CRNA GORA
MINISTARSTVO ZA INFORMACIONO DRUŠTVO
I TELEKOMUNIKACIJE

Izvještaj o realizaciji aktivnosti iz akcionog plana za implementaciju Strategije sajber bezbjednosti u Crnoj Gori za period 2013-2015. godine

Podgorica, oktobar 2015. godine

SADRŽAJ

UVOD

Vlada Crne Gore, na sjednici održanoj 12. septembra 2013. godine, razmotrila je i usvojila Strategiju sajber bezbjednosti Crne Gore 2013-2017, sa pratećim Akcionim planom za implementaciju Strategije 2013-2015. godine.

U Strategiji je jasno definisana vizija, strateški ciljevi, institucionalni i pravni okvir, a usvojeni akcioni plan sadrži jasnu podjelu aktivnosti koje treba realizovati.

Prilikom izrade Strategije, korišćene su preporuke vodećih međunarodnih organizacija na polju sajber bezbjednosti (NATO, ENISA). Jedna od ključnih preporuka međunarodnih subjekata je da Strategiju treba razvijati u okviru životnog ciklusa koji treba da sadrži sljedeće faze:

1. Razvoj;

2. Implementacija;

3. Evaluacija;

4. Prilagođavanje Strategije.

Imajući u vidu gore navedene faze, cilj ovog dokumenta je da izvrši evaluaciju Strategije osvrćući se na realizovane aktivnosti iz postojećeg Akcionog plana. Ministarstvo za informaciono društvo i telekomunikacije (MIDT) je pripremilo predmetni Izvještaj na osnovu podataka i informacija dobijenih od strane nosilaca realizacije pojedinih aktivnosti određenih Akcionim planom i to Agencije za nacionalnu bezbjednost, Ministarstva odbrane i Ministarstva unutrašnjih poslova (Uprava policije, Forenzički centar).

U daljem tekstu je predstavljen detaljan pregled trenutne situacije i status realizovanih aktivnosti.

PREGLED AKTIVNOSTI I STATUS REALIZACIJE MJERA UTVRĐENIH AKCIONIM PLANOM 2013-2015

Akcioni plan za implementaciju Strategije sajber bezbjednosti Crne Gore proizilazi direktno iz strateških ciljeva, analize aktuelnog stanja i ciljeva koji se žele postići u pojedinim oblastima.

Nosioci realizacije zadataka iz Akcionog plana su resorna ministarstva, državni organi kao i druge institucije. Namjera je da se kroz koordinirani pristup, uz maksimalno učešće i stručnu podršku Ministarstva za informaciono društvo i telekomunikacije, u razvojnom i implementacionom pogledu, obezbijedi što je moguće veći stepen izvodljivosti navedenih ciljeva.

U nastavku informacije je prikazano stanje aktivnosti koje su predviđene Akcionim planom za period 2013-2015. Svi ciljevi u Akcionom planu detaljno su predstavljeni sa dolje navedenim podacima:

- Zadatak
- Opis mjere
- Odgovorni organ
- Rok za realizaciju mjere
- Status realizacije
- Opis statusa realizacije

Zadatak br. 1: Osnivanje Nacionalnog Savjeta za sajber bezbjednost (informaciona bezbjednost)

- Opis: Članovi Savjeta su predstavnici institucija koje su prepoznate kao ključne u oblasti sajber bezbjednosti. Članove Savjeta će imenovati Vlada Crne Gore na preporuku MIDT. U nadležnosti Savjeta će biti aktivnosti iz domena sajber bezbjednosti i INFOSEC-a.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije
- Rok: Decembar 2013.

- Status: Nije realizovano

Opis statusa realizacije:

Ministarstvo za informaciono društvo i telekomunikacije je, u roku predviđenim Strategijom, pokrenulo proceduru za osnivanje Savjeta. Ključne institucije su odredile svoje predstavnike u Savjetu. Vlada Crne Gore je u tom periodu donijela odluku o smanjenju broja savjetodavnih tijela, pa je shodno tome Ministar za informaciono društvo i telekomunikacije formirao Savjet za informacionu bezbjednost. S obzirom na kadrovske promjene, koje su se odnosile na prestanak radnog odnosa članova Savjeta u institucijama iz kojih su predloženi, a samim tim i prestanak mandata u Savjetu, pokrenute aktivnosti nije bilo moguće realizovati.

