



**CRNA GORA
MINISTARSTVO FINANSIJA**

Broj: 02-03-21021/1

Podgorica, 14. decembar 2017. godine

**MINISTARSTVO JAVNE UPRAVE
-n/r ministarke, gospođe Suzane Pribilović-**

Poštovana gospođo Pribilović,

Povodom *Nacrta strategije sajber bezbjednosti Crne Gore 2018-2021. godine*,
Ministarstvo finansija daje sljedeće

MIŠLJENJE

Na tekst *Nacrta strategije* i pripremljeni *Izveštaj o sprovedenoj analizi procjene uticaja propisa, sa aspekta implikacija na poslovni ambijent, nemamo primjedbi.*

Na osnovu uvida u dostavljeni tekst i *Izveštaj o sprovedenoj analizi procjene uticaja propisa* utvrđeno je da za implementaciju i realizaciju *Strategije sajber bezbjednosti Crne Gore 2018-2021. godine*, nije potrebno obezbijediti dodatna finansijska sredstva za 2018. godinu, dok će sredstva neophodna za implementaciju strategije u narednom periodu (2019-2021) biti predviđena kroz godišnje akcione planove.

Shodno navedenom, *Ministarstvo finansija, sa aspekta budžeta, daje saglasnost na Nacrt strategije sajber bezbjednosti Crne Gore 2018-2021. godine, uz obavezu da se budžetska sredstva potrebna za implementaciju Nacrta startegije prilagode sredstvima opredijeljenim nosiocima aktivnosti godišnjim zakonima o budžetu.*

S poštovanjem,



IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	Ministarstvo javne uprave
NAZIV PROPISA	Nacrt Strategija sajber bezbjednosti Crne Gore 2018 - 2021
1. Definisanje problema <ul style="list-style-type: none"> - Koje probleme treba da riješi predloženi akt? Probleme sistematskog unapređenja sajber bezbjednosti Crne Gore - Koji su uzroci problema? Sajber napadi i rizici - Koje su posljedice problema? Finansijske, ugrožavanje kredibiliteta i druge - Koji su subjekti oštećeni, na koji način i u kojoj mjeri? Cjelokupno društvo - Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)? 	
2. Ciljevi <ul style="list-style-type: none"> - Koji ciljevi se postižu predloženim propisom? Postiže se cilj sistematskog unapređenja sajber bezbjednosti Crne Gore - Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo. Programom rada Vlade za 2017. godinu predviđeno je usvajanje Strategije sajber bezbjednosti 2018-2021 	
3. Opcije <ul style="list-style-type: none"> - Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa). Cilj: Razviti savremen i moderan nacionalni koncept sajber bezbjednosti koji će kroz jasno precizirane strateške ciljeve biti u potpunosti kompatibilan sa konceptima najrazvijenijih zemalja članica EU i NATO saveza. Koncept treba da obezbijedi preduslove za postojanje sigurnog i bezbjednog informacionog društva jedne države i na taj način omogućiti sve koristi njegovog postojanja. Koncept treba da omogućiti radni okvir za nesmetanu i uspješnu implementaciju Nacionalne strategije sajber bezbjednosti zajedno sa postojećom domaćom i međunarodnom zakonskom legislativom iz ove oblasti. <p>ATIVNOSTI I INDIKATORI:</p> <p>a. Usvajanje koncepta koji će biti jasan i potpuno prihvatljiv kako od strane domaće javnosti tako i od relevantnih međunarodnih činilaca uz sagledavanje svih specifičnosti države Crne Gore i crnogorskog društva. Indikator uspjeha bi bio usvajanje koncepta od strane nadležnog tijela Vlade Crne Gore zaduženog za sajber bezbjednost.</p>	

b. Koncept mora da generiše aktivnosti na kontinuiranom unapređenju nacionalnog zakonodavnog okvira, uz nužno praćenje razvoja legislative na međunarodnom nivou, pri čemu bi ono sadržavalo najveći dio ENISA preporuka. Indikator uspjeha bi bio usvajanje nove nacionalne legislative sa prihvaćenim ENISA preporukama.

c. Koncept se mora podudarati u ključnim djelovima sa konceptima razvijenih zemalja EU i NATO, u prvom redu u pogledu standardizacije pojmova, metoda, polisa i procedura u skladu sa prihvaćenim evropskim i međunarodnim standardima. Indikator uspjeha bi bio izvršena nacionalna standardizacija pojmova, metoda i termina vezanih za oblast sajber bezbjednosti.

