**OBRAZAC**

|  |  |
| --- | --- |
| IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA | |
| PREDLAGAČ PROPISA | Ministarstvo javne uprave |
| NAZIV PROPISA | Nacrt 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 ("Službeni list CG", br. [14/2010](javascript:void(0)), [40/2016](javascript:void(0)), [74/2020](javascript:void(0)) i 67/2021) kada je prvi put uređena oblast bezbjednosti u informaciono-komunikacionim tehnologijama.  Izradi novog Zakona o informacionoj bezbjednosti pristupilo se u cilju jačanja informacione bezbjednosti u Crnoj Gori, prepoznavanjem mehanizama za jačanje informacione bezbjednosti (Agencija za sajber bezbjednost i Vladin CIRT), stvaranjem jasno definisanog nacionalnog okvira za upravljanje sajber bezbjednošću, kao i usaglašavanjem sa Direktivom (EU) 2022/2555 EVROPSKOG PARLAMENTA I SAVJETA od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i o ukidanju Direktive (EU) 2016/1148 (NIS 2 Direktiva).  Naime, Crna Gora našla se na meti sajber napada visokog nivoa sofisticiranosti, koji se dogodio 20. avgusta 2022. godine. Predmetnim sajber napadom primarno je pogođena Vladina informatička infrastruktura i informaciono-komunikaciona mreža organa, koji su bili pod kontinuiranim sajber napadima velikog intenziteta i kompleksnosti. Nastali sajber napad onemogućio 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.  Neusaglašenosti Direktivom (EU) 2022/2555 EVROPSKOG PARLAMENTA I SAVJETA od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i o ukidanju Direktive (EU) 2016/1148 (NIS 2 Direktiva).  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]](#footnote-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 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?  Cilj ovog zakona je:   * Postizanje visokog nivoa informacione i sajber bezbjednosti kroz izgradnju sajber bezbjednosnih kapaciteta na nivou Crne Gore; * 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 prijetnji mrežnim i informacionim sistemima koji se koriste za pružanje osnovnih usluga u ključnim i važnim sektorima * Osiguravanje kontinuiteta pružanja usluga u slučaju incidenata, čime se doprinosi efikasnijem funkcionisanju privrede i društva. * 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”, regulatorna i neregulatorna opcija.  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.  U procesu usaglašavanja sa evropskom pravnom tekovinom, Crna Gora ima obavezu usaglašavanja propisa sa Direktivom NIS 2, koja je usvojena 14. decembra 2022. godine. | |
| 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, privrednih društva, pravnih lica sa javnim ovlašćenjima i drugih pravnnih i fizičkih lica koja ostvaruju pristup ili postupaju podacima i koji koriste i upravljaju mrežnim i informacionim sistemima (organi), ključnih i važnih subjekata, u smislu ovog zakona, 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 Nacionalnog 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 u velikom rasponu, 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 20 ovog zakona propisano je sledeće:  Ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti od čl. 6 do čl. 11 ovog Zakona.  Ključni i važni subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti.  Ključni subjekti dužni su da primjenjuju međunarodni standard ISO/IEC 27001 za upravljanje informacionom bezbjednošću.  Budući da se propisom zahtijeva određivanje zaposlenog lica za praćenje mjera informacione bezbjednosti kao i primjena standarda ISO 27001, u tom smislu troškovi ključnih i važnih subjekata koji nemaju stručno lice za praćenje primjene mjera, kao i koji nemaju implementiran standard 27001 bi bili povezani sa troškovima zapošljavanja stručnog lica i uspostavljanja standarda 27001. Međutim smatra se da je određeni broj ključnih i važnih subjekata već ispunjava ove uslove. | |
| 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 33 ovog zakona propisano je da se sredstva za rad Agencije za sajber bezbjednost obezbjeđuju u Budžetu Crne, kao da odobrena sredstva za funkcionisanje i rad Agencije ne mogu biti manja od 0.2% tekućeg budžeta Crne Gore.  Za implementaciju ovog propisa potrebno je obezbijediti finansijskih sredstava iz Budžeta Crne Gore, prije svega za ispunjenje tehničkih i drugih uslova za rad Agencije i Vladinog CIRT-a, potrebno je:   1. posjedovati sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku imaju na raspolaganju više sredstava za dvosmjernu komunikaciju; 2. posjedovati prostorije i informacione sisteme smještene na sigurnim lokacijama; 3. posjedovati adekvatan sistem za prijavljivanje i upravljanje incidenatima; 4. obezbijediti povjerljivost i pouzdanost svojih operacija; 5. biti opremljen redundantnim sistemima i rezervnim radnim prostorom kako bi se obezbjedio kontinuitet rada; 6. imati dovoljan broj zaposlenih kako bi se obezbijedila dostupnost 24 sata.   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.   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]](#footnote-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 kompanije 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]](#footnote-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 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.  Najveći sajber napad u Crnoj Gori dogodio su 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 različitih 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](https://www.danas.rs/vesti/drustvo/novi-sad-ce-se-nedeljama-oporavljati-od-sajber-napada/) 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.  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.  Nije korišćena metodologija.  Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?  Naknadno.  Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.  Naknadno. | |
