VLADA REPUBLIKE HRVATSKE

2106

Na temelju članka 1. stavka 2. i članka 31. stavka 2. Zakona o Vladi Republike Hrvatske (»Narodne novine«, br. 150/11 i 119/14), a u svezi s točkom V. stavka 3. Odluke o osnivanju Povjerenstva za izradu Nacrta prijedloga nacionalne strategije kibernetičke sigurnosti, klase: 022-03/14-04/136, urbroja: 50301-09/09-14-2, od 30. travnja 2014. godine, Vlada Republike Hrvatske je na sjednici održanoj 7. listopada 2015. godine donijela

ODLUKU

O DONOŠENJU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

I.

Donose se Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, u tekstovima koje je izradilo Povjerenstvo za izradu Nacrta prijedloga nacionalne strategije kibernetičke sigurnosti, a dostavio Vladi Republike Hrvatske Ured Vijeća za nacionalnu sigurnost aktom, klase: 011-01/15-01/10, urbroja: 50439-05/21-15-40, od 29. rujna 2015. godine.

Nacionalna strategija i Akcijski plan sastavni su dio ove Odluke.

II.

Zadužuju se javnopravna tijela i druga tijela određena nositeljima i sunositeljima pojedinih mjera iz Akcijskog plana iz točke I. ove Odluke da u predviđenim rokovima provedu mjere i aktivnosti iz svoje nadležnosti.

III.

Zadužuje se Ured Vijeća za nacionalnu sigurnost da o donošenju ove Odluke obavijesti tijela iz točke II. ove Odluke.

IV.

Ova Odluka stupa na snagu danom donošenja, a objavit će se u »Narodnim novinama«.

Klasa: 022-03/15-07/81

Urbroj: 50301-09/09-15-5

Zagreb, 7. listopada 2015.

Predsjednik

Zoran Milanović, v. r.

NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI

1. UVOD

Tehnološki razvoj nigdje nije bio tako dinamičan i sveobuhvatan kao što je u području komunikacijske i informacijske tehnologije. Težište je uvijek bilo na brzom razvoju i uvođenju novih usluga i proizvoda, dok su sigurnosni aspekti, u pravilu, imali vrlo mali utjecaj na široko prihvaćanje novih tehnologija.

Životni ciklusi suvremenih informacijskih sustava, od procesa planiranja, uvođenja, korištenja, do povlačenja iz uporabe, vrlo su kratki, pa njihovo sustavno testiranje često nije moguće, odnosno najčešće se primjenjuje kao izuzetak, u slučajevima koji su izrijekom propisani.

Korisnici najčešće imaju minimalno znanje o tehnologiji koju koriste, a način primjene tehnologije je takav da je vrlo teško procijeniti sigurnosna obilježja većine komercijalnih proizvoda s obzirom na zaštitu povjerljivosti, odnosno privatnosti podataka korisnika. Sve je to dovelo do toga da se odnos korisnika prema komunikacijskoj i informacijskoj tehnologiji zasniva gotovo isključivo na slijepom povjerenju.

Suvremena društva duboko su prožeta komunikacijskom i informacijskom tehnologijom. Ljudi su danas povezani putem raznovrsnih tehnologija za prijenos teksta, slike i zvuka, a u porastu je i povezivanje elektroničkih uređaja u nepregledne mreže na koje čovjek nema utjecaj.

Dok bi odstupanje u normalnom funkcioniranju jedne vrste komunikacijskog i informacijskog sustava moglo proći nezapaženo, neispravan rad nekih drugih sustava mogao bi imati teške posljedice na funkcioniranje države, dovesti do gubitka života, zdravlja ljudi, velikih materijalnih šteta, onečišćenja okoliša i drugih funkcionalnosti bitnih za kvalitetno funkcioniranje društva u cjelini.

Od početaka razvoja komunikacijske i informacijske tehnologije do danas, odstupanja u njihovom ispravnom radu nastajala su zbog različitih razloga, od ljudskih pogrešaka ili zlonamjernih postupaka, do tehnoloških grešaka ili organizacijskih propusta.

Stvaranjem Interneta i povezivanjem niza komunikacijskih i informacijskih sustava javnog, akademskog i gospodarskog sektora te građanstva, stvoren je suvremeni kibernetički prostor koji sačinjava ne samo ova međusobno povezana infrastruktura, već i stalno rastuća količina raspoloživih podataka te korisnici koji međusobno komuniciraju u sve većem broju, pri čemu koriste rastući broj različitih usluga, neke potpuno nove, a neke tradicionalne, ali u novom, virtualnom obliku.

Odstupanja od ispravnog rada tih međusobno povezanih sustava ili njihovih dijelova više nisu samo tehničke smetnje, već predstavljaju opasnost globalnih sigurnosnih razmjera. Njima se suvremena društva suprotstavljaju nizom različitih aktivnosti i mjera

koje skupno nazivamo »kibernetička sigurnost«.

Pojam »kibernetički« uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu[1] još 2002. godine. Slijedom toga, uvriježilo se koristiti pojam »kibernetički« u obliku pridjeva za nešto što uključuje, koristi ili je povezano s računalima, a osobito s Internetom.

Izvorni pojam »kibernetika« nastao je sredinom prošlog stoljeća i predstavlja znanost o sustavima automatskog upravljanja te općenito procesima upravljanja u biološkim, tehničkim, ekonomskim i drugim sustavima. Pridjevska inačica »kibernetički« danas se u hrvatskom jeziku uvriježila na sličan način i s istim, prethodno uvedenim značenjem kakvo ima i prefiks »cyber-« u engleskom jeziku. Pojam »kibernetika« danas se u hrvatskom jeziku vrlo malo koristi u svom izvornom značenju, slično kao i pojam »cybernetics« u engleskom jeziku. U tehnički usmjerenim znanostima o upravljanju sustavima prevladava pojam »automatsko upravljanje«, a u širem smislu značenja pojma kibernetika, o procesima upravljanja u različitim sustavima, puno više se koristi »teorija sustava«, uvedena u drugoj polovini prošlog stoljeća.

Prepoznavanje važnosti sigurnosti kibernetičkog prostora kao zajedničke odgovornosti svih segmenata društva, potaklo je izradu ove Strategije. Njena svrha je sustavno i koordinirano provođenje aktivnosti potrebnih za podizanje sposobnosti RH u području kibernetičke sigurnosti, a s ciljem izgradnje sigurnog društva u kibernetičkom prostoru. Cilj je, također, i korištenje svih tržišnih potencijala informacijskog društva u cjelini te posebno proizvoda i usluga kibernetičke sigurnosti.

S obzirom na to da se radi o prvoj sveobuhvatnoj Strategiji u RH u području kibernetičke sigurnosti, primarni cilj Strategije je prepoznavanje organizacijskih problema u njezinoj provedbi te širenje razumijevanja važnosti ove problematike u društvu.

Poticanje koordinacije i suradnje svih državnih tijela i pravnih osoba s javnim ovlastima, ali i drugih sektora društva, nužno je kako bi se uspostavile nove funkcionalnosti, podigla učinkovitost rada relevantnih aktera te učinkovitije koristilo već postojeće resurse i bolje planiralo potrebu i ostvarenje novih resursa.

Temeljna uloga Strategije stoga je u povezivanju i međusobnom razumijevanju ove složene problematike u različitim sektorima društva te među različitim tijelima i pravnim osobama kao dionicima ove Strategije koji imaju različite nadležnosti, obveze, zadatke, potrebe, očekivanja i interese. Ovo je naročito važno za osiguravanje potrebne razine razumijevanja složene operativne i tehničke problematike kibernetičke sigurnosti, a koja je nužna nositeljima javne vlasti i odlučivanja u svim sektorima društva, kao i za sigurnost građanstva i prosperitet društva u cjelini, a time i za konačni cilj ove Strategije: provedbu zakona i poštivanja svih temeljnih ljudskih prava u novoj virtualnoj dimenziji društva.

Kako bi se obuhvatila vrlo široka i složena problematika na koju se odnosi Strategija te uskladio zajednički rad niza dionika koji su sudjelovali u izradi ove Strategije, upotrijebljena je metoda za razvoj sadržaja Strategije koja se sastoji od definiranja osnovnih načela pristupa području kibernetičke sigurnosti, zatim definiranja ciljeva Strategije te opsega primjene Strategije u odnosu na društvo u cjelini.

Nastavno na prethodno, utvrđena su prioritetna područja kibernetičke sigurnosti za RH, koja su analizirana prvenstveno u odnosu na opće ciljeve Strategije, a na isti način definirani su i posebni ciljevi svakog od utvrđenih područja kibernetičke sigurnosti za koje će se detaljnije provedbene mjere razraditi akcijskim planom za provedbu Strategije. Na ovaj način obuhvaćene su i specifičnosti svakog pojedinog područja vezano za Strategijom definirane sektore društva i oblike međusobne suradnje i koordinacije različitih dionika kibernetičke sigurnosti.

Kako bi se cjelovito obuhvatilo i one segmente kibernetičke sigurnosti za koje je procijenjeno da su u velikoj mjeri zajednički za sva, ili za većinu, prethodno utvrđenih područja kibernetičke sigurnosti, definirane su poveznice područja kibernetičke sigurnosti. Poveznice područja kibernetičke sigurnosti bitne su za poboljšanje i učinkovitije ostvarenje ciljeva i mjera u područjima kibernetičke sigurnosti. Stoga se i u odnosu na poveznice područja kibernetičke sigurnosti Strategijom definiraju posebni ciljevi koji su procijenjeni ključnim za unaprjeđenje razine sigurnosti u kibernetičkom prostoru. Posebna pažnja i ovdje je usmjerena na definirane sektore društva i utjecaj svake poveznice područja kibernetičke sigurnosti na pojedine sektore društva i oblike suradnje i međusobne koordinacije rada dionika kibernetičke sigurnosti.

2. NAČELA

Sveobuhvatnost pristupa kibernetičkoj sigurnosti obuhvaćanjem kibernetičkog prostora te infrastrukture i korisnika koji pripadaju pod nadležnost RH (državljanstvo, registracija, domena, adresa);

Integracija aktivnosti i mjera koje proizlaze iz različitih područja kibernetičke sigurnosti i njihovo međusobno povezivanje i nadopunjavanje u cilju stvaranja sigurnijeg zajedničkog kibernetičkog prostora;

Proaktivni pristup stalnom prilagodbom aktivnosti i mjera, kao i povremenom odgovarajućom prilagodbom strateških okvira iz kojih one proizlaze;

Jačanje otpornosti, pouzdanosti i prilagodljivosti primjenom univerzalnih kriterija povjerljivosti, cjelovitosti i raspoloživosti određenih skupina podataka i prepoznatih društvenih vrijednosti, uz poštivanje odgovarajućih obveza vezanih uz zaštitu privatnosti odnosno povjerljivosti, cjelovitosti i raspoloživosti, koje se nameću za pojedine skupine podataka, uključujući provedbu odgovarajuće certifikacije i akreditacije kako različite vrste uređaja i sustava, tako i poslovnih procesa u kojima se koriste takvi podaci.

Primjena osnovnih načela na kojima se temelji uređenje suvremenog društva i u području kibernetičkog prostora kao virtualne dimenzije društva:

1. Primjena zakona u svrhu zaštite ljudskih prava i sloboda, osobito privatnosti, vlasništva i svih drugih bitnih obilježja uređenog suvremenog društva;

2. Razvoj usklađenog zakonodavnog okvira kroz stalno poboljšavanje svih segmenata regulatornih mehanizama državne i sektorskih razina te kroz usklađene inicijative svih sektora društva, odnosno tijela i pravnih osoba u ulozi dionika ove Strategije;

3. Primjena načela supsidijarnosti kroz sustavno razrađen prijenos ovlasti za odlučivanje i obavještavanje o pitanjima kibernetičke sigurnosti na odgovarajuće tijelo čija nadležnost najbliže pokriva problem koji se rješava u područjima važnim za kibernetičku sigurnost, od organizacije, preko koordinacije i suradnje, do tehničke problematike odgovora na računalne ugroze određene komunikacijske i informacijske infrastrukture;

4. Primjena načela proporcionalnosti kako bi razina povećanja zaštite i povezanih troškova za tu svrhu, u svakom području bila proporcionalna s povezanim rizicima i mogućnostima ograničavanja prijetnji koje ih uzrokuju.

3. OPĆI CILJEVI STRATEGIJE

1. Sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, kibernetička dimenzija društva, vodeći računa o usklađenosti s međunarodnim obvezama te globalnim trendovima kibernetičke sigurnosti;

2. Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, koje je s ciljem osiguravanja svojstava raspoloživosti, cjelovitosti i povjerljivosti odgovarajućih skupina podataka korištenih u okviru kibernetičkog prostora, potrebno primijeniti kako na strani davatelja različitih elektroničkih i infrastrukturnih usluga, tako i na strani korisnika, odnosno svih pravnih i fizičkih osoba čiji su informacijski sustavi povezani s kibernetičkim prostorom;

3. Uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru, uz obvezu svakog dionika da pri tome, osobito u odnosu na pojedine skupine podataka, mora osigurati primjenu odgovarajućih i usklađenih normi zaštite podataka;

4. Jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora kroz pristup koji razlikuje specifičnosti javnog i gospodarskog sektora, pravnih i fizičkih osoba te koji uključuje uvođenje potrebnih obrazovnih elemenata u okviru redovnih školskih, kao i drugih izvannastavnih programa, ali i organiziranje i provedbu različitih aktivnosti usmjerenih osvješćivanju šire javnosti o pojedinim aktualnim pitanjima iz ove domene;

5. Poticanje razvoja usklađenih obrazovnih programa u školama, visokim učilištima, kroz namjenske i specijalističke tečajeve, povezivanjem akademskog, javnog i gospodarskog sektora;

6. Poticanje razvoja e-usluga kroz razvoj povjerenja korisnika u e-usluge definiranjem odgovarajućih minimalnih sigurnosnih zahtjeva;

7. Poticanje istraživanja i razvoja u svrhu aktiviranja potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora;

8. Sustavni pristup međunarodnoj suradnji koji omogućava učinkovit prijenos znanja i koordiniranu razmjenu, ustupanje i pristup potrebnim podacima između različitih nacionalno nadležnih tijela, institucija i sektora društva, a s ciljem prepoznavanja i stvaranja sposobnosti za uspješno sudjelovanje u poslovnim aktivnostima u globalnom okruženju.

4. SEKTORI DRUŠTVA I OBLICI SURADNJE DIONIKA KIBERNETIČKE SIGURNOSTI

Definiranjem sektora društva i njihovog značenja za potrebe ove Strategije, kao i načina suradnje dionika kibernetičke sigurnosti, definiran je i opseg primjene ove Strategije.

Sektori društva i njihovo značenje za potrebe ove Strategije su:

1. Javni sektor s različitim nadležnim tijelima koja su dionici Strategije te ostalim državnim tijelima, tijelima jedinica lokalne i područne (regionalne) samouprave, odnosno pravnim osobama s javnim ovlastima te institucijama, koji na različite načine predstavljaju korisnike kibernetičkog prostora i obveznike primjene mjera koje proizlaze iz Strategije;

2. Akademski sektor u uskoj suradnji s nadležnim državnim tijelima koja su dionici Strategije, kao i druge obrazovne institucije iz javnog i gospodarskog sektora koje na različite načine predstavljaju korisnike kibernetičkog prostora i obveznike primjene mjera koje proizlaze iz Strategije;

3. Gospodarski sektor u uskoj suradnji s nadležnim državnim i regulatornim tijelima koja su dionici Strategije, napose pravne osobe koje su obveznici posebnih propisa o kritičnim infrastrukturama i obrani, kao i sve druge pravne osobe, odnosno poslovni subjekti koji na različite načine predstavljaju korisnike kibernetičkog prostora i obveznike primjene mjera koje proizlaze iz Strategije, sa svim specifičnostima tih pravnih osoba i subjekata, s obzirom na djelatnosti kojima se bave, broj zaposlenika koji imaju te tržišta koja pokrivaju;

4. Građanstvo u cjelini koje predstavlja korisnike komunikacijskih i informacijskih tehnologija i usluga i na koje se na različite načine reflektira stanje sigurnosti u kibernetičkom prostoru. Odnosi se i na one građane koji ne koriste aktivno kibernetički prostor, ali se njihovi osobni podaci nalaze u njemu.

