Crna Gora
Ministarstvo javne uprave,
digitalnog društva i medija

ZAVRŠNI IZVJEŠTAJ
o sprovođenju Strategije sajber bezbjednosti Crne Gore 2018-2021. godine

Podgorica, decembar 2021. godine

SADRŽAJ

**** Smatra se da se svi izrazi u ovom dokumentu koji su vezani za zanimanja, a upotrijebljeni su u muškom gramatičkom rodu odnose bez diskriminacije i na žene.***

I Uvodni rezime

Ministarstvo javne uprave, digitalnog društva i medija je, u saradnji sa ključim institucijama uključenim u razvoj sajber bezbjednosti - Ministarstvom odbrane, Ministarstvom unutrašnjih poslova, Ministarstvom pravde, ljudskih i manjinskih prava, Ministarstvom prosvjete, nauke, kulture i sporta, Ministarstvom vanjskih poslova, Agencijom za nacionalnu bezbjednost, Direkcijom za zaštitu tajnih podataka i CIRT-om, pripremilo Završni izvještaj o sprovođenju Strategije sajber bezbjednosti Crne Gore za period 2018-2021, sa osvrtom na stepen realizacije aktivnosti iz Akcionog plana za 2021. godinu.

Strategija sajber bezbjednosti Crne Gore 2018-2021, čije sprovođenje je pratio Savjet za informacionu bezbjednost, implementirana je kroz četiri Akciona plana.

Strategija je identifikovala strateške pravce razvoja u ovoj oblasti sa ciljem izgradnje integrisanog, funkcionalnog i efikasnog sajber prostora u skladu sa međunarodnim standardima i principima. Na tom putu, trebalo je ispuniti 8 strateških ciljeva: (1) unaprijediti kapacitete za sajber odbranu, (2) centralizovati sajber ekspertizu i resurse, (3) zaštiti kritičnu informatičku infrastrukturu, (4) ojačati međuinstitucionalnu saradnju, (5) obezbjediti zaštitu podataka, (6) sprovesti edukaciju u oblasti sajber bezbjednosti, (7) osnažiti partnerstvo javnog i privatnog sektora, kao i (8) ojačati regionalnu i međunarodnu saradnju.

Kako bi se dostigli postavljeni strateški ciljevi, definisano je 28 indikatora učinka, te je u periodu 2018-2021. godine ispunjeno njih 13 (47%), delimično su ispunjena 4 (14%), dok nije ispunjeno 11 (39%) indikatora učinka.

Nakon isteka četvorogodišnjeg perioda važenja Strategije kada je riječ o edukaciji i regionalnoj i međunarodnoj saradnji, može se zaključiti da su strateški ciljevi ostvareni, ili uglavnom ostvareni. Na polju snaženja kapaciteta za sajber odbranu i partnerstva javnog i privatnog sektora, te zaštite podataka i jačanja međuinstitucionalne saradnje, dok je primjetan pozitivan trend, dalje aktivnosti ostaju preduslov kontinuiranog napretka u ovim oblastima. Zaštita kritične informatičke infrastrukture i centralizacija sajber ekspertize i resursa, notirane su kao oblasti u kojima nije ostvaren zadovoljavajući napredak u poređenju sa početnim vrijednostima iz 2018. godine. S tim u vezi, moraju biti u posebnom fokusu narednog strateškog dokumenta o sajber bezbjednosti.

1.1. Ključna dostignuća u periodu važenja Strategije

Tokom perioda važenja Strategije, dodatno je unaprijeđen pravni okvir kroz, između ostalog, izmjene i dopune Zakona o informacionoj bezbjednosti („Službeni list CG“, br. br. 14/10, 40/16 i 67/21) i donošenje Zakona o određivanju i zaštiti kritične infrastrukture ("Službeni list CG", br. 72/2019) čime stvoreni preduslovi za preduzimanje aktivnosti na planu utvrđivanja liste KI i KII i obezbjeđivanja njihove adekvatne zaštite.

Važan iskorak napravljen je formiranjem organizacione jedinice u Ministarstvu odbrane i Vojsci Crne Gore nadležne za sajber bezbjednost, čime su unaprijeđeni organizaciono-

upravljački mehanizmi za razvoj sajber odbrane i sajber operacija. Takođe, uspostavljen je Bezbjednosno operativni centar – SOC MO i VCG, u kojem implementirana najsavremenija tehnološka rješenja i obezbjeđena adekvatna prevencija sajber prijetnji, kao i adekatan mehanizam za odgovore na sajber incidente.

Višestruko je osnažena mreža CIRT-ova na nacionalnom i lokalnom nivou, unaprijeđeni su kapaciteti sajber bezbjednosti u Agenciji za nacionalnu bezbjednost, kako u organizacionom tako i tehnološkom pogledu, te reorganizovana i opremljena jedinica Uprave policije za borbu protiv visoko-tehnološkog kriminala. Paralelno, preduzimane su značajne aktivnosti na unapređenju kapaciteta iz oblasti sertifikacije klasifikovanih informacionih sistema, TEMPEST zaštite i rukovanja kripto materijalima, kao i daljoj implementaciji informacionog sistema za razmjenu domaćih tajnih podataka.

U domenu edukacije, realizovane su edukacije za blizu 3.000 učenika, više od 500 nastavnika u cilju podizanja svijesti o sajber bezbjednost. Omogućeno je da se kroz portal za roditelje (i kroz web aplikaciju www.dnevnik.edu.me i kroz mobilne aplikacije), koji služi za praćenje uspjeha djece, šalju informacije roditeljima od strane Ministarstva prosvjete, nauke, kulture i sporta, koje se odnose na bezbjedno korišćenje tehnologije i interneta. Takođe, uspostavljeno je praćenje slučajeva sajber nasilja među učenicima, kroz evidenciju pedagoško-psiholoških službi obrazovno-vaspitnih ustanova u Informacionom sistemu obrazovanja (MEIS).

Kroz dvogodišnje Programe stručnog osposobljavanja i usavršavanja državnih i lokalnih službenika i namještenika Uprave za kadrove, planirane su i realizovane redovne obuke o sajber bezbjednosti, tajnosti podataka, kao i informatičkoj zaštiti podataka.

Na planu međunarodne saradnje, važno notirati da je Crna Gora 2019. godine postala i članica Evropskog centra izvrsnosti za suprotstavljanje hibridnim prijetnjama čime stvorene pretpostavke za razmjenu iskustava i najbolje prakse sa državama članicama NATO i EU, kao i obezbjeđena podrška naporima Crne Gore u izgradnji i jačanju nacionalnih kapaciteta u suprostavljanju hibridnim prijetnjama.

Takođe, 2020. godine, pristupili smo NATO Centru izvrsnosti za kooperativnu sajber odbranu u Talinu, čija je misija jačanje kapaciteta za kooperativnu sajber odbranu, kako NATO-a, tako i samih NATO članica, u cilju unapređenja interoperabilnosti na ovom planu. Centar pruža podršku svojim članicama i NATO-u u oblasti sajber odbrane kroz multidisciplinarna primijenjena istraživanja, ekspertska savjetovanja, obuke i vježbe.

Dodatni napori su učinjeni u pravcu intenziviranja kako međunarodne, tako i bilateralne saradnje, gdje se izdvaja podatak da su predstavnici Crne Gore 2019. potpisali s NATO-om Memorandum o saradnji u sajber odbrani kojim se olakšava razmjena informacija o sajber napadima, a da su 2021. godine Ministarstvo javne uprave, digitalnog društva i medija i Britanska ambasada u Crnoj Gori potpisali Memorandum o sajber partnerstvu.

1.1.1. Dostignuća po institucijama

Ministarstvo javne uprave, digitalnog društva i medija je tokom izvještajnog perioda pristupilo izmjenama i dopunama Zakona o informacionoj bezbjednosti kako bi se obezbjedilo normativno usklađivanje sa Zakonom o tajnosti podataka, a organizacionoj jedinici CIRT koja je u sastavu Direkcije za zaštitu tajnih podataka, stvorile pretpostavke za nesmetano obavljanje poslova u skladu za svojim nadležnostima.

Nastavljeno je sa ulaganjem sredstava u sofisticirana Firewall rješenja koja štite mrežu i serversku opremu organa državne uprave, kao i izvršena analiza rizika informacionih sistema iz nadležnosti Ministarstva.

U saradnji sa Upravom za kadrove u kontinuitetu su realizovane obuke o sajber bezbjednosnoj kulturi, prema Programu stručnog osposobljavanja i usavršavanja državnih i lokalnih službenika i namještenika. Takođe, Ministarstvo je 2018. i 2019. organizovalo tradicionalni godišnji Infofest na kojem su učešće uzeli predstavnici ICT sektora, državnih organa, finansijskih institucija, telekomunikacionog i energetskog sektora, industrije, javnih preduzeća i drugih značajnih privrednih subjekata, kao i renomirani eksperati i nezavisni ICT autoriteti iz više od 20 zemalja. U takvom ambijentu, tokom trajanja Infofesta obrađivane su i teme o sigurnosti informacionih sitema i sajber bezbjednost, kao i mogućnosti snaženja javno-privatnog partnerstva.

Ministarstvo je bilo pokrovitelj druge regionalne Cyber Security konferencije 2019. godine, kao i domaćin IV Digitalnog samita Zapadnog Balkana 2021. godine koji je okupio visoke predstavnike vlada zemalja Zapadnog Balkana, Evropske komisije, Savjeta za regionalnu saradnju, poslovne zajednice i relevantnih aktera. Iste godine, potpisan je Memorandum o sajber partnerstvu sa britanskom ambasadom u Crnoj Gori.

Ministarstvo odbrane i Vojska Crne Gore (MO i VCG) su ostvarili značajan iskorak u dijelu izgradnje sajber kapaciteta, posebno od kada je Crna Gora 2017. godine postala članica NATO. Fokus je bio na ispunjenje strateških ciljeva koji su definisani ovom strategijom i Strategijom sajber bezbjednosti Vojske Crne Gore 2019-2022, kao i dostizanje NATO ciljevima sposobnosti.

U tom smislu, formirane su organizacione jedinice u MO i VCG nadležne za sajber bezbjednost, čime su unaprijeđeni organizaciono-upravljački mehanizmi za razvoj sajber odbrane i sajber operacija. Paralelno sa tim, investirana su značajna sredstva u nabavku i implementaciju najsavremenijih tehnoloških rješenja, koja su kroz uspostavljanje Bezbjednosno operativnog centra – SOC MO i VCG obezbijedila adekvatnu prevenciju sajber prijetnji i mehanizme za odgovore na sajber incidente. Razvoj organizaciono-tehničkih kapaciteta je praćen i intenzivnim trening programom, koji je posebno bio usmjeren na sticanje tehničkih vještina.

MO i VCG su aktivno učestvovali u svim ključnim aktivnostima na nacionalnom i međunarodnom nivou (NATO, OEBS). Ostvarena je i konkretna bilateralna saradnja sa strateškim partnerima, prije svih SAD i UK, posebno u savjetodavnom dijelu, obučavanju sajber eksperata i donacija.

Ministarstvo prosvjete, nauke, kulture i sporta je za period od 2018. do 2021. godine na polju sajber bezbjednosti sprovelo sljedeće aktivnosti:

- Kreirana NetPrijatelji web aplikacija za djecu (www.netprijatelji.edu.me). Ona sadrži edukativnu igricu koja vodi djecu kroz realne životne scenarije i uči ih da prepoznaju, spriječe, zaustave i prijave nasilje na internetu. Aplikacija je namijenjena djeci uzrasta od 9 do 11 godina.
- Kontinuirano se održava stranica o Bezbjednosti djece na internetu unutar Školskog portala (www.skolskiportal.edu.me). Ova stranica sadrži članke, brošure, video zapise, preporuke, uputstva, smjernice, istraživanja, tutorijale, TV emisije, aplikacije, kvizove, priče, kao i linkove za prijavu nelegalnog sadržaja ili sajber incidenta.
- Svake godine osnovne i srednje škole kroz radionice, prezentacije, debate, predstave za učenike, nastavnike i roditelje obilježavaju Dan sigurnog interneta. Takođe se i sa centralnog nivoa uz podršku NVO organizacija, volonterskih klubova, telekomunikacionih kompanija, UNICEF-a, održavaju manifestacije koje su usmjerene na veći broj učesnika iz svih škola.
- Na portalu Uči doma (www.ucidoma.edu.me), koji je kreiran zbog onlajn nastave tokom Covid-19 pandemije, nalazi se između svih ostalih lekcija i lekcija posvećena Bezbjednosti djece na internetu.
- Omogućeno je da se kroz portal za roditelje (i kroz web aplikaciju www.dnevnik.edu.me i kroz mobilne aplikacije), koji služi za praćenje uspjeha djece, šalju informacije roditeljima od strane Ministarstva koje se odnose na bezbjedno korišćenje tehnologije i interneta.
- Uspostavljeno je praćenje slučajeva sajber nasilja među učenicima, kroz evidenciju pedagoško-psiholoških službi obrazovno-vaspitnih ustanova u Informacionom sistemu obrazovanja (MEIS).