| 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 obrasce u početnoj fazi bio je formiran radni tim koji su činili predstavnici Ministarstva javne uprave. Planirane su konsultacije sa posebnim fokus grupama, kao i okrugli sto za svu zainteresovanu javnost.  U cilju predstavljanja Nacrt zakona i dobijanja sugestija za unapređenje teksta održano je dvodnenvno prezentovanje i usaglašavanje sa Savjetom za informacionu bezbjednost.  Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.  Naknadno. | |
| 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 Vladin CIRT).  Nedostatak službenika osposobljenih na odgovarajući način, prije svega za poslove rješavanja incidenata, stručnog i inspekcijskog nadzora u odnosu na ključne i važne subjekte, 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 Agenciojm za sajber bezbijednost izradiće se Nacionalni plan za odgovor na sajber prijetnju, incidente i sajber krizu, u kojem se utvrđuje način upravljanja sajber prijetnjama, incidentima i sajber krizama.  U vezi primjene ovog propisa Ministarstvo će obaviti aktivnosti u smislu uspostavljanja Nacionalog registra ključnih i važnih subjekata.  Za sprovođenje i unapređenje mjera informacione bezbjednosti, vršenja nadzora nad primjenom tih mjera, kao i za uspostavljanje sistema za rano otkrivanje i odbranu od sajber prijetnji i incidenata, osniva se Agencija za sajber bezbjednost. Ovo tijelo će se baviti informacionom bezbjednošću svih organa koji su u obavezi da postupaju po ovom propisu, osim organa državne uprave.  Nacionalni okvir za bezbjednost mrežnih i informacionih sistema obuhvata i Savjet za informacionu bezbijednost kao tijelo za praćenje razvoja i predlaganja mjera za unaprjeđenje informacione bezbjednosti, praćenja rada i predlaganja aktivnosti Agenciji i Ministarstvu na uspostavljanju sistema zaštite od sajber prijetnji i incidenata, kao i razmatranja stručnih pitanja u oblasti informacione bezbjednosti.  Upravni nadzor nad sprovođenjem ovog propisa vršiće Ministarstvo javne uprave, dok će stručni nadzor vršiti Agencija za sajber bezbjednost  Inspekcijski nadzor vršiće inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.  Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?  Indikatori su:   1. Broj organa i ključnih i važnih subjekata koji primjenjuju mjere informacione bezbjednosti   Naime, ovim zakonom definisani su kriterijumi za određivanje ključnih i važnih subjekata, kao i mjere zaštite u cilju održavanja adekvatnog nivoa bezbijednosti sistema. Shodno tome, ključni i važni subjekti dužni su da primjenjuju mjere kojima se obezbjeđuje zaštita od sajber prijetnji mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču. Kako bi se pratila primjena mjera propisano je da su ključni i važni subjekti dužni da donesu: politiku analize rizika i bezbjednosti mrežnih i informacionih sistema; politiku postupanja sa incidenatima (sprečavanje, otkrivanje i odgovor na incidente); plan kontinuiteta poslovanja i postupanja u sajber krizama; politiku bezbjednosti kojom se uređuje bezbjednost lanca snabdijevanja između subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga; akte kojima se uređuje upostavljanje, razvoj i održavanje mrežnih i informacionih sistema, uključujući bezbjednosne aspekte; politike i postupke za procjenu efikasnosti mjera upravljanja sajber bezbjednosnim rizicima; kao i da primjenjuju kriptovane zaštite podataka, ukoliko priroda posla to zahtjeva.  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.  Nadzorom će se utvrditi da li se primjenuju propisane mjere, 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.   1. 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.   1. Uspostavljen Nacionalni registar ključnih i važnih subjekata.   Po prvi put će se uspostaviti Nacionalni regiostar 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 preko godišnjeg Izvještaja Ministarstva javne uprave i Agencije, kao i godišnjeg izvještaja o radu Savjeta za informacionu bezbjednost.  Jedan od načina praćenja evaluacije su i izvještaji organa koji su obavezni da postupaju po ovom zakonu. | |
|  | |

**Datum i mjesto Starješina**

28.02.2023. godine

\_\_\_\_\_\_\_\_\_\_\_\_\_

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)](https://www.gov.me/dokumenta/0e592446-8546-4a0c-98a8-8f844f639f76) [↑](#footnote-ref-1)
2. Izvor: https://www.techrepublic.com/article/top-cybersecurity-threats/ [↑](#footnote-ref-2)
3. Izvor: https://www.forbes.com/advisor/business/common-cyber-security-threats/ [↑](#footnote-ref-3)