Crna Gora
Ministarstvo javne uprave

Predlog akcionog plana za implementaciju Strategije sajber bezbjednosti Crne Gore 2018-2021 za 2019. godinu sa Izvještajem o realizaciji Akcionog plana za 2018. godinu

Podgorica, mart 2019. godine

SADRŽAJ

I UVODNI REZIME

Strategija sajber bezbjednosti Crne Gore (u daljem tekstu Strategija) je najviši državni strateški dokument kojim se uređuje sistem sajber bezbjednosti u Crnoj Gori. Vlada Crne Gore (u daljem tekstu Vlada), na sjednici održanoj 21. decembra 2017. godine, donijela je Strategiju koja obuhvata period od 2018. do 2021. godine.

Uredbom Vlade o načinu i postupku izrade, usklađivanja i praćenja sprovođenja strateških dokumenta propisano je da Strategija mora imati izrađen Akcioni plan, koji definiše aktivnosti za sprovođenje strategije ili programa u cilju postizanja utvrđenih strateških i operativnih ciljeva.

U Strategiji je jasno definisana vizija, nacionalna organizaciona struktura, strateški ciljevi, a 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 sledeće faze:

1. Razvoj
2. Implementacija
3. Evaluacija
4. Prilagođavanje Strategije

Akcioni plan definiše aktivnosti za sprovođenje sledećih strateških ciljeva:

1. Kapaciteti za sajber odbranu
2. Centralizacija sajber ekspertize i eksperata
3. Zaštita kritične informatičke infrastrukture
4. Međuinstitucionalna saradnja
5. Zaštita podataka
6. Edukacija u oblasti sajber bezbjednosti
7. Saradnja javnog i privatnog sektora
8. Regionalna i međunarodna saradnja

Navedeni strateški ciljevi predstavljaju kombinaciju bezbjednosnih interesa i odgovora Crne Gore na izazove, rizike i prijetnje definisane u Strategiji, a čija implementacija kroz mjere i aktivnosti u Akcionom planu predstavlja prioritet u periodu na koji se odnosi ovaj dokument, kako bi Strategija bila dosledno implementirana.

Prilikom izrade Akcionog plana za 2019. godinu, obuhvaćene su aktivnosti koje nisu u potpunosti realizovane ili se realizuju u kontinuitetu. Na ovaj način se najefikasnije i dugoročno održivo obezbjeđuje adekvatno upravljanje sajber bezbjednošću u Crnoj Gori.

Predlog akcionog plana pripremio je Radni tim koji čine predstavnici sledećih institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Ministarstvo vanjskih poslova, Agencija za nacionalnu bezbjednost i Direkcija za zaštitu tajnih podataka.

U izvještaju o realizaciji Akcionog plana za 2018. godinu naveden je stepen realizacije aktivnosti za 2018. godinu i na osnovu toga je pripremljen Predlog akcionog plana za 2019. godinu.

AKCIONI PLAN IMPLEMENTACIJU STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE 2018-2021 ZA 2019. GODINU

STRATEŠKI CILJ: 1 **Kapaciteti za sajber odbranu**		**Vlada Crne Gore će nastaviti sa posvećenim radom na daljem jačanju sajber bezbjednosnih kapaciteta u smislu obezbjeđivanja adekvatnih ljudskih i finansijskih resursa, kao i drugih potreba neophodnih za efikasne i agilne sajber kapacitete institucija Crne Gore koje imaju za cilj da obezbijede siguran sajber prostor, omoguće podsticaj biznisa i u krajnjem doprinesu ekonomskom prosperitetu Crne Gore.**				
INDIKATORI UČINKA		***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***			***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.**		31 lokalni CIRT-a	Povećati broj lokalnih CIRT-ova za 30% u odnosu na početnu vrijednost			Povećati broj lokalnih CIRT-ova za 50% u odnosu na početnu vrijednost
Indikator učinka b) **Broj izrađenih analiza rizika u odnosu na broj institucija.**		Nosioci aktivnosti nemaju izrađenu analizu rizika	50% nosioca aktivnosti ima izrađenu analizu rizika			Svi nosioci aktivnosti izradili analizu rizika
Indikator učinka c) **Broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.**			Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 10% u odnosu na početnu vrijednost			Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 20% u odnosu na početnu vrijednost
Indikator učinka d) **Izrađen izvještaj o minimalnom broju službenika za sajber bezbjednost.**		Ne postoji izvještaj	Izrađena analiza sa predlogom aktivnosti			Izrađen izvještaj
Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum završetka**	**Planirana sredstva**	**Izvor finansiranja**

1.1. Uspostavljanje strukture lokalnih CIRT-ova, sa revizijom postojećeg stanja	1. analiza postojećeg stanja 2. formiranje lokalnih CIRT-ova u organmima lokalne samouprave	Ministarstvo javne uprave	I kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.2. Planiranje budžetskih sredstava opredjelinih za sajber bezbjednost u okviru institucije koje su prepoznate kao nosioci	Broj institucija koje su izradile plan budžetskih sredstava opredjeljenih za sajber bezbjednost	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	III kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.3. Jačanje administrativnih kapaciteta institucija zaduženih za sajber bezbjednosti	Izrađena analiza trenutnog stanja sa predlogom sistematizacije	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	II kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.4. Jačanje tehničkih kapaciteta institucija zaduženih za sajber bezbjednosti	1. Implementirani sistemi za zaštitu 2. Nabavljena oprema	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	II kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
1.5. Analiza i audit ICT sistema	1. Formiran tim 2. Prikupljeni podaci 3. Pripremljen izvještaj	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	III kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

1.5. Analiza rizika	1. Formiran tim 2. Prikupljeni podaci 3. Pripremljen izvještaj	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	II kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

STRATEŠKI CILJ: 2 **Centralizacija sajber ekspertize i resursa**	**Vlada Crne Gore će preduzimati aktivnosti na centralizaciji i okupljanju ekspertize u oblasti sajber bezbjednosti kako bi se: ojačali kapaciteti za adekvatan odgovor na sofisticirane sajber prijetnje po kritične infomatičke infra- strukture i druge bitne informacione sisteme; razumjeli rizici po sajber prostor Crne Gore; pružile adekvatne preporuke i unaprijedila sa- radnja sa privatnim i javnim sektorom.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj zaposlenih u Nacionalnom CIRT-u.**	U Nacionalnom CIRT-u zaposleno 4 osobe (sistematizovano 6 mjesta)	14 službenika u NCIRT	20 službenika u NCIRT
Indikator učinka b) **Usvojen pravilnik o unutrašnjoj organizaciji i sistematiza- ciji Ministarstva javne uprave (dva odjeljenja u CIRT).**	Ne postoje odsjeci u okviru Direkcije	Formirana dva odsjeka u okviru Direkcije	
Indikator učinka c) **Broj prostorija koje ispunjavaju minumum tehničkih karakteristika, u odnosu na broj predviđenih**	Ne postoji nijedna prostorija	Jedna specijalizovan prostorija za rad 10 osoba	Dvije specijalizovane prostorije
Indikator učinka d) **Broj organizovanih vježbi i uključenih aktera.**	Jedna vježba	Organizovane 2 vježbe	Organizovane 4 vježbe