Ministarstvo vanjskih poslova je uložilo značajna sredstva u sajber odbranu, odnosno u sofisticirana Firewall rješenja koja štite mrežu i serversku opremu ministarstva. Tendencija je dalje ulaganje u sajber bezbjednost, tačnije širenje mreže i sertifikacija informacionih sistema u zemlji i inostranstvu (DKP).

Ministarstvo pravde, ljudskih i manjinskih prava je u toku trajanja strateškog dokumenta, preciznije početkom 2018. godine počelo sa projektom implementacije standarda bezbjednosti informacija i usklađivanje politike bezbjednosti sa ovim standardom *MEST ISO/IEC 27001:2014*, kao i relevantnim zakonima Crne Gore.

Ministarsvo pravde je u toku uvođenja standarda sprovelo analizu i popis informacione imovine informacionog sistema pravosuđa (ISP), te izvršilo procjenu rizika i izradilo plan tretiranja svakog identifikovanog rizika. Rizici su identifikovani, evaluirani i klasifikovani u nekoliko kategorija, zavisno od vjerovatnoće njihovog nastupanja, te uticaja koji bi mogli imati na sistem ukoliko nastupe. Sastavni dio ovog procesa je bila i procjena ranjivosti ISP-a, koja je imala za cilj da ukaže na slabosti sistema, odnosno bezbjednosne rupe, te predloži kratkoročne, srednjoročne i dugoročne mjere za uklanjanje bezbjednosnih nedostataka. Kao rezultat procjene rizika donijeta je lista kontrola, odnosno organizacionih i tehničkih mjera koje treba preduzeti za ublažavanje svakog identifikovanog rizika.

U nastavku procesa usklađivanja radilo se na izmjenama/dopunama postojećih pravilnika i procedura i donošenju novih, koje bi omogućile implementaciju kontrola predloženih u planu tretiranja rizika, te implementaciji tehničkih rješenja koje nameću pojedine kontrole. Posebna pažnja je posvećena revidiranju „Politike informacione bezbjednosti informacionog sistema pravosuđa“, u cilju obezbjeđivanja dobrog balansa između potreba korisnika, bezbjednosti i dostupnosti sistema. Politika informacione bezbjednosti ISP-a je usvojena, čime su ustanovljeni principi i procedure za dodjeljivanje i kontrolu prava pristupa i privilegije za svaku od institucija u sistemu pravosuđa. Politika informacione bezbjednosti informacionog sistema pravosuđa je usklađena sa relevantnim pravnim okvirom Crne Gore (Zakon o informacionoj bezbjednosti, Zakon o zaštiti podataka o ličnosti, Zakon o tajnosti podataka itd.), te EU konvencijama o zaštiti podataka. U sklopu ovog projekta službenici pravosuđa su stekli odgovarajuće certifikate iz oblasti primjene ovog standarda, tipa: vodeći implementator, interni auditor, Risk menadžer, GDPR - Certified data protection officer.

Implementacija ISO 27001 standarda je nastavljena u 2021. godini u dijelu unapređenja mjera fizičke, informatičke i personalne bezbjednosti korisnika, dok su prepoznati izazovi na primjeni i unapređenju tih mjera.

U cilju povećanja transparentnosti pravosuđa i uvođenja elektronskih servisa (e-servisa) završen je razvoj novog web portala pravosuđa sa migracijom postojećih podataka.

Takođe, u cilju podizanja stepena informacione bezbjednosti u Ministarstvu je implementirano novo rješenje - sistem log mrežnog saobraćaja, koji omogućava pregled događaja(logova) na serverima i mrežnim uređajima koji su dio infrastrukture Ministarstva.

Dodatno, Ministarstvo pravde ima ključnu ulogu u sprovođenju Programa razvoja IKT pravosuđa 2021-2023, te koordinira cjelokupni procesa reforme pravosuđa u IKT segmentu, u cilju uspostavljanja jedinstvenog informacionog sitema koji ce objediniti sudove, tužlilaštvo, zatvorski sistem i postojeće Registre kaznene i prekršajne evidencije u Ministarstvu, sa posebnim naglaskom na interoperabilnost ovih podsistema.

Kao značajne aktivnosti koje su urađene u periodu važenja Strategije sajber bezbjednosti 2018-2021, a posredno se odnose na podizanje nivoa informacione bezbjednosti kada se implementiraju, navodimo:

- Projekat Log Management Sistema i Sistema za prevenciju gubitka podataka na nivou pravosuđa-urađena je tehnička dokumentacija i specifikacija potrebne opreme i softverskih licenci, procedura nabavke se sprovodi preko Delegacije EU u Crnoj Gori.
- U proceduri je izrada Kataloga osjetljivih podataka u okviru ISP-a, Pravila za upravljanje promjenama i Uputstvo za razmjenu podataka između podsistema ISP-a.
- Projekat uspostavljanja Disaster Recovery lokacije ISP-a- završena tehnička dokumentacija i specifikacija potrebne opreme i softverskih licenci – takođe nabavku sprovodi Delagacija EU.

Nastavljene su aktivnosti na projektu implementacije standarda MEST ISO/IEC 27001:2014, u dijelu donošenja i usvajanja internih pravilnika i procedura koji se tiču ISP-a:

- Urađen Business Continuity plan Ministarstva pravde
- Pravila o korišćenju i razvoju podsistema Ministarstva pravde urađena i usvojena.

Takođe, obavljeno je niz specijalističkih obuka za potrebe službenika pravosudnih institucija, kojima se podiže nivo stručnih znanja:

- Basic database training,
- Computer ethical hacking,
- Database administrator,
- ITIL V4 Foundations (SM2188)**,**
- Obuka za softverske/sistem inženjere,
- ECDL (European Computer Driving Licence) Start obuka i certifikacija službenika pravosudnih institucija, od strane akreditovanog ECDL testnog centra.

Usvajanjem Politike informacione bezbjednosti su stvoreni uslovi za pisanje, usvajanje i primjenu procedura koje treba da obezbijede visok stepen zaštite podataka. Imenovanje ISMS menadžera i sprovođenje internog i eksternog audita su neophodni koraci ka cilju postavljenom za 2023 – certifikovanje bar 3 pravosudna organa po standardu ISO 27001. U periodu važenja Strategije ***Agencija za nacionalnu bezbjednost*** je značajno razvila svoje kapacitete iz domena sajber bezbjednosti. To se ogleda kroz sledeće parametere:

- Unaprijeđene su tehničke mogućnosti kroz nabavku novih i unapređenje postojećih hardverskih i softverskih alata za zaštitu i monitoring sopstvene informatičke infrastrukture.
- Unaprijeđene su tehničke i kadrovske sposobnosti u odgovoru na incidentne situacije kroz unapređenje tehničkih sredstava i adekvatne obuke službenika Agencije.
- Angažovanje tehničkih i kadrovskih sposobnosti Agencije u rješavanju incidentnih situacija u crnogorskom sajber prostoru u saradnji sa drugim institucijama, a posebno sa nacionalnim CIRT-om.
- Inteizivirana je saradnja sa drugim institucijama, kako iz javnog, tako i iz privatnog sektora.
- Nastavljena je intenzivna saradnja sa međunarodnim partnerima i NATO-om, u vidu razmjene informacija i iskustava kao i u zajedničkom rješavanju incidentnih situacija vezanih za crnogorski sajber prostor.
- Edukacija službenika na polju sajber bezbjednosti je kontinuirana i ogleda se u učešću pripadnika Agencije na zajedničkim konferencijama, sastancima i obukama kako u Crnoj Gori, tako i u partnerskim zemljama.

Direkcija za zaštitu tajnih podataka, u čijem sastavu se nalazi Nacionalni CIRT, se kontinuirano bavila edukacijom i sprovođenjem aktivnosti iz svojih nadležosti, kao i intezivnom saradnjom sa međunarodnim partnerima u cilju informisanja i unapređenja svojih kapaciteta iz oblasti sertifikacije klasifikovanih informacionih sistema, TEMPEST zaštite i rukovanja kripto materijalima, kao i unapređenjem i daljom implementacijom informacionog sistema za razmjenu domaćih tajnih podataka.

1.2. Izazovi u dostizanju strateških ciljeva

Proglašenje pandemije COVID19 u 2020. godini, koje uslovilo drugačiju prioritizaciju politika i pomjeranje fokusa na ulaganje u zdravstveni sistem i ekonomski oporavak, kao i kašnjenje sa usvajanjem Budžeta za 2021. godinu, koji postao operativan sredinom godine, što se nepovoljno odrazilo na implementaciju aktivnosti iz Akcionog plana za 2021. godinu, usporilo je dinamiku ostvarenja postavljenih strateških ciljeva u drugoj polovini sprovođenja Strategije.

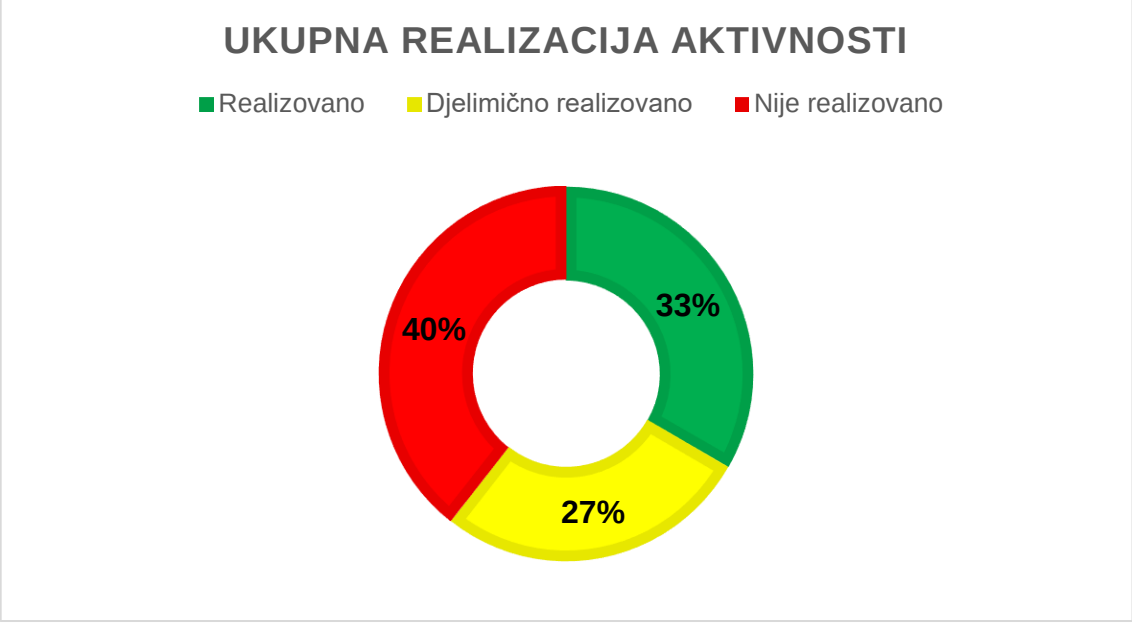
Nedovoljna sredstva opredijeljena u poslednje dvije godine realizacije Strategije, nisu omogućila nastavak trenda povećanja ulaganja u ljudske resurse i tehničke kapacitete.

Poseban izazov je nastao kada je CIRT iz Ministarstva javne uprave, krajem 2020. godine prešao u sastav Direkcije za zaštitu tajnih podataka, što se negativno odrazilo na njegovu funkcionalnost usled nedostatnih prostornih, tehničkih i kadrovskih kapaciteta, kao i realizaciju planiranih aktivnosti na snaženju kapaciteta za prevenciju i suzbijanje svih vrsta sajber napada u Crnoj Gori.

