Adresa: Ul.Stanka Dragojevića br.2
81000 Podgorica Crna Gora
www.mif.gov.me

Ministarstvo
finansija

Br: 05-02-07-040/24-2827/3

Podgorica, 10.05.2024. godine

Za: MINISTARSTVO JAVNE UPRAVE, Rimski trg br. 45, Podgorica

gospodinu, Marashu Dukaju, ministru

Predmet: Mišljenje na inovirani Predlog zakona o informacionoj bezbjednosti

Veza: Vaš akt br. 01-040/24-2028 od 19.04.2024. godine i 01-040/24-2827/3 od 26.04.2024. godine

Poštovani gospodine Dukaj,

Povodom *inoviranog Predloga zakona o informacionoj bezbjednosti*, Ministarstvo finansija daje sledeće:

MIŠLJENJE

Uvidom u tekst Predloga zakona i Izvještaj o analizi uticaja propisa, sa aspekta uticaja na poslovni ambijent ukazujemo na sljedeće:

Primjena mjera informacione bezbjednosti podrazumijeva primjenu tehničkih i organizacionih mjera, tako da su organi u obavezi da svoje mrežne i informacione sisteme unaprijede u skladu sa propisanim mjerama za čiju primjenu su potrebna finansijska ulaganja. Ukoliko su oni već uspostavili sistem upravljanja informacionom bezbjednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primjena zakona izazove značajne troškove. Međutim, organi koji su u skladu sa zakonom prepoznati kao ključni i važni subjekti, a koji do sada nijesu uspostavili odgovarajući sistem upravljanja informacionom bezbjednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično. Naime, koliko će finansijskih sredstava za primjenu zakona izdvojiti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posjedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbjednosti, i drugih faktora od kojih funkcionisanje informacione bezbjednosti zavisi.

U Izvještaju o analizi uticaja propisa nije kvantifikovana procjena i na taj način navedeni subjekti su onemogućeni da planiraju buduće troškove i nije izvršena procjena finansijskih izdataka budući da ne postoje zvanični podaci o finansijskim izdacima koji bi se mogli koristiti, kao i zvanična analiza nastale štete.

Uvažavajući da Ministarstvo javne uprave predlaže propis kako bi se stvorio zakonski osnov za izgradnju informacionih i sajber bezbjedonosnih kapaciteta na nivou države Crne Gore, nemamo primjedbi, uz napomenu da uvođenje svakog dodatnog zahtjeva ili uslova ne proizvede barijere i dodatna opterećenja za privredne subjekte.

Uvidom u dostavljeni inovirani Izvještaj o analizi uticaja propisa utvrđeno je da je za implementaciju ovog Zakona potrebno obezbjeđivanje finansijskih sredstava iz Budžeta Crne Gore, u ukupnom iznosu od 2.620.000,00 €, a koja se odnose na:

- **Troškove u vezi ispunjenja tehničkih i drugih uslova za rad Agencije** u iznosu od 2.090.000,00 €, od čega najveći dio sredstava u iznosu od 1.500.000,00 € je za prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama, u prostorijama poslovne zgrade Respa u Danilovgradu, kao i opremanje server sale sa infrastrukturnom i mrežnom opremom, kao i posebne mjere fizičke zaštitte (dojava požara, gašenje požara, video nadzor) i obezbjeđenje agregatskog napajanja i obezbjeđivanje redudanse svih sistema. Zatim nabavka softverskih alata za forenziku, analitiku, bezbjedonosnih alata 300.000,00 €. Pored navedenog, sredstva u iznosu od 200.000,00 € za redundantne sisteme i rezervne radne prostorije kako bi se obezbijedio kontinuitet rada, obezbijediće se prostorija u Disaster recovery u Bijelom Polju, ali je neophodno obezbijediti opremu za redudantne sisteme. Dodatno, sredstva u iznosu od po 30.000,00 € potrebna su za: nabavku satelitskog linka za internet i telefonsku komunikaciju, prostorije za rad i informacione sisteme, kao i dovoljan broj zaposlenih (sedam) u sektoru za nadzor i odgovor na incidente kako bi se obezbijedio kontinuitet rada 24/7 časa.
- **Troškove povećanja kapaciteta Ministarstva javne uprave (CIRT državne uprave)** u ukupnom iznosu od 530.000,00 €, od čega je najveći dio sredstava u iznosu od 300.000,00 € predviđen za bezbjedonosni sistem nad mrežom državnih organa i Vladinom infrastruktrom koji mogu biti promptno aktivirani sa druge lokacije, zatim sredstva u iznosu od 120.000,00 € za dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa, odnosi se na uvećanje broja izvršilaca za tri, kao i za obezbjeđivanje naknade za rad GSOC-a za 24/7 nadzor i monitoring koji čine Direkcija Vladin CIRT i Direkcija za infrastrukturu. Pored navedenog, sredstva u iznosu od 50.000,00 € za opremanje prostorija za rad i informacione sisteme, smještene na sigurnim lokacijama, u smislu obezbjeđivanja prostorija za rad CIRT-a. Takođe, sredstva u iznosu od po 30.000,00 € za adekvatan sistem za prijavljivanje i upravljanje incidentima, kao i za nabavku satelitskog linka za internet i telefonsku komunikaciju.

Ministarstvo finansija je na inovirani Predlog zakona o informacionoj bezbjednosti dalo mišljenje br. 02-05-04/24-2827/2 od 24.04.2024. godine, nakon čega je Ministarstvo javne uprave dostavilo inovirani Izvještaj o analizi uticaja propisa (akt br.01-040/24-2827/3 od 26.04.2024.godine), u kojem se navodi, da su sredstva za osnovne potrebe funckionisanja Agencije u toku 2024. godine, odnosno od momenta stupanja na snagu Odluke o osnivanju Agencije, potrebna u ukupnom iznosu od 281.500,00 € i to:

- sredstva za zarade za 20 zaposlenih, u iznosu od 125,000 eura; (4111-4115)
- naknadu za članove Savjeta Agencije za četiri mjeseca u iznosu od 12.000 eura; (4127)
- računarsku opremu za zaposlene, u iznosu od 35.000 eura; (4415)
- održavanje računarske mreže, u iznosu od 5.000 eura; (4153)
- kancelarijska oprema, u iznosu od 20.000 eura; (4415)
- adaptaciju, odnosno prilagođavanje prostorija zgrade Respa u Danilovgradu za rad zaposlenih, u iznosu od 40.000 eura; (4149)
- sredstva za prevoz zaposlenih u Danilovgradu, u iznosu od 5.000 eura; (4145)
- sredstva za službena putovanja, u iznosu od 10.000 eura;
- izrada web sajta Agencije, u iznosu od 20.000 eura; (4193)
- administrativni materijal, u iznosu od 3.000 eura; (4131)
- troškovi reprezentacije, u iznosu od 1.500 eura; (4142)
- komunikacione usluge, u iznosu od 2.000 eura; (4143)
- osiguranje zaposlenih, u iznosu od 500 eura; (4194)
- troškovi goriva, u iznosu od 1.000 eura; (4135)
- konsultantske usluge, u iznosu od 1.500 eura (4147);
- izdaci za ugovore o djelu, u iznosu od 1.500 eura (4191).

Razmatrajući dostavljenu dokumentaciju, obavještavamo Vas da je Ministarstvo finansija na inovirani Predlog zakona o informacionoj bezbjednosti iskazalo stav mišljenjem br. 02-05-04/24-2827/2 od 24.04.2024. godine, s tim što je **potrebno u članu 51 st. 2 i 3 koji se se odnose na utvrđivanje zarade direktora i dodatka na zaradu zaposlenih u Agenciji, brisati, iz razloga što će isto biti predmet novog Zakona o zaradama zaposlenih u javnom sektoru.** Međutim, imajući u vidu važnost otpočinjanja rada Agencije u 2024. godini, Ministarstvo finansija u načelu nema primjedbi da se, u cilju stvaranja uslova za početak rada Agencije u 2024. godini, obezbijede sredstva u iznosu od 281.500,00 €.

Budući da sredstva za navedeno nijesu predviđena Zakonom o budžetu Crne Gore za 2024. godinu, upućujemo na član 43 Zakona o budžetu i fiskalnoj odgovornosti, kojim je između ostalog propisano da se za neplanirane i nedovoljno planirane izdatke tokom fiskalne godine koriste sredstva tekuće rezerve uz prethodnu saglasnost Vlade.

S poštovanjem,

MINISTAR
Novica Vuković

Crna Gora
MINISTARSTVO FINANSIJA
PODGORICA

OBRAZAC

IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	Ministarstvo javne uprave
NAZIV PROPISA	Predlog zakona o informacionoj bezbjednosti

1. Definisanje problema

- **Koje probleme treba da riješi predloženi akt?**
- **Koji su uzroci problema?**
- **Koje su posljedice problema?**
- **Koji su subjekti oštećeni, na koji način i u kojoj mjeri?**
- **Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?**

Koje probleme treba da riješi predloženi akt?

Važeći Zakon o informacionoj bezbjednosti u Crnoj Gori donijet je 2010. godine, kada je prvi put uređena oblast bezbjednosti u informaciono-komunikacionim tehnologijama.
Prvi Zakon o informacionoj bezbjednosti u Crnoj Gori donijet je 2010. godine i uredio je mjere i standarde informacione bezbjednosti, kao i sistem zaštite i prevencije od bezbjednosnih incidenata na internetu. Ovaj zakon donijet je u periodu prije usvajanja Direktive EU o mjerama za visok nivo informacione bezbjednosti mrežnih i informacionih sistema u Evropskoj uniji br. 2016/1148 (NIS Direktiva). Izmjenama i dopunama Zakona iz 2016. godine, kroz prepoznavanje Savjeta za informacionu bezbjednost, kao i osnova za uređivanje mjera zaštite kritične informatičke infrastrukture, ovaj zakon je djelimično usklađen sa pomenutom direktivom.
Evropska unija krajem 2022. godine, usvojila je Direktivu (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2), nakon čega je Crna Gora prateći trendove EU pristupila transponovanju navedene direktive u Predlog zakona o informacionoj bezbjednosti.
Programom rada Vlade za 2023. godinu, u okviru oblasti 5. Digitalna transformacija pod ciljem 5.2 Jačanje Vladine informatičke infrastrukture, kao aktivost pod br. ND 130 predviđen je Predlog zakona o informacionoj bezbjednosti, čiji rok završetka je planiran za III kvartal 2023. godine.

Nakon sajber napada visokog nivoa sofisticiranosti od 20. avgusta 2022. godine, a koji je bio usmjeren na Vladinu informatička infrastruktura i informaciono-komunikacionu mrežu organa, onemogućen je nesmetan rad i funkcionisanje javne uprave, pa se sa elektronskog poslovanja moralo preći na tradicionalni način poslovanja. Ugrožen je veliki broj informacionih sistema, od kojih je zavisio kontinuitet pružanja usluga i ostvarena značajna šteta, koja je iziskivala oporavak u više faza.

Predloženi akt treba da riješi sledeće probleme:

1. Nepostojanje opštih kriterijuma za prepoznavanje ključnih i važnih subjekata od kojih zavisi vršenje djelatnosti od javnog interesa;
2. Upravljanje sajber bezbjednošću;
3. Neobavještavanje o sajber prijetnjama i incidentima;
4. Rješavanje incidenta i postupanje u slučaju sajber prijetnji i incidenata sa značajnim uticajem. Naime, dosadašnjim propisom nije regulisano ko se obavještava, ko rješava ili u saradnji s kim rješava sajber prijetnje i incidente sa značajnim uticajem;
5. Rješavanje i postupanja u slučaju sajber krize. Ko se obavještava? Kada i na koji način se proglašava sajber kriza?
6. Nepostojanje nadležnih tijela odgovornih za sajber bezbjednost i za nadzorne zadake sa propisanim nadležnostima;
7. Nepostojanje obaveze izvještavanja na nivou subjekata;
8. Nepostojanje jasno propisanih mjera u pogledu sajber bezbjednosnih rizika;
9. Nepostojanje stručnog nadzora; i
10. Nepostojanje kaznenih odredbi.

Koji su uzroci problema?

Uzroci nabrojanih problema prije svega su:

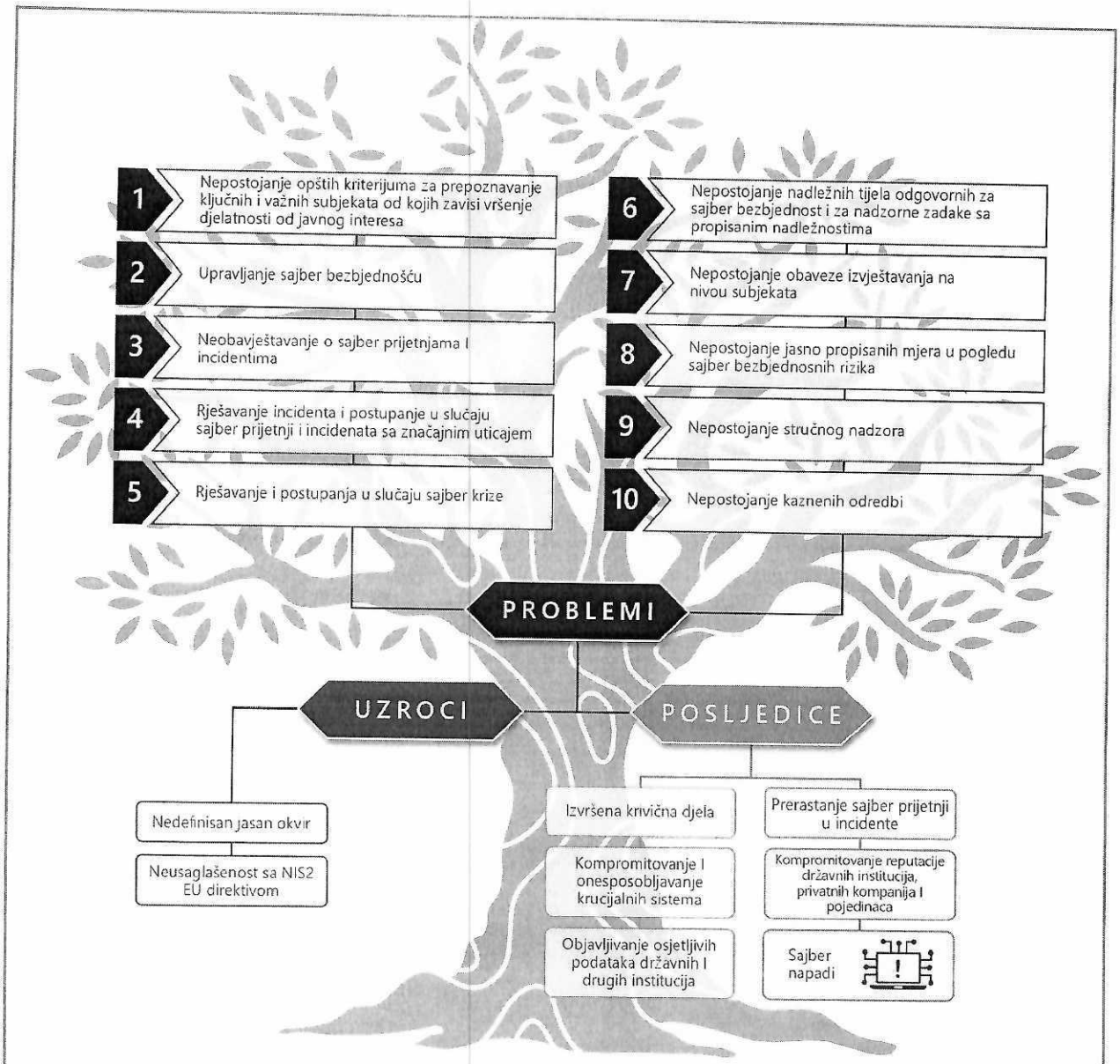
Nedefinisan jasan okvir, koji omogućava organizaciju i koordinaciju u slučajevima rješavanja sajber prijetnji, sajber incidenata sa značajnim uticajem i sajber krize.