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum završetka	Planirana sredstva	Izvor finansiranja
2.1. Jačanje administrativnih kapaciteta CIRT-a	Zaposleno 10 službenika	Ministarstvo javne uprave	II kvartal	IV kvartal	Nisu potrebana dodatna sredstva	Budžet
2.2. Jačanje organizacionih kapaciteta CIRT-a	Sistematizovana dva odsjeka (odgovor na incidente, tehničkog karaktera i odsjek za strateške pravce, politike i preventivu)	Ministarstvo javne uprave	II kvartal	IV kvartal	Nisu potrebana dodatna sredstva	Budžet
2.3. Uspostavljanje Bezbjednosnog operativnog centra (GSOC)	Nabavljena osnovna oprema za uspostavljanje GSOC-a 1. obezbjeđen prostor 40m2 2. 4 TV/monitor 3. 6 računara 4. SIEM rešenje 5. nabavljena oprema za kontrolu pristupa	Ministarstvo javne uprave	II kvartal	IV kvartal	114.900 €	Budžet
STRATEŠKI CILJ: 3 **Zaštita kritične informatičke infrastrukture**	**Vlada Crne Gore će nastaviti da jača kapacite- te za odbranu KII, a s obzirom da noseću ulogu na ovom polju ima nacionalni CIRT - on mora imati adekvatne resurse i alate kako bi na efi- kasan način mogao da razumije, analizira i odgovori na širok spektar prijetnji na ovom polju.** **Resursi državnih organa zaduženih za kontrolu bezbjednosti KII moraju biti adekvatni zadatku, odnosno državni organi moraju imati službenike koji razumiju prijetnje i rizike koji postoje za specifične KII koje pripadaju njihovom sektoru. Ljudski i tehnički resursi moraju biti ojačani u cilju efektivnog obavljanja ove funkcije.**					
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***		***Vrijednosti u poslednjoj godini sprovođenja Strategije***		

Indikator učinka a) **Broj urađenih analiza u odnosu na broj KII, kao i kvalitet istih.**		Nema izrađenih analiza	Svi vlasnici identifikovanih KII imaju izrađene analize rizika			Svi vlasnici identifikovanih KII imaju izrađene analize rizika na godišnjem nivou
Indikator učinka b) **Usvojena Uredba o zaštiti KII.**		Ne postoji uredba	Pripremljen nacrt uredbe			Usvojena uredba o Zaštiti kritične informatičke infrastrukture i njenoj zaštiti
Indikator učinka c) **Broj formalizovanih partnerstava sa nosiocima KII.**		Ne postoje formalizovana strateška partnerstva sa vlasnicima KII	Definisan model za razmjenu informacija i ekspertize			Formalizuje strateška partnerstva sa vlasnicima KII
Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum ravršetka**	**Planirana sredstva**	**Izvor finansiranja**
3.1. Uredba o zaštiti kritične informatičke infrastrukture	1. Pripreljmljen predlog 2. Predlog usvojen	Ministarstvo javne uprave	II kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
3.2.Opremljena specijalizovana prostorija	1. Obezbjeđena prostorija 2. nabavljeno 6 računara 3. nabavljena kotrola pristupa 4. instalirana open source rešenja za monitoring	Ministarstvo javne uprave	II kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
STRATEŠKI CILJ: 4 **Međuinstitucionalna saradnja**		**Prepoznata je potreba za jačanjem međuinstitucionalne saradnje, pri čemu će poseban akcenat biti stavljen na efikasnu i pravovremenu razmjenu informacija i najboljih praksi. U tom kontekstu, nadležne institucije će raditi na snaženju komunikacionih metoda kroz, između ostalog, organizovanje vježbi kriznog komuniciranja u slučaju sajber incidenata i napada većih razmjera. Vježbe će imati za cilj definisanje jasnih procedura komuniciranja u kriznim situacijama, kao i pravovremeno revidiranje istih.**				

INDIKATORI UČINKA	*Polazne vrijednosti*	*Vrijednost na sredini sprovođenja Strategije*	*Vrijednosti u poslednjoj godini sprovođenja Strategije*
Indikator učinka a) **Broj imenovanih kontakt osoba, u odnosu na broj institucija.**	31 kontak osoba	Povećanje broja kontakt osoba za 30% u odnosu na početnu vrijednost	Povećanje broja kontakt osoba za 50% u odnosu na početnu vrijednost
Indikator učinka b) **Aktivan registar sajber eksperata.**	Ne postoji registar	Napravljena tehnička specifikacija	Uspostavljen registar
Indikator učinka c) **Uspostavljena operativna platforma.**	Ne postoji platforma	Pripremljena tehnička specifikacija	Uspostavljena platforma
Indikator učinka d) **Formirana interresorna grupa.**	Ne postoji	Formirana grupa	Usvojen pravilnik o radu
Indikator učinka e) **Broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.**	Jedna vježba	Organizovane 2 vježbe	Organizovane 4 vježbe
Indikator učinka f) **Definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.**	Ne postoji pravilnik	Definisane procedure razmjene informacija o sajber incidentima i komunikacija između organa	Usvojen pravilnik

Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum završetka**	**Planirana sredstva**	**Izvor finansiranja**

4.1. Platforma za razmjenu informacija	Operativna platforma	Ministarstvo javne uprave	III kvartal	IV kvartal	14.000 €	Budžet
4.2. Interresorni operativni tim	Formiran operativni tim	Savjet za informacionu bezbjednost	II kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
4.3. Jačanje međuinstitucionalne saradnje	Održane 3 zajedničke obuke, konferencije, sastanaka…	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Sredstva iz donacija	Nisu potrebna sredstva Donacije
STRATEŠKI CILJ: 5 **Zaštita podataka**		**Vlada Crne Gora će u cilju sprovođenja adekvatne zaštite važnog dijela informatičke infrastrukture jačati nacionalne kapacitete potrebne za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci, kao i kapaciteti u oblasti kripto zaštite.**				
INDIKATORI UČINKA		***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***		***Vrijednosti u poslednjoj godini sprovođenja Strategije***	
Indikator učinka a) **Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.**		Ne postoji pogovarajući pravni akt	Formirana radna grupa i izrađen predlog odgovarajućeg pravnog akta		Usvojen odgovarajući pravni akt	

Indikator učinka b) **Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.**	Dva zaposlena službenika	Zaposlena 3 službenika			Zaposlena 3 službenika
Indikator učinka c) **Broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.**		Prepoznati radna mjesta i predložiti izmjene sistematizacije			Usvojena sistematizacija
Indikator učinka d) **Broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.**	Nema	Jedan sertifikovani sistem			Tri sertifikovana sistema

Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum ravršetka**	**Planirana sredstva**	**Izvor finansiranja**
5.1. Jačanje institucionalnih kapaciteta potrebnih za sertifikaciju informaciono - komunikacionih sistema u kojima se obrađuju tajni podaci	Implementirana jedan novi sistem	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
5.2. Unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za obradu tajnih podataka	Izrađeni odgovarajući pravni akti i prateća dokumenata od strane međuresorne radne grupe	Direkcija za zaštitu tajnih podataka	I kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

5.3. Obuke po pitanju implementacije standarda informacione bezbjednosti (sertifikovani implementator, interni revizor ili eksterni revizor)	Sertifikovano 10 službenika	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
5.4. Donošenje pravnog akta o imenovanju savjetnika za informacionu bezbjednost	Izrada odgovarajućeg pravnog akta Donošenje pravnog osnova za imenovanje lica koja bi bila zadužena za poslove informacione bezbjednosti i predstavljala kontakt tačke u institucijama za akreditaciju informacionih sistema ili implementaciju standarda informacione bezbjednosti.	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	III kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

STRATEŠKI CILJ: 6 **Edukacija u oblasti sajber bezbjednosti**	**Nadležni državni organi u cilju najbolje sajber bezbjednosne prakse će informisati o najnovijim sajber prijetnjama i preduzimati aktivnosti na edukaciji građana i organizacija u pogledu mehanizmima zaštite u sajber prostoru. Potrebni su održivi, kontinuirani i koordinirani napori kako bi se postigle šire promjene ponašanja i kako bi osigurali da sve ciljne grupe, javni i privatni sektor, kao i pojedinačni građanin, razumiju rizike i prijetnje koje postoje u sajber prostoru.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.**		5 konferencija/obuka/gostovanja u emisijama	10 konferencija/obuka/gostovanja u emisijama
Indikator učinka b) **Broj objavljenih sadržaja na portalu CIRT.ME i broj ažuriranih materijala.**	Ažuriranje informacija na mjesečnom nivou	Ažuriranje informacija na portalu na nedeljnom nivou	Ažuriranje informacija na portalu na dnevnom nivou

Indikator učinka c) **Broj obučenih nastavnika po predhodno utvrđenom programu obuke.**	Definasan program obuke	Obučeno 250 nastavnika			Obučeno 500 nastavnika
Indikator učinka e) **Broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.**	Definisan plan aktivnosti	Održane radionice 1.000 učenika			Održane radionice 2.000 učenika

Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum ravršetka**	**Planirana sredstva**	**Izvor finansiranja**
6.1. Edukacija državnih službenika i namještenika na temu sajber bezbjednosti	Edukovano 50 službenika	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije
6.2. Obuke za zaposlene koji rade na polju sajber bezbjednost u okviru Nacionalnog CIRT-a i lokalnih CIRT-ova	Obezbjediti 10 obuka	Ministarstvo javne uprave	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije

6.3. Podizanje svijesti građana o bezbjednom korišćenju interneta	1. Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa 2. Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe 3. Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti	Ministarstvo jvne uprave Ministarstvo prosvjete	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet / Donacije
6.4. Unapređenje informacionog sistema u obrazovanju	Nadograđen modul za pedagoško-psihološke službe u Informacionom sistemu obrazovanja (MEIS) u cilju evidencije sajber nasilja kod djece školskog uzrasta i implementacija u svim osnovnim i srednjim školama	Ministarstvo prosvjete	II kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet / Donacije
STRATEŠKI CILJ: 7 **Saradnja javnog i privatnog sektora**	**Vlada Crne Gore će i u narednom periodu nastaviti sa posvećenim radom u cilju podrške, kako u odgovoru na incidente, tako i u dijeljenju informacija i zajedničke inicijative u partnerstvu sa privatnim sektorom. Dakle, jedino visok stepen komunikacije, saradnje i integracije može biti efikasan način da se razumije i na pravi način odgovori na potrebe i izazove privatnih kompanija, a u cilju preduzimanja neophodnih mjera kako bi se postigao dovoljan stepen bezbjednosti.**					
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***			***Vrijednosti u poslednjoj godini sprovođenja Strategije***	
Indikator učinka b) **Definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.**	Ne postoji pravilnik	Definsane procedure			Usvojen pravilnik	
Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum završetka**	**Planirana sredstva**	**Izvor finansiranja**

71. Unapređenje saradnje sa privatnim sektorom i akademskom zajednicom	Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom, Broj zajedničkih učešća na događajima u oblasti sajber bezbjednosti	Savjet za informacionu bezbjednost Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebana dodatna sredstva	Budžet/Donacije
STRATEŠKI CILJ: 8 **Regionalna i međunarodna saradnja**		**Vlada Crne Gore će nastaviti sa regionalnim i međunarodnim aktivnostima i vršiti svoj uticaj ulaganjem u partnerstva koja oblikuju globalnu evoluciju sajber prostora na način koji unaprjeđuje i širi ekonomske i bezbjednosne interese i poboljšava kolektivnu bezbjednost.**				
INDIKATORI UČINKA		***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***			***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih obuka, konferencija, seminara, vježbi, sastanaka i biće kvalitativnog karaktera.**		Jedna vježba na godišnjem nivou	Tri održane obuke/konferencije/seminara/vježbi/sastanaka			Šest održanih obuka/konferencija/seminara/vježbi/sastanaka
Indikator učinka b) **Broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.**		Ne postoji nijedan	Jedan memorandum			Dva memoranduma
Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum završetka**	**Planirana sredstva**	**Izvor finansiranja**

8.1. Unapređenje saradnje sa međunarodnim organizacijama i CERT/CIRT-ovima na regionalnom i međunarodnom nivou	Učestvovanje/organizacija tri konferencije, radionice, okrugla stola…	Savjet za informacionu bezbjednost Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije

REALIZACIJA MJERA IZ AKCIONOG PLANA 2018. GODINE PREMA STRATEŠKIM CILJEVIMA

Akcioni plan sadrži 8 ciljeva i 15 aktivnosti i mjera. Realizovano je jedanaest aktivnosti, u toku je realizacija još tri aktivnosti, dok jedna aktivnost nije realizovana. Mjere iz Akcionog plana su realizovane samostalno ili u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti.

1. KAPACITETI ZA SAJBER ODBRANU

1.1. Uspostavljanje strukture lokalnih CIRT timova

- Podaktivnost: Uspostavljanje lokalnih CIRT timova / određivanje kontakt osoba
- Nadležna institucija: Ministarstvo javne uprave
- Rok: Kontinuirano
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj uspostavljenih lokalnih CIRT timova u odnosu na trenutno stanje; sačinjena lista kontakt osoba
- Status realizacije: Realizovano

U skladu sa aktivnostima Ministarstvo javne uprave je pokrenulo proceduru za uspostavljanje lokalnih CIRT timova. Obaveza formiranja lokalnih CIRT timova u institucijama jeste u cilju uspostavljanja sistema zaštite od računarskih bezbjednosnih incidenata na internetu i koji će imati direktnu komunikaciju sa Nacionalnim CIRT-om.

Ministarstvo javne uprave pripremilo je i Izvještaj o uspostavljanju timova za upravljanje incidentnim situacijama na internet u Crnoj Gori – lokalni CIRT timovi, koji je Vlada Crne Gore usvojila na sjednici održanoj 27. decembra 2018. godine.

Od ukupno formirana 63 lokalna tima koja sarađuju sa članovima Nacionalnog CIRT-a vezano za pitanja zaštite od računarskih bezbjednosnih incidenata na internetu, 32 lokalna tima su formirana u 2018. godini što je povećanje za preko 100%.

1.2. Planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost u okviru institucija koje su prepoznati kao nosioci

- Podaktivnost: Za efikasno funkcionisanje u okviru institucija koje su prepoznate kao nosioci sajber bezbjednosti moraju postojati opredijeljena budžetska sredstva za sajber bezbjednost
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: III kvartal
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj institucija koje su izradile plan budžetskih sredstava opredijeljenih za sajber bezbjednost
- Status realizacije: Realizovano

Ministarstvo javne uprave je tokom 2018. godine obezbijedilo sredstva za produžetak licenci postojećih bezbjednosnih uređaja kao i za nabavku novih. Planom za 2019. godinu takođe su predviđena određena sredstva.

Ministarstvo odbrane je tokom 2018. godine obezbijedilo 100 000,00€ za potrebe jačanja sajber kapaciteta. Planom za 2019. godinu, takođe je predviđeno izdvajanje sredstava u iznosu od minimum 75 000,00€.

Ministarstvo vanjskih poslova je u izvještajnom periodu za unapređenje sajber bezbjednosti izdvojilo budžetska sredstva u iznosu od 50 501,00€. Sredstva su bila planirana u okviru redovnih sredstava Ministarstva vanjskih poslova.

Ministarstvo pravde je planom budžetskih sredstava za 2019. godinu planiralo određena sredstva za sajber bezbjednost. Planirana je nabavka određenog broja bezbjednosnih uređaja.

Planom rada Direkcije za zaštitu tajnih podataka za 2019. godinu predviđena je realizacija projekta nadogradnje postojećeg informacionog sistema za razmjenu domaćih podataka sa stepena tajnosti POVJERLJIVO na stepen TAJNO. U okviru projekta, planirano je da Direkcija za zaštitu tajnih podataka unaprijedi dio opreme i softver na centralnoj lokaciji u zgradi Direkcije za zaštitu tajnih podataka /Ministarstva odbrane. Shodno tome, u budžetu Direkcije za zaštitu tajnih podataka za 2019. godinu predviđena su sredstva u iznosu od 50 000,00€ za realizaciju ovog projekta. Planirana su i sredstva za obuke i posjete važnim događajima iz oblasti sajber bezbjednosti koje su u nadležnosti Direkcije za zaštitu tajnih podataka (NDA konferencija, BSAB sastanak).

Takođe, i Agencija za nacionalnu bezbjednost izvršila je planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost.

1.3. Jačanje administrativnih kapaciteta zaduženih za sajber bezbjednost

- Podaktivnost: Analiza trenutnog stanja i procjena optimalnog broja službenika zaduženih za sajber bezbjednost
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: III kvartal
- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Izrađena analiza trenutnog stanja
- Status realizacije: Realizovano

U Ministarstvu javne uprave je izvršena analiza trenutnog stanja i procjena optimalnog broja službenika zaduženih za sajber bezbjednost i dostavljen je predlog nove organizacione strukture.