Procedura da Vlada Crne Gore formira Savjet za informacionu bezbjednost ponovo je pokrenuta 2015. godine, u skladu sa izmjenama i dopunama Zakona o informacionoj bezbjednosti kojeg je Vlada utvrdila na sjednici od 29.01.2015.godine.

Zadatak br. 2: Formiranje lokalnih CIRT timova u ključnim institucijama za borbu protiv sajber kriminala u cilju uspostavljanja Nacionalne CIRT infrastrukture

- Opis: Svi državni organi i organi uprave, koji vode baze podataka od nacionalnog značaja ili upravljaju dijelom kritične informatičke infrastrukture, u obavezi su da formiraju lokalne CIRT timove.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije
- Rok: Mart 2014.
- Status: Realizovano

Opis statusa realizacije:

U skladu sa zadatkom, MIDT je pokrenuo proceduru za uspostavljanje lokalnih CIRT timova. Obaveza formiranja lokalnih CIRT timova proizilazi i iz Zaključka Vlade broj 06-1293/3 od 14. juna 2012. godine, kojim se zadužuju državni organi, organi državne uprave, organi jedinica lokalne samouprave, pravna lica sa javnim ovlašćenjima i druga pravna i fizička lica koja ostvaruju pristup ili postupaju s podacima da, u saradnji sa Nacionalnim

CIRT-om, formiraju svoje lokalne CIRT timove koji će se baviti uspostavljanjem sistema zaštite od računarskih bezbjednosnih incidenata na Internetu i koji će imati direktnu komunikaciju sa Nacionalnim CIRT timom.

Ministarstvo je pripremilo i Izvještaj o uspostavljanju timova za upravljanje incidentnim situacijama na Internetu u Crnoj Gori - lokalni CIRT timovi, koji je usvojen na sjednici Vlade Crne Gore održanoj 13. marta 2014. godine.

MIDT je kreirao bazu uspostavljenih lokalnih CIRT timova (Tabela 1.) i kontakt osoba, i za sada se u njoj nalazi 28 institucija:

R.br.	Institucija
1.	Agencija za nacionalnu bezbjednost
2.	Agencija za zaštitu konkurencije
3.	Agencija za zaštitu ličnih podataka i slobodan pristup informacijama
4.	Direkcija za zaštitu tajnih podataka
5.	Državna revizorska institucija
6.	Ministarstvo finansija
7.	Ministarstvo kulture
8.	Ministarstvo odbrane
9.	Ministarstvo pravde
10.	Ministarstvo saobraćaja i pomorstva
11.	Opština Berane
12.	Opština Cetinje
13.	Opština Kotor
14.	Opština Pljevlja
15.	Poreska uprava
16.	Sekretarijat za zakonodavstvo
17.	Uprava carina
18.	Uprava policije
19.	Uprava pomorske sigurnosti Bar
20.	Uprava za antikorupcijsku inicijativu
21.	Uprava za javne nabavke
22.	Uprava za nekretnine
23.	Uprava za sprječavanje pranja novca i finansiranja terorizma
24.	Uprava za šume
25.	Uprava za zaštitu kulturnih dobara
26.	Vrhovno državno tužilaštvo
27.	Zavod za hidrometeorologiju i seizmologiju
28.	Zavod za statistiku - Monstat

Tabela 1: Spisak lokalnih CIRT timova

Zadatak br. 3: Definisanje i zaštita kritične informatičke infrastrukture

- Opis: Definisati Metodologiju koja će se koristiti za potrebe identifikovanja kritične informatičke infrastrukture. Neophodno je definisati kritičnu informatičku infrastrukturu u Crnoj Gori i razviti procedure za zaštitu kako bi se osiguralo njeno nesmetano funkcionisanje.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Agencija za nacionalnu bezbjednost
- Rok: Septembar 2014.
- Status: Djelimično realizovano