Oblici suradnje dionika kibernetičke sigurnosti predviđeni ovom Strategijom su:

1. Koordinacija unutar javnog sektora;

2. Nacionalna suradnja javnog, akademskog i gospodarskog sektora;

3. Savjetovanje sa zainteresiranom javnošću i informiranje građanstva;

4. Međunarodna suradnja dionika kibernetičke sigurnosti.

Svi ovi oblici suradnje provode se na sustavan i koordiniran način, sukladno nadležnostima, sposobnostima, ciljevima i prema funkcionalno razrađenim područjima kibernetičke sigurnosti.

5. PODRUČJA KIBERNETIČKE SIGURNOSTI

Područja kibernetičke sigurnosti definirana su sukladno procjeni prioritetnih potreba RH u trenutku izrade Strategije i obuhvaćaju sigurnosne mjere u području komunikacijske i informacijske infrastrukture i usluga, u kojem razlikujemo javne elektroničke komunikacije, elektroničku upravu i elektroničke financijske usluge, kao infrastrukturu od primarnog strateškog interesa društva u cjelini.

Vrlo važno područje kibernetičke sigurnosti predstavlja i zaštita kritične komunikacijske i informacijske infrastrukture koja se može nalaziti u svakom od prethodna tri infrastrukturna područja, ali koja ima bitno različita obilježja te je potrebno utvrditi kriterije za prepoznavanje takvih obilježja.

Kibernetički kriminalitet prisutan je u društvu već dugo vremena u različitim pojavnim oblicima, ali na današnjem stupnju razvoja virtualne dimenzije društva predstavlja stalnu i rastuću prijetnju razvoju i gospodarskom prosperitetu svake suvremene države. Stoga se suzbijanje kibernetičkog kriminaliteta, također, prepoznaje kao prioritetno područje kibernetičke sigurnosti za koje je nužno definirati strateške ciljeve u svrhu unaprjeđenja u suzbijanju ovog oblika kriminaliteta u narednom razdoblju.

Područje kibernetičke obrane predstavlja dio strategije obrane za koje je zaduženo ministarstvo nadležno za poslove obrane i ono je predmet zasebne obrade i rješavanja, pri čemu će se koristiti svi potrebni elementi koji proizlaze iz ove Strategije. Kibernetički terorizam i drugi kibernetički aspekti nacionalne sigurnosti obrađuju se u okviru manjeg broja nadležnih tijela sigurnosno-obavještajnog sustava te zahtijevaju zaseban pristup u rješavanju, pri čemu će se, također, koristiti svi potrebni elementi koji proizlaze iz ove Strategije.

Područja kibernetičke sigurnosti analiziraju se u odnosu na opće ciljeve Strategije, radi identificiranja posebnih ciljeva usmjerenih na poboljšanje u svakom pojedinom području i mjera potrebnih za ostvarenje postavljenih ciljeva Strategije. Posebni ciljevi, kao i mjere koje će se detaljnije razraditi akcijskim planom za provedbu Strategije, utvrđuju se s osvrtom na definirane sektore društva i utjecaj područja kibernetičke sigurnosti na svaki pojedini sektor, ali i s osvrtom na oblike međusobne suradnje i koordinacije dionika kibernetičke sigurnosti. Pri tome se kroz razradu područja kibernetičke sigurnosti prate načela definirana Strategijom.

5.1 Elektronička komunikacijska i informacijska infrastruktura i usluge

5.1.1 Javne elektroničke komunikacije (A)

Javne elektroničke komunikacije podrazumijevaju davanje na korištenje elektroničke komunikacijske mreže i/ili pružanje elektroničke komunikacijske usluge. Elektronička komunikacijska i informacijska infrastruktura, obavljanje djelatnosti elektroničkih komunikacijskih mreža i usluga, prostorno planiranje, gradnja, održavanje, razvoj i korištenje elektroničkih komunikacijskih mreža, elektroničke komunikacijske infrastrukture i druge povezane opreme te upravljanje i uporaba radiofrekvencijskog spektra, adresnog i brojevnog prostora, kao prirodno ograničenih općih dobara, od interesa su za RH.

Pravne, regulatorne i tehničke odredbe koje se usvoje na razini EU-a, u vezi sa zaštitom osobnih podataka, privatnosti i legitimnih interesa pravnih osoba u području elektroničkih komunikacija, treba nastaviti trajno usklađivati kako bi se zajamčilo da neće postojati zapreke promicanju i razvoju novih elektroničkih komunikacijskih mreža i usluga između država članica EU-a.

Osnovni ciljevi RH vezani uz kibernetičku sigurnost u području javnih elektroničkih komunikacija su:

Cilj A.1 *Nadzor tehničkih i ustrojstvenih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga, kao i usmjeravanje operatora javnih komunikacijskih mreža i/ili usluga u cilju osiguranja visoke razine sigurnosti i dostupnosti javnih komunikacijskih mreža i usluga.*

Potrebno je obuhvatiti različite zahtjeve koji se postavljaju prema operatorima, od kvalitete i dostupnosti mreža i usluga, preko zahtjeva vezanih za zaštitu osobnih podataka, zahtjeva za osiguravanje primjerene pažnje u provedbi sigurnosnih mjera na temelju odgovarajućih međunarodnih normi, zahtjeva za provedbu zakonskih obveza tajnog nadzora elektroničkih komunikacijskih mreža i usluga, kao i potrebu razvijanja i stalnog unaprjeđivanja sigurnosne suradnje i razmjene podataka s tijelima nadležnim za računalne sigurnosne incidente u području javnih elektroničkih komunikacija te tijelima kaznenog progona.

Cilj A.2 *Neposredna tehnička koordinacija regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti.*

Potrebno je stvoriti i kontinuirano razvijati međusektorsku suradnju nacionalnih regulatornih tijela i tijela odgovornih za područje informacijske sigurnosti i politike zaštite podataka te uspostaviti međusobnu koordinaciju i razmjenu iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira.

Cilj A.3 *Poticanje korištenja nacionalnog čvora za međusobnu razmjenu internetskog prometa pružatelja javnih komunikacijskih mreža i/ili usluga za davanje usluga korisnicima u RH.*

Neprofitna usluga Croatian Internet eXchange (CIX) osigurava međusobnu razmjenu internetskog prometa između korisnika različitih usluga najkraćim komunikacijskim putem u okviru nacionalnog sustava javnih elektroničkih komunikacija. Ovaj način razmjene internetskog prometa predstavlja sigurnosni zahtjev za operatore koji pružaju usluge državnim tijelima, ali i potrebu učinkovitog i ekonomičnog nacionalnog povezivanja svih drugih korisnika u gospodarskom sektoru i samog građanstva RH.

5.1.2 Elektronička uprava (B)

Elektronička uprava strateški je cilj RH kojim se osigurava brza, transparentna i sigurna usluga svim građanima putem kibernetičkog prostora. U tu svrhu nužno je uspostaviti sustav javnih registara i njime upravljati kroz jasno definirana prava, obveze i odgovornosti nadležnih tijela javnog sektora. Za osiguranje potrebne razine sigurnosti podataka pohranjenih u takvim registrima nužno je korištenje zajedničke osnovice za sigurnu razmjenu podataka unutar sustava državne informacijske infrastrukture, zajedničkog sustava identifikacije i autentifikacije. RH će i dalje razvijati i unaprjeđivati elektroničku komunikaciju s građanima, kao i međusobno povezivanje državnih tijela odnosno tijela javnog sektora općenito. Osobita pažnja će se staviti na:

1. Dostupnost podataka iz javnih registara svim tijelima javnog sektora, građanima i drugim korisnicima sukladno propisima o zaštiti osobnih podataka, tajnosti podataka, informacijske sigurnosti te propisima o pravu na pristup informacijama;

2. Sustavni razvitak državne informacijske infrastrukture uključujući i prostorno planiranje, gradnju, održavanje, razvoj i korištenje elektroničkih komunikacijskih mreža i infrastrukture za potrebe javnog sektora;

3. Sustavnu zaštitu i sigurnost državne informacijske infrastrukture sukladno propisima o sigurnosti informacijskih sustava;

4. Jedinstveno upravljanje Vlade RH razvitkom državne informacijske infrastrukture na osnovi usuglašavanja potreba i prioriteta;

5. Usklađivanje planova i projekata informatizacije s normama i drugim odrednicama izgradnje informacijske infrastrukture u RH i EU;

6. Interoperabilnost, skalabilnost i ponovno korištenje;

7. Racionalizaciju izdataka za izgradnju i zaštitu informacijske infrastrukture na razini svih tijela javnog sektora.

Cilj B.1 *Poticati povezivanje informacijskih sustava tijela javnog sektora međusobno i na javni Internet kroz državnu informacijsku infrastrukturu.*

Tijela javnog sektora koja nisu obuhvaćena zakonom koji regulira područje državne informacijske infrastrukture, u suradnji s nadležnim državnim tijelima za razvoj i sigurnost državne informacijske infrastrukture, provest će analizu potreba i mogućnosti

povezivanja na državnu informacijsku infrastrukturu te u skladu s rezultatima analize planirati povezivanje na državnu informacijsku infrastrukturu ili dodatne mjere zaštite.

Cilj B.2 *Podići razinu sigurnosti informacijskih sustava javnog sektora.*

Provest će se analiza postojećeg stanja u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora te će se definirati dinamika primjene sustava NIAS i odgovarajućih normi (ISO 27001 i sl.). Organizacijske i tehničke norme za povezivanje na državnu informacijsku infrastrukturu, uvjeti i aktivnosti nužni za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoja te ostali elementi neophodni za rad državne informacijske infrastrukture trajno će se procjenjivati kroz koordinaciju nadležnih tijela, uključujući i sigurnosna tijela.

Cilj B.3 *Donošenje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica.*

Standardna jednostupanjska autentifikacija, odnosno vjerodajnice razine 2 sukladno dokumentu »Kriteriji za određivanje razine osiguranja kvalitete autentifikacije za NIAS«[2] nisu zadovoljavajuće razine sigurnosti za pristup osjetljivim podacima. Zadovoljavajuće rješenje u smislu smanjenja sigurnosnih rizika, prihvatljivo za korištenje u okviru usluga elektroničke uprave, je korištenje vjerodajnica viših (razina 3) ili najviših (razina 4) razina sigurnosti. Nadležna tijela će provesti analizu i međusobnu koordinaciju u svrhu donošenja kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica. U okviru ove analize obuhvatit će se i procjena mogućnosti korištenja buduće elektroničke osobne iskaznice građana za potrebe elektroničke uprave i drugih javnih i financijskih usluga. Također će se obuhvatiti i drugi aspekti povezani s nacionalnim mogućnostima za uspostavu odgovarajućih akreditacijskih i certifikacijskih sposobnosti u području kvalificiranih elektroničkih potpisa, sukladno EU zahtjevima.

5.1.3 Elektroničke financijske usluge (C)

Informacijska tehnologija i njezine pogodnosti uvelike se koriste i u području pružanja financijskih usluga. Postizanje zadovoljavajuće razine sigurnosti cilj je svake suvremene države, a osnovni ciljevi RH vezani uz kibernetičku sigurnost u području elektroničkih financijskih usluga su:

Cilj C.1 *Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, a s ciljem poticanja razvoja elektroničkih financijskih usluga.*

Kontinuirano poticati pružatelje elektroničkih financijskih usluga na uvođenje novih te unaprjeđivanje postojećih mehanizama zaštite od zlonamjernih aktivnosti, a sukladno aktualnim prijetnjama te procjeni rizika. Pri tome posebnu pozornost treba posvetiti identifikaciji i autentifikaciji korisnika elektroničkih financijskih usluga, autorizaciji financijskih transakcija te pravovremenom otkrivanju i ograničavanju utjecaja neovlaštenih aktivnosti.

Cilj C.2 *Unaprijediti razmjenu i ustupanje podataka o nastalim računalnim sigurnosnim incidentima između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela.*

Osigurati uvjete za provedbu učinkovite razmjene i ustupanja podataka čime se unaprjeđuje rješavanje nastalih računalnih sigurnosnih incidenata te ujedno osigurava sprječavanje nastanka ili ograničavanje učinka takvih incidenata u budućnosti. Pri tome posebnu pozornost treba posvetiti zaštiti osobnih, kao i drugih podataka na koje se odnose zakonska ograničenja vezana uz korištenje, pa tako i dijeljenje podataka, razvoju povjerenja između uključenih strana te uspostavi protokola i mehanizama koji će osigurati učinkovito i sigurno prikupljanje, dijeljenje i razmjenu takvih podataka. Razmjena i ustupanje podataka o nastalim računalnim sigurnosnim incidentima provodi se između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela, kao i tijela nadležnih za računalne sigurnosne incidente u području javnih elektroničkih komunikacija te tijela kaznenog progona.

5.2 Kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama (D)

Donošenjem Zakona o kritičnim infrastrukturama[3] i pratećim podzakonskim aktima stvoreni su legislativni preduvjeti za uspješno upravljanje rizicima kritične komunikacijske i informacijske infrastrukture unutar utvrđenih sektora kritične infrastrukture, u cilju:

1. povećanja otpornosti/smanjenja ranjivosti komunikacijskih i informacijskih sustava;

2. umanjivanja posljedica negativnih događaja (prirodne i tehničko-tehnološke nesreće) i mogućih napada (namjernih i nenamjernih);

3. omogućavanja brzog i učinkovitog oporavka te nastavka rada.

Odlukom Vlade RH[4] sektor komunikacijske i informacijske tehnologije utvrđen je kao jedan od sektora iz kojih središnja tijela državne uprave primjenom odgovarajuće metode identificiraju nacionalne kritične infrastrukture. Kao njegovi podsektori utvrđuju se: elektroničke komunikacije, prijenos podataka, informacijski sustavi i pružanje audio i audio-vizualnih medijskih usluga. Ovi se podsektori dalje raščlanjuju na elektroničke komunikacijske mreže, infrastrukturu i povezanu opremu, informatičku infrastrukturu te sustave zemaljske radiodifuzije.

Od strateškog je interesa nastaviti s poduzimanjem aktivnosti u području zaštite kritične komunikacijske i informacijske infrastrukture, u svrhu osiguravanja svih potrebnih uvjeta za njihov rad i kontinuirano djelovanje.

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.

Stoga je identificiranje kritične komunikacijske i informacijske infrastrukture i propisivanje obveznih tehničkih i organizacijskih mjera, uključujući i postupke izvješćivanja o računalnim sigurnosnim incidentima, potrebno provesti u koordinaciji središnjih državnih tijela za pojedine sektore kritične infrastrukture, vlasnika/upravitelja kritične infrastrukture te nadležnih tehničkih i sigurnosnih državnih tijela.

