2216

Na temelju članka 81. Ustava Republike Hrvatske, Hrvatski sabor na sjednici 15. studenoga 2024. donio je

ODLUKU
O IMENOVANJU ZAMJENICE ČLANA IZASLANSTVA HRVATSKOGA SABORA U PARLAMENTARNOJ SKUPŠTINI VIJEĆA EUROPE

I.

Za zamjenicu člana Izaslanstva Hrvatskoga sabora u Parlamentarnoj skupštini Vijeća Europe imenuje se DANIJELA BLAŽANOVIĆ.

II.

Ova Odluka objavit će se u »Narodnim novinama«, a stupa na snagu danom donošenja.

Klasa: 021-04/24-04/11
Zagreb, 15. studenoga 2024.

HRVATSKI SABOR

Predsjednik
Hrvatskoga sabora
Gordan Jandroković, v. r.

VLADA REPUBLIKE HRVATSKE

2217

Na temelju članka 24. Zakona o kibernetičkoj sigurnosti (»Narodne novine«, broj 14/24.), Vlada Republike Hrvatske je na sjednici održanoj 21. studenoga 2024. donijela

UREDBU
O KIBERNETIČKOJ SIGURNOSTI

DIO PRVI
OPĆE ODREDBE

Članak 1.

Ovom se Uredbom uređuju mjerila za razvrstavanje subjekata temeljem posebnih kriterija za provedbu kategorizacije subjekata, kriteriji za provođenje procjena u svrhu kategorizacije subjekata javnog sektora i subjekata iz sustava obrazovanja, prikupljanje podataka u svrhu provođenja kategorizacije subjekata i vođenja posebnog registra subjekata, vođenje popisa ključnih i važnih subjekata, vođenje posebnog registra subjekata, mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe, provođenje samoprocjena kibernetičke sigurnosti, obrazac izjave o sukladnosti, kriteriji za utvrđivanje značajnih incidenata, obavještavanje o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima, prava pristupa i druga pitanja bitna za korištenje nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, podnošenje zahtjeva i prijedloga, prikupljanje podataka potrebnih za provođenje procjene kritičnosti subjekata, kao i druga pitanja bitna za provedbu pristupanja subjekata nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora.

Članak 2.

Sastavni su dio ove Uredbe:

– Prilog I. – Popis sektora djelatnosti (u daljnjem tekstu: Prilog I. ove Uredbe)

– Prilog II. – Mjere upravljanja kibernetičkim sigurnosnim rizicima (u daljnjem tekstu: Prilog II. ove Uredbe)

– Prilog III. – Posebne mjere fizičke sigurnosti za subjekte iz sektora digitalne infrastrukture (u daljnjem tekstu: Prilog III. ove Uredbe) i

– Prilog IV. – Obrazac izjave o sukladnosti (u daljnjem tekstu: Prilog IV. ove Uredbe).

Članak 3.

Ovom se Uredbom u hrvatsko zakonodavstvo preuzima Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS2) (SL L 333/80, 27. 12. 2022.).

Članak 4.

(1) U smislu ove Uredbe pojedini pojmovi imaju sljedeće značenje:

1. *djelatnost* je svaka djelatnost izrijekom navedena u Prilogu I. i Prilogu II. Zakona o kibernetičkoj sigurnosti (»Narodne novine«, broj 14/24.; u daljnjem tekstu: Zakon)

2. *haktivizam* podrazumijeva korištenje kibernetičkih napada u svrhu promoviranja i poticanja određenih političkih stavova ili društvenih promjena, kao i s ciljem izražavanja neke vrste građanskog neposluha, a provode ga organizirane kibernetičke grupe ili pojedinci, koji se nazivaju haktivisti

3. *indikatori kompromitacije* (*Indicators of Compromise – IoCs*) su podaci koji predstavljaju indikatore moguće kompromitacije mrežnog i informacijskog sustava, koji se koriste u svrhu otkrivanja i sprečavanja kibernetičkih napada, odnosno u cilju smanjenja potencijalne štete zaustavljanjem kibernetičkog napada u njegovim ranijim fazama, a tipični indikatori kompromitacije su IP adrese, imena datoteka, kriptografski sažeci datoteka, maliciozne domene i domene upravljanja i kontrole kibernetičkih napadača

4. *javni pružatelj medijske usluge* je pružatelj medijske usluge kako je definiran Uredbom (EU) 2024/1083 Europskog parlamenta i Vijeća od 11. travnja 2024. o uspostavi zajedničkog okvira za medijske usluge na unutarnjem tržištu i izmjeni Direktive 2010/13/EU (Europski akt o slobodi medija) (Tekst značajan za EGP) (SL L, 17.4.2024.)

5. *nadležna tijela za provedbu kategorizacije subjekata* su nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona, prema podjeli nadležnosti iz Priloga III. Zakona

6. *nadležno tijelo za vođenje posebnog registra subjekata* je Sigurnosno-obavještajna agencija

7. *obveznici dostave podataka za kategorizaciju subjekata* su subjekti iz Priloga I. i II. Zakona

8. *obveznici dostave podataka za vođenje posebnog registra subjekata* su pružatelji usluga DNS-a, registar naziva vršne nacionalne internetske domene, registrari, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih

sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica i pružatelji platformi za usluge društvenih mreža

9. *operativna tehnologija (OT)* predstavlja širok raspon programabilnih sustava i uređaja koji su u određenoj interakciji s fizičkim okruženjem ili upravljaju drugim uređajima koji su u interakciji s fizičkim okruženjem te otkrivaju ili uzrokuju izravnu promjenu fizičkog okruženja putem nadzora i/ili upravljanja uređajima, procesima i događajima

10. *osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima* su članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršnih tijela jedinica lokalne i područne (regionalne) samouprave

11. *primatelj usluge* je svaka fizička i pravna osoba kojoj ključan ili važan subjekt pruža uslugu temeljem zakona ili ugovora o pružanju usluge. Ugovor o pružanju usluge je ugovor kojim se uređuje pružanje i korištenje usluge ili drugi pravno obvezujući dokument koji uređuje pravni odnos između primatelja usluge i ključnog ili važnog subjekta kao pružatelja usluge, uključujući opće uvjete poslovanja subjekta i druga unaprijed sastavljena pisana pravila kojima subjekt unaprijed regulira pravne odnose s primateljima svojih usluga

12. *primijenjeno znanstveno istraživanje* je industrijsko istraživanje, eksperimentalni razvoj ili njihova kombinacija. Industrijsko istraživanje je planirano istraživanje ili kritički pregled radi stjecanja novih znanja i vještina za razvoj novih proizvoda, procesa ili usluga odnosno za postizanje znatnog poboljšanja postojećih proizvoda, procesa ili usluga. Eksperimentalni razvoj je stjecanje, kombiniranje, oblikovanje i uporaba postojećih znanstvenih, tehnoloških, poslovnih i ostalih mjerodavnih znanja i vještina radi razvoja novih ili poboljšanih proizvoda, procesa ili usluga. Eksperimentalni razvoj može uključivati aktivnosti kojima je cilj konceptualno definiranje, planiranje i dokumentiranje novih proizvoda, procesa ili usluga

13. *smanjena razina kvalitete usluge* je razina kvalitete usluge koja je manja od propisane ili ugovorene razine kvalitete usluge

14. *učinak na autentičnost* je utjecaj na svojstvo da je entitet ono za što tvrdi da jest

15. *učinak na cjelovitost* je utjecaj na svojstvo točnosti i potpunosti

16. *učinak na dostupnost* je utjecaj na kontinuitet pružanja usluge, smanjenje razine kvalitete usluge te djelomični ili potpuni prekid pružanja usluge

17. *učinak na povjerljivost* je utjecaj na svojstvo dostupnosti na način da je informacija dostupna neovlaštenim osobama, pojedincima, entitetima ili procesima

18. *usluga* je svaka usluga izrijekom navedena u Prilogu I. i Prilogu II. Zakona, kao i svaka druga usluga koju ključan ili važan subjekt pruža temeljem zakona ili drugih propisa u okviru obavljanja djelatnosti iz Priloga I. i Priloga II. Zakona.

(2) Ostali pojmovi koji se koriste u ovoj Uredbi imaju jednako značenje kao pojmovi koji se koriste u Zakonu.

(3) Izrazi koji se koriste u ovoj Uredbi, a imaju rodno značenje odnose se jednako na muški i ženski rod.

Članak 5.

Odredbe ove Uredbe koje se odnose na nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti odnose se i na nadležna tijela za provedbu posebnih zakona kada se tim odredbama uređuju pitanja vezana uz zahtjeve kibernetičke sigurnosti i njihovu provedbu, a koja nisu uređena posebnim zakonima i podzakonskim propisima donesenim na temelju tih zakona, u smislu članka 8. Zakona.

Članak 6.

Nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka dužna su, u skladu s pravom Europske unije i relevantnim nacionalnim pravom, čuvati sigurnost i komercijalne interese ključnih i važnih subjekata te povjerljivost dostavljenih informacija u provedbi njihovih obveza sukladno ovoj Uredbi.

DIO DRUGI
KATEGORIZACIJA SUBJEKATA TEMELJEM POSEBNIH KRITERIJA, KATEGORIZACIJA SUBJEKATA JAVNOG SEKTORA I SUBJEKATA IZ SUSTAVA OBRAZOVANJA

POGLAVLJE I.
MJERILA ZA KATEGORIZACIJU SUBJEKATA TEMELJEM POSEBNIH KRITERIJA

Članak 7.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 1. Zakona provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona za koje se u postupku kategorizacije subjekata utvrdi da su na području najmanje jedne županije, neovisno o broju stanovnika gradova i općina u njezinom sastavu, jedini pružatelj usluge zbog koje je subjekt predmet postupka kategorizacije subjekata.

(2) Temeljem mjerila iz stavka 1. ovoga članka:

– privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se u kategoriju ključnih subjekata

– privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

Članak 8.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju obavlja, mogao imati na javnu sigurnost, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona od kojih se izravno dobavljaju proizvodi ili naručuju usluge obuhvaćene Prilogom I. ili Prilogom II. Zakona za:

– policijske namjene

– zaštitu državne granice ili

– zaštitu i spašavanje u slučaju velikih nesreća, katastrofa i kriza.

(2) Temeljem mjerila iz stavka 1. ovoga članka:

– privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se u kategoriju ključnih subjekata

– privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

(3) Postupci kategorizacije subjekata iz stavka 1. ovoga članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za unutarnje poslove.

Članak 9.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju

obavlja, mogao imati na javnu zaštitu, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona:

– koji su odlukama nadležnog tijela državne uprave određeni kao operativne snage sustava civilne zaštite od posebnog interesa na državnoj razini ili su

– odlukama izvršnih tijela jedinica lokalne i područne (regionalne) samouprave određeni pravnom osobom od interesa za sustav civilne zaštite.

(2) Temeljem mjerila iz stavka 1. podstavka 1. ovoga članka privatni i javni subjekti iz Priloga I. i Priloga II. Zakona razvrstavaju se u kategoriju ključnih subjekata.

(3) Temeljem mjerila iz stavka 1. podstavka 2. ovoga članka privatni i javni subjekti iz Priloga I. i Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

(4) Postupci kategorizacije subjekata iz stavka 1. ovoga članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za uspostavu sustava civilne zaštite.

Članak 10.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju subjekt obavlja, mogao imati na javno zdravlje, provodi se za pružatelje zdravstvene zaštite iz Priloga I. Zakona koji pružaju jednu od sljedećih zdravstvenih djelatnosti:

– suzbijanje zaraznih bolesti

– opskrbu lijekovima i medicinskim proizvodima za zdravstvenu zaštitu

– prikupljanje i pripremu medicinskih pripravaka i presadaka ljudskog podrijetla ili

– hitnu medicinu.

(2) Pružatelji zdravstvene zaštite iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovoga članka u kategoriju ključnih subjekata, neovisno o tome pružaju li zdravstvene djelatnosti iz stavka 1. ovoga članka na primarnoj, sekundarnoj ili tercijarnoj razini.

(3) Postupci kategorizacije subjekata iz stavka 1. ovoga članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za zdravstvo.

Članak 11.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 3. Zakona provodi se za privatne i javne subjekte iz sektora energetike, sektora prometa, sektora digitalne infrastrukture te pružatelje upravljanih usluga i pružatelje upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona, za koje se u postupku kategorizacije subjekata utvrdi da tržišni udio subjekta u pružanju usluga, odnosno obavljanju djelatnosti zbog koje je subjekt predmet postupka kategorizacije subjekata, na području Republike Hrvatske iznosi 25 % ili više.

(2) Razvrstavanje subjekata temeljem članka 11. podstavka 3. Zakona provodi se i za pružatelje upravljanih usluga i pružatelje upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona koji upravljanje usluge i upravljane sigurnosne usluge pružaju ključnim i važnim subjektima.

(3) Privatni i javni subjekti iz sektora energetike, sektora prometa, sektora digitalne infrastrukture i pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovoga članka u kategoriju ključnih subjekata.

(4) Pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 2. ovoga članka u kategoriju važnih subjekata.

Članak 12.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 4. Zakona, prema kriteriju posebne važnosti subjekta na nacionalnoj razini, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona koji su odlukom Vlade Republike Hrvatske određeni pravnom osobom od posebnog interesa za Republiku Hrvatsku.

(2) Privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovoga članka u kategoriju ključnih subjekata.

(3) Privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovoga članka u kategoriju važnih subjekata.

(4) Razvrstavanje subjekata temeljem članka 11. podstavka 4. Zakona, prema kriteriju posebne važnosti subjekta na regionalnoj i lokalnoj razini, provodi se za:

– privatne i javne subjekte iz sektora energetike, podsektora električna energija, podsektora centralizirano grijanje i hlađenje i podsektora plin, sektora voda za ljudsku potrošnju i sektora otpadne vode iz Priloga I. Zakona

– privatne i javne subjekte iz sektora poštanske i kurirske usluge iz Priloga II. Zakona,

za koje se u postupku kategorizacije subjekata utvrdi da tržišni udio subjekta u pružanju usluga, odnosno obavljanju djelatnosti zbog koje je subjekt predmet postupka kategorizacije subjekata, na području jedne županije, neovisno o broju stanovnika gradova i općina u njezinom sastavu, iznosi 40 % ili više.

(5) Privatni i javni subjekti iz sektora energetike, podsektora električna energija, podsektora centralizirano grijanje i hlađenje i podsektora plin, sektora voda za ljudsku potrošnju i sektora otpadne vode iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 4. ovoga članka u kategoriju ključnih subjekata.

(6) Privatni i javni subjekti iz sektora poštanske i kurirske usluge iz Priloga II. Zakona razvrstavaju se temeljem mjerila iz stavka 4. ovoga članka u kategoriju važnih subjekata.

Članak 13.

Mjerila za kategorizaciju temeljem posebnih kriterija iz članaka 7. do 12. ove Uredbe primjenjuju se na privatne i javne subjekte iz Priloga I. i II. Zakona koji nisu kategorizirani temeljem općih kriterija za kategorizaciju subjekata iz članaka 9. i 10. Zakona.

POGLAVLJE II.
PROVOĐENJE KATEGORIZACIJE SUBJEKATA JAVNOG SEKTORA I SUBJEKATA IZ SUSTAVA OBRAZOVANJA

Članak 14.

(1) Državna tijela i pravne osobe s javnim ovlastima razvrstavaju se u kategoriju ključnih subjekata ako ispunjavaju sljedeće kriterije:

– osnivač subjekta je Republika Hrvatska, a ustanovljava se za područje Republike Hrvatske i djelatnost obavlja na nacionalnoj razini i pritom nije kategoriziran niti u jednom drugom sektoru visoke

kritičnosti ili drugom kritičnom sektoru iz Priloga I. i Priloga II. Zakona i

– utjecaj značajnog kibernetičkog incidenta i ozbiljne kibernetičke prijetnje na mrežni i informacijski sustav tog subjekta može izazvati značajne:

1. posljedice za život i zdravlje ljudi ili na okoliš

2. materijalne i nematerijalne štete tom subjektu ili drugim pravnim i fizičkim osobama

3. poremećaje kod subjekta u obavljanju redovnih djelatnosti

4. međuresorne posljedice (utjecaj na druge sektore društvenih ili gospodarskih djelatnosti) ili

5. negativne javne utjecaje.

(2) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti prilikom kategorizacije subjekata javnog sektora provodi procjenu kriterija iz stavka 1. podstavka 2. ovoga članka na način da procjenjuje svaku od posljedica utjecaja značajnog kibernetičkog incidenta i ozbiljne kibernetičke prijetnje zasebno i u odnosu s drugim posljedicama.

Članak 15.

Jedinice lokalne i područne (regionalne) samouprave razvrstavaju se u kategoriju važnih subjekata ako ispunjavaju najmanje jedan od sljedećih kriterija:

– obavljaju poslove od područnog (regionalnog) značaja

– predstavljaju gospodarska, financijska, kulturna, zdravstvena, prometna i znanstvena središta razvitka šireg okruženja

– ovlaštene su provoditi poslove u području gospodarskog razvoja te planiranja i razvoja mreže obrazovnih, zdravstvenih, socijalnih i kulturnih ustanova ili

– su im povjereni poslovi državne uprave.

Članak 16.

Subjekti iz sustava obrazovanja razvrstavaju se temeljem članka 13. Zakona u kategoriju važnih subjekata po osnovi procjene njihove posebne važnosti za obavljanje odgojnog odnosno obrazovnog rada ako ispunjavaju najmanje jedan od sljedećih kriterija:

– pružaju e-usluge nacionalnih informacijskih sustava značajnih za sustav odgoja i obrazovanja u Republici Hrvatskoj

– predstavljaju visoko učilište koje provodi primijenjena znanstvena istraživanja u svrhu inovacija i razvoja tehnologija, neovisno o osnivaču ustanove

– predstavljaju visoko učilište koje pruža usluge informacijskih sustava značajnih za sustav obrazovanja u Republici Hrvatskoj ili

– predstavljaju javnu ustanovu koja provodi vanjsko vrednovanje u odgojno-obrazovnom sustavu Republike Hrvatske i ispite temeljene na nacionalnim standardima.

DIO TREĆI
POPISI KLJUČNIH I VAŽNIH SUBJEKATA I POSEBAN REGISTAR SUBJEKATA

POGLAVLJE I.
OBVEZE SUBJEKATA IZ PRILOGA I. I PRILOGA II. ZAKONA

Članak 17.

(1) Obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su imenovati osobu za kontakt odgovornu za dostavu podataka.