Ministarstvo odbrane je u skladu sa ciljevima iz Strategije i partnerskim ciljevima izradilo predlog izmjene organizacione strukture u okvirima Ministarstva odbrane i Vojske Crne Gore, kao i minimalan broj zaposlenih koji bi obezbijedili bazične kapacitete za sajber odbranu.

Ministarstvo vanjskih poslova dodatno je ojačalo administrativne kapacitete za sajber odbranu, na način da je tokom 2018. godine zaposlena još jedna osoba u Odjeljenju za upravljanje informacionim sistemima kao organizacionoj jedinici zaduženoj za pitanja bezbjednosti.

Analiza trenutnog stanja u Ministarstvu pravde pokazuje da trenutno u ministarstvu rade dva službenika/načelnika koji su pored osnovnih nadležnosti uključeni u oblast sajber bezbjednosti načelnik Direkcije za informacioni sistem pravosuđa, koji je i član Savjeta za informacionu bezbjednost i načelnik Direkcije za informatičku infrastrukturu i bezbjednost podataka se između ostalog bavi i informatičkom bezbjednošću, što je predvidjeno opisom radnog mjesta koje pokriva. Procjena Ministarstva pravde je da je na nivou Direktorata za IKT pravosuđa potreban jedan službenik za sajber bezbjednost, koji bi bio kontakt osoba u slučaju incidenata sa Nacionalnim CIRT-om. U budućem periodu planirano je formiranje pravosudnog CIRT tima, kao odgovor na računarske incidente u okviru pravosudnih institucija Crne Gore. Ovaj tim bi trebao da bude zadužen za preventivno i korektivno djelovanje, radi zaštite fizičkih i logičkih komponenti informaciono komunikacionog sistema pravosuđa Crne Gore.

Direkcija za zaštitu tajnih podataka je izvršila procjenu trenutnog stanja i optimalnog broja službenika prilikom izrade Pravilnika o unutrašnjoj organizaciji i sistematizaciji i predvidjela novo radno mjesto u Odjeljenju

za informatičku zaštitu tajnih podataka. Ovo radno mjesto je i popunjeno u aprilu 2018.godine u skladu sa aktivnošću broj 5.2. ovog Akcionog plana.

Agencija za nacionalnu bezbjednost ulaže značajne napore u cilju stvaranja administrativnih kapaciteta za borbu protiv sajber kriminala i špijunaže, koji uz terorizam i organizovani kriminal, postaje najveći bezbjednosni izazov današnjice. Iz navedenih razloga, potrebno je i dalje jačanje administrativnih kapaciteta Agencije u oblasti sajber bezbjednosti, uključujući i kapacitete za digitalnu forenziku. Izrađena je analiza trenutnog stanja i izvršena procjena optimalnog broja službenika zaduženih za sajber bezbjednost. Ovaj proces će se i dalje obavljati kontinuirano.

1.4. Jačanje tehničkih kapaciteta institucija zaduženih za sajber bezbjednost

- Podaktivnost: Analiza trenutnih i planiranih tehničkih kapaciteta; Nabavka opreme
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: IV kvartal
- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Izrađena analiza trenutnih i planiranih tehničkih kapaciteta i nabavka opreme
- Status realizacije: Realizovano

Ministarstvo javne uprave je sprovelo aktivnosti u cilju jačanja bezbjednosnog okvira, odnosno sajber zaštite, za informacione sisteme i mrežu organa državne uprave. Nabavljene su licence za postojeće bezbjednosne uređaje kao i nabavka novih uređaja. U Zgradi Vlade Crne Gore tokom 2018 godine, realizovana je zamjena komunikacione opreme u cilju bolje konekcije i unapređenja nivoa bezbjednosti lokalne mreže. Uspostavljena je kontrola i ograničenje pristupa, antivirusna kontrola, smanjena mogućnost penetracije sistema, detektovanje malicioznih aktivnosti i sprečavanje istih, prevencija pristupa malicioznim sajtovima i druge bezbjednosne kontrole.

Ministarstvo odbrane i Vojska Crne Gore su sagledali potrebe i napravili procjenu troškova nabavke opreme za uspostavljanje Bezbjednosnog Operativnog Centra (SOC), koji će biti centralna tačka za nadzor sistema Ministarstva odbrane i Vojske Crne Gore, prevenciju prijetnji, upravljanje incidentima i analizu. U skladu sa tim, izvršena je nabavka uređaja za prevenciju prijetnji i nadzor mrežnog saobraćaja i opredijeljena su dodatna sredstva za opremanje SOC-a.

Ministarstvo vanjskih poslova je za potrebe Generalnog direktorata za NATO i politiku bezbjednosti nabavilo TEMPEST računarsku opremu za potrebe NATO sistema razmjene tajnih podataka, kao i interne offline mreže u Generalnom direktoratu, čime su ispunjeni tehnički uslovi za rad sa tajnim podacima i zamijenjena kompletna računarska oprema.

U cilju jačanja otpornosti informacionih sistema na potencijalne incidente, Direktorat za IKT u Ministarstvu pravde je u 2018. godini sproveo sledeće redovne aktivnosti, koje u velikoj mjeri smanjuju ranjivost postojećih sistema ministarstva, u sajber prostoru: izvršen je update firewall-a Fortigate i kupljene su licence za tekuću godinu za sve lokacije Ministarstva pravde; web aplikativni firewall je update-ovan u okviru nabavke pomenutih licenci; izvršeno je tjuniranje pravila na Database Activity Monitoring(DAM) sistemu, shodno novim verzijama aplikacija koje su postavljene. Ministarstvo pravde kontinuirano vrši ažuriranje svih operativnih sistema, antivirusnih softvera, pravila na mrežnim uređajima i sl.

Direkcija za zaštitu tajnih podataka je izvršila procjenu trenutnog stanja tehničkih kapaciteta i predvidjela nabavku neophodne opreme za 2019.godinu. Imajući u vidu da je predviđena realizacija projekta nadogradnje postojećeg informacionog sistema za razmjenu domaćih podataka sa stepena tajnosti POVJERLJIVO na stepen TAJNO, planirano je da Direkcija za zaštitu tajnih podataka unaprijedi dio opreme i softver na centralnoj lokaciji u zgradi Direkcije za zaštitu tajnih podataka/Ministarstva odbrane. Tokom 2019.godine planirana je nabavka opreme koja je neophodna za realizaciju ovog projekta. Takođe, tokom

2018.godine izvršena je nabavka novih radnih stanica za potrebe informacionog sistema za razmjenu tajnih podataka sa NATO.

U prethodnom periodu Agencija za nacionalnu bezbjednost intenzivno je radila na jačanju tehničkih kapaciteta u oblasti sajber bezbjednosti. Urađena je analiza trenutnog stanja i izvršena procjena nabavke novih tehničkih sredstava predviđenih za sajber bezbjednost. Ovaj proces će se i dalje obavljati kontinuirano. Agencija za nacionalnu bezbjednost kontinuirano radi na nabavci i implementiranju novih hardverskih i softverskih rješenja u cilju jačanja otpornosti i zaštite informacionih sistema koje koristi. Odabir opreme i softvera vrši se u skladu sa propisima koji propisuju oblast tajnih podataka kao i u skladu sa setom standarda ISO 27001.

2. CENTRALIZACIJA SAJBER EKSPERTIZE I RESURSA

2.1. Jačanje administrativnih kapaciteta CIRT-a

- Podaktivnost: Povećanje broja službenika CIRT-a kroz izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane
- Rok: IV kvartal
- Procjena troškova: Budžet nadležnih institucija
- Indikator uspjeha: Osam sistematizovanih radnih mjesta u MJU CIRT-u do kraja 2018. godine; 5 sistematizovanih radnih mjesta u MOD CIRT-u
- Status realizacije: Realizovano

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (u okviru koje je i Nacionalni CIRT) sistematizovano je 8 radnih mjesta od kojih je popunjeno 5. Takođe, u Ministarstvu odbrane, formiran je Odsjek za sajber bezbjednost i odgovore na kompjuterske incidente CD/CIRT, u kojem je predviđeno da bude 5 zaposlenih. Takođe, Vojska Crne Gore je u okviru organizacijsko formacijske strukture (OFS) planirala 2 pozicije u okviru Odjeljenja za komunikaciono informacione sisteme G-6 i 4 pozicije u okviru Čete za vezu i elektronsko ratovanje. Usvajanje OFS se očekuje do kraja I kvartala 2019. godine.

