Crna Gora
Ministarstvo javne uprave,
digitalnog društva i medija

Adresa: Rimski trg br. 45
81000 Podgorica, Crna Gora
tel:+382 20 482 131
fax:+382 20 241 790
www.mju.gov.me

# IZVJEŠTAJ O SPROVEDENOJ JAVNOJ RASPRAVI O NACRTU STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE ZA PERIOD 2022-2026. GODINE

**Vrijeme trajanja javne rasprave:** 35 dana (11. oktobra – 15. novembra 2021)

**Način sprovođenja javne rasprave:**

- Održavanje okruglog stola o Nacrtu Strategije sajber bezbjednosti Crne Gore za period 2022-2026. godine (8.11.2021. godine u 10:00 časova, u sali Stare zgrade Vlade, ul. Jovana Tomaševića bb);
- Dostavljanje primjedbi, predloga i sugestija na Nacrt Strategije sajber bezbjednosti Crne Gore za period 2022-2026. godine u pisanoj formi Ministarstvu javne uprave, digitalnog društva i medija na adresu: Rimski trg, broj 45, 81000 Podgorica ili na e-mail adrese: srdjan.damjanovic@mju.gov.me i dusan.krkotic@mju.gov.me tokom cijelog trajanja javne rasprave.

**Ovlašćeni predstavnici Ministarstva koji su učestvovali u javnoj raspravi:**

- **Srđan Damjanović**, načelnik Direkcije za sistemsku infrastrukturu, informaciono komunikacionu infrastrukturu i informacionu bezbjednost;
- **Dušan Krkotić**, šef Odsjeka za informaciono-komunikacionu infrastrukturu i informacionu bezbjednost.

**Podaci o broju i strukturi učesnika u javnoj raspravi:**

U okviru javne rasprave održan je okrugli sto povodom Nacrta Strategije, kojem je prisustvovalo 20 predstavnika ključnih partnera i zainteresovanih strana. U periodu javne rasprave na obaveznom obrazcu 4 propisanom Uredbom o izboru predstavnika nevladinih organizacija u radna tijela organa državne uprave i sprovođenju javne rasprave u pripremi zakona i strategija ("Službeni list CG", broj 41/18), pristigle su u elektronskom obliku primjedbe, predlozi i sugestije od strane Agencije za elektronske komunikacije i poštansku djelatnost – EKIP, Američke privredne komore u Crnoj Gori – AmCham Montenegro i Misije OEBS-a u Crnoj Gori.

**Rezime dostavljenih primjedbi, predloga i sugestija sa navedenim razlozima njihovog prihvatanja, odnosno neprihvatanja:**

| Agencija za elektronske komunikacije i poštansku djelatnost – EKIP | | |
|---|---|---|
| **Br** | **Primjedbe, predlozi, sugestije** | **Odgovor predlagača** |
| **1.** | U strategiji je navedeno, da je detektovano da trenutno u Crnoj Gori ne postoji nadležno tijelo za analizu i gašenje internet stranica s kojih se vrše razna krivična djela, posebno krivična djela dječje pornografije, ksenofobije, terorizma, širenja vjerske i nacionalne mržnje, kao i krivična djela koja se tiču sive ekonomije. Takođe je predloženo, da s tim u vezi, je potrebno razmotriti izmjenu postojećeg Zakona o elektronskim komunikacijama u dijelu omogućavanja preduzimanja aktivnosti na planu gašenja pomenutih internet stranica pod određenim uslovima.<br><br>Napominjemo da se Zakon o elektronskim komunikacijama ne bavi sadržajima na Internetu, tako da se ovaj problem ne može riješiti izmjenama Zakona o elektronskim komunikacija, već samo formiranjem nadležnog tijela, koje će se baviti analizom sadržaja na internetu i koje će imati nadležnosti da naloži uklanjanja neprikladnih sadržaja ili blokiranje pristupa tim sadržajima, a Internet Servis Provajderi, provajderi sadržaja i usluge hostiga će postupati u skladu sa naredbama tog tijela. Zato treba brisati dio koji se poziva da će se izmjenama Zakona o elektronskim komunikacijama riješiti ovo pitanje. Jedan od primjera, kako je ovo riješeno u EU je Uredba (EU) 2021/784 Evropskog Parlamenta i Savjeta od 29.04.2021. godine o borbi protiv terorističkog sadržaja na internetu. | Ne prihvata se.<br>Napominjemo, da za sada internet servis provajderi u Crnoj Gori nemaju mogućnost blokiranja sadržaja na nivou subdomena, jer ih Zakon o elektornskim komunikacijama ne obavezuje na isti. Stoga je namjera da se pristupi izmjeni predmetnog Zakona na način da se predvidi obaveza ISP da posjeduju mogućnost, odnosno tehnologiju za blokiranje sadržaja na internetu. |
| **2.** | S obzirom da će 5G u Crnoj Gori komercijalno biti dostupan krajem 2022. godine, mislimo da je potrebno da jedan od strateških ciljeva bude implementacija paketa instrumenta EU za sigurnost 5G tehnologije (The EU toolbox for 5G security). Na temelju usklađene procjene rizika na nivou EU-a za sigurnost 5G mreža, u paketu instrumenata utvrđen je niz sigurnosnih mjera kojima je cilj stvarno smanjenje rizika i uvođenje sigurnih 5G mreža u cijeloj Evropi. U | Nije prihvaćeno.<br><br>Pitanje uvođenja 5G mobilnih komunikacionih mreža u Crnoj Gori tretirano je kroz druga strateška dokumenta (*MoR o mapi puta za 5G digitalnu transformaciju šest ekonomija Zapadnog Balkana, Strategiju digitalne transformacije Crne Gore 2022-2026. i sl*).<br><br>Pitanje implementacije IPv6 takođe |