Neusaglašenost sa Direktivom (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

Koje su posljedice problema?

Posljedice problema su: krivična djela izvršena u ovom domenu, objavljivanje osjetljivih podatka državnih i drugih institucija, kompromitovanje i onesposobljavanje krucijalnih mrežnih i informacionih sistema na kojima su bazirani poslovni i društveni procesi, kompromitovanje reputacije kako državnih i privatnih institucija, tako i pojedinaca.

Prerastanje sajber prijetnji u incidente sa visokim značajnim negativnim učinkom, može dovesti do znatnog oštećenja, poremećaja i negativnih uticaja na podatke i mrežne i informacione sisteme.



Primjer:

Sajber napad na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa od 20. avgusta 2022. godine.

Detaljnom analizom[1] utvrđeno je djelovanje ransomware malicioznog koda i detektovani su DDoS i Botnet napadi visokog nivoa sofisticiranosti. U cilju predostrožnosti i sprječavanja daljih posljedica napada, izvršeno je isključivanje servera na kojima su smješteni informacioni sistemi organa, sa informaciono-komunikacione mreže organa. Nastali sajber napad onemogućio je nesmetan rad i funkcionisanje javne uprave, te se sa elektronskog poslovanja moralo preći na

[1] Informacija o preduzetim aktivnostima povodom saniranja posljedica izazvanih sajber napadima na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa (Informacija o preduzetim aktivnostima povodom saniranja posljedica izazvanih sajber napadima na vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa (www.gov.me)

tradicionalni način poslovanja. Ugrožen je veliki broj informacionih sistema, od kojih je zavisio kontinuitet pružanja usluga i ostvarena značajna šteta, koja je iziskivala oporovak u više faza.

Oporavak od sajber napada, je bio dugotrajan proces u kome su pored domaćih, podršku pružili i međunarodni partneri. Ekspertski tim iz Sjedinjenih Američkih Država pružio je stručnu (konsultativnu) podršku u prevazilaženju novonastale situacije i planiranju i stvaranju mehanizama za adekvatniju sajber zaštitu u slučaju novog sajber napada visokog nivoa sofisticiranosti. Od strane eksperata iz Republike Francuske, odnosno Nacionalne agencije za bezbjednost informacionih sistema (ANSSI), Ministarstvu je pružena podrška na ponovnom uspostavljanju pojedinih informacionih sistema. Sa partnerima iz Velike Britanije razmijenjena su iskustva u vezi aktuelnih sajber napada i planirani su zajednički projekti za unapređenje informacione bezbjednosti u Crnoj Gori.
Nacionalna infrastruktura je sve izloženija sajber rizicima koji proističu iz integrisanosti informaciono komunikacionih tehnologija sa poslovima koji se obavljaju preko infrastrukture. Rastuća zavisnost od informaciono komunikacionih tehnologija stvorila je slabe tačke, što daje prilike sajber kriminalu da raznim hakerskim alatima ugrozi funkcionisanje vitalne infrastrukture. Tokom analize utvrđeno je da je kriptovano ukupno 17 informacionih sistema u 10 institucija, dok je sajber napad direktno uticao na 150 računara.
U cilju preduzimanja mjera i aktivnosti za otklanjanje posljedica sajber napada i sprječavanje nastanka novih, organi su, u koordinaciji sa Ministarstvom javne uprave, intezivno radili na oporavku korisničkih računara. Izvršena je reinstalacija svih računara u mreži organa državne, pri čemu su postojeći podaci arhivirani i izuzeti, kako bi se izvršilo skeniranje i mogućnost ponovne infekcije prethodno reinstalitanih uređaja svela na minimum.

Koji su subjekti oštećeni, na koji način i u kojoj mjeri?

Oštećeni su brojni subjekti - kako institucije, privreda tako i građani. Napad na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu doveo je do onemogućavanja elektronske komunikacije među institucijama i prema korisnicima elektronskih usluga.

Načini na koji su oštećene institucije su:
Onemogućavanje rada informacionih sistema na kojima se zasnivaju biznis procesi, kao i procesi od nacionalne bitnosti (npr. nacionalni telekomunikacioni sistemi, sl).
Onemogućavanje pružanja elektronskih usluga građanima, privredi i organima državne uprave.
Onemogućavanje obavljanja svakodnevnih aktivnosti koje se zasnivaju na informaciono komunikacionim tehnologijama, a koje su dio jedinstvenog informacionog sistema kojim upravlja Ministarstvo javne uprave.
Narušavanje ugleda objavljivaljem lažnih informacija ili krađom informacija.

Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?

Opcija „status quo" bi dovela do još veće eskalacije problema koji su nabrojani. Naime, bez jasno propisanog okvira za bezbjednost mrežnih i informacionih sistema, sa definisanim tijelima za sprovođenje i unapređenje mjera informacione bezbjednosti, propisanog vršenja nadzora nad primjenom tih mjera, kao i bez uspostavljenog sistema za rano otkrivanje i odbranu od sajber prijetnji i incidenata, povećava se opasnost od potencijalnih napada u sajber prostoru. Nastali sajber napadi mogu pruzrokovati značajnu štetu uslijed prekida električne energije, nedostatka vode, nemogućnost javnog transporta i drugo.

2. Ciljevi

- **Koji ciljevi se postižu predloženim propisom?**

- **Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo.**

Koji ciljevi se postižu predloženim propisom?

Glavni cilj ovog zakona je: izgradnja informacionih i sajber bezbjedonosnih kapaciteta na nivou države Crne Gore, ublažavanje prijetnji mrežnim i informacionim sistemima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju incidenata, čime se doprinosi sigurnosti i efikasnijem funkcionisanju privrede i društva.

Predloženi propis se priprema u skladu sa Programom rada Vlade za 2023. godinu, u okviru oblasti 5. Digitalna transformacija pod ciljem 5.2 Jačanje Vladine informatičke infrastrukture, kao aktivost pod br. ND 130, a čiji rok završetka je planiran za III kvartal 2023. godine.

Donošenjem ovog propisa stvara se zakonski osnov za realizacilju sledećih ciljeva:

- Usklađivanje sa pravnom tekovinom EU kroz transponovanje Direktive (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2). Kroz Program pristupanja Crne Gore Evropskoj uniji 2023 – 2024. u okviru usluga informatičkog društva planirana je izrada ovog propisa.
- Izgradnja sajber bezbjednosnih kapaciteta na nivou Crne Gore, poput Agencije za sajber bezbjednost i CIRTa državne uprave;
- Identifikovanje ključnih i važnih subjekata od kojih zavisi vršenje djelatnosti od javnog interesa;
- Stvaranje održivog sistema za efikasno otkrivanje i odbranu od sajber prijetnji i incidenata visokog nivoa.
- Ublažavanje i sprječavanje prijetnji mrežnih i informacionih sistemima koji se koriste za pružanje osnovnih usluga u ključnim i važnim sektorima
- Jačanje povjerenja korisnika u smislu zaštite njihovih podataka.

3. Opcije

- **Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa).**
- **Obrazložiti preferiranu opciju?**

Prilikom pripreme Predloga zakona razmatrana je "status quo", neregulatorna i regulatorna opcija.
Status quo opcija: Ova opcija omogućava nastavak postojećih praksi i procedura, to bi značilo da se u slučaju zadržavanja "status quo" opcije ne bi se postigao zadovoljavajući nivo informacione bezbjednosti mrežnih i informacionih sistema. Zadržavanjem "Status quo" opcije izalazi se iz regulatornih tokova EU, koji imaju za cilj da nizom propisa podignu nivo informacione bezbjednosti na području Unije, jedan od njih je i Direktiva NIS 2.

Neregulatorna opcija: Ova opcija nije prihvatljiva budući da država Crna Gora u procesu usaglašavanja sa evropskom pravnom tekovinom, ima obavezu usaglašavanja propisa sa pravnom tekovinom EU, u ovom slučaju sa Direktivom NIS 2, koja je usvojena 14. decembra 2022. godine, te razmatranje neregulatorne opcije nije prihvatljivo.

Regulatorna opcija: Preferirana opcija je donošenje ovog propisa čime će se stvoriti zakonski osnov za izgradnju informacionih i sajber kapaciteta na nivou države, ublažavanje prijetnji mrežnim i informacionim sistemima i osiguravanje kontinuiteta usluga u slučaju prijetnji i incidenata. Takođe doprinijeće se uklanjanju razlika u pogledu informacionu i sajber bezbjednosti na nivou EU i države Crne Gore kao kandidata za ulazak u EU.

4. Analiza uticaja

- **Na koga će i kako će najvjerovatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.**
- **Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima).**
- **Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.**
- **Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.**
- **Uključiti procjenu administrativnih opterećenja i biznis barijera.**

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

Donošenje ovog propisa će pozitivno uticati na rad državnih organa, organa državne uprave, organa jedinica lokalne samouprave, organa lokalne uprave, i službi obrazovanih u skladu sa zakonom kojim se uređuje lokalna samouprava, pravnih lica koja vrše javna ovlašćenja (organi), privrednih društava i drugih pravnih i fizičkih lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom (drugi subjekti), kao i na građane Crne Gore.

Takođe, pozitivan uticaj će se odraziti i na investicioni ambijent u Crnoj Gori, čime se stvaraju bolji uslovi za razvoj investicija. uz sigurnije i bezbjednije funkcionisanje informacionih sistema na kojima su zasnovani kritični i biznis procesi.

Rješenja u ovom zakonu doprineće boljoj povezanosti svih relevantnih aktera u oblasti informacione bezbjednosti, budući da se ovim zakonom predviđa uspostavljanje Zbirnog registra ključnih i važnih subjekata koji pružaju usluge od opšteg interesa za Crnu Goru . Na taj način Ministarstvo javne uprave kao organ nadležan za informacionu bezbjednost i Agencija za sajber bezbjednost, čije osnivanje se predviđa ovim zakonom, uspostaviće intenzivniju saradnju sa svim ključnim i važnim subjektima, naročito u slučaju kada se dešava sajber prijetnja, incident ili kriza.

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

Budući da primjena mjera informacione bezbjednosti podrazumijeva primjenu tehničkih i organizacionih mjera, organi su u obavezi da svoje mrežne i informacione sisteme unaprijede u skladu sa propisanim mjerama za čiju primjenu su potrebna finansijska ulaganja. Ukoliko su

oni već uspostavili sistem upravljanja informacionom bezbednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primjena zakona izazove značajne troškove. Međutim, organi koji su u skladu sa zakonom prepoznati kao ključni i važni subjekti, a koji do sada nijesu uspostavili odgovarajući sistem upravljanja informacionom bezbjednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično.

Precizni iznosi dodatnih troškova za navedene organe variraju , budući da isti zavise od više faktora koji mogu da budu veoma različiti u različitim organima. Naime, koliko će finansijskih sredstava za primjenu zakona izdvojiti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posjedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbjednosti, i drugih faktora od kojih funkcionisanje informacione bezbjednosti zavisi. Shodno navedenom, nije moguće dati ni tačne, ni okvirne iznose po organu.

Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti?

Primjena mjera informacione bezbjednosti je od posebnog značaja i zahtijeva finansijska ulaganja, ali i smanjuje i sprječava finansijske izdatke koje mogu nastati kao posledica sajber incidenata sa značajnim uticajem na mrežne i informacione sisteme.
U većini slučajeva, onemogućavanje obavljanja svakodnevnih aktivnosti koje se zasnivaju na upotrebi mrežnih i informacionih sistema, izaziva veće finasijske izdatke od samih ulaganja u sprovođenje mjera zaštite.
Neispunjavanje mjera informacione bezbjednosti od strane ključnih i važnih subjekta koji su prepoznati u sektorima energetike, transporta, finansija, sanbdijevanja vodom i dr. može značajno da ugrozi normalno funkcionisanje društva.
Opasnost od potencijalnih napada može da se odrazi na bezbjednost i javno zdravlje građana, ekonomiju, životnu sredinu i dr.
Narušavanje reputacije objavljivanjem lažnih informacija ili krađom održava se na poslovni uspjeh i poslovanje organa.

Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija?

Primjena ovog propisa podržava stvaranje novih privrednih subjekata koji će pružati usluge informacione bezbjednosti i sajber zaštite.