STRATEŠKI CILJ:

Vlada Crne Gore će nastaviti sa posvećenim radom na daljem jačanju sajber bezbjednosnih kapaciteta u smislu obezbjeđivanja adekvatnih ljudskih, 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.

AKTIVNOSTI I INDIKATORI:

a. Relevantne institucije na polju sajber bezbjednosti će osnovati CIRT timove ili prepoznati službenike čija će osnovna funkcija biti aktivnosti iz domena sajber bezbjednosti tzv. lokalni CIRT. Indikator uspjeha će biti procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.

b. Relevantne institucije moraju imati kapacitete da prepoznaju, identifikuju i urade godišnje ili ukoliko je potrebno vremenski kraće analize rizika po informacione sisteme u okviru istih ili u okviru njihove nadležnosti. Indikator uspjeha predstavljace broj izrađenih analiza rizika u odnosu na broj institucija.

c. Posebni organi ili organizacione jedinice, u okviru institucija koje su prepoznate kao nosioci funkcije sajber bezbjednosti Crne Gore, moraju da imaju opredijeljena budžetska sredstva svake godine, kojima bi nabavljali adekvatne resurse i alate za efikasno funkcionisanje. Indikatori uspjeha će predstavljati broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.

d. Relevantni organi moraju definisati optimalan broj zaposlenih službenika u njihovom CIRT timu odnosno službenika zaduženih za sajber bezbjednost u cilju adekvatnog odgovora na prijetnje, izazove, analize rizika i potencijalne napade na njihove informacione sisteme. Prethodno mora biti urađeno na godišnjem nivou a kako bi imali pregled broja zaposlenih i broja potrebnih službenika na Nacionalnom nivou. Na osnovu preporuka ENISE minimalan broj zaposlenih u CIRT koji ima funkciju 24/7 jeste 12. Indikator uspjeha predstavlja izvještaj o minimalnom broju službenika za sajber bezbjednost.

STRATEŠKI CILJ:

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 infrastrukture i druge bitne informacione sisteme; razumijeli rizici po sajber prostor Crne Gore; pružile adekvatne preporuke i unaprijedila saradnja sa privatnim i javnim sektorom.

AKTIVNOSTI I INDIKATORI:

a. U skladu sa Strategijom razvoja informacionog društva do 2020. godine Nacionalni CIRT tim će do 2018. godine imati 10 službenika, a do 2020. godine imati 20 službenika. Indikator uspjeha predstavljaće ispunjenost zadatah rokova i broj zaposlenih u Nacionalnom CIRT-u.

b. U okviru Nacionalnog CIRT-a sistematizovaće se dva odeljenja - za odgovor na incidente, tehničkog karaktera i za strateške pravce, politike i preventivu. Indikator uspjeha predstavljaće izmjena Pravilnika o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave.

c. Za funkcionisanje Nacionalnog CIRT-a opredijeliće se dvije specijalizovane prostorije u kojima će se obezbijediti rad i eksperata iz drugih institucija u slučaju napada na KII i napada širokih razmjera na Crnu Goru. Indikator uspjeha broj prostorija koje ispunjavaju minimum tehničkih karakteristika u odnosu na broj predviđenih

d. Nacionalni CIRT će u redovnim vremeskim intervalima organizovati specijalističke vježbe, simulacije napada na KII i napada širokih razmjera za pripadnike relevantnih organa, kao i kompanije nosioce KII. Indikator uspjeha predstavljaće broj organizovanih vježbi i uključenih aktera.

STRATEŠKI CILJ:

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 organizovanju 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.

AKTIVNOSTI I INDIKATORI:

- a. Kako bi saradnja i komunikacija među institucijama bila dodatno olakšana, evidentirana je potrebna imenovanja kontakt osoba za sajber bezbjednost ispred svih uključenih aktera. Indikator uspjeha predstavljaće broj imenovanih kontakt osoba u odnosu na broj institucija.
- b. Uspostavljanje javno dostupnog registra sajber eksperata koji bi vodilo nadležno Ministarstvo za ovu oblast. Indikator uspjeha predstavljaće funkcionisanje registra sajber eksperata.
- c. Razvoj platforme za dijalog i razmjenu informacija koja bi povezala eksperte za sajber bezbjednost iz javnog i privatnog sektora kako na lokalnom, tako i na nacionalnom nivou. Indikator uspjeha predstavljaće operativna platforma.
- d. Uspostavljanje inter-resorne radne grupe na tehničkom nivou koja bi okupila eksperte sajber bezbjednosti i stvorila kapacitete za odbranu od sajber napada. Indikator uspjeha predstavljaće formirana inter-resorna grupa.
- e. U cilju efikasnosti, koordinacije i komunikacije inter-resorna radna grupa organizovaće simulacije i vježbe. Indikator uspjeha predstavljaće broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.
- f. Izrada pravilnika i procedura za razmjenu informacija o sajber incidentima, načinima komuniciranja u slučaju sajber napada, načinima pomoći i kooperaciji između državnih organa. Indikator uspjeha predstavljaće definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.