Također, uspostavljanje sustava upravljanja kibernetičkim krizama koji će osigurati pravovremenu i učinkovitu reakciju/odgovor na prijetnju i osigurati oporavak infrastrukture ili usluge od naročitog je sigurnosnog interesa 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 i NATO-a,

4. usklađenost s nacionalnim nadležnostima tijela zakonom zaduženih za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

U tom smislu, potrebno je:

Cilj D.1 *Utvrditi kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture.*

Kriteriji za prepoznavanje kritične komunikacijske i informacijske infrastrukture moraju pratiti i dalje razrađivati Zakonom o kritičnoj infrastrukturi predviđenu metodologiju pristupa. Pri tome se kritična komunikacijska i informacijska infrastruktura utvrđuje u okvirima sektora utvrđenih ranije spomenutom Odlukom Vlade RH o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te listom redoslijeda sektora kritičnih infrastruktura. Kriteriji koji se definiraju za utvrđivanje kritične komunikacijske i informacijske infrastrukture moraju proizlaziti iz metodologije koju primjenjuje Zakon o kritičnim infrastrukturama te se, prema potrebi koja proizlazi iz analize stanja, mogu dodatno razraditi i propisati odgovarajućim podzakonskim aktima.

Cilj D.2 *Utvrditi obvezujuće sigurnosne mjere koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture.*

Potrebno je utvrditi skup sigurnosnih mjera koje na sustavan način primjenjuju svi utvrđeni vlasnici/upravitelji kritične komunikacijske i informacijske infrastrukture, kao i potrebnu vezu prema općim propisima informacijske sigurnosti u segmentima kao što su zahtjevi sigurnosnog provjeravanja osoba ili potreba klasificiranja podataka.

Cilj D.3 *Ojačati prevenciju i zaštitu kroz upravljanje rizikom.*

Prioritetna aktivnost je osigurati provedbu odredbi Zakona o kritičnim infrastrukturama u dijelovima koji se odnose na sektorsku procjenu rizika kritične komunikacijske i informacijske infrastrukture, sektorske planove osiguranja rada kritične komunikacijske i informacijske infrastrukture i sigurnosne planove vlasnika/upravitelja kritične komunikacijske i informacijske infrastrukture.

Sektorska procjena rizika uključuje:

1. identifikaciju kritičnih funkcija (službe, podaci, mreže, itd.);

2. identifikaciju prijetnji;

3. procjenu prijetnji, ranjivosti i posljedica;

4. analizu i prioritetiziranje rizika;

5. utvrđivanje prihvatljivog rizika i obradu rizika.

Sektorski planovi osiguranja rada kritične infrastrukture i sigurnosni planovi vlasnika/upravitelja ove kritične infrastrukture sadrže mjere i aktivnosti za pripravnost, prevenciju, zaštitu, odgovor i oporavak u slučaju računalnih sigurnosnih incidenata koji imaju negativan utjecaj na funkcioniranje sektora kritične infrastrukture, odnosno proizvodnju, isporuku roba i usluga i druge funkcije vlasnika/upravitelja kritične infrastrukture upravljanje kojom ili čije funkcioniranje se bazira na kritičnoj komunikacijskoj i informacijskoj infrastrukturi. Posebnu pozornost potrebno je posvetiti stručnom usavršavanju osoba koje će biti uključene u postupak utvrđivanja kritične komunikacijske i informacijske infrastrukture.

Cilj D.4 *Ojačati javno-privatno partnerstvo i tehničku koordinaciju u obradi računalnih sigurnosnih incidenata.*

U sklopu sektora kritične infrastrukture utvrđenih ranije spomenutom Odlukom Vlade RH o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te listom redoslijeda sektora kritičnih infrastruktura, potrebno je putem sektorski nadležnih središnjih tijela državne uprave poticati javno-privatno partnerstvo u cilju osiguravanja nesmetanog rada za poslovne subjekte koji predstavljaju vlasnike/upravitelje kritične infrastrukture. U tom smislu potrebno je utvrditi odgovarajuće postupke nadzora, koordinacije, kao i razmjene i ustupanja potrebnih sigurnosnih podataka. Razmjena i ustupanje podataka provode se između sektorskih nositelja i vlasnika/upravitelja kritične infrastrukture, s tijelima koja su nadležna za računalne sigurnosne incidente u područjima javne elektroničke komunikacijske i informacijske infrastrukture i usluga, kao i s tijelima kaznenog progona. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata provodi se suradnjom tijela koja imaju izgrađene sposobnosti odgovora na takvu vrstu incidenata.

Cilj D.5 *Uspostaviti kapacitete za učinkoviti odgovor na prijetnju koja može imati za posljedicu kibernetičku krizu.*

U RH je potrebno izgraditi nacionalni sustav upravljanja u kibernetičkim krizama, kao dio nacionalnog sustava upravljanja u krizama, u kojem će odgovornosti relevantnih sudionika biti jednoznačno određene na temelju postojećih nadležnosti tijela i dodatnog definiranja uloga tijela u slučajevima koji predstavljaju krizna stanja.

Nacionalni sustav upravljanja u kibernetičkim krizama treba osigurati:

– sustavno praćenje stanja sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu,

– periodično izvješćivanje o stanju kibernetičke sigurnosti,

– učinkovito planiranje postupanja u kibernetičkim krizama,

– usklađeno i koordinirano postupanje državnih tijela u kibernetičkim krizama.

U tu svrhu potrebno je provesti iscrpnu analizu postojećeg stanja, osobito u odnosu na pravni okvir i potrebe za njegovim doradama u kontekstu možebitnog uvođenja novih nadležnosti koje zahtjeva bavljenje ovom problematikom. Temeljem rezultata provedene analize, predložit će se definicija pojma kibernetičke krize u okviru šireg koncepta nacionalnog upravljanja u krizama, kao i kriteriji za utvrđivanje kibernetičke krize.

5.3 Kibernetički kriminalitet (E)

Računalni, odnosno kibernetički kriminalitet obuhvaća kaznena djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom komunikacijskih i informacijskih tehnologija i predstavlja prijetnju ostvarenju sigurnijeg informacijskog društva.

Uspostava učinkovitih preventivnih mjera, ali i odgovori kaznenog prava na ovu vrstu kriminaliteta ključni su element za postizanje odgovarajuće razine zaštite, nesmetanog djelovanja i sigurnosti računalnih sustava.

S ciljem kvalitetnijeg i uspješnijeg suzbijanja ovog oblika kriminaliteta potrebno je:

Cilj E.1 *Kontinuirano unaprjeđivati nacionalni zakonodavni okvir, vodeći pri tome računa o međunarodnim obvezama.*

S obzirom na to da ubrzani napredak tehnologija dovodi do pojave novih modaliteta počinjenja kaznenih djela putem računalnih sustava i mreža, što prati i razvoj legislative na međunarodnoj razini u ovoj domeni, nužno je kontinuirano pratiti, analizirati i, po potrebi, prilagođavati nacionalno zakonodavstvo novonastalim promjenama.

Cilj E.2 *Unaprjeđivati i poticati međunarodnu suradnju u svrhu učinkovite razmjene informacija.*

Globalizacija kibernetičkog kriminaliteta kao pojave čiji počinitelji ne poznaju fizičke državne granice, legislativne različitosti država u kojima djeluju te ignoriraju jezične barijere, zahtijeva kvalitetnu suradnju između država članica EU, članica NATO-a kao i međunarodnu suradnju s trećim državama, kako bi se pravodobno identificirao svaki novi pojavni oblik ili prijetnja, kao i njegov izvor te kako bi reakcija na pojedine ugroze bila što brža. U tom smislu potrebno je koristiti raspoložive mogućnosti već uspostavljenih načina suradnje putem kontakt točaka, odnosno mogućnosti brze razmjene informacija putem kanala Europola i Eurojusta i drugih međunarodnih organizacija.

Cilj E.3 *Kvalitetna međuinstitucionalna suradnja u svrhu učinkovite razmjene informacija na nacionalnoj razini, a posebno u slučaju računalnog sigurnosnog incidenta.*

Računalni sigurnosni incident zahtijeva brzo i adekvatno rješavanje. U tom smislu potrebno je uspostavljanje kvalitetne koordinacije svih tijela koja tome u konkretnom slučaju mogu doprinijeti. Postojanje stalnih »kontakt točaka« doprinijelo bi neposrednoj i učinkovitoj komunikaciji, a samim time prevenciji i učinkovitijem rješavanju nastalog incidenta.

Cilj E.4 *Jačanje ljudskih potencijala, adekvatni razvoj kompetencija i tehničkih mogućnosti nadležnih državnih tijela za otkrivanje, kriminalističko istraživanje i procesiranje kaznenih djela iz domene računalnog kriminaliteta te osiguranje potrebne financijske potpore.*

Paralelno s razvojem infrastrukture elektroničkih komunikacija i uvođenjem novih inovativnih usluga pojavljuju se i novi, sve sofisticiraniji načini počinjenja kaznenih djela iz domene računalnog kriminaliteta. Ti procesi moraju biti popraćeni kontinuiranim jačanjem ljudskih potencijala, odgovarajućim nadogradnjama forenzičkih alata i sustava, kao i sustava za tajni nadzor elektroničkih komunikacijskih mreža i usluga.

Cilj E.5 *Poticanje i stalni razvoj suradnje s gospodarskim sektorom.*

Poticanje i stalni razvoj suradnje s gospodarskim sektorom (osobito s nezavisnim regulatorom i pravnim osobama u okviru sektora javnih elektroničkih komunikacija i sektora elektroničkih financijskih usluga), kao i dvosmjerna razmjena podataka o svim novim zabilježenim računalnim sigurnosnim incidentima, kako bi gospodarski sektor mogao prepoznati potencijalni incident koji moguće predstavlja kazneno djelo te pravodobno ažurirati vlastiti sigurnosni sustav, odnosno, kako bi tijela državne uprave pravodobno reagirala na eventualno kazneno djelo. Također, kroz kvalitetnu suradnju s gospodarskim sektorom poticati komunikaciju u svrhu obrazovanja krajnjih korisnika pojedinih usluga, a kako bi se neposredno doprinijelo prevenciji pojave konkretnih oblika kibernetičkog kriminaliteta.

6. POVEZNICE PODRUČJA KIBERNETIČKE SIGURNOSTI

Poveznice područja kibernetičke sigurnosti definirane su sukladno procjeni potreba RH u trenutku izrade Strategije i obuhvaćaju segmente kibernetičke sigurnosti za koje je procijenjeno da su u velikoj mjeri zajednički za sva, ili većinu, prethodno odabranih područja kibernetičke sigurnosti. Odabrane poveznice područja kibernetičke sigurnosti su:

1. Zaštita podataka;

2. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata;

3. Međunarodna suradnja te

4. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.

Poveznice područja kibernetičke sigurnosti bitne su za poboljšanje i efikasnije ostvarenje ciljeva i mjera u područjima kibernetičke sigurnosti, stoga se i u odnosu na poveznice Strategijom definiraju posebni ciljevi koji se cijene ključnim za unaprjeđenje razine sigurnosti u kibernetičkom prostoru, s posebnim osvrtom na definirane sektore društva i utjecaj svake poveznice područja kibernetičke sigurnosti na pojedine sektore društva i oblike suradnje i međusobne koordinacije rada dionika kibernetičke sigurnosti. Pri tome se kroz razradu poveznica područja kibernetičke sigurnosti prate načela definirana Strategijom.

6.1 Zaštita podataka (F)

U životnom ciklusu podatka, već pri njegovom nastanku, neophodno je prepoznati pripada li pojedini podatak određenoj skupini zaštićenih podataka te primijeniti odgovarajući skup mjera u svrhu zaštite takvog podatka. Odgovornost je svakog vlasnika, svakog voditelja zbirke, ali i svakog izvršitelja obrade zaštićenih podataka i ovlaštenog korisnika zaštićenih podataka, skrbiti ne samo o povjerljivosti i privatnosti podataka koje koriste u svom radu, već biti odgovoran i za cjelovitost i raspoloživost podataka koji se javno objavljuju u kibernetičkom prostoru (web-stranice, društvene mreže i sl.).

Kako bi se na odgovarajući način usmjerilo postupanje sa zaštićenim podacima, osobito nositelja odgovornosti za zaštićene podatke, u okviru izrade ove Strategije kao najvažnije posebne skupine zaštićenih podataka za koje je potrebno implementirati adekvatne politike zaštite, prepoznate su sljedeće skupine zaštićenih podataka: klasificirani podatak, označeni neklasificirani podatak, osobni podatak i poslovna tajna.

U područjima kibernetičke sigurnosti utvrđenim ovom Strategijom postoji velika potreba međusobne razmjene ili ustupanja podataka koji u većini slučajeva predstavljaju neku od gore navedenih posebnih skupina zaštićenih podataka.

Svaka od ovih skupina zaštićenih podataka regulirana je odgovarajućim paketom zakonskih i podzakonskih propisa, a do sada uočeni problemi u praksi, u većini slučajeva, povezani su s provedbenim politikama zaštite podataka, osobito u pravnim osobama, kao i sa širim nedostatnim razumijevanjem i sviješću u različitim sektorima društva o potrebi i nužnosti razvoja kulture postupanja s određenim skupinama zaštićenih podataka.

Kako bi se unaprijedilo stanje sigurnosti i osigurali svi preduvjeti nužni za nesmetanu razmjenu ili ustupanje takvih podataka među različitim nadležnim dionicima uključenima u određene aktivnosti kibernetičke sigurnosti, potrebno je:

Cilj F.1 *Doraditi nacionalnu regulativu u području poslovne tajne.*

Uočeno je da u području regulative poslovne tajne na nacionalnoj razini postoji prostor za njezinu doradu, koja bi trebala pratiti i aktualnu unifikaciju ovog područja koju je EU započela u državama članicama 2013. godine. Trenutno stanje može dovesti do pravne nesigurnosti te se smatra nužnim razraditi kriterije za utvrđivanje i zaštitu poslovne tajne, uz obvezujuću primjenu načela primjerene pažnje nositelja odgovornosti pri korištenju ove skupine zaštićenih podataka.

Cilj F.2 *Poticanje stalne suradnje između tijela nadležnih za posebne skupine zaštićenih podataka u nacionalnom okruženju u svrhu postizanja usklađenosti u provedbi relevantnih propisa.*

Uočena je potreba međuresorne i međusektorske koordinacije društva u cjelini u svrhu usklađivanja pojedinih provedbenih elemenata zakonske regulative. Ističe se potreba i važnost međusobne razmjene iskustava nadležnih nacionalnih i međunarodnih tijela za pojedine skupine zaštićenih podataka u nacionalnom okruženju, kao i za praćenje svih aktualnih izmjena u pravilima pristupa podacima, osobito u EU i NATO okruženju te u okviru potreba i obveza RH kao članice EU-a i NATO-a. Mjerama akcijskog plana za provedbu Strategije potrebno je usmjeriti pažnju prema institucijama, odnosno svim nositeljima odgovornosti za zaštićene podatke. Uloga nositelja odgovornosti za zaštićene podatke je osigurati ujednačen pristup provedbi relevantne zakonske regulative kod svih izvršitelja obrade, ali i ovlaštenih korisnika takvih podataka, odnosno u okviru odgovarajućih internih politika informacijske sigurnosti koje ti izvršitelji odnosno korisnici provode.