Uključiti procjenu administrativnih opterećenja i biznis barijera.

Odredbama člana 18 ovog zakona propisano je sledeće:
Organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona. Ključni i važni subjekti određuju se Odlukom Vlade, nakon sprovedenog postupka prepoznavanja od strane nadležnih organa u skladu sa ovim zakonom.
Organi i drugi subjekti koji nijesu u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona.
Organi i drugi subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti u skladu sa st. 1 i 2 ovog člana.
Radi sprovođenja mjera informacione bezbjednosti, organi i drugi subjekti koji su u sladu sa ovim zakonom određeni kao ključni subjekti moraju da ispunjavaju uslove u skladu sa

važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001.
O ispunjenosti uslova iz stava 4 ovog člana ključnim subjektima akreditovano pravno lice izdaje certifikat.
Ključni subjekti dužni su da od akreditovanog pravnog lica zahtijevaju periodičnu provjeru ispunjenosti uslova u skladu sa standardom iz stava 4 ovog člana.

Budući da se propisom pored primjene mejra informacione bezbjednosti na propisani način u članu 18 ovog zakona, zahtijeva određivanje zaposlenog lica za praćenje mjera informacione bezbjednosti od strane organa i drugih subjekata, kao i primjena važećeg crnogorskog standarda za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 od strane ključnih subjekata, u tom smislu troškovi organa i drugih subjekata koji nemaju stručno lice za praćenje primjene mjera, kao i troškovi ključnih usbjekata koji nemaju implementiran navedeni standard bi bili povezani sa troškovima zapošljavanja stručnog lica i uspostavljanja navedenog standarda.

Međutim kroz dosadašnju saradnju, objavljene godišnje izvještaje o radu institucija smatra se da u cilju digitalne transformacije društva veći broj organa i drugih subjekata ima zaposleno lice za praćenje primjene mjera informacione bezbjednosti, kao i da određeni broj ključnih i važnih subjekata već ispunjava uslove propisane ovim zakonom, uključujući i primjenu važećeg crnogorskog standarda za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 od strane ključnih subjekata.

Najveći sajber napad u Crnoj Gori dogodio se 20. avgusta 2022. godine.

- Tokom napada obustavljena je svaka međusobna elektronska komunikacija organa, kao i komunikacija sa privredom i građanima preko 5. 500 službenih e-mail adresa.

- Informacioni sIstem socijalnog staranja ISSS (tzv. Socijalni karton) je jedan od ključnih informacionih sistema bez kojeg praktično nije moguće sprovesti postupke podnošenja zahtjeva utvrđivanja prava na materijalna davanja i socijalne usluge, izdavanje pojedinačnih rješenja, mjesečne revizije postojećih korisnika, obračun i isplatu. Kroz ISSS mjesečno se obračuna i uputi na isplatu oko 200.000, 00 pojedinačnih isplata ka građanima u ukupnom iznosu od oko 200 miliona eura za 2023. godinu.
  Onemogućavanje rada ovog informacionog sistema uslijed sajber napada bi ugrozilo egzistenciju velikog broja građana Crne Gore. Takođe, ISSS je interoperabilan za devet razliičitih institucija sa kojima se razmjenjuju podaci .

- Elektronski sistem javnih nabavki nije bio u funkciji, te su se javne nabavke odložile za nekoliko mjeseci, što se posebno odrazilo na nabavku ljekova.

- Prestao je da radi Portala eUprava, te su građanima, pravnim licima, kao i cjelokupnoj upravi par mjeseci bile nedostupne 383 elektronske usluge. Iz tih razloga za 2.743 visokoškolaca prolongiran je Program stručnog osposobljavanja lica sa stečenim visokim obrazovanjem za 2022-2023. za mjesec dana kao i podnošenja zahtjeva za dodjelu studentskog kredita za 3.900 studenata.

- Zapošljavanje preko sistema za elektro testiranje kandidata odloženo je za dva mjeseca.

- Portal elektronskih sjednica Vlade koji podržava elektronska zasijedanje Vlade i Vladinih komisija nije bio u funkciji tako da je 10 sjednica održano uz upotrebu papirne dokumentacije.

- Portal Vlade GOV.ME preko kojeg se objavljuju informacije u skladu sa Zakonom o slobodnom pristupu informacija i ažuriraju ostale informacije koje su važne za rad organa državne uprave, nije bio u funkciji oko mjesec dana.

- Sistem za elektronsko upravljanje dokumentima (eDMS) nije bio u funkciji tri mjeseca. Samim tim komunikacija se obavljala isključivo u papirnoj formi.

Osim ovog sajber napada, za vrijeme napada koji se dogodio 2016. godine oboreni su sajtovi državnih institucija, a i 2017. bili su ugroženi servisi Vlade i državnih institucija.

Sajber napadima su izložene sve države u region i šire, primjera radi susjedne države Albanija i Srbija bile su skorije mete snažnih sajber napada.
Albanija - Javni onlajn servisi Albanije bili su blokirani u julu 2022. nakon sajber napada.
Hakeri su pokušali da onesposobe ključne sisteme Metod koji su koristili identičan je napadima viđenim u međunarodnom sajber prostoru", poput izvedenih u Ukrajini, Nemačkoj, Litvaniji, Malti, Holandiji i Belgiji.
Srbija - Hakeri su preko sajta javno-komunalnog preduzeća Informatika blokirali informatički sistem Novog Sada u martu 2020. godine.
U zamjenu za kod kojim bi se, navodno, otključale blokirane baze podataka zatražili su otkup od 50 bitkoina (400.000 eura). Kako je grad odbio da plati ucjenu, ostao je bez velikog broja podataka. Tokom napada nijesu mogle da se izdaju građevinske dozvole, nije radila objedinjena naplata, prestao je da radi sistem video nadzora, internet je prestao da radi u upravama.

5. Procjena fiskalnog uticaja

- **Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?**
- **Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Obrazložiti.**
- **Da li implementacijom propisa proizilaze međunarodne finansijske obaveze? Obrazložiti.**
- **Da li su neophodna finansijska sredstva obezbijeđena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskalnu godinu?**
- **Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteći finansijske obaveze?**
- **Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?**
- **Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.**
- **Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda? Obrazložiti.**
- **Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?**

Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.

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

Članom 50 ovog zakona propisano je da se Sredstva za rad Agencije obezbjeđuju se u budžetu Crne Gore, u skladu sa zakonom kojim se uređuje oblast budžetskog sistema i budžetskog računovodstva, kao i da je Agencija je dužna da svoje finansijsko poslovanje organizuje i vodi, u skladu sa propisima kojima se uređuje oblast budžetskog sistema. Takođe Članom 51 stav 2 ovog zakona, propisano je da zaposleni u Agenciji imaju mjesečni dodatak na zaradu u iznosu do 30%, što je od izuzetnog značaja imajući u vidu nadležnosti Agencije, kao i poslove koje će zaposleni raditi, a posebno pri činjenici da broj kadrova u Crnoj Gori u ovoj oblasti nije zadovoljavajući, te da ih treba dodatno motivisati i spriječiti odliv takvih kadrova na rad van Grne Gore. Trenutno na tržištu rada ne postoje kadrovi sa ovim znanjima i postoji velika potražnja od strane država Zapadne Evrope ka angažovanju lica sa ovakvim specifičnim znanjima. Ujedno je i potražnja od strane privatnog sektora takođe izražena i u tom smislu je neophodno obezbijediti mjesečni dodatak u navedenom iznosu. Za popunjavanje radnih mjesta u agenciji neophodno je poznavanje rada na kompleksnim platformama i posebno iskustvo u radu sa mrežnim uređajima. Ujedno, zaposleni u Agenciji će imati potrebu za pristupu i obradi tajnih podataka, a to se odnosi na kompletan kadar.

Za implementaciju ovog propisa potrebno je obezbijediti finansijska sredstva iz Budžeta Crne Gore, prije svega za ispunjenje tehničkih i drugih uslova za rad Agencije i CIRT-a državne uprave,a to je da:

1) posjeduju sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju;
2) posjeduju prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama;
3) posjeduju adekvatan sistem za prijavljivanje i upravljanje incidentima;
4) obezbjeđuju povjerljivost i pouzdanost procesa rada;
5) posjeduju redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada;
6) imaju dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa.

U tom smislu troškovi povećanja kapaciteta Ministarstva javne uprave (CIRT državne uprave) bi bili okvirno sledeći:

- sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju predviđaju nabavku satelitskog linka za internet i telefonsku komunikaciju - **30 000 eura,**
- opremanje prostorija za rad i informacione sisteme, smještene na sigurnim lokacijama, u smislu obezbjeđivanja prostorija za rad CIRT-a **– 50 000 eura,**
- adekvatan sistem za prijavljivanje i upravljanje incidentima **– 30 000 eura,**
- redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada, na način da u slučaju kompromitacije ili fizičke nedostupnosti primarne lokacije, bezbjedonosni sistemi nad mrežom državnih organa i Vladinom infrastruktrom mogu biti promptno aktivirani sa druge lokacije **– 300 000 eura,**
- dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa, odnosi se na uvećanje broja izvršilaca za tri, kao i za obezbjeđivanje naknade za rad GSOC-a za 24/7 nadzor i monitoring koji čine Direkcija Vladin CIRT i Direkcija za infrastrukturu - **120 000 eura.**

Troškovi u vezi ispunjenja tehničkih i drugih uslova Agencije za sajber bezbijednosti bili bi sledeći:

- sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju predviđaju nabavku satelitskog linka za internet i telefonsku komunikaciju - **30 000 eura,**
- prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama , u skladu sa Zakljuljčcima Vlade koristiće prostorije poslovne zgrade Respa u Danilovgradu, ali je neophodno opremanje server sale sa infrastrukturnom i mrežnom opremom, kao i posebne mjere fizičke zaštitte(dojava požara, gašenje požara, video nadzor), obezbijediti agregatsko napajanje i obezbjediti redudansu svih sistema **1 500 000 eura,**
- nabavka softverskih alata za forenziku , analitiku, bezbjedonosnih alata – **300.000**
- adekvatan sistem za prijavljivanje i upravljanje incidentima – **30 000 eura,**
- redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada, obezbijediće se prostorija u Disaster recovery u Bijelom polju, ali je neophodno obezbujediti opremu za redudantne sisteme – **200 000 eura.**
- dovoljan broj zaposlenih (sedam) u sektoru za nadzor i odgovor na incidente kako bi se obezbijedio kontinuitet rada 24/7 časa –**30 000 eura.**

Planirani broj zaposlenih u Agenciji za sajber bezbjednost je 39.

Odredbama, čl. 74 do 76 propisano je da će se Odluka o osnivanju Agencije donijeti u roku od 15 dana od dana stupanja na snagu ovog zakona, da će se imenovanje predsjednika i članova Savjeta Agencije izvršiti u roku od 60 dana od dana stupanja na snagu ovog zakona, kao i da će se imenovanje direktora Agencije izvršiti se u roku od 90 dana od dana izbora Savjeta Agencije, a da će do imenovanja direktora Agencije, u skladu sa ovim zakonom poslove direktora Agencije obavljati vršilac dužnosti, koga, na predlog ministra javne uprave, određuje Vlada, u roku od 15 dana od dana stupanja na snagu ovog zakona.

Naime, nakon stupanja na snagu Zakona potrebno je donijeti Odluku o osnivanju Agencije i sprovesti ostale aktivnosti za njeno nesmetano funkcionisanje, te je neophodno obezbijediti sredstva za osnovne potrebe u cilju nesmetanog funckionisanja Agencije u toku 2024. godine, odnosno od momenta stupanja na snagu Odluke o osnivanju Agencije, i to:

- sredstva za zarade za 20 zaposlenih, u iznosu od 125,000 eura; (4111-4115)
- naknadu za članove Savjeta Agencije za četiri mjeseca u iznosu od 12.000 eura; (4127)
- računarsku opremu za zaposlene, u iznosu od 35.000 eura; (4415)
- održavanje računarske mreže, u iznosu od 5.000 eura; (4153)
- kancelarijska oprema, u iznosu od 20.000 eura; (4415)
- adaptaciju, odnosno prilagođavanje prostorija zgrade Respa u Danilovgradu za rad zaposlenih, u iznosu od 40.000 eura; (4149)
- sredstva za prevoz zaposlenih u Danilovgradu, u iznosu od 5.000 eura; (4145)
- sredstva za službena putovanja, u iznosu od 10.000 eura;
- izrada web sajta Agencije, u iznosu od 20.000 eura; (4193)
- administrativni materijal, u iznosu od 3.000 eura; (4131)
- troškovi reprezentacije, u iznosu od 1.500 eura; (4142)
- komunikacione usluge, u iznosu od 2.000 eura; (4143)
- osiguranje zaposlenih, u iznosu od 500 eura; (4194)
- troškovi goriva, u iznosu od 1.000 eura; (4135)
- konsultantske usluge, u iznosu od 1.500 eura (4147);

- izdaci za ugovore o djelu, u iznosu od 1.500 eura (4191).

Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteći finansijske obaveze?

Radi realizacije Predloga zakona, predviđeno je donošenja sledećih podzakonskih akata iz kojih neće proisteći dodatne finansijske obaveze:

- Uredbe o bližem način utvrđivanja mjera informacione bezbjednosti,
- Uredbe o bližem načinu određivanja nivoa incidenta prema nivou značaja i način reagovanja na incidente,
- Pravilnik o izgledu i sadržaju obrasca za dostavljanje obavještenja o incident.

Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?

Ulaskom u 2023. sajber bezbjednost je i dalje na vrhu liste briga kako državne uprave tako i privrede. Ovo nije iznenađenje ako imamo u vidu da je u prvoj polovini 2022. godine bilo je 2,8 milijardi malver napada širom svijeta i 236,1 miliona ransomver napada, kao i da je procijenjeno da je na globalnom nivou 2022. godine, pokrenuto šest milijardi fišing napada.
U novoj anketi IEEE (Institut inženjera elektrotehnike i elektronike- najveće svjetsko stručno udruženje za unaprjeđivanje tehnologije) anketirano je 350 glavnih tehnoloških službenika, direktora za informacione tehnologije i IT direktora, 51% ispitanika je navelo ranjivost oblaka kao najveću zabrinutost (u odnosu na 35% u 2022.), a 43% je navelo ranjivost centara podataka kao najveću zabrinutost (sa 27% u 2022.)[2].