STRATEŠKI CILJ:

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.

AKTIVNOSTI I INDIKATORI:

a. U martu 2017. godine donešen je set pravnih propisa neophodnih za sprovođenje sertifikacije komunikaciono informacionih sistema i procesa u kojima se koriste tajni podaci većih stepena tajnosti. Prepoznato je da postoji prostor za unapređenje ovog seta propisa, posebno u dijelu sertifikacije 'standalone' mašina i interkonekcije komunikaciono-informacionih sistema. Indikator uspjeha predstavljaće izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.

b. Jačanje informatičkih kapaciteta državnog organa nadležnog za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci (SAA – engl. Security Accreditation Authority) i nadležnog za upravljanje materijalima za kriptografsku zaštitu tajnih podataka (NDA – engl. National Distribution Authority). Indikator uspjeha je broj

novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.

c. Jačanje institucionalnih kapaciteta potrebnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i njihovih interkonekcija kroz uvođenje sistematizovane funkcije koja obuhvata opisa posla za informacionu bezbjednost tajnih podataka u državnim institucijama u kojima se u većoj mjeri rukuje tajnim podacima u elektronskoj formi (za veće stepene tajnosti sistematizovano kao posebno radno mjesto, za najniži stepen tajnosti moguće kao dodati opis poslova kod postojećeg radnog mjesta). Indikator uspjeha je broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.

d. Sertifikacija komunikaciono-informacionih sistema u kojima se koriste podaci većih stepena tajnosti, uvođenje sistema menadžmenta bezbjednošću informacija i upravljanja rizika u komunikaciono-informacionim sistemima u kojima se koriste tajni podaci stepena tajnosti INTERNO (ISO/IEC 27000 certifikacija uz dodatne mjere bezbjednosti) i neklasifikovani osjetljivi podaci (ISO/IEC 27001). Indikator uspjeha je broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.

e. Uspostavljanje saradnje sa obrazovnim i naučnim institucijama u cilju dugoročne edukacije i osposobljavanja kadra za potrebe kreiranja nacionalnih kriptografskih rješenja. Indikator uspjeha je broj uspostavljenih saradnji i iz njih pokrenutih obrazovnih ili naučnih projekata.

STRATEŠKI CILJ:

adležni 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 naponi 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.

AKTIVNOSTI I INDIKATORI:

a. U cilju promovisanja i širenja kulture o sajber bezbjednosti neophodno je kontinuirano nastaviti sa učešćem na i organizovanjem konferencija, radionica, obuka, kao i sa izradom publikacija, pisanjem radova i članaka, te i, gostovanjima u obrazovnim emisijama. Indikator uspjeha predstavljaju broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.

b. Kako je konstantna edukacija, praćenje trendova i širenje svijesti od velikog značaja za sajber bezbjednost, trebalo bi konstantno unapređivati sadržaj na portalu CIRT.ME, sa materijalima vezanim za bezbjednost, koji se kontinuirano ažuriraju u skladu sa novim tehnologijama (savjeti, upozorenja, obavještenja, smjernice, priručnici, prezentacije, vebinari, predavanja). Indikator uspjeha predstavljaju, uz broj objavljenih sadržaja na portalu CIRT.ME i broj ažuriranih materijala.

c. Potrebno je edukovati nastavni kadar kako bi se svijest o sajber bezbjednost kod njih podigla na veći nivo jer najviše vremena provode u neposrednom radu sa djecom pa su u prilici da utiču i na podizanju njihove svijesti o ovoj temi. Indikator uspjeha predstavljaju broj obučeni nastavnika po predhodno utvrđenom programu obuke.