(2) Za osobu za kontakt odgovornu za dostavu podataka mora biti:

– imenovana osoba iz reda članova upravljačkog tijela subjekta

– imenovana osoba iz reda državnih dužnosnika u tijelima državne uprave i drugim državnim tijelima ili

– imenovano izvršno tijelo jedinice lokalne i područne (regionalne) samouprave.

Članak 18.

(1) Osoba za kontakt odgovorna za dostavu podataka odgovorna je za pravodobnu dostavu točnih i potpunih podataka i obavijesti o promjenama podataka sukladno člancima 20. i 23. Zakona te odredbama ove Uredbe.

(2) Osoba za kontakt odgovorna za dostavu podataka dužna je imenovati najmanje dvije osobe ovlaštene za operacionalizaciju dostave podataka i obavijesti o promjenama podataka iz članaka 20. i 23. Zakona.

Članak 19.

(1) Obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su nadležnom tijelu za provedbu kategorizacije subjekata odnosno nadležnom tijelu za vođenje posebnog registra subjekata, bez odgode, a najkasnije u roku od osam dana od dana zaprimanja zahtjeva iz članka 20. stavka 1. i članka 23. stavka 2. Zakona, dostaviti podatke o imenovanoj osobi za kontakt odgovornoj za dostavu podataka i osobama ovlaštenima za operacionalizaciju dostave, i to:

– ime i prezime imenovanih osoba

– podatke o njihovom radnom mjestu odnosno dužnosti u subjektu

– adresu elektroničke pošte osobe za kontakt odgovorne za dostavu podataka i

– adrese elektroničke pošte koje će osobe ovlaštene za operacionalizaciju dostave koristiti u svrhe dostave podataka i obavijesti o promjenama podataka.

(2) U slučaju promjene osoba iz stavka 1. ovoga članka ili pojedinih podataka dostavljenih sukladno stavku 1. ovoga članka, obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su o promjeni obavijestiti nadležno tijelo za provedbu kategorizacije subjekata odnosno nadležno tijelo za vođenje posebnog registra subjekata, bez odgode, a najkasnije u roku od 15 dana od dana imenovanja nove osobe odnosno promjene pojedinih podataka dostavljenih sukladno stavku 1. ovoga članka.

(3) Obavijesti iz stavaka 1. i 2. ovoga članka dostavljaju se nadležnom tijelu za provedbu kategorizacije subjekata odnosno nadležnom tijelu za vođenje posebnog registra subjekata prema uputama iz članka 22. ove Uredbe.

Članak 20.

Obveznici dostave podataka za kategorizaciju subjekata dužni su nadležnom tijelu za provedbu kategorizacije subjekata dostavljati podatke i obavijesti o promjenama podataka iz članka 20. Zakona kako slijedi:

– »*naziv subjekta*« naziv odnosno ime pod kojim subjekt posluje odnosno obavlja djelatnost u Republici Hrvatskoj, s naznakom i skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu, te osobni identifikacijski broj subjekta (u daljnjem tekstu: OIB)

– »*adresa*« adresa sjedišta subjekta, te adresa kontakt osobe odgovorne za dostavu podataka, ako je različita od adrese sjedišta subjekta

– »*ažurirane podatke za kontakt, uključujući adrese e-pošte*« adresa mrežne stranice subjekta, ime i prezime kontakt osobe odgovorne za dostavu podataka i osoba ovlaštenih za operacionalizaciju dostave, brojeve telefona, brojeve mobitela i adrese elektroničke pošte kontakt osobe odgovorne za dostavu podataka i osoba ovlaštenih za operacionalizaciju dostave

– »*IP adresne raspone*« IP adresne raspone koje subjekt koristi u Republici Hrvatskoj

– »*relevantni sektor, podsektor i vrstu subjekta iz Priloga I. i Priloga II. Zakona*« nazive sektora, podsektora i vrste subjekta, prema nazivima iz Priloga I. ove Uredbe

– »*popis država članica u kojima subjekt pruža usluge obuhvaćene područjem primjene Zakona*« popis država članica Europske unije (u daljnjem tekstu: država članica) u kojima subjekt pruža usluge odnosno obavlja djelatnosti iz Priloga I. odnosno Priloga II. Zakona i pravni oblik pružanja odnosno obavljanja tih djelatnosti u drugim državama članicama i

– »*druge podatke o pružanju svojih usluga ili obavljanju svojih djelatnosti bitne za provedbu kategorizacije subjekta ili utvrđivanje nadležnosti nad subjektom*« podatke o veličini subjekta i druge podatke koje je od subjekta zatražilo nadležno tijelo za provedbu kategorizacije subjekata, u svrhu provedbe kategorizacije subjekta ili utvrđivanja nadležnosti nad subjektom.

Članak 21.

Obveznici dostave podataka za vođenje posebnog registra subjekata dužni su nadležnom tijelu za vođenje posebnog registra subjekata dostavljati podatke i obavijesti o promjenama podataka iz članka 23. Zakona kako slijedi:

– »*naziv subjekta*« naziv odnosno ime pod kojim subjekt posluje odnosno obavlja djelatnost u Republici Hrvatskoj, s naznakom skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu, te OIB

– »*adresa glavnog poslovnog nastana subjekta*« adresa glavnog poslovnog nastana subjekta u smislu članka 14. stavaka 3. i 4. Zakona

– »*popis usluga iz članka 22. Zakona*« popis usluga iz članka 22. Zakona koje subjekt pruža u Republici Hrvatskoj

– »*adrese poslovnih jedinica u Republici Hrvatskoj*« adrese svih poslovnih jedinica subjekta koje se nalaze u Republici Hrvatskoj

– »*IP adresne raspone*« IP adresne raspone koje subjekt koristi u Republici Hrvatskoj

– »*popis drugih država članica u kojima subjekt posluje*« popis drugih država članica u kojima subjekt pruža usluge iz članka 22. Zakona

– »*adrese drugih poslovnih jedinica*« adrese poslovnih jedinica subjekta u kojima subjekt pruža usluge iz članka 22. Zakona koje se nalaze u drugim državama članicama i

– »*ažurirane podatke za kontakt, uključujući adrese e-pošte i telefonske brojeve subjekta*« adresa mrežne stranice subjekta, ime i prezime kontakt osobe odgovorne za dostavu podataka, broj telefona, broj mobitela i adresa elektroničke pošte osobe za kontakt odgovorne za dostavu podataka, ako subjekt ima glavni poslovni nastan u Republici Hrvatskoj u smislu članka 14. stavaka 3. i 4. Zakona ili

– »*naziv i adresa predstavnika, ažurirani podaci za kontakt, uključujući adrese e-pošte i telefonske brojeve predstavnika*« naziv odnosno ime, adresa, broj telefona, broj mobitela i adresa elektroničke pošte fizičke ili pravne osobe koja ima poslovni nastan u Republici Hrvatskoj ili drugoj državi članici, a koju je obveznik dostave podataka za vođenje posebnog registra subjekata koji nema poslovni nastan u Europskoj uniji izričito imenovao da djeluje u njegovo ime te kojoj se nadležno tijelo može obratiti umjesto samom subjektu vezano uz obveze tog subjekta na temelju ove Uredbe.

Članak 22.

(1) Podaci iz članaka 20. i 21. ove Uredbe i obavijesti o njihovoj promjeni dostavljaju se u elektroničkom obliku, prema uputama koje nadležna tijela za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata objavljuju na svojim mrežnim stranicama.

(2) Nadležna tijela za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata dužni su u uputama iz stavka 1. ovoga članka definirati način dostave u iznimnim slučajevima kada dostava u elektroničkom obliku iz opravdanih razloga nije moguća.

(3) Nadležno tijelo za vođenje posebnog registra subjekata dužno je u uputama iz stavka 1. ovoga članka definirati način sastavljanja i dostave podataka i obavijesti o promjenama podataka u slučaju kada su mu isti subjekti dužni dostavljati podatke i obavijesti o promjenama podataka po osnovi obveza koje za te subjekte proizlaze kao obveznika dostave podataka za vođenje posebnog registra subjekata i obveznika dostave podataka za kategorizaciju subjekata.

Članak 23.

(1) Upute iz članka 22. ove Uredbe sadržavaju i upute za dobrovoljnu dostavu podataka u svrhu provedbe postupka kategorizacije subjekta.

(2) Dostava podataka o subjektu sukladno uputama za dobrovoljnu dostavu podataka iz stavka 1. ovoga članka smatra se jednakovrijednoj dostavi podataka na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti iz članka 20. stavka 1. Zakona.

(3) Dostava podataka o subjektu sukladno stavcima 1. i 2. ovoga članka ne utječe na obvezu obavještavanja subjekta o provedenoj kategorizaciji sukladno članku 19. Zakona.

(4) Dostava podataka o subjektu sukladno stavcima 1. i 2. ovoga članka ne utječe na obveze subjekta iz članaka 17. do 19. ove Uredbe.

Članak 24.

(1) Ukoliko podaci ili obavijesti o promjenama podataka nisu dostavljeni u skladu s člancima 19. do 23. ove Uredbe, nadležno tijelo za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata će o tome obavijestiti subjekta i odrediti rok u kojem je subjekt dužan otkloniti nedostatke i dostaviti podatke odnosno izmjenu, dopunu ili ispravak podataka, uz upozorenje na pravne posljedice sukladno Zakonu ako to ne učini u ostavljenom roku.

(2) Obavijest iz stavka 1. ovoga članka dostavlja se na adresu elektroničke pošte kontakt osobe odgovorne za dostavu podataka odnosno adresu elektroničke pošte predstavnika obveznika dostave podataka za vođenje posebnog registra subjekata koji nema poslovni nastan u Europskoj uniji.

POGLAVLJE II.
PRIKUPLJANJE PODATAKA IZ DRUGIH IZVORA

Članak 25.

(1) U svrhu provedbe obveza iz članka 21. podstavka 1. Zakona, tijela državne uprave, druga državna tijela, jedinice lokalne i po-

područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti dužni su voditi popis subjekata iz Priloga I. i Priloga II. Zakona za koje u okviru svog djelokruga prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka.

(2) Popis subjekata iz stavka 1. ovoga članka sadrži sljedeće podatke:

– sektore, podsektore i vrste subjekata iz Priloga I. i Priloga II. Zakona za koje prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka, prema nazivima iz Priloga I. ove Uredbe

– za svaki sektor, podsektor i vrstu subjekta iz podstavka 1. ovoga stavka, nazive subjekata odnosno nazive ili imena pod kojima subjekti posluju odnosno obavljaju djelatnosti iz Priloga I. i Priloga II. Zakona u Republici Hrvatskoj, s naznakom i skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu

– pravnu osnovu temeljem koje prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka o subjektima iz podstavka 2. ovoga stavka

– naznaku o tome vode li registre, evidencije i zbirke podataka koji se odnose na veličinu subjekata u smislu članka 15. Zakona i koje podatke prikupljaju i

– podatak o tome vode li registre, evidencije i zbirke podataka za subjekte iz podstavka 2. ovoga stavka u elektroničkom obliku, uz očitovanje o mogućnostima pristupa podacima u tim registrima, evidencijama i zbirkama podataka elektroničkim putem.

(3) Popisi subjekata iz stavka 1. ovoga članka dostavljaju se prema uputama koje nadležna tijela za provedbu kategorizacije subjekata objavljuju na svojim mrežnim stranicama.

(4) Popisi subjekata iz stavka 1. ovoga članka dostavljaju se nadležnim tijelima za provedbu kategorizacije subjekata jednom godišnje, najkasnije do 1. ožujka tekuće godine za prethodnu godinu.

(5) Iznimno od stavka 4. ovoga članka, ako u odnosu na prethodno dostavljeni popis subjekata nije bilo promjena, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti o tome obavještavaju nadležno tijelo za provedbu kategorizacije subjekata, bez obveze dostave novoga popisa subjekata.

(6) Iznimno od stavaka 1. i 4. ovoga članka, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti nisu u obvezi voditi i redovito dostavljati popise subjekata iz stavka 1. ovoga članka, ako su nadležnim tijelima za provedbu kategorizacije subjekata omogućili elektroničkim putem pristup odgovarajućim podacima o subjektima u registrima, evidencijama i zbirkama podataka.

Članak 26.

Članak 25. ove Uredbe ne primjenjuje se na:

– sektor bankarstva

– sektor infrastruktura financijskog tržišta i

– podsektor zračnog prometa.

POGLAVLJE III.
NAČIN VOĐENJA I SADRŽAJ POPISA KLJUČNIH I VAŽNIH SUBJEKATA

Članak 27.

(1) Popisi ključnih i važnih subjekata vode se u elektroničkom obliku.

(2) U Popise ključnih i važnih subjekata upisuju se podaci propisani ovom Uredbom i sve promjene tih podataka, na način da su iz istih vidljivi izvorno upisani podaci i naknadno unesene promjene tih podataka.

Članak 28.

(1) Popisi ključnih i važnih subjekata vode se po sektorima, podsektorima i vrstama subjekata iz Priloga I. i Priloga II. Zakona, prema nazivima iz Priloga I. ove Uredbe.

(2) Popisi ključnih i važnih subjekata sadrže opće podatke o subjektu i podatke o provedenoj kategorizaciji subjekta.

(3) U Popise ključnih i važnih subjekata pod »*opći podaci o subjektu*« upisuju se sljedeći podaci:

– naziv subjekta

– OIB subjekta

– adresa subjekta

– broj telefona, broj mobitela i adresa elektroničke pošte kontakt osobe odgovorne za dostavu podataka

– IP adresni rasponi koje subjekt koristi u Republici Hrvatskoj

– popis država članica u kojima subjekt pruža usluge odnosno obavlja djelatnosti iz Priloga I. odnosno Priloga II. Zakona

– datum upisa subjekta u Popis ključnih i važnih subjekata.

(4) U Popise ključnih i važnih subjekata pod »*podaci o provedenoj kategorizaciji subjekta*« upisuju se sljedeći podaci:

– podatak o kategoriji subjekta odnosno naznaku je li subjekt razvrstan kao ključan i/ili važan subjekt

– podatak temeljem koje odredbe Zakona je provedena kategorizacija subjekta

– naziv sektora, podsektora i vrste subjekta u koju je subjekt razvrstan, prema nazivima iz Priloga I. ove Uredbe

– datum provedene kategorizacije subjekta

– za subjekt utvrđenu obvezujuću razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe

– datum obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 2. Zakona, kada je primjenjivo

– napomenu je li za subjekt izrađen protokol o postupanju nadležnih tijela iz članka 59. stavka 3. Zakona, kada je primjenjivo

– datum provedene provjere Popisa iz članka 17. stavka 2. Zakona.

(5) Opći podaci o subjektu upisuju se u Popis ključnih i važnih subjekata temeljem podataka dostavljenih sukladno člancima 19., 20., 22. i 23. ove Uredbe.

(6) Podaci o provedenoj kategorizaciji subjekta i obvezujućoj razini mjera upravljanja kibernetičkim sigurnosnim rizicima upisuju se temeljem podataka utvrđenih u postupku kategorizacije subjekta ili provedenih provjera Popisa ključnih i važnih subjekata iz članka 17. stavka 2. Zakona.

Članak 29.

(1) Nadležna tijela za provedbu kategorizacije subjekata dužna su subjekt upisati u Popis ključnih i važnih subjekata najkasnije u roku od osam dana od dana provedene kategorizacije subjekta.

(2) Nadležna tijela za provedbu kategorizacije subjekata dužna su upisati promjenu kategorije subjekta i drugih povezanih podataka u Popis ključnih i važnih subjekata najkasnije u roku od osam dana od dana dostave obavijesti iz članka 19. stavka 2. Zakona.

(3) Nadležna tijela za provedbu kategorizacije subjekata dužna su upisati promjene općih podataka o subjektu u roku od osam dana

od dana primitka obavijesti o promjenama podataka iz članaka 19. i 20. ove Uredbe.

Članak 30.

(1) Nadležna tijela za provedbu kategorizacije subjekata dužna su subjekte koji se nakon ažuriranja Popisa ključnih i važnih subjekata više ne smatraju ni ključnim subjektima ni važnim subjektima voditi u Popisu ključnih i važnih subjekata s naznakom »neaktivan«.

(2) Nadležna tijela za provedbu kategorizacije subjekata dužna su provjerama Popisa ključnih i važnih subjekata iz članka 17. stavka 2. Zakona obuhvatiti i subjekte iz stavka 1. ovoga članka, osim ako je za subjekta u prethodnom postupku provjere utvrđeno da je prestao s radom.

Članak 31.

(1) U svrhu provedbe obveza iz članka 18. stavka 2. Zakona, nadležna tijela za provedbu kategorizacije subjekata dužna su podatke o provedenim kategorizacijama subjekata dostavljati jedinstvenoj kontaktnoj točki sukladno smjernicama jedinstvene kontaktne točke o sadržaju, načinu dostave i rokovima dostave obavijesti o provedenim kategorizacijama subjekata.

(2) U svrhu provedbe članka 43. Zakona, nadležna tijela za provedbu kategorizacije subjekata dužna su Popise ključnih i važnih subjekata, uključujući sva naknadna ažuriranja Popisa, dostavljati pravovremeno i u odgovarajućem formatu Hrvatskoj akademskoj i istraživačkoj mreži – CARNET (u daljnjem tekstu: CARNET).

POGLAVLJE IV.
NAČIN VOĐENJA I SADRŽAJ POSEBNOG REGISTRA SUBJEKATA

Članak 32.

(1) Poseban registar subjekata vodi se u elektroničkom obliku.

(2) U Poseban registar subjekata upisuju se podaci propisani ovom Uredbom i sve promjene tih podataka, na način da su iz istog vidljivi izvorno upisani podaci i naknadno unesene promjene tih podataka.

Članak 33.

(1) U Posebnom registru subjekata vode se sljedeći podaci:

– naziv subjekta

– OIB subjekta

– popis usluga iz članka 22. Zakona koje subjekt pruža u Republici Hrvatskoj

– adresa glavnog poslovnog nastana subjekta

– adrese poslovnih jedinica subjekta u Republici Hrvatskoj

– IP adresni rasponi koje subjekt koristi u Republici Hrvatskoj

– popis drugih država članica u kojima subjekt pruža usluge iz članka 22. Zakona

– adrese poslovnih jedinica subjekta u kojima subjekt pruža usluge iz članka 22. Zakona koje se nalaze u drugim državama članicama

– broj telefona, broj mobilnog telefona i adresa elektroničke pošte kontakt osobe odgovorne za dostavu podataka ili predstavnika subjekta, ako subjekt nema poslovni nastan u Europskoj uniji

– datum upisa subjekta u Poseban registar subjekata.