Cilj F.3 *Određivanje kriterija za prepoznavanje nacionalnih elektroničkih registara koji su kritični informacijski resursi te nositelja odgovornosti za njihovu zaštitu.*

Jedan od važnih uočenih problema su neodgovarajuće politike zaštite podataka u nacionalnim elektroničkim registrima. Ovdje se pojavljuje problem kumulacije velikog broja podataka iz određene skupine (npr. nacionalni podaci koji se prikupljaju za sve građane), čime ranjivost ovakvih informacijskih resursa postaje kritična i za druge povezane informacijske resurse. Potrebna je pažljiva analiza ovog područja te određivanje kriterija po kojima bi se mogli definirati nacionalni elektronički registri koji predstavljaju kritične informacijske resurse te utvrditi dodatni zahtjevi zaštite ovakvih kritičnih informacijskih resursa, s jedne strane prateći mogućnost primjene propisa o kritičnim nacionalnim infrastrukturama te s druge strane kroz moguće povezivanje s kriterijima za određivanje stupnja tajnosti klasificiranog podatka za zbirke podataka čiji zbirni elektronički oblik postaje kritičan na nacionalnoj razini i u opisanom smislu.

Cilj F.4 *Unaprjeđenje postupanja sa zaštićenim podacima kod nositelja odgovornosti za zaštićene podatke, izvršitelja obrade zaštićenih podataka i ovlaštenih korisnika zaštićenih podataka.*

Unatoč zadovoljavajućoj regulativi, usuglašenoj s međunarodnim zahtjevima EU-a i NATO-a, postoji prostor za praktična provedbena poboljšanja i u području korištenja, odnosno razmjene i ustupanja, kako klasificiranih tako i osobnih podataka, naročito u odnosu na pravne osobe i korištenje podataka u elektroničkom obliku, bilo da se pravne osobe pojavljuju kao izvršitelji obrade zaštićenih podataka ili kao korisnici takvih podataka. Naročitu pažnju ovdje valja usmjeriti na specifičnosti kibernetičkog prostora i usluga koje proizlaze vezano za računalnu infrastrukturu, programske platforme ili razvojne aplikacije u računalnom oblaku. Potrebna je razrada prilagođenih obrazaca ugovora (prilozi, aneksi, klauzule), koji bi se odgovarajuće unificirali i pripremili za različite praktične primjene, čime bi se obveznici primjene zakonskih propisa usmjeravali na detalje provedbe svih onih obveza koje su od visoke važnosti za zaštitu podataka, osobito u okviru ugovora čija provedba ili već samo sklapanje zahtijeva ustupanje i korištenje zaštićenih podataka. Obuhvatile bi se i specifičnosti kibernetičkog prostora i usluga, odnosno uvjeti korištenja računalne infrastrukture, platforme, ili aplikacije u računalnom oblaku. Problematika se promatra u kontekstu pojedinih skupina zaštićenih podataka i pripadnih regulatornih zahtjeva te s obzirom na specifičnosti kibernetičkog prostora i usluga računalstva u oblaku, kao što su problemi podataka koji su izvan fizičke kontrole vlasnika prilikom komunikacije, obrade ili pohrane, problemi povezani s različitom pravnom odgovornošću davatelja usluga unutar različitih pravnih okvira (nacionalni, EU, treće zemlje), odnosno povezana problematika relevantnog nacionalnog okvira za identifikaciju, autentifikaciju i autorizaciju korisnika određenih elektroničkih usluga u javnom i gospodarskom sektoru.

Cilj F.5 *Unificiranje pristupa u korištenju palete normi HRN ISO/IEC 27000.*

Paleta normi HRN ISO/IEC 27000 koristi se u više sektora društva i za zaštitu različitih skupina podataka (npr. područje zaštite osobnih podataka, područje zaštite označenih neklasificiranih podataka, kreditne institucije – smjernice središnje banke RH, davatelji javnih elektroničkih usluga – pravilnik nacionalnog regulatornog tijela za mrežne djelatnosti). Nadležna sektorska i podatkovna tijela trebala bi provesti analizu mogućnosti unificiranja pristupa i međusobnog preuzimanja pozitivnih iskustava i najbolje prakse u primjeni iste palete normi u različitom kontekstu primjene, ali s vrlo sličnim ciljevima primjene, čime će se postići ekonomičnija rješenja za sve obveznike provedbe propisa, a istovremeno osigurati bolje razumijevanje najbolje sigurnosne prakse i sigurnosno znatno učinkovitija rješenja na nacionalnoj razini.

6.2 Tehnička koordinacija u obradi računalnih sigurnosnih incidenata (G)

Tehnička koordinacija je jedna od primarnih funkcija koju je potrebno provesti pri obradi računalnih sigurnosnih incidenata kod kojih je došlo do narušavanja dostupnosti, povjerljivosti ili integriteta podataka, a sa zadaćom ponovne uspostave prijašnjeg stanja. S obzirom na tehničku sofisticiranost današnjih vrsta napada presudna je visoka razina tehničke osposobljenosti zaposlenika CERT[5]-ova,

kao tijela za prevenciju i odgovor na računalne sigurnosne incidente. Nužni uvjet za efikasnost tehničke koordinacije je daljnje unapređenje međusektorske organiziranosti te razmjena i ustupanje informacija o računalnim sigurnosnim incidentima, vodeći pri tome računa o zaštiti osjetljivih podataka (statistika, anonimizacija), a u cilju rješavanja incidenata ili redovitog izvještavanja te kako bi se dobila što jasnija slika o stanju sigurnosti u kibernetičkom prostoru na nacionalnoj razini RH. Nacionalna razina uključuje objedinjavanje statističkih pokazatelja sektora društva preko nadležnih CERT tijela za nacionalnu i sektorske razine. Pri tome moraju

biti jasno definirane usluge i korisnička baza svakog CERT-a, sukladno načelu supsidijarnosti djelovanja, odnosno djelovanja jednog ili više CERT-ova koji su nadležni za komunikacijsku i informacijsku infrastrukturu na kojoj je nastao i rješava se računalni sigurnosni incident. Od posebnog su značaja preventivne aktivnosti kojima se uz mala ulaganja mogu postići veliki učinci i spriječiti značajnije štete.

Tehnička koordinacija ima značajnu ulogu u obradi i saniranju računalnih sigurnosnih incidenata, a u svrhu njezinog unaprjeđenja potrebno je:

Cilj G.1 *Kontinuirano unaprjeđivati postojeće sustave za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te voditi brigu o ažurnosti drugih podataka bitnih za brzu i učinkovitu obradu takvih incidenata.*

Prikupljanje, analiza i pohrana podataka o računalnim sigurnosnim incidentima vrlo je važna za praćenje stanja i trendova u nacionalnom kibernetičkom prostoru. Podaci o računalnim sigurnosnim incidentima prikupljaju se u nadležnim CERT-ovima po načelu supsidijarnosti, a objedinjavaju se i prate po sektorski nadležnim tijelima. Vodeći računa o specifičnostima različitih sektora društva i područja kibernetičke sigurnosti, definirat će se vrste podataka o računalnim sigurnosnim incidentima, načini i preduvjeti razmjene takvih podataka među sektorski nadležnim tijelima. Sektorski nadležna tijela će periodično izvješćivati Nacionalno vijeće za kibernetičku sigurnost[6] o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja. Sektorski nadležna tijela će provoditi odgovarajuće izvješćivanje dionika unutar sektora o računalnim sigurnosnim incidentima. Posebna pažnja će se posvetiti unapređivanju postojećih sustava za prikupljanje, analizu i pohranu podataka o incidentima.

Cilj G.2 *Redovito provoditi mjere za poboljšanje sigurnosti kroz izdavanje upozorenja i preporuka.*

Centralno prikupljene podatke o računalnim sigurnosnim incidentima potrebno je analizirati te razmjenjivati i ustupati nadležnom nezavisnom regulatoru i drugim relevantnim dionicima. Temeljem analiza ovih podataka te podataka prikupljenih na druge načine, tijela nadležna za sigurnost javnih informacijskih sustava i tijela nadležna za sigurnost informacijskih sustava tijela državne uprave poduzimat će mjere za poboljšanje sigurnosti kroz definiranje upozorenja i preporuka.

Cilj G.3 *Uspostava stalne razmjene informacija o računalnim sigurnosnim incidentima te relevantnih podataka i ekspertnih znanja u rješavanju specifičnih slučajeva kibernetičkog kriminaliteta.*

Spoznaje do kojih tijela kaznenog progona i sigurnosno-obavještajnog sustava dolaze prilikom rješavanja slučajeva kibernetičkog kriminaliteta značajno doprinose ukupnoj slici o kibernetičkoj sigurnosti RH, ali i boljoj prevenciji. Stoga je potrebna stalna međusobna razmjena odgovarajućih podataka između tih tijela i nadležnih CERT-ova u opsegu u kojem je to moguće s obzirom na nadležnosti i potrebe pojedinih dionika. Osim razmjene tehničkih podataka, potrebna je suradnja i u području ekspertnih znanja, osobito pri rješavanju složenijih slučajeva kibernetičkog kriminaliteta.

6.3 Međunarodna suradnja (H)

Kibernetički prostor i s njime povezane tehnologije i znanja imaju značajno rastuću ulogu u sveukupnom razvoju društva, uključujući time i političku, sigurnosnu, gospodarsku i socijalnu dimenziju. Iz navedenoga je potpuno razvidno kako je od iznimne važnosti i u ovom prostoru ljudskog djelovanja ostvariti jednaka načela sigurnosti, vladavine prava te jamčenja utvrđenih prava i sloboda svima pojedincima i pravnim subjektima, i to na identičan način kako se oni ostvaruju i izvan kibernetičkog prostora. S obzirom na to da je i u razvoju, proizvodnji i korištenju informacijske i komunikacijske opreme, programa, usluga ili mreža samo-razvidan međunarodni aspekt, također je jasna potreba za koordiniranim djelovanjem, kako na nacionalnoj, tako i na međunarodnoj razini.

Nacionalni interesi, kao i sve potrebne aktivnosti, ostvarivat će se sukladno načelima, vrijednostima i obvezama utemeljenim na Ustavu RH, Povelji Ujedinjenih naroda, međunarodnom pravu i međunarodnom humanitarnom pravu, kao i relevantnom zakonodavnom i strateškom okviru RH i EU te drugim međunarodnim obvezama proisteklim iz članstva u Ujedinjenim narodima, NATO-u, Vijeću Europe, Organizaciji za europsku sigurnost i suradnju te ostalim multilateralnim okvirima i inicijativama.

Prioriteti RH u području kibernetičke sigurnosti na međunarodnom planu uključuju:

Cilj H.1 *Jačanje i širenje međunarodne suradnje na područjima vanjske i sigurnosne politike s partnerskim državama, posebice unutar EU-a i NATO-a, uključujući i zajedničke suradnje s trećim državama.*

Organiziranje međunarodne suradnje različitih dionika kibernetičke sigurnosti s temeljnim ciljem sustavnog pristupa međunarodnoj suradnji. Koordinaciju međunarodne suradnje potrebno je organizirati tako da se uskladi sudjelovanje nacionalno nadležnih tijela na odgovarajućim međunarodnim skupovima s inozemnim partnerskim tijelima sukladnih nadležnosti. Međunarodna suradnja treba biti praćena odgovarajućim izvješćima nadležnih nacionalnih tijela kao nositelja međunarodnih aktivnosti, koja se razmjenjuju i ustupaju drugim odgovarajućim nacionalnim dionicima kibernetičke sigurnosti koja imaju tematski povezane nadležnosti.

Cilj H.2 *Jačanje međunarodnog pravnog okvira, s naglaskom na promicanje i unaprjeđenje provedbe Konvencije Vijeća Europe o kibernetičkom kriminalu i pripadajućim protokolima.*

Potrebno je usko povezati aktivnosti različitih dionika kibernetičke sigurnosti, naročito diplomatskih i pravosudnih nadležnosti, kako bi se osiguralo učinkovito sudjelovanje RH u razvoju međunarodnog pravnog okvira i adekvatno usklađivanje i razvoj nacionalnog pravnog okvira u ovom području.

Cilj H.3 *Nastavak i razvijanje bilateralne i multilateralne suradnje u okviru postojećih i budućih sporazuma s međunarodnim asocijacijama.*

U cilju ispunjenja ugovorenih obveza RH i povećanja nacionalnih sposobnosti provedbe zajedničkih aktivnosti u području kibernetičke sigurnosti nužno je osigurati učinkovit i jasan okvir suradnje tijela dionika kibernetičke sigurnosti u RH s pojedinim međunarodnim partnerima i asocijacijama, prateći pri tome nacionalne nadležnosti tijela koje ostvaruju ovu međunarodnu suradnju.

Cilj H.4 *Promicanje koncepta izgradnje mjera povjerenja u kibernetičkoj sigurnosti.*

Sudjelovanje u diplomatskim aktivnostima u okviru međunarodnih organizacija i drugih foruma radi davanja doprinosa RH aktivnostima usmjerenima na izgradnju povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijskih i komunikacijskih tehnologija.

Cilj H.5 *Sudjelovanje i organizacija međunarodnih civilnih i vojnih vježbi i drugih stručnih programa.*

Kako bi se osiguralo učinkovit razvoj i jačanje sposobnosti koordiniranog nacionalnog i međunarodnog odgovora na prijetnje

kibernetičke sigurnosti, kao i usklađivanje, provjera i unaprjeđenje dostignutog stupnja provedbe zajedničke obrane kibernetičkog prostora, nužno je sudjelovati u međunarodnim vježbama i na stručnim skupovima iz područja kibernetičke sigurnosti te ih i organizirati. Pri tome je potrebno pratiti i koordinirati te aktivnosti s obzirom na nacionalne nadležnosti pojedinih tijela kao dionika kibernetičke sigurnosti RH.

Cilj H.6 *Jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.*

Zakonom o kritičnim infrastrukturama definirane su europske kritične infrastrukture te je propisano njihovo određivanje i zaštita. U skladu s Direktivom Vijeća 2008/114/EC o identifikaciji i određivanju europskih kritičnih infrastruktura i procjeni potrebe za unaprjeđenjem njihove zaštite, države članice dužne su surađivati, razmjenjivati informacije, iskustva i dobru praksu u cilju što bolje i učinkovitije zaštite identificiranih europskih kritičnih infrastruktura.

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

U svrhu izgradnje sigurnog društva te iskorištavanja tržišnog potencijala informacijske sigurnosti i informacijskog društva u cjelini, potrebno je sustavno pristupiti podizanju razine kompetencija cjelokupnog društva u području kibernetičke sigurnosti.

Ciljane skupine na koje je potrebno usmjeriti odgovarajuće edukativne aktivnosti su:

– sudionici formalnog obrazovanja – potrebno je osigurati da učenici osnovnih i srednjih škola te studenti stručnih i sveučilišnih studija ovladaju znanjima o opasnostima na koje mogu naići u virtualnom okruženju te vještinama i kompetencijama kako bi uspješno osigurali vlastito sigurno korištenje informacijskih i komunikacijskih tehnologija kroz sve razine formalnog obrazovanja te svijesti o potrebi zaštite osobnih podataka;

– građani različitih profila – kroz cjeloživotno učenje uključiti sve segmente građanstva u stjecanje znanja o informacijskoj sigurnosti te podizanje svijesti o potrebi zaštite;

– voditelji zbirki osobnih podataka, primatelji osobnih podataka, izvršitelji obrade podataka te sve ostale osobe koje dolaze u dodir s kritičnim nacionalnim infrastrukturama i bazama zaštićenih skupina podataka – osigurati pojačano obrazovanje u području kibernetičke sigurnosti i podizanje svijesti o potrebi zaštite podataka u elektroničkom obliku;

– stručnjaci koji će se baviti informatičkom sigurnošću – razvijati diplomske, poslijediplomske i specijalističke studije u skladu s potrebama tržišta.