Implementacijom predloga zakona neće se ostvariti direktan prihod u budžetu, ali njegovom primjenom doprinosi se smanjenju negativnog finansijskog uticaja koje bi potencijalne sajber prijetnje, incidenti ili sajber krize mogle da izazovu.

Finansijsku procjenu štete, koja je prouzrokovana sajber napadima teško je izraziti. Cijena sajber napada zavisi od više faktora. Ukoliko se radi o klasičnom sajber kriminalu u cilju otkupa ukradenih podataka ne postoji pravilo koliko će se za otkup potraživati. Osim toga napadnuti subjekt koji je odgovoran za čuvanje prikupljenih podataka moraće da snosi i zakonske kazne. Korisnici usluga gube povjerenje u pružaoce usluga koji su bili meta napada.
Posljedice sajber napada mogu biti dalekosežne, kako u finansijskom tako i političkom smislu. Kontinuiranim ulaganjem u informacionu bezbjednost troškovi se znatno umanjuju i jača povjerenje korisnika.

Od sajber pretnji nisu zabrinute samo velike kompanijama koje vrijede milijardu dolara i više. Naime, mala i srednja preduzeća su sve češće žrtve sajber pretnji jer sa slabijom primjenom mjera informacione bezbjednosti imaju tendenciju da budu ranjivija. Prema Izveštaju Verizon Data Breach Investigations za 2021.[3]
1 od 5 žrtava bila su mala i srednja preduzeća — sa srednjom cijenom gubitaka od 21.659 dolara.

Prekid poslovanja izazvan sajber napadima može prouzrokovati ogromne gubitke u neostvarenom profitu. Gubitak povjerenja korisnika često zna da bude nepovratan. Zato čak

[2] Izvor: https://www.techrepublic.com/article/top-cybersecurity-threats/

[3] Izvor: https://www.forbes.com/advisor/business/common-cyber-security-threats/

57% evropskih malih i srednjih preduzeća strahuje da bi sajber napad mogao veoma lako da ih dovede do bankrotstva (Izvor: EU Agencija za sajber bezbejdnost- ENISA).

Zbog nedostatka adekvatnih struktura i mehanizama zaštite, kao i bezbjednosne politike, razvijene zemlje, ali i zemlje u razvoju, podjednako su na meti napada.
Napadima na energetski sistem Sjedinjenih Američkih Država oko 50 miliona ljudi ostalo je bez električne energije.

U toku 2014. godine, samo u jednom danu 50 norveških naftnih kompanija je napadnuto sajber napadima različitih intenziteta. Cjelokupna naftna industrija ove skandinavske države bila je žrtva masovnog napada. U napadima je došlo do hakovanja i krađe podataka bušenja, istraživanja i inženjeringa.

Njemačka željezara je bila meta napada krajem 2014. godine. Hakeri su uspješno preuzeli kontrolu nad programom čija je funkcija bila gašenje visoke peći. Ovo je jedan od primjera gde je sajber napad izazvao direktnu fizičku štetu.

Nedostatak ulaganja u bezbjednosna rješenja su globalni problemi, kojem su sve više izložena mala i srednja preduzeća dok velike koorporacije, nakon neugodnih iskustava koja su rezultirala velikim materijalnim štetama sve više ulažu u informacionu bezbjednost kroz primjenu mjera i poštovanje najsavremenijih standarda. Osim toga, kako se ne bi došlo u situaciju da, zahvaljujući sopstvenim bezbjednosnim propustima, sajber napad bude uspješan neophodno je kontinuirano raditi na razvoju bezbjednosne kulture.

Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.
Prilikom obračuna finansijskih izdataka/prihoda uzete su u obzir tri početne osnove:

- Odredbe Predloga zakona o informacionoj bezbjednosti Crne Gore koje regulišu djelokrug rada Agencije i obaveze primjene propisa;
- Preporuke Microsofta o organizacionoj strukturi agencije za sajber bezbjednost („Building an effective national cybersecurity agency")
- Analiza različitih struktura agencija za sajber bezbjednost i posledica sajber napada na osnovu javno dostupnih izvora koji su navedeni u prethodnom tekstu.

Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?
Ne.
Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.
/

6. Konsultacije zainteresovanih strana

- **Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.**
- **Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).**
- **Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.**

Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.

Tokom izrade ovog zakona korišćena je ekspertska podrška od strane eksperta iz Hrvatske, koji je angažovan uz podršku Ženevskog centra za upravljanje sektorom bezbjednosti (DCAF) koji finansira Ministarstvo spoljnih poslova Velike Britanije (UK FCDO).

Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).

Za potrebe izrade ovog propisa, kao i izrade RIA obrasca u početnoj fazi bio je formiran radni tim koji su činili predstavnici Ministarstva. U pripremnoj fazi izrade Nacrt zakona, prije raspisivanja javnog poziva za javnu raspravu, Nacrt zakona u dvodnevnom trajanju prezentovan je Savjetu za informacionu bezbjednost, koji čine predstavnici institucija za koje je informaciona bezbjednost od posebnog značaja, radi dobijanja inputa i smjernica.

Takođe, u skladu sa Uredbom o izboru predstavnika nevladinih organizacija u radna tijela organa državne uprave i sprovođenju javne rasprave u pripremi zakona i strategija („Službeni list CG", broj: 41/18), 10. novembra 2022. godine, raspisan je javni poziv za zainteresovanoj javnosti da se uključe u početnu fazu pripreme Nacrta zakona na internet stranici **http://www.mju.gov.me/ministarstvo** i portalu e-uprave **https://www.euprava.me/** , i u roku od 25 dana dostave svoje sugestje i predloge, o čemu je sačijen Izvještaj o obavljenom konsultovanju zainteresovane javnosti, u propisanom roku.

Isto tako, shodno navedenoj uredbi, 01. marta 2023. godine, raspisan je i javni poziv građanima, privrednim društvima, preduzetnicima, nezavisnim i regulatornim tijelima, pravnim i fizičkim licima koja vrše javna ovlašćenja, državnim organima, organima državne uprave, organima lokalne samouprave, organima lokalne uprave, nevladinim organizacijama i drugim organima i organizacijama (zainteresovani subjekti) da se uključe u javnu raspravu i daju svoj doprinos u razmatranju Nacrta zakona o informacionoj bezbjednosti i dostave svoje predloge, sugestije i primjedbe, a koja javna rasprava je trajala 20 dana od dana objavljivanja javnog poziva na internet stranici Ministarstva javne uprave **https://www.gov.me/mju** i portalu e-uprave **www.euprava.me** . Na javnoj raspravi pored Nacrta zakona, objavljen je bio i Izvještaj o sprovedenoj analizi procjene uticaja propisa (RIA obrazac), međutim na isti nije bilo nikakvih sugestija ni primjedbi.
Tokom trajanja javne rasprave, pored redovnih javnih konsultacija (okruglog stola), sa ciljem kreiranja šireg inkluzivnog procesa, Ministarstvo javne uprave, organizovalo je i konsultacije sa "fokus grupama" koje su činile predstavnici ambasada, predstavnici privrede, akademske zajednice, NVO sektora i predstavnici međunarodnih udruženja u Crnoj Gori.

U toku trajanja javne rasprave od ukupno devet učesnika dostavljeno je 96 primjedbi/ predloga/sugestija, od čega je prihvaćeno 13 primjedbi/predloga/sugestija, dva su djelimično prihvaćena, a 77 primjedbi/ predloga/sugestija nije prihvaćeno, dok su ostali komentari (četiti) bili u vidu pitanja na koje je dat odgovor. O sprovedenoj javnoj raspravi sačinjen je Izvještaj o sprovedenoj javnoj raspravi u propisanom roku, koji je takođe javno objavljen na navedenim linkovima.
Tokom sprovedenog postupka javnog konusultovanja svi zainteresovani subjekti imali su priliku da se uključe u proces javne rasprave, kako putem dostavljenih komentara, primjedbi i sugestija u skladu sa javnim pozivom, tako i putem održavanja okruglo stola, o čemu je zainteresovana javnost mogla da se informiše na zvaničnoj stranici Ministarstva.

Sve informacije o sprovedenoj javnoj raspravi i obavještenjima objavljene su na zvaničnoj internet stranici Ministarstva na linku nacrt zakona o informacionoj bezbjednosti - Pretraga - GOV.ME (www.gov.me)

7: Monitoring i evaluacija

- **Koje su potencijalne prepreke za implementaciju propisa?**
- **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?**
- **Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?**
- **Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?**

Koje su potencijalne prepreke za implementaciju propisa?

Kao potencijalne prepreke za implementaciju propisa izdvajaju se prije svega:
Potrebno je obezbijediti značajana finansijska sredstva za nesmetan rad tijela koja sačinjavaju okvir informacione bezbjednosti Crne Gore (Agencija za sajber bezbjednost i CIRT državne uprave).
Nedostatak službenika osposobljenih na odgovarajući način, prije svega za poslove rješavanja incidenata, stručnog i inspekcijskog nadzora, koji bi trebalo da posjeduju vještine potrebne za obavljenje tih zadataka u smislu utvrđivanje nedostataka hardvera, softvera, kriptovanja, mreža i sl.
Nerazumijevanje značaja primjene mjera informacione bezbjednosti od strane obveznika zakona u smislu podizanja svijesti zaposlenih u obalasti sajber bezbjednosti i integrisanja tehnologija kojima se jača informaciona bezbjednost.

Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?

U saradnji sa Agencijom za sajber bezbijednostMinistarstvo javne uprave izradiće Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu, u kojem će se utvrditi način upravljanja sajber prijetnjama, incidentima i sajber krizama.

Zaštitu mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata vršiće Agencija za sajber bezbjednost. Ovo tijelo će se baviti informacionom bezbjednošću svih organa i drugih subjekata u smislu ovog zakona, osim organa državne uprave, za koje je zadužen CIRT državne uprave.

Takođe, važnu ulogu ima i Savjet za informacionu bezbijednost, radi praćenja razvoja informacione bezbjednosti, a naročito sajber bezbjednosti u cilju obezbjeđivanja bezbjednog sajber prostora Crne Gore.

Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?

Indikatori su:

1. Broj organa i drugih subjekata u smislu ovog zakona, a naročito ključnih i važnih subjekata koji primjenjuju mjere informacione bezbjednosti, a praćenje indikatora vršiće se preko stručnog i inspekcijskog nadzora koji e vršiti nadzornik, odnosno inspektor za usluge informacionog društva.

Naime, ovim zakonom definisani su kriterijumi za određivanje ključnih i važnih subjekata, kao i mjereinformacione bezbjednosti u cilju postizanja najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema.
Stručnim i inspekcijskim nadzorom utvrdiće se da li je postignut adekvatan nivo bezbjednosti.

Budući da u važećim Zakonom o informacionoj bezbjednosti nije opširnije razrađen nadzor, u prilog tome govori činjenica da nijesu postojale kaznene odredbe, novim zakonskim rješenjem je, kroz propisivanje stručnog i inspekcijskog nadzora, naglašen značaj praćenja i primjene mjera informacione bezbjednosti.

Stručnim nadzorom će se posebno utvrditi da li se primjenuju propisane mjere informacione bezbjednosti, posebno one koje se odnose na rad ključnih i važnih subjekata u smislu da li su donijeli propisane akte o sajber bezbjednosnim rizicima, odnosno da li je uspostavljen adekvatan nivo bezbijednosti sistema.

2. Broj prijavljenih sajber prijetnji i incidenata

Ovim zakonom propisana je obaveza izvještavanja o sajber prijetnjama i incidentima. Na osnovu broja prijavljenih sajber prijetnji i incidenata moći će se pratiti stanje u ovoj oblasti u smislu koliko je sajber prijetnji prijavljeno, koliko je preraslo u incidente, koliko je incidenata prijavljeno i kog su nivoa.

3. Uspostavljen Zbirni registar ključnih i važnih subjekata.

Po prvi put će se uspostaviti Zbirni registar ključnih i važnih subjekata, koji će voditi Ministarstvo javne uprave.

Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?

Monitoring i evaulaciju primjene propisa vršiće Ministarstvo javne uprave i Agencija za sajber bezbjednost, preko godišnjih izvještaja, kao i godišnjeg izvještaja o radu Savjeta za informacionu bezbjednost.
Jedan od načina praćenja evaluacije su i izvještaji organa i drugih subjekata o sajber prijetnjama i incidentima koji su obavezni da postupaju po ovom zakonu.

Datum i mjesto
26.04.2024. godine

Starješina

MINISTAR

mr Marash Dukaj

Crna Gora MINISTARSTVO JAVNE UPRAVE PODGORICA

Crna Gora
Ministarstvo javne uprave

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

Br: 01-040/24-2028

19. aprila 2024. godine

Crna Gora
MINISTARSTVO FINANSIJA
Podgorica

Primljeno: 19. 04. 2024				
Org. jed.	Broj	Redni broj	Prilog	Vrijednost
01-	040/24-2827/1			

Za: Ministarstvo finansija

gospodin Novica Vuković, ministar

Predmet: Dostavljanje inoviranog Predloga zakona o informacionoj bezbjednosti, na mišljenje

Poštovani ministre Vuković,

U prilogu akta dostavljamo na mišljenje inovirani Predlog zakona o informacionoj bezbjednosti, shodno odredbama člana 41 Poslovnika Vlade Crne Gore ("Službeni list CG", br. 3/12, 31/15, 48/17 i 62/18).

S poštovanjem,

Crna Gora Ministarstvo javne uprave Podgorica

MINISTAR
mr Marash Dukaj

Prilog:

- Inovirani Predlog zakona o informacionoj bezbjednosti
- Mišljenje Sekretarijata za zakonodavstvo
- RIA obrazac

Dostavljeno:
- naslovu ✓
- a/a

Kontakt osoba: Jelena Knežević
Načelnica
Tel: +382 68 822 970
email: jelena.knezevic@mju.gov.me

PREDLOG

ZAKON O INFORMACIONOJ BEZBJEDNOSTI*

I. OSNOVNE ODREDBE

Predmet
Član 1

Ovim zakonom propisuju se mjere informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema, uključujući sajber bezbjednost, određivanje ključnih i važnih subjekata, upravljanje sajber bezbjednošću, kao i druga pitanja od značaja za informacionu bezbjednost.

