrebno je u narednom razdoblju intenzivirati aktivnosti na kurikularnoj reformi.

Za razliku od navedenog, mjere u okviru kojih je u programe na visokoškolskoj razini potrebno ugraditi sadržaje vezane uz kibernetičku sigurnost, provode se na javnim visokim učilištima u velikoj mjeri. 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 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, kako bi se nastavno i stručno osoblje i djelatnici visokih škola sustavno obrazovali u području kibernetičke sigurnosti, a broj studija vezanih uz kibernetičku sigurnost sa sadašnja dva (jedan poslijediplomski stručni i jedan poslijediplomski specijalistički), povećao u skladu s trendovima i potrebama.

Mjera, u okviru koje se provode aktivnosti poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja, provodi se u potpunosti i kontinuirano, kao i stalno stručno usavršavanje policijskih službenika u području informacijske sigurnosti i kibernetičkog kriminaliteta koje provodi specijalizirana obrazovna akademija i druge ustrojstvene jedinice MUP-a sukladno svojim nadležnostima, a usklađivanje programa provodi se u suradnji sa stručno nadležnim tijelima. U tim se pitanjima u znatnoj mjeri provodi stalno stručno usavršavanje državnih odvjetnika i sudaca, međutim zbog nedostatnih financijskih sredstava određene edukacije o kibernetičkom kriminalitetu se ne provode. U narednom je razdoblju potrebno intenzivirati aktivnosti u ovim pitanjima te prijaviti projekte edukacije prema nadležnim tijelima EU-a, radi korištenja dostupnih fondova.

Ključni problem na kojem je potrebno raditi jest potreba puno veće konzistentnosti programa kibernetičke sigurnosti te bolje osposobljenosti predavača na različitim razinama i vrstama obrazovanja. Aktualno stanje još uvijek 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, potrebno je u odgovarajućoj mjeri uključiti u savjetodavni proces nadležnog ministarstva i drugih tijela povezanih s kurikularnom reformom i unaprjeđenjem svih vrsta i razina obrazovanja u RH.

Iako je mjera sigurnosnog osvješćivanja i edukacijskih kampanja najšire javnosti provedena u većoj 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.

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.

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 eventualno osiguraju u okviru raspoloživih EU fondova.

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,, uglavnom niskim, a ne koordinirano u okviru mjere. Vrlo česta poteškoća u provedbi je nedostatak financijskih sredstava za održavanje raznih projekata u ovim pitanjima, poput radionica, za što se u narednom razdoblju planira uključiti i druge relevantne čimbenike i dionike kibernetičke sigurnosti. Analizira se mogućnost uključenja nadležnih tijela u programe koji se financiraju iz programa EU.

Za potrebe CERT funkcionalnosti, tijela koja posjeduju CERT sposobnosti, u manjoj su mjeri definirala, na godišnjoj razini, potrebna područja ekspertize te potrebne izobrazbe i načine stjecanja tih znanja za svoje zaposlenike, kao i u manjoj mjeri realizirali definiranu specijalističku izobrazbu ili samoučenje za određeni broj djelatnika za potrebe CERT funkcionalnosti, sukladno godišnjoj listi potrebnih ekspertiza i izobrazbi. Potrebe se definiraju

individualno, prema potrebama pojedinog CERT-a, i nisu ujednačene na razini CERT-ova. U narednom je razdoblju potrebno poticati isti pristup u svim organizacijskim segmentima s CERT funkcionalnostima, kako u definiraju godišnjih lista, tako i u realizaciji definiranih specijalističkih izobrazbi i samoučenja, a u čemu će biti potrebno uskladiti i zahtjeve koje na EU razini za ove poslove utvrđuje NIS direktiva.

Aktivnosti koje su u okviru mjere trebale osigurati 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, provode se u manjoj mjeri. U tim pitanjima, planira se u narednom razdoblju održati nekoliko seminara, odnosno webinara.

U manjoj su mjeri provođene aktivnosti koje su trebale osigurati aktivno poticanje 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, u manjoj mjeri, provođene 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 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.