| | | |
|---|---|---|
| | njemu se navode detaljni planovi smanjenja za svaki od utvrđenih rizika i preporučuje niz ključnih strateških i tehničkih mjera koje bi trebale preduzeti sve države članice i/ili Komisija.<br><br>Takođe bi se strategijom trebala ubrzati implementacija IPv6, čijom bi se implementacijom povećala sigurnost sajber prostora Crne Gore. | je tretirano Strategijom digitalne transformacije Crne Gore za period 2022-2026. godine. |
| **3.** | Potrebno je dodati definicije i termine kao aneks ove strategije, kao što je urađeno u trenutnoj strategiji, što bi doprinijelo boljem razumijevanju strategije, a samim tim i obaveza koje iz nje proističu. | Prihvaćeno. |
| **4.** | Umjesto termina “operater” u strategiji treba koristi termin “operator”, jer se misli na operatore elektronskih komunikacija i operatore kritičke infrastrukture, jer ih tako definišu Zakon o elektronskim komunikacijama ("Službeni list Crne Gore", br. 40/13, 56/13, 2/17, 49/19) i Zakon o određivanju i zaštiti kritične infrastrukture ("Službeni list Crne Gore", br. 72/19). | Prihvaćeno. |
| **5.** | Mišljenja smo, da treba koristiti domaće izvore podatke, posebno kada su dostupni. Za podatke o broju korisnika interneta, korišćenju interneta, primjenjenim tehnologijama postoje podaci Uprave za statistiku Crne Gore i Agencije za elektronske komunikacije i poštansku djelatnost koji su javno dostupni. | Pri pripremi Nacrta Strategije korišćeni su i domaći izvori podataka kada je riječ o upotrebi informaciono-komunikacionih tehnologija u preduzećima i domaćinstvima u Crnoj Gori. |
| **6.** | U šemi 1*:* Prikaz organizacione strukture u oblasti sajber bezbjednosti, u istom bloku se nalaze Mobilni operatori (pogrešno napisano Mobilni operateri) i Internet servis provajderi, mislimo da nema potrebe posebno izdvajati mobilne operatore jer su oni Internet Servis Provajderi, a svakako će mobilni operatori, fiksni operatori, kao i svi veći operatori elektronskih komunikacija biti prepoznati kao vlasnici kritične infrastrukture. | Prihvaćeno. |
| **7.** | U dijelu koji se odnosi na CIRT, gdje se navodi da predstavlja kontaktu tačku za | Prihvaćeno. |

| | | |
|---|---|---|
| | sve računarske bezbjedonosne incidente, poistovjećen je domen .me sa crnogorskim IP adresnim prostorom, što nije tačno jer se domen .me može koristiti i sa IP adresama koje nijesu iz crnogorskog adresnog prostora. | |