Opis statusa realizacije:

U skladu sa zadatkom, Ministarstvo za informaciono društvo i telekomunikacije je u predviđenom roku pripremilo Predlog Metodologije izbora kritične informatičke infrastrukture. Predlog Metodologije je potom usaglašen sa svim institucijama prepoznatim kao nosioci kritičnih sektora: Ministarstvo unutrašnjih poslova, Ministarstvo odbrane, Agencija za nacionalnu bezbjednost, Ministarstvo pravde, Ministarstvo finansija, Ministarstvo ekonomije, Ministarstvo zdravlja, Ministarstvo poljoprivrede i ruralnog razvoja i Ministarstvo saobraćaja i pomorstva.

Vlada Crne Gore je, na sjednici održanoj 16. oktobra 2014. godine, usvojila Metodologiju izbora kritične informatičke infrastrukture i Akcioni plan za implementaciju metodologije. Zaključkom br 08-2417/3, Ministarstvo za informaciono društvo i telekomunikacije se zadužuje da koordinira aktivnosti na implementaciji Akcionog plana iz Metodologije.

Akcionim planom su jasno definisani dalji koraci za identifikovanje kritične informatičke infrastrukture u Crnoj Gori. Predviđeno je da kreiranje konačnog spiska kritične informatičke infrastrukture bude završeno do kraja 2015. godine

Zadatak br. 4: Unaprijediti saradnju između državnih organa i organa uprave

- Opis: Obezbijediti preko Nacionalnog Savjeta za sajber bezbjednost, proceduru za razmjenu informacija između državnih organa i organa uprave.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije
- Rok: Maj 2014.
- Status: Djelimično realizovano

Opis statusa realizacije:

S obzirom na to, da formirani Savjet za sajber bezbjednost, zbog kadrovskih promjena, nije radio u punom kapacitetu, što je bio preduslov za izvršenje ovog zadatka, još uvijek nisu izrađene procedure za razmjenu informacija između državnih organa i organa uprave. Ipak, ovaj zadatak je djelimično realizovan kroz uspostavljanje CIRT infrastrukture, tj. formiranje lokalnih CIRT timova. Lokalni CIRT timovi mogu poslužiti kao odličan mehanizam za razmjenu informacija između državnih organa i organa uprave na polju sajber bezbjednosti. Takođe, saradnja i razmjena informacija je dodatno unaprijeđena kroz zajedničko učešće predstavnika državnih organa i organa uprave na obukama, konferencijama i drugim aktivnostima iz ove oblasti.

Nacionalni CIRT ima odličnu saradnju sa ključnim državnim institucijama i nadležnim agencijama koje su prepoznate kao garanti sajber bezbjednosti pa se u određenim slučajevima koordinišu zajedničke aktivnosti. (Uprava policije, Tužilaštvo, nadležne agencije).

Zadatak br. 5: Obezbijediti obuke za zaposlene koji rade na polju sajber bezbjednosti u okviru Nacinalnog CIRT-a i lokalnih CIRT timova

- Opis: Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, neophodno je obezbijediti obuke za stručno usavršavanje kadrova koje rade na rješavanju incidenata
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije
- Rok: Januar - decembar 2014.

- Status: Realizovano

Opis statusa realizacije:

U prethodnom periodu, Ministarstvo za informaciono društvo i telekomunikacije je organizovalo i učestvovalo u brojnim obukama iz oblasti sajber bezbjednosti, kako bi na što efikasniji način odgovorili na incidentne situacije u crnogorskom sajber prostoru.

Organizovane su sljedeće obuke:

1. U organizaciji Međunarodne unije za telekomunikacije (ITU), održana je obuka pod nazivom: „Sajber bezbjednost – regionalni forum“ u Sofiji, Bugarska. Obuci su prisustvovali predstavnici MIDT i Agencije za nacionalnu bezbjednost.