(2) Podaci o subjektu upisuju se u Poseban registar subjekata temeljem podataka dostavljenih sukladno člancima 19., 21. i 22. ove Uredbe.

Članak 34.

U svrhu provedbe obveza iz članka 23. stavka 4. Zakona, nadležno tijelo za vođenje posebnog registra subjekata dužno je podatke o subjektima iz članka 22. Zakona dostavljati, putem jedinstvene kontaktne točke, Europskoj agenciji za kibernetičku sigurnost (u daljnjem tekstu: ENISA) u rokovima i na način kako je definirano njezinim smjernicama.

DIO ČETVRTI
UPRAVLJANJE KIBERNETIČKIM SIGURNOSNIM RIZICIMA

POGLAVLJE I.
NACIONALNA PROCJENA KIBERNETIČKIH SIGURNOSNIH RIZIKA

Članak 35.

(1) U okviru postupka kategorizacije subjekta provodi se nacionalna procjena kibernetičkih sigurnosnih rizika (u daljnjem tekstu: nacionalna procjena rizika) za svaki subjekt kategoriziran kao ključan ili važan subjekt.

(2) Cilj provođenja nacionalne procjene rizika je definirati razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koju je dužan provoditi svaki pojedini subjekt koji je kategoriziran kao ključan odnosno važan subjekt.

Članak 36.

Nacionalna procjena rizika provodi se temeljem podataka o:

– veličini subjekta i

– pripadnosti subjekta određenom sektoru iz Priloga I. i Priloga II. Zakona,

kao i temeljem praćenja stanja kibernetičke sigurnosti na globalnoj i nacionalnoj razini te provođenja povezanih procjena:

– odabiru tipičnih vrsta kibernetičkih napada, koje se uzimaju kao relevantne za ovu procjenu, kao što su: poremećaj poslovanja ili sabotaža, krađa podataka ili špijunaža, kibernetički kriminal, vandalizam sadržaja i dostupnosti podataka na Internetu, politički utjecaj i dezinformacije

– je li pojedina vrsta tipičnih kibernetičkih napada općenito moguća u nekom sektoru ili se procjenjuje kao ciljana za pojedini sektor

– razine ozbiljnosti poremećaja u funkcioniranju usluga odnosno obavljanju djelatnosti koje odabrane vrste tipičnih kibernetičkih napada mogu uzrokovati u pojedinom sektoru prema raspoloživim podacima

– odabiru tipičnih vrsta kibernetičkih napadača koji se uzimaju kao relevantni za ovu procjenu, kao što su: državno-sponzorirane APT grupe, teroristi, kibernetičke kriminalne grupe, haktivističke grupe, konkurentski poslovni napadači, zajedno s procjenom tipične razine kibernetičkih vještina odabranih vrsta napadača

– vjerojatnosti pojave pojedine vrste kibernetičkih napada, koju uzrokuje određena vrsta kibernetičkih napadača za svaki pojedini sektor i za sve odabrane tipične vrste kibernetičkih napada, kao i za sve odabrane vrste kibernetičkih napadača.

Članak 37.

(1) Potrebnu razradu podataka i procjena iz članka 36., za potrebu provedbe nacionalne procjene rizika za subjekte u sektorima iz Priloga I. i Priloga II. Zakona, provodi središnje državno tijelo za

kibernetičku sigurnost, u suradnji s drugim nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti.

(2) Nacionalnu procjenu rizika za svaki pojedini subjekt, koji se kategorizira u području nadležnosti pojedinog nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, na temelju podataka i procjena iz stavka 1. ovoga članka, provodi nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

(3) Nacionalna procjena rizika iz stavka 2. ovoga članka provodi se u okviru prvog postupka kategorizacije subjekta, nakon svakog ažuriranja popisa ključnih i važnih subjekata sukladno članku 17. stavku 2. Zakona te prilikom svake kategorizacije nekog subjekta koju provodi nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

Članak 38.

(1) Rezultat nacionalne procjene rizika je utvrđivanje niske, srednje ili visoke razine kibernetičkih sigurnosnih rizika, za svaki pojedini subjekt iz članka 37. stavka 2. ove Uredbe.

(2) Ovisno o utvrđenoj razini kibernetičkih sigurnosnih rizika za svaki subjekt koji je kategoriziran kao ključan ili važan subjekt utvrđuje se obveza provedbe jedne od tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima, na sljedeći način:

– za nisku razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu osnovne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. stavka 1. i Priloga II. ove Uredbe

– za srednju razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu srednje razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. stavka 2. i Priloga II. ove Uredbe

– za visoku razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu napredne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. stavka 3. i Priloga II. ove Uredbe.

Članak 39.

(1) Ukoliko subjekt pruža usluge ili obavlja djelatnosti koje pripadaju u više različitih sektora iz Priloga I. i Priloga II. Zakona, nacionalna procjena rizika se provodi za glavnu djelatnost subjekta.

(2) Ukoliko se glavna djelatnost subjekta ne može nedvojbeno utvrditi, nacionalna procjena rizika provodi se za sve usluge i djelatnosti zbog pružanja odnosno obavljanja kojih je subjekt kategoriziran kao ključan ili važan subjekt te se kao konačna nacionalna procjena rizika subjekta uzima tako utvrđena najviša razina kibernetičkih sigurnosnih rizika.

Članak 40.

(1) Nacionalna procjena rizika i utvrđivanje obvezujuće razine mjera upravljanja kibernetičkim sigurnosnim rizicima za ključne i važne subjekte iz članka 38. ove Uredbe, provodi se sukladno smjernicama za provedbu nacionalne procjene kibernetičkih sigurnosnih rizika, koje se izrađuju na temelju podataka i procjena iz članka 36. ove Uredbe i čiji sastavni dio je pripadni kalkulator za izračun razine kibernetičkih sigurnosnih rizika.

(2) Smjernice za provedbu nacionalne procjene rizika iz stavka 1. ovoga članka, kojima se opisuje postupak izračuna rizika na temelju podataka i procjena iz članka 36. ove Uredbe, kao i korištenje pripadnog kalkulatora, donosi središnje državno tijelo za kibernetičku sigurnost.

(3) Središnje državno tijelo za kibernetičku sigurnost objavljuje smjernice iz stavka 2. ovoga članka na svojim mrežnim stranicama.

POGLAVLJE II.
MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

Članak 41.

Popis mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđeni su Prilogom II. ove Uredbe za sve tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe.

Članak 42.

(1) Osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 1. ove Uredbe predstavlja opći skup mjera kibernetičke sigurnosne prakse koji je moguće postići s lako dostupnim tehnologijama i dobro poznatim i dokumentiranim najboljim kibernetičkim sigurnosnim praksama, primjeren u slučaju subjekata čije djelatnosti pripadaju sektorima za koje nisu tipični ciljani kibernetički napadi koje provode napadači s višom razinom kibernetičkih vještina, a cilj primjene osnovne razine je zaštiti subjekt od većine globalno prisutnih kibernetičkih napada, odnosno od kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(2) Srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 2. ove Uredbe predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima, a cilj primjene srednje razine je dodatno umanjiti rizike od ciljanih kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(3) Napredna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 3. ove Uredbe predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima, a cilj primjene napredne razine je smanjenje rizika od naprednih kibernetičkih napada koje provode kibernetički napadači s naprednim vještinama i resursima.

Članak 43.

Popis mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe, za svaku mjeru sadrži:

– naziv mjere

– cilj mjere

– razradu mjere na podskupove mjera upravljanja kibernetičkim sigurnosnim rizicima

– primjenjivost mjere u kontekstu IT i OT sustava i

– tablični prikaz raspodjele podskupova mjera iz podstavka 3. ovoga stavka po razinama mjera iz članka 38. ove Uredbe.

Članak 44.

(1) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz članka 38. ove Uredbe obvezujuća, označeni su u tabličnom prikazu iz članka 43. podstavka 5. ove Uredbe oznakom »A«.

(2) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz članka 38. ove Uredbe obvezujuća pod uvjetima opisanim u razradi mjere iz članka 43. podstavka 4. ove Uredbe pod »UVJET:«, označeni su u tabličnom prikazu iz članka 43. podstavka 5. ove Uredbe oznakom »B«.

(3) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz član-

ka 38. ove Uredbe dobrovoljna, označeni su u tabličnom prikazu iz članka 43. podstavka 5. ove Uredbe oznakom »C«.

Članak 45.

(1) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima koji su u tabličnom prikazu iz članka 43. podstavka 5. ove Uredbe označeni oznakom »C«, preporučuju se za provedbu ovisno o rezultatima procjene rizika koju subjekt provodi u okviru provedbe mjere naziva »Upravljanje rizicima« iz točke 3. Priloga II. ove Uredbe.

(2) Provedba podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima koji su u tabličnom prikazu iz članka 43. podstavka 5. ove Uredbe označeni oznakom »C« dodatno se vrednuje kroz postupak samoprocjene kibernetičke sigurnosti i revizije kibernetičke sigurnosti.

(3) Za potrebe provedbe procjene rizika iz stavka 1. ovoga članka, središnje državno tijelo za kibernetičku sigurnost donosi smjernice za procjenu, obradu, praćenje i ažuriranje rizika za mrežne i informacijske sustave, koje se mogu koristiti u okviru provedbe mjere naziva »Upravljanje rizicima« iz točke 3. Priloga II. ove Uredbe.

(4) Središnje državno tijelo za kibernetičku sigurnost objavljuje smjernice iz stavka 3. ovoga članka na svojim mrežnim stranicama.

Članak 46.

(1) Usluge koje pružaju, odnosno djelatnosti koje obavljaju privatni i javni subjekti iz sektora digitalne infrastrukture iz Priloga I. Zakona, temelje se na mrežnim i informacijskim sustavima te se ovom Uredbom za te vrste subjekata utvrđuje posebni, prošireni skup mjera fizičke sigurnosti kao dio mjera upravljanja kibernetičkim sigurnosnim rizicima koje su ti subjekti dužni provoditi.

(2) Prošireni skup mjera fizičke sigurnosti iz stavka 1. ovoga članka utvrđen je Prilogom III. ove Uredbe.

Članak 47.

(1) U svrhu provedbe dobrovoljnih mehanizama kibernetičke zaštite iz članka 50. Zakona, subjekti koji nisu kategorizirani kao ključni i važni subjekti provode najmanje osnovnu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima.

(2) U slučajevima iz članka 60. Zakona, nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su provoditi naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima.

Članak 48.

Sve provedene mjere upravljanja kibernetičkim sigurnosnim rizicima, ključni i važni subjekti i subjekti iz članka 47. ove Uredbe moraju ažurirati:

– u planiranim vremenskim razdobljima, a najmanje jednom godišnje u okviru redovite godišnje procjene rizika subjekta

– kada dođe do značajnog incidenta

– kada provode značajne promjene u okviru mrežnog i informacijskog sustava

– u okviru većih poslovno-organizacijskih promjena, spajanja ili promjene vlasničke strukture subjekta koja može imati utjecaja na upravljanje subjektom

– kada se utvrdi neusklađenost subjekta u postupku revizije kibernetičke sigurnosti ili samoprocjene kibernetičke sigurnosti ili

– kada se subjektu izreknu korektivne mjere u postupku stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti.

Članak 49.

(1) Kako bi se olakšala provedba mjera upravljanja kibernetičkim sigurnosnim rizicima, središnje državno tijelo za kibernetičku sigurnost izrađuje korelacijski pregled mjera iz Priloga II. ove Uredbe, kao i svih podskupova ovih mjera, na najvažnije europske i međunarodne norme i najbolje prakse iz otvorenih izvora (mapiranje mjera).

(2) Središnje državno tijelo za kibernetičku sigurnost objavljuje korelacijski pregled iz stavka 1. ovoga članka na svojim mrežnim stranicama.

Članak 50.

U svrhu podizanja razine kibernetičke sigurnosti subjekata koji nisu kategorizirani kao ključni ili važni subjekti i ne provode dobrovoljne mehanizme kibernetičke zaštite iz članka 50. Zakona, subjekata koji tek započinju s uvođenjem mjera upravljanja kibernetičkim sigurnosnim rizicima ili predstavljaju mikro ili mali subjekt malog gospodarstva s ograničenim resursima i znanjem u pitanjima upravljanja kibernetičkim sigurnosnim rizicima, središnje državno tijelo za kibernetičku sigurnost priprema i na svojim mrežnim stranicama objavljuje preporuke za provođenje dobre prakse kibernetičke sigurnosti.

POGLAVLJE III.
SAMOPROCJENA KIBERNETIČKE SIGURNOSTI

Članak 51.

(1) Samoprocjenom kibernetičke sigurnosti utvrđuje se stupanj usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe utvrđenim za razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe koju je subjekt dužan provoditi, kao i trend podizanja razine zrelosti kibernetičke sigurnosti subjekta.

(2) Samoprocjenu kibernetičke sigurnosti važni subjekti i subjekti iz članka 47. ove Uredbe provode najmanje jednom u dvije godine.

(3) Samoprocjenu kibernetičke sigurnosti ključni subjekti mogu provoditi kao pripremu za provedbu revizije kibernetičke sigurnosti ili stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti iz članka 75. stavka 1. Zakona.

Članak 52.

(1) Stupanj usklađenosti uspostavljenih mjera temelji se na procjeni stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima u subjektu.

(2) Procjenom stupnja usklađenosti dokumentiranih mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se postoje li dokumentirane sigurnosne politike o provedbi mjera i u kojoj mjeri su u skladu sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima Prilogom II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe koju je subjekt dužan provoditi.

(3) Procjenom stupnja usklađenosti implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se u kojoj mjeri su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima usklađene sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima u Prilogu II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe koju je subjekt dužan provoditi.

Članak 53.

(1) Stupanj usklađenosti uspostavljenih mjera iz članka 52. stavaka 2. i 3. ove Uredbe utvrđuje se temeljem bodovanja podskupova

mjera upravljanja kibernetičkim sigurnosnim rizicima koje subjekt provodi kao obvezujuće sukladno članku 44. stavcima 1. i 2. ove Uredbe.

(2) U svrhu provedbe bodovanja iz prethodnog stavaka ovoga članka, za svaku razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe utvrđuje se broj bodova potreban za potvrđivanje sukladnosti subjekta s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe.

Članak 54.

(1) Trend podizanja razine zrelosti kibernetičke sigurnosti utvrđuje se dodatnim bodovanjem podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima koje subjekt provodi na temelju mjere 3. »Upravljanje rizicima« iz Priloga II. ove Uredbe, u smislu podizanja razine provedbe pojedinih obvezujućih mjera sukladno članku 44. stavcima 1. i 2. ove Uredbe, kao i u smislu provedbe dobrovoljnih mjera sukladno članku 44. stavku 3. ove Uredbe.

(2) U svrhu provedbe bodovanja iz prethodnog stavaka, za svaku razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe utvrđuje se broj bodova potreban za utvrđivanje trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

Članak 55.

(1) Ako rezultati bodovanja stupnja usklađenosti mjera sukladno članku 53. ove Uredbe pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe, subjekt sastavlja izjavu o sukladnosti iz stavka 3. ovoga članka.

(2) Ako rezultati bodovanja stupnja usklađenosti mjera sukladno članku 53. ove Uredbe pokazuju da nisu uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe, subjekt utvrđuje plan daljnjeg postupanja, koji uključuje plan za pravodobnu ponovnu samoprocjenu kibernetičke sigurnosti i ispravljanje utvrđenih nedostataka.

(3) Izjava o sukladnosti iz članka 35. stavka 3. Zakona sadrži sljedeće podatke:

– naziv i adresu subjekta

– naziv sektora, podsektora i vrstu subjekta, prema nazivima iz Priloga I. ove Uredbe, za ključne i važne subjekte, odnosno

– naziv sektora i glavne poslovne djelatnosti za subjekte iz članka 47. stavka 1. ove Uredbe

– utvrđenu razinu kibernetičkih sigurnosnih rizika za subjekt, kada je primjenjivo

– razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe

– rezultate bodovanja stupnja usklađenosti mjera upravljanja kibernetičkim sigurnosnim rizicima s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe

– rezultate bodovanja trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta

– popis dokumentacije nastale u postupku samoprocjene kibernetičke sigurnosti

– ime, prezime i potpis osobe koja je provela postupak samoprocjene kibernetičke sigurnosti

– izjavu osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima da rezultati provedene samoprocjene kibernetičke sigurnosti za subjekt pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom i ovom Uredbom

– ime, prezime i potpis osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima.

(4) Subjekt izjavu o sukladnosti iz članka 35. stavka 3. Zakona sastavlja na obrascu iz Priloga IV. ove Uredbe.

(5) Subjekt je dužan izjavu o sukladnosti iz članka 35. stavka 3. Zakona i drugu dokumentaciju nastalu u postupku samoprocjene kibernetičke sigurnosti čuvati deset godina od sastavljanja takve izjave.

Članak 56.

Za provedbu samoprocjene kibernetičke sigurnosti subjekt je dužan odrediti svoje zaposlenike ili vanjske suradnike koji posjeduju najmanje:

– relevantna znanja iz implementacije međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti

– potvrdu o završenoj vanjskoj ili internoj edukaciji za internog revizora po nekoj od relevantnih međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti

– jednu godinu radnog iskustva u okviru provođenja sličnih vrsta interne revizije u području mrežnih i informacijskih sustava odnosno kibernetičke sigurnosti.

Članak 57.

(1) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti donosi smjernice za provedbu samoprocjena kibernetičke sigurnosti, čiji je sastavni dio kalkulator za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.

(2) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti objavljuje smjernice iz stavka 1. ovoga članka na svojim mrežnim stranicama.

DIO PETI
PRAVILA OBAVJEŠTAVANJA O KIBERNETIČKIM PRIJETNJAMA I INCIDENTIMA ZA KLJUČNE I VAŽNE SUBJEKTE

POGLAVLJE I.
OBAVJEŠTAVANJE O ZNAČAJNIM INCIDENTIMA

Članak 58.

Značajan incident je svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 59. do 62. ove Uredbe, uzimajući u obzir kriterijske pragove, kada su propisani.

ODJELJAK 1
KRITERIJI ZA UTVRĐIVANJE ZNAČAJNIH INCIDENATA

Članak 59.

(1) Incidenti koji uzrokuju ili mogu uzrokovati ozbiljne poremećaje u funkcioniranju usluga su incidenti:

– koji negativno utječu na dostupnost usluge ili narušavaju kvalitetu usluge ili

– imaju ili mogu imati negativan učinak na autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga.