| **Američka privredna komora u Crnoj Gori – AmCham Montenegro** | | |
|---|---|---|
| **Br** | **Primjedbe, predlozi, sugestije** | **Odgovor predlagača** |
| **1.** | Predlaže se jasno utvrđivanje nadležnosti u odnosima CIRT-Agencija, kao i propisivanje finansiranja Agencije.<br><br>***Obrazloženje:***<br>U okviru tačke 3.1. koja se odnosi na kapacitet sajber bezbjednosti, pominje se uvođenje Agencije za sajber bezbjednost u okviru koje bi funkcionisao Tim za odgovor na računarsko bezbjednosne incidente u sajber prostora Crne Gore – CIRT. Ali, istom nije precizirano kakve bi bile nadležnosti Agencije, da li bi se CIRT transformirao u Agenciju, ili bi Agencija bila nezavisna od CIRT-a, pa predlažemo da se Nacrt Strategije dopuni u tom dijelu, kao i predlogom načina finansiranja Agencije, kako bi se ICT zajednica i bankarski sektor na vrijeme upoznali sa eventualnim uvođenjem novih obaveta i troškova u tom smjeru. | Strategijom se predviđa potreba uspostavljanja novog tijela – Agencije, u čiji sastav će ući CIRT (strana 15).<br><br>Dodatno, u okviru strateškog cilja 1, definisan je Operativni cilj 2: Definisanje i uspostavljanje novog i održivog tijela za sajber bezbjednost na nacionalnom nivou.<br><br>U pravcu ostvarivanja navedenog operativnog cilja, biće preduzete prateće aktivnosti definisane kroz Akcioni plan, a koje će podrazumijevati preciziranje nadležnosti, organizacione strukture i potrebnih budžetskih sredstava za funkcionisanje novog organa uprave. |
| **2.** | Potrebno je unaprijediti koordinaciju zarad boljeg odgovora na prijetnje.<br><br>***Obrazloženje:***<br>Radi unapređenja koordinacije i saradnje zainteresovanih strana istaknuta je potreba razmjene podataka sa CIRT-om/Agencijom za sajber bezbjednost, kao i uklanjanje zakonskih barijera u dijelu razmjene informacija, pa smatramo da je ove obaveze potrebno prethodno precizirati odgovarajućim zakonskim i podzakonskim aktima, te u nacrt Strategije predvidjeti i ovaj predlog.<br><br>Smatramo da bi CIRT trebalo da ima povezanost i sa privredom i fizičkim licima na nivou online izvještavanja u slučaju pojave cyber incidenata. Ova komunikacija treba da bude obostrana i da o istom obje strane izvještavaju jedna drugu. | Propisaće se način Pravilnikom o bližem načinu uspostavljanja zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema, kao i koordinacija prevencije i zaštite. |
| **3.** | U okviru tačke 3.3, Sajber kriminal, navedeno je da je potrebno razmotriti izmjenu postojećeg Zakona o elektronskim komunikacijama u dijelu omogućavanja | Nije prihvaćeno.<br>Krivičnim zakonikom već propisana sva krivična djela koja se tiču dječije pornografije, širenje rasne vjerske i |