Kako bi se postigli ciljevi Strategije, u području obrazovanja, istraživanja, razvoja i jačanja svijesti potrebno je:

1. Sve obrazovne institucije povezati kako bi se programi i kurikulumi poučavanja usustavili te kako ne bi dolazilo do nepotrebnih paralelizma niti izvođenja obrazovnih programa vezanih uz informacijsku sigurnost koji su upitne kvalitete. Potrebno je povezati institucije poput Državne škole za javnu upravu, Policijske akademije, Pravosudne akademije i sl. sa sveučilištima, osobito sa sastavnicama koje imaju uspostavljene i kvalitetne programe s područja informacijske sigurnosti, zaštite osobnih podataka, kibernetičkog kriminaliteta i slično.

2. Podići razinu znanja o informacijskoj sigurnosti svih dijelova društva putem kampanja u koje su uključeni i javni mediji.

3. S obzirom na nedostatno obrazovanje učenika u području kibernetičke sigurnosti, osim u predmetu informatike, implementirati sadržaje vezane uz jačanje svijesti o kibernetičkoj sigurnosti i u ostale nastavne predmete kao međupredmetne sadržaje.

4. U školama na satovima razredne zajednice, roditeljskim sastancima, tematskim predavanjima i ostalim izvanškolskim aktivnostima učenike i roditelje osvješćivati o opasnostima unutar informacijskog društva.

5. U programe za profesionalni razvoj učitelja i nastavnika uključiti i teme kibernetičke sigurnosti.

6. U okviru izobrazbe državnih službenika osigurati teme o kibernetičkoj sigurnosti u okviru posla koji obavljaju.

7. Pružatelje elektroničkih usluga obvezati da se uz proizvod obvezno kupcu pruža i informacija o posljedicama sigurnosnih rizika te mehanizmima zaštite, vezano uz taj proizvod ili uslugu. Obvezati pružatelje usluga na ugrađivanje sigurnosnih mjera te na pružanje informacija o sigurnosnoj problematici i sigurnosnim implikacijama za te usluge ili proizvode, na korisniku razumljiv način.

8. Definirati strateške grane istraživanja na području informacijske sigurnosti (s aspekta defenzivnih i ofenzivnih tehnologija, metoda, algoritama, uređaja, softvera i hardvera). Poticati istraživačke timove i istraživačke projekte u području informacijske sigurnosti prema smjernicama strateški interesantnih istraživačkih i praktičnih područja za RH. Strateški omogućiti da RH ima kapacitete za istraživanje, razvoj, izradu, verifikaciju, sigurnosnu provjeru i ekspertizu iz područja informacijske sigurnosti. Poboljšati komunikaciju između akademskog, gospodarskog i javnog sektora te razmjenu relevantnih informacija vezanih uz informacijsku sigurnost.

Osnovni ciljevi RH vezani uz obrazovanje, istraživanje, razvoj i jačanje svijesti u području kibernetičke sigurnosti su:

Cilj I.1 Razvoj ljudskih potencijala u području sigurnosti komunikacijsko-informacijskih tehnologija.

Potrebno je sustavno obrazovati osobe uključene u provedbu obrazovnih programa (učitelje, nastavnike, ravnatelje, stručne suradnike i druge osobe) o kibernetičkoj sigurnosti. Programe formalnog obrazovanja treba nadopuniti elementima kibernetičke sigurnosti i sustavno ih primjenjivati, naročito u četiri najveće obrazovne skupine, počevši od predškolskog uzrasta, preko osnovnog i srednjeg do visokog školstva. Mladež treba poticati da se bave informacijskom sigurnošću u skladu s pozitivnim propisima. Potrebno je potaknuti izvođenje diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti. Potrebno je planirati i provoditi specijaliziranu izobrazbu državnih službenika, tehničkog osoblja te drugog osoblja koje na različite načine koristi komunikacijske i informacijske tehnologije ili je angažirano na provođenju njezine zaštite odnosno zaštite njezinih korisnika.

Cilj I.2 *Razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.*

Potrebno je uspostaviti mehanizme stalnog upoznavanja korisnika i pružatelja usluga u kibernetičkom prostoru o sigurnom načinu njegova korištenja. Prema široj javnosti treba provoditi prilagođene obrazovne kampanje. Davatelji usluga će, prema uputama sektorskih regulatora, provoditi dodatne aktivnosti kako bi i davatelji i korisnici usluga bili adekvatno zaštićeni.

Cilj I.3 *Razvoj nacionalnih sposobnosti, istraživanje i poticanje gospodarstva.*

Potrebno je potaknuti razvoj nacionalnih sposobnosti po pojedinim područjima informacijske sigurnosti, kako u akademskom sektoru kroz istraživanja, tako i u gospodarskom dijelu kroz razvoj novih proizvoda i usluga. Državna tijela će kroz koordinirani pristup poticati javno-privatno partnerstvo, povezivanje akademskog, državnog i gospodarskog sektora te predstavljanje i promociju rješenja razvijenih u RH na globalnom tržištu.

7. PROVEDBA STRATEGIJE

U svrhu provedbe Strategije izrađen je Akcijski plan za provedbu Strategije kojim se razrađuju definirani strateški ciljevi, odnosno utvrđuju provedbene mjere nužne za ostvarenje tih ciljeva, zajedno s nadležnim tijelima i popisom rokova za njihovu provedbu.

Akcijski plan za provedbu Strategije omogućava sustavan nadzor provedbe Strategije i predstavlja 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.

Kako bi se pravodobno ustanovilo ostvaruje li Strategija željene rezultate, odnosno ostvaruju li se zadani ciljevi i provode li se utvrđene mjere u postavljenim vremenskim okvirima, nužno je uspostaviti sustav kontinuiranog praćenja ostvarivanja Strategije i provedbe Akcijskog plana, kojim će se ujedno uspostaviti mehanizam koordiniranja svih nadležnih državnih tijela u kreiranju odgovarajućih politika i odgovora na prijetnje u kibernetičkom prostoru.

Radi razmatranja i unaprjeđenja provođenja Strategije i Akcijskog plana za njezinu provedbu, Vlada RH će osnovati Nacionalno vijeće za kibernetičku sigurnost (dalje u tekstu: Nacionalno vijeće) 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.

Slijedom potreba opisanih u području upravljanja u kibernetičkim krizama, Nacionalno vijeće će:

– razmatrati pitanja bitna za upravljanje u kibernetičkim krizama i predlagati mjere za veću učinkovitost,

– razmatrati izvješća o stanju sigurnosti koje mu dostavlja Operativno-tehnička koordinacija za kibernetičku sigurnost,

– izrađivati periodične procjene o stanju sigurnosti,

– utvrđivati planove postupanja u kibernetičkim krizama,

– izrađivati programe i planove aktivnosti Operativno-tehničke koordinacije za kibernetičku sigurnost i usmjeravati njezin rad.

Radi osiguranja podrške radu Nacionalnog vijeća, Vlada RH će osnovati Operativno-tehničku koordinaciju za kibernetičku sigurnost koja će:

– 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.

Predstavnici međuresornih tijela u Operativno-tehničkoj koordinaciji za kibernetičku sigurnost osiguravaju međusobno pristup operativnim podacima iz svoje nadležnosti, u svrhu koordiniranog postupanja u kibernetičkim krizama.

Nositelji mjera iz Akcijskog plana za provedbu Strategije odgovorni su za praćenje i prikupljanje podataka o provedbi i učinkovitosti mjera, o čemu su dužni podnositi objedinjena izvješća Nacionalnom vijeću jednom godišnje i to najkasnije do kraja prvog kvartala tekuće godine za prethodnu godinu ili po potrebi i češće, odnosno na zahtjev Nacionalnog vijeća.

Izvješća o provedbi Akcijskog plana za provedbu Strategije Nacionalno vijeće će podnositi Vladi RH najkasnije do kraja drugog kvartala tekuće godine, za prethodnu godinu.

Strategija će se revidirati nakon tri godine primjene, na temelju izvješća nositelja mjera iz Akcijskog plana za provedbu Strategije. Nacionalno vijeće dostavlja Vladi RH objedinjeno izvješće s prijedlogom izmjena i dopuna Strategije najkasnije do kraja godine u kojoj se revizija provodi.

DODATAK: POJMOVI I KRATICE

Pojmovi

Državna informacijska infrastruktura – čine ju zajednička državna osnovica za sigurnu razmjenu podataka i alati za razmjenu podataka kao što su metaregistar, tehničke norme, klasifikacije, javni registri, NIAS, sustav e-Građani te mreže državne informacijske infrastrukture HITRONet i CARNet.

Elektroničke financijske usluge (EFU) – financijske usluge koje njihovi ovlašteni pružatelji izravno pružaju korisnicima, posredstvom elektroničke komunikacijske i informacijske infrastrukture (primjerice internetsko i mobilno bankarstvo, bankomati, EFTPOS sustavi).

Elektronička komunikacijska i informacijska infrastruktura – obuhvaća računalne i komunikacijske sustave i programsku podršku koja služi za prijenos, obradu, pohranu podataka.

Elektroničke komunikacijske i informacijske usluge – profesionalne komercijalne i nekomercijalne usluge koje se realiziraju putem informacijskih i komunikacijskih sustava

Financijske usluge – usluge iz područja bankarstva i platnog prometa, tržišta vrijednosnih papira, udjela u investicijskim fondovima, osiguranja te usluga leasinga i factoringa.

Informacijska sigurnost – stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom odgovarajućih sigurnosnih mjera.

Internet – globalna mreža koja povezuje različite internetske mreže bazirane na TCP/IP protokolu, kao što je primjerice CARNet ili HITRONET.

Izvršitelji obrade zaštićenih podataka – fizičke ili pravne osobe, državna ili druga tijela koja obrađuju zaštićene podatke u ime nositelja odgovornosti za zaštićene podatke.

Kibernetički (računalni) kriminalitet – činjenje kaznenih djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom informacijskih i komunikacijskih tehnologija.

Kibernetička kriza – događaj ili niz događaja u kibernetičkom prostoru, koji bi mogli uzrokovati ili su već prouzročili veći poremećaj u društvenom, političkom i ekonomskom životu RH. Takvo stanje u konačnici može utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti odnosno na nacionalnu sigurnost i obranu države općenito.

Kibernetički prostor – prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća Internet i sve sustave povezane na njega.

Kibernetička sigurnost – obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru.

Kritična komunikacijska i informacijska infrastruktura – komunikacijski i informacijski sustavi čiji bi poremećaj u funkcioniranju bitno poremetio rad pojedine ili više identificiranih nacionalnih kritičnih infrastruktura.

Nositelji odgovornosti za zaštićene podatke – vlasnici zaštićenih podataka i voditelji zbirki zaštićenih podataka.

Obrada zaštićenih podataka – svaka radnja ili skup radnji izvršenih na zaštićenim podacima, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili činjenje podataka na drugi način dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje te provedba logičkih, matematičkih i drugih operacija s tim podacima.

Osjetljivi podaci – skupine podataka koje se koriste samo za službene potrebe ili skupine podataka koje su zaštićene odgovarajućim propisima, a pri tome nemaju svojstvo tajnosti (npr. označeni neklasificirani podaci ili osobni podaci).

Ovlašteni korisnici zaštićenih podataka – korisnici zaštićenih podataka koji svoju ovlast odnosno pravo korištenja temelje na zakonom ili ugovorom utvrđenoj osnovi, a ne predstavljaju nositelje odgovornosti za zaštićene podatke ili izvršitelje obrade zaštićenih podataka.

Podatak – različite skupine elektroničkih zapisa koji imaju vrijednost za korisnike koji s njima postupaju.

Pružatelji elektroničkih financijskih usluga – subjekti koje je nadležno tijelo ovlastilo za pružanje elektroničkih financijskih usluga.

Računalni sigurnosni incident – jedan ili više računalnih sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava.

Sigurnosne mjere – opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

Sustav identifikacije i autentifikacije – sustav kojim se utvrđuje i verificira identitet osoba, uređaja ili usluga na informacijskim sustavima.

Vjerodajnice – skup podataka kojim se predstavlja korisnik elektroničke usluge, a služi kao dokaz za provjeru elektroničkog identiteta (e-ID) kako bi se omogućio pristup elektroničkim uslugama (e-uslugama).

Zaštićeni podaci – podaci koji zbog svog sadržaja imaju osobit značaj za vrijednosti štićene u demokratskom društvu, zbog čega ih država prepoznaje kao osjetljive te ih razvrstava u različite skupine podataka za koje vrijede specifični zahtjevi postupanja u odnosu na svojstva podatka kao što su povjerljivost, cjelovitost, raspoloživost, odnosno privatnost.

Kratice

CARNet	Hrvatska akademska i istraživačka mreža (eng. Croatian Academic and Research Network).
CERT	(Computer Emergency Response Team) Uobičajena kratica za skupinu stručnjaka odgovornih za rješavanje sigurnosnih incidenata na računalnim mrežama. U kontekstu Strategije, kratica CERT se koristi za svaku organizacijsku cjelinu, podcjelinu ili pojedinca odgovornog za koordinaciju, prevenciju i zaštitu od računalnih ugroza sigurnosti informacijskih sustava. Uz kraticu CERT, u međunarodnoj praksi prisutna je i kratica CSIRT (Computer Security Incident Response Team).
Croatian Internet eXchange	Hrvatsko nacionalno središte za razmjenu internetskog prometa udomljeno u Sveučilišnom računskom centru (Srcu), koje je otvoreno za sve davatelje internetskih usluga u RH (za komercijalne i za nekomercijalne, odnosno privatne mreže).

(CIX)	
EFU	Elektroničke financijske usluge.
e-Građani	Sustav e-Građani je dio državnog informacijskog sustava, a čine ga središnji državni portal, nacionalni identifikacijski i autentifikacijski sustav i sustav osobnog korisničkog pretinca.
EU	Europska unija.
e-usluga	Elektronička usluga.
EUROJUST	The European Union's Judicial Cooperation Unit.
EUROPOL	The European Police Office.
EFTPOS sustav	Electronic Fund Transfer Point Of Sale – terminal na prodajnom mjestu namijenjen bezgotovinskom plaćanju pomoću kojeg se transakcije provode elektroničkim putem.
HITRONet	Računalna komunikacijska mreža tijela državne uprave.
HR ISO/IEC 27000	Skup međunarodnih normativnih dokumenata za područje upravljanja informacijskom sigurnošću, prihvaćen kao Hrvatska norma.
NATO	Organizacija Sjevernoatlantskog ugovora.
NIAS	Nacionalni identifikacijski i autentifikacijski sustav.
OIB	Osobni identifikacijski broj.
RH	Republika Hrvatska.
Strategija	Nacionalna strategija kibernetičke sigurnosti.

AKCIJSKI PLAN ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

1. UVOD

Ovim Akcijskim planom razrađuju se ciljevi definirani Nacionalnom strategijom kibernetičke sigurnosti (dalje u tekstu: Strategija) na način da se njime utvrđuju provedbene mjere nužne za ostvarenje tih ciljeva.

Akcijski plan zamišljen je kao živi dokument koji omogućuje sustavan nadzor provedbe Strategije i predstavlja kontrolni mehanizam pomoću kojega će se moći vidjeti je li određena mjera provedena u potpunosti, je li cilj postignut ili je ciljeve i mjere potrebno redefinirati u skladu s novim potrebama.

Akcijskim planom utvrđuju se tijela odgovorna za provedbu predviđenih mjera, u svojstvu nositelja i sunositelja. Sukladno procjeni i potrebama provedbe pojedine mjere, nositelji i sunositelji mogu uključiti i druge sudionike u provedbu mjera iz ovog Akcijskog plana.