d. Posebna ciljna grupa koja je prepoznata su školski pedagozi i psiholozi. Većina problema najčešće se rješava u pedagoško-psihološkoj službi škole pa je njihovo poznavanje i razumjevanje ove problematike od velikog značaja za pomoć djeci. Predhodno je potrebno utvrditi da li su svi školski pedagozi digitalno pismeni i ukoliko nisu neophodno im je pružiti elementarno znanje rada na računaru a nakon toga sprovesti obuke koje se odnose na sajber bezbjednost. Indikator uspjeha je broj obučeni pedagoga i psihologa na osnovu unaprijed definisanog programa obuke.

e. Redavan predmet Informatika sa tehnikom koji se izučava tek od petog razreda osnovne škole a obuhvata određeni broj nastavnih jedinica nije dovoljan kada je tema sajber bezbjednost u pitanju pa je za djecu školskog uzrasta neophodno organizovanje niza vannastavnih aktivnosti

na ovu temu, posebno za djecu manjeg uzrasta. Indikator uspjeha broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.

f. Neophodno je razviti niz materijala na razne teme sajber bezbjednosti koje će biti prilagođene različitim uzrastima djece. Materijale objaviti na školskom portalu (www.skolskiportal.edu.me) u kategoriji Bezbjednost djece na internetu. Indikator uspjeha bi bio broj kreiranih materijala (foto, video, priručnik, smjernica, preporuka, igrica itd).

STRATEŠKI CILJ: 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 da se preduzmu neophodne mjere kako bi se postigao dovoljan stepen bezbjednosti.

AKTIVNOSTI I INDIKATORI:

- a. U cilju razvoja efikasnog odgovora za sajber bezbjednost trebalo bi raditi na unaprjeđenju i institucionalizaciji saradnje između javnog i privatnog sektora. Indikator uspjeha predstavljaće broj uspostavljenih javno-privatnih partnerstava.
- b. Izrada procedura za razmjenu informacija o sajber incidentima, načinima komuniciranja u slučaju sajber napada, načinima pomoći i kooperaciji između javnog i privatnog sektora. Indikator uspjeha predstavljaće definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektor

- **Objasni preferiranu opciju?**

Sve aktivnosti je neophodno ispuniti u pravcu potpunog ispunjenja ciljeva

4. Analiza uticaja

- **Na koga će i kako će najvjerojatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.**

Na državne institucije i društvo u cjelini.

Direktni: jačanje kapaciteta za sajber odbranu u institucijama prepoznatim kao nosici sajber bezbjednosti

Indirektni: Sigurniji sajber proctor Crne Gore

- **Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima)**

Neće biti troškova za građane i privredu

- **Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.**

Da

- **Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.**

Ne

- **Uključiti procjenu administrativnih opterećenja i biznis barijera.**

U ovom trenutku nije moguće utvrditi da li će biti dodatnih opterećenja iz razloga što postoji mogućnost nametanja sigurnosnih mjera kompanijama vlasnicima kritične informatičke infrastructure, ali se jos uvijek nije pristupilo uređivanju ovoga problema.

5. Procjena fiskalnog uticaja

- **Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?**

Da, uglavnom na povećanju kapaciteta ljudskih resursa. U okviru Ministarstva javne uprave ovo povećanje je prepoznato prethodno usvojenom Strategijom razvoja informacionog društva do 2020. godine

- **Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Objasni.**

- U toku 4 godine, Strategija je za četvorogodišnji period 2018. – 2021. godina
- **Da li implementacijom propisa proizilaze međunarodne finansijske obaveze? Obrazložiti.**
Ne
 - **Da li su neophodna finansijska sredstva obezbijeđena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskalnu godinu?**
Ne
 - **Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteći finansijske obaveze?**
Ne
 - **Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?**
Ne
 - **Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.**
Nije rađena metodologija i nema troškova za 2018. godinu
 - **Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda? Obrazložiti.**
 - **Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?**
Ne
 - **Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.**
Ne

6. Konsultacije zainteresovanih strana

- **Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.**
Ne
- **Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).**
Ministarstvo javne uprave,
Ministarstvo prosvjete,
Ministarstvo odbrane,
Uprava policije,
Agencija za nacionalnu bezbjednost
Ministarstvo prosvjete
- **Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.**
Svi državni organi su u okviru svojih nadležnosti izradili djelove strategije

7: Monitoring i evaluacija

- **Koje su potencijalne prepreke za implementaciju propisa?**
Finansijske
- **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?**
Prateći akcioni planovi
- **Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?**
Kvantitativni indikatori navedeni u Strategiji
- **Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?**
Da, Savjet za informacionu bezbjednost

Datum i mjesto

Podgorica 01.12.2017.godine



Starješina

[Handwritten signature]