2. U okviru IPA projekta “Strengthening administrative capacity in information society - Montenegro” u prostorijama Ministarstva je održana obuka za državne službenike pod nazivom: “Elementi ICT bezbjednosti”. Obuci su prisustvovali predstavnici sljedećih institucija: Ministarstvo za informaciono društvo i telekomunikacije (CIRT), Ministarstvo odbrane, Ministarstvo pravde, Ministarstvo unutrašnjih poslova (Uprava policije), Ministarstvo vanjskih poslova i evropskih integracija, Agencija za nacionalnu bezbjednost i Direkcija za zaštitu tajnih podataka.

3. Stručnjaci iz IMPACT-a su održali obuku koja je imala za cilj da poboljša odgovor na incidentne situacije, a koja je organizovana za članove CIRT tima, kao i za članove drugih organizacija koja se bave zaštitom od sajber napada na Internetu, kao što su Uprava policije, Agencija za nacionalnu bezbjednost, Ministarstvo unutrašnjih poslova i Ministarstvo odbrane.

4. Kroz donaciju japanske agencije za internacionalnu saradnju (JICA), tri člana Nacionalnog CIRT-a prisustvovala su obuci u Japanu na temu informacione bezbjednosti.

5. U Ankari je organizovana obuka pod nazivom: „Trening za rukovođenje sajber odbranom za sistemske i mrežne administratore“, pod pokroviteljstvom NATO programa za nauku i mir. Pomenutu obuku su pohađali službenici: MIDT, Ministarstva odbrane, Ministarstva pravde, Agencije za nacionalnu bezbjednost, Vojske Crne Gore, Fonda za zdravstveno osiguranje, Direkcije za zaštitu podataka, Univerziteta Crne Gore i Univerziteta Mediteran.

6. Nacionalni CIRT je, u saradnji sa organizacijom JICA iz Japana, organizovao dvodnevnu obuku na temu: “Penetration Testing”. Ovoj obuci su prisustvovali predstavnici iz sljedećih institucija: Agencija za nacionalnu bezbjednost, Ministarstvo odbrane,

Univerzitet Crne Gore, FIT- Mediteran, Poreska uprava i Direkcija za zaštitu tajnih podataka.

Pored navedenih obuka, organizovanih od strane MIDT, Agencija za nacionalnu bezbjednost je stipendirala magistarske studije, smjer sajber bezbjednost na Univerzitetu Donja Gorica, za dvojicu svojih službenika u cilju stvaranja visoko obučenog kadra i eksperata iz oblasti sajber bezbjednosti. Takođe, Agencija je u saradnji sa partnerskim službama organizovala obuke i seminare iz oblasti sajber kriminala i digitalne forenzike za zaposlene koji rade na poslovima sajber bezbjednosti.

Zadatak br. 6: Unaprijediti saradnju između javnog i privatnog sektora

- Opis: Preko Nacionalnog Savjeta za informacionu bezbjednost, obezbijediti procedure za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora, naročito sa: Internet provajderima, agentom za .me domen, bankarskim sektorom, elektroprivredom, kompanijama koje hostuju e-servise servise u Crnoj Gori. U zavisnosti od sprovedene Analize, Savjet će definisati i način saradnje sa drugim subjektima.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Agencija za nacionalnu bezbjednost
- Rok: Jul 2014.
- Status: Nije realizovano

Opis statusa realizacije:

Aktivnosti u okviru ovog zadatka su trebale da se realizuju uz posredstvo Nacionalnog Savjeta za informacionu bezbjednost. S obzirom na poteškoće u radu Savjeta, aktivnosti vezane za obezbjeđivanje procedure za razmjenu informacija između javnog i privatnog sektora, nije bilo moguće realizovati.