1.3. Stepen realizacije Akcionog plana za 2021. godinu

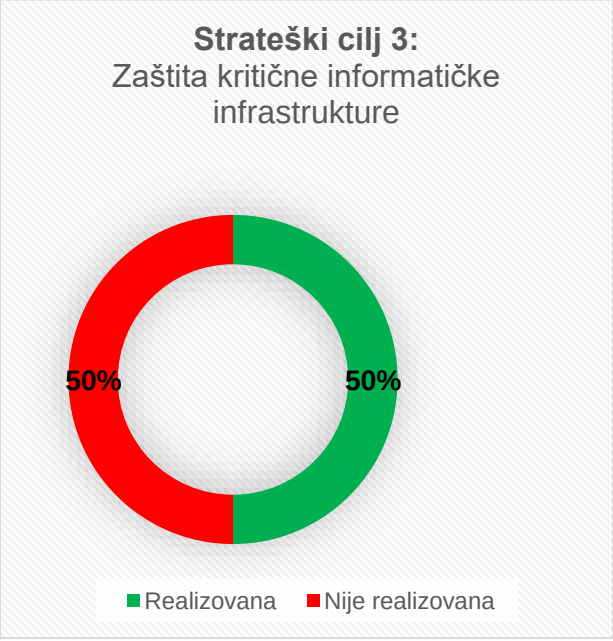
Aktivnosti iz Akcionog plana za 2021. godinu su realizovane samostalno ili u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti.

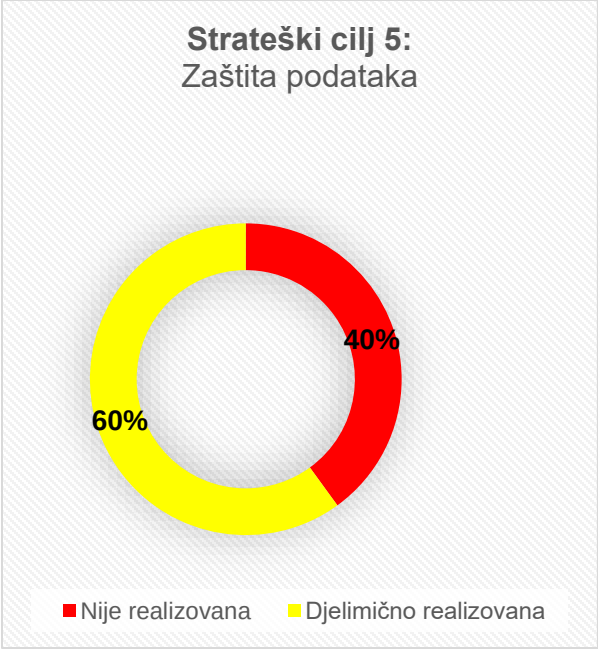
Od 33 planirane aktivnosti Akcionim planom za 2021. godinu, realizovano je 11 (33%), djelimično je realizovano 9 (27%), dok nije realizovano 13 (40%) aktivnosti.



Na osnovu podataka iz Tabele o implementaciji Akcionog plana, može se konstatovati da su nadležni organi većinom realizovali, odnosno djelimično realizovali utvrđene aktivnosti tokom 2021. godine.

U nastavku je dat prikaz realizacije aktivnosti po strateškim ciljevima:





Posmatrajući **po strateškim ciljevima**, može se konstatovati zadovoljavajuća dinamika u realizaciji aktivnosti kada je riječ o edukaciji, partnerstvu javnog i privatnog sektora, kao i regionalnoj i međunarodnoj saradnji. U dijelu međuinstitucionalne saradnje i zaštite podataka, aktivnosti su većinom realizovane, odnosno djelimično realizovane, dok su uočeni izazovi u realizaciji aktivnosti u okviru strateških ciljeva 1, 2 i 3, odnosno u oblasti snaženja kapaciteta za sajber odbranu, centralizacije sajber ekspertize i resursa, te zaštite kritične informatičke infrastrukture.

Na dinamiku realizacije aktivnosti dominantno su uticali:

- usvajanje Budžeta za 2021. godinu u junu 2021. godine;

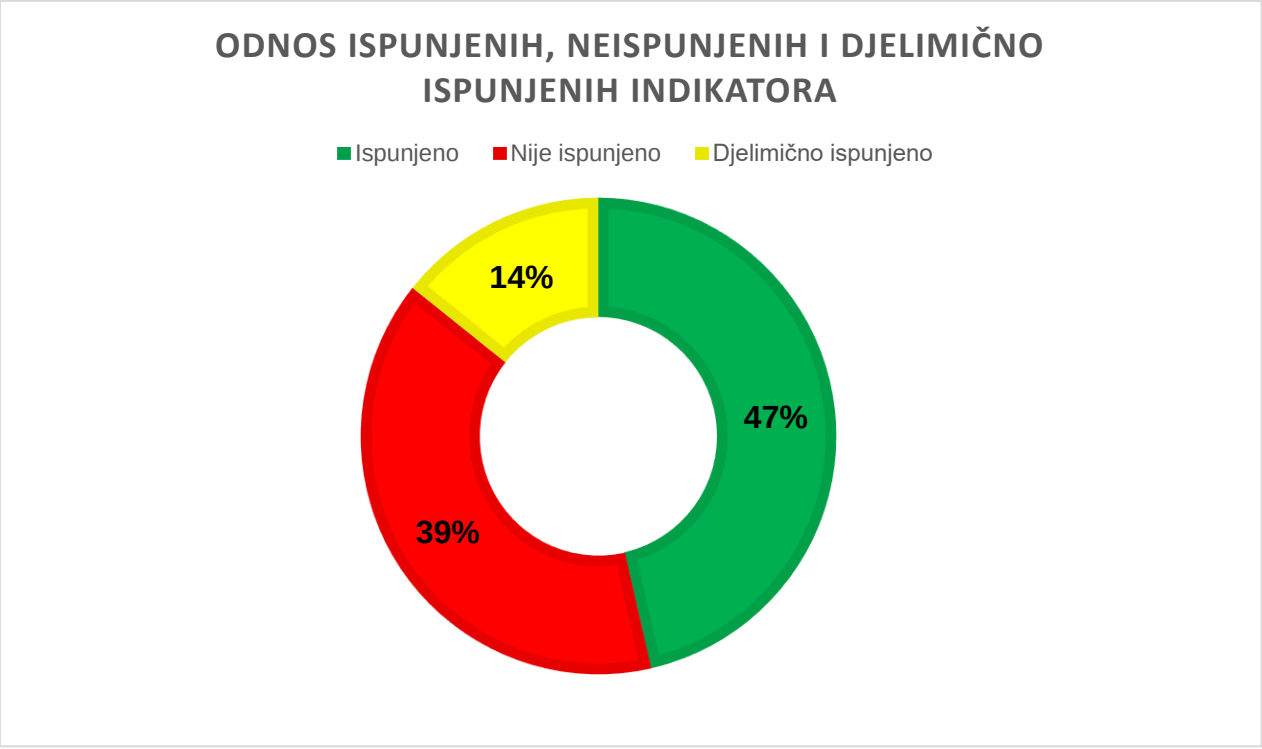
- neopredjeljivanje dovoljno sredstava za realizaciju aktivnosti;
- ambiciozno postavljeni rokovi za realizaciju određenih aktivnosti;
- prelazak CIRT-a iz Ministarstva javne uprave u Direkciju za zaštitu tajnih podataka, bez obezbjeđivanja potrebnih prostornih, kadrovskih i tenhičkih resursa; kao i
- povezanost, odnosno, međusobna uslovljenost određenih aktivnosti gdje u slučaju zastoja u realizaciji jedne aktivnosti je onemogućena realizacija povezanih aktivnosti.

II Informacija o ispunjenosti strateških ciljeva i indikatora

Strategija sajber bezbjednosti Crne Gore 2018-2021. čije sprovođenje je pratio Savjet za informacionu bezbjednost, implementirana je kroz četiri Akciona plana, a u realizaciji planiranih aktivnosti učestvovali su organi državne uprave - Ministarstvo javne uprave, digitalnog društva i medija, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo prosvjete, nauke, kulture i sporta, Ministarstvo vanjskih poslova, Ministarstvo pravde, ljudskih i manjinskih prava, Agencija za nacionalnu bezbjednost i Direkcija za zaštitu tajnih podataka.

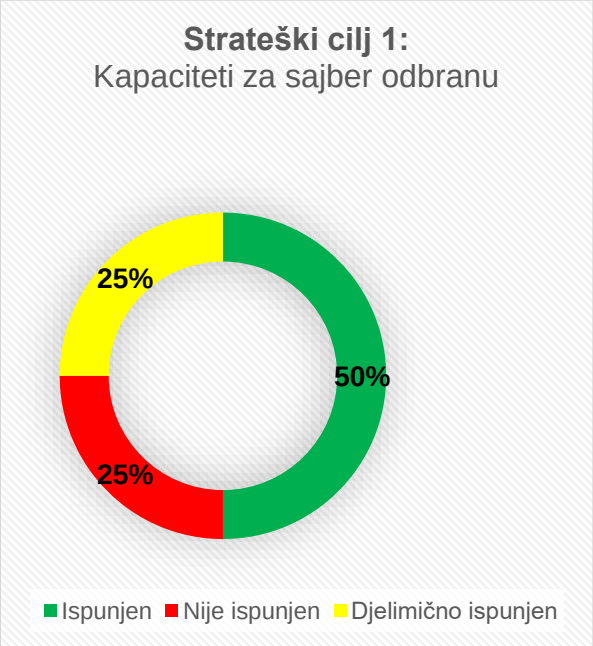
Budući da Strategija nije donijeta u skladu sa Metodologijom razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata koja je donijeta naknadno, ista ne sadrži operativne ciljeve, već 8 strateških ciljeva, 28 pravaca djelovanja i isto toliko indikatora učinka.

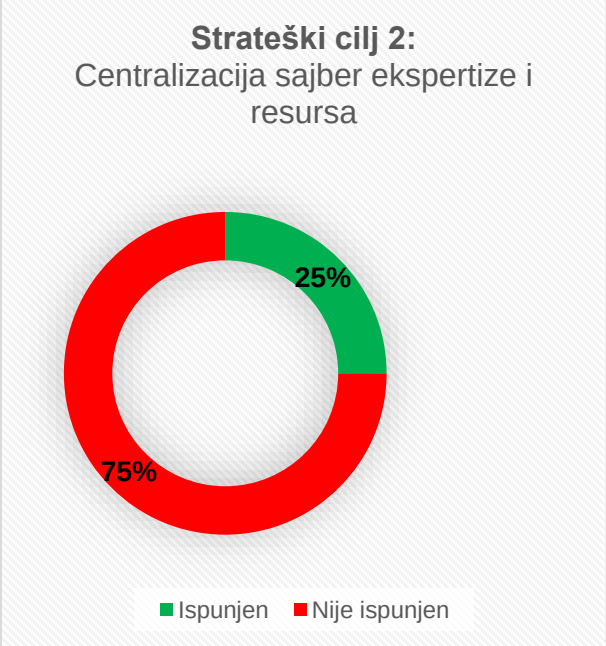
Od 28 indikatora učinka koji su trebali obezbjediti ispunjenje 8 postavljenih strateških ciljeva, ispunjeno je 13 (47%), nije ispunjeno 11 (39%), dok su djelimično ispunjena 4 (14%) indikatora učinka.



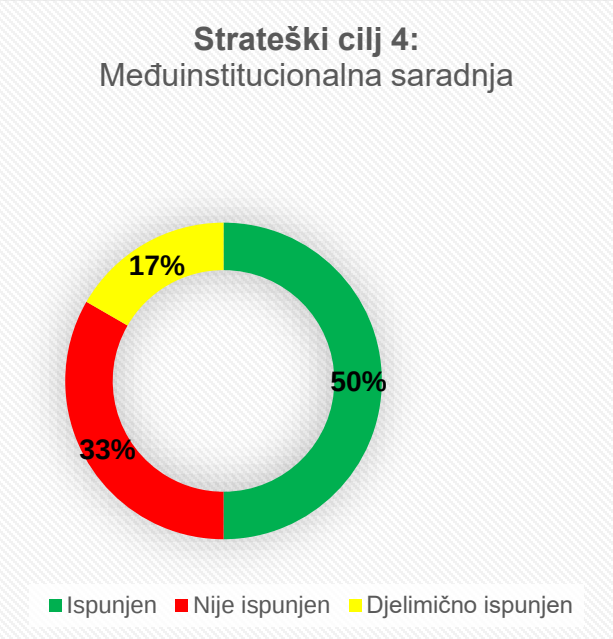
Od 28 indikatora učinka, 4 su trebala biti ispunjena u okiviru strateškog cilja 1, 4 u okviru strateškog cilja 2, 3 u okviru strateškog cilja 3, 6 u okviru strateškog cilja 4, 4 u o okviru strateškog cilja 5, 4 u okviru strateškog cilja 6, 1 u okviru strateškog cilja 7, i 2 u okviru strateškog cilja 8.