| | | |
|---|---|---|
| | preduzimanja aktivnosti na planu gašenja internet stranica. Smatramo da je adekvatnije i praktičnije da se razmotri izmjena/dopuna legislative koja uređuje konkretno krivično djelo i krivični postupak. | nacionalne mržnje, terorizma kao i nedozvoljene trgovine, te stoga, navedeno ne treba dodatno mijenjati, već je potrebno razmotriti izmjenu Zakona o elektronskim komunikacijama na način da se predvidi obaveza ISP (koja trenutno nije predviđena) da posjeduju mogućnost, odnosno tehnologiju za blokiranje sadržaja na internetu. |
| **4.** | Predlažemo korekciju radnog vremena CIRT-a, sa osmočasovnog radnog vremena na 24*7*365.<br><br>***Obrazloženje:***<br>Mišljenja smo da je kroz Nacrt ove Strategije potrebno korigovati radno vrijeme CIRT-a, jer trenutno važeće osmočasovno radno vrijeme, pet dana u nedjelji nije u potpunosti optimalno i praktično, s obzirom na to da se sajber kriminal ne dešava nužno radnim danima u radno vrijeme. Zato, predlažemo da se i okviru zasebnog operativnog cilja Strategije razmotri prelazak CIRT-a na radno vrijeme 24/7+365, imajući u vidu ulogu koju ovo tijelo ima, trebala bi i njegova raspoloživost i dostupnost biti na maksimalnom nivou. Pored toga, mišljenja smo da CIRT treba tehnološki i funkcionalno da ima DR (backup lokaciju) zbog kritičnosti ovog servisa. | Prihvata se.<br><br>DZTP (u okviru koje funkcioniše CIRT) trenutno nema dovoljno tehničkih ni kadrovskih kapaciteta za uspostavljanje radnog vremena 24/7 i DR lokacije.<br><br>Nakon formiranja Agencije, u skladu sa opredjeljenim sredstvima, planiraće se i ove aktivnosti kroz indikatore i AP. |
| **5.** | Potrebno je redovno vršiti javnu informisanost o napadima i opasnostima.<br><br>***Obrazloženje:***<br>Ovu vrstu informacije bi trebalo, pored portal otvorenih podataka, objavljivati i na drugim portalima gdje bi korisnici e-usluga mogli biti obavješteni, a u cilju povećanja svijesti privrede i građana. | Informacije se objavljuju na sajtu www.cirt.me. |
| **6.** | Na strani 23, gdje je naglašen plan da se pristupi izmjeni regulative, kako bi i sistemi za registrovanje domena i DNS sistem bili definisani kao kritični sistemi, razmotriti da se regulativom definiše kako su takođe infrastrukture nacionalne eID seme i e-governmenta prepoznati kao KII. | Biće razmotreno kroz implementaciju aktivnosti u okviru Akcionog plana Strategije koje su usmjerene na usklađivanje i izmjenu regulative koja tretira pitanje zaštite KI i KII. |
| **7.** | Na strani 23, u okviru strateškog cilja 2: Uspostavljen sistem zaštite kritične informatičke infrastrukture – a vezano za – "Operativni cilj 4: Usvojen set minimalnih tehnoloških i operativnih mjera koje su neophodne za zaštitu KII", predlažemo da se dodatno prezicira: Usvojen i implementiran | Nije prihvaćeno.<br><br>Kod operativnog cilja 4, pod "tehnološkim mjerama" biće obuhvaćene i preventivne i detektivne mjere". |

| | | |
|---|---|---|
| | set minimalnih preventivnih, detektivnih i korektivnih mjera koje su neophodne za zaštitu KII.<br><br>***Obrazloženje:***<br>U proteklom period su primjećeni problem sa javnom infrastrukturom i servisima – poput sajta MUP-a na kojem je browser upozoravao da konekcija nije privatna (nevalidan sertifikat), nadalje, mobilna verzija sajta eUprave šalje korisniku poruku "Connection Is Not Secure", privremena nedostupnost portal eZdravlje, itd. Mišljenja smo da bi implementacija preventivnih mjera, poput automatizovanog skeniranja ranjivosti i disaster recovery testiranja ukazala na rizike, koji u pomenutim slučajevima nisu značajni, ali bi preduprijedili nastanak nekih budućih događaja koji mogu imati višestruko veći uticaj. | |
| **8.** | Podržavamo prepoznatu potrebu za partnerstvom privatnog i javnog sektora, ali ukazujemo da saradnja treba da bude iskazana i uključivanjem privatnog sektora u rad svih relevantnih državnih organa kroz Savjet za informacionu bezbjednosti, program obuka i slično. | Strategija navodi da je dosadašnje fukcionisanje Savjeta za informacionu bezbjednost ukazalo na neophodnost da se po potrebi u rad Savjeta uključe i predstavnici privatnog sektora.<br><br>Takođe, kako bi se obezbijedila razmjena informacija, unapređenje koordinacije i komunikacije na planu prevencije, prijave i rješavanja sajber incidenata, kao i zaštita KII, između CIRT-a, odnosno budućeg tijela – Agencije za sajber bezbjednost i privatnog sektora, biće planirane aktivnosti u okviru Akcionog plana za implementaciju Strategije, a koje će podrazumijevati i organizovanje periodičnih obuka/brifinga/radionica za predstavnike privatnog sektora. |

| **Misija OEBS-a u Crnoj Gori** | | |
|---|---|---|
| **Br** | **Primjedbe, predlozi, sugestije** | **Odgovor predlagača** |
| **1.** | Implementacija edukativnih programa i obuka o sajber bezbednosti i bezbednom korišćenju informacija su veoma dobrodošli. Predlog je da se tokom razrade AP razmotri proširenje aktivnosti podizanja svesti o sajber bezbednosti na nacionalni nivo organizovanjem javnih kampanja koje će se baviti različitim slojevima društva, tj. svima onima koji koriste neki od e-servisa, uključujući zdravstveni sistem, banke, penzionere, U oktobru se globalno označava mesec podizanja svesti o bezbednosti u sajber prostoru, iskoristiti globalnu kampanju | Prihvaćeno. |