Zadatak br. 7: Izvršiti analizu prijetnji u sajber prostoru Crne Gore

- Opis: Zbog konstantnog rasta broja usluga koje državni i privatni sektor pružaju putem interneta, kako građanima tako i drugim pravnim subjektima, moramo težiti ka zaštiti sajber prostora Crne Gore. Prvi korak jeste analiza sajber prijetnji.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Agencija za nacionalnu bezbjednost
- Rok: Decembar 2014.
- Status: Realizovano

Opis statusa realizacije:

U skladu sa zadatkom, Ministarstvo za informaciono društvo i telekomunikacije je u predviđenom roku izradilo Analizu prijetnji u sajber prostoru Crne Gore. Vlada Crne Gore je 18. decembra 2014. godine usvojila Analizu prijetnji u sajber prostoru Crne Gore i zadužila Ministarstvo za informaciono društvo i telekomunikacije da pripremi Smjernice za bezbjednost i zaštitu informacija u sajber prostoru.

Analiza je pokazala da su globalne sajber prijetnje itekako prisutne u Crnoj Gori i da je u budućnosti neophodno posvetiti više pažnje ovoj tematici. U samoj Analizi, dati su savjeti za zaštitu za državne organe i privatni sektor kao i za pojedince kada je u pitanju ponašanje u sajber prostoru.

Takođe u drugom kvartalu 2015.godine, usvojene su Smjernice za bezbjednost i zaštitu informacija u sajber prostoru. Smjernice definišu način na koji treba informacioni sistem učiniti bezbjednim i kako zaštititi njegove tehnološke i informacione vrijednosti koje obezbjeđuju povjerljivost, integritet i raspoloživost informacionog sadržaja, sistema i procesa unutar organizacije.

Zadatak br. 8: Organizovati projekte i kampanje za promovisanje sigurnog korišćenja Interneta sa posebnim fokusom na zaštitu djece na internetu

- Opis: Obezbijediti sigurnije Internet okruženje za stanovnike Crne Gore i osposobljavanje korisnika kroz jačanje svijesti o sigurnom korišćenju Interneta. Posebnu pažnju posvetiti kampanjama i promociji zaštite djece na Internetu.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije
- Rok: Mart 2014.
- Status: Realizovano

Opis statusa realizacije:

U prethodnom periodu, Ministarstvo za informaciono društvo i telekomunikacije, posvetilo je veliku pažnju zaštiti djece na Internetu. U tom pogledu, sprovedene su sljedeće aktivnosti:

1. Ministarstvo za informaciono društvo i telekomunikacije, u saradnji sa institucijom Crnogorskog ombudsmana, u decembru 2014. godine, je otvorilo elektronsku liniju za prijavu nelegalnog sadržaja kojim se ugrožavaju dječja prava. Formular za prijavu se nalazi na web portalu Nacionalnog CIRT-a (www.cirt.me), i omogućava svim crnogorskim građanima, prije svega djeci i roditeljima, da prijave materijal koji predstavlja psihičku ili fizičku zloupotrebu djeteta, njegovog zdravlja i integriteta, zlostavljanje, nedopustivo ponašanje ili drugi vid ugrožavanja dječjih prava.

2. Projekat „Osvoji Internet - Surfuj pametno“, Ministarstvo za informaciono društvo i telekomunikacije realizuje u saradnji sa kompanijom „Telenor“, Ministarstvom prosvjete, Zaštitnikom ljudskih prava i sloboda i Udruženjem „Roditelji“. Projekat je nastao kao potvrda dugoročne zajedničke posvećenosti u oblasti povećanja bezbjednosti i zaštite djece na Internetu, odnosno kreiranja sigurne digitalne sredine za najmlađe korisnike modernih tehnologija u Crnoj Gori. Cilj Projekta je podizanje nivoa društvene svijesti o ovom pitanju i pružanje edukacije i vještina djeci završnih razreda osnovnih škola, njihovim roditeljima i nastavnicima.

   O samom obimu i značaju projekta vršnjačke edukacije govore i statistički podaci. U 2014. godini Projekat je realizovan u 70 osnovnih škola u 20 gradova u Crnoj Gori i njime je, u okviru 400 radionica vršnjačke edukacije, obuhvaćeno oko 9200 učenika završnih razreda. Odabrano je 100 ambasadora sigurnog Interneta koji su svojim

vršnjacima u školama ukazivali na prednosti korišćenja Interneta kroz prizmu zaštite na njemu. Sam Projekat vođen je idejom vršnjačke edukacije, stoga, uloga Ambasadora sigurnog Interneta je presudna.