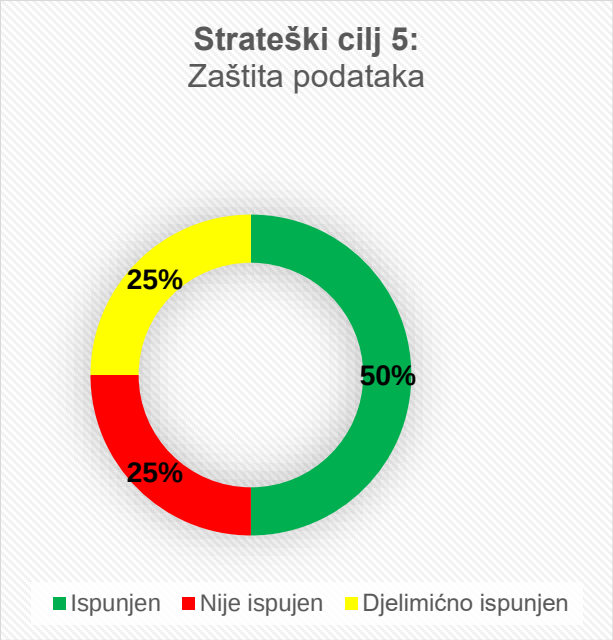
S tim u vezi, u nastavku je grafički prikaz ispunjenosti indikatora učinka u odnosu na strateške ciljeve.

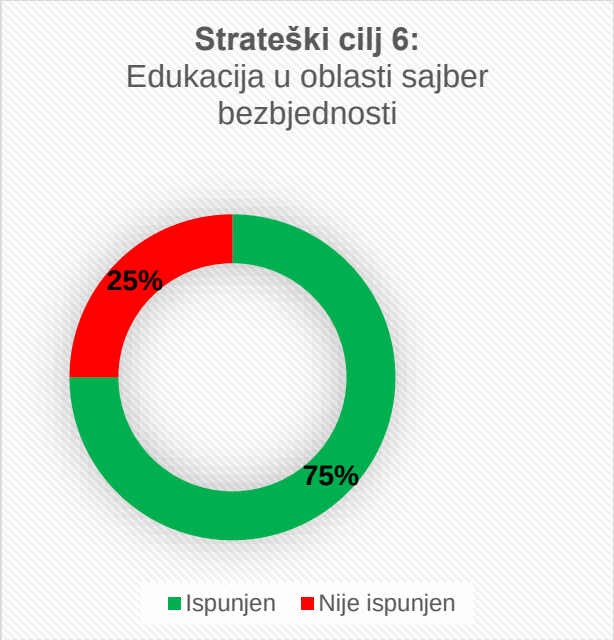

Strateški cilj 1:
Kapaciteti za sajber odbranu
25%
50%
25%
Ispunjen
Nije ispunjen
Djelimično ispunjen


Strateški cilj 2:
Centralizacija sajber ekspertize i resursa
25%
75%
Ispunjen
Nije ispunjen


Strateški cilj 3:
Zaštita kritične informatičke infrastrukture
100%
Nije ispunjeno


Strateški cilj 4:
Međuinstitucionalna saradnja
17%
50%
33%
Ispunjen
Nije ispunjen
Djelimično ispunjen





Kada je riječ o edukaciji i regionalnoj i međunarodnoj saradnji, može se zaključiti da su strateški ciljevi ostvareni, ili uglavnom ostvareni. Na polju snaženja kapaciteta za sajber odbranu i partnerstva javnog i privatnog sektora, te zaštite podataka i jačanja međuinstitucionalne saradnje, dok je primjetan pozitivan trend, dalje aktivnosti ostaju preduslov kontinuiranog napretka u ovim oblastima. Zaštita kritične informatičke infrastrukture i centralizacija sajber ekspertize i resursa, notirane su kao oblasti u kojima nije ostvaren zadovoljavajući napredak u poređenju sa početnim vrijednostima iz 2018. godine. S tim u vezi, moraju biti u posebnom fokusu narednog strateškog dokumenta o sajber bezbjednosti.

STRATEŠKI CILJ 1: Kapaciteti za sajber odbranu

Pravci djelovanja 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 učinka: procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.
Ciljna vrijednost: Povećan broj lokalnih CIRT-ova za 50%.
Rezultat: **Ciljna vrijednost ostvarena.**

Ciljna vrijednost (50% u odnosu na početnu vrijednost – kada je postojao 31 lokalni CIRT) je ostvarena već 2019. godine kada je identifikovano 80 lokalnih timova/kontakt osoba u institucijama koji će neposredno sarađivati sa nacionalnim CIRT-om.

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 učinka: Broj izrađenih analiza rizika u odnosu na broj institucija.
Rezultat: **Ciljna vrijednost ostvarena.**

Sve relevantne institucije koje u djelokrugu svojih nadležnosti imaju pitanja zaštite informacionih sistema, izradile su analize rizika.

Tako Agencija za nacionalnu bezbjednost redovno radi analizu rizika i kontrolu primjene mjera reakcija i kontrolnih mehanizama, kao i ažurira postojeći Registar rizika sa relevantnim predlozima za reakciju i kontrolne mehanizme.

Direkcija za zaštitu tajnih podataka je, prilikom razvoja komunikaciono-informacionog sistema za razmjenu domaćih tajnih podataka između državnih organa Crne Gore, do i uključujući stepen tajnosti „TAJNO“, tokom 2020. i 2021. godine bavila procjenom i analizom rizika za potrebe akreditacije ovog sistema.

Ministarstvo vanjskih poslova je odradilo analizu rizika i prepoznalo ključne ranjive tačke vezano za funkcionisanje KII, generalno funkcionisanje MVP i Diplomatsko konzularnih predstavništava.

U 2020. godni Ministarstvo pravde je u skladu sa Strategijom razvoja IKT pravosuđa 2016-2020. nastavilo aktivnosti na projektu „Implementacija informacione bezbjednosti u informacioni sistem pravosuđa Crne Gore prema međunarodnom i nacionalnom standardu MEST ISO/IEC 27001:2014.“ Urađena je GAP analiza trenutnog stanja u vezi bezbjednosti informacija, na osnovu koje je sačinjen Plan tretiranja rizika. Plan sadrži listu kontrola, odnosno organizacionih i tehničkih mjera koje treba preduzeti za ublažavanje, odnosno eliminisanje svakog identifikovanog rizika. Takođe je urađena i Analiza uticaja na

poslovanje, koja sadrži neophodne procedure na osnovu postojećih poslovnih procesa, IT infrastrukture i bezbjednosne politike u ministarstvu.

U planu je imenovanje ISMS menadžera i sprovođenje internog i eksternog audita, kao neophodnih koraka ka cilju postavljenom za 2023. godinu – certifikovanje bar 3 pravosudna organa po standardu ISO 27001.

Ministarstvo javne uprave, digitalnog društva i medija, kao i Ministarstvo odbrane su takođe uradili analizu rizika informacionih sistema u njihovoj nadležnosti.

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.

Indikator učinka: Broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.
Ciljna vrijednost: Povećanje budžetskih sredstava opredijeljenih za sajber bezbjednost za 20%.
Rezultat: **Ciljna vrijednost djelimično ostvarena.**

Budžetska sredstva opredijeljena za sajber bezbjednost u odnosu na izdvajanja za 2018. godinu nisu povećana za 20% na kraju ciklusa važenja Strategije u Ministarstvu vanjskih poslova, Direkciji za zaštitu tajnih podataka i Ministarstvu pravde, ljudskih i manjinskih prava. Postavljena ciljna vrijednost jeste dostignuta u Ministarstvu javne uprave, digitalnog društva i medija, kao i u Agenciji za nacionalnu bezbjednost.

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.

Indikator učinka: Izrađen izvještaj o minimalnom broju službenika za sajber bezbjednost.
Ciljna vrijednost: Izrađen izvještaj.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Kumulativan izvještaj o optimalnom broju potrebnih službenika na nivou državne uprave koji bi bili zaduženi za sajber bezbjednost u cilju adekvatnog odgovora na prijetnje, izazove, analize rizika i potencijalne napade na informacione sisteme, nije izrađen.

Resori, odnosno organi državne uprave koji u svom djelokrugu rada imaju i pitanja informacione/sajber bezbjednosti na godišnjem nivou definišu kadrovske planove u okviru kojih prepoznaju potrebu za angažovanjem dodatnog kadra koji bi pokrivao, između ostalog, i pitanja sajber bezbjednosti.

STRATEŠKI CILJ 2: Centralizacija sajber ekspertize i resursa

Pravci djelovanja 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 učinka: Broj zaposlenih u CIRT-u.
Ciljna vrijednost: Zaposleno 20 službenika u CIRT-u.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Usled organizacionih izmjena, gdje je CIRT iz Ministarstva javne uprave prešao u sastav Direkcije za zaštitu tajnih podataka, kao i zbog finansijskih ograničenja nametnutih pandemijom COVID19 tokom 2020. godine i usvajanjem Zakona o Budžetu za 2021. godinu tek u junu 2021, broj zaposlenih nije dostigao ciljnu vrijednost.

b. U okviru Nacionalnog CIRT-a sistematizovaće se dva odeljenja - za odgovor na incidente, tehničkog karaktera i za strateške pravce, politike i preventivu.

Indikator učinka: Usvojen pravilnik o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave kojim bi se predvidjelo postojanje dva odjeljenja u CIRT-u.
Ciljna vrijednost: Fomirana dva odjeljenja.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Budući da je CIRT iz Ministarstva javne uprave prešao u sastav Direkcije za zaštitu tajnih podataka (DZTP) krajem 2020. godine, te Pravilnikom o unutrašnjoj organizaciji i sistematizaciji DZTP prepoznat kao Odjeljenje u okviru DZTP, iz organizacionih razloga nisu se mogle u okviru Odjeljenja prepoznati dva nova odjeljenja/odsjeka.

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 učinka: Broj prostorija koje ispunjavaju minumum tehničkih karakteristika, u odnosu na broj predviđenih.
Ciljna vrijednost: Obezbijeđene dvije specijalizovane prostorije.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Planirane aktivnosti na obezbjeđivanju dvije specijalizovane prostorije za funkcionisanje CIRT-a zaustavljene su zbog nemogućnosti opredjeljivanja potrebnih sredstava usled ograničenja nametnutih pandemijom COVID19, kao i zbog odluke da se CIRT premjesti u sastav Direkcije za zaštitu tajnih podataka što se nepovoljno odrazilo i na obezbjeđivanje optimalnih prostornih uslova za rad CIRT-a, sada Odjeljenja za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT).

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 učinka: Broj organizovanih vježbi i uključenih aktera.

Ciljna vrijednost: Organizovane 4 vježbe.
Rezultat: **Ciljna vrijednost ostvarena.**

CIRT je tokom trajanja Strategije ulagao napor u organizaciji različitih događaja iz oblasti sajber bezbjednosti.

U 2018. godini - u saradnji sa Ambasadom Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske i DCAF-om (*The Geneva Centre for the Democratic Control of Armed Forces*) organizovana sajber vježba za kadar zadužen za pitanja informacione bezbjednosti, pretežno za institucije nosioce kritične informatičke infrastrukture. U istoj godini organizovan je i okrugli sto pod nazivom „State-sponsored attacks in cyberspace" u saradnji sa Ambasadom Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske i DCAF-om u okviru projekta „Poboljšanje upravljanja sajber bezbjednošću na Zapadnom Balkanu".

U 2019. godini - u saradnji sa DCAF-om organizovan „Regional TRANSITS I training for CERTs". 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.

Zbog specifične situacije izazvane virusom COVID-19, obuke/vježbe u 2020. godini organizovane su u onlajn okruženju. U saradnji sa DCAF-om, organizovano je šest CompTIA obuka (*CompTIA Linux+, CompTIA Network+, CompTIA Server+, CompTIA Security+, CompTIA CySA+, CompTIA CASP+)* za zaposlene u CIRT-u i za predstavnike lokalnih CIRT-ova odnosno kontakt osoba, koje su održali sertifikovani predavači.

Tokom 2021. godine organizovan je dvonedjeljni onlajn seminar o sajber bezbjednosti u saradnji sa korejskom Agencijom za internet i bezbjednost (KISA) i Svjetskom bankom. Kroz 11 različitih sesija eksperti su elaborirali različite aspekte incidenata u sajber prostoru, počevši od preventivnih mjera, analiza, procjena, aktivnosti koje treba preduzeti, do nivoa međunarodne komunikacije i saradnje o pitanjima sajber bezbjednosti.