2.2. Jačanje organizacionih kapaciteta CIRT-a

- Podaktivnost: U okviru CIRT-a sistematizovaće se dva odjeljenja: odjeljenje za odgovor na incidente, tehničkog karaktera i odjeljenje za strateške pravce, politike i preventivu
- Nadležna institucija: Ministarstvo javne uprave
- Rok: IV kvartal
- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Izmjena Pravilnika o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave
- Status realizacije: Nije realizovano

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (CS/NCIRT) nisu formirana dva odjeljenja sa jasno podijeljenim nadležnostima.

3. ZAŠTITA KRITIČNE INFORMATIČKE INFRASTRUKTURE

3.1. Donošenje Uredbe o mjerama za zaštitu Kritične informatičke infrastrukture

- Podaktivnost: Donošenje regulative koja treba da definiše procedure komunikacije između vlasnika KII i nadležnih institucija, kao i osnovne tehničke i organizacione mjere koje vlasnici KII moraju da ispune
- Nadležna institucija: Ministarstvo javne uprave
- Rok: III kvartal

- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Pripremljen Predlog uredbe o mjerama zaštite KII
- Status realizacije: Djelimično realizovano

U skladu sa zadatkom Ministarstvo javne uprave pripremilo je i usaglasilo Predlog uredbe o mjerama zaštite kritične informatičke infrastrukture sa nosiocima kritičnih sektora i njeno usvajanje se očekuje tokom 2019. godine.

3.2. Analiza rizika po informacione sisteme u okviru nadležnosti

- Podaktivnost: Izvršiti analizu rizika po informacione sisteme u okviru nadležnosti ključnih institucija
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: IV kvartal
- Procjena troškova: Redovna sredstva iz budžeta / Moguća donatorska sredstva
- Indikator uspjeha: Izrađena analiza rizika
- Status realizacije: Realizovano

Shodno zadatku u Ministarstvu javne uprave kao i u Ministarstvu odbrane i Vojsci Crne Gore izrađene su analize rizika po informacione sisteme u okviru nadležnosti.

U Ministarstvu pravde je Izrađena analiza rizika u sklopu projekta implementacije standarda MEST ISO 27001:2014. Izvršena je analiza trenutnog stanja bezbjednosti informacija u postojećim informacionim sistemima, kao i identifikacija, evaluacija i klasifikacija rizika za bezbjednost informacija. Takođe, izrađen je plan tretiranja rizika koji sadrži listu kontrola, odnosno organizacionih i tehničkih mjera koje treba preduzeti za ublažavanje, odnosno eliminisanje svakog identifikovanog rizika. Pripremljena je draft verzija „Politike informacione bezbjednosti informacionog sistema pravosuđa“, u narednom periodu se očekuje njeno usvajanje od strane nadležnog tijela i institucije. Izvršena je i Analiza uticaja na poslovanje, izrada procedura na osnovu postojećih poslovnih procesa, IT infrastrukture i bezbjedonosne politike i izradu plana za nastavak poslovanja i reakcija na incidente.

Agencija za nacionalnu bezbjednost je izvršila Analizu rizika po komunikaciono informacione sisteme iz okvira svojih nadležnosti, izrađena je analiza trenutnog stanja i izvršena procjena uticaja rizika na stanje informacione bezbjednosti. Ovaj proces će se u Agenciji za nacionalnu bezbjednost i dalje obavljati kontinuirano.

4. MEĐUINSTITUCIONALNA SARADNJA

4.1. Definisanje modela za razmjenu informacija iz oblasti sajber bezbjednosti između državnih organa

- Podaktivnost: Definisanje modela za razmjenu informacija iz oblasti sajber bezbjednosti (o sajber incidentima, načinima komuniciranja u slučaju sajber napada itd.) između državnih organa
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: IV kvartal
- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Definisan model za razmjenu informacija između državnih organa
- Status realizacije: Djelimično realizovano

Ministarstvo javne uprave je tokom 2018. godine planiralo sredstva za implementaciju specijalizovanog web-portala za razmjenu informacija o napadima i prijetnjama između institucija nosioca, dok se tokom 2019. godine očekuje izrada pravilnika/protokola o međusobnoj razmjeni.

Ministarstvo vanjskih poslova je u saradnji sa Direkcijom za zaštitu tajnih podataka planiralo podizanje postojećeg sistema za razmjenu domaćih tajnih podataka sa stepena tajnosti POVJERLJIVO na TAJNO. S tim u vezi, planirana su sredstva u Ministarstvu vanjskih poslova za realizaciju projekta, čime će se dodatno ojačati trenutni model za razmjenu informacija između državnih organa.

U skladu sa zadatkom Agencija za nacionalnu bezbjednost kontinuirano radi na unapređenju saradnje sa drugim državnim organima. U prethodnom periodu nastavljena je odlična saradnja sa svim ključnim institucijama u oblasti sajber bezbjednosti.

5. ZAŠTITA PODATAKA

5.1. Unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa

- Podaktivnost: Formiranje međuresorne radne grupe za unapređenje propisa / Unapređenje propisa za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: III kvartal / kontinuirano
- Procjena troškova: Nisu potrebna sredstva
- Indikator uspjeha: Formirana međuresorna radna grupa / Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe
- Status realizacije: Djelimično realizovano

U skladu sa zadatkom Direkcija za zaštitu tajnih podataka pokrenula je proceduru za realizaciju ove aktivnosti. Direkcija je u decembru 2018. godine uputila dopis institucijama da odrede svoje predstavnike u Radnoj grupi za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke. Svoje predstavnike odredile su sledeće institucije: Direkcija za zaštitu tajnih podataka, Ministarstvo javne uprave, Ministarstvo odbrane, Generalštab Vojske Crne Gore, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo vanjskih poslova i Agencija za nacionalnu bezbjednost. Do kraja prvog kvartala 2019. godine očekuje se formalno kreiranje i početak rada radne grupe na unapređenju propisa.

5.2. Jačanje informatičkih kapaciteta Direkcije za zaštitu tajnih podataka

- Podaktivnost: Jačanje informatičkih kapaciteta državnog organa nadležnog za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci i nadležnog za upravljanje materijalima za kriptografsku zaštitu tajnih podataka
- Nadležna institucija: Direkcija za zaštitu tajnih podataka
- Rok: IV kvartal
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima
- Status realizacije: Realizovano

U skladu sa predviđenim rokom, Direkcija je Pravilnikom o unutrašnjoj organizaciji i sistematizaciji predvidjela novo radno mjesto u Odjeljenju za informatičku zaštitu tajnih podataka i u aprilu 2018. godine zaposlila novog informatičara koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.

6. EDUKACIJA U OBLASTI SAJBER BEZBJEDNOSTI

6.1. Edukacija državnih službenika i namještenika na temu sajber bezbjednosti

- Podaktivnost: Organizovanje/učešće na obukama, konferencijama, vježbama, sastancima, forumima, seminarima, radionicama
- Nadležna institucija: Ministarstvo javne uprave u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti
- Rok: Kontinuirano
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj organizovanih događaja (npr. konferencije, radionice, obuke, vježbe)
- Status realizacije: Realizovano

Ministarstvo javne uprave ulaže kontinuirani napor u organizaciju različitih događaja iz oblasti sajber bezbjednosti.