(2) Smatra se da incident negativno utječe na dostupnost usluge ili narušava kvalitetu usluge, ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

– najmanje 20 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje jedan sat

– najmanje 1 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje osam sati, pod uvjetom da 1 % primatelja usluge čini najmanje 100 primatelja usluge

– pristup usluzi nije bio moguć u trajanju od jednog sata ili više, a subjekt nije u mogućnosti utvrditi koliko primatelja usluge nije moglo pristupiti usluzi tijekom vremenskog perioda u kojem usluga nije bila dostupna

– najmanje 30 % primatelja usluge povremeno nije moglo pristupiti usluzi ili nije moglo uslugu funkcionalno koristiti zbog smanjene razine kvalitete usluge, ako su povremeni prekidi pristupa usluzi, odnosno nemogućnost funkcionalnog korištenja usluge, trajali ukupno najmanje jedan sat tijekom vremenskog perioda od četiri sata

– pristup usluzi u bolnici, zračnoj luci, zračnom prijevozniku, objektu banke s podatkovnim centrima, objektu policijskog sustava, aktivnom vodocrpilištu i centru upravljanja, objektu operatora elektroničkih komunikacija, objektu tijela sigurnosno-obavještajnog sustava, objektu profesionalne vatrogasne postrojbe ili subjektu koji su utvrđeni kao kritični subjekti na temelju zakona kojim se uređuje područje kritične infrastrukture nije bio moguć u trajanju od najmanje jedan sat

– pristup usluzi kontrole zračnog prometa nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna

– pristup usluzi koja se koristi za potrebe Ministarstva obrane i Oružanih snaga Republike Hrvatske, civilnih nositelja obrambenog planiranja, odnosno za potrebe pravnih osoba posebno važnih za obranu nije bio moguć u trajanju od najmanje jedan sat

– pristup usluzi Centra 112 i drugih hitnih službi nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna

– pristup usluzi na području najmanje jedne županije ili jednog velikog grada ili grada koji predstavlja sjedište županije nije bio moguć u trajanju od najmanje jedan sat.

(3) Smatra se da incident ima ili može imati negativan učinak na autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

– kritičnim dijelovima mrežnog i informacijskog sustava subjekta ili kritičnim podacima ostvaren je pristup od strane neovlaštene osobe ili su stečeni preduvjeti za ostvarivanje pristupa neovlaštenoj osobi

– kritični mrežni i informacijski sustavi subjekta konfigurirani su od strane neovlaštene osobe ili su stečeni preduvjeti koji omogućavaju konfiguraciju kritičnog mrežnog i informacijskog sustava neovlaštenoj osobi

– zbog incidenta su nastupile okolnosti koje onemogućuju ovlaštenoj osobi konfiguriranje kritičnog mrežnog i informacijskog sustava

– konfiguracija kritičnog mrežnog i informacijskog sustava subjekta neovlašteno je mijenjana, dopunjavana ili je iz drugih razloga postala nepouzdana ili su kritični podaci neovlašteno uklonjeni, mijenjani, dopunjavani ili su iz drugih razloga postali nepouzdani

– kritični mrežni i informacijski sustavi subjekta i/ili drugi mrežni i informacijski sustavi subjekta koji mogu utjecati na kritične mrežne i informacijske sustave subjekta obavljaju zadaće koje odstupaju od uspostavljenih procedura obavljanja poslovnih aktivnosti na sustavu i/ili uspostavljenog okvira kontrola u kojem ti sustavi uobičajeno djeluju, a osobito ako obavljaju zadaće za koje nije predviđeno da ih ti sustavi obavljaju ili ne obavljaju osnovne zadaće za koje je predviđeno da ih ti sustavi obavljaju.

(4) U smislu stavka 3. ovoga članka smatra se da su svi sustavi i podaci kritični, ako subjekt nije proveo klasifikaciju kritičnosti mrežnih i informacijskih sustava, nije utvrdio kritične podatke ili ne može utvrditi kritične mrežne i informacijske sustave ili kritične podatke na koje je incident negativno utjecao.

Članak 60.

(1) Smatra se da incident uzrokuje ili može uzrokovati financijske gubitke za subjekt ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

– ako gubitak prihoda ili troškovi uzrokovani incidentom ili zbroj tih dvaju faktora iznosi stotinu tisuća eura ili najmanje 5 % ukupnog godišnjeg poslovnog prihoda subjekta, ovisno o tome koji iznos je niži

– ako pristup usluzi nije bio moguć najmanje jedan sat primateljima usluga od kojih je subjekt u prethodnoj godini ostvario prihode u iznosu od stotinu tisuća eura ili najmanje 5 % ukupnog godišnjeg poslovnog prihoda subjekta, ovisno o tome koji iznos je niži

– ako je incident uzrokovao reputacijsku štetu subjektu.

(2) Ukupnim godišnjim poslovnim prihodom subjekta u smislu stavka 1. ovoga članka smatra se ukupan godišnji poslovni prihod subjekta prema financijskim izvještajima za prethodnu godinu, neovisno o tome pruža li subjekt i druge usluge odnosno obavlja li i druge djelatnosti koje nisu obuhvaćene Prilogom I. i Prilogom II. Zakona.

(3) Prihodom u smislu stavka 1. ovoga članka smatraju se svi prihodi subjekta na godišnjoj razini, neovisno o tome ostvaruje li ih ili ih je planirao ostvariti redovnim poslovanjem subjekta ili radnjama koje izlaze izvan opsega redovnog poslovanja subjekta.

(4) Troškovima u smislu stavka 1. ovoga članka smatraju se svi troškovi koji su za subjekt nastali zbog poduzimanja radnji i aktivnosti radi zaustavljanja incidenta, odgovora na incident ili oporavka od incidenta, uključujući sve radnje i aktivnosti poduzete radi uspostavljanja redovnog opsega poslovanja subjekta. Troškovima se ne smatraju ugovorne kazne ili druge vrste naknada koje je subjekt u obvezi namiriti zbog povrede ugovornih odnosa uzrokovanih incidentom, neovisno o tome radi li se o fizičkim i pravnim osobama, zaposlenicima subjekta ili njegovim vanjskim suradnicima.

(5) Smatra se da je incident uzrokovao štetu ugledu subjekta u smislu stavka 1. podstavka 3. ovoga članka, ako je ispunjen jedan od sljedećih kriterijskih pragova:

– o incidentu je izvještavao javni pružatelj medijske usluge

– incident je rezultirao podizanjem prigovora, tužbi ili drugih pravnih lijekova najmanje 1 % primatelja njegovih usluga protiv subjekta.

Članak 61.

(1) Smatra se da je incident utjecao ili bi mogao utjecati na druge fizičke i pravne osobe uzrokovanjem znatne materijalne ili

nematerijalne štete, ako je zbog incidenta posljedično nastupilo jedno od sljedećeg:

– smrt ili tjelesna ozljeda koja je zahtijevala hospitalizaciju ili terapijske postupke

– potpuno uništenje ili znatno oštećenje materijalne imovine drugih fizičkih ili pravnih osoba

– obustava ili znatno smanjenje poslovanja drugih fizičkih ili pravnih osoba

– gubitak ili kompromitacija osobnih ili osjetljivih podataka drugih fizičkih ili pravnih osoba.

(2) Drugim fizičkim i pravnim osobama u smislu stavka 1. ovoga članka smatraju se primatelji usluga ključnog i važnog subjekta, ali i svaka druga fizička i pravna osoba koja je zbog značajnog incidenta pretrpjela materijalnu ili nematerijalnu štetu iz stavka 1. ovoga članka.

Članak 62.

Incidenti koji pojedinačno ne ispunjavaju kriterije za značajan incident iz članaka 59. do 61. ove Uredbe, smatrat će se značajnim incidentom ako su se:

– dogodili najmanje dva puta u razdoblju od šest mjeseci

– imaju isti temeljni uzrok

– zajedno ispunjavaju najmanje jedan kriterij za značajan incident iz članaka 59. do 61. ove Uredbe.

Članak 63.

Prekidi u pružanju usluge ili narušavanje kvalitete usluge uslijed planiranog redovnog održavanja mrežnog i informacijskog sustava ključnih i važnih subjekata ne smatraju se značajnim incidentom u smislu članaka 59. do 62. ove Uredbe.

ODJELJAK 2
OBAVIJESTI O ZNAČAJNIM INCIDENTIMA

Članak 64.

Ključni i važni subjekti dužni su nadležni CSIRT obavijestiti o svakom značajnom incidentu.

Članak 65.

Ključni i važni subjekti dužni su nadležnom CSIRT-u dostavljati sljedeće vrste obavijesti o značajnom incidentu:

– rano upozorenje o značajnom incidentu

– početnu obavijest o značajnom incidentu

– privremeno izvješće o značajnom incidentu

– izvješće o napretku

– završno izvješće o značajnom incidentu.

Članak 66.

(1) Rano upozorenje o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u, bez odgode, a najkasnije u roku od 24 sata od trenutka saznanja za značajan incident.

(2) Rano upozorenje o značajnom incidentu mora sadržavati:

– datum i vrijeme saznanja za incident

– opis osnovnih značajki incidenta

– podatak o tome postoji li sumnja da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem

– procjenu subjekta može li incident imati prekogranični utjecaj

– procjenu subjekta može li incident imati međusektorski utjecaj.

Članak 67.

(1) Početnu obavijest o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u, bez odgode, a najkasnije u roku od 72 sata od trenutka saznanja za značajan incident.

(2) Početna obavijest o značajnom incidentu mora sadržavati:

– ažurirani opis osnovnih značajki incidenta i drugih informacija dostavljenih sukladno članku 66. ove Uredbe

– početnu procjenu značajnog incidenta

– indikatore kompromitacije, ako su dostupni.

(3) Početna procjena značajnog incidenta uključuje procjenu ključnog i važnog subjekta o:

– tome koji mrežni i informacijski sustav subjekta je pogođen incidentom i važnosti tog sustava za pružanje usluga odnosno obavljanje djelatnosti subjekta

– ozbiljnosti i učinku incidenta, uzimajući pri tome u obzir mjeru u kojoj je ugroženo pružanje usluga odnosno obavljanje djelatnosti subjekta, trajanje incidenta i broj primatelja usluga na koje je incident utjecao

– tehničkim značajkama incidenta

– ranjivostima koje se iskorištavaju

– iskustvima subjekta sa sličnim incidentima.

Članak 68.

Iznimno od članka 66. stavka 1. ove Uredbe i članka 67. stavka 1. ove Uredbe, pružatelji usluga povjerenja dužni su nadležnom CSIRT-u, bez odgode, a najkasnije u roku od 24 sata od trenutka saznanja za značajan incident, dostaviti početnu obavijest o značajnom incidentu, uključujući podatak o datumu i vremenu saznanja za incident.

Članak 69.

(1) Ključni i važni subjekti dužni su dostaviti privremeno izvješće o značajnom incidentu na zahtjev nadležnog CSIRT-a.

(2) U zahtjevu iz stavka 1. ovoga članka, nadležni CSIRT dužan je odrediti:

– na koje podatke iz članka 67. ove Uredbe se zahtjev odnosi

– rok za dostavu privremenog izvješća o značajnom incidentu.

(3) Rok za dostavu privremenog izvješća o značajnom incidentu određuje se ovisno o opsegu i složenosti podataka na koje se zahtjev iz stavka 1. ovoga članka odnosi, s tim da ostavljeni rok ne može biti kraći od 48 sati niti duži od sedam dana od primitka zahtjeva za dostavu privremenog izvješća.

(4) Ako to ocijeni potrebnim, nadležni CSIRT može višekratno, sve do dostave završnog izvješće o značajnom incidentu, podnositi zahtjeve iz stavka 1. ovoga članka.

Članak 70.

(1) Završno izvješće o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u najkasnije u roku od 30 dana od dana dostave početne obavijesti o značajnom incidentu.

(2) Završno izvješće o značajnom incidentu mora sadržavati:

– detaljan opis incidenta

– vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident

– potvrđene indikatore kompromitacije

– podatke o kibernetičkom napadaču na kojeg se sumnja ili je potvrđen

– podatke o ozbiljnosti i učinku incidenta, koji obvezno uključuju opis poremećaja koje je incident izazvao u pružanju usluga odnosno obavljanju djelatnosti subjekta, trajanju incidenta i broju primatelja usluga na koje je incident utjecao te o možebitnoj kompromitaciji osjetljivih podataka

– primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku

– mjere za postizanje više razine kibernetičke sigurnosti koje subjekt planira primijeniti kako bi se minimizirala mogućnost ponavljanja istog ili sličnog incidenta te kako bi se ublažio rizik

– podatke o prekograničnom učinku incidenta, ako je incident imao takav učinak

– podatke o međusektorskom učinku incidenta, ako je incident imao takav učinak.

Članak 71.

(1) U slučaju da je incident još u tijeku, ključni i važni subjekti dužni su u roku iz članka 70. stavka 1. ove Uredbe nadležnom CSIRT-u, umjesto završnog izvješća o značajnom incidentu, dostaviti izvješće o napretku.

(2) Izvješće o napretku mora sadržavati:

– ažurirani opis osnovnih značajki incidenta, početne procjene značajnog incidenta i drugih informacija dostavljenih sukladno člancima 67. do 69. ove Uredbe

– vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident

– primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku

– procjenu i obrazloženje uzroka koji su doveli do produženog trajanja odgovora na incident.

(3) U slučaju trajanja značajnog incidenta duže od 60 dana od dana podnošenja početne obavijesti o značajnom incidentu, ključni i važni subjekti dužni su dostavljati nadležnom CSIRT-u izvješće o napretku svakih 30 dana.

(4) U slučajevima iz stavaka 1. i 3. ovoga članka, ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u završno izvješće o značajnom incidentu najkasnije u roku od 30 dana od posljednje dostavljenog izvješća o napretku.

Članak 72.

(1) Obavijesti o značajnim incidentima dostavljaju se na obrascima koji se utvrđuju općim smjernicama za provedbu obveze obavještavanja o značajnim incidentima.

(2) Opće smjernice iz stavka 1. ovoga članka donose zajedno nadležni CSIRT-ovi, uz naknadnu suglasnost središnjeg državnog tijela za kibernetičku sigurnost.

(3) Obrasci i opće smjernice iz stavka 1. ovoga članka izrađuju se vodeći računa o ENISA-inim tehničkim smjernicama o parametrima za informacije u svrhu obavještavanja ENISA-e temeljem članka 42. stavka 2. Zakona.

(4) Nadležni CSIRT-ovi, nakon dobivene suglasnosti središnjeg državnog tijela za kibernetičku sigurnost na opće smjernice iz stavka 1. ovoga članka, objavljuju opće smjernice na svojim mrežnim stranicama.

Članak 73.

(1) Nadležni CSIRT-ovi mogu donositi sektorske smjernice za provedbu obveze obavještavanja o značajnim incidentima, ako postoje sektorske specifičnosti koje nisu obuhvaćene općim smjernicama iz članka 72. ove Uredbe.

(2) Nadležni CSIRT-ovi objavljuju sektorske smjernice iz stavka 1. ovoga članka na svojim mrežnim stranicama.

Članak 74.

(1) O provedbi obveze ključnih i važnih subjekata vezano uz dostavu obavijesti o značajnim incidentima tijelima kaznenog progona u slučajevima iz članka 37. stavka 3. Zakona, donose se posebne smjernice.

(2) Smjernice iz stavka 1. ovoga članka donose zajedno nadležni CSIRT-ovi, u suradnji s tijelima kaznenog progona.

(3) Nadležni CSIRT-ovi objavljuju smjernice iz stavka 1. ovoga članka na svojim mrežnim stranicama.

ODJELJAK 3
POSTUPANJA NADLEŽNOG CSIRT-a POVODOM ZAPRIMLJENIH OBAVIJESTI O ZNAČAJNIM INCIDENTIMA

Članak 75.

Ako obavijest o značajnom incidentu nije dostavljena u skladu s člancima 66. do 72. ove Uredbe, nadležni CSIRT će o tome obavijestiti subjekta i odrediti rok u kojem je subjekt dužan otkloniti nedostatke, uz upozorenje na pravne posljedice sukladno Zakonu ako to ne učini u ostavljenom roku.

Članak 76.

(1) Nadležni CSIRT dužan je bez odgode, a najkasnije u roku od 24 sata od primitka ranog upozorenja o značajnom incidentu, dostaviti subjektu početne povratne podatke o incidentu.

(2) Uz početne povratne podatke o incidentu, nadležni CSIRT dostavit će ključnom i važnom subjektu smjernice i operativne savjete o provedbi mogućih mjera ublažavanja incidenta, ako je subjekt to zatražio u ranom upozorenju o značajnom incidentu odnosno početnoj obavijesti o značajnom incidentu u slučajevima iz članka 68. ove Uredbe.

(3) U slučaju da je subjekt sukladno članku 75. ove Uredbe pozvan na otklanjanje nedostataka u dostavljenom ranom upozorenju o značajnom incidentu, rok iz stavka 1. ovoga članka računa se od dostave ispravljenog ranog upozorenja o značajnom incidentu.

(4) Rokovi iz stavaka 1. i 3 ovoga članka u slučajevima iz članka 68. ove Uredbe računaju se od primitka početne obavijesti o značajnom incidentu.

Članak 77.

Nadležni CSIRT po zaprimanju obavijesti iz članaka 67. do 71. ove Uredbe provodi analizu i klasifikaciju incidenta prema nacionalnoj taksonomiji incidenata te, ako to dopuštaju okolnosti, nakon primitka takve obavijesti, dostavlja ključnim i važnim subjektima informacije relevantne za daljnje postupanje sa značajnim incidentom, a osobito informacije koje bi mogle pridonijeti djelotvornom rješavanju značajnog incidenta.

Članak 78.

Nacionalnu taksonomiju incidenata iz članka 77. ove Uredbe donosi središnje državno tijelo za kibernetičku sigurnost, na prijedlog nadležnih CSIRT-ova.

Članak 79.

(1) Nadležni CSIRT uključuje se u postupak rješavanja značajnog incidenta na zahtjev ključnog i važnog subjekta.

(2) Zahtjev iz stavka 1. ovoga članka ključni i važni subjekti mogu podnijeti u okviru bilo koje od faza izvještavanja o značajnom incidentu iz članka 65. ove Uredbe, koristeći obrasce za izvještavanje iz članka 72. ove Uredbe.

(3) U slučaju iz stavka 1. ovoga članka, ključni i važni subjekti dužni su nadležnom CSIRT-u, na njegov zahtjev, dostaviti sve podatke potrebne za djelotvorno rješavanje značajnog incidenta.