STRATEŠKI CILJ 3: Zaštita kritične informatičke infrastrukture

Pravci djelovanja i indikatori:

a. Vlasnici identifikovanih KII dužni su da rade godišnje analize rizika. Nacionalni CIRT tim u saradnji sa ostalim nadležnim CIRT timovima, ima funkciju da uradi reviziju analiza, da pruži pomoć u izradi analiza gdje vlasnici KII nemaju dovoljnih kapaciteta.

Indikator učinka: Broj urađenih analiza u odnosu na broj KII, kao i kvalitet istih.
Ciljna vrijednost: Svi vlasnici identifikovanih KII imaju izrađene analize rizika na godišnjem nivou.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Budući da nije utvrđena lista KII, nije se moglo pristupiti izradi analizi rizika. Ova oblast biće dodatno tretirana kroz novi strateški dokument o sajber bezbjednosti.

b. Donošenje podzakonskih akata za zaštitu KII. Ova regulativa treba da definiše procedure komunikacije između vlasnika KII i nadležnih istitucija, kao i osnovne tehničke i organizacione mjere koje vlasnici KII moraju da ispune.

Indikator učinka: Usvojena Uredba o mjerama zaštite KII.
Ciljna vrijednost: Usvojena uredba o Zaštiti kritične informatičke infrastrukture i njenoj zaštiti.
Rezultat: **Ciljna vrijednost nije ostvarena.**

U skladu sa Zakonom o informacionoj bezbjednosti u cilju zaštite kritične informatičke infrastrukture, organ državne uprave nadležan za informaciono društvo preduzima mjere zaštite te infrastrukture.

Kritičnu informatičku infrastrukturu čine informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa.

Kritičnu informatičku infrastrukturu i način njene zaštite propisaće Vlada Crne Gore.

c. Nacionalni CIRT tim u saradnji sa ostalim CIRT timovima treba da uspostavi i formalizuje strateška partnerstva sa vlasnicima KII, gdje između ostalog treba specificirati razmjenu informacija, načine razmjene informacija i ekspertize.

Indikator učinka: Broj formalizovanih partnerstava sa nosiocima KII.
Ciljna vrijednost: Formalizovana strateška partnerstva sa vlasnicima KII.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Prelaskom CIRT-a iz Ministarstva javne uprave u sastav Direkcije za zaštitu tajnih podataka, nisu mogla biti formalizovana strateška partnerstva sa vlasnicima KII kako to nije, organizaciono, više u nadležnosti CIRT-a.

STRATEŠKI CILJ 4: Međuinstitucionalna saradnja

Pravci djelovanja 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 učinka: Broj imenovanih kontakt osoba, u odnosu na broj institucija.
Ciljna vrijednost: Povećanje broja kontakt osoba za 50% u odnosu na početnu vrijednost.
Rezultat: **Ciljna vrijednost ostvarena.**

Svi organi državne uprave imenovali su kontakt osobu za sajber bezbjednost za saradnju sa CIRT-om.

b. Uspostavljanje javno dostupnog registra sajber eksperata koji bi vodilo nadležno Ministarstvo za ovu oblast.

Indikator učinka: Aktivan registar sajber eksperata.
Ciljna vrijednost: Uspostavljen registar.
Rezultat: **Ciljna vrijednost nije ostvarena**

Ministarstvu javne uprave, digitalnog društva i medija nisu odobrena budžetska sredstva potrebna za uspostavljanje Registra.

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 učinka: Uspostavljena operativna platforma.
Ciljna vrijednost: Uspostavljena operativna platforma.
Rezultat: **Ciljna vrijednost nije ostvarena.**

U periodu 2018-2020, dok je CIRT bio organizaciona jedinica u Ministarstvu javne uprave, opredijeljena su sredstva za realizaciju ove aktivnosti, ali su sredstva preusmjerena za realizaciju drugih aktivnosti, dok je postizanje predmetne ciljne vrijednosti planirano u poslednjoj godini važenja Strategije sajber bezbjednosti Crne Gore 2018-2021. Međutim, sredstva planirana za uspostavljanje operativne platforme u 2021. godini nisu odobrena Direkciji za zaštitu tajnih podataka, u okviru koje sada funkcioniše CIRT.

d. Uspostavljanje inter-resorne radne grupe na tehničkom nivou koja bi okupila eksperte sajber bezbjednosti i stvorila kapacitete za odbranu od sajber napada.

Indikator učinka: Formirana interresorna grupa.
Ciljna vrijednost: Formirana interresorna grupa i usvojen pravilnik o radu.
Rezultat: **Ciljna vrijednost ostvarena.**

Ministarstvo javne uprave, digitalnog društva i medija je 2020. godine formiralo interresornu radnu grupu i donijelo akt kojim definisani njeni zadaci.

e. U cilju efikasnosti, koordinacije i komunikacije inter-resorna radna grupa organizovaće simulacije i vježbe.

Indikator učinka: Broj organizovanih vježbi.
Ciljna vrijednost: Organizovane 4 vježbe
Rezultat: **Ciljna vrijednost ostvarena.**

Institucije nadležne za pitanja sajber/informacione bezbjednosti, koje imaju svoje predstavnike u Savjetu za informacionu bezbjednost i Operativnom interresornom radnom timu, učestvovale su u organizaciji vježbi i simulacija.

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 učinka: Definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.
Ciljna vrijednost: Usvojen Pravilnik.
Rezultat: **Ciljna vrijednost djelimično ostvarena.**

Predlog Pravinika je pripremljen, a njegovo donošenje se očekuje u prvom kvartalu 2022. godine.

STRATEŠKI CILJ 5: Zaštita podataka

Pravci djelovanja 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 učinka: Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.
Ciljna vrijednost: Usvojen odgovarajući pravni akt
Rezultat: **Ciljna vrijednost djelimično ostvarena.**

Interresorni Radni tim za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke formalno je uspostavljen u martu 2019. godine, na inicijativu Direkcije za zaštitu tajnih podataka. Zadatak Radnog tima bio je unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke. U skladu sa ovim zadatkom, članovi radnog tima izradili su Predlog izmjena i dopuna Uredbe o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka, kao i Predlog Pravilnika o certifikovanju komunikaciono-informacionih sistema i procesa za obradu tajnih podataka. Formalno usvajanje predloženih dokumenata očekuje se u 2022. godini.

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 učinka: Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.
Ciljna vrijednost: Zaposlena 3 službenika.
Rezultat: **Ciljna vrijednost ostvarena.**

U Odjeljenju za informatičku zaštitu tajnih podataka Direkcije za zaštitu tajnih podataka zaposleni su informatičari koji se bave 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 opis 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 učinka: Broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.
Rezultat: **Ciljna vrijednost ostvarena.**

Radna mjesta sistematizovana u organima državne uprave u kojima se u većoj mjeri rukuje tajnim podacima obuhvataju i opise poslova vezane za informacionu bezbjednost tajnih podataka.

d. Sertifikacija komunikacionoinformacionih 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 učinka: Broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.
Ciljna vrijednost: Tri sertifikovana sistema.
Rezultat: **Ciljna vrijednost nije ostvarena.**

I pored napora u cilju dostizanja pomenutih standarda nijedan sistem nije još uvijek sertifikovan (ISO/IEC 27001).

Direkcija za zaštitu tajnih podataka razvila je i sertifikovala komunikaciono-informacioni sistem za razmjenu domaćih tajnih podataka između državnih organa Crne Gore, do i uključujući stepen tajnosti „TAJNO"

Tri službenika Direkcije za zaštitu tajnih podataka prošli su obuku i dobili sertifikat za ISO/IEC 27001:2013 eksternog revizora.

U prethodnom periodu Agencija za nacionalnu bezbjednost je intezivno radila na jačanju tehničkih kapaciteta u oblasti sajber bezbjednosti. Iz tog razloga je i izvršena nabavka i implementacija novih tehničkih sredstava koja su doprinijela boljoj zaštiti i bezbjednosti IK sistema Agencije. Takođe je izvršeno i godišnje produženje licenci za softversku i hardversku opremu u cilju postizanja kontinuiranog tehničkog održavanja i upgrade-a postojeće opreme. Odabir opreme i softvera se vrši u skladu sa propisima koji propisuju oblast tajnih podataka, kao i u skladu sa setom standarda ISO 27001.

U Ministarstvu pravde su nastavljene aktivnosti vezano za „Implementaciju informacione bezbjednosti u informacioni sistem pravosuđa Crne Gore prema međunarodnom i nacionalnom standardu MEST ISO/IEC 27001:2014." U Programu razvoja IKT pravosuđa 2021-2023 kroz poseban operativni cilj planirano je Imenovanje ISMS menadžera i sprovodjenje internog i eksternog audita, kao i certifikovanje bar 3 pravosudna organa po standardu ISO 27001.

Dodatno, kako inicijalni projekat podrazumijeva uspostavljanje, primjenu, održavanje i stalno poboljšavanje sistema menadžmenta bezbjednošću informacija ISMS prema međunarodnom standardu ISO/IEC 27001, koje treba da obuhvati sve poslovne procese i IT servise koji se u pravosudnim organima obavljaju, takođe je neophodno njihovo poboljšavanje prema međunarodnim standardima:

- ISO/IEC 27701:2019,
- ISO/IEC 27005:2018,
- ISO 21500:2021,
- ISO 31000:2018,
- ISO 22301:2019,

koji sadrže ITIL najbolju praksu. Tokom 2021. godine su preko UNDP projekta organizovani navedeni kursevi za službenike pravosuđa i MP.

STRATEŠKI CILJ 6: Edukacija u oblasti sajber bezbjednosti

Pravci djelovanja 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 učinka: Broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.
Ciljna vrijednost: 10 konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.
Rezultat: **Ciljna vrijednost ostvarena.**

U periodu trajanja Strategije CIRT je kontinuirano radio na edukaciji u obasti sajber bezbjednosti. Predstavnici CIRT-a učestvovali su na niz regionalnih i međunardnih obuka/konferencija. U cilju podizanja svijesti o bezbjednom korišćenju interneta, CIRT redovno objavljuje sigurnosne savjete. Početkom 2021. godine, CIRT je realizovao onlajn kampanju čiji je moto „Budi oprezan! Život nije bajka!", a koja je imala za cilj podizanje svijesti i znanja o bezbjednom i odgovornom korišćenju interneta, prednostima i bezbjednosnim rizicima, te zaštiti od neprimjerenih sadržaja i negativnih efekata korišćenja interneta. U okviru kampanje, putem društvenih mreža, distribuirani su edukativni materijali koji ukazuju na opasnosti koje vrebaju na internetu i savjetima za zaštititu, kao i bezbjednu kulturu korišćenja interneta i popularnih društvenih mreža koji su pripremljeni u saradnji sa Centrom za upravljanje sektorom bezbjednosti iz Ženeve (DCAF).

Direkcija za zaštitu tajnih podataka, u saradnji sa Upravom za kadrove, u kontinuitetu je sprovodila obuke za državne službenike na temu zaštite tajnih podataka i primjene Zakona o tajnosti podataka.

Ministarstvo javne uprave, digitalnog društva i medija je sa Upravom za kadrove realizovalo obuke u cilju promovisanja i širenja sajber bezbjednosne kulture u skladu sa Programom stručnog osposobljavanja i usavršavanja državnih i lokalnih službenika i namještenika. Ministarstvo je organizovalo i tradicionalni godišnji Infofest u okviru kojeg su obrađivane i teme sajber bezbjednosti, bilo pokrovitelj druge regionalne Cyber Security konferencije 2019. godine, kao i domaćin IV Digitalnog samita Zapadnog Balkana 2021. godine.

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 učinka: Broj objavljenih sadržaja na portalu CIRT-a i broj ažuriranih materijala.
Ciljna vrijednost: Ažuriranje informacija na portalu na dnevnom nivou.
Rezultat: **Ciljna vrijednost nije ostvarena.**

Kako je konstantna edukacija, praćenje trendova i podizanja svijesti od velikog značaja za sajber bezbijednost, CIRT je kontinuirano unapređivao sadržaj na portalu sa materijalima vezanim za ovu oblast, ali se, usled nedovoljno osnaženih kadrovskih kapaciteta, informacije nisu mogle ažurirati na dnevnom nivou.

c. Potrebno je edukovati nastavni kadar kako bi se svjest 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 učinka: Broj obučenih nastavnika po predhodno utvrđenom programu obuke.
Ciljna vrijednost: Obučeno 500 nastavnika.
Rezultat: **Ciljna vrijednost ostvarena.**

Već 2019. godine je ostvarena ciljna vrijednost kada je obučeno 530 nastavnika.

d. Redovan 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 učinka: Broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.
Ciljna vrijednost: Održane radionice za 2.000 učenika.
Rezultat: **Ciljna vrijednost ostvarena.**

Kroz radionice koje su realizovane u obrazovno-vaspitnim ustanovama edukovano je preko 2000 učenika osnovnih i srednjih škola (obuhvaćeno više uzrasta) u svim regijama.