Obaveza primjene
Član 2

Po ovom zakonu obavezni su da postupaju državni organi, ministarstva i drugi organi uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica koja vrše javna ovlašćenja (u daljem tekstu: organi), privredna društva i druga pravna lica i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom, (u daljem tekstu: drugi subjekti).

Informaciona bezbjednost
Član 3

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti, dostupnosti i zaštite podatka, kao i sajber bezbjednost.

Povjerljivost podatka podrazumijeva da je podatak dostupan samo licima koja su ovlašćena da ostvare pristup ili postupe sa tim podatkom.

Cjelovitost podatka podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podatka, kao i zaštitu procesa ili programa koji sprečavaju neovlašćene izmjene podataka.

Dostupnost podatka podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku kad god za tim imaju potrebu.

Ključni i važni subjekti
Član 4

Ključni subjekti su organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od posebnog značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do ugrožavanja života, zdravlja, bezbjednosti građana i funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastruktre u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture.

Važni subjekti su organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do otežanog funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastruktre u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture.

CIRT državne uprave i jedinstvena nacionalna kontakt tačka za infomacionu bezbjednost

Član 5

Zaštitu mrežnih i informacionih sistema organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata vrši organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave (u daljem tekstu: Ministarstvo) preko posebne organizacione jedinice (u daljem tekstu: CIRT državne uprave).

Ministarstvo predstavlja jedinstvenu nacionalnu kontaktnu tačku za informacionu bezbjednost i sarađuje sa jedinstvenim nacionalnim kontakt tačkama drugih država.

Agencija za sajber bezbjednost

Član 6

Zaštitu mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata vrši Agencija za sajber bezbjednost (u daljem tekstu: Agencija).

Izuzeće od primjene

Član 7

Ovaj zakon ne primjenjuje se na organ državne uprave nadležan za poslove odbrane, Vojsku Crne Gore, Agenciju za nacionalnu bezbjednost, organizacionu jedinicu organa državne uprave nadležnog za unutrašnje poslove koja vrši policijske poslove, kao i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

Zaštita podataka o ličnosti

Član 8

Podaci o ličnosti koriste se i obrađuju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

Upotreba rodno osjetljivog jezika

Član 9

Izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

Značenje izraza

Član 10

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) **mrežni i informacioni sistem** podrazumijeva:

- elektronsku komunikacionu mrežu koja obuhvata sisteme koji omogućavaju prenos signala žičnim, radio, optičkim ili drugim elektromagnetnim sredstvima koja obuhvataju satelitske mreže, zemaljske fiksne (sa prebacivanjem kanala, komutacijom paketa podataka, uključujući internet) i mobilne mreže, sisteme električnih kablova, u mjeri u kojoj se koriste za prenos signala, kao i mreže koje se koriste za radio i televizijsko emitovanje i kablovske televizijske mreže, bez obzira na vrstu informacija koje prenose,
- svaki uređaj ili skup povezanih ili sličnih uređaja, od kojih najmanje jedan programski izvršava automatsku obradu podataka u elektronskom obliku, i
- podatke u elektronskom obliku koji se čuvaju, obrađuju, dobijaju ili prenose na način iz al. 1 i 2 ove tačke, u svrhu rada, korišćenja, zaštite i održavanja tih mrežnih i informacionih sistema;

2) **informaciona bezbjednost mrežnog i informacionog sistema** je sposobnost mrežnog i informacionog sistema da se na određenom nivou pouzdanosti odupre svakom događaju koji može da ugrozi povjerljivost, cjelovitost i dostupnost sačuvanih, prenesenih ili obrađenih podataka ili usluga koje taj mrežni i informacioni sistem nudi ili kojima omogućava pristup;

3) **podatak** je svaka informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom;

4) **kriptografska zaštita podataka** je primjena programskih rješenja ili uređaja za zaštitu podataka koji obezbjeđuju povjerljivost, cjelovitost i dostupnost podataka;

5) **sajber bezbjednost** podrazumijeva sve aktivnosti koje su nužne za zaštitu od sajber prijetnji i incidenata kojima su izloženi mrežni i informacioni sistemi, korisnici tih sistema i drugi organi i lica na koje te sajber prijetnje i incidenti utiču;

6) **sajber prijetnja** je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na podatke ili mrežne i informacione sisteme, korisnike tih sistema i druge organe i lica;

7) **ozbiljna sajber prijetnja** je sajber prijetnja za koju se na osnovu njenih tehničkih karakteristika može pretpostaviti da može ozbiljno uticati na podatke ili mrežne i informacione sisteme, korisnike tih sistema i druge organe i lica, uzrokovanjem značajne materijalne ili nematerijalne štete;

8) **incident** je svaki događaj koji kompromituje povjerljivost, cjelovitost i dostupnost skladištenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacioni sistemi pružaju ili kojima omogućavaju pristup;

9) **rješavanje incidenta** podrazumijeva sve radnje i postupke čiji je cilj otkrivanje, analiza i zaustavljanje incidenta, kao i odgovor na njega;

10) **ranjivost** je slabost, osjetljivost ili nedostatak nekog resursa, sistema, procesa ili kontrole koji sajber prijetnja može iskoristiti;

11) **rizik** je bilo koja okolnost ili događaj koji ima potencijalno negativan uticaj na bezbjednost podataka i mrežnog i informacionog sistema;

12) **sajber kriza** je događaj ili stanje u sajber prostoru koje ugrožava nacionalnu bezbjednost, zdravlje i život većeg broja građana, značajno narušava životnu sredinu ili uzrokuje značajnu ekonomsku štetu, a odgovor na takav događaj ili stanje zahtijeva učešće više nadležnih organa, kao i primjenu odgovarajućih mjera;

13) **sajber prostor** je zamišljeni prostor u kojem se odvija komunikacija preko interneta.

II. MJERE INFORMACIONE BEZBJEDNOSTI

Vrste mjera informacione bezbjednosti
Član 11

Mjere informacione bezbjednosti su:

1) zaštita podataka i
2) zaštita od sajber prijetnji i incidenata.

Zaštita podataka
Član 12

Zaštita podataka podrazumijeva prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka.

Zaštita iz stava 1 ovog člana obuhvata:

1) pravila za postupanje sa podacima;
2) vođenje evidencije o izvršenim pristupima podacima;
3) nadzor nad bezbjednošću podataka.

Zaštita od sajber prijetnji i incidenata

Član 13

Zaštita od sajber prijetnji i incidenata obuhvata:

1) fizičku zaštitu;

2) zaštitu mrežnog i informacionog sistema;

3) upravljanje rizicima u oblasti sajber bezbjednosti.

Fizička zaštita

Član 14

Fizička zaštita obuhvata zaštitu objekta, prostora i uređaja u kojem se nalazi mrežni i informacioni sistem.

Zaštita mrežnog i informacionog sistema

Član 15

Zaštita mrežnog i informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u mrežnom i informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti podataka u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

Upravljanje rizicima u oblasti sajber bezbjednosti

Član 16

Upravljanje rizicima u oblasti sajber bezbjednosti obuhvata:

1) izradu analize rizika i bezbjednosti mrežnog i informacionog sistema;

2) donošenje pravila postupanja sa incidentima (sprečavanje, otkrivanje i odgovor na incidente);

3) donošenje plana kontinuiteta poslovanja i postupanja u sajber krizama;

4) donošenje akta kojim se uređuje bezbjednost lanca snabdijevanja između organa, odnosno drugog subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga;

5) donošenje akata kojima se uređuje uspostavljanje, razvoj i održavanje mrežnih i informacionih sistema, kao i informacionu bezbjednost mrežnih i informacionih sistema;

6) primjenu kriptografske zaštite podataka, ako priroda poslova iz nadležnosti organa, odnosno drugog subjekta to zahtijeva;

7) donošenje pravila postupanja prilikom procjene efikasnosti mjera iz tač. 1 do 6 ovog člana.

Bliži sadržaj mjera informacione bezbjednosti

Član 17

Bliži sadržaj mjera informacione bezbjednosti iz čl. 11 do 16 ovog zakona propisuje Vlada Crne Gore (u daljem tekstu: Vlada).

Obaveza primjene mjera informacione bezbjednosti

Član 18

Organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona.

Organi i drugi subjekti koji nijesu u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Organi i drugi subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti u skladu sa st. 1 i 2 ovog člana.

Radi sprovođenja mjera informacione bezbjednosti, organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni subjekti moraju da ispunjavaju uslove u

skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001.

O ispunjenosti uslova iz stava 4 ovog člana ključnim subjektima akreditovano pravno lice izdaje certifikat.

Ključni subjekti dužni su da od akreditovanog pravnog lica zahtijevaju periodičnu provjeru ispunjenosti uslova u skladu sa standardom iz stava 4 ovog člana.

III. ODREĐIVANJE KLJUČNIH I VAŽNIH SUBJEKATA

Sektori i podsektori u kojima se određuju ključni i važni subjekti

Član 19

Ključni subjekti određuju se u okviru sljedećih sektora, odnosno podsektora:

1) energetika (električna energija, daljinsko grijanje i hlađenje, nafta, gas i vodonik);

2) saobraćaj (vazdušni, željeznički, pomorski i drumski);

3) bankarstvo (kreditne institucije);

4) infrastruktura finansijskog tržišta (mjesta trgovanja i centralne druge ugovorne strane utvrđeni zakonom kojim se uređuje tržište kapitala);

5) zdravlje (pružanje zdravstvene zaštite na primarnom, sekundarnom i tercijalnom nivou, rad nacionalnih referentnih laboratorija, registracija i istraživanje ljekova);

6) voda za piće (snabdijevanje i distribucija vode namijenjene za ljudsku potrošnju);

7) otpadne vode (sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda i otpadnih voda privrede);

8) digitalna infrastruktura (pružaoci usluga za razmjenu internet saobraćaja, pružaoci DNS usluga osim operatora korijenskih servera naziva, registar naziva domena najvišeg nivoa, pružaoci usluge računarstva u oblaku, pružaoci usluga data centara, pružaoci mreže za isporuku sadržaja, pružaoci kvalifikovanih elektronskih usluga povjerenja, pružaoci javnih elektronskih komunikacionih mreža i javno dostupnih elektronskih komunikacionih usluga);

9) upravljanje uslugama informaciono-komunikacionih tehnologija (pružaoci usluga informaciono-komunikacionih tehnologija);

10) javna uprava (organi državne uprave i organi lokalne samouprave);

11) svemir.

Važni subjekti određuju se u okviru sljedećih sektora, odnosno podsektora:

1) poštanske i kurirske usluge (pružaoci univerzalnih poštanskih usluga, pružaoci komercijalnih poštanskih usluga);

2) upravljanje otpadom (sakupljanje, odnosno transport otpada, prerada i zbrinjavanje otpada);

3) izrada, proizvodnja i distribucija hemikalija (proizvodnja i snabdijevanje hemikalijama u skladu sa zakonom kojim se uređuju hemikalije);

4) proizvodnja, prerada i distribucija hrane (veleprodaja, industrijska proizvodnja i prerada);

5) proizvodnja (proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda; proizvodnja računara, elektronskih i optičkih proizvoda; proizvodnja električne opreme; proizvodnja mašina i uređaja; proizvodnja motornih vozila, prikolica i poluprikolica; proizvodnja ostale opreme za transport);

6) pružaoci elektronskih usluga (pružaoci usluga na internet tržištu);

7) istraživačka djelatnost (subjekti koji imaju za primarni cilj da sprovedu primijenjena istraživanja ili eksperimentalni razvoj kako bi se rezultati tih istraživanja koristili u komercijalne svrhe).

Pored subjekata iz stava 2 ovog člana, kao važni subjekti mogu biti određeni i subjekti u okviru sektora, odnosno podsektora iz stava 1 ovog člana, koji nijesu određeni kao ključni subjekti, ako se ispune kriterijumi iz člana 4 stav 2 ovog zakona.

Prikupljanje podataka od značaja za određivanje ključnih i važnih subjekata

Član 20

Ministarstvo nadležno za sektor, odnosno podsektor u kojem se određuju ključni, odnosno važni subjekti (u daljem tekstu: nadležno ministarstvo) sačinjava listu svih organa i drugih subjekata u tom sektoru, odnosno podsektoru i dostavlja im zahtjev za prikupljanje podataka od značaja za određivanje ključnih i važnih subjekata.

Podaci od značaja za određivanje ključnih i važnih subjekata su:

1) naziv organa, odnosno drugog subjekta;
2) sjedište, odnosno adresa organa, odnosno drugog subjekta;
3) poreski identifikacioni broj organa, odnosno drugog subjekta;
4) ime i prezime odgovornog lica u organu, odnosno drugom subjektu;
5) jedinstvena službena adresa za elektronsku komunikaciju organa, odnosno drugog subjekta;
6) kontakt telefon odgovornog lica u organu, odnosno drugom subjektu;
7) podaci o nadležnosti, odnosno djelatnosti organa, odnosno drugog subjekta;
8) podaci kojem sektoru, odnosno podsektoru iz člana 19 st. 1 i 2 ovog zakona pripada organ, odnosno drugi subjekat.

Organi i drugi subjekti iz stava 1 ovog člana dužni su da nadležnom ministarstvu podatke iz stava 2 ovog člana dostave u roku od sedam dana od dana prijema zahtjeva.

U slučaju promjene podataka iz stava 2 ovog člana, organi i drugi subjekti dužni su da o tome obavijeste nadležno ministarstvo, u roku od 14 dana od dana nastanka promjene.

Predlog sektorske liste ključnih i važnih subjekata

Član 21

Na osnovu podataka iz člana 20 stav 2 ovog zakona, nadležno ministarstvo sačinjava predlog sektorske liste ključnih i važnih subjekata.