Nadzor provedbe nad ovim Akcijskim planom provodit će se putem redovitih i izvanrednih izvješća koja su Nacionalnom vijeću za kibernetičku sigurnost dužni podnositi svi nositelji mjera iz ovog Akcijskog plana, u rokovima utvrđenim Strategijom. Nositelji podnose objedinjena izvješća koje se odnose na sve aktivnosti provedene u okviru mjere, neovisno o tome tko je odgovoran za provedbu pojedine aktivnosti (nositelj, sunositelj, sudionik).

Akcijski plan obuhvaća područja kibernetičke sigurnosti i poveznice područja kibernetičke sigurnosti koje tematski obrađuje i Strategija, kako slijedi:

A. Javne elektroničke komunikacije;

B. Elektronička uprava;

C. Elektroničke financijske usluge.

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama.

E. Kibernetički kriminalitet.

F. Zaštita podataka.

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata.

H. Međunarodna suradnja.

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

2. PODRUČJA I POVEZNICE PODRUČJA KIBERNETIČKE SIGURNOSTI

A. Javne elektroničke komunikacije

Cilj A.1 *Nadzor tehničkih i ustrojstvenih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga, kao i usmjeravanje operatora javnih komunikacijskih mreža i/ili usluga u cilju osiguranja visoke razine sigurnosti i dostupnosti javnih komunikacijskih mreža i usluga.*

Mjera A.1.1 Provoditi nadzor i usmjeravanje operatora javnih komunikacijskih mreža i/ili usluga, kojim će se obuhvatiti različiti zahtjevi koji se postavljaju prema operatorima, od kvalitete i dostupnosti mreža i usluga, preko zahtjeva vezanih za zaštitu osobnih podataka, zahtjeva za osiguravanje primjerene pažnje u provedbi sigurnosnih mjera na temelju odgovarajućih međunarodnih normi, zahtjeva za provedbu zakonskih obveza tajnog nadzora elektroničkih mreža i usluga, ali i potreba razvijanja i stalnog unaprjeđivanja sigurnosne suradnje i razmjene podataka s tijelima nadležnim za računalne sigurnosne incidente u području javnih elektroničkih komunikacija te tijelima kaznenog progona.

Nositelj	HAKOM
Sunositelji	MPPI, AZOP
Početak provedbe	siječanj 2017.
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	Ne
Pokazatelji provedbe	Definiranje načina provedbe nadzora. Broj provedenih nadzora operatora.

Cilj A.2 *Neposredna tehnička koordinacija regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti.*

Mjera A.2.1 Razvijati međusektorsku suradnju nacionalnih regulatornih tijela i tijela odgovornih za područje informacijske sigurnosti i politike zaštite podataka te međusobnu koordinaciju i razmjenu iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira.

Nositelj	HAKOM, Nacionalni CERT, ZSIS, UVNS, SOA, VSOA, OTC
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	Ne
Pokazatelji provedbe	Uspostava mehanizma za razmjenu informacija.

Cilj A.3 *Poticanje korištenja nacionalnog čvora za međusobnu razmjenu internetskog prometa pružatelja javnih komunikacijskih mreža i/ili usluga za davanje usluga korisnicima u RH.*

Mjera A.3.1 Izraditi i objaviti Preporuke za korištenje nacionalnog čvora za međusobnu razmjenu internetskog prometa, s posebnim osvrtom na prednosti njegova korištenje s aspekta sigurnosti razmjene internetskog prometa.

Nositelj	SRCE
Sunositelji	ZSIS, HAKOM
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	Ne
Pokazatelji provedbe	Izrađene i objavljene preporuke.

B. Elektronička uprava

Cilj B.1 *Poticati povezivanje informacijskih sustava tijela javnog sektora međusobno i na javni Internet kroz državnu informacijsku infrastrukturu.*

Mjera B.1.1 Analizirati potrebe i mogućnosti povezivanja na državnu informacijsku infrastrukturu šireg kruga tijela javnog sektora te u skladu s rezultatima analize, izraditi preporuke za povezivanje na državnu informacijsku infrastrukturu ili uvođenje dodatnih mjera zaštite za informacijske sustave onih tijela javnog sektora koja nisu povezana na državnu informacijsku infrastrukturu.	
Nositelj	MU u suradnji s tijelima javnog sektora
Sunositelji	ZSIS, CARNet
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj izrađenih analiza. Izrađene i distribuirane preporuke.
Mjera B.1.2 Analizirati mogućnosti povezivanja državnih tijela klasificiranom mrežom te u skladu s rezultatima analize, izraditi plan povezivanja koristeći državnu informacijsku infrastrukturu. Plan će se provoditi u fazama sukladno prioritetima utvrđenim analizom.	
Nositelj	ZSIS u suradnji s MU
Sunositelji	SOA, UVNS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađena analiza. Izrađen plan povezivanja.

Cilj B.2 *Podići razinu sigurnosti informacijskih sustava javnog sektora.*

Mjera B.2.1 Analizirati postojeće stanje u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora.

Mjera B.2.2 Izrada smjernica za primjenu sustava NIAS i odgovarajućih normi (ISO 27001 i sl.).	
Nositelj	MU u suradnji sa ZSIS-om i CARNet-om
Sunositelji	
Početak provedbe	12 mjeseci po donošenju Strategije
Kraj provedbe	2 godine od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađene i distribuirane smjernice.

Mjera B.2.3 Definirati organizacijske i tehničke zahtjeve za povezivanje na državnu informacijsku infrastrukturu, uvjete i aktivnosti nužne za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostale elemente neophodne za rad državne informacijske infrastrukture.	
Nositelj	MU u suradnji sa ZSIS-om i CARNet-om
Sunositelji	
Početak provedbe	12 mjeseci po donošenju Strategije
Kraj provedbe	2 godine od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Doneseni odgovarajući podzakonski akti.

Mjera B.2.4 Periodična procjena organizacijskih i tehničkih zahtjeva za povezivanje na državnu informacijsku infrastrukturu, uvjeta i aktivnosti nužnih za pokretanje, implementaciju, razvoj i nadzor projekata vezanih uz državnu informacijsku infrastrukturu, način upravljanja, razvoj te ostale elemente neophodne za rad državne informacijske infrastrukture.	
Nositelj	MU u suradnji sa ZSIS-om i CARNet-om
Sunositelji	
Početak provedbe	2 godine po donošenju smjernica iz mjere B.2.3
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrada periodične procjene.

Cilj B.3 *Donošenje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica.*

Mjera B.3.1 Provesti analizu u svrhu donošenja kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica, kojom će se obuhvatiti i kako procjena mogućnosti korištenja buduće elektroničke osobne iskaznice građana za potrebe elektroničke uprave i drugih javnih i financijskih usluga, tako i drugi aspekti povezani s nacionalnim mogućnostima za

uspostavu odgovarajućih akreditacijskih i certifikacijskih sposobnosti u području kvalificiranih elektroničkih potpisa, sukladno EU zahtjevima.

Nositelj	MU u suradnji s MUP-om i MinGo
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci po donošenju Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedena analiza. Doneseni kriteriji za korištenje razina autentifikacije.

Mjera B.3.2 Utvrditi kriterije za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica.

Nositelj	MU u suradnji s MUP-om i MinGo
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci po provedbi mjere B.3.1
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Doneseni kriteriji.

C. Elektroničke financijske usluge

Cilj C.1 *Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, a s ciljem poticanja razvoja elektroničkih financijskih usluga.*

Mjera C.1.1 Objaviti i implementirati Smjernice o sigurnosti internetskih plaćanja. Smjernice o sigurnosti internetskih plaćanja sadrže niz preporuka čije usvajanje i provođenje unaprjeđuje sigurnost plaćanja koja se odvijaju posredstvom Interneta. Navedene smjernice će se na odgovarajući način implementirati u svim kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac koje omogućuju provođenje internetskih plaćanja.

Nositelj	HNB
Sunositelji	–
Početak provedbe	31. ožujka 2015.
Kraj provedbe	Rok za objavu Smjernica o sigurnosti internetskih plaćanja: 1. kolovoza 2015. Rok za procjenu usklađenosti relevantnih institucija (kreditne institucije, institucije za platni promet te institucije za elektronički novac koje omogućuju provođenje internetskih plaćanja) s odredbama Smjernica o sigurnosti internetskih plaćanja: 31. prosinca 2016.
Dodatno financiranje (DA/NE)	NE

Pokazatelji provedbe	Objavljene Smjernice o sigurnosti internetskih plaćanja. Provedena procjena usklađenosti relevantnih institucija s odredbama Smjernica o sigurnosti internetskih plaćanja.

Mjera C.1.2 Objaviti i implementirati Smjernice o sigurnosti mobilnih plaćanja. Smjernice o sigurnosti mobilnih plaćanja sadrže niz preporuka čije usvajanje i provođenje unaprjeđuje sigurnost plaćanja koja se zadaju putem mobilnih telefonskih uređaja. Navedene smjernice će se na odgovarajući način implementirati u svim kreditnim institucijama, institucijama za platni promet te institucijama za elektronički novac koje omogućuju provođenje mobilnih plaćanja.

Nositelj	HNB
Sunositelji	–
Početak provedbe	Ovisno o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europske agencije za bankarstvo (EBA)
Kraj provedbe	Ovisno o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europske agencije za bankarstvo (EBA)
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Objavljene Smjernice o sigurnosti mobilnih plaćanja. Provedena procjena usklađenosti relevantnih institucija (kreditne institucije, institucije za platni promet te institucije za elektronički novac koje omogućuju provođenje internetskih plaćanja) s odredbama Smjernica o sigurnosti mobilnih plaćanja.

Cilj C.2 *Unaprijediti razmjenu i ustupanje podataka o nastalim računalnim sigurnosnim incidentima između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela.*

Mjera C.2.1 Procijeniti zakonske mogućnosti, ograničenja te poželjne mehanizme razmjene informacija o incidentima vezanima uz informacijske sustave kreditnih institucija s relevantnim institucijama u RH.

Nositelj	HNB
Sunositelji	Nacionalni CERT, MUP
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađeno izvješće s procjenom zakonskih mogućnosti, ograničenja te poželjnih mehanizama razmjene informacija o incidentima vezanima uz informacijske sustave kreditnih institucija s relevantnim institucijama u RH.

Mjera C.2.2 Objaviti i implementirati Smjernice za izvješćivanje o incidentima. Smjernice za izvješćivanje o incidentima upućivat će kreditne institucije, institucije za platni promet te institucije za elektronički novac na vrste incidenata koje je potrebno prijavljivati Hrvatskoj narodnoj banci, kao i na informacije koje je potrebno dostaviti.

Nositelj	HNB

Sunositelji	–
Početak provedbe	Ovisno o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europske agencije za bankarstvo (EBA)
Kraj provedbe	Ovisno o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europske agencije za bankarstvo (EBA)
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Objavljene Smjernice za izvješćivanje o incidentima.

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

Cilj D.1 *Utvrditi kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture.*

Mjera D.1.1 Utvrditi kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture.	
Nositelj	ZSIS u suradnji s DUZS
Sunositelji	Središnja tijela državne uprave u suradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor
Početak provedbe	Po donošenju Strategije
Kraj provedbe	6 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Utvrđeni kriteriji za prepoznavanje kritične komunikacijske i informacijske infrastrukture. Donesen/izmijenjen odgovarajući podzakonski akt iz područja kritične infrastrukture, kojim se utvrđeni kriteriji propisuju.

Mjera D.1.2 Analizirati te po potrebi ažurirati kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture.	
Nositelj	ZSIS u suradnji s DUZS
Sunositelji	Središnja tijela državne uprave u suradnji s regulatornim tijelima i strukovnim udruženjima za svaki pojedini sektor
Početak provedbe	2,5 godine po donošenju Strategije
Kraj provedbe	Kontinuirano – svake 2 godine
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedena analiza. Provedena prilagodba propisa prema potrebi.

Cilj D.2 *Utvrditi obvezujuće sigurnosne mjere koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture.*

Mjera D.2.1 Temeljem utvrđenih kriterija za prepoznavanje kritične komunikacijske i informacijske infrastrukture, za svaku pojedinu kritičnu infrastrukturu utvrditi da li postoji kritična komunikacijska i informacijska infrastruktura i koji su zahtjevi prema istoj.	
Nositelj	Središnje tijelo državne uprave nadležno za sektor kritične infrastrukture u suradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor i vlasnikom/upraviteljem kritične infrastrukture u okviru koje je utvrđena kritična komunikacijska i informacijska infrastruktura
Sunositelji	
Početak provedbe	Po donošenju kriterija iz mjere D.1.1
Kraj provedbe	6 mjeseci od donošenja kriterija iz mjere D.1.1
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj vlasnika/upravitelja kritične infrastrukture, po sektorima kritične infrastrukture koji su provjerili postojanje kritične komunikacijske i informacijske infrastrukture i broj utvrđenih kritičnih komunikacijskih i informacijskih infrastruktura u odnosu na broj obrađenih kritičnih infrastruktura.

Mjera D.2.2 Analiza sektorskih zahtjeva prema kritičnim komunikacijskim i informacijskim infrastrukturama.	
Nositelj	Središnje tijelo državne uprave nadležno za sektor kritične infrastrukture u suradnji s regulatornim tijelima i strukovnim udruženjima za svaki pojedini sektor
Sunositelji	ZSIS u suradnji s DUZS
Početak provedbe	6 mjeseci od donošenja kriterija iz mjere D.1.1
Kraj provedbe	9 mjeseci od donošenja kriterija iz mjere D.1.1
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedena analiza

Mjera D.2.3 Definiranje i propisivanje minimalnih standarda za kritične komunikacijske i informacijske infrastrukture u okviru sektora kritične infrastrukture.	
Nositelj	Središnje tijelo državne uprave nadležno za sektor kritične infrastrukture
Sunositelji	ZSIS u suradnji s DUZS
Početak provedbe	Po završetku mjere D.2.2
Kraj provedbe	6 mjeseci po završetku mjere D.2.2
Dodatno financiranje (DA/NE)	NE

Pokazatelji provedbe	Donošenje/izmjena podzakonskog akta iz područja kritičnih infrastruktura, kojim se uređuju minimalni standardi.

Mjera D.2.4 Implementacija propisanih standarda za zaštitu kritične komunikacijske i informacijske infrastrukture.	
Nositelj	Vlasnik/upravitelj kritične infrastrukture u okviru koje je utvrđena kritična komunikacijska i informacijska infrastruktura
Sunositelji	
Početak provedbe	Po završetku mjere D.2.3
Kraj provedbe	12 mjeseci po završetku provedbe mjere D.2.3.
Dodatno financiranje (DA/NE)	DA
Pokazatelji provedbe	Broj vlasnika/upravitelja kritične infrastrukture u okviru koje je utvrđena kritična komunikacijska i informacijska infrastruktura i koji su ispunili propisane minimalne standarde.

Mjera D.2.5 Nadzor provedbe propisanih standarda.	
Nositelj	Središnja tijela državne uprave u čijem su djelokrugu pojedine kritične infrastrukture te nadležna regulatorna tijela
Sunositelji	ZSIS u suradnji s DUZS
Početak provedbe	Po završetku mjere D.2.4
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj vlasnika/upravitelja kritične komunikacijske i informacijske infrastrukture kod kojih je proveden nadzor.

Cilj D.3 *Ojačati prevenciju i zaštitu kroz upravljanje rizikom.*

Mjera D.3.1 Razraditi metodu procjene rizika za kritične komunikacijske i informacijske infrastrukture te je periodično ili prema potrebi ažurirati.	
Nositelj	Središnja tijela državne uprave u suradnji s regulatornim tijelima i strukovnim udruženjima za svaki pojedini sektor kritične infrastrukture
Sunositelji	ZSIS u suradnji s DUZS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE

Pokazatelji provedbe	Razrađena metoda procjene rizika. Donesen/izmijenjen odgovarajući podzakonski akt iz područja kritične infrastrukture, kojim se utvrđuje obveza provedbe.

Mjera D.3.2 Izraditi procjene rizika za kritične komunikacijske i informacijske infrastrukture te ih periodično ažurirati.	
Nositelj	Središnja tijela državne uprave u suradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor kritične infrastrukture
Sunositelji	ZSIS u suradnji s DUZS
Početak provedbe	Po završetku mjere D.3.1
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj izrađenih novih i ažuriranih procjena rizika.

Cilj D.4 *Ojačati javno-privatno partnerstvo i tehničku koordinaciju u obradi računalnih sigurnosnih incidenata.*

Mjera D.4.1 Uspostaviti sustav izvješćivanja u slučajevima računalnih sigurnosnih incidenta po sektorima kritične infrastrukture. U tu svrhu potrebno je utvrditi odgovarajuće postupke razmjene i ustupanja potrebnih sigurnosnih podataka, koordinacije, kao i nadzora provedbe sigurnosnih mjera.	
Nositelj	DUZS, središnja tijela državne uprave u suradnji s regulatornim tijelima i strukovnim udruženjima za svaki pojedini sektor
Sunositelji	Vlasnici/upravitelji kritične infrastrukture u okviru koje je utvrđena kritična komunikacijska i informacijska infrastruktura, tijela kaznenog progona, Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj sektora kritične infrastrukture unutar kojih je uspostavljen sustav izvješćivanja.

Cilj D.5 *Uspostaviti kapacitete za učinkoviti odgovor na prijetnju koja može imati za posljedicu kibernetičku krizu.*

Mjera D.5.1 Provesti analizu kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza kao dijelu nacionalnog sustava upravljanja u krizama.	
Nositelj	Nacionalno vijeće za kibernetičku sigurnost
Sunositelji	Operativno-tehnička koordinacija za kibernetičku sigurnost
Početak provedbe	Po donošenju Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost

Kraj provedbe	6 mjeseci od donošenja Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedena analiza.

Mjera D.5.2 Utvrditi kriterije za definiranje pojma kibernetičke krize u okviru šireg koncepta nacionalnog upravljanja u krizama, kao i kriterije za utvrđivanje/proglašavanje kibernetičke krize.

Nositelj	Nacionalno vijeće za kibernetičku sigurnost
Sunositelji	Operativno-tehnička koordinacija za kibernetičku sigurnost
Početak provedbe	Po donošenju Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost
Kraj provedbe	6 mjeseci od donošenja Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Utvrđeni kriteriji.

Mjera D.5.3 Izrada planova postupanja u kibenetičkim krizama i njihovo kontinuirano ažuriranje.

Nositelj	Nacionalno vijeće za kibernetičku sigurnost
Sunositelji	Operativno-tehnička koordinacija za kibernetičku sigurnost
Početak provedbe	Po donošenju Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost
Kraj provedbe	12 mjeseci od donošenja Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađeni planovi i utvrđen način njihovog ažuriranja.

E. Kibernetički kriminalitet

Cilj E.1 *Kontinuirano unaprjeđivati nacionalni zakonodavni okvir, vodeći pri tome računa o međunarodnim obvezama.*

Mjera E.1.1 Kontinuirano pratiti, analizirati i, po potrebi, prilagođavati nacionalno zakonodavstvo novonastalim promjenama u domeni kibernetičkog kriminaliteta i međunarodnim obvezama s tim u svezi.

Nositelj	MP
Sunositelji	MUP, DORH
Početak provedbe	Po donošenju Strategije

Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj usklađenih propisa.

Cilj E.2 *Unaprjeđivati i poticati međunarodnu suradnju u svrhu učinkovite razmjene informacija.*

Mjera E.2.1 Kontinuirano koristiti raspoložive mogućnosti međunarodne suradnje u svrhu brze razmjene informacija putem već uspostavljenih kontakt točaka, odnosno policijskih i pravosudnih kanala, kao i drugih kanala međunarodnih organizacija.	
Nositelj	MUP
Sunositelji	MVEP, DORH, ZSIS, SOA, Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Evidencija učinka uspostavljenih kontakata i razmjene informacija.

Cilj E.3 *Kvalitetna međuinstitucionalna suradnja u svrhu učinkovite razmjene informacija na nacionalnoj razini, a posebno u slučaju računalnog sigurnosnog incidenta.*

Mjera E.3.1 Uspostava stalnih »kontakt točaka« sa svrhom prevencije i efikasnijeg rješavanja incidenta na nacionalnom nivou.	
Nositelj	MUP
Sunositelji	ZSIS, Nacionalni CERT, SOA, DORH
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj održanih savjetovanja/sastanaka »kontakt točaka«. Evidencija učinka uspostavljenih »kontakt točaka«.

Cilj E.4 *Jačanje ljudskih potencijala, adekvatni razvoj kompetencija i tehničkih mogućnosti nadležnih državnih tijela za otkrivanje, kriminalističko istraživanje i procesiranje kaznenih djela iz domene računalnog kriminaliteta te osiguranje potrebne financijske potpore.*

Mjera E.4.1 Kontinuirano jačanje ljudskih potencijala, odgovarajuća nadogradnja forenzičkih alata i sustava, kao i sustava za tajni nadzor elektroničkih mreža i usluga.	
Nositelj	OTC, MUP
Sunositelji	SOA

Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj novozaposlenih i/ili stručno osposobljenih djelatnika. Količina i vrsta nabavljene opreme. Tehnološka ažurnost raspoložive opreme.

Cilj E.5 *Poticanje i stalni razvoj suradnje s gospodarskim sektorom.*

Mjera E.5.1 Stalni razvoj suradnje s gospodarskim sektorom.	
Nositelj	MUP
Sunositelji	Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj »partnera« iz gospodarskog sektora s kojima je uspostavljena suradnja. Evidencija učinka razmijenjenih podataka o stvarno zabilježenim incidentima.

F. Zaštita podataka

Cilj F.1 *Doraditi nacionalnu regulativu u području poslovne tajne.*

Mjera F.1.1 Doraditi nacionalnu regulativu u području poslovne tajne, te u tu svrhu osnovati radnu skupinu za izradu analize i prijedloga poboljšanih kriterija za utvrđivanje i zaštitu poslovne tajne.	
Nositelj	MinGO
Sunositelji	MZOS, Državni zavod za intelektualno vlasništvo
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Ovisno o rokovima donošenja EU Direktive i obveze preuzimanja u nacionalno pravo.
Dodatno financiranje (DA/NE)	NE.
Pokazatelji provedbe	Osnovana radna skupina. Izrađena analiza i prijedlozi kriterija za utvrđivanje i zaštitu poslovne tajne. Dorađena nacionalna regulativa koja se odnosi na utvrđivanje i zaštitu poslovne tajne.

Cilj F.2 *Poticanje stalne suradnje između tijela nadležnih za posebne skupine zaštićenih podataka u nacionalnom okruženju u svrhu postizanja usklađenosti u provedbi relevantnih propisa.*

Mjera F.2.1 Uspostava 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.	
Nositelj	AZOP, UVNS, MinGO
Sunositelji	–
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Uspostava redovite suradnje i razmjene iskustava. Periodična izrada analiza i preporuka za rješavanje utvrđenih problema odnosno neujednačenosti u primjeni propisa. Provedba preporuka u primjeni.

Cilj F.3 *Određivanje kriterija za prepoznavanje nacionalnih elektroničkih registara koji su kritični informacijski resursi te nositelja odgovornosti za njihovu zaštitu.*

Mjera F.3.1 Izraditi 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 rezultata analize izraditi kriterije po kojima se definiraju nacionalni elektronički registri koji predstavljaju kritične informacijske resurse i nositelje odgovornosti za njihovu zaštitu.	
Nositelj	MU
Sunositelji	AZOP, UVNS, SOA, DUZS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađena analiza postojećeg stanja. Izrađeni kriteriji po kojima se definiraju nacionalni elektronički registri koji predstavljaju kritične informacijske resurse i nositelji odgovornosti za njihovu zaštitu.

Mjera F.3.2 Utvrditi dodatne mjere zaštite za nacionalne elektroničke registre koji predstavljaju kritične informacijske resurse i obveze nositelja odgovornosti za njihovu provedbu.	
Nositelj	MU
Sunositelji	AZOP, UVNS, ZSIS, MF, MUP, MZOS, Ministarstvo zdravlja, HZZO (moguće i druga tijela ovisno o rezultatima mjere F.3.1)
Početak provedbe	Po provedbi mjere F.3.1
Kraj provedbe	12 mjeseci od početka provedbe

Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Utvrđene dodatne mjere zaštite za nacionalne elektroničke registre koji predstavljaju kritične informacijske resurse. Utvrđene obveze nositelja odgovornosti za njihovu provedbu.

Cilj F.4 *Unaprjeđenje postupanja sa zaštićenim podacima kod nositelja odgovornosti za zaštićene podatke, izvršitelja obrade zaštićenih podataka i ovlaštenih korisnika zaštićenih podataka.*

Mjera F.4.1 Izraditi predloške sadržaja dijelova ugovora (prilozi, aneksi, klauzule) 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.

Nositelj	AZOP, UVNS, MinGO
Sunositelji	SOA
Početak provedbe	Po donošenju Strategije
Kraj provedbe	12 mjeseci od donošenja Strategije, osim za poslovnu tajnu gdje je rok ovisan o provedbi mjere F.1.1
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izrađeni predlošci za svaku zaštićenu kategoriju podataka.

Cilj F.5 *Unificiranje pristupa u korištenju palete normi HRN ISO/IEC 27000.*

Mjera F.5.1 Osnovati radnu skupinu 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.

Nositelj	ZSIS
Sunositelji	UVNS, AZOP, HNB, HAKOM
Početak provedbe	Po donošenju Strategije
Kraj provedbe	2 godine od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Osnovana radna skupina. Izrađeni kriteriji. Provedene sektorske analize. Provedena evaluacija i izrađene preporuke.

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata

Cilj G.1 *Kontinuirano unaprjeđivati postojeće sustave za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te voditi brigu o ažurnosti drugih podataka bitnih za brzu i efikasnu obradu takvih incidenata.*

Mjera G.1.1 Definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka.

Nositelj	Nacionalni CERT, ZSIS, HAKOM, HNB
Sunositelji	
Početak provedbe	Po donošenju Strategije.
Kraj provedbe	12 mjeseci od donošenja Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Definirana taksonomija i protokol za razmjenu anonimiziranih podataka o značajnijim incidentima, te uspostavljena platforma ili tehnologija za razmjenu anonimiziranih podataka.

Mjera G.1.2 Sektorski nadležna tijela prikupljaju podatke o incidentima od dionika, poput regulatora i drugih CERT-ova iz njihove sektorske nadležnosti te objedinjavaju na sektorskoj razini. Prethodno anonimizirane podatke o incidentima, sektorski nadležna tijela razmjenjuju koristeći definiranu taksonomiju i protokole (Mjera G.1.1).

Nositelj	Nacionalni CERT, ZSIS, HNB, HAKOM
Sunositelji	
Početak provedbe	Po završetku mjere G.1.1
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Uspostavljeno sektorsko objedinjavanje podataka. Uspostavljena razmjena podataka između sektorski nadležnih tijela sukladno dogovorenoj taksonomiji i protokolu iz mjere G.1.1.

Mjera G.1.3 Izvješćivati dionike unutar sektora o računalnim sigurnosnim incidentima. Periodično izvješćivati Nacionalno vijeće za kibernetičku sigurnost o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja.

Nositelj	HAKOM, HNB, ZSIS, Nacionalni CERT
Sunositelji	
Početak provedbe	6 mjeseci od početka provedbe mjere G.1.2
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Uspostavljena sustavna distribucija periodičkih izvješća i lista institucionalnih primatelja.

Cilj G.2 *Redovito provoditi mjere za poboljšanje sigurnosti kroz izdavanje upozorenja i preporuka.*

Mjera G.2.1 U okvirima svoje nadležnosti, nacionalno nadležni CERT i sektorski nadležna tijela izdavat će upozorenja o uočenim sigurnosnim ugrozama i trendovima te odgovarajuće preporuke za postupanje.

Nositelj	Nacionalni CERT
Sunositelji	ZSIS, HAKOM, HNB
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj izdanih upozorenja i preporuka na nacionalnoj razini i po sektorima.

Cilj G.3 *Uspostava stalne razmjene informacija o računalnim sigurnosnim incidentima te relevantnih podataka i ekspertnih znanja u rješavanju specifičnih slučajeva kibernetičkog kriminaliteta.*

Mjera G.3.1 Održavanje periodičkih (ili po potrebi) koordinacija vezano za razmjenu iskustva i znanja te informacija o sigurnosti kibernetičkog prostora RH do kojih su došla tijela kaznenog progona i sigurnosno-obavještajnog sustava.	
Nositelj	MUP, SOA
Sunositelji	ZSIS, Nacionalni CERT, UVNS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj sastanaka odnosno koordinacija.

H. Međunarodna suradnja

Cilj H.1 *Jačanje i širenje međunarodne suradnje na područjima vanjske i sigurnosne politike s partnerskim državama, posebice unutar EU i NATO-a, uključujući i zajedničke suradnje s trećim državama.*

Mjera H.1.1 Uspostaviti koordinaciju za jačanje i širenje međunarodne suradnje u području kibernetičke sigurnosti.	
Nositelj	MVEP, UVNS
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Uspostava koordinacije. Broj provedenih koordiniranih aktivnosti

Cilj H.2 *Jačanje međunarodnog pravnog okvira, s naglaskom na promicanje i unaprjeđenje provedbe Konvencije Vijeća Europe o kibernetičkom kriminalu i pripadajućim protokolima.*

Mjera H.2.1 Sudjelovanje u i organiziranje međunarodnih aktivnosti na kojima se razvija međunarodni pravni okvir kibernetičke

sigurnosti.	
Nositelj	MVEP u suradnji s MP i MUP-om
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj provedenih aktivnosti

Cilj H.3 *Nastavak i razvijanje bilateralne i multilateralne suradnje u okviru postojećih i budućih sporazuma s međunarodnim asocijacijama.*

Mjera H.3.1 Poticati i potpomagati bilateralnu i multilateralnu suradnju u okviru postojećih i budućih sporazuma s međunarodnim asocijacijama.	
Nositelj	MVEP u suradnji s UVNS
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Praćenje broja i sadržaja bilateralnih i multilateralnih inicijativa.

Cilj H.4 *Promicanje koncepta izgradnje mjera povjerenja u kibernetičkoj sigurnosti.*

Mjera H.4.1 Sudjelovanje u diplomatskim aktivnostima u okviru međunarodnih organizacija i drugih foruma radi davanja doprinosa RH aktivnostima usmjerenima na izgradnju povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija.	
Nositelj	MVEP
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Priprema preliminarnih stajališta RH te evidencija sudjelovanja RH na mogućim međunarodnim skupovima na ovu temu.

Cilj H.5 *Sudjelovanje i organizacija međunarodnih civilnih i vojnih vježbi i drugih stručnih programa.*

Mjera H.5.1 Sudjelovanje i organizacija međunarodnih civilnih i vojnih vježbi i drugih stručnih programa.

Nositelj	MVEP, MORH, MUP
Sunositelji	UVNS, ZSIS, Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj provedenih aktivnosti.