STRATEŠKI CILJ 7: Partnerstvo javnog i privatnog sektora

Pravac djelovanja i indikator:

a. Izrada procedura za razmjenu informacija o sajber incidentima, načinima komuniciranja u slučaju sajber napada, načinima pomoći i kooperaciji između javnog i privatnog sektora.

Indikator učinka: Definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.
Ciljna vrijednosti: Usvojen Pravilnik.
Rezultat: **Ciljna vrijednost djelimično ostvarena.**

Predlog Pravinika je pripremljen, a njegovo donošenje se očekuje u prvom kvartalu 2022. godine.

STRATEŠKI CILJ 8: Regionalna i međunarodna saradnja

Pravci djelovanja i indikatori:

a. Kako razmjena regionalnih i međunarodnih iskustava i najbolje prakse doprinosi jačanju i razvoju sajber bezbjednosti treba nastaviti sa aktivnim učešćem kroz zajedničke vježbe, obuke, sastanke, forume, konferencije, seminare.

Indikator učinka: Broj održanih obuka, konferencija, seminara, vježbi, sastanaka i biće kvalitativnog karaktera.
Ciljna vrijednost: Šest održanih obuka / konferencija / seminara / vježbi / sastanaka.
Rezultat: **Ciljna vrijednost ostvarena.**

Ciljna vrijednost je realizovana i prije datog roka. Naime, sve institucije koje u svojoj nadležnosti imaju pitanja sajber/informacione bezbjednosti su u periodu 2018-2021. u cilju jačanja saradnje na regionalnom i međunarodnom nivou učestvovale na velikom broju sajber vježbi, obuka, konferencija, kao i na više međunarodnih sastanaka i konferencija na teme akreditacije informacionih sistema, kripto zaštite i usaglašenosti sa EU i NATO legislativom iz oblasti zaštite tajnih podataka.

b. U cilju jačanja saradnje sa ključnim međunarodnim institucijama u oblasti sajber bezbjednosti treba nastaviti sa kontinuiranom saradnjom sa organizacijama čiji smo član (FIRST, ITU, NATO) i raditi na pristupanju i promociji novih partnerstava.

Indikator učinka: Broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.
Ciljna vrijednost: Potpisana dva Memoranduma.
Rezultat: **Ciljna vrijednost ostvarena.**

2018 - Vlada je prihvatila Memorandum o razumijevanju između Ministarstva odbrane Republike Estonije, Saveznog ministarstva odbrane SR Njemačke, Ministarstva odbrane Republike Italije, Ministarstva odbrane Republike Letonije, Ministarstva nacionalne odbrane Republike Litvanije, Ministarstva odbrane Republike Slovačke, Ministarstva odbrane Kraljevine Španije, kao i Sjedišta Vrhovnog savezničkog komandanta za transformaciju o funkcionalnom odnosu u Centru izvrsnosti za kooperativnu sajber odbranu i Drugi amandman na Memorandum o razumijevanju između Ministarstva odbrane Republike Estonije, Saveznog ministarstva odbrane SR Njemačke, Ministarstva odbrane Republike Mađarske, Ministarstva odbrane Republike Italije, Ministarstva odbrane Republike Letonije, Ministarstva nacionalne odbrane Republike Litvanije, Ministra odbrane Kraljevine Holandije, Ministra nacionalne odbrane Republike Poljske, Ministarstva odbrane Republike Slovačke, Ministra odbrane Kraljevine Španije i Ministarstva odbrane Sjedinjenih Američkih Država u vezi sa osnivanjem, upravljanjem i radom NATO Centra izvrsnosti za kooperativnu sajber odbranu.

2019 - Predstavnici Crne Gore i NATO potpisali su Memorandum o saradnji u sajber odbrani kojim se olakšava razmjena informacija o sajber napadima.

2021 - Britanska ambasada i Ministarstvo javne uprave, digitalnog društva i medija potpisali Memorandum o sajber partnerstvu.

III Tabela za izvještavanje o implementaciji Akcionog plana za posljednju godinu sprovođenja Strategije

Akcionim planom za 2021. godinu planirano je ukupno 33 aktivnosti, od kojih je 11 realizovano, 9 djelimično realizovano i 13 nerealizovano.

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.**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost na polovini sprovođenja strateškog dokumenta**	**Ciljna vrijednost na kraju sprovođenja strateškog dokumenta**
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 Ostvarena vrijednost: 80 lokalnih timova	Povećati broj lokalnih CIRT-ova za 50% u odnosu na početnu vrijednost Ciljna vrijednost ostvarena. Evidentirano 70 lokalnih timova.
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 Ostvarena vrijednost: 50%	Svi nosioci aktivnosti izradili analizu rizika Ciljna vrijednost ostvarena.
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 opredijeljenih za sajber bezbjednost za 10% u odnosu na početnu vrijednost Ostvarena vrijednost: 10%	Povećanje budžetskih sredstava opredijeljenih za sajber bezbjednost za 20% u odnosu na početnu vrijednost Ciljna vrijednost nije ostvarena.
Indikator učinka d) **Izrađen izvještaj o minimalnom broju službenika za sajber bezbjednost.**	Ne postoji izvještaj	Izrađena analiza sa predlogom aktivnosti Ostvarena vrijednost: napravljen predlog	Izrađen izvještaj Nije izrađen izvještaj.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
1.1 Uspostavljanje strukture lokalnih CIRT-ova, sa revizijom postojećeg stanja	1. Analiza postojećeg stanja	Direkcija za zaštitu tajnih podataka	I	IV			Nisu potrebna sredstva	-	-	
1.2 Povećanje budžetskih sredstava opredijeljenih za sajber bezbjednost u okviru instiicija koje su prepoznate kao nosioci sajber bezbjednosti	Povećanje odobrenog budžeta za minumum 5% kod svih institucija pojedinačno ili povećanje sveukupnog budžeta za 5% u odnosu na 2021. godinu	MJUDDM ANB DZTP MVP MO MUP MPA	II	IV		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026. Zbog potrebe za konsolidacijom finansija kao posledice pandemije COVID19, i pored pozitivnog trenda u pogledu sredstava opredijeljenih za sajber bezbjednost koji je bio prisutan tokom prethodnih godina, u 2021. godini nije došlo do povećanja budžetskih sredstava u nadležnim institucijama, osim u MVP i MJUDDM.	-	-	-	Kako bi se na pravi način odgovorilo dinamičnim izazovima u sajber prostoru, potrebno je u kontinuitetu izdvajati za unaprjeđenje tehnologija za odgovor na sajber prijetnje. Odnosno, potrebno praviti godišnje informacije o potrebnim sredstvima za oblast sajber bezbjednosti, kumulativno i po institucijama, radi pravovremenog planiranja Budžeta.

1.3 Stvaranje uslova za bolju efikasnost službenika koji se bave poslovima sajber i informacionom bezbjednosti i priliv perspektivnog kadra	Izmjene i dopune odluke o dodatku na osnovnu zaradu za obavljanje poslova na određenim radnim mjestima	MJUDDM DZTP DZTP MO ANB MUP MVP MPA MFSS	III	IV		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026.	Budžet		Budžet	Potrebno inicirati prema starješinama resora da se licima angažovanim na poslovima sajber/informacione bezbjednosti obezbjedi dodatak na osnovu zaradu za obavljanje specifičnih poslova.
1.4 Uspostavljanje nove organizacione strukture CIRT-a	Usvojen predlog strukture CIRT-a	DZTP	III	IV		S obzirom na to da je CIRT odjeljenje u okviru DZTP, ne postoji mogućnost da se u okviru istog formiraju dva odsjeka. Poslovi CIRTa-nisu srodni poslovima DZTP, čija je izvorna nadležnost zaštita tajnih podataka. Trenutno rješenje je privremenog karaktera do formiranja novog organa nadležnog za sajber bezbjednost, čija okosnica bi bio CIRT i u okviru kojeg bi se mogla uspostaviti nova organizaciona struktura. Ova aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026.	Nisu potrebna sredstva	-	-	Neophodno je intenzivirati aktivnosti u narednom periodu na planu formiranja novog tijela za sajber bezbjednost u kojem bi CIRT funkcionisao.

1.5 Uspostavljanje tehničkih kapaciteta CIRT-a	1. Nabavljena oprema 2. Nabavljeni sistemi 3. Implementirani sistemi	DZTP	II	kontinuirano		II-IV kvartal 2022. Sredstva planirana za realizaciju ove aktivnosti nisu odobrena DZTP budžetom za 2021. godinu.	Budžet	Opredijeljeno 0,00€	Budžet	Potrebno je osnažiti ljudske i tehničke kapacitete CIRT-a.
1.6 Usklađivanje zakonske regulative u skladu sa planom reorganizacije CIRT-a	1. Izmjene i dopune Zakona o informacionoj bezbjednosti 2. Izmjene i dopune Zakona o zaradama zaposlenih u javnom sektoru 3. Izmjene i dopune Uredbe o organizaciji i načinu rada državne uprave 4. Izmjene Zakona o tajnosti podataka	DZTP 1,2,3,4 MJUDDM 1,3 MFSS 2	II	IV		Aktivnost iz tačke 2 će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026.	Nisu potrebna sredstva	-	-	Ukoliko nije moguće pitanje povećanja zarada riješiti kroz izmjenu Takona o zaradama zaposlenih u javnom sektoru, pristupiti izmjeni i dopuni odluke o dodatku na osnovnu zaradu za obavljanje poslova na određenim radnim mjestima.
1.7 Analiza rizika	Izvršena analiza rizika, izrađen dokument u kome su prepoznati rizici i dat predlog za njihova prihvatanja ili tretman.	MJUDDM ANB DZTP MVP MO MUP MPA	II	IV			Nisu potrebna sredstva	-	-	
1.8 Izrada akta (sistematizacija radnih mjesta Agencije za nacionalnu bezbjednost) u cilju dodatnog definisanja	Izrađen pravni akt sa povećanjem broja radnih mjesta za dva službenika koji se bave	ANB	II	IV		IV kvartal 2022.	Nisu potrebna sredstva	-	-	Potrebno donijeti novi akt o sistematizaciji kojim bi se predvidjelo zapošljavanje dodatnog broja službenika.

radnih mjesta i nadležnosti službenika Agencije koji se bave sajber bezbjednošću	sajber bezbjednošću									

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 kapa- citeti 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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
Indikator učinka a) **Broj zaposlenih u CIRT-u.**	U CIRT-u zaposlene 4 osobe (sistematizovano 6 mjesta)	14 službenika u CIRT Ostvarena vrijednost: 6	20 službenika u CIRT Ostvarena vrijednost: 6.
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 Ostvarena vrijednost: nije realizovano	-
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 Ostvarena vrijednost: nije realizovano	Dvije specijalizovane prostorije Ostvarena vrijednost: nije realizovano
Indikator učinka d) **Broj organizovanih vježbi i uključenih aktera.**	Jedna vježba	Organizovane 2 vježbe Ostvarena vrijednost: organizovane tri vježbe	Organizovane 4 vježbe Ostvarena ciljna vrijednost.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansira nja	Preporuke
2.1 Jačanje administrativnih kapaciteta CIRT-a	Zaposleno 20 službenika	DZTP MO MFSS	III	IV		II-IV kvartal 2023. U CIRT-u je od 2019. godine zaposleno šest (6) službenika. Taj	Budžet	-	Budžet	Neophodno je obezbjediti povećanje broja službenika.

						broj se nije promijenio ni nakon prelaska CIRT-a u sastav DZTP-a.				
2.2 Uspostavljanje bezbjednosnog operativnog centra (CIRT SOC-a)	Nabavljena osnovna oprema za uspostavljanje CIRT SOC-a 1. obezbijeđen prostor oko 50m2 2. 4 TV/monitor (video zid) 3. 6 računara 4. SIEM rešenje 5. nabavljena oprema za kontrolu pristupa 6. opremljena prostorija 7. nabavljeno i implemetirano SIEM rešenje	DZTP	II	IV		I-III kvartal 2022. Uprava za katastar i državnu imovinu od novembra 2020. godine do kraja 2021. godine nije obezbijedila adekvatan prostor za nesmetano funkcionisanje CIRT-a u okviru koga bi se opremila jedna prostorija za SOC.	Budžet	Opredijeljeno 0,00€	Budžet	Potrebno je da Uprava za katastar i državnu imovinu što prije obezbijedi adekvatne prostorije za rad CIRT-a.
2.3 Implementacija mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata	1. Implementacija minimum jednog rješenja, IT sistema a koje će povećati nivo monitoringa, zaštite, upravljanja ranjivostima ili mehanizama za forenziku i analizu.	MJUDDM DZTP CIRT MO ANB MUP MVP MPA	II	IV			Budžet		Budžet	
2.4 Analiza institucionalnih kapaciteta državnih organa u cilju optimizacije radnih mjesta	1. Izrađena analiza trenutnih kapaciteta u državnim organima i predlog za	MJUDDM DZTP CIRT MO ANB MUP MVP	III	IV		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne	Nisu potrebna sredstva	-	-	Potrebno utvrditi broj službenika koji u vodećim institucijama za sajber bezbjednost angažovani na pitanjima

predviđenih za sajber bezbjednost, analiza institucionalnih kapaciteta u privatnom sektoru.	optimizaciju sa fokusom na jačanje sajber ekspertize gdje je potrebno. 2. Izrađena analiza institucionalnih kapaciteta u privatnom sektoru (ISP i dio privrede koji je odgovoran za kritičnu informatičku infrastrukturu) .	MPA				Gore za period 2022-2026				informacione/sajber bezbjednosti, kao i koliko je potrebno zaposliti novog kadra kako bi se obezbjedilo dalje snaženje kapaciteta za prevenciju i odgovor na sajber incidente.