Predlog sektorske liste iz stava 1 ovog člana nadležno ministarstvo dostavlja Ministarstvu.

Lista ključnih i važnih subjekata

Član 22

Nakon dobijanja predloga sektorskih lista od nadležnih ministarstava, Ministarstvo sačinjava objedinjeni predlog liste ključnih i važnih subjekata i dostavlja ga Vladi.

Vlada, na predlog Ministarstva, utvrđuje Listu ključnih i važnih subjekata.

Lista iz stava 2 ovog člana sadrži sljedeće podatke o ključnim i važnim subjektima, i to:

1) naziv;
2) sjedište, odnosno adresu;
3) poreski identifikacioni broj.

Obavještavanje ključnih i važnih subjekata

Član 23

U roku od sedam dana od dana utvrđivanja Liste ključnih i važnih subjekata, nadležno ministarstvo obavještava ključne i važne subjekte u sektoru, odnosno podsektoru za koji je nadležno da su određeni kao ključni, odnosno važni subjekti.

Sektorski registar ključnih i važnih subjekata

Član 24

Na osnovu Liste ključnih i važnih subjekata, nadležno ministarstvo vodi Sektorski registar ključnih i važnih subjekata, koji sadrži podatke iz člana 20 stav 2 tač. 1 do 7 ovog zakona koji se odnose na ključne i važne subjekte u sektoru, odnosno podsektoru za koji je nadležno.

Podatke iz stava 1 ovog člana nadležno ministarstvo dostavlja Ministarstvu radi vođenja registra iz člana 25 ovog zakona.

Zbirni registar ključnih i važnih subjekata

Član 25

Na osnovu Liste ključnih i važnih subjekata i podataka koje nadležna ministarstva dostave saglasno članu 24 ovog zakona, Ministarstvo vodi Zbirni registar ključnih i važnih subjekata.

Zbirni registar ključnih i važnih subjekata sadrži podatke iz člana 20 stav 2 tač. 1 do 7 ovog zakona koji se odnose na sve ključne i važne subjekte.

Ažuriranje registara i Liste ključnih i važnih subjekata

Član 26

Ključni i važni subjekti dužni su da nadležnom ministarstvu dostave obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene.

Na osnovu obavještenja iz stava 1 ovog člana, nadležno ministarstvo ažurira Sektorski registar ključnih i važnih subjekata i o promjeni podataka obavještava Ministarstvo.

Na osnovu obavještenja iz stava 2 ovog člana, Ministarstvo ažurira Zbirni registar ključnih i važnih subjekata.

Ako, na osnovu obavještenja iz stava 1 ovog člana, utvrdi da je potrebno izvršiti izmjene, odnosno dopune Liste ključnih i važnih subjekata, Ministarstvo sačinjava predlog izmjena, odnosno dopuna Liste ključnih i važnih subjekata i dostavlja ga Vladi radi utrđivanja tih izmjena, odnosno dopuna.

Tajnost podataka, registara i listi ključnih i važnih subjekata

Član 27

Podaci iz člana 20 stav 2 ovog zakona i obavještenje iz člana 20 stav 4 ovog zakona, predlog sektorske liste iz člana 21 ovog zakona, predlog liste i Lista ključnih i važnih subjekata iz člana 22 ovog zakona, obavještenje iz člana 23 ovog zakona, Sektorski registar iz člana 24 ovog zakona, Zbirni registar iz člana 25 ovog zakona, obavještenja iz člana 26 st. 1 i 2 ovog zakona, kao i predlog izmjena, odnosno dopuna Liste ključnih i važnih subjekata iz člana 26 stav 4 ovog zakona označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

IV. PROCJENA UTICAJA SAJBER PRIJETNJE, OZBILJNE SAJBER PRIJETNJE I INCIDENTA I RJEŠAVANJE INCIDENTA I SAJBER KRIZE

Kriterijumi za procjenu uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta

Član 28

U slučaju nastanka sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta na mrežnom i informacionom sistemu, organi i drugi subjekti dužni su da vrše procjenu uticaja tih sajber prijetnji, odnosno incidenta na kontinuitet pružanja usluga.

Procjena iz stava 1 ovog člana vrši se na osnovu sljedećih kriterijuma:

1) broj korisnika koji nijesu mogli da ostvare pristup usluzi;
2) broj korisnika koji su imali značajne teškoće u ostvarivanju pristupa usluzi;
3) vrijeme trajanja sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta;
4) geografska zastupljenost sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta (ako je moguće utvrditi).

Sajber prijetnja, ozbiljna sajber prijetnja i incident koji nemaju uticaj na kontinutet pružanja usluga

Član 29

U slučaju da se na osnovu kriterijuma iz člana 28 stav 2 ovog zakona, procijeni da sajber prijetnja, ozbiljna sajber prijetnja, odnosno incident nemaju uticaj na kontinuitet pružanja

usluga, izvještaj o tim sajber prijetnjama i incidentima, jednom mjesečno, organi i drugi subjekti, osim organa državne uprave dostavljaju Agenciji, a organi državne uprave CIRT-u državne uprave.

U slučaju iz stava 1 ovog člana, organi i drugi subjekti sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidente rješavaju bez učešća Agencije, odnosno CIRT-a državne uprave.

Sajber prijetnja, ozbiljna sajber prijetnja i incident koji negativno utiču na kontinutet pružanja usluga

Član 30

U slučaju da se na osnovu kriterijuma iz člana 28 stav 2 ovog zakona, procijeni da bi sajber prijetnja, ozbiljna sajber prijetnja, odnosno incident mogli u značajnoj mjeri negativno da utiču na kontinuitet pružanja usluga, o tim sajber prijetnjama i incidentima, organi i drugi subjekti, osim organa državne uprave dostavljaju početno obavještenje Agenciji, a organi državne uprave CIRT-u državne uprave.

Početno obavještenje dostavlja se najkasnije u roku od 24 časa od trenutka saznanja za taj incident, na propisanom obrascu.

Izgled i sadržaj obrasca početnog obavještenja propisuje Ministarstvo.

Određivanje nivoa negativnog uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta na kontinuitet pružanja usluga

Član 31

Po prijemu početnog obavještenja Agencija, odnosno CIRT državne uprave sprovodi analizu uticaja sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta na kontinuitet pružanja usluga i mogućih načina reagovanja na te sajber prijetnje, odnosno incident i utvrđuje nivo incidenta koji može biti niski, srednji ili visoki.

Bliži način sprovođenja analize i kriterijume za utvrđivanje nivoa incidenta iz stava 1 ovog člana propisuje Vlada.

Incident niskog nivoa

Član 32

Ako, po prijemu početnog obavještenja, utvrdi da je incident niskog nivoa, Agencija, odnosno CIRT državne uprave, u roku od 24 časa od prijema tog obavještenja, organu, odnosno drugom subjektu može, ako je to potrebno, dati smjernice za reagovanje na nastali incident.

Incident srednjeg nivoa

Član 33

Ako, po prijemu početnog obavještenja, utvrdi da je incident srednjeg nivoa, Agencija, odnosno CIRT državne uprave, odmah, a najkasnije u roku od 24 časa od prijema tog obavještenja, daje smjernice za reagovanje na nastali incident i učestvuje u rješavanju tog incidenta.

U toku trajanja incidenta iz stava 1 ovog člana, organi i drugi subjekti dužni su da, u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave dostave prvi izvješta trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Ako tokom trajanja incidenta iz stava 1 ovog člana organi i drugi subjekti saznaju za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident, dužni su da, o tome Agenciji, odnosno CIRT-u državne uprave, bez odlaganja, dostave poseban izvještaj na propisanom obrascu.

Ako incident iz stava 1 ovog člana traje i nakon isteka roka iz stava 2 ovog člana, organi i drugi subjekti dužni su da, svakih 72 časa, dostavljaju Agenciji, odnosno CIRT-u državne uprave kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Nakon rješavanja incidenta iz stava 1 ovog člana, a najkasnije u roku od 30 dana od dana rješavanja tog incidenta, organi i drugi subjekti dužni su da Agenciji, odnosno CIRT-u državne uprave dostave završni izvještaj o tom incidentu, na propisanom obrascu.

Izgled i sadržaj obrazaca izvještaja iz st. 2 do 5 ovog člana propisuje Ministarstvo.

Incident visokog nivoa
Član 34

Ako, po prijemu početnog obavještenja, utvrdi da je incident visokog nivoa, Agencija je dužna o tome da obavijesti CIRT državne uprave, odnosno CIRT državne uprave Agenciju, bez odlaganja, u pisanoj formi.

U slučaju iz stava 1 ovog člana, Agencija i CIRT državne uprave zajedno učestvuju u rješavanju incidenta i organu i drugom subjektu daju smjernice za reagovanje na nastali incident.

Tokom trajanja incidenta iz stava 1 ovog člana, organi i drugi subjekti dužni su da u roku od 72 časa od podnošenja početnog obavještenja Agenciji, odnosno CIRT-u državne uprave dostave prvi izvještaj o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Ako tokom trajanja incidenta iz stava 1 ovog člana organi i drugi subjekti saznaju za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident, dužni su da o tome Agenciji, odnosno CIRT-u državne uprave, bez odlaganja, dostave poseban izvještaj na propisanom obrascu.

Ako incident iz stava 1 ovog člana traje i nakon isteka roka iz stava 3 ovog člana, organi i drugi subjekti dužni su da, svakih 24 časa, Agenciji, odnosno CIRT-u državne uprave dostavljaju kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Nakon rješavanja incidenta iz stava 1 ovog člana, a najkasnije u roku od 30 dana od dana rješavanja tog incidenta, organi i drugi subjekti dužni su da Agenciji, odnosno CIRT-u državne uprave dostave završni izvještaj o tom incidentu, na propisanom obrascu.

Izgled i sadržaj obrazaca izvještaja iz st. 3 do 6 ovog člana propisuje Ministarstvo.

Sajber kriza
Član 35

Ako Agencija i CIRT državne uprave ne mogu da riješe incident visokog nivoa u skladu sa članom 34 ovog zakona, u roku od deset dana od dana dostavljanja početnog obavještenja, Ministarstvo, uz prethodno pribavljeno mišljenje Agencije, dostavlja Vladi predlog za proglašenje sajber krize.

Predlog iz stava 1 ovog člana sadrži podatke o incidentu, preduzetim mjerama, razloge za proglašenje sajber krize i predlog mjera za rješavanje te krize.

Na osnovu predloga iz stava 1 ovog člana, Vlada donosi odluku o proglašenju sajber krize, sa mjerama za rješavanje sajber krize i zadužuje organe koji su dužni da učestvuju u rješavanju sajber krize.

Ministarstvo koordinira radom organa iz stava 3 ovog člana u rješavanju sajber krize i najmanje jednom nedeljno izvještava Vladu o svim aktivnostima.

Agencija u saradnji sa Ministarstvom sprovodi operativnu koordinaciju rješavanja sajber krize u skladu sa Nacionalnim planom za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu.

Nakon rješavanja sajber krize, Ministarstvo u saradnji sa Agencijom sačinjava završni izvještaj o sajber krizi i predlog za proglašenje da je sajber kriza završena, koje dostavlja Vladi.

Na osnovu izvještaja i predloga iz stava 6 ovog člana, Vlada donosi odluku o proglašenju završetka sajber krize.

Pomoć u rješavanju incidenta i sajber krize

Član 36

U rješavanju incidenta srednjeg, odnosno visokog nivoa i sajber krize Agencija i CIRT državne uprave mogu koristiti ekspertsku pomoć domaćih i međunarodnih institucija i organizacija, kao i razmjenjivati informacije sa tim instutucijama i organizacijama.

Tajnost obavještenja, izvještaja i smjernica

Član 37

Izvještaj iz člana 29 stav 1 ovog zakona, početno obavještenje iz člana 30 stav 1 ovog zakona, smjernice iz člana 32 i člana 33 stav 1 ovog zakona, izvještaji iz člana 33 st. 2 do 5 ovog zakona, obavještenje iz člana 34 stav 1 ovog zakona, smjernice iz člana 34 stav 2 ovog zakona, izvještaji iz člana 34 st. 3 do 6 ovog zakona, predlog i mišljenje iz člana 35 stav 1 ovog zakona, odluka iz člana 35 stav 3 ovog zakona, izvještaj iz člana 35 stav 4 ovog zakona, kao i izvještaj i predlog iz člana 35 stav 6 ovog zakona označavaju se odgovarajućim stepenom tajnosti u skladu sa zakonom kojim se uređuje tajnost podataka.

V. MINISTARSTVO I CIRT DRŽAVNE UPRAVE

Nadležnosti Ministarstva

Član 38

Ministarstvo:

1) predlaže Vladi strategije i akcione planove, kao i propise iz oblasti informacione bezbjednosti;

2) izrađuje Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu, u saradnji sa Agencijom;

3) vrši skeniranje mrežnih i informacionih sistema organa državne uprave, u cilju otkrivanja ranjivosti tih sistema;

4) donosi uputstva i procedure koje se sprovode prilikom procjene informacione bezbjednosti mrežnih i informacionih sistema organa državne uprave;

5) daje upozorenja, najave i informacije o rizicima i incidentima organima državne uprave;

6) postupa po prijavljenim incidentima na mrežnim i informacionim sistemima organa državne uprave;

7) vodi evidenciju o prijavljenim incidentima na mrežnim i informacionim sistemima organa državne uprave;

8) sarađuje sa Agencijom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize, u skladu sa ovim zakonom;

9) u cilju unapređenja informacione bezbjednosti sarađuje sa domaćim i međunarodnim institucijama i organizacijama, kao i privatnim i civilnim sektorom;

10) dostavlja Vladi izvještaj o stanju informacione bezbjednosti mrežnih i informacionih sistema organa državne uprave, najmanje jednom godišnje;

11) dostavlja Vladi i druge izvještaje, u skladu sa ovim zakonom;

12) vrši i druge poslove, u skladu sa ovim zakonom.

CIRT državne uprave

Član 39

Poslove iz člana 38 stav 1 tač. 3 do 9 ovog zakona vrši CIRT državne uprave.