U manjoj se mjeri provode aktivnosti u poticanju organiziranja natjecanja u području informacijske sigurnosti, primarno zbog nedovoljne informiranosti o važnosti kibernetičke sigurnosti, kao i aktivnosti usmjerene na povećanje broja studijskih programa koji uključuju veći broj kolegija vezano uz informacijsku sigurnost. Potrebno je intenzivirati aktivnosti u ovim područjima kako bi se ukazalo na značaj i ulogu informacijske sigurnosti i sigurnosti kibernetičkog prostora.

Aktivnosti koje su trebale rezultirati uspostavom sustava izobrazbe i provjere znanja iz područja informacijske sigurnosti u državnim i stručnim ispitima te periodično za rukovodno i tehničko osoblje te ostale korisnike informacijskih sustava nisu provođene, kao niti aktivnosti kojima se trebala ostvariti uska suradnja s tijelima za koordinaciju prevencije i odgovar na ugroze informacijskih sustava, radi izrade obrazovnog modula o sigurnom korištenju informacijskih sustava. Razlozi neprovedbe su u kašnjenju ispunjavanja drugih preduvjeta nužnih za početak provedbe ovih mjera.

Provođenje mjera u okviru kojih aktivnosti u području kibernetičke sigurnosti trebaju biti usmjerene na poticanje znanstvenih istraživanja, razvoja novih proizvoda i usluga, razvoja tehnološke infrastrukture, kako za tržište EU, tako i za svjetsko tržište, nije sustavno započelo. Potrebno je pokrenuti niz koordiniranih inicijativa kroz nacionalnu normizaciju i organizaciju koja će osigurati odgovarajuće akreditirane, certificirane i evaluirane domaće proizvođače i proizvode za EU tržište te poticanje vlastite proizvodnje i promicanje primjene domaćih rješenja koja bi mogla doprinijeti određenim gospodarskim prednostima za RH. U ovom segmentu aktivnosti nužno je napraviti iskorak i povezati gospodarski nadležna tijela, komore i udruge, akademske institucije i klastere tvrtki te započeti sustavni i usklađeni pristup podizanja potencijala RH i većeg korištenja instrumenata EU-a u propulzivnom području tehnologije i usluga za primjenu u kibernetičkom prostoru.

# IV. ZAKLJUČAK

Većina institucija u svojstvu nositelja pojedinih mjera Akcijskog plana, od kojih je Nacionalno vijeće za kibernetičku sigurnost zatražilo popunjavanje obrazaca, provelo je svoju obavezu te dostavilo potrebne podatke na analizu Vijeću.

U 2016. g. bio je primjetan nedostatak Vijeća kao međuresornog tijela koje će poticati provedbu mjera Akcijskog plana i provesti potrebnu medijaciju u slučajevima gdje je potrebno dodatno tumačenje ili usklađivanje različitog tumačenja dionika provedbe Strategije, što je rezultiralo sporijim početkom provedbe mjera i otežanom provedbom u mjerama koje se odnose na složeniju problematiku i veći broj institucija nositelja/sunositelja.

Početak provedbe Akcijskog plana u 2016. ipak je dao određene rezultate u velikom broju od 30-tak zaduženih institucija raznorodnih profila. Početak provedbe Akcijskog plana rezultirao je i bitno većim razumijevanjem problematike kibernetičke sigurnosti u vrlo različitim institucijama koje su uključene u provedbu Akcijskog plana. Sve institucije su u ovoj početnoj fazi provedbe Akcijskog plana prepoznale i povezale aktivnosti iz svoje 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 institucije, ali se u tom dijelu mora s nekim dionicima raditi na učinkovitijem određivanju koordinatora provedbe mjera Akcijskog plana. U području kritične informacijske infrastrukture uočen je problem nemogućnosti korištenja nacionalnih rezultata u sektorima kritične infrastrukture, zbog spore provedbe zakona u nacionalno definiranim sektorima te se pristupilo reorganizaciji u svrhu provedbe sličnih obaveza koje za RH proizlaze iz obaveza provedbe EU NIS direktive. U cilju daljnje provedbe nacionalnih mjera iz ovog područja nužno je prethodno dovršiti provedbu aktivnosti, po potrebi uz promjenu zakonodavnog okvira u području nacionalnih kritičnih infrastruktura, kako bi se moglo pristupiti provođenju mjera u području kritičnih komunikacijskih i informacijskih sustava.