STRATEŠKI CILJ 3 **Zaštita kritične informatičke infrastrukture**	**Vlada Crne Gore će nastaviti da jača kapacitete 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 efikasan 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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
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 Ostvarena vrijednost: izrađena analiza rizika sistema	Svi vlasnici identifikovanih KII imaju izrađene analize rizika na godišnjem nivou Ciljna vrijednost nije ostvarena.
Indikator učinka b) **Usvojena Uredba o mjerama zaštite KII.**	Ne postoji uredba	Pripremljen nacrt uredbe Ostvarena vrijednost: pripremljen nacrt	Usvojena uredba o Zaštiti kritične informatičke infrastrukture i njenoj zaštiti Ciljna vrijednost nije ostvarena.
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 Ciljna vrijednost nije ostvarena.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
3.1 Donošenje podzakonskih akata u vezi sa KII	1. Pripreljmljen predlog 2. Predlog usvojen	MUP	II	IV			Nisu potrebna sredstva	-	-	
3.2 Opremljena specijalizovana prostorija za forenziku i analitiku	1. Obezbjeđena prostorija 2. Nabavljeno 6 računara 3. Nabavljena kontrola pristupa 4. Instalirana open source rešenja za monitoring 5. Nabavka alata za forenziku i analitiku	DZTP	III	Kontinuirano		I-III kvartal 2022. Uprava za katastar i državnu imovinu od novembra 2020. godine do kraja 2021. godine nije obezbijedila adekvatan prostor za nesmetano funkcionisanje CIRT-a u okviru koga bi se opremila jedna prostorija za SOC.	Budžet	-	Budžet	Potrebno je da Uprava za katastar i državnu imovinu što prije obezbijedi adekvatne prostorije za rad CIRT-a. Potrebno je planirati dovoljno sredstava u Budžetu za nabavku nedostajeće opreme.

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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
Indikator učinka a) **Broj imenovanih kontakt osoba, u odnosu na broj institucija.**	31 kontakt osoba	Povećanje broja kontakt osoba za 30% u odnosu na početnu vrijednost Ostvarena vrijednost: 109 kontakt osoba	Povećanje broja kontakt osoba za 50% u odnosu na početnu vrijednost Ciljna vrijednost je ostvarena.
Indikator učinka b) **Aktivan registar sajber eksperata.**	Ne postoji registar	Napravljena tehnička specifikacija	Uspostavljen registar Ciljna vrijednost nije ostvarena.

Indikator učinka c) **Uspostavljena operativna platforma.**	Ne postoji platforma	Pripremljena tehnička specifikacija	Uspostavljena platforma Ciljna vrijednost nije ostvarena
Indikator učinka d) **Formirana interresorna grupa.**	Ne postoji	Formirana grupa Ostvarena vrijednost: formirana grupa	Usvojen pravilnik o radu Donijet akt kojim definisani zadaci interresorne grupe.
Indikator učinka e) **Broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.**	Jedna vježba	Organizovane 2 vježbe Ostvarena vrijednost: organizovane dvije vježbe	Organizovane 4 vježbe Ciljna vrijednost ostavrena.
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 Nije usvojen Pravilnik

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
4.1 Platforma za razmjenu informacija	Operativna platforma	DZTP	III	IV		II-IV kvartal 2022. Sredstva planirana za realizaciju ove aktivnsti nisu odobrena DZTP-u Budžetom za 2021. godinu.	Budžet	-	Budžet	Potrebno u Budžetu DZTP predvidjeti sredstva za ovu aktivnost naredne godine, kao i intenzivirati aktivnosti na uspostavljanju platforme.
4.2 Nastavak rada Operativnog radnog tima, kao jedan od modela optimizacije zajedničkih napora u domenu prevencije sajber prijetnji i odgovora na	1. Usvojene izmjene i dopune Odluke o obrazovanju Operativnog radnog tima. 2. Napravljen plan za odgovore na incidente koji imaju uticaj na veći dio	MJUDDM DZTP MO ANB MUP MVP MPA AEKIP Predstavnici ISP	II	III		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026.	Budžet		Budžet	

kompjuterske incidente	sistema državnih organa. Plan treba da sadrži definisane uloge i raspoložive stručne i tehničke kapacitete po institucijama 2. Obezbjeđivanje naknade za članove tima 4. Obezbjeđena i opremljena prostorija za rad tima									
4.3 Saradnja kroz Savjet za informacionu bezbjednost	1. Savjet prati i daje preporuke za sve projekte koji se odnosne na povećanje mjera prevencije sajber prijetnji, a koja su dokumentova u zapisniku sa sastanaka. 2. Savjet predložio plan obuke za Operativni radni tim za period od 1 godine, sa ciljem dostizanja adekvatnog nivoa vještina.	MJUDDM	II	IV			Nisu potrebna sredstva	-	-	

4.4 Zajednički program edukacije	Zajedničko učešće na jednom kursu, obuci ili konferenciji	MJUDDM DZTP MO ANB MUP MVP MPA AEKIP	I	IV			Sredstva iz donacija		Sredstva iz donacija	
4.5 Izmjene i dopune pravilnika o radu CIRT-a	Unaprijeđen pravilnik u dijelu razmjene informacija i izvještavanja	DZTP	I	IV		Pripremljen Pravilnik, dok se usvajanje očeuje u I kvartalu 2022.	Nisu potrebna sredstva	-	-	Potrebno donijeti Pravilnik o načinu razmjene informacija i izvještavanju o incidentima.
4.6 Uspostavljanje mogućnost slanja informacija roditeljima kroz portal za rodItelje (i kroz web aplikaciju www.dnevnik.edu.me i kroz mobilne aplikacije) od strane Ministarstva koje se odnose na bezbjedno korišćenje tehnologije i interneta	Razmjena informacija kroz različite aplikacije	MPNKS	II	III			Nisu potrebna sredstva	-	-	

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.**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost na polovini sprovođenja strateškog dokumenta**	**Ciljna vrijednost na kraju sprovođenja strateškog dokumenta**
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 Ostvarena vrijednost: formirana radna grupa i izrađen predlog	Usvojen odgovarajući pravni akt Izrađen Predlog izmjena i dopuna Uredbe o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka, kao i Predlog Pravilnika o certifikovanju komunikaciono-informacionih sistema i

			procesa za obradu tajnih podataka. Formalno usvajanje predloženih dokumenata očekuje se u 2022. godini.
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 Ostvarena vrijednost: 3 službenika	Zaposlena 3 službenika Ciljna vrijednost ostvarena.
Indikator učinka c) **Broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.**	Nema	Prepoznati radna mjesta i predložiti izmjene sistematizacije	Usvojena sistematizacija Radna mjesta sistematizovana u organima državne uprave u kojima se u većoj mjeri rukuje tajnim podacima obuhvataju i opise poslova vezane za informacionu bezbjednost tajnih podataka.
Indikator učinka d) **Broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.**	Nema	Jedan sertifikovani sistem Ostvarena vrijednost: jedan sertifikovan sistem.	Tri sertifikovana sistema Nije ostvarena ciljna vrijednost.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
5.1 Unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa za obradu tajnih podataka	1.Usvojena Uredba o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka 2.Usvojen Pravilnik o certifikovanju komunikacion o informacionih sistema	DZTP	II	IV		2022. Izrađeni su predlozi propisa, a formalno usvajanje se očekuje u 2022. godini.	Nisu potrebna sredstva	-	-	
5.2 Obuke po pitanju implementacije standarda informacione	Sertifikovano minimum po jedan službenik iz instituicija,	MJUDDM DZTP MO ANB MUP	II	IV		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber	Budžet		Budžet	Potrebno sertifikovati službenike u institucijama nadležnim za pitanja

bezbjednosti (sertifikovani implementator, interni revizor)	poželjno standard.	MVP MPA				bezbjednosti Crne Gore za period 2022-2026 Postoji mogućnost da će se do kraja tekuće godine obezbijediti obuka za 1-2 službenika MO i VCG. Službenici Odjeljenju za informatičku zaštitu tajnih podataka u DZTP sertifikovani za eksternog revizora ISO 27000. U 2021. godini nije sertifikovan nijedan službenik.				informacione sigurnosti kroz pravovremeno planiranje potrebnih budžetskih sredstava.
5.3 Stvaranje uslova za prijem i čuvanje podataka označenih stepenima tajnosti “Povjerljivo”, “Tajno” i “Strogo tajno” odnosno, do stepena tajnosti koji je potreban instituciji.	Institucije koje imaju potrebu da vrše razmjenu tajnih podataka su obezbijedile adekvatne prostorije, računarsku opremu ili sistem (u slučaju da je potreban) za prijem, obradu i čuvanje tajnih podataka a nakon toga u skladu sa zakon iste sertifikovali od strane DZZTP	MJUDDM DZTP MO ANB MUP MVP MPA	II	Kontinuirano		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026 MO i VCG imaju uslove da vrše razmjenu tajnih podataka. U toku je izrada dokumentacije za sertifikaciju novog informacionog sistema.	Budžet		Budžet	Potrebno planirati sedstva za obezbjeđivanje prostornih i tehničkih kapaciteta za prijem i čuvanje podataka označenih stepenima tajnosti u institucijama u kojima za to postoji potreba.

5.4 Primjena standarda iz oblasti informacione bezbjednosti, u skladu sa zakonom	Sve institucije koje su vlasnici informacionih sistema su unaprijedile postojeće propise ili izradile nove, sa ciljem ispunjenja standarda iz oblasti informacione bezbjednosti.	MJUDDM DZTP MO ANB MUP MVP MPA	II	IV		Aktivnost će se realizovati kroz dostizanje strateških ciljeva Strategije sajber bezbjednosti Crne Gore za period 2022-2026 MO i VCG će do kraja godine završiti proces revizije postojećih i izrade novih pravila i procedura, kako bi se uskladili sa standardima informacione bezbjednosti, u skladu sa zakonom.	Nisu potrebna sredstva	-	-	
5.5 Prepoznati ključne institucije u kojima treba urgentno uraditi penetraciono testiranje	Prepoznate ključne institucije u kojima trena urgentno uraditi penetraciono testiranje	DZTP	III	IV		II-IV kvartal 2022.	Nisu potrebna sredstva	-	-	Predvidjeti ovu aktivnost u okviru AP nove Strategije sajber bezbjednosti 2022-2026.