CIRT državne uprave mora da ispunjava tehničke i druge uslove, i to da:

1) posjeduje sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju;

2) posjeduje prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama;

3) posjeduje adekvatan sistem za prijavljivanje i upravljanje incidentima;
4) obezbijedi povjerljivost i pouzdanost procesa rada;
5) posjeduje redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada;
6) ima dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa.

Redundantni sistemi, u smislu stava 2 tačka 5 ovog člana, su rezervni sistemi koji zamjenjuju primarni sistem, ako je došlo do prekida rada primarnog sistema.

VI. AGENCIJA ZA SAJBER BEZBJEDNOST

Poslovi Agencije
Član 40

Agencija:
1) prati i analizira primjenu propisa, strategija i akcionih planova u oblasti informacione bezbjednosti i daje predloge i preporuke za unapređenje informacione bezbjednosti;
2) prati i analizira propise Evropske unije i država članica Sjevernoatlantskog saveza u oblasti informacione bezbjednosti;
3) vrši proaktivno skeniranje mrežnih i informacionih sistema ključnih i važnih subjekata koji nijesu organi državne uprave, uz njihovu prethodnu saglasnost;
4) donosi uputstva i procedure koje se sprovode prilikom procjene informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, osim organa državne uprave;
5) daje upozorenja, najave i informacije o rizicima i incidentima organima i drugim subjektima, osim organa državne uprave;
6) postupa po prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;
7) vodi evidenciju o prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;
8) vrši stručni nadzor nad primjenom mjera informacione bezbjednosti kod organa i drugih subjekata, osim organa državne uprave;
9) vrši stručni nadzor utvrđivanjem da li ključni subjekti posjeduju certifikat o ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom;
10) učestvuje u implementaciji međunarodnih projekata u oblasti informacione bezbjednosti;
11) vrši edukaciju zaposlenih u organima i drugim subjektima u cilju jačanja informacione bezbjednosti;
12) sarađuje sa Ministarstvom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize, u skladu sa ovim zakonom;
13) u cilju unapređenja informacione bezbjednosti sarađuje sa domaćim i međunarodnim institucijama i organizacijama, kao i privatnim i civilnim sektorom;
14) dostavlja Vladi izvještaj o stanju informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata koji nijesu organi državne uprave, najmanje jednom godišnje.

Organi Agencije
Član 41

Organi Agencije su: Savjet Agencije i direktor Agencije.

Savjet Agencije
Član 42

Savjet Agencije ima predsjednika i četiri člana koje imenuje i razrješava Vlada.

Predsjednika Savjeta Agencije predlaže Ministarstvo, a po jednog člana Savjeta Agencije predlažu:

1) Univerzitet Crne Gore;
2) Privredna komora Crne Gore;
3) Crnogorska akademija nauka i umjetnosti;
4) Agencija iz reda zaposlenih.

Predsjednik i članovi Savjeta Agencije imenuju se na period od četiri godine.

Poslovi Savjeta Agencije
Član 43

Savjet Agencije:

1) donosi statut Agencije;
2) donosi godišnji program rada i finansijski plan Agencije;
3) usvaja i podnosi Vladi godišnji izvještaj o radu i finansijski izvještaj Agencije;
4) imenuje i razrješava direktora Agencije;
5) utvrđuje plan obuka za stručno usavršavanje zaposlenih u Agenciji;
6) donosi Etički kodeks zaposlenih u Agenciji;
7) vrši i druge poslove u skladu sa zakonom i statutom Agencije.

Finansijski plan Agencije donosi se uz prethodnu saglasnost organa državne uprave nadležnog za poslove finansija.

Prestanak mandata predsjednika i člana Savjeta Agencije
Član 44

Predsjedniku, odnosno članu Savjeta Agencije prestaje mandat:

1) istekom vremena na koje je imenovan;
2) ostavkom;
3) razrješenjem.

Predsjednik, odnosno član Savjeta Agencije razrješava se ako:

1) je osuđen na bezuslovnu kaznu zatvora;
2) je osuđen za krivično djelo koje ga čini nedostojnim za vršenje dužnosti;
3) postupa suprotno zakonu ili aktima Agencije;
4) nestručno ili nesavjesno vrši poslove za koje je imenovan.

Direktor Agencije
Član 45

Direktor Agencije imenuje se osnovu javnog konkursa koji raspisuje Savjet Agencije.

Za direktora Agencije može biti imenovano lice koje, pored opštih uslova za zasnivanje radnog odnosa u državnim organima, ispunjava sljedeće uslove, i to da ima:

1) VII1 nivo kvalifikacije obrazovanja i
2) radno iskustvo, i to:

- pet godina radnog iskustva u oblasti informacione bezbjednosti ili
- sedam godina radnog iskustva u državnim organima ili organima državne uprave ili deset godina radnog iskustva, od čega pet godina radnog iskustva na poslovima rukovođenja.

Mandat direktora Agencije traje pet godina.

Poslovi direktora Agencije
Član 46

Direktor Agencije:

1) predstavlja i rukovodi Agencijom;

2) zastupa Agenciju i odgovara za zakonitost i kvalitet rada Agencije;
3) organizuje rad u Agenciji;
4) predlaže Savjetu Agencije statut Agencije, godišnji program rada i finansijski plan Agencije, godišnji izvještaj o radu i finansijski izvještaj Agencije, kao i druge odluke;
5) izvršava odluke Savjeta Agencije;
6) upravlja ljudskim i finansijskim resursima;
7) utvrđuje akt o unutrašnjoj organizaciji i sistematizaciji Agencije;
8) stara se o obezbjeđivanju javnosti rada Agencije;
9) predlaže plan obuka za stručno usavršavanje zaposlenih u Agenciji;
10) sarađuje sa domaćim i međunarodnim organizacijama, kao i privatnim i civilnim sektorom u cilju unapređenja informacione bezbjednosti;
11) vrši druge poslove u skladu sa zakonom i statutom Agencije.

Akt o unutrašnjoj organizaciji i sistematizaciji Agencije utvrđuje se uz prethodnu saglasnost organa državne uprave nadležnog za poslove finansija.

Prestanak mandata direktora Agencije
Član 47

Na prestanak mandata direktora Agencije primjenjuju se odredbe zakona kojim se uređuju prava i obaveze državnih službenika i namještenika, a koje se odnose na prestanak mandata starješine organa uprave.

Status Agencije
Član 48

Agencija ima svojstvo pravnog lica i status državne agencije.
Agencija za svoj rad odgovara Vladi.
Odluku o osnivanju Agencije donosi Vlada.

Statut Agencije
Član 49

Agencija ima statut.
Statutom Agencije uređuju se sjedište Agencije, unutrašnja organizacija Agencije, način rada, odlučivanja i nadležnosti organa Agencije, javnost rada i druga pitanja od značaja za rad Agencije.
Na statut Agencije saglasnost daje Vlada.

Finansiranje Agencije
Član 50

Sredstva za rad Agencije obezbjeđuju se u budžetu Crne Gore.
Agencija je dužna da svoje finansijsko poslovanje organizuje i vodi u skladu sa propisima kojima se uređuje oblast budžetskog sistema i budžetskog računovodstva.

Primjena drugih propisa
Član 51

Na prava, obaveze i odgovornosti zaposlenih u Agenciji primjenjuju se propisi o državnim službenicima i namještenicima.
Zaposleni u Agenciji imaju mjesečni dodatak na zaradu u iznosu do 30%.
Direktor Agencije ima pravo na zaradu u visini koja je određena za direktora Agencije za sprječavanje korupcije.

VII. STRUČNI NADZOR

Nadzornik
Član 52

Agencija vrši stručni nadzor u skladu sa ovim zakonom preko zaposlenih lica u Agenciji, koja su ovlašćena za obavljanje poslova stručnog nadzora u skladu sa aktom o unutrašnjoj organizaciji i sistematizaciji Agencije (u daljem tekstu: nadzornik).

Nadzornik može biti lice koje, pored opštih uslova za zasnivanje radnog odnosa u državnim organima, ispunjava sljedeće uslove, i to da ima:

1) VII1 nivo kvalifikacije obrazovanja i
2) pet godina radnog iskustva u oblasti informacione bezbjednosti.

Ovlašćenja nadzornika
Član 53

U postupku stručnog nadzora, nadzornik ima ovlašćenje da kod organa i drugih subjekata, osim organa državne uprave vrši kontrolu primjene mjera informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Pored ovlašćenja iz stava 1 ovog člana, u postupku stručnog nadzora, nadzornik ima ovlašćenje da kod ključnih i važnih subjekata osim organa državne uprave vrši i kontrolu primjene mjera informacione bezbjednosti iz člana 16 ovog zakona.

Pored ovlašćenja iz st. 1 i 2 ovog člana, u postupku stručnog nadzora, nadzornik ima ovlašćenje da kod ključnih subjekata osim organa državne uprave vrši kontrolu da li ti subjekti posjeduju certifikat o ispunjenost uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom.

Obaveze ključnih i važnih subjekata prilikom vršenja stručnog nadzora
Član 54

Radi vršenja stručnog nadzora, organi i drugi subjekti, osim organa državne uprave dužni su da nadzorniku omoguće pristup prostoru, računarskoj opremi i uređajima, kao i da bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora.

Zapisnik
Član 55

O izvršenom stručnom nadzoru nadzornik sačinjava zapisnik i dostavlja ga organu, odnosno drugom subjektu, osim organa državne uprave kod kojeg je vršen stručni nadzor, u roku od tri dana od dana izvršenog nadzora.

Otklanjanje nepravilnosti
Član 56

U slučaju da su u vršenju stručnog nadzora utvrđene nepravilnosti, nadzornik upozorava organ, odnosno drugi subjekat, osim organa državne uprave kod kojeg je utvrđena nepravilnost i ostavlja mu primjeren rok za otklanjanje te nepravilnosti, što konstatuje u zapisniku iz člana 55 ovog zakona.

Ako organ, odnosno drugi subjekat, osim organa državne uprave ne otkloni nepravilnosti u skladu sa stavom 1 ovog člana, zapisnik iz člana 55 ovog zakona, nadzornik dostavlja i direktoru Agencije.

U slučaju iz stava 2 ovog člana, direktor Agencije donosi rješenje kojim nalaže mjere za otklanjanje nepravilnosti.

Protiv rješenja iz stava 3 ovog člana može se pokrenuti upravni spor.

Primjena drugih propisa u vršenju stručnog nadzora
Član 57

Na postupak i način vršenja stručnog nadzora, obaveze i ovlašćenja nadzornika i druga pitanja od značaja za vršenje stručnog nadzora shodno se primjenjuju propisi kojima se uređuje inspekcijski nadzor i upravni postupak, ako ovim zakonom nije drukčije određeno.

Postupanje sa podacima
Član 58

Nadzornik je dužan da čuva i štiti podatke do kojih je došao prilikom vršenja stručnog nadzora, u skladu sa zakonima kojima se uređuju tajnost podataka, zaštita podataka o ličnosti i zaštita poslovne tajne.

Službena legitimacija nadzornika
Član 59

Nadzorniku se, radi dokazivanja svojstva nadzornika, izdaje službena legitimacija.

Službenu legitimaciju iz stava 1 ovog člana izdaje Agencija na propisanom obrascu.

U slučaju gubitka ili nestanka službene legitimacije iz stava 1 ovog člana, nadzornik o tome obavještava direktora Agencije, u roku od tri dana od dana gubitka, odnosno nestanka legitimacije i oglašava je nevažećom u "Službenom listu Crne Gore".

Danom prestanka radnog odnosa u Agenciji, odnosno prestankom svojstva nadzornika, nadzornik vraća službenu legitimaciju iz stava 1 ovog člana Agenciji.

O izdatim i vraćenim službenim legitimacijama iz stava 1 ovog člana Agencija vodi evidenciju koja sadrži: redni broj, ime i prezime nadzornika, serijski broj legitimacije, datum izdavanja, datum vraćanja, odnosno gubitka ili nestanka legitimacije, potpis nadzornika i napomenu.

Izgled i sadržaj obrasca službene legitimacije iz stava 1 ovog člana propisuje Agencija.

Tehnički i drugi uslovi koje treba da ispunava Agencija
Član 60

Agencija mora da ispunjava tehničke i druge uslove iz člana 39 stav 2 ovog zakona.

VIII. SAVJET ZA INFORMACIONU BEZBJEDNOST

Obrazovanje Savjeta za informacionu bezbjednost
Član 61

Radi praćenja razvoja informacione bezbjednosti, a naročito sajber bezbjednosti u cilju obezbjeđivanja bezbjednog sajber prostora Crne Gore, Vlada obrazuje Savjet za informacionu bezbjednost.

Savjet za informacionu bezbjednost obrazuje se na vrijeme od četiri godine.

Sastav Savjeta za informacionu bezbjednost
Član 62

Savjet za informacionu bezbjednost čine predstavnici Ministarstva, Agencije, organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa državne uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.

Stručne i administrativno-tehničke poslove za potrebe Savjeta za informacionu bezbjednost obavlja Ministarstvo.

Akt o obrazovanju Savjeta za informacionu bezbjednost
Član 63

Aktom o obrazovanju Savjeta za informacionu bezbjednost utvrđuju se zadaci, način rada, kao i druga pitanja od značaja za rad tog Savjeta

IX. INSPEKCIJSKI NADZOR

Upravni nadzor
Član 64

Upravni nadzor nad sprovođenjem ovog zakona, drugih propisa i akata donijetih na osnovu ovog zakona vrši Ministarstvo.

Inspekcijski nadzor
Član 65

Inspekcijski nadzor nad primjenom mjera informacione bezbjednosti kod organa državne uprave vrši inspektor za usluge informacionog društva (u daljem tekstu: inspektor) u skladu sa ovim zakonom i zakonom kojim se uređuje inspekcijski nadzor.