Ključni problem na kojem je potrebno raditi jest potreba puno veće konzistentnosti obrazovnih programa u području kibernetičke sigurnosti te bolje osposobljenosti predavača na različitim razinama i vrstama obrazovanja. Aktualno stanje još uvijek 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, potrebno je u odgovarajućoj mjeri uključiti u savjetodavni proces nadležnog ministarstva i drugih tijela povezanih s kurikularnom reformom i unaprjeđenjem svih vrsta i razina obrazovanja u RH.

# Prilog: SMJERNICE VIJEĆA ZA PROVEDBU MJERA IZ AKCIJSKOG PLANA U RAZDOBLJU DO KRAJA 2017. GODINE

Ove Smjernice izrađene su temeljem uočenih ključnih nedostataka u provedbi mjera iz Akcijskog plana u 2016. godini.

Prvo izvještajno razdoblje ukazuje na nedostatnu horizontalnu komunikacije između uključenih institucija – dionika provedbe mjera Akcijskog plana, što je jedan od temelja za uspješnost provedbe Akcijskog plana za provedbu Nacionalne strategije za kibernetičku sigurnost.

Također, dio dostavljenih izvješća o provedbi mjera oslanja se isključivo na rezultate redovnih aktivnosti institucije, što daje zaključiti da su se u prvom izvještajnom razdoblju rijetko provodile ciljane aktivnosti dionika, utemeljene na opsegu i sadržaju pojedine mjere iz Akcijskog plana. Za prvu fazu provedbe u 2016. godini, već i samo prepoznavanje redovnih aktivnosti institucija i njihovo ispravno povezivanje s tematskim mjerama Akcijskog plana predstavlja zadovoljavajući nacionalni rezultat, napose uz činjenicu da u razdoblju tijekom 2016. godine nije bilo uspostavljeno Nacionalno vijeće za kibernetičku sigurnost koje bi poticalo koordinaciju na međuresornoj i međusektorskoj razini.

Nacionalno vijeće za kibernetičku sigurnost stoga je odlučno u 2017. godini pokrenuti koordiniranu i ciljanu provedbu mjera kako su definirane Strategijom i Akcijskim planom te potaknuti sve dionike da dodatno razvijaju svoje temeljne sposobnosti i međusobno se povezuju i koordiniraju, stvarajući sinergijski učinak i na nacionalnoj i na sektorskim razinama.

U tu svrhu potrebno je:

- zadužiti nositelje (i sunositelje) provedbe mjera Akcijskog plana da odrede koordinatore provedbe svake od mjera za koje su Akcijskim planom zadužene;
- uvesti **ciljani izbor koordinatora provedbe svake mjere** na način da to budu osobe koje su po svom djelokrugu rada najbliže opsegu/sadržaju pojedine mjere i koje mogu stečena iskustva, postignute rezultate, ali i poteškoće u provedbi mjere, sustavno objediniti s drugim nositeljima i sunositeljima, analizirati i prikazati godišnjim popunjavanjem obrasca o provedbi pojedine mjere;
- inicirati **uspostavu radnih skupina koordinatora za sve mjere sa više nositelja i sunositelja**, kako bi se potaknuo sinergijski učinak u horizontalnoj suradnji institucija;
- potaknuti institucije nositelje provedbe pojedinih mjera na uspostavu proaktivne horizontalne koordinacije i **usklađivanje redovnih aktivnosti tijela nositelja i sunositelja u okviru provedbe mjera iz Akcijskog plana**;
- potaknuti nositelje na **uključivanje drugih sudionika u provedbu mjera** gdje god se time može postići dodatna kvaliteta u realizaciji ciljeva iz kojih mjera proizlazi.