(4) Dostava podataka sukladno stavku 3. ovoga članka ne utječe na provedbu obveza ključnih i važnih subjekata iz članaka 65. do 72. ove Uredbe.

Članak 80.

(1) Nadležni CSIRT po zaprimanju obavijesti iz članaka 66. do 72. ove Uredbe o značajnim incidentima koji imaju prekogranični ili međusektorski učinak, dužan je bez odgode, a najkasnije u roku od tri dana od primitka takve obavijesti, dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti izvješće o mogućem prekograničnom i međusektorskom učinku značajnog incidenta, s procjenom potencijalnog učinka incidenta.

(2) Prilikom izrade izvješća iz stavka 1. ovoga članka nadležni CSIRT je dužan uzeti u obzir i podatke koje su mu o značajnom incidentu dostavili jedinstvena kontaktna točka i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

Članak 81.

Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je bez odgode, a najkasnije u roku od tri dana od primitka izvješća iz članka 80. stavka 1. ove Uredbe, očitovati se nadležnom CSIRT-u o procjeni prekograničnog i međusektorskog učinka incidenta.

Članak 82.

(1) Ako zaprimi nove podatke o značajnom incidentu koji su od utjecaja na prethodno danu procjenu učinka incidenta ili kada to od njega zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, nadležni CSIRT dužan je izraditi novo izvješće o prekograničnom i međusektorskom učinku značajnog incidenta, s novom procjenom učinka incidenta.

(2) U slučaju iz stavka 1. ovoga članka na odgovarajući način se primjenjuju članci 80. i 81. ove Uredbe.

Članak 83.

Izvješća nadležnog CSIRT-a iz članaka 80. i 82. ove Uredbe dostavljaju se jedinstvenoj kontaktnoj točki najkasnije u roku od tri dana od sačinjavanja, a očitovanje nadležnog tijela iz članka 81. ove Uredbe dostavlja se jedinstvenoj kontaktnoj točki najkasnije u roku od tri dana od zaprimanja.

Članak 84.

U obavljanju zadaća iz članaka 75. do 83. ove Uredbe, nadležni CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika.

POGLAVLJE II.
OBAVJEŠTAVANJE PRIMATELJA USLUGA O ZNAČAJNIM INCIDENTIMA I OZBILJNIM KIBERNETIČKIM PRIJETNJAMA

Članak 85.

(1) Ključni i važni subjekti su dužni, bez odgode, a najkasnije u roku od 72 sata od saznanja za značajan incident, na jasan i lako dokaziv način, o značajnom incidentu obavijestiti primatelje svojih usluga na koje bi takav incident mogao utjecati.

(2) Obavijest iz stavka 1. ovoga članka mora sadržavati sljedeće podatke o značajnom incidentu:

– vrstu i kratki opis incidenta

– uzrok incidenta

– mogući utjecaj incidenta na uslugu

– kontakt podatke subjekta

– upute o postupanju primatelja usluga u svrhu ublažavanja učinka nastalog incidenta i naknade uzrokovane štete.

(3) U slučaju da u trenutku slanja obavijesti iz stavka 1. ovoga članka ključnom i važnom subjektu nisu poznati neki od podataka iz stavka 2. ovoga članka, subjekt je dužan najkasnije u roku od 72 sata od slanja obavijesti, dostaviti i te preostale podatke primateljima usluga na koje bi takav incident mogao utjecati.

Članak 86.

(1) U slučaju pojave ozbiljne kibernetičke prijetnje, ključni i važni subjekti dužni su primatelje svojih usluga, na koje bi takva prijetnja mogla utjecati, obavijestiti o svim mogućim mjerama zaštite ili pravnim sredstvima koje mogu uporabiti u svrhu sprečavanja ili naknade uzrokovane štete te, po potrebi, obavijestiti primatelje usluga i o samoj ozbiljnoj kibernetičkoj prijetnji.

(2) Na obavještavanje primatelja usluga o ozbiljnim kibernetičkim prijetnjama na odgovarajući način se primjenjuje članak 85. ove Uredbe.

POGLAVLJE III.
OBAVIJESTI KLJUČNIH I VAŽNIH SUBJEKATA NA DOBROVOLJNOJ OSNOVI

Članak 87.

(1) Kada dobrovoljno obavještavaju o ostalim incidentima na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o incidentu koja mora sadržavati:

– datum i vrijeme saznanja za incident

– opis tehničkih značajki incidenta, uključujući trajanje incidenta i vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident

– indikatore kompromitacije, ako su dostupni

– podatke o ranjivostima koje se iskorištavaju

– podatke o tome koji mrežni i informacijski sustav subjekta je pogođen incidentom

– opis poremećaja koje je incident izazvao u pružanju usluga odnosno obavljanju djelatnosti subjekta te broj primatelja usluga subjekta i/ili korisnika mrežnog i informacijskog sustava subjekta na koje je incident utjecao

– primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku

– iskustva subjekta sa sličnim incidentima u prošlosti

– podatak o tome postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovoga članka odmah po saznanju za incident, a najkasnije u roku od 30 dana od trenutka saznanja za incident, vodeći pri tome računa o ozbiljnosti incidenta i opsegu podataka o izbjegnutom incidentu kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o incidentu do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovoga članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovoga članka.

Članak 88.

(1) Kada dobrovoljno obavještavaju o kibernetičkim prijetnjama na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o kibernetičkoj prijetnji koja mora sadržavati:

– datum i vrijeme saznanja za kibernetičku prijetnju

– opis kibernetičke prijetnje i njezin trenutni status

– podatke o potencijalnom učinku kibernetičke prijetnje na mrežne i informacijske sustave subjekta i njegove korisnike, uključujući opis poremećaja koje bi kibernetička prijetnja mogla izazvati u pružanju usluga odnosno obavljanju djelatnosti subjekta

– opis mjera primijenjenih u svrhu sprječavanja učinka kibernetičke prijetnje na mrežne i informacijske sustave subjekta.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovoga članka odmah po saznanju za kibernetičku prijetnju, a najkasnije u roku od 30 dana od trenutka saznanja za kibernetičku prijetnju, vodeći pri tome računa o ozbiljnosti kibernetičke prijetnje i opsegu podataka o kibernetičkoj prijetnji kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o kibernetičkoj prijetnji do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovoga članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovoga članka.

Članak 89.

(1) Kada dobrovoljno obavještavaju o izbjegnutim incidentima na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o izbjegnutom incidentu koja mora sadržavati:

– datum i vrijeme saznanja za izbjegnuti incident

– opis tehničkih značajki izbjegnutog incidenta, uključujući vrstu prijetnje ili temeljnog uzroka koji je mogao uzrokovati incident

– indikatore kompromitacije, ako su dostupni

– podatke o ranjivostima koje se pokušalo iskoristiti

– podatke o tome koji mrežni i informacijski sustav subjekta je bio izložen izbjegnutom incidentu

– podatke o potencijalnom učinku izbjegnutog incidenta na mrežne i informacijske sustave subjekta i njegove korisnike, uključujući opis poremećaja koje je izbjegnuti incident mogao izazvati u pružanju usluga odnosno obavljanju djelatnosti subjekta

– iskustva subjekta sa sličnim izbjegnutim incidentima u prošlosti

– podatak o tome postoji li sumnja da je izbjegnuti incident uzrokovan nezakonitim ili zlonamjernim djelovanjem.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovoga članka odmah po saznanju za izbjegnuti incident, a najkasnije u roku od 30 dana od trenutka saznanja za izbjegnuti incident, vodeći pri tome računa o ozbiljnosti izbjegnutog incidenta i opsegu podataka o izbjegnutom incidentu kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o izbjegnutom incidentu do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovoga članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovoga članka.

Članak 90.

(1) Obavijesti o incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima dostavljaju se na obrascima koji se utvrđuju smjernicama za provedbu dobrovoljnog obavještavanja.

(2) Smjernice iz stavka 1. ovoga članka zajednički donose nadležni CSIRT-ovi, uz naknadnu suglasnost središnjeg državnog tijela za kibernetičku sigurnost.

(3) Obrasci i smjernice iz stavka 1. ovoga članka izrađuju se vodeći računa o ENISA-inim tehničkim smjernicama o parametrima za informacije u svrhu obavještavanja ENISA-e temeljem članka 42. stavka 2. Zakona.

(4) Nadležni CSIRT-ovi, nakon dobivene suglasnosti središnjeg državnog tijela za kibernetičku sigurnost na donesene smjernice iz stavka 1. ovoga članka, objavljuju smjernice na svojim mrežnim stranicama.

Članak 91.

(1) U povodu obavijesti iz članaka 87. do 89. ove Uredbe, nadležni CSIRT dostavit će ključnom i važnom subjektu preporuke i operativne savjete o provedbi mogućih mjera ublažavanja i djelotvornog rješavanja incidenta, sprečavanja nastanka potencijalnog učinka kibernetičke prijetnje i izbjegnutog incidenta, ako je subjekt to zatražio u dostavljenoj obavijesti o incidentu, obavijesti o kibernetičkoj prijetnji odnosno izbjegnutom incidentu.

(2) Kada iz dostavljenih podataka proizlazi da prijavljeni događaj ima obilježja značajnog incidenta iz članaka 59. do 62. ove Uredbe, nadležni CSIRT dostavit će ključnom i važnom subjektu obavijest o obvezi obavještavanja o značajnom incidentu sukladno člancima 64. do 74. ove Uredbe.

Članak 92.

(1) Nadležni CSIRT uključuje se u postupak rješavanja incidenta o kojem je obavješten temeljem članka 87. ove Uredbe, ako je subjekt to zatražio u dostavljenoj obavijesti o incidentu.

(2) U slučaju iz stavka 1. ovoga članka na odgovarajući način se primjenjuje članak 79. stavak 3. ove Uredbe.

Članak 93.

U obavljanju zadaća iz članaka 91. i 92. ove Uredbe, nadležni CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika, a prilikom obrade zaprimljenih obavijesti ključnih i važnih subjekata na temelju članaka 37. i 39. Zakona, daje prednost obradi obavijesti o značajnim incidentima.

POGLAVLJE IV.
NACIONALNA PLATFORMA ZA PRIKUPLJANJE, ANALIZU I RAZMJENU PODATAKA O KIBERNETIČKIM PRIJETNJAMA I INCIDENTIMA

Članak 94.

(1) Ključni i važni subjekti dužni su koristiti nacionalnu platformu za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima (u daljnjem tekstu: nacionalna platforma) kao primarni način dostave obavijesti o:

– značajnim incidentima sukladno članku 37. Zakona i člancima 58. do 73. ove Uredbe i

– ostalim incidentima, izbjegnutim incidentima i kibernetičkim prijetnjama sukladno članku 39. Zakona i člancima 87. do 90. ove Uredbe.

(2) U iznimnim slučajevima kada dostava obavijesti sukladno stavku 1. ovoga članka iz opravdanih razloga nije moguća, ključni i važni subjekti dužni su obavijesti iz stavka 1. ovoga članka dostavljati komunikacijskim kanalima definiranim u smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

Članak 95.

(1) Ključni i važni subjekti stječu status subjekta korisnika nacionalne platforme na dan upisa subjekta u Popis ključnih i važnih subjekata.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su u obavijesti o provedenoj kategorizaciji subjekata iz članka 19. stavka 1. Zakona obavijestiti ključnog i važnog subjekta o stjecanju statusa subjekta korisnika nacionalne platforme i obvezama koje za njega proizlaze iz članaka 96. i 97. ove Uredbe.

Članak 96.

(1) Ključni i važni subjekti dužni su u roku od osam dana od primitka obavijesti iz članka 95. stavka 2. ove Uredbe imenovati osobu odgovornu za administriranje računa subjekta na nacionalnoj platformi (u daljnjem tekstu: administrator).

(2) Ključni i važni subjekti dužni su administratora imenovati iz reda svojih zaposlenika.

(3) Ključni i važni subjekti mogu imenovati do dva administratora.

(4) Podatke o imenovanim administratorima, uključujući promjene osoba administratora ili pojedinih podataka o imenovanim administratorima, ključni i važni subjekti unose u nacionalnu platformu sukladno uputi koja čini sastavni dio obavijesti iz članka 19. stavka 1. Zakona.

Članak 97.

(1) Ključni i važni subjekti dužni su u roku od osam dana od primitka obavijesti iz članka 95. stavka 2. ove Uredbe imenovati osobe ovlaštene za provedbu obavještavanja iz članaka 37. i 39. Zakona (u daljnjem tekstu: korisnici nacionalne platforme).

(2) Ključni i važni subjekti mogu korisnike nacionalne platforme imenovati iz reda svojih zaposlenika ili zaposlenika vanjskog davatelja povezanih usluga u subjektu, pri čemu odgovornost za provedbu obavještavanja iz članaka 37. i 39. Zakona ostaje na ključnom i važnom subjektu.

(3) Ključni i važni subjekti dužni su u odluci o imenovanju korisnika nacionalne platforme odrediti opseg njihovih korisničkih prava na način da odrede:

– zadužuje li se osoba za obavještavanje iz članka 37. Zakona i/ili za obavještavanje iz članka 39. Zakona

– vrstu usluga odnosno djelatnosti subjekta iz Priloga I. i II. Zakona na koje se zaduženje iz podstavka 1. ovoga stavka odnosi.

(4) Prilikom određivanja ukupnog broja korisnika nacionalne platforme ključni i važni subjekti dužni su uzeti u obzir veličinu subjekta, njegovu strukturu, stupanj izloženosti subjekta rizicima i vjerojatnost pojave incidenata.

(5) Administrator može biti imenovan i korisnikom nacionalne platforme.

Članak 98.

U nacionalnoj platformi administrator ima sljedeće ovlasti za subjekta za kojeg je imenovan:

– unošenja korisnika nacionalne platforme i njihovih korisničkih prava,

– ažuriranja podataka o korisnicima nacionalne platforme i

– deaktiviranja korisnika nacionalne platforme

– deaktiviranja korisničkih prava.

Članak 99.

Na temelju odluke o imenovanju korisnika nacionalne platforme iz članka 97. ove Uredbe, u okvirima njihovih korisničkih prava, administrator u nacionalnoj platformi dodjeljuje korisnicima nacionalne platforme subjekta za kojeg je imenovan sljedeće ovlasti:

– unošenja obavijesti o značajnim incidentima iz članka 37. Zakona i/ili

– unošenja obavijesti o ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima iz članka 37. Zakona.

Članak 100.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su u obavijesti iz članka 19. stavka 3. Zakona obavijestiti subjekta o prestanku statusa subjekta korisnika nacionalne platforme.

(2) Obavijest iz stavka 1. ovoga članka nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dostavlja i CARNET-u, radi provedbe deaktivacije korisničkih računa administratora i korisnika nacionalne platforme za subjekta na kojeg se obavijest odnosi.

(3) CARNET je dužan provesti deaktivaciju korisničkih računa najkasnije u roku od tri dana od zaprimanja obavijesti iz stavka 1. ovoga članka.

Članak 101.

(1) Ključni i važni subjekti dužni su koristiti nacionalnu platformu sukladno uvjetima korištenja nacionalne platforme koji su sadržani u smjernicama za korištenja nacionalne platforme.

(2) Smjernice za korištenja nacionalne platforme donosi CARNET, po prethodno pribavljenom mišljenju nadležnih CSIRT-ova i nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti.

(3) Prilikom utvrđivanja i ažuriranja uvjeta korištenja nacionalne platforme CARNET je dužan voditi računa o smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

(4) Uvjetima korištenja nacionalne platforme utvrđuju se, između ostalog, uvjeti korištenja nacionalne platforme u slučajevima iz članka 59. stavka 3. Zakona, a sukladno protokolu o postupanju nadležnih tijela koji je sklopljen za subjekt.

Članak 102.

(1) Nadležnim tijelima iz Priloga III. Zakona i jedinstvenoj kontaktnoj točki, CARNET dodjeljuje prava pristupa nacionalnoj platformi i omogućava njezino korištenje u opsegu koji je tim tijelima potreban za provedbu njihovih zadaća propisanih Zakonom i to:

– nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti za provedbu zadaća iz članka 59. stavaka 1. do 5. i članaka 64. i 65. Zakona

– nadležnim CSIRT-ovima za provedbu zadaća iz članka 66. Zakona i

– jedinstvenoj kontaktnoj točki za provedbu zadaća iz članaka 40. do 42. Zakona.

(2) Nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka dužni su CARNET obavijestiti o:

– zaposlenicima odgovornim za administriranje računima nadležnog tijela odnosno jedinstvene kontaktne točke na nacionalnoj platformi

– ostalim zaposlenicima nadležnog tijela odnosno jedinstvene kontaktne točke ovlaštenim za korištenje nacionalne platforme

– opsegu korisničkih prava za osobe iz podstavka 1. i 2. ovoga stavka.

(3) U slučajevima iz članka 94. stavka 2. ove Uredbe nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka ostvaruju pristup dostavljenim obavijestima ključnih i važnih subjekata sukladno smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

Članak 103.

(1) Podaci o pojedinom značajnom incidentu čuvaju se u nacionalnoj platformi 25 godina od dana dostave završnog izvješća o značajnom incidentu iz članka 70. ove Uredbe.

(2) Podaci o pojedinim ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima čuvaju se u nacionalnoj platformi 15 godina od dana dostave obavijesti iz članaka 87. do 89. ove Uredbe.

(3) Podaci o subjektima korisnicima nacionalne platforme, njihovim administratorima i korisnicima nacionalne platforme čuvaju se 15 godina od dana deaktivacije korisničkog računa subjekta sukladno članku 100. ove Uredbe, pod uvjetom da su u tom roku istekli rokovi čuvanja za sve značajne incidente o kojima je dotični subjekt obavijestio nadležni CSIRT.

(4) Nadležni CSIRT-ovi dužni su, prema podjeli nadležnosti iz Priloga III. Zakona, nakon isteka rokova čuvanja iz stavaka 1. i 2. ovoga članka, brisati u nacionalnoj platformi podatke o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima.

(5) CARNET je dužan nakon isteka roka čuvanja iz stavka 3. ovoga članka brisati u nacionalnoj platformi podatke o subjektima korisnicima nacionalne platforme, njihovim administratorima i korisnicima nacionalne platforme.

DIO ŠESTI
PROVEDBA OBAVJEŠTAVANJA O INCIDENTIMA I KIBERNETIČKIM PRIJETNJAMA KAO DOBROVOLJNI MEHANIZAM KIBERNETIČKE ZAŠTITE

Članak 104.