| | | |
|---|---|---|
| | da se pojačaju aktivnosti na nacionalnom nivou u ovoj oblasti.<br><br>***Obrazloženje:***<br>Svi korisnici e-usluga, odnosno pametnih telefona, računara, kreditnih kartica, onlajn platformi itd. su u potencijalnom riziku od sajber kriminala i prevara. Osoblje u zdravstvu, bankama, telekomunikacijama,… poseduje mnogo ličnih i privatnih podataka građana, stoga bi svi slojevi društva trebali biti barem svjesni potencijalnih sajber prijetnji i informisani kako da iste prenuprede ili smanje. | |
| **2.** | Strateški i operativni ciljevi u nacrtu dokumenta su dobro definisani. Akcioni plan nije predstavljen jer je označen kao povjerljiv. Predlog je da se u AP uključe realni i merljivi indikatori što je sigurno i cilj predlagača nacrta.<br><br>***Obrazloženje:***<br>Predlog je da se u AP razviju indikatori za merenje napretka ostvarenih dostignuća, kao i da se identifikuju nedostaci tokom odgovarajućeg perioda implementacije strategije kako bi se mere prilagođavanja mogle uvoditi pravovremeno. | Akcionim planom, u skladu sa propisanim Obrascem i Metodologijom razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata, biće definisani indikatori učinka i indikatori rezultata.<br><br>Strategijom, u poglavlju “Monitoring, izvještavanje i evaluacija” na stranama 31-32, se definiše način identifikovanja “uskih grla” i zastoja u realizaciji aktivnosti na implementaciji Strategije, davanje preporuka za njihovo prevazilaženje, a po potrebi i ažuriranje Akcionog plana. |
| **3.** | Predlog je da se sajber diplomatija uključi u obrazovanje-obuku za karijerne diplomate i visoke zvaničnike u javnim institucijama.<br><br>***Obrazloženje:***<br>Postoji potreba za intenzivnom edukacijom diplomata i visokih državnih službenika i službenica koji predstavljaju državu na nacionalnom i međunarodnom nivou u ovoj oblasti. Trenutno se pominje edukacija i obuka za sve javne službenike javne uprave, MUP-a, UP itd. ali se ne pominje sajber diplomatija. | Prihvaćeno.<br>Kroz aktivnosti AP razmotriće se kreiranje obuke u sklopu UzK za MVP iz oblasti sajber diplomatije. |
| **4.** | U poglavlju obrazovanje, kao modele učenja navesti e-učenje i hibridno učenje.<br><br>***Obrazloženje:***<br>E-učenje i hibridno učenje imaju svoje specifičnosti u poređenju sa tradicionalnim učenjem in-person, te ih stoga treba pomenuti kao takve. | Prihvaćeno. |
| **5.** | Mere za izgradnju poverenja u sajber prostoru OSCE ICT CBMs (OSCE ICT CBM) se mogu razmotriti da se uključe u document kao alat za jačanje regionalne i međunarodne | Kroz Akcioni plan za implementaciju Strategije biće razmotrene dodatne aktivnosti na jačanju implementacije OSCE ICT CBM. |

| | | |
|---|---|---|
| | saradnje u izgradnji poverenja u sajber prostoru.<br><br>***Obrazloženje:***<br>OSCE ICT CBMs su veoma dobro sredstvo u razvoju poverenja između zemalja u sajber prostoru i razvoju zajedničke platforme za razmenu informacija. OEBS je razvio mapu puta sa predlogom za jačanje implementacije OSCE ICT CBMs u Crnoj Gori u aprilu 2020. godine kao smernicu za nacionalne vlasti za jačanje implementacije pomenutih mera. | |

**Mjesto i datum sačinjavanja izvještaja**: Podgorica, 30. novembar 2021.

**Naziv organizacione jedinice Ministarstva odgovornog za pripremu Nacrta Strategije**: Direkcija za sistemsku infrastrukturu, informaciono komunikacionu infrastrukturu i informacionu bezbjednost