Ministarstvo javne uprave je u periodu od 26. do 28. februara 2018. godine, pod vođstvom Savjeta za informacionu bezbjednost, u saradnji sa Ambasadom Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske i njihovim ekspertskim partnerom DCAF-om (The Geneva Centre for the Democratic Control of Armed Forces), organizovalo sajber vježbu za kadar zadužen za pitanja informacione bezbjednosti, pretežno za institucije nosioce kritične informatičke infrastrukture. Cilj vježbe bio je da okupi predstavnike glavnih aktera u crnogorskom sajber prostoru kako bi između ostalog unaprijedili saradnju, povećali nivo svijesti o sajber prijetnjama i razvili što bolju koordinaciju na ovom polju. Tokom vježbe, međunarodni eksperti iz Velike Britanije, Srbije i Slovenije podijelili su svoja iskustva o najboljim praksama i razmjeni informacija tokom sajber incidenata. Drugog dana učesnici vježbe učestvovali su u simulaciji incidenata tako što su testirali postojeći model komunikacije i koordinacije u Crnoj Gori, dok je treći dan bio fokusiran na analizu rezultata drugog dana i pomoć ključnim institucijama u pripremi planova za razvoj kapaciteta. Važno je istaći da su se među učesnicima, osim predstavnika organa državne uprave, našli i predstavnici privatnog sektora i akademske zajednice.

Okrugli sto pod nazivom „State-sponsored attacks in cyberspace“ je organizovalo Ministarstvo javne uprave 3. i 4. decembra 2018. godine, u saradnji Ambasadom Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske i njihovim ekspertskim partnerom DCAF-om i u okviru projekta "Poboljšanje upravljanja sajber bezbjednošću na zapadnom Balkanu", za donosioce odluka i lica zadužena za pitanja informacione bezbjednosti, kako iz javnog tako i iz privatnog sektora. Cilj okruglog stola bio je jačanje saradnje između relevantnih nacionalnih organa sajber odbrane u cilju efikasnije saradnje i razmjene najboljih praksi, razvijanje vještina i svijesti među svim akterima sajber odbrane na nacionalnom nivou.

Takođe, Ministarstvo javne uprave je u saradnji sa Upravom za kadrove sprovelo obuke za državne službenike i namještenike na kojima je obučeno oko 100 državnih službenika i namještenika.

6.2. Podizanje svijesti građana o bezbjednom korišćenju interneta

- Podaktivnost: Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa / Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe / Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo prosvjete
- Rok: Kontinuirano
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj obučene djece, nastavnog kadra, školskih pedagoga i psihologa / Broj izrađenih brošura i objavljenih članaka i gostovanja u medijima / Broj materijala postavljenih na portalu CIRT-a (savjeti, upozorenja, obavještenja, smjernice, priručnici, prezentacije, vebinari, predavanja)
- Status realizacije: Realizovano

Zbog konstantnog rasta broja usluga koje javni i privatni sektor pružaju putem Interneta, kako građanima, tako i drugim pravnim subjektima, bezbjedan sajber prostor Crne Gore postaje jedan od nacionalnih prioriteta.

Povodom Dana sigurnog interneta, predstavnik Ministarstva javne uprave učestvovao je na panel diskusiji „Bezbjedno korišćenje digitalnih medija“ koju je organizovao Crnogorski Telekom. Na panelu je bilo riječi o digitalnoj pismenosti i pozitivnim aspektima upotrebe digitalnih tehnologija, kao i o zaštiti podataka, pravilima ponašanja na internetu i društvenim mrežama, zaštiti od online opasnosti. Poseban akcenat je stavljen na izazove sa kojima se susreću roditelji i nastavnici u radu sa djecom. Takođe, u okviru Dana sigurnog interneta, u saradnji sa Ministarstvom prosvjete, predstavnici Ministarstva javne uprave održali su prezentaciju za roditelje učenika u OŠ „Oktoih“ na temu bezbjednog korišćenja interneta.

Ministarstvo javne uprave u kontinuitetu radi na podizanju svijesti kada je bezbjedno korišćenje interneta u pitanju kroz objavu sigurnosnih savjeta, objavu članaka i gostovanja u medijima.

Ministarstvo prosvjete je realizovalo radionice za oko 1.100 učenika i 250 nastavnika u cilju podizanja svijesti o bezbjednom korišćenju interneta, koje takođe obilježava Dan sigurnog internet svake godine u obrazovno-vaspitnim ustanovama. Pored toga, povećana je upotreba kviza o bezbjednom korišćenju interneta (www.pokazistaznas.edu.me) u školama u obliku pomoćnog nastavnog sredstva kroz informatičke predmete. Ministarstvo prosvjete je radilo i na promociji aplikacija NET prijatelj koja je namjenjena za mlađi uzrast djece (www.netprijatelji), a koja je razvijena u saradnji sa Kancelarijom UNICEF-a u Crnoj Gori. Ovo Ministarstvo kontinuirano radi i na promociji portala za nastavnike (www.skolskiportal.edu.me) na kojem je posebna kategorija posvećena bezbjednosti djece na internetu, na kojem se često objavljuju vijesti, uputstva, preporuke i slični materijali vezani za ovu temu.

7. SARADNJA JAVNOG I PRIVATNOG SEKTORA

7.1. Uspostavljanje saradnje sa privatnim sektorom (ISP, banke, ...) i akademskom zajednicom

- Podaktivnost: Formalizovanje saradnje sa privatnim sektorom u vidu definisanja procedura za razmjenu informacija, organizovanje zajedničkih vježbi, konferencija, obuka, sastanaka
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: Kontinuirano
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom kroz definisanje procedura za razmjenu informacija i učešća na zajedničkim događajima
- Status realizacije: Realizovano

Tokom godine predstavnici privatnog sektora i akademske zajednice učestvovali su na sajber vježbi i okruglom stolu u organizaciji Ministarstva javne uprave u saradnji sa Ambasadom Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske i njihovim ekspertskim partnerom DCAF-om (The Geneva Centre for the Democratic Control of Armed Forces). Tokom 2019. godine očekuje se definisanje procedura za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora.

U okviru INFOFEST-a 2018 održan je panel „Tehnologije, privatnost i politike privatnost za digitalnu ekonomiju**“** u organizaciji Ministarstva javne uprave. Panelu su prisustvovali predstavnici javnog, privatnog sektora i akademske zajednice.

Obavljeni su sastanci sa predstavnicima Ministarstva prosvjete sa fokusom na podizanje svijesti o sajber bezbjednosti u srednjim školama i osmišljavanjem edukativnih poduhvata iz te oblasti. Takođe, obavljeni su sastanci sa predstavnicima univerziteta, gdje su razmatrani modeli međusobne saradnje, sa fokusom na jačanje nastavnog programa iz oblasti sajbera i uključivanje profesora i studenata u dešavanja koja su organizovana od strane državnih institucija (seminari, radionice, kursevi i sl.).

8. REGIONALNA I MEĐUNARODNA SARADNJA

8.1. Jačanje saradnje na regionalnom i međunarodnom nivou u cilju obezbjeđivanja nacionalne bezbjednosti

- Podaktivnost: Organizacija konferencija, okruglih stolova, radionica, studijskih posjeta sa regionalnim i međunarodnim organizacijama
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Rok: Kontinuirano
- Procjena troškova: Redovna sredstva iz budžeta
- Indikator uspjeha: Broj održanih konferencija, studijskih posjeta, radionica
- Status realizacije: Realizovano

U cilju jačanja saradnje na regionalnom i međunarodnom nivou predstavnici Ministarstva javne uprave su učestvovali na sajber vježbama, obukama, konferencijama koje su imale za cilj jačanje kapaciteta tima za odgovor na incidentne situacije. Takođe, u organizaciji Ministarstva vanjskih poslova SAD-a i Ambasadom SAD-a u Podgorici organizovana je posjeta relevantnih institucija za sajber bezbjednost u SAD.

Ministarstvo odbrane je organizovalo dvodnevnu radionicu u sklopu Projekta izgradnje sajber kapaciteta u Crnoj Gori, pokrenut od strane Velike Britanije. Na radionici su uzele učešće sve ključne institucije koje se bave pitanjima sajber bezbjednosti i participiraju u okviru Savjeta za informacionu bezbjednost. Vojska Crne Gore je u sklopu saradnje sa SAD (Komandom oružanih snaga za Evropu - USEUCOM) organizovala u Podgorici „Cyber Endeavor Seminar“.