Zadatak br. 9: Jačanje specijalizovane jedinice za borbu protiv računarskog kriminala u okviru Uprave policije.

- Opis: Kako bi se omogućilo nesmetano procesuiranje djela protiv kompjuterskih podataka i sistema, djela koja se vrše pomoću kompjutera, potrebno je unaprijediti kapacitete specijalizovane jedinice za borbu protiv računarskog kriminala u okviru Uprave policije.
- Odgovorni organ: Ministarstvo unutrašnjih poslova
- Rok: Do kraja 2014.
- Status: Djelimično realizovano

Opis statusa realizacije:

Shodno akcionom planu Ministarstva unutrašnjih poslova, u planu je da se ove godine formira Grupa za borbu protiv visokotehnološkog kriminala a koja će biti pozicionirana u Odsjeku za borbu protiv organizovanog kriminala i korupcije.

U navedenoj grupi planirana su 3 službenička mjesta koji će se baviti problematikom visokotehnološkog kriminala (klasičnim djelima kompjuterskog kriminala, dječijom pornografijom, zloupotrebom brojeva kreditnih kartica i zloupotrebom autorskih prava).

Sa gore formiranom grupom Sektor kriminalističke policije ispunio je planove propisane Strategijom sajber bezbjednosti 2013.-2015. godine.

Zadatak br. 10: Unaprijediti kapacitete za digitalnu forenziku

- Opis: Potrebno je unaprijediti kapacitete Forenzičkog centra u Danilovgradu kako bi se omogućilo adekvatno prikupljanje i analiza elektronskog dokaznog materijala.
- Odgovorni organ: Ministarstvo unutrašnjih poslova

- Rok: Septembar 2015.
- Status: Djelimično realizovano

Opis statusa realizacije:

U Forenzičkom centru Uprave policije u Danilovgradu, od juna 2013. godine sistematizovana je grupa za ispitivanje informacionih tehnologija.

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mjesta sistematizovano je 5 radnih mjesta, i trenutno na tim poslovima upošljen je samo jedan službenik.

Kako proces i obim posla na ovoj liniji rada zahtijevaju popunjavanje upražnjenih radnih mjesta, Ministarstvo unutrašnjih poslova je u nekoliko navrata prema nadležnim Službama uputilo Predlog za popunjavanje radnih mjesta, ali do današnjeg dana isto nije izvršeno.

Kad su u pitanju tehnički kapaciteti, pored uređaja „En Case" za ispitavanje računara, nedavno je izvršena nabavka uređaja za ispitivanje mobilnih telefona, za koje će biti potrebna obuka službenika.

Zadatak br. 11: Jačanje kapaciteta Ministarstva odbrane i Vojske Crne Gore u oblasti sajber odbrane

- Opis: Definisati ulogu Ministartva odbrane i Vojske Crne Gore u sajber prostoru Crne Gore
- Odgovorni organ: Ministarstvo odbrane, Vojska Crne Gore
- Rok: Mart 2015.
- Status: Djelimično realizovano

Opis statusa realizacije:

Strategija sajber bezbjednosti Crne Gore i Akcioni plan koji je proistekao iz ove strategije su inicirali niz aktivnosti u Ministarstvu odbrane (MO) i Vojsci Crne Gore (VCG) ka stvaranju sigurnog informaciono-komunikacionog (IK) okruženja.

U prethodnom periodu u Ministarstvu odbrane otpočeto je sa sistematičnim pristupom u stvaranju povoljnih uslova za razvoj i unaprijeđenje sajber bezbjednosti. U cilju stvaranja stabilne platforme definisane su interne procedure, pravila ponašanja u informaciono-komunikacionom sistemu, potpuna separacija IK mreža (koje su formirane u odnosu na namjenu i nivo tajnosti podataka koji se razmjenjuje u mrežama), elaborat o sajber bezbjednosti, a radi se na stvaranju uslova za obezbjeđenje kontinuiteta funkcionisanja sistema zaštite IK sistema.

U MO su, u skladu sa akcionim planom, sistematizovana radna mjesta koja imaju obavezu komunikacije sa CIRT timovima u ostalim državnim organima i organima uprave i realizacije aktivnosti iz djelokruga CIRT timova.

Po pitanju definisanja uloge MO i VCG u sajber prostoru Crne Gore potrebno je zajedničkim kapacitetima definisati sve polazne parametre, na nacionalnom nivou, kako bi ovaj zadatak bio kvalitetno i u potpunosti realizovan.

Zadatak br. 12: Organizovati konferencije/obuke na temu sajber bezbjednosti

- Opis: Postaviti temelje za organizovanje regionalne konferencije/obuke na temu sajber bezbjednosti na godišnjem nivou. Na ovaj način se poboljšava regionalna saradnja, podiže nivo svijesti, i Crna Gora se promoviše kao jedna od vodećih zemalja u regionu na ovom polju.
- Odgovorni organ: Ministarstvo za informaciono društvo i telekomunikacije, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova
- Rok: Oktobar 2015.
- Status: Realizovano

Opis statusa realizacije:

Ministarstvo za informaciono društvo i telekomunikacije je, u cilju ispunjavanja ovog zadatka, donijelo odluku da se u okviru INFOFEST-a, svake godine organizuje poseban segment koji se bave pitanjem sajber bezbjednosti. INFOFEST je festival informatičkih dostignuća koji se na godišnjem nivou održava u Budvi.

1. U okviru INFOFEST-a 2013. godine organizovana je panel diskusija na temu “Informaciona bezbjednost - stanje i perspektive“. Okruglom stolu je prisustvovao i

u uvodnom dijelu govorio predstavnik CERT-a Slovenije. Na panelu poslije prezentacije CIRT-a razmijenjena su mišljenja i pogledi na razne aspekte ugrožavanja sajber prostora, kao i na načine preventivnog odgovora na polju zaštite kritične informatičke infrastrukture u državi.

2. U okviru INFOFEST-a 2014. godine MIDT je, u saradnji sa Centralnom bankom, organizovao specijalni program - savjetovanje na temu "Savremeni bezbjednosni izazovi u ICT svijetu", koje je bilo podijeljeno u dva bloka. Prvim blokom, pod nazivom: „Sajber bezbjednost u finansijskom sektoru" je moderirao predstavnik Centralne banke, dok je drugim blokom: „Kritična nacionalna informatička infrastruktura" moderirao predstavnik MIDT. Na savjetovanju su učestvovali i predstavnici ključnih međunarodnih institucija na polju sajber bezbjednosti, kao što su ENISA i Međunarodna unija za telekomunikacije (ITU).

3. U okviru INFOFEST-a 2015. godine MIDT je u saradnji sa ITU održao po prvi put na ovim prostorima regionalnu konferenciju i seminar pod nazivom Sajber vježbe (Regional Cyber Drill Exercises). Ovo je prva treća po redu manifestacija ovog tipa koju je ITU organizovao u Evropi, dok se u regionu održao po prvi put u cilju doprinosa daljem razvitku sajber bezbjednosti. Cilj vježbi je bio povećanje razumijevanja država kod postupanja u slučaju sajber-incidenata i testiranje komunikacionih veza i procedura kod pravih sajber-incidenta širokih razmjera. Vježbama su prisustvovali članovi Nacionalnog CIRT tima i lokalnih CIRT timova iz Crne Gore kao i predstavnici iz nekoliko zemalja iz regiona i EU: Srbije, Hrvatske, Bosne i Hercegovine, Bugarske, Litvanije, Rumunije, Slovačke i drugi.

Takođe, CIRT, je ispred Ministarstva za informaciono društvo i telekomunikacije uključen u realizaciju TEMPUS projekta ECESM – „Unapređenje sajber obrazovnog sistema Crne Gore". Projekat je započeo u januaru 2014. godine i trajaće tri godine. Dizajniran je sa ciljem da poboljša opštu poziciju Crne Gore u oblasti sajber bezbjednosti, kroz širenje dostupnosti obrazovanja i specijalističkih obuka kreiranih sa ciljem da poboljšaju opštu poziciju Crne Gore u oblasti sajber bezbjednosti. Osnovni cilj projekta je da se poboljšaju, razviju i implementiraju standardi, smjernice i procedure na nacionalnom nivou u Crnoj Gori, kako bi se omogućilo stvaranje agilnih i visoko obučenih kadrova, sposobnih da odgovore na dinamične i brzo rastuće elektronskeprijetnje. ECESM projekat će obezbijediti opsežne radionice, prezentacije i promocije namijenjene građanima i zaposlenim u širokoj sferi privrede, kao i pojedinačnim akterima, predstavnicima organizacija, itd., u cilju povećanja svijesti o rizicima sajber bezbjednosti i razumijevanja specijalizovanih domena sajber bezbjednosti; specijalizovane obuke za posebne grupe radnika, koje se odnose na spektar njihovih odgovornosti i nadležnosti, počev od državnih i lokalnih uprava, privatnog

sektora, vlasnika/operatera kritične infrastrukture, velikih kompanija, malih preduzeća, akademskih institucija i drugih zainteresovanih strana; akreditaciju master programa, prepoznatog i podržanog od strane relevantnih međunarodnih akademskih institucija, za kontinuiranu edukaciju budućih visoko kvalifikovanih stručnjaka u određenim oblastima sajber bezbednosti, i podsticanje okruženja za dalji istraživački rad u oblasti sajber bezbednosti.

OCJENA STANJA

Sajber bezbjednost i zaštita integriteta sajber prostora Crne Gore predstavlja zajedničku odgovornost i zahtijeva blisku i koordinisanu saradnju svih subjekata, od pojedinca, preko državnih i nedržavnih aktera, mehanizmima nacionalnog sistema bezbjednosti i mehanizmima međunarodne saradnje.

Strategijom sajber bezbjednosti Crne Gore 2013-2017, prepoznato je sedam ključnih ciljeva, čija je realizacija detaljnije definisana kroz pojedinačne zadatke postojećeg Akcionog plana za realizaciju Strategije u periodu od 2013-2015.

Uvidom u status realizacije Akcionog plana za implementaciju Strategije evidentna je intezivna aktivnost nadležnih organa u ispunjavanju zacrtanih strateških ciljeva kojim su, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom. Realizovano je deset aktivnosti, a u toku je realizacija još dvije aktivnosti. Iz navedenog se može zaključiti da postoji visok nivo posvećenosti državnih organa u realizaciji mjera i aktivnosti iz Akcionog plana, i da su ostvareni značajni rezultati.

Dakle, na aktivnosti koje nisu realizovane u predviđenom roku, a prvenstveno se misli na aktivnosti koje bi trebale da se realizuju uz posredstvo Savjeta za informacionu bezbjednost, neophodno je obratiti posebnu pažnju u narednom periodu, kako bi se intezivirale u cilju koordinacije svih aktivnosti na nacionalnom nivou.

S tim u vezi, pripremljen je Predlog zakona, o izmjenama i dopunama Zakona o informacionoj bezbjednosti, koji je Vlada razmotrila u januaru i u kojem je predviđeno formiranje Savjeta za informacionu bezbjednost. Nakon formiranja Savjeta, slijedi izrada novog Akcionog plana i predlog daljih aktivnosti.

U tom pravcu pripremiće se Akcioni plan za naredni period u kojem će se odrediti smjernice dalje reforme, u pravcu:

- Unapređenje nacionalne, regionalne i međunarodne saradnje;
- Jačanja kapaciteta u cilju osavremenjavanja grupe za VTK;
- Jačanja kapaciteta državnog tužilaštva i sudstva u oblasti računarskog kriminala i elektronskog dokaznog materijala;
- Implementacije hardverskih i softverskih rješenja u cilju jačanja otpornosti informacionih sistema državnih organa;
- Jačanje organizacionih i tehničkih kapaciteta Agencije za nacionalnu bezbjednost u oblasti sajber bezbjednosti i drugo.