(1) Subjekti iz članka 47. stavka 1. ove Uredbe koji namjeravaju koristiti mogućnost obavještavanja o incidentima i kibernetičkim prijetnjama temeljem članka 50. stavka 2. Zakona, dužni su o takvoj namjeri obavijestiti nadležni CSIRT.

(2) U prilogu obavijesti iz stavka 1. ovoga članka, subjekt je dužan dostaviti izjavu o sukladnosti iz članka 35. stavka 3. Zakona, koja nije starija od godine dana od dana sastavljanja obavijesti iz stavka 1. ovoga članka.

Članak 105.

(1) Subjekti iz članka 47. stavka 1. ove Uredbe dužni su najmanje jednom u dvije godine provoditi samoprocjene kibernetičke sigurnosti sve dok koriste mogućnost obavještavanja o incidentima i kibernetičkim prijetnjama temeljem članka 50. stavka 2. Zakona, a sastavljene izjave o sukladnosti iz članka 35. stavka 3. Zakona dužni su dostaviti nadležnom CSIRT-u bez odgode, a najkasnije u roku od osam dana od dana njihova sastavljanja.

(2) Rok iz stavka 1. ovoga članka računa se od dana sastavljanja izjave o sukladnosti dostavljene nadležnom CSIRT-u sukladno članku 104. stavku 2. ove Uredbe odnosno od dana sastavljanja dostavljene izjave o sukladnosti iz članka 35. stavka 3. Zakona nadležnom CSIRT-u.

Članak 106.

Značajan incident u smislu članka 50. stavka 2. Zakona, o kojem subjekti iz članka 47. stavka 1. ove Uredbe dobrovoljno obavještavaju nadležni CSIRT, je svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 58. do 62. ove Uredbe, uzimajući u obzir kriterijske pragove, kada su propisani.

Članak 107.

(1) Na provedbu obavještavanja o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima temeljenog na članku 50. stavku 2. Zakona na odgovarajući način se primjenjuju članci 87. do 92. ove Uredbe.

(2) Subjekti iz članka 47. stavka 1. ove Uredbe dužni su obavijesti o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima dostavljati isključivo komunikacijskim kanalima definiranim u smjernicama nadležnih CSIRT-ova iz članka 90. stavka 1. ove Uredbe.

Članak 108.

Prilikom obrade obavijesti o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima zaprimljenih temeljem članaka 37., 39. i članka 50. stavka 2. Zakona, nadležni CSIRT daje prednost obradi obavijesti zaprimljenih temeljem članaka 37. i 39. Zakona.

DIO SEDMI
NACIONALNI SUSTAV ZA OTKRIVANJE KIBERNETIČKIH PRIJETNJI I ZAŠTITU KIBERNETIČKOG PROSTORA

Članak 109.

(1) Ključni subjekti, važni subjekti i drugi subjekti koji nisu kategorizirani kao ključni ili važni subjekti mogu dobrovoljno provesti mjeru kibernetičke zaštite pristupom nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora (u daljnjem tekstu: nacionalni sustav), ako je središnje državno tijelo za kibernetičku sigurnost procijenilo subjekta kritičnim u smislu članka 52. stavka 1. Zakona.

(2) U svrhu provedbe procjena kritičnosti subjekata u smislu članka 52. stavka 1. Zakona i odlučivanja o prioritetima u provedbi dobrovoljne mjere kibernetičke zaštite pristupa nacionalnom sustavu, središnje državno tijelo za kibernetičku sigurnost razvrstava subjekte prema kategorijama rizičnosti.

Članak 110.

(1) Procjena kritičnosti subjekta u smislu članka 52. stavka 1. Zakona provodi se na temelju zahtjeva za pristupanje nacionalnom sustavu kojeg podnosi subjekt, odnosno na temelju prijedloga za pristupanje nacionalnom sustavu kojeg podnosi tijelo državne

uprave ili regulatorno tijelo nadležno za sektor kojem pravna osoba pripada.

(2) Zahtjevi i prijedlozi za pristupanje nacionalnom sustavu moraju sadržavati podatke o:

– uslugama koje subjekt pruža ili djelatnostima koje subjekt obavlja u odnosu na druge pružatelje istih ili istovrsnih usluga i djelatnosti u Republici Hrvatskoj

– mrežnim i informacijskim sustavima kojima se subjekt koristi u pružanju usluga ili obavljanju djelatnosti te njihovoj izloženosti rizicima, opasnostima i prijetnjama u kibernetičkom prostoru

– načinu projektiranja, upravljanja i održavanja mrežnih i informacijskih sustava subjekta, kao i primijenjenim relevantnim europskim i međunarodnim normama i najboljim sigurnosnim praksama.

(3) Osim podataka iz stavka 2. ovoga članka, prijedlozi za pristupanje nacionalnom sustavu moraju sadržavati i očitovanje podnositelja prijedloga o razlozima zbog kojih se za subjekta predlaže provesti mjeru kibernetičke zaštite pristupanja nacionalnom sustavu.

(4) Zahtjevi i prijedlozi za pristupanje nacionalnom sustavu podnose se središnjem državnom tijelu za kibernetičku sigurnost prema uputama koje središnje državno tijelo za kibernetičku sigurnost objavljuje na svojim mrežnim stranicama.

(5) O podnesenom prijedlogu za pristupanje nacionalnom sustavu, podnositelj prijedloga je dužan obavijestiti i subjekta za kojeg je takav prijedlog podnio.

Članak 111.

(1) Središnje državno tijelo za kibernetičku sigurnost može, po potrebi, od subjekta za kojeg se provodi procjena u svrhu kritičnosti subjekta za pristupanje nacionalnom sustavu, zatražiti dostavljanje dodatnih podataka o mrežnim i informacijskim sustavima subjekta.

(2) Zatražene podatke subjekt dostavlja središnjem državnom tijelu za kibernetičku sigurnost sukladno uputama iz članka 110. stavka 4. ove Uredbe.

Članak 112.

(1) Iznimno od članka 109. ove Uredbe, ministarstva su dužna provesti mjeru kibernetičke zaštite obveznog pristupa nacionalnom sustavu.

(2) Iznimno od članka 109. ove Uredbe, druga tijela državne uprave, državna tijela i pravne osobe s javnim ovlastima su dužna provesti mjeru kibernetičke zaštite obveznog pristupa nacionalnom sustavu kada su ispunjeni sljedeći kriteriji:

– subjekt je kategoriziran kao ključan subjekt ili

– je središnje državno tijelo za kibernetičku sigurnost procijenilo subjekta kritičnim u smislu članka 52. stavka 1. Zakona.

(3) Procjena kritičnosti subjekata iz stavka 2. podstavka 2. ovoga članka provodi se u povodu prijedloga nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti za javni sektor.

(4) Središnje državno tijelo za kibernetičku sigurnost dužno je obavijestiti subjekta o ispunjavanju kriterija iz stavka 2. podstavka 2. ovoga članka i o obvezi pristupanja nacionalnom sustavu.

Članak 113.

(1) Neovisno o tome provodi li se kao obvezujuća ili dobrovoljna mjera kibernetičke zaštite, pristupanje nacionalnom sustavu provodi se na temelju sporazuma koji sklapaju središnje državno tijelo za kibernetičku sigurnost i subjekt koji pristupa nacionalnom sustavu.

(2) Sporazumom iz stavka 1. ovoga članka uređuju se:

– međusobna prava i obveze središnjeg državnog tijela i subjekta koji pristupa nacionalnom sustavu

– obostrani uvjeti zaštite podataka i povjerljivosti

– održavanje i zaštita programske opreme i alata nacionalnog sustava

– tehnički i drugi uvjeti za pristupanje i korištenje nacionalnog sustava.

(3) Sporazumi iz stavka 2. ovoga članka klasificiraju se odgovarajućim stupnjem tajnosti.

DIO OSMI
PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 114.

(1) Jedinstvena kontaktna točka donijet će smjernice iz članka 31. stavka 1. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(2) Središnje državno tijelo za kibernetičku sigurnost donijet će smjernice iz članka 40. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(3) Središnje državno tijelo za kibernetičku sigurnost donijet će smjernice iz članka 45. stavka 3. ove Uredbe u roku od šest mjeseci od dana stupanja na snagu ove Uredbe.

(4) Središnje državno tijelo za kibernetičku sigurnost izradit će korelacijski pregled mjera iz članka 49. ove Uredbe u roku od šest mjeseci od dana stupanja na snagu ove Uredbe.

(5) Središnje državno tijelo za kibernetičku sigurnost donijet će nacionalnu taksonomiju incidenata iz članka 77. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(6) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti donijet će smjernice iz članka 57. ove Uredbe u roku od šest mjeseci od dana stupanja na snagu ove Uredbe.

(7) Nadležni CSIRT-ovi donijet će smjernice iz članaka 72., 74. i 90. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(8) CARNET će donijeti smjernice iz članka 101. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

Članak 115.

Danom stupanja na snagu ove Uredbe prestaje važiti Odluka o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza, klasa: 022-03/21-04/91, urbroj: 50301-29/09-21-2, od 1. travnja 2021.

Članak 116.

Ova Uredba stupa na snagu osmoga dana od dana objave u »Narodnim novinama«, osim odredaba članaka 104. i 105. ove Uredbe koje stupaju na snagu 1. siječnja 2026.

Klasa: 022-03/24-03/108
Urbroj: 50301-29/23-24-5
Zagreb, 21. studenoga 2024.

Predsjednik
mr. sc. Andrej Plenković, v. r.

PRILOG I.

POPIS SEKTORA DJELATNOSTI[1]

A. POPIS ZA PRILOG I. ZAKONA – SEKTORI VISOKE KRITIČNOSTI

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	– elektroenergetski subjekti
		– operatori distribucijskog sustava
		– operatori prijenosnog sustava
		– proizvođači električne energije
		– nominirani operatori tržišta električne energije
		– sudionici na tržištu koji pružaju usluge agregiranja, upravljanja potrošnjom ili skladištenja energije
		– operatori mjesta za punjenje koji su odgovorni za upravljanje i rad mjesta za punjenje kojim se krajnjim korisnicima pruža usluga opskrbe, među ostalim u ime i za račun pružatelja usluga mobilnosti
	(b) centralizirano grijanje i hlađenje	– operator sustava centraliziranog grijanja ili centraliziranog hlađenja
	(c) nafta	– operatori naftovoda
		– operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		– središnja tijela za zalihe
	(d) plin	– opskrbljivači plinom, uključujući opskrbljivače u obvezi javne usluge
		– operatori distribucijskog sustava
		– operatori transportnog sustava
		– operatori sustava skladišta plina
		– operatori terminala za UPP
		– poduzeća za prirodni plin
		– operatori postrojenja za rafiniranje i obradu prirodnog plina
	(e) vodik	– operatori proizvodnje, skladištenja i prijenosa vodika
2. Promet	(a) zračni promet	– zračni prijevoznici
		– upravna tijela zračne luke, zračne luke, uključujući osnovne zračne luke te tijela koja upravljaju pomoćnim objektima u zračnim lukama
		– operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC)
	(b) željeznički promet	– upravitelji infrastrukture
		– željeznički prijevoznici, među ostalim i operatori uslužnih objekata
	(c) vodeni promet	– kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale, ne uključujući pojedinačna plovila kojima upravljaju te kompanije
		– upravljačka tijela luka, uključujući njihove luke, te subjekti koji upravljaju postrojenjima i opremom u lukama
		– služba za nadzor i upravljanje pomorskim prometom (VTS)
	(d) cestovni promet	– tijela nadležna za ceste, odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključan dio njihove opće djelatnosti
		– operatori inteligentnih prometnih sustava
3. Bankarstvo		– kreditne institucije
4. Infrastruktura financijskog tržišta		– operatori mjesta trgovanja
		– središnje druge ugovorne strane (CCP-i)
5. Zdravstvo		– pružatelji zdravstvene zaštite
		– referentni laboratoriji
		– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova
		– subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. (»Narodne novine«, br. 58/07. i 72/07.)
		– subjekti koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja (»popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja«)
6. Voda za ljudsku potrošnju		– dobavljači i distributeri vode namijenjene za ljudsku potrošnju, isključujući distributere kojima distribucija vode za ljudsku potrošnju nije ključan dio njihove općenite djelatnosti distribucije druge robe i proizvoda
7. Otpadne vode		– poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, sanitarne otpadne vode ili industrijske otpadne vode, isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključan dio njihove općenite djelatnosti
8. Digitalna infrastruktura		– pružatelji središta za razmjenu internetskog prometa

[1] Vrste subjekata označene * su subjekti koji su ujedno i obveznici dostave podataka o kategorizaciji subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata.

		– pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva*
		– registar naziva vršne nacionalne internetske domene*
		– pružatelji usluga računalstva u oblaku*
		– pružatelji usluga podatkovnog centra*
		– pružatelji mreže za isporuku sadržaja*
		– pružatelji usluga povjerenja
		– pružatelji javnih elektroničkih komunikacijskih mreža
		– pružatelji javno dostupnih elektroničkih komunikacijskih usluga
9. Upravljanje uslugama IKT-a (B2B)		– pružatelji upravljanih usluga*
		– pružatelji upravljanih sigurnosnih usluga*
		– informacijski posrednici kako su definirani propisom kojim se uređuje razmjena elektroničkog računa između poduzetnika
10. Javni sektor		– tijela državne uprave – druga državna tijela i pravne osobe s javnim ovlastima – privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu kojim se uređuje državna informacijska infrastruktura
		– jedinice lokalne i područne (regionalne) samouprave
11. Svemir		– operatori zemaljske infrastrukture koji su u vlasništvu, kojima upravljaju i koje vode države članice ili privatne strane te koji podupiru pružanje usluga u svemiru, isključujući pružatelje javnih elektroničkih komunikacijskih mreža

B. POPIS ZA PRILOG II. ZAKONA – DRUGI KRITIČNI SEKTORI

Sektor	Podsektor	Vrsta subjekta
1. Poštanske i kurirske usluge		– davatelji poštanskih usluga
		– pružatelji kurirskih usluga
2. Gospodarenje otpadom		– subjekti koji se bave gospodarenjem otpadom, isključujući subjekte kojima gospodarenje otpadom nije glavna gospodarska djelatnost
3. Izrada, proizvodnja i distribucija kemikalija		– subjekti koji se bave izradom tvari te distribucijom tvari ili mješavina
		– subjekti koji se bave proizvodnjom proizvoda iz tvari ili mješavina
4. Proizvodnja, prerada i distribucija hrane		– poduzeća za poslovanje s hranom, koja se bave veleprodajom te industrijskom proizvodnjom i preradom
5. Proizvodnja	(a) proizvodnja medicinskih proizvoda i *in vitro* dijagnostičkih medicinskih proizvoda	– subjekti koji proizvode medicinske proizvode i subjekti koji proizvode *in vitro* dijagnostičke medicinske proizvode, osim subjekata koji proizvode medicinske proizvode navedene u točki 5. petoj alineji Popisa za Prilog I. Zakona – Sektori visoke kritičnosti
	(b) proizvodnja računala te elektroničkih i optičkih proizvoda	– proizvođači računala te elektroničkih i optičkih proizvoda
	(c) proizvodnja električne opreme	– proizvođači elektroničke opreme
	(d) proizvodnja strojeva i uređaja, d. n.	– proizvođači strojeva i uređaja d.n.
	(e) proizvodnja motornih vozila, prikolica i poluprikolica	– proizvođači motornih vozila, prikolica i poluprikolica
	(f) proizvodnja ostalih prijevoznih sredstava	– proizvođači ostalih prijevoznih sredstava
6. Pružatelji digitalnih usluga		– pružatelji internetskih tržišta*
		– pružatelji internetskih tražilica*
		– pružatelji platformi za usluge društvenih mreža*
7. Istraživanje		– istraživačke organizacije
8. Sustav obrazovanja		– privatni i javni subjekti iz sustava obrazovanja

C. POPIS ZA SUBJEKTE KOJI NISU UVRŠTENI U PRILOGE ZAKONA

1. Kritični subjekti – subjekti koji su utvrđeni kao kritični subjekti na temelju zakona kojim se uređuje područje kritične infrastrukture.

2. Registrari[2] – subjekti koji pružaju usluge registracije naziva domena odnosno pravna ili fizička osoba koja obavlja samostalnu djelatnost ovlaštena za registraciju i administraciju .hr domena u ime registra naziva vršne nacionalne internetske domene.

[2] Uvršteni u Popis sektora djelatnosti isključivo kao obveznici dostave podataka za vođenje posebnog registra subjekata.

PRILOG II.

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima

Cilj: Cilj mjere je osigurati da osobe odgovorne za upravljanje mjerama iz članka 29. Zakona (u daljnjem tekstu: osobe odgovorne za upravljanje mjerama) prepoznaju kibernetičku sigurnost kao ključni aspekt poslovanja subjekta i aktivno sudjeluju u upravljanju kibernetičkom sigurnošću i poboljšanju razine kibernetičke sigurnosti u subjektu kroz integraciju kibernetičke sigurnosti u strateške planove i odluke o poslovanju subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

1.1. definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu. Subjekt je dužan najmanje jednom godišnje provoditi provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenjivati njihovu djelotvornost te prema potrebi ažurirati strateški akt kibernetičke sigurnosne politike

1.2. osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, s glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose

1.3. osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima. U svrhu osiguranja kontinuiteta u provedbi odgovarajućih mjera upravljanja kibernetičkim sigurnosnim rizicima i održavanja visoke razine njihove djelotvornosti, subjekt će potrebne resurse najmanje jednom godišnje procjenjivati i po potrebi prilagođavati

1.4. uspostaviti, dokumentirati i održavati aktivnim uloge i odgovornosti za kibernetičku sigurnost sukladno veličini subjekta i njegovoga mrežnog i informacijskog sustava te prema potrebi provesti ažuriranje uspostavljenih uloga i odgovornosti u subjektu. S obzirom na veličinu subjekta, uloge u pitanjima kibernetičke sigurnosti mogu biti dodijeljene osobama unutar subjekta s dediciranim ulogama isključivo u pitanjima kibernetičke sigurnosti (posebne uloge) ili ih se može dodijeliti zaposlenicima u okviru njihovih postojećih uloga u subjektu

1.5. potrebno je razdvojiti pojedine uloge u pitanjima kibernetičke sigurnosti koje bi mogle rezultirati potencijalnim sukobom interesa (primjerice razdvojiti uloge za provedbu procjena rizika i uloge za provedbu mjera)

1.6. imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost i kojoj je osiguran adekvatan pristup osobama odgovornim za provedbu mjera u subjektu

1.7. osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti

1.8. definirati i osigurati sigurnosne metrike o stanju kibernetičke sigurnosti, potrebne za izvještavanje osoba odgovornih za provedbu mjera u subjektu, tj. definirati ključne sigurnosne metrike koje će omogućiti precizno praćenje stanja kibernetičke sigurnosti. Ove metrike trebaju uključivati pokazatelje koji podrazumijevaju praćenje i prikupljanje podataka poput broja i vrste incidenata, vremena reakcije, te postotka usklađenosti s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima. Redovito prikupljanje i analiza ovih podataka treba osigurati kvalitetno izvještavanje osoba odgovornih za provedbu mjera

1.9. osigurati odgovarajuće aktivnosti nužne za podizanje svijesti osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja. Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti

1.10. osigurati adekvatne mehanizme sudjelovanja osoba odgovornih za provedbu mjera u inicijativama kibernetičke sigurnosti i promociji kontinuiranog unaprjeđenja kibernetičke sigurnosti. Ovi mehanizmi uključuju redovite sastanke, radne skupine i odbore posvećene pitanjima kibernetičke sigurnosti, te transparentan protok informacija između operativnog tima za kibernetičku sigurnost i upravljačkog tijela subjekta. Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati uključenost osoba odgovornih za provedbu mjera u donošenje odluka i utvrđivanje prioriteta u području kibernetičke sigurnosti

1.11. osigurati adekvatne mehanizme praćenja glavnih indikatora stanja kibernetičke sigurnosti u praktički stvarnom vremenu. Ovi mehanizmi uključuju implementaciju naprednih sustava za nadzor, automatske alarme i nadzorne ploče (*dashboarde*), koji omogućavaju kontinuirano praćenje i brzu detekciju potencijalnih kibernetičkih prijetnji. Na taj način se omogućava pravovremena reakcija na incidente i minimiziranje potencijalnih utjecaja incidenata.