Predstavnici Ministarstva vanjskih poslova su učestvovali na različitim bilateralnim i multilateralnim forumima gdje je jedna tema bila i sajber bezbjednost. Takođe, Ministarstvo vanjskih poslova je, preko Misije Crne Gore pri NATO, aktivno uključeno u sve rasprave i odluke o politici sajber odbrane NATO i redovno učestvuje na sastancima radnih tijela NATO posvećenih sajber bezbjednosti.

Na sastanku Upravnog odbora Mreže za ministarstva vanjskih poslova država Zapadnog Balkana koji je održan u Beču u novembru 2018. godine, Ministarstvo vanjskih poslova je predložilo organizaciju obuke u oblasti sajber bezbjednosti i hibridnih prijetnji, u okviru koje bi se realizovala i posjeta Centru za sajber bezbjednost u Briselu, što je prihvaćeno. Održavanje pomenute obuke planirano je za septembar 2019. godine.

Crna Gora se, 12. novembra 2018. godine, pridružila inicijativi francuskog predsjednika Emanuela Makrona „Paris Call for rust and Security in Cyberspace“ koja poziva na razvoj zajedničkih principa za jačanje otpornosti sajber prostora na napade.

Predstavnik Ministarstva pravde je učestvovao na dvodnevnoj Regionalnoj radionici o statistici krivičnih djela iz oblasti sajber kriminala i elektronskim dokazima u pravosuđu, koja je održana u Bukureštu, 14-15 maja 2018.godine. FFRadionica je organizovana u okviru iPROCEEDS projekta, koji predstavlja zajednički projekat Evropske unije i Savjeta Evrope, sa ciljem prevencije sajber kriminala u Jugoistočnoj Evropi i Turskoj, kao i poboljšanju statističkih sistema i izvještaja, metodologiji prikupljanja elektronskih dokaza i regulativi koja prati ovu oblast.

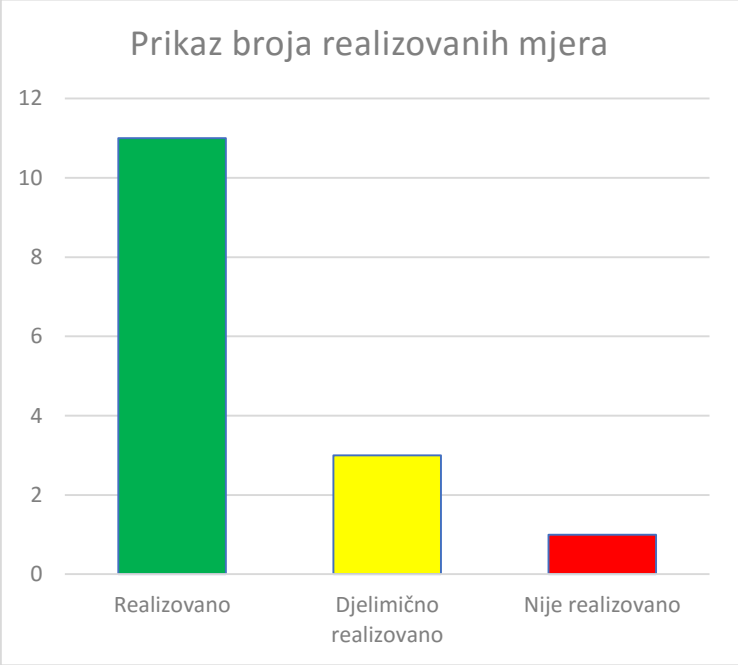
Predstavnici Direkcije za zaštitu tajnih podataka učestvovali su na godišnjoj NDA (National Distribution Authority) konferenciji koja okuplja NDA tijela iz država članica NATO. Potpisan je sporazum o razmjeni i uzajamnoj zaštiti tajnih podataka sa Njemačkom, dok su završeni pregovori o potpisivanju sporazuma sa Makedonijom. U okviru intenzivne saradnje sa NATO, u periodu od 16. do 20. aprila 2018. godine, Direkcija za zaštitu tajnih podataka imala je čast da bude domaćin sastanaka NATO Bezbjednosnog komiteta u Podgorici. Sastanku su prisustvovali predstavnici 23 zemlje članice NATO Bezbjednosnog komiteta. U okviru regionalne saradnje, u periodu od 10. do 13. septembra 2018. godine, delegacija Direkcije za zaštitu tajnih podataka učestvovala je na SEENSA konferenciji. SEENSA konferencija je inicijativa pokrenuta od strane Regionalnog vijeća za saradnju (RCC) i okuplja nadležne Nacionalne bezbjednosne organe (NSA) iz zemalja jugo-istočne

Evrope. U Skoplju su održane bilateralne konsultacije između predstavnika Direkcije za zaštitu tajnih podataka Crne Gore i predstavnika makedonske Direkcije za zaštitu tajnih podataka.

Predstavnici Agencije na nacionalnu bezbjednost su u saradnji sa partnerskim službama učestvovali na konferencijama, okruglim stolovima i studijskim posjetama sa regionalnim i međunarodnim organizacijama. Takođe su učestvovali i u aktivnostima u organizaciji Ministarstva javne uprave.

GRAFIČKI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA

Od planiranih 15 mjera i aktivnosti realizovano je jedanaest, u toku je realizacija još tri aktivnosti, dok jedna aktivnost nije realizovana. 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.



FINANSIJSKI POKAZATELJI

Finansijska sredstva za realizaciju mjera iz Akcionog plana planiraju su u okviru redovnih ciklusa planiranja budžeta od strane nosioca mjera i ostvaruju se kroz budžet ili donacije.

II TABELARNI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA

Akcioni plan za implementaciju Strategije sajber bezbjednosti 2018-2021, za 2019. godinu									
RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata	Planirana sredstva	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
Clj 1: Kapaciteti za sajber odbranu									
1.1.	Uspostavljanje strukture lokalnih CIRT timova	Uspostavljanje lokalnih CIRT timova / određivanje kontakt osoba	Ministarstvo javne uprave	Broj uspostavljenih lokalnih CIRT timova u odnosu na trenutno stanje; sačinjena lista kontakt osoba		Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Redovno ažuriranje liste
1.2.	Planiranje budžetskoh sredstava opredijeljenih za sajber bezbjednost u okviru institucija koje su prepoznati kao nosioci	Za efikasno funkcionisanje u okviru institucija koje su prepoznate kao nosioci sajber bezbjednosti moraju postojati opredijeljena budžetska sredstva za sajber bezbjednost	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Broj institucija koje su izradile plan budžetskih sredstava opredijeljenih za sajber bezbjednost		III kvartal	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti na obezbjeđivanju finansijskih sredstava opredijeljenih za sajber bezbjednost

1.3.	Jačanje administrativnih kapaciteta zaduženih za sajber bezbjednost	Analiza trenutnog stanja i procjena optimalnog broja službenika zaduženih za sajber bezbjednost	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Izrađena analiza trenutnog stanja		III kvartal	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti na obezbjeđivanju ljudskih resursa u institucijama zaduženim za sajber bezbjednost
1.4.	Jačanje tehničkih kapaciteta institucija zaduženih za sajber bezbjednost	Analiza trenutnih i planiranih tehničkih kapaciteta; Nabavka opreme	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Izrađena analiza trenutnih i planiranih tehničkih kapaciteta i nabavka opreme		IV kvartal	Nisu potrebna sredstva	**Realizovano**	Nabavka opreme u skladu sa izrađenom analizom
Cilj 2: Centralizacija sajber ekspertize i resursa									
2.1.	Jačanje administrativnih kapaciteta CIRT-a	Povećanje broja službenika CIRT-a kroz izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji	Ministarstvo javne uprave Ministarstvo odbrane	Osam sistematizovanih radnih mjesta u MJU CIRT-u do kraja 2018. godine; 5 sistematizovanih radnih mjesta u MOD CIRT-u		IV kvartal	Budžet nadležnih institucija	**Realizovano**	Dalje jačanje administrativnih kapaciteta CIRT tima i povećanje broja službenika