Posebna ovlašćenja inspektora
Član 66

U postupku inspekcijskog nadzora inspektor, pored ovlašćenja utvrđenih zakonom kojim se uređuje oblast inspekcijskog nadzora, ima ovlašćenje da kod organa državne uprave vrši kontrolu primjene mjera informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Pored ovlašćenja iz stava 1 ovog člana, u postupku inspekcijskog nadzora, inspektor ima ovlašćenje da kod organa državne uprave koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti vrši kontrolu primjene mjera informacione bezbjednosti iz člana 16 ovog zakona.

Pored ovlašćenja iz st. 1 i 2 ovog člana, u postupku inspekcijskog nadzora, inspektor ima ovlašćenje da kod organa državne uprave koji su u skladu sa ovim zakonom određeni kao ključni subjekti vrši kontrolu da li ti organi posjeduju certifikat o ispunjenost uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom.

Obaveze organa državne uprave prilikom vršenja inspekcijskog nadzora
Član 67

Radi vršenja inspekcijskog nadzora, organi državne uprave dužni su da inspektoru omoguće pristup prostoru, računarskoj opremi i uređajima, kao i da bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora.

X. KAZNENE ODREDBE

Član 68

Novčanom kaznom u iznosu od 500 do 20.000 eura kazniće se za prekršaj pravno lice - ključni subjekat, ako:

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona (član 18 stav 1);

2) ne ispunjava uslove u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 (član 18 stav 4);

3) od akreditovanog pravnog lica ne zahtijeva periodičnu provjeru ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 (član 18 stav 6);

4) nadležnom ministarstvu ne dostavi obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene (član 26 stav 1).

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 1.500 eura.

Član 69

Novčanom kaznom u iznosu od 500 do 10.000 eura kazniće se za prekršaj pravno lice - važni subjekat, ako:

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona (član 18 stav 1);

2) nadležnom ministarstvu ne dostavi obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene (član 26 stav 1).

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 1.500 eura.

Član 70

Novčanom kaznom u iznosu od 500 do 5.000 eura kazniće se za prekršaj pravno lice, ako:

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona (član 18 stav 2);

2) ne odredi zaposleno lice za praćenje primjene mjera informacione bezbjednosti (član 18 stav 3);

3) nadležnom ministarstvu ne dostavi podatke u roku od sedam dana od dana prijema zahtjeva (član 20 stav 3);

4) nadležno ministarstvo ne obavijesti o promjeni podataka u roku od 14 dana od dana nastanka promjene (član 20 stav 4);

5) izvještaj o sajber prijetnjama, ozbiljnim sajber prijetnjama, odnosno incidentima, jednom mjesečno ne dostavi Agenciji, odnosno CIRT-u državne uprave (član 29 stav 1);

6) ne dostavi početno obavještenje Agenciji, odnosno CIRT-u državne uprave o sajber prijetnji, ozbiljnoj sajber prijetnji odnosno incidentu koji bi mogli u značajnoj mjeri da utiču na kontinuitet pružanja usluga (član 30 stav 1);

7) ne dostavi početno obavještenje za incident na propisanom obrascu u roku od 24 časa (član 30 stav 2);

8) u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave ne dostavi prvi izvještaj o trajanju incidenta srednjeg nivoa i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 33 stav 2);

9) bez odlaganja ne dostavi poseban izvještaj na propisanom obrascu, Agenciji, odnosno CIRT-u državne uprave, a tokom trajanja incidenta srednjeg nivoa sazna za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident (član 33 stav 3);

10) Agenciji, odnosno CIRT-u državne uprave svakih 72 časa, ne dostavi kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje incidenta srednjeg nivoa, na propisanom obrascu (član 33 stav 4);

11) Agenciji, odnosno CIRT-u državne uprave ne dostavi završni izvještaj o incidentu srednjeg nivoa, najkasnije u roku od 30 dana od dana rješavanja tog incidenta, na propisanom obrascu (član 33 stav 5);

12) u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave ne dostavi prvi izvještaj o trajanju incidenta visokog nivoa i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 34 stav 3);

13) bez odlaganja ne dostavi poseban izvještaj na propisanom obrascu, Agenciji, odnosno CIRT-u državne uprave, a tokom trajanja incidenta visokog nivoa sazna za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident (član 34 stav 4);

14) svakih 24 časa, Agenciji, odnosno CIRT-u državne uprave ne dostavi kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 34 stav 5);

15) Agenciji, odnosno CIRT-u državne uprave ne dostavi završni izvještaj o incidentu srednjeg nivoa, najkasnije u roku od 30 dana od dana rješavanja tog incidenta, na propisanom obrascu (član 34 stav 6).

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 1.500 eura.

U slučaju ponavljanja povreda iz stava 1 ovog člana izreći će se zabrana obavljanja vršenja poziva, djelatnosti ili dužnosti u trajanju od tri do šest mjeseci.

XI. PRELAZNE I ZAVRŠNE ODREDBE

Rok za donošenje podzakonskih akata
Član 71

Podzakonski akti za sprovođenje ovog zakona donijeće se u roku od šest mjeseci od dana stupanja na snagu ovog zakona.

Do donošenja podzakonskih akata iz stava 1 ovog člana primjenjivaće se podzakonski akti donijeti na osnovu Zakona o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21).

Rok za dostavljanje predloga sektorskih listi
Član 72

Nadležna ministarstva dužna su da predloge sektorskih listi iz člana 21 stav 1 ovog zakona dostave Ministarstvu, najkasnije u roku od devet mjeseci od dana stupanja na snagu ovog zakona.

Rok za dobijanje certifikata
Član 73

Ključni subjekti dužni su da dobiju certifikat o ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001, u roku od dvije godine i šest mjeseci od dana stupanja na snagu ovog zakona.

Rok za osnivanje Agencije
Član 74

Odluka o osnivanju Agencije donijeće se u roku od 15 dana od dana stupanja na snagu ovog zakona.

Rok za imenovanje predsjednika i članova Savjeta Agencije
Član 75

Imenovanje predsjednika i članova Savjeta Agencije izvršiće se u roku od 60 dana od dana stupanja na snagu ovog zakona.

Rok za imenovanje direktora Agencije
Član 76

Imenovanje direktora Agencije izvršiće se u roku od 90 dana od dana izbora Savjeta Agencije.

Do imenovanja direktora Agencije, u skladu sa ovim zakonom poslove direktora Agencije obavljaće vršilac dužnosti, koga, na predlog ministra javne uprave, odredi Vlada.

Predlog iz stava 2 ovog člana dostaviće se Vladi u roku od 15 dana od dana stupanja na snagu ovog zakona.

Donošenje akata Agencije
Član 77

Statut Agencije, akt o unutrašnjoj organizaciji i sistematizaciji Agencije, poslovnik o radu Savjeta i drugi akti Agencije donijeće se u roku od 90 dana od dana izbora vršioca dužnosti direktora Agencije.

Preuzimanje državnih službenika

Član 78

Danom donošenja akta o unutrašnjoj organizaciji i sistematizaciji Agencije, Agencija će od Direkcije za zaštitu tajnih podataka preuzeti državne službenike koji su vršili poslove u okviru organizacione jedinice CIRT, opremu i službenu dokumentaciju.

Državni službenici iz stava 1 ovog člana, do donošenja akta o raspoređivanju u skladu sa aktom u unutrašnjoj organizaciji i sistematizaciji Agencije, nastavljaju sa radom u zvanjima koja su stekli prije preuzimanja.

Državni službenici iz stava 1 ovog člana koji ne budu raspoređeni u skladu sa aktom o unutrašnjoj organizaciji i sistematizaciji Agencije ostvaruju prava u skladu sa propisima o državnim službenicima i namještenicima.

Rad Savjeta za informacionu bezbjednost

Član 79

Savjet za informacionu bezbjednost koji se obrazovan u skladu sa Zakonom o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21) nastavlja sa radom do obrazovanja Savjeta za informacionu bezbjednost u skladu sa ovim zakonom.

Prestanak važenja propisa

Član 80

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21) i odredbe člana 74 stav 1 tačka 8b i člana 74a Zakona o tajnosti podataka ("Službeni list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20).

Stupanje na snagu

Član 81

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

---

* Ovaj zakon usklađen je sa Direktivom (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

OBRAZLOŽENJE

I. USTAVNI OSNOV ZA DONOŠENJE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u odredbi člana 16 Ustava Crne Gore kojim je, između ostalog, propisano da se zakonom, u skladu sa Ustavom, uređuju određena pitanja od interesa za Crnu Goru.

II. RAZLOZI ZA DONOŠENJE ZAKONA

Prvi Zakon o informacionoj bezbjednosti u Crnoj Gori donijet je 2010. godine i uredio je mjere i standarde informacione bezbjednosti, kao i sistem zaštite i prevencije od bezbjednosnih incidenata na internetu. Ovaj zakon donijet je u periodu prije usvajanja Direktive EU o mjerama za visok nivo informacione bezbjednosti mrežnih i informacionih sistema u Evropskoj uniji br. 2016/1148 (NIS Direktiva). Izmjenama i dopunama Zakona iz 2016. godine, kroz prepoznavanje Savjeta za informacionu bezbjednost, kao i osnova za uređivanje mjera zaštite kritične informatičke infrastrukture, ovaj zakon je djelimično usklađen sa pomenutom direktivom.

Evropska unija krajem 2022. godine, usvojila je Direktivu (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2), nakon čega je Crna Gora prateći trendove EU pristupila transponovanju navedene direktive u Predlog zakona o informacionoj bezbjednosti.

Programom rada Vlade za 2023. godinu, u okviru oblasti 5. Digitalna transformacija pod ciljem 5.2 Jačanje Vladine informatičke infrastrukture, kao aktivost pod br. ND 130 predviđen je Predlog zakona o informacionoj bezbjednosti, čiji rok završetka je planiran za III kvartal 2023. godine.

Novi izazov sa kojim se Crna Gora suočila tokom sajber napada visokog nivoa sofisticiranosti koji se dogodio u avgustu 2022. godine, zahtijeva osnaživanje postojećih mehanizama za odgovor na iste, kao i stvaranje novih mehanizama, sa posebnim akcentom na upravljanje kriznim situacijama, koje u važećoj zakonskoj regulativi nijesu bile prepoznate.

U cilju efikasnijeg odgovora na sajber prijetnje, ozbijne sajber prijetnje, incidente i sajber krizu, planirano je uspostavljanje Agencije za sajber bezbjednost, kao i podizanje kapaciteta za sajber odbranu između ostalog i kroz formiranje i stavljanje u funkciju tima za odbranu od sajber prijetnji i incidenata - CIRTa državne uprave, organizacione jedinice u Ministarstvu javne uprave koje je u skladu sa posebnim zaduženo za upravljanje Vladinom informačkom infrastrukturom i informaciono-komunikacionom mrežom organa.

Kako bi se realizovale planirane aktivnosti u cilju podizanja informacione i sajber bezbjednosti na najviši nivo, neophodno je ovu oblast normativno urediti, čime bi se definisale nadležnosti Agencije za sajber bezbjednost i CIRT-a državne uprave. Takođe, po prvi put ovim zakonom definisaće se ključni i važni subjekti kao nosioci kritične informatičke infrastrukture, mjere informacione bezbjednosti, uključujući mjeru upravljanja rizicima u oblasti sajber bezbjednosti, kao i postupak kontrole primjene tih mjera kroz uspostavljanje stručnog nadzora čime će biti omogućena regulatorna funkcija nad ključnim i važnim subjektim.

Donošenjem novog Zakona o informacionoj bezbjednosti značajno bi se unaprijedila ova oblast, uspostavile jasne nadležnosti i procedure u slučaju budućih eventualnih sajber prijetnji i incidenata, kao i mjere informacione bezbjednosti koje prate trendove Evropske unije. Takođe, uspostavio bi se održiv sistem za efikasno otkrivanje i odbranu od sajber prijetnji i incidenata visokog nivoa sofisticiranosti i osigurao kontinuitet pružanja usluga u slučaju budućih incidenata, čime se doprinosi efikasnijem funkcionisanju privrede i društva uopšte i jačanju povjerenja korisnika elektronske uprave u zaštitu njihovih podataka.

III. USAGLAŠENOST SA PRAVNOM TEKOVINOM EVROPSKE UNIJE I POTVRĐENIM MEĐUNARODNIM KONVENCIJAMA

U okviru pregovaračkog procesa za pridruživanje Evropskoj uniji, oblast informacione bezbjednosti razmatra se u okviru Pregovaračkog poglavlja 10 „Informatičko društvo i mediji". Zakon o informacionoj bezbjednosti predstavlja jedan od ključnih koraka ka harmonizaciji pravnog okvira države Crne Gore sa Evropskom unijom u oblasti informacionog društva.

Predlog zakona usklađen je sa Direktivom (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

IV. OBJAŠNJENJE OSNOVNIH PRAVNIH INSTITUTA

U poglavlju I. U osnovnim odredbama Nacrta zakona o informacionoj bezbjednosti članom 1 ovog zakona definisan je predmet zakona, odnosno da se ovim zakonom propisuju mjere informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema, uključujući sajber bezbjednost, određivanje ključnih i važnih subjekata, upravljanje sajber bezbjednošću, kao i druga pitanja od značaja za informacionu bezbjednost.

Odredbom člana 2 propisano se da su po ovom zakonu obavezni da postupaju državni organi, ministarstva i drugi organi uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica koja vrše javna ovlašćenja (organi), privredna društva i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom (drugi subjekti).

Takođe, u ovom poglavlju pored ostalog, definisana je i sama informaciona bezbjednost, kao i ključni i važni subjekti, na način što je propisano da se ključnim subjektima smatraju organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od posebnog značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do ugrožavanja života, zdravlja, bezbjednosti građana i funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastruktre u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture, dok se važnim subjektima smatraju organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do otežanog funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastruktre u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture.

Isto tako definsano je da zaštitu mrežnih i informacionih sistema organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata vrši organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave (Ministarstvo) preko posebne organizacione jedinice (CIRT državne uprave), kao i da Ministarstvo predstavlja jedinstvenu nacionalnu kontaktnu tačku za informacionu bezbjednost i sarađuje sa jedinstvenim nacionalnim kontakt tačkama drugih država, dok je u odnosu na Agenciju za sajber bezbejdnost propisano da vrši zaštitu mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata.