NN 108/2015 (9.10.2015.), Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti

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