Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije

SAŽETAK

Nacionalna strategija kibernetičke sigurnosti je dokument kojim Republika Hrvatska nastoji započeti sustavno i sveobuhvatno planiranje najvažnijih aktivnosti u svrhu zaštite svih korisnika suvremenih elektroničkih usluga, kako u javnom i gospodarskom sektoru, tako i u građanstvu u cjelini. Strategijom se želi postići uravnotežen i koordiniran odgovor niza institucija koje predstavljaju sve sektore društva, na sigurnosne prijetnje u suvremenom kibernetičkom prostoru. Strategija prepoznaje vrijednosti koje je potrebno zaštititi, nadležne institucije i mjere kojima se zaštita sustavno provodi. Strategijom se iskazuje odlučnost dionika kibernetičke sigurnosti za poduzimanje mjera iz svoje nadležnosti, za suradnju s drugim dionicima, razmjenu potrebnih podataka, spremnost na vlastiti razvoj i stalno prilagođavanje, kako bi hrvatski kibernetički prostor bio uređen, dostupan, otvoren i siguran za korištenje.

Strategija i Akcijski plan za njenu provedbu predviđaju pristup kibernetičkom prostoru kao virtualnoj dimenziji društva. Stoga je krajnji cilj izrade Strategije i njene provedbe mjerama razrađenim u Akcijskom planu, sukladan Strategiji kibernetičke sigurnosti Europske Unije[1] i usmjeren punom osposobljavanju i međusobnoj koordinaciji svih sektora našeg društva, a u cilju učinkovite provedbe zakona i zaštite demokratskih vrijednosti u virtualnoj dimenziji današnjeg društva, odnosno kibernetičkom prostoru. Ovakav cilj moguće je postići jedino zajedničkim, učinkovito koordiniranim pristupom čitavog niza različitih, sektorski nadležnih institucija. Razlog tome je što vrlo složeno područje kibernetičke sigurnosti obuhvaća sve segmente društva i široko nadilazi usko tehničku problematiku iz koje je nekoć proizašlo brzim razvojem Interneta i prateće informacijsko-komunikacijske tehnologije.

Stoga je temeljno pitanje kibernetičke sigurnosti prije svega organizacijsko pitanje, koje se u Strategiji rješava boljim i učinkovitijim povezivanjem svih segmenta društva, koristeći pri tome u najvećoj mogućoj mjeri već postojeća tijela i njihove propisane nadležnosti. Prepoznati ciljevi u pojedinim područjima kibernetičke sigurnosti planiraju se provesti mjerama koje su za svaki pojedini cilj Strategije razrađene u Akcijskom planu. Opis mjera koji se daje u Prijedlogu Akcijskog plana za provedbu Strategije, pokazuje kako će se realizacija Strategije najvećim dijelom provesti u okviru postojećih financijskih sredstava tijela koja su nositelji i sunositelji aktivnosti u pojedinim mjerama. Dodatna vrijednost ovih postojećih financijskih sredstava i drugih resursa, ostvaruje se organizacijskim mjerama međusobnog usklađivanja i bolje koordinacije rada više tijela na sličnim aktivnostima, učinkovitijom međusobnom razmjenom podataka, odnosno općenito sinergijom djelovanja različitih institucija i sektora društva koji su do sada u velikoj mjeri bili međusobno nepovezani i slabo koordinirani kada se radi o aktivnostima vezanim za kibernetički prostor.

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN(2013) 1 final

Donošenjem Strategije i Akcijskog plana i uvođenjem sustavnog i sveobuhvatnog pristupa području kibernetičke sigurnosti namjerava se postići niz ciljeva koji su od iznimne važnosti za razvoj društva u cjelini, a napose:

- sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, kibernetička dimenzija društva;
- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora;
- uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru;
- jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora;
- poticanje razvoja usklađenih obrazovnih programa;
- poticanje istraživanja i razvoja, napose u području e-usluga;
- sustavni pristup međunarodnoj suradnji u području kibernetičke sigurnosti.

Metodologija pristupa, odabrana za definiranje sadržaja Strategije, utemeljena je na određivanju općih ciljeva Strategije, sektora društva koji se obuhvaćaju Strategijom, kao i temeljnih načela pristupa provedbi Strategije. Društveni segmenti važni za kibernetičku sigurnost podijeljeni su na područja koja su procijenjena najvažnijim za RH na ovom stupnju razvoja informacijskog društva. Tako su odabrana sljedeća područja kibernetičke sigurnosti:

- elektronička komunikacijska i informacijska infrastruktura i usluge, koja je dalje podijeljena na javne elektroničke komunikacije, elektroničku upravu i elektroničke financijske usluge;
- kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama;
- kibernetički kriminalitet.

Pored područja kibernetičke sigurnosti, Strategija prepoznaje i poveznice područja kibernetičke sigurnosti, čime se osigurava koordinirano planiranje svih zajedničkih aktivnosti i resursa u spomenutim područjima kibernetičke sigurnosti. U tom smislu odabrane su sljedeće poveznice područja kibernetičke sigurnosti:

- zaštita podataka (skupine zaštićenih podataka kao što su klasificirani podaci, osobni podaci, poslovna tajna);
- tehnička koordinacija u obradi računalnih sigurnosnih incidenata;
- međunarodna suradnja;
- obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.

Strategija je utemeljena na postojećim zakonskim rješenjima i odgovornostima, ali prepoznaje potrebu da se neka zakonska rješenja kroz provedbu mjera Akcijskog plana preispitaju i usklade s prepoznatim potrebama virtualne dimenzije društva, koja je već danas postala neizostavni dio i privatnih i poslovnih života te aktivnosti svih građana i institucija. Donošenjem Strategije ne može se odmah riješiti sve probleme nastale i akumulirane tijekom posljednja dva desetljeća brzog razvoja tehnologije i sveopće globalizacije društva, probleme

koji su danas prisutni u svim porama našeg društva. Strategija je svakako početni korak u smjeru sustavnog i trajnog poboljšanja trenutnog stanja u području kibernetičke sigurnosti, a istovremeno predstavlja i početak uvođenja trajne i sustavne brige za sve buduće izazove virtualne dimenzije društva, što je iznimno važno za daljnji razvoj društva.