2.2.	Jačanje organizacionih kapaciteta CIRT-a	U okviru CIRT-a sistematizovaće se dva odjeljenja: odjeljenje za odgovor na incidente, tehničkog karaktera i odjeljenje za strateške pravce, politike i preventivu	Ministarstvo javne uprave	Izmjena Pravilnika o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave		IV kvartal	Nisu potrebna sredstva	**Nije realizovano** Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave u okviru CIRT-a povećan je broj službenika, međutim aktivnost nije realizovana budući da nisu formirana dva odjeljenja sa jasno podijeljenim nadležnostima.	Aktivnost nije realizovana shodno Planu optimizacije javne uprave, realizacija ove aktivnosti predviđena je Akcionim planom za 2019. godinu
Cilj 3: Zaštita kritične informatičke infrastrukture									
3.1.	Donošenje Uredbe o mjerama za zaštitu KII	Donošenje regulative koja treba da definiše procedure komunikacije između vlasnika KII i nadležnih institucija, kao i osnovne tehničke i organizacione mjere koje vlasnici KII moraju da ispune	Ministarstvo javne uprave	Pripremljen Predlog uredbe o mjerama zaštite KII		III kvartal	Nisu potrebna sredstva	**Djelimično realizovano** U skladu sa zadatkom Ministarstvo javne uprave pripremilo je i usaglasilo Predlog uredbe o mjerama zaštite kritične informatičke infrastrukture sa nosiocima kritičnih sektora i njeno usvajanje se očekuje tokom 2019. godine.	Intenziviranje aktivnosti na donošenju Uredbe o kritičnoj informatičkoj infrastrukturi i načinu njene zaštite.

3.2.	Analiza rizika po informacione sisteme u okviru nadležnosti	Izvršiti analizu rizika po informacione sisteme u okviru nadležnosti ključnih institucija	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Izrađena analiza rizika		IV kvartal	Redovna sredstva iz budžeta / Moguća donatorska sredstva	**Realizovano**	Na osnovu odrađene analize i preporuka održavati postojeće i razvijati nova IT rješenja
Cilj 4: Međuinstitucionalna saradnja									
4.1.	Definisanje modela za razmjenu informacija iz oblasti sajber bezbjednosti između državnih organa	Definisanje modela za razmjenu informacija iz oblasti sajber bezbjednosti (o sajber incidentima, načinima komuniciranja u slučaju sajber napada itd.) između državnih organa	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Definisan model za razmjenu informacija između državnih organa		III kvartal	Nisu potrebna sredstva	**Djelimično realizovano** Planirana su sredstva za implementaciju specijalizovanog web-portala za razmjenu informacija o napadima i prijetnjama između institucija nosioca, dok se tokom 2019. godine očekuje izrada pravilnika/protokola o međusobnoj razmjeni.	Intenzivirati aktivnosti na izradi pravilnika/protokola o međusobnoj razmjeni
Cilj 5: Zaštita podataka									

5.1.	Unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa	Formiranje međuresorne radne grupe za unapređenje propisa / Unapređenje propisa za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Formirana međuresorna radna grupa / Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe		Kontinuirano	Nisu potrebna sredstva	**Djelimično realizovano** Do kraja prvog kvartala 2019. godine očekuje se formalno kreiranje i početak rada radne grupe na unapređenju propisa.	Ubrzati rad na unapređenju propisa za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa
5.2.	Jačanje informatičkih kapaciteta Direkcije za zaštitu tajnih podataka	Jačanje informatičkih kapaciteta državnog organa nadležnog za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci i nadležnog za upravljanje materijalima za kriptografsku zaštitu tajnih podataka	Direkcija za zaštitu tajnih podataka	Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima		IV kvartal	Redovna sredstva iz budžeta	**Realizovano**	
Cilj 6: Edukacija u oblasti sajber bezbjednosti									
6.1.	Edukacija državnih službenika i namještenika na temu sajber bezbjednosti	Organizovanje/učešće na obukama, konferencijama, vježbama, sastancima, forumima, seminarima, radionicama	Ministarstvo javne uprave u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti	Broj organizovanih događaja (npr. konferencije, radionice, obuke, vježbe)		Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti sa edukacijom državnih službenika i namještenika na temu sajber bezbjednosti

6.2.	Podizanje svijesti građana o bezbjednom korišćenju interneta	Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa / Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe / Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti	Ministarstvo javne uprave Ministarstvo prosvjete	Broj obučene djece, nastavnog kadra, školskih pedagoga i psihologa / Broj izrađenih brošura i objavljenih članaka i gostovanja u medijima / Broj materijala postavljenih na portalu CIRT-a (savjeti, upozorenja, obavještenja, smjernice, priručnici, prezentacije, vebinari, predavanja)		Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Organizovati bolju promociju portala CIRT.ME; izraditi promotivne materijale; nastaviti sa održavanjem radionica
Cilj 7: Saradnja javnog i privatnog sektora									
7.1.	Uspostavljanje saradnje sa privatnim sektorom (ISP, banke, ...) i akademskom zajednicom	Formalizovanje saradnje sa privatnim sektorom u vidu definisanja procedura za razmjenu informacija, organizovanje zajedničkih vježbi, konferencija, obuka, sastanaka	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom kroz definisanje procedura za razmjenu informacija i učešća na zajedničkim događajima		Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Jačanje saradnje sa privatnim sektorom i akademskom zajednicom
Cilj 8: Regionalna i međunarodna saradnja									

8.1.	Jačanje saradnje na regionalnom i međunarodnom nivou u cilju obezbjeđivanja nacionalne bezbjednosti	Organizacija konferencija, okruglih stolova, radionica, studijskih posjeta sa regionalnim i međunarodnim organizacijama	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Broj održanih konferencija, studijskih posjeta, radionica		Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	

III PREPORUKE ZA DALJE FAZE SPROVOĐENJA STARTEŠKOG DOKUMENTA

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 je prepoznato osam ciljeva, čija je realizacija detaljnije definisana kroz pojedinačne zadatke postojećeg Akcionog plana.

Uvidom u status realizacije Akcionog plana za implementaciju Strategije evidentna je intenzivna aktivnost nadležnih institucija u ispunjavanju zacrtanih ciljeva kojim su, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom.

Aktivnost 2.2. nije realizovana u 2018. godini shodno Planu optimizacije javne uprave, i kao takva naći će se u Akcionom planu za 2019. godinu

Preporuke za dalje faze sprovođenja strateškog dokumenta po ciljevima su:

STRATEŠKI CILJ 1: Jačanja kapaciteta za sajber odbranu

- redovno ažurirati listu lokalnih CIRT timova/kontakt osoba
- na osnovu izrađene analize stanja i procjene budžetom predvidjeti sredstva za zapošljavanje službenika zaduženih za sajber bezbjednost
- nabaviti opremu u skladu sa izrađenom analizom

STRATEŠKI CILJ 2: Centralizacija sajber ekspertize i resursa

- shodno izrađenoj analizi predložiti izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji sa ciljem da se u CIRT-u sistematizuju dva odjeljenja (odjeljenje tehničkog karaktera i odjeljenje za strateške pravce, politiku i preventive) kao i popuniti upražnjena mjesta

STRATEŠKI CILJ 3: Zaštita kritične informatičke infrastrukture

- intenzivirati aktivnosti na donošenju Uredbe o kritičnoj informatičkoj infrastrukturi i načinu njene zaštite
- ažurirati postojeću listu kritične informatičke infrastrukture

STRATEŠKI CILJ 4: Međuinstitucionalna saradnja

- implementirati platformu za razmjenu informacija
- formirati operativni tim koji bi bio na raspolaganju organima državne uprave u slučaju napada većih razmjera
- predložiti pravilnik/protokol o međusobnoj razmjeni

STRATEŠKI CILJ 5: Zaštita podataka

- usvojiti pravne propise za sertifikaciju komunikaciono-informacionih sistema

STRATEŠKI CILJ 6: Edukacija u oblasti sajber bezbjednosti

- organizovati pet događaja (konferencije, radionice, seminare, obuke…) za edukaciju državnih službenika i namještenika