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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
Indikator učinka a) **Broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.**		5 konferencija/obuka/gostovanja u emisijama Ostvarena vrijednost: 5	10 konferencija/obuka/gostovanja u emisijama Ciljna vrijednost ostvarena
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 Ostvarena vrijednost: ažuriranje po potrebi	Ažuriranje informacija na portalu na dnevnom nivou Ostvarena vrijednost: ažuriranje po potrebi

Indikator učinka c) **Broj obučenih nastavnika po predhodno utvrđenom programu obuke.**	Definasan program obuke	Obučeno 250 nastavnika Ostvarena vrijednost: 530 nastavnika	Obučeno 500 nastavnika Ciljna vrijednost ostvarena već 2019.
Indikator učinka d) **Broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.**	Definisan plan aktivnosti	Održane radionice 1.000 učenika Ostvarena vrijednost: 2.600 učenika	Održane radionice 2.000 učenika Ciljna vrijednost ostvarena.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
6.1 Edukacija lokalnih i državnih službenika i namještenika na temu sajber bezbjednosti a koji ne obavljaju poslove sajber bezbjednosti i nijesu iz IT struke	1. Sve ključne institucije su realizovale periodične “security awareness” programe 2. Ministarstvo javne uprave digitalnog društva i medija u saradnji sa Upravom za kadrove realizovalo security awareness” programe u kojima su učestvovali minimum 150 državnih i lokalnih službenika	MJUDDM DZTP MO ANB MUP MVP MPA	II	IV		2022-2023.	Budžet		Budžet	
6.2 Profesionalni treninzi iz oblasti sajber bezbjednosti za sajber eskperte	Minimum 10 službenika je pohađalo profesionalne treninge i kurseve	MJUDDM DZTP MO ANB MUP MVP MPA	II	IV			Budžet/donacije		Budžet/donacije	

iz ključnih institucija										
6.3 Podizanje svijesti građana o bezbjednom korišćenju internet	1.Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa minimum 300 osoba 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. 4. Organizovanje focus grupa na temu sajber bezbjednost sa raznim ciljnim grupama za minimum 100 osoba	DZTP MPNKS	II	IV		Tačke 1, 2 i 3 su realizovane, dok tačka 4 nije.	Budžet/donacije		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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
Indikator učinka a)	Ne postoji pravilnik	Definsane procedure	Usvojen pravilnik

Definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.		Ostvarena vrijednost: definisan način za razmjenu informacija.	Pripremljen Pravilnik, očekuje se usvajanje.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
7.1 Unapređenje saradnje sa privatnim sektorom i akademskom zajednicom	1.Uspostavljen formalan vid saradnje u skladu sa svojim nadležnostima, u kojem će biti definisan način saradnje u cilju obostranog jačanja. 2. Minumim 1 zajednička sajber konferencija ili vježba u kojoj bi uzeli učešće 3 institucija iz privatnog ili akademskog sektora	Svi	I	IV			Budžet/donacije		Budžet/donacije	
7.2 Unapređenje zakonskih preduslova za jačanja saradnje sa privatnim sektorom, a u cilju podizanja nivoa kolektivne prevencije sajber prijetnji	Izmjene i dopune Zakona o informacionoj bezbjednosti i drugih akata, kojima će se jasno definisati međusobna prava i obaveze sa ciljem jačanja otpornosti na	DZTP MJUDDM	II	IV		I kvartal 2022. Zakon izmijenjen, ali podzakonski akt nije usvojen.	Nisu potrebna sredstva	-	-	

	sajber prijetnje.									

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.**

Indikator učinka	Početna vrijednost	Ciljna vrijednost na polovini sprovođenja strateškog dokumenta	Ciljna vrijednost na kraju sprovođenja strateškog dokumenta
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 / sastanka Ostvarena vrijednost: četiri.	Šest održanih obuka / konferencija / seminara / vježbi / sastanaka Ciljna vrijednost ostvarena.
Indikator učinka b) **Broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.**	Ne postoji nijedan	Jedan memorandum Ostvarena ciljna vrijednost.	Dva memoranduma Ciljna vrijednost ostvarena.

Aktivnost	Indikator rezultata	Nadležna institucija	Datum početka (kvartal)	Planirani datum završetka (kvartal)	Status realizacije	Novi rok za realizaciju (uz obrazloženje)	Sredstva planirana za sprovođenje aktivnosti	Sredstva realizovana	Izvor finansiranja	Preporuke
8.1. Jačanje bilateralne i multilateralne saradnje na polju sajber bezbjednosti	Realizovana minimum 1 aktivnosti (kursevi, radionice, konferencije, vježbe i drugo).	MJUDDM DZTP MO ANB MUP MPA MVP	I	IV			Budžet/donacije		Budžet/donacije	
8.2. Jačanje saradnje sa NATO, OEBS i drugim međunarodnim organizacijama	Učešća na redovnim događajima u organizaciji NATO, OEBS i drugih međunarodnih organizacija (sastanci komiteta, bordova, radnih grupa, konferencije,	MJUDDM DZTP MO ANB MVP MPA AEKIP	I	IV			Budžet/donacije		Budžet/donacije	

	obuke, seminari, radionice i drugo)									
8.3. Izrada pravilnika i procedura za razmjenu informacija o sajber incidentima	Pripremljen predlog pravilnika i procedura za razmjenu informacija o sajber incidentima	DZTP	II	IV		I kvartal 2022. Predlog Pravilnika pripremljen, očekuje se usvajanje.	Nisu potrebna sredstva	-	-	

IV Nalazi evaluacije

Kada je riječ o nalazima evaluacije, treba napomenuti da je Strategija sajber bezbjednosti Crne Gore za period 2018-2021. godine donijeta u decembru 2017. godine, te da nije rađena u skladu sa važećom Metodologijom razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata budući da je ista donijeta naknadno.

S tim u vezi, Strategija nije predvidjela sprovođenje evaluacije, zbog čega ovaj izvještaj ne sadrži njene nalaze.

Novim strateškim dokumentom - Strategijom sajber bezbjednosti Crne Gore za period 2022-2026. godine, planiranja je evaluacija kako bi se obezbijedilo preciznije izvještavanje, a kroz nalaze evaluacije jasne smjernice za dalje planiranje politike u oblasti sajber bezbjednosti.

V Osvrt na planirana i utrošena finansijska sredstva

Kako Strategija sajber bezbjednosti Crne Gore za period 2018-2021. godine nije rađena u skladu sa Metodologijom razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata, nije postojala obaveza navođenja finansijskih pokazatelja u vezi sa realizacijom aktivnosti.

Na toj liniji, ne može se govoriti o egzaktnim iznosima planiranih i utrošenih sredstava za realizaciju aktivnosti iz četiri akciona plana, čijim sprovođenjem se trebalo obezbjediti dostizanje postavljenih strateških ciljeva. Dostupna je stoga samo okvirna procjena, napravljena na temelju dostavljenih informacija nadležnih institucija, u skladu s kojom, tokom 2018-2021. godine utrošeno je 1 700 000 eura.

Važno napomenuti da su aktivnosti planirane kroz akcione planove za sprovođenje Strategije realizovane iz sredstava Budžeta za godine trajanja strateškog dokumenta, odnosno iz godišnjih budžeta nosilaca aktivnosti, kao i kroz bilateralnu i međunarodnu saradnju, donacije i programe.

VI Preporuke za naredni ciklus planiranja politika

Završni izvještaj o implemetaciji Strategije pokazao je da kada je riječ o edukaciji i regionalnoj i međunarodnoj saradnji, može se zaključiti da su strateški ciljevi ostvareni, ili uglavnom ostvareni. Svakako, to ne znači nužno da ove ciljeve ne treba dodatno nadgraditi i stepen njihove ostvarenosti povećati u okviru novog strateškog dokumenta. Na ovaj način se najefikasnije i dugoročno održivo obezbjeđuje adekvatno upravljanje sajber bezbjednošću u Crnoj Gori.

Na polju snaženja kapaciteta za sajber odbranu i partnerstva javnog i privatnog sektora, te zaštite podataka i jačanja međuinstitucionalne saradnje, dok je primjetan pozitivan trend, planiranje novih operativnih ciljeva i indikatora učinka ostaju preduslov kontinuiranog napretka u ovim oblastima.

Zaštita kritične informatičke infrastrukture i centralizacija sajber ekspertize i resursa notirane su kao oblasti u kojima nije ostvaren zadovoljavajući napredak u poređenju sa početnim vrijednostima iz 2018. godine, pa je u novom strateškom dokumentu potrebno posebnu pažnju posvetiti ovim strateškim ciljevima.

Preporuke po institucijama:

SAJVET ZA INFORMACIONU BEZBJEDNOST

- Monitoring sprovođenja Strategije i pratećih AP mora biti unaprijeđen kako bi omogućio pravovremeno identifikovanje prepreka na planu ispunjavanja planiranih aktivnosti u predviđenim rokovima i pružanje preporuka za njihovo prevazilaženje.
- Potrebno je prema starješinama i upravljačkom kadru u javnoj upravi adresirati pitanje opredjeljivanja potrebnih sredstava nadležnim resorima za jačanje kapaciteta za sajber odbranu kroz snaženje operativnih, ljudskih i tehničkih resursa.
- Interresorna saradnja treba da bude dodatno unaprijeđena kroz umrežavanje i kontinuirano usavršavanje službenika koji se bave pitanjima sajber bezbjednosti, uz obezbjeđivanje optimalnih podsticajnih mjera, kako bi se smanjio „odliv“ stručnog kadra.
- Potrebno je osmisliti modele interresornog djelovanja, kao i modele takve vrste saradnje u domenu privatno-javnog partnerstva.
- Na osnovu analize trenutne organizacione strukture u oblasti sajber bezbjednosti, kao i analize položaja, kapaciteta i nadležnosti CIRT.ME, potrebno ozbiljno razmotriti formiranje posebnog organa nadležnog za sajber bezbjednost.

MINISTARSTVO JAVNE UPRAVE, DIGITALNOG DRUŠTVA I MEDIJA

- Oblast zaštite kritične informatičke infrastrukture (KII) mora biti dodatno unaprijeđena, kroz a) utvrđivanje KII, b) definisanje osnovnih mjera zaštite KII od sajber prijetnji, i c) nadzor nad primjenom propisanih mjera.
- Edukacija zaposlenih u javnoj upravi o sajber bezbjednosti i sigurnom korišćenju ICT-a mora ostati temelj strateškog odgovora na sajber izazove i prijetnje.

MINISTARSTVO ODBRANE

- Nastaviti sa primjenom tehnoloških rješenja i unapređenjem znanja stručnog kadra, kako bi se dodatno osnažili mehanizmi prevencije sajber prijetnji i odgovor na sajber incidente, kao i zaštita informaciono-komunikacionih sistema MO i VCG.
- Obezbjediti dalju nadogradnju postojeće i razvijanje nove sajber sposbnosti, kako bi obezbijedili kapacitete za sajber odbranu, u skladu sa nacionalnim i NATO strateškim ciljevima.

MINISTARSTVO UNUTRAŠNJIH POSLOVA – UPRAVA POLICIJE

- Pitanje snaženja kapaciteta i saradnje organa za sprovođenje zakona i pravosuđa na planu borbe protiv sajber kriminala, mora biti obuhvaćeno novom Strategijom.
- Dalje aktivnosti na snaženju ljudskih resura moraju biti planirane, a finansijska sredstva blagovremeno opredijeljena.

MINISTARSTVO PROSVJETE, NAUKE, KULTURE I SPORTA

- Neophodno je kreirati radionice za učenike osnovnih i srednjih škola, kao i obuke za nastavnike, pedagoge, psihologe, rukovodioce škola.
- Potrebno je kontinuirano raditi na podizanju svijesti kod djece, koja su u fokusu pažnje kada je obrazovanje u pitanju, a takođe i kod nastavnika, stručnih saradnika i roditelja, o bezbjednom korišćenju informacionih tehnologija.

AGENCIJA ZA NACIONALNU BEZBJEDNOST

- Potrebno je nastaviti sa aktivnostima na podizanju kadrovskih, tehničkih i analitičkih kapaciteta i sposobnosti, prije svega kroz izmjenu organizacije i sistematizacije radnih mjesta u cilju povećanja broja zaposlenih na poslovima sajber bezbjednosti, kao i implementaciji savremenih rješenja i izbora opreme u skladu sa standardima ISO 27001 i EU i NATO standardima.

DIREKCIJA ZA ZAŠTITU TAJNIH PODATAKA – CIRT.ME

- Intenzivirati saradnju sa međunarodnim partnerima u cilju informisanja i unapređenja kapaciteta iz oblasti sertifikacije klasifikovanih informacionih sistema, TEMPEST zaštite i rukovanja kripto materijalima.
- Potrebno je nastaviti sa unapređenjem i daljom implementacijom informacionog sistema za razmjenu domaćih tajnih podataka.
- Preduzeti dalje aktivnosti u pravcu unaprjeđenja mehanizama za odgovor na incidente i upravljanje kriznim situacijama izazvanim sajber prijetnjama.
- Snaženje operativnih i tehničkih kapaciteta CIRT-a mora biti prepoznato kao kontinuirana obaveza i u okviru novog strateškog dokumenta.