Mjere 1.1 do 1.11. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere										
	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11
osnovna	A	A	A	A	C	C	A	C	C	C	C
srednja	A	A	A	A	A	A	A	A	A	C	C
napredna	A	A	A	A	A	A	A	A	A	A	C

2. Upravljanje programskom i sklopovskom imovinom

Cilj: Cilj mjere je uspostaviti strukturirani pristup identifikaciji i klasifikaciji programske i sklopovske imovine subjekta te uspostaviti potpunu kontrolu i zaštitu programske i sklopovske imovine subjekta prilikom njezina korištenja, skladištenja, prijevoza i u konačnici brisanja ili uništavanja, odnosno upravljanja životnim ciklusom programske i sklopovske imovine.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

2.1. aktom koji usvajaju osobe odgovorne za upravljanje mjerama potrebno je definirati pravila i odgovornosti za upravljanje programskom i sklopovskom imovinom i utvrditi kriterije za uspostavu »inventara kritične programske i sklopovske imovine« (u daljnjem tekstu: inventar kritične imovine). Ovo uključuje izradu i dokumentiranje detalja kao što su: tko je odgovoran za različite aspekte upravljanja imovinom, kako se imovina treba klasificirati na kritičnu i ostalu imovinu, odnosno na više grupa ili kategorija u smislu njene kritičnosti za poslovanje subjekta, te postupke koji se provode za redovito praćenje i održavanje imovine. Subjekt može definirati nekoliko jasno prepoznatljivih grupa ili kategorija imovine sukladno njihovoj kritičnosti (primjerice »infrastruktura«, »poslovne aplikacije«, »aplikacije za podršku«, »testni sustavi« ili »javno dostupni servisi«, »interni servisi« ili »produkcija«, »test«, »razvoj« ili kombinacija sličnih kategorija). Potom subjekt mora ovim aktom odrediti koje grupe ili kategorije predstavljaju kritičnu programsku i sklopovsku imovinu, pri čemu je moguće definirati samo kategoriju kritične programske i sklopovske imovine, koja tada obavezno uključuje: poslužitelje elektroničke pošte, VPN uređaje, sigurnosne uređaje, kao i drugu programsku i sklopovsku opremu prema procjeni kritičnosti koju provodi subjekt. Subjekt u okviru ovoga postupka mora definirati kriterije za uspostavu inventara kritične imovine (primjerice sva imovina označena kao »infrastruktura« ili kao »poslovne aplikacije«, odnosno u slučaju odabira istodobnog korištenja više kategorija, kritična imovina može biti definirana kao »svi javno dostupni servisi«, »kompletna infrastruktura« i »sve poslovne aplikacije na produkciji«). Klasifikacija programske i sklopovske imovine subjekta može se primjerice temeljiti na zahtjevima za dostupnost, autentičnost, cjelovitost i povjerljivost imovine, ali mora uzeti u obzir rizike kojima je imovina izložena i značaj imovine za poslovanje subjekta (kao u prethodnim primjerima), jer konačni cilj nije sama klasifikacija imovine već omogućavanje subjektu da primjeni drugačije mjere za različite kategorije imovine, sukladno različitom profilu rizika koji subjekt procjeni

2.2. izraditi detaljan inventar kritične imovine koji će sadržavati sve informacije nužne za učinkovito upravljanje i osigurati njegovo ažuriranje sve do razine koja omogućava učinkovito operativno upravljanje imovinom i provođenje adekvatnih mjera i kontrola. Detaljnost inventara kritične imovine mora biti na razini koja odgovara poslovnim potrebama subjekta, a inventar treba sadržavati najmanje sljedeće:

– popis mrežnih i informacijskih sustava koje subjekt koristi prilikom pružanja usluga ili obavljanja djelatnosti

– popis ključnih elemenata mrežnih i informacijskih sustava koji se procjenjuju kritičnim za održavanje kontinuiteta poslovanja subjekta

– jedinstveni identifikator svake pojedine imovine (primjerice inventurni broj, ime ili FQDN – Fully Qualified Domain Name)

– lokaciju imovine

– odgovornu osobu i organizacijsku jedinicu subjekta ili vanjskog davatelja usluge

2.3. utvrditi kritične podatke subjekta, vodeći računa o zahtjevima za dostupnost, autentičnost, cjelovitost i povjerljivost podataka i uzimajući u obzir rizike kojima su podaci izloženi, kao i značaj podataka za poslovanje subjekta. Subjekt može definirati nekoliko jasno prepoznatljivih grupa ili kategorija kritičnih podataka (primjerice svi podaci koji predstavljaju poslovnu tajnu, osobne podatke, klasificirane podatke ili druge podatke koje subjekt procjenjuje kritičnim po osnovi njihove važnosti za poslovanje subjekta)

2.4. definirati pravila korištenja prijenosnih medija za pohranu kritičnih podataka, s kojima trebaju biti upoznati svi zaposlenici, a tim pravilima potrebno je osigurati korištenje prijenosnih medija isključivo u poslovne svrhe, onemogućiti izvršenje programskog kôda s prijenosnih medija te osigurati automatsku provjeru postojanja malicioznih sadržaja na njima, a kada je potrebno i korištenje odgovarajuće enkripcije

2.5. utvrditi je li kritična programska i sklopovska imovina na korištenju isključivo u prostorima subjekta ili se koristi i izvan prostora subjekta, te definirati odgovornosti za čuvanje, korištenje i vraćanje iste, kada je na korištenju izvan prostora subjekta

2.6. proširiti inventar kritične imovine s programskom i sklopovskom imovinom manje kritičnosti, tj. s drugim grupama ili kategorijama imovine, za subjekte koji imovinu prema točki 2.1. klasificiraju na više grupa kritične programske i sklopovske imovine, a s ciljem povećanja obuhvata procjene rizika na imovinu koja može utjecati na zaštitu kritične imovine i omogućavanje proširenja primjene dodatnih mjera zaštite, ovisno o klasifikaciji kritičnosti imovine (primjerice proširiti kategorizaciju s »testnim sustavima«, s obzirom da su isti javno dostupni trećim stranama koji sudjeluju u njihovom razvoju)

2.7. uspostaviti provedbu redovnih aktivnosti za pravovremenu nadopunu i ažuriranje inventara kritične imovine na način da: a) ažuriranje inventara kritične imovine predstavlja sastavni dio procesa nabave nove programske i sklopovske imovine, uključujući nabavu radi zamjene ranije nabavljene imovine ili b) uvede adekvatnu automatizaciju na način da nije moguće uvesti promjene programske i sklopovske imovine a da se inventar kritične imovine ne ažurira

2.8. implementirati detaljne procedure i adekvatne tehničke mjere za sigurno zbrinjavanje, sigurni prijevoz imovine koja sadržava kritične podatke, pritom koristeći opće poznate i provjerene metode za sigurno zbrinjavanje ili brisanje podataka s uređaja i medija za pohranu podataka te osigurati mjere zaštite uređaja i medija za pohranu podataka u slučaju prijevoza. Jednokratni prijevoz opreme ili medija može se zaštititi kompenzacijskim mjerama kao što je pohrana u sigurne spremnike, izvanredni nadzor prijevoza ili slično, dok oprema namijenjena za učestali prijevoz ili mobilni uređaji bilo kojeg tipa, moraju posjedovati i koristiti ugrađene i neodvojive mehanizme zaštite kao što je kriptiranje medija za pohranu. Ukoliko opisane tehničke mjere nije moguće primijeniti, programska i sklopovska imovina ili podaci smiju biti izneseni izvan prostorija subjekta samo nakon odgovarajućeg odobrenja osoba odgovornih za upravljanje mjerama

2.9. implementirati mehanizme za fizičku identifikaciju i označavanje fizičke imovine za obradu podataka ovisno o količini i rasprostranjenosti iste, što može uključivati i praćenje i nadzor imovine u stvarnom vremenu koristeći automatizaciju pomoću Internet stvari (*Internet of Things – IoT*) i radio frekvencijske identifikacije (*Radio Frequency Identification – RFID*).

Mjere 2.1. do 2.9. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere								
	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.
osnovna	A	A	A	A	A	C	C	C	C
srednja	A	A	A	A	A	A	A	C	C
napredna	A	A	A	A	A	A	A	A	A

3. Upravljanje rizicima

Cilj: Cilj mjere je uspostaviti odgovarajući organizacijski okvir za upravljanje rizikom kako bi subjekt utvrdio i odgovorio na sve rizike koji prijete sigurnosti njegovih mrežnih i informacijskih sustava i pri tome predstavljaju rizik za poslovanje subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

3.1. razviti, dokumentirati, implementirati i na godišnjoj osnovi ažurirati proces upravljanja rizicima koji uključuje procjenu rizika (identifikacija, analiza, evaluacija), određivanje razine i kritičnosti rizika, načine obrade rizika, identifikaciju vlasnika rizika i njihovo područje odgovornosti. Subjekt mora dokumentirati, komunicirati i zaposlenicima subjekta, koji su odgovorni za segmente poslovanja subjekta povezane s rizicima, učiniti dostupnim kibernetičke sigurnosne politike i upute o osnovnim procedurama za identifikaciju, analizu, procjenu i obradu rizika, poglavito za pojedine rizike koji mogu dovesti do poremećaja u dostupnosti, cjelovitosti, autentičnosti i povjerljivosti mrežnih i informacijskih sustava subjekta

3.2. provesti procjenu rizika nad imovinom iz inventara kritične imovine zasnovanom na načelu procjene svih vrsta rizika (*all-hazards approach)* te na određivanju razine svakog pojedinog rizika. S obzirom da kibernetičke prijetnje mogu imati različito podrijetlo, procjena rizika se treba temeljiti na pristupu koji uključuje sve opasnosti po programsku i sklopovsku imovinu što uključuje i fizičke prijetnje kao što su krađe, požari, poplava, prirodni fenomeni, kvarovi, ispad elektroničke komunikacijske infrastrukture, nestanak struje ili neovlašteni fizički pristup i oštećenje imovine, ali uključuje i sve prijetnje koje bi mogle ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga. Posebnu pozornost potrebno je pridati rizicima koji proizlaze iz korištenja usluga trećih strana. Moguće je koristiti pristup procjeni rizika temeljen na opisanom pristupu prepoznavanja operativnih rizika za imovinu iz inventara subjekta (*Asset-based approach*), kao i pristup temeljen na scenarijima i prepoznavanju izvora strateških rizika za poslovanje subjekta (*Event-based approach*)

3.3. identificirane rizike potrebno je dokumentirati te definirati odgovor na tako utvrđene rizike, razmjerno njihovoj razini i kritičnosti, što uključuje poduzimanje odgovarajućih i razmjernih tehničkih, operativnih i organizacijskih mjera upravljanja rizicima. Subjekti bi trebali u okviru svoje procjene rizika poduzeti i prioritizirati mjere upravljanja kibernetičkim sigurnosnim rizicima razmjerne stupnju izloženosti svog poslovanja rizicima i vjerojatnosti nastanka incidenata te njihovoj ozbiljnosti za poslovanje subjekta, uključujući mogući društveni i gospodarski, odnosno međusektorski ili prekogranični utjecaj ovih rizika

3.4. implementirati detaljne metode za analizu i procjenu rizika te izvještavanje o tim rizicima. Subjekt mora osigurati redovito izvještavanje o identificiranim rizicima, uključujući sve promjene u procjenama rizika i predloženim mjerama za njihovo ublažavanje ili eliminaciju. Izvještaji moraju biti dostavljeni relevantnim poslovnim segmentima unutar subjekta, kako bi se omogućilo donošenje informiranih odluka o mjerama upravljanja kibernetičkim sigurnosnim rizicima koje se poduzimaju i potrebi ažuriranja strateških dokumenata subjekta u pitanjima kibernetičke sigurnosti

3.5. održavati registar identificiranih rizika. Ovaj registar treba sadržavati detaljne informacije o svim prepoznatim rizicima, uključujući opis rizika, procjenu vjerojatnosti i potencijalnog utjecaja rizika, te trenutni status i poduzete mjere obrade rizika. Registar mora biti redovito ažuriran kako bi odražavao prepoznate nove rizike i promjene u postojećim rizicima. Također, subjekt mora osigurati da su svi relevantni poslovni segmenti unutar subjekta informirani o sadržaju i promjenama u registru identificiranih rizika, kako bi se omogućilo učinkovito upravljanje rizicima i donošenje informiranih odluka o potrebnim mjerama upravljanja kibernetičkim sigurnosnim rizicima

3.6. osigurati provedbu procjene rizika prilikom implementacije rješenja koja povećavaju površinu izloženosti mrežnog i informacijskog sustava subjekta kibernetičkom napadu, proširuju rizike ili uvode u korištenje u subjektu do sada nepoznate arhitekture mrežnih i informacijskih sustava ili mjera zaštite. Ova procjena treba uključivati identifikaciju novih prijetnji i ranjivosti koje proizlaze iz implementacije novih tehnologija ili rješenja, te analizu njihovoga potencijalnog utjecaja na cjelokupnu kibernetičku sigurnost subjekta. Na temelju rezultata procjene, subjekt mora poduzeti odgovarajuće mjere za ublažavanje identificiranih rizika prije implementacije uvodno opisanih rješenja. Sve aktivnosti i rezultati vezani uz procjenu rizika moraju biti dokumentirani i pregledani od strane relevantnih osoba zaduženih za pitanja sigurnosti subjekta

3.7. koristiti napredne softverske alate za procjenu i praćenje rizika. Ovi alati trebaju omogućiti detaljnu analizu i procjenu kibernetičkih prijetnji, identifikaciju ranjivosti, te praćenje incidenata u stvarnom vremenu. Softverski alati moraju biti sposobni za automatizirano prikupljanje i analizu relevantnih podataka, generiranje izvještaja i pružanje preporuka za ublažavanje ili eliminaciju rizika. Subjekt mora osigurati redovitu upotrebu i ažuriranje ovih alata kako bi se osigurala njihova učinkovitost u prepoznavanju i upravljanju rizicima. Rezultati dobiveni korištenjem ovih alata moraju biti integrirani u sveukupni proces upravljanja rizicima unutar subjekta

3.8. upravljanje rizicima integrirati kao dio upravljanja rizicima na razini poslovanja subjekta (ERM).

UVJET: Mjera 3.8. je obvezujuća za subjekt koji ima uspostavljene procese upravljanja rizicima na razini poslovanja subjekta te se u tom slučaju upravljanje rizikom, opisano u okviru podskupova mjere 3. (3.1. do. 3.7.), provodi integrirano, kao dio uspostavljenog procesa upravljanja rizicima poslovanja subjekta. Ako subjekt nema uspostavljene procedure upravljanja rizicima na razini poslovanja subjekta, uspostavlja mjeru 3. (3.1. do 3.7.) kao novi poslovni proces.