Cilj H.6 *Jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.*

Mjera H.6.1 Jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.	
Nositelj	DUZS
Sunositelji	Središnja tijela državne uprave u suradnji s regulatornim tijelima i strukovnim udruženjima za svaki pojedini sektor kritične infrastrukture
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj provedenih aktivnosti.

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

Cilj I.1 *Razvoj ljudskih potencijala u području sigurnosti komunikacijsko-informacijskih tehnologija.*

Mjera I.1.1 Potrebno je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije u programe ranog i predškolskog odgoja uvrstiti sadržaje vezane uz kibernetičku sigurnost.	
Nositelj	MZOS
Sunositelji	Radna skupina za provođenja kurikularne reforme AZOO/ASOO
Početak provedbe	2015.
Kraj provedbe	2017. – 2018.
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj sadržaja vezanih uz kibernetičku sigurnost.

Mjera I.1.2 Potrebno je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije u osnovnoškolske programe obrazovanja uvrstiti predmetne i međupredmetne sadržaje vezane uz kibernetičku sigurnost.	
Nositelj	MZOS

Sunositelji	Radna skupina za provođenja kurikularne reforme AZOO/ASOO
Početak provedbe	2015.
Kraj provedbe	2017. – 2018.
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj kurikuluma u koje su uvršteni predmetni i međupredmetni sadržaji vezani uz kibernetičku sigurnost.

Mjera I.1.3 Potrebno je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije u srednjoškolske programe obrazovanja uvrstiti predmetne i međupredmetne sadržaje vezane uz kibernetičku sigurnost.

Nositelj	MZOS
Sunositelji	Radna skupina za provođenja kurikularne reforme AZOO/ASOO
Početak provedbe	2015.
Kraj provedbe	2017. – 2018.
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj kurikuluma u koje su uvršteni predmetni i međupredmetni sadržaji vezani uz kibernetičku sigurnost.

Mjera I.1.4 Potrebno je u programe na visokoškolskoj razini uvrstiti sadržaje vezane uz kibernetičku sigurnost.

Nositelj	MZOS
Sunositelji	
Početak provedbe	Po donošenju strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj uvrštenih sadržaja vezanih uz kibernetičku sigurnost.

Mjera I.1.5 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.

Nositelj	MZOS
Sunositelji	AZOO/ASOO, visoka učilišta
Početak provedbe	2016.
Kraj provedbe	Kontinuirano

Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Postotni udio učitelja, nastavnika, ravnatelja i stručnih suradnika te djelatnika visokih učilišta koji su prošli obrazovanje.

Mjera I.1.6 Poticati uspostavljanje i izvođenje diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti.

Nositelj	MZOS
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj uspostavljenih studija te broj polaznika po svakom izvođenom studiju.

Mjera I.1.7 Poticanje uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja.

Nositelj	MZOS
Sunositelji	Akademska zajednica, Udruge
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj financiranih projekata prijavljenih na natječaj MZOS-a za dodjelu bespovratnih sredstava u području izvaninstitucionalnog odgoja i obrazovanja.

Mjera I.1.8 Poticanje organiziranja natjecanja u području informacijske sigurnosti.

Nositelj	AZOO, ASOO
Sunositelji	Škole, Akademska zajednica, udruge
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj natjecanja iz područja informacijske sigurnosti

Mjera I.1.9 Uvrštavati teme informacijske sigurnosti u programe sveučilišta kroz programske ugovore.

Nositelj	MZOS
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj kolegija iz područja informacijske sigurnosti.

Mjera I.1.10 Uspostaviti sustav izobrazbe i provjere znanja iz područja informacijske sigurnosti, koji će se ugraditi u odgovarajuće stručne i državne ispite za državne službenike i namještenike, te koja će se periodično izvoditi za rukovodno osoblje, tehničko osoblje i ostale korisnike informacijskih sustava u tijelima državne uprave.

Nositelj	MU
Sunositelji	UVNS, ZSIS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Revidiran program stručnih i državnih ispita za državne službenike i namještenike. Uspostavljen sustav izobrazbe i provjere znanja za rukovodno osoblje, tehničko osoblje i ostale korisnike informacijskih sustava u tijelima državne uprave. Broj polaznika po vrsti stručnog programa i uspješnost u pratećem testiranju znanja.

Mjera I.1.11 Stalno stručno usavršavanje policijskih službenika u području informacijske sigurnosti i kibernetičkog kriminaliteta koju će provoditi specijalizirana obrazovna akademija i druge ustrojstvene jedinice MUP-a sukladno svojim nadležnostima, a usklađivanje programa provesti u suradnji sa stručno nadležnim tijelima.

Nositelj	MUP
Sunositelji	UVNS, ZSIS, Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Definirani plan načina stjecanja specijalističkih znanja. Broj održanih programa stručnog usavršavanja.

Mjera I.1.12 Stalno stručno usavršavanje državnih odvjetnika i sudaca u području informacijske sigurnosti i kibernetičkog kriminaliteta koju će provoditi specijalizirana obrazovna akademija, a usklađivanje programa provesti u suradnji sa stručno nadležnim tijelima.

Nositelj	Pravosudna akademija
Sunositelji	UVNS, ZSIS, Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	DA – 145.190,00 kuna
Pokazatelji provedbe	Definirani plan načina stjecanja specijalističkih znanja. Broj održanih programa stručnog usavršavanja.

Mjera I.1.13 Za potrebe CERT funkcionalnosti, Nacionalni CERT, ZSIS, MORH CERT definirat će za svoje zaposlenike, na godišnjoj razini, potrebna područja ekspertize te potrebne izobrazbe i načine stjecanja tih znanja. Poticati isti pristup u svim organizacijskim segmentima s CERT funkcionalnošću u drugim tijelima i pravnim osobama.

Nositelj	Nacionalni CERT, ZSIS, MORH CERT
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Definirane godišnje liste potrebnih područja ekspertize i plan izobrazbe ili načina stjecanja specijalističkih znanja.

Mjera I.1.14 Za potrebe CERT funkcionalnosti, realizirati definiranu specijalističku izobrazbu ili samoučenje za određeni broj djelatnika Nacionalnog CERT-a, ZSIS-a, MORH CERT-a, na temelju godišnjih lista potrebnih ekspertiza i izobrazbi. Poticati isti pristup u svim organizacijskim segmentima s CERT funkcionalnošću u drugim tijelima i pravnim osobama.

Nositelj	Nacionalni CERT, ZSIS, MORH CERT
Sunositelji	
Početak provedbe	Po donošenju godišnje liste potrebnih ekspertiza i izobrazbi
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	DA – 205.000,00 kuna
Pokazatelji provedbe	Broj osposobljenih djelatnika za svaku potrebnu ekspertizu.

Cilj I.2 *Razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.*

Mjera I.2.1 Nezavisno regulatorno tijelo za područje javnih elektroničkih komunikacija u RH treba sustavno razvijati program sigurnosnog osvješćivanja i obrazovnih kampanja usmjerenih na najširi krug korisnika postojećih i svih budućih elektroničkih usluga u RH te osigurati ujednačenu provedbu kroz usmjeravanje i obvezivanje različitih operatora i davatelja usluga u RH na provedbu odgovarajućih mjera prema svojim korisnicima.

Nositelj	HAKOM

Sunositelji	Nacionalni CERT
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Izvještaji o provedenim projektima.

Mjera I.2.2 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.

Nositelj	MZOS
Sunositelji	ASOO, AZOO, Akademska zajednica
Početak provedbe	Kontinuirano
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj informativnih sadržaja uključenih u svaku od razina formalne edukacije.

Mjera I.2.3 U okviru problematike davatelja usluga udomljavanja različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi) koje postaju masovno korištene, potrebno je izraditi i publicirati preporuke o minimalnim o sigurnosnim zahtjevima za davatelje i korisnike ovakvih usluga, s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva.

Nositelj	Nacionalni CERT
Sunositelji	HAKOM
Početak provedbe	Po donošenju Strategije
Kraj provedbe	6 mjeseci po donošenju Strategije
Dodatno financiranje (DA/NE)	DA – 70.000,00 kuna
Pokazatelji provedbe	Izrađene i publicirane preporuke.

Mjera I.2.4 Pružatelji e-usluga ostvarit će blisku suradnju s nadležnim tijelima za koordinaciju prevencije i odgovara na ugroze informacijskih sustava. Razmotrit će se potreba prilagodbe zakonskih rješenja kako bi ta suradnja bila brza i efikasna. Izradit će se obrazovni modul o sigurnom korištenju informacijskih sustava te organizirati provedbu obuke zaposlenih u javnom sektoru, kao i korisnika usluga e-Građani (e-learning).

Nositelj	MU i pružatelji usluga elektroničke uprave
Sunositelji	
Početak provedbe	Po donošenju Strategije

Kraj provedbe	12 mjeseci po donošenju Strategije
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Uspostavljena stalna koordinacija između MU i nadležnih tijela. Izrađen obrazovni modul za e-učenje korisnika usluge e-Građanin.

Mjera I.2.5 Kontinuirano informirati kreditne institucije, institucije za platni promet te institucije za elektronički novac o aktualnim i potencijalnim sigurnosnim prijetnjama, kao i odgovornostima vezanima uz njihov djelokrug rada.

Nositelj	HNB
Sunositelji	–
Početak provedbe	31. ožujka 2015.
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedene aktivnosti (korespondencije, održani sastanci, prezentacije, radionice, itd.).

Mjera I.2.6 Osmisliti i provesti usklađene kampanje o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u RH o značaju kibernetičke sigurnosti.

Nositelj	Nacionalni CERT, HAKOM
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedene kampanje ili druge akcije usmjerene prema najširem krugu korisnika Interneta u RH.

Mjera I.2.7 Osmisliti i provesti usklađene kampanje o podizanju svijesti o značaju kibernetičke sigurnosti za državna tijela i pravne osobe s javnim ovlastima.

Nositelj	ZSIS
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Provedene kampanje vezane za korisnike u državnim tijelima i pravnim osobama s javnim ovlastima.

Mjera I.2.8 U slučaju nastanka računalnih sigurnosnih incidenata koji se mogu lako multiplicirati i pogoditi veliki broj korisnika u kibernetičkom prostoru, putem javnih medija pravodobno će obavještavati javnost, vodeći računa o interesima istrage, te davati upute o prevenciji takvih prijetnji radi smanjenja posljedica, odnosno ublažavanja obima već nastalog incidenta.	
Nositelj	MUP u suradnji s Nacionalnim CERT-om i ZSIS-om
Sunositelji	DORH
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Pravodobno informiranje javnosti. Broj obavijesti/provedenih kampanja putem javnih medija.

Cilj I.3 *Razvoj nacionalnih sposobnosti, istraživanje i poticanje gospodarstva.*

Mjera I.3.1 Potrebno je poticati i podupirati znanstvena istraživanja u području informacijske i komunikacijske tehnologije s posebnim naglaskom na informacijskoj sigurnosti i područjima poput kriptologije, identifikacije, metoda napada te metode zaštite sustava.	
Nositelj	MZOS
Sunositelji	Hrvatska zaklada za znanost, Akademska zajednica
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj znanstvenih istraživanja.

Mjera I.3.2 Potaknuti organiziranje redovitih znanstvenih i stručnih skupova te drugih oblika razmjene znanja i iskustva i homogeniziranja stručne zajednice radi bolje interakcije u incidentnim situacijama.	
Nositelj	MZOS
Sunositelji	Znanstvene organizacije i organizacije civilnog društva (organizatori znanstvenih i stručnih skupova), Akademska zajednica
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj prijava na javni poziv MZOS-a za sufinanciranje organizacije stručnih skupova.

Mjera I.3.3 Potrebno je poticati znanstvena istraživanja u području kibernetičke sigurnosti za razvoj novih proizvoda i usluga za tržište, te poticati razvoj tehnološke infrastrukture.

Nositelj	MinGO
Sunositelji	MZOS
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj pokrenutih povezanih sektorskih inicijativa.

Mjera I.3.4 Potrebno je poticati razvoj novih proizvoda i usluga iz područja kibernetičke sigurnosti za unutarnje tržište EU i svjetsko tržište, otvaranjem novih mogućnosti za RH kroz poticanje nacionalne normizacije i organizacije koja može osigurati odgovarajuće akreditirane, certificirane i evaluirane domaće proizvođače i proizvode za svjetsko tržište.

Nositelj	MinGO
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj projekata utemeljenih na primjenama normi čija je provedba podržana odgovarajućom organizacijom sposobnosti državnog sektora i međusektorskom suradnjom.

Mjera I.3.5 Poticanje potencijala RH u području kibernetičke sigurnosti za vlastitu proizvodnju u segmentima u kojima postoje potencijali za proizvode i usluge te gdje bi poticanje primjene domaćih rješenja, naročito kod korisnika državnog proračuna, javnih ustanova i drugih gospodarskih subjekata moglo donijeti određene gospodarske i/ili sigurnosne prednosti.

Nositelj	MinGO
Sunositelji	
Početak provedbe	Po donošenju Strategije
Kraj provedbe	Kontinuirano
Dodatno financiranje (DA/NE)	NE
Pokazatelji provedbe	Broj projekata utemeljenih na primjeni konkurentnih domaćih rješenja za proizvode i usluge prema sektorima primjene.

DODATAK: Kratice

ASOO – Agencija za strukovno obrazovanje i obrazovanje odraslih.

AZOO – Agencija za odgoj i obrazovanje.

AZOP – Agencija za zaštitu osobnih podataka.

CARNet – Hrvatska akademska i istraživačka mreža.

CERT – Computer Emergency Response Team.

DORH – Državno odvjetništvo Republike Hrvatske.

DUZS – Državna uprava za zaštitu i spašavanje.

EU – Europska unija.

HAKOM – Hrvatska regulatorna agencija za mrežne djelatnosti.

HNB – Hrvatska narodna banka.

HRN ISO/IEC – hrvatska norma preuzeta od International Organization for Standardization (ISO) / the International Electrotechnical Commission (IEC)

HZZO – Hrvatski zavod za zdravstveno osiguranje.

MF – Ministarstvo financija.

MinGo – Ministarstvo gospodarstva.

MORH – Ministarstvo obrane.

MP – Ministarstvo pravosuđa.

MPPI – Ministarstvo prometa, pomorstva i infrastrukture.

MU – Ministarstvo uprave.

MUP – Ministarstvo unutarnjih poslova.

MVEP – Ministarstvo vanjskih i europskih poslova.

MZOS – Ministarstvo znanosti obrazovanja i sporta.

NATO – Organizacija sjevernoatlantskog ugovora.

NIAS – Nacionalni identifikacijski i autentifikacijski sustav.

RH – Republika Hrvatska.

SOA – Sigurnosno-obavještajna agencija.

SRCE – Sveučilišni računski centar.

OTC – Operativno-tehnički centar za nadzor telekomunikacija.

UVNS – Ured Vijeća za nacionalnu sigurnost.

VSOA – Vojna sigurnosno-obavještajna agencija.

ZSIS – Zavod za sigurnost informacijskih sustava.

[1] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu (»Narodne novine«, broj 9/02) i Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava (»Narodne novine«, broj 4/08).

[2]https://www.gov.hr/UserDocsImages//e-Gradjani_dok
//NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2

[3] Objavljen u Narodnim novinama, broj 56/13.

[4] 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).

[5]U kontekstu Strategije pojam CERT se odnosi na svaku ustrojstvenu cjelinu (ili podcjelinu do uključujući pojedinca) odgovornu za poslove koordinacije, prevencije i zaštite od računalnih ugroza.

[6]Vidjeti poglavlje 7.