Mjere 3.1. do 3.8. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere							
	3.1.	3.2.	3.3.	3.4.	3.5.	3.6.	3.7.	3.8.
osnovna	A	A	A	A	A	C	C	B
srednja	A	A	A	A	A	A	C	B
napredna	A	A	A	A	A	A	C	B

4. Sigurnost ljudskih potencijala i digitalnih identiteta

Cilj: Cilj mjere je uspostaviti strukturirani pristup koji omogućuje subjektu učinkovito upravljanje zapošljavanjem odgovarajućeg ljudskog potencijala te upravljanje pravima pristupa zaposlenika i vanjskog osoblja mrežnim i informacijskim sustavima subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

4.1. razviti, dokumentirati, implementirati i redovno održavati pravila sigurnosti ljudskih potencijala uzimajući u obzir sve korisnike mrežnih i informacijskih sustava, uključujući vanjske suradnike. Odgovornosti vezane za kibernetičku sigurnost utvrđuju se ovisno o dodijeljenim ulogama korisnika sustava, utvrđenim prema poslovnim potrebama subjekta. Subjekti moraju osigurati da:

– svi zaposlenici subjekta razumiju svoje odgovornosti u pitanjima kibernetičke sigurnosti i da primjenjuju osnovne prakse kibernetičke higijene

– sve osobe s administrativnim ili povlaštenim pristupom mrežnom i informacijskom sustavu subjekta su svjesne povećane odgovornosti te predano izvršavaju svoje uloge i ovlasti dodijeljene prema kibernetičkoj sigurnosnoj politici subjekta

– osobe odgovorne za upravljanje mjerama u subjektu razumiju svoju ulogu, odgovornosti i ovlasti

4.2. provjeravati adekvatnost i kvalifikacije kandidata prije njihova zapošljavanja sukladno značaju radnog mjesta na koje se osoba zapošljava i primjenjivim propisima (primjerice provjera referenci, provjera valjanosti posjedujućih certifikata, svjedodžbi i diploma, pismeni testovi, potvrde o nekažnjavanju itd.). Potrebno je utvrditi za koje uloge, odgovornosti i ovlasti u subjektu je potrebno provjeravati adekvatnost i kvalifikacije kandidata prije zapošljavanja, odnosno zahtijevati primjerice periodičnu dostavu potvrde o nekažnjavanju. Provjera kandidata mora se provesti u skladu s važećim zakonima, propisima i etikom i mora biti razmjerna poslovnim zahtjevima, usklađena sa zahtjevima pristupa pojedinim vrstama podataka i prepoznatim rizicima

4.3. za sve zaposlenike čija redovna radna zaduženja uključuju projektiranje, provođenje, nadzor ili revidiranje mjera upravljanja kibernetičkih sigurnosnih rizika, osigurati specifično i dokumentirano osposobljavanje i to neposredno nakon stupanja osobe u radni odnos, kao i kontinuirano osposobljavanje svih takvih postojećih zaposlenika tijekom radnog odnosa, radi osiguravanja adekvatnog stupnja znanja o novim tehnologijama i kibernetičkim prijetnjama. Subjekt mora uspostaviti program osposobljavanja u skladu s kibernetičkom sigurnosnom politikom subjekta, tematski specifičnim politikama i relevantnim procedurama kibernetičke sigurnosti u okviru mrežnog i informacijskog sustava subjekta. Osposobljavanje mora obuhvatiti potrebne vještine, stručnosti i znanja za određena radna mjesta te kriterije prema kojima se utvrđuje potrebno osposobljavanje za pojedine uloge (primjerice IT administratori moraju proći dodatno osposobljavanje za sigurne konfiguracije programske i sklopovske imovine subjekta). Program osposobljavanja treba sadržavati poglavlja kao što su:

– uobičajene i dokumentirane upute koje se odnose na sigurnu konfiguraciju i rukovanje mrežnim i informacijskim sustavima subjekta, uključujući i mobilne uređaje

– uobičajeno i dokumentirano informiranje o poznatim kibernetičkim prijetnjama

– uobičajeno i dokumentirano postupanje prilikom incidenta

4.4. osigurati redovnu obuku o osnovnim praksama kibernetičke higijene i podizanje svijesti o rizicima i kibernetičkim prijetnjama za sve zaposlenike, neposredno nakon stupanja osobe u radni odnos u subjektu te kasnije redovito tijekom radnog odnosa. Subjekt mora uspostaviti program podizanja svijesti u skladu s kibernetičkom sigurnosnom politikom, tematski specifičnim politikama i relevantnim procedurama kibernetičke sigurnosti u okviru mrežnog i informacijskog sustava subjekta. Podizanje svijesti mora obuhvatiti osnovne IT vještine i znanja (primjerice svi zaposlenici moraju proći osposobljavanje za sigurno korištenje e-pošte i pretraživanje Interneta). Program podizanja svijesti treba sadržavati poglavlja kao što su:

– uobičajene i dokumentirane upute koje se odnose na sigurnost IT sustava i osobne IT imovine što uključuje i mobilne uređaje

– sigurno korištenje autentifikacijskih sredstava i vjerodajnica (primjerice izbjegavanje korištenja istih lozinki na različitim javnim servisima te izbjegavanje korištenja službenih adresa na javnim servisima radi smanjivanja rizika od napada, izbjegavanje spremanja lozinki u web preglednike itd.)

– prepoznavanje i prijavu najčešćih incidenata

4.5. definirati adekvatne disciplinske mjere za zaposlenike u slučaju nepridržavanja relevantnih pravila kibernetičke sigurnosti ovisno o radnom mjestu zaposlenika, a sve sukladno primjenjivom zakonskom okviru. Prilikom utvrđivanja povreda radnih obveza i određivanja disciplinskih mjera zbog kršenja kibernetičkih sigurnosnih politika subjekta uzimaju se u obzir svi primjenjivi propisi, kao i posebni ugovorni ili drugi poslovni zahtjevi

4.6. osigurati da svaki korisnik mrežnog i informacijskog sustava (neovisno o tome je li ili nije zaposlenik subjekta), gdje god je to tehnički moguće i sustav dozvoljava, posjeduje jedan ili više digitalnih identiteta koji su samo njegovi te ih koristi tijekom rada na mrežnim i informacijskim sustavima subjekta. Ukoliko sustav ne omogućava stvaranje adekvatnog broja digitalnih identiteta ili je to neopravdano skupo, neki korisnici mogu koristiti iste digitalne identitete isključivo ukoliko subjekt osigura kompenzacijsku mjeru koja osigurava nedvosmislenu i dokazivu evidenciju korištenja dijeljenih digitalnih identiteta (primjerice grupno korištenje institucionalne email adrese). Subjekt mora:

– kreirati jedinstvene digitalne identitete za korisnike i mrežne i informacijske sustave

– za korisnike se mora povezati digitalni identitet s jedinstvenom osobom kako bi se osoba mogla držati odgovornom za aktivnosti provedene s tim specifičnim identitetom

– omogućiti nadzor sustava digitalnih identiteta

– voditi evidencije digitalnih identiteta i osigurati praćenje i dokumentiranje svih promjena

– digitalni identiteti koji su dodijeljeni većem broju osoba (primjerice grupni računi e-pošte) mogu biti dopušteni jedino kada je to nužno zbog poslovnih ili operativnih razloga, te se oni moraju posebno odobriti i dokumentirati, uz uspostavu kompenzacijske mjere evidentiranja zapisa koja osigurava podatke o svakom pojedinom korisniku i vremenu korištenja takvog digitalnog identiteta

4.7. odgovornosti za kibernetičku sigurnost definirati prema jasnim radnim ulogama zaposlenika i uz osiguravanje zamjenskih osoba za svaku ulogu. Prava pristupa zaposlenika mrežnim i informacijskim sustavima subjekta potrebno je implementirati sukladno dodijeljenim poslovnim zaduženjima i uz primjenu načela »po-

slovne potrebe« (*need-to-know)*, »minimalno potrebnih ovlaštenja za provedbu zadaća« (*least privilege)* te »razdvajanja nadležnosti« (*segregation of duties*)

4.8. osigurati provedbu jasnog i učinkovitog procesa koji će osigurati da se digitalni identiteti svih korisnika mrežnog i informacijskog sustava pravovremeno dodijele te pravovremeno promijene ili ukinu uslijed organizacijskih ili poslovnih promjena. Ovaj proces mora osigurati pravovremenu dodjelu digitalnih identiteta novim korisnicima i njihovo brzo ukidanje kada više nisu potrebni. Prava pristupa moraju se evidentirati te redovito revidirati i prilagođavati u skladu s organizacijskim ili poslovnim promjenama, čime se minimizira rizik od neovlaštenog pristupa i štite kritični podaci subjekta

4.9. razviti i provoditi obuku za odgovor na incidente u subjektu za ključne osobe koje sudjeluju u tom procesu. Obuka mora uključivati praktične scenarije i redovite vježbe kako bi se osiguralo da su svi sudionici dobro pripremljeni za učinkovito reagiranje na incidente. Redovitim ažuriranjem obuke, subjekt je dužan prilagoditi obuku novim prijetnjama i najboljim praksama u području kibernetičke sigurnosti. Time se povećava otpornost subjekta na incidente i osigurava brza i adekvatna reakcija u slučaju njihovoga pojavljivanja

4.10. koristiti sustave za udaljeno digitalno učenje za kontinuiranu obuku i certifikacije svojeg osoblja u području kibernetičke sigurnosti, osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja. Subjekt se može odlučiti za udaljeno digitalno učenje i zbog jednostavnosti provedbe obuke neovisno o tome je li mu moguće organizirati i obuku u živo

4.11. implementirati testiranje socijalnog inženjeringa, simulacije krađe identiteta (*phishing*) i programe podizanja svijesti. Ove aktivnosti moraju biti redovite i obuhvatiti sve zaposlenike subjekta kako bi se identificirale ranjivosti i educiralo osoblje o prepoznavanju i odgovoru na takve ranjivosti. Programi podizanja svijesti trebaju uključivati edukativne materijale, radionice i praktične vježbe. Time se jača sigurnosna kultura unutar subjekta i smanjuje rizik od uspješnih napada socijalnog inženjeringa

4.12. integrirati sustav za vođenje evidencije i upravljanje ljudskim potencijalima sa sustavima za upravljanje digitalnim identitetom i pravima pristupa mrežnom i informacijskom sustavu, kako bi se osiguralo učinkovito upravljanje digitalnim identitetima i pravima pristupa u stvarnom vremenu. Subjekt je dužan:

– dodjeljivati i ukidati prava pristupa na temelju načela »poslovne potrebe« (*need-to-know*), načela »najmanje privilegije« (*least privilege*) i sukladno potrebi načela »razdvajanja nadležnosti« (*segregation of duties*)

– osigurati da prava pristupa budu revidirana u slučaju prekida ili druge promjene statusa zaposlenja (primjerice ukidanje ili promjena prava pristupa, deaktivacija korisničkih računa itd.)

– osigurati da se prava pristupa odgovarajuće dodjeljuju trećim stranama, poput izravnih dobavljača ili pružatelja usluga, vodeći računa o primjeni načela iz alineje 1. ovoga podskupa mjera. Posebno je važno ograničiti takva prava pristupa, kako po opsegu tako i po trajanju.

– voditi registar dodijeljenih prava pristupa po korisnicima i

– koristiti evidentiranje pristupa pri upravljanju pravima pristupa na mrežnom i informacijskom sustavu.

Mjere od 4.1.do 4.12. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere											
	4.1.	4.2.	4.3.	4.4.	4.5.	4.6.	4.7.	4.8.	4.9.	4.10.	4.11.	4.12.
osnovna	A	A	A	A	A	A	A	A	C	C	C	C
srednja	A	A	A	A	A	A	A	A	A	A	C	C
napredna	A	A	A	A	A	A	A	A	A	A	C	A

5. Osnovne prakse kibernetičke higijene

Cilj: Cilj mjere je za sve zaposlenike i mrežne i informacijske sustave subjekta osigurati implementaciju temeljnih sigurnosnih postavki, pravila i procedura koje osiguravaju zaštitu mrežnih i informacijskih sustava subjekta i njegovih podataka, pri čemu je fokus na sprječavanju najčešćih vrsta incidenata koji nastaju kao posljedica maliciozne infekcije sustava, *phishing* napada, nepropisne i nepravilne konfiguracija sustava ili upotrebe slabih lozinki.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

5.1. razviti, dokumentirati, održavati i implementirati pravila osnovne prakse kibernetičke higijene te redovito educirati sve korisnike svojih mrežnih i informacijskih sustava o tim pravilima

5.2. osigurati da se na svim mrežnim i informacijskim sustavima za pristup kojima se koriste lozinke, kao sredstvo autentifikacije koriste politike »najjačih mogućih lozinki« ili ukoliko zbog operativnih razloga to nije moguće, subjekt će definirati i obrazložiti svoju politiku korištenja lozinki koja mora biti u skladu s trenutnim dobrim praksama, kao što je primjerice »*Password Policy Guide of Center for Internet Security (CIS)*«. Ukoliko je subjekt odlučio implementirati svoju politiku korištenja lozinki ona treba uključivati različite smjernice za različite mrežne i informacijske sustave i namjene korištenja lozinki, s obzirom da razina potrebne zaštite često nije ista na svim vrstama mrežnih i informacijskih sustava (primjerice na novijim Windows Server sustavima korištenje lozinke dulje od 14 znakova onemogućava korištenje zastarjele LAN Manager autentifikacije). Općenito na svim mrežnim i informacijskim sustavima koji nemaju mogućnost više-faktorske autentifikacije (MFA) ili za korisničke račune na kojima MFA nije tehnički moguć, minimalna duljina je 14 znakova koji moraju predstavljati kombinaciju velikih i malih slova, znamenki te specijalnih znakova. Lozinka za korisničke račune s privilegiranim pravima pristupa mrežnom i informacijskom sustavu treba biti duga najmanje 16 znakova, a lozinke za servisne račune najmanje 24 znaka, koristeći ranije opisano pravilo o kombinaciji velikih i malih slova, znamenki i specijalnih znakova. Za korisničke račune, uključujući one s privilegiranim pravima pristupa i servisne račune, za koje je uključena provjera drugog faktora, duljina lozinke može biti kraća, ali ne kraća od 8 znakova, ukoliko je to tehnički izvedivo, vodeći pri tome računa o potrebi korištenja ranije opisanog pravila o kombinaciji velikih i malih slova, znamenki i specijalnih znakova. U slučaju da mrežni i informacijski sustav ne može podržati primjenu opisanih pravila određivanja lozinki, subjekt je dužan osigurati druge kompenzacijske mjere za-

štite, odnosno ograničavanje pristupa mrežnom i informacijskom sustavu temeljem odgovarajuće kompenzacijske mjere (primjerice obavezno ograničenje fizičkog pristupa ili obavezni udaljeni pristup koji je zaštićen s dva autentifikacijska faktora). Ukoliko se subjekt odlučio za autentifikaciju koja ne uključuje korištenje lozinki, nužno je korištenje dva faktora (biometrija i posjedovanje drugog autentifikacijskog uređaja ili upravljanog pristupnog uređaja). U okviru ovoga podskupa mjere subjekt je dužan:

– osigurati da je snaga provjere autentičnosti prikladna kritičnosti mrežnog i informacijskog sustava te u sladu s procjenom rizika

– provoditi korištenje metoda autentifikacije (lozinke, digitalni certifikati, pametne kartice, biometrija i sl.) koje su u skladu sa stanjem razvoja tehnologije i koristiti jedinstvena autentifikacijska sredstva (nešto što korisnik zna kao lozinka ili pin, nešto što korisnik posjeduje kao pametni telefon ili token, te nešto što korisnik jeste kao otisak prsta, prepoznavanje lica i sl.)

– osigurati sigurnu dodjelu i korištenje autentifikacijskih sredstava (primjerice pohranjivanje i prijenos takvih sredstava u zaštićenom obliku, automatsko generiranje, izrada kriptografskih sažetaka uz »soljenje« i/ili »paprenje« itd.), što uključuje i savjetovanje osoblja o prikladnom postupanju

– zahtijevati inicijalnu promjenu osobnih pristupnih podataka (lozinke i PIN) prilikom prvog korištenja korisničkog računa, kao i u slučaju postojanja sumnje da su osobni pristupni podaci kompromitirani

– ukoliko je tehnički izvedivo, potrebno je zabraniti spremanje lozinki u web-preglednike

– osigurati zaključavanje korisničkih računa nakon prekomjernih neuspjelih pokušaja prijave (*account lockout*), uz mogućnost automatskog otključavanja nakon razumnog vremenskog perioda radi sprječavanja napada uskraćivanjem usluge

– ugasiti neaktivne korisničke sjednice nakon unaprijed određenog perioda neaktivnosti gdje to poslovni proces dopušta i

– zahtijevati posebne vjerodajnice za pristup privilegiranim ili administratorskim korisničkim računima

5.3. uz provedbu politike korištenja lozinki, implementirati višefaktorsku autentifikaciju (MFA) za kritične mrežne i informacijske sustave koji su više izloženi potencijalnim kibernetičkim napadima. Primjena MFA je potrebna na VPN pristupu, SaaS alatima dostupnim s Interneta itd. Potrebno je osigurati da se korisnička imena i lozinke korištene na servisima s dvofaktorskom autentifikacijom ne koriste na drugim servisima bez dvofaktorske autentifikacije. Snaga provjere autentičnosti mora biti usklađena s procjenom rizika i izloženosti mrežnog i informacijskog sustava. Potrebno je uzeti u obzir višefaktorsku provjeru autentičnosti prilikom pristupanja kritičnim mrežnim i informacijskim sustavima s udaljene lokacije, sustavima za administriranje korisnika i mrežnih i informacijskih sustava, kritičnim podacima subjekta itd. Višefaktorska provjera autentičnosti se može kombinirati s drugim tehnikama kako bi se zahtijevali dodatni faktori u specifičnim okolnostima, temeljeno na unaprijed definiranim pravilima i obrascima, poput pristupa s neuobičajene lokacije, s neuobičajenog uređaja ili u neuobičajeno vrijeme

5.4. osigurati korištenje osnovnog antivirusnog alata na svim radnim stanicama. Samo korištenje programskih antivirusnog alata za detekciju zlonamjernog softvera i oporavak često nije dovoljno pa je, sukladno procjeni rizika koju provodi subjekt, potrebno primijeniti i dodatne mjere odnosno koristiti alate za otkrivanje i odgovor na kibernetičke prijetnje na krajnjim točkama (EPP/EDR), s prikladnom razinom automatskog odgovora na prijetnje, u svrhu napredne zaštite na svim radnim stanicama i poslužiteljima gdje je to tehnički izvedivo. Subjekt može, zbog tehničke složenosti ili vrlo visoke cijene implementacije, odlučiti mjeru primijeniti samo na odabranom i obrazloženom podskupu programske ili sklopovske imovine sukladno procjeni rizika, primjerice na poslužiteljskoj infrastrukturi, ali onda ista mora biti logički odvojena od nezaštićene programske i sklopovske imovine, kako kompromitacija nezaštićene programske i sklopovske imovine ne bi lako dovela do kompromitacije zaštićenog dijela programske i sklopovske imovine

5.5. osigurati pravovremenu i cjelovitu primjenu sigurnosnih zakrpa na kompletnoj programskoj i sklopovskoj imovini subjekta, čim iste bude primjenjive, ili je potrebno razraditi, definirati, dokumentirati i implementirati drugačiji proces upravljanja ranjivostima na korištenim mrežnim i informacijskim sustavima, koji će osigurati trijažu, procjenu te prioritiziranu i dokumentiranu postepenu primjenu sigurnosnih zakrpa. Ukoliko se subjekt odluči da neće odmah primjenjivati sve sigurnosne zakrpe već implementirati svoju politiku primjene sigurnosnih zakrpa, ista mora prilikom definiranja internog roka za primjenu sigurnosnih zakrpa uzeti u obzir faktore kritičnosti i izloženosti mrežnog i informacijskog sustava, ozbiljnost otkrivene ranjivosti tj. kritičnosti primjene sigurnosne zakrpe te opće stanje kibernetičke sigurnosti i eventualne aktualne kibernetičke napade koji iskorištavaju dotične ranjivosti. Pritom su subjekti dužni utvrditi i primijeniti postupke kojima će osigurati sljedeće:

– sigurnosne zakrpe na odgovarajući način se provjeravaju i testiraju prije nego što se primjene u produkcijskoj okolini

– sigurnosne zakrpe preuzimaju se iz pouzdanih izvora te se provjeravaju u smislu cjelovitosti

– sigurnosne zakrpe se ne primjenjuju ako uvode dodatne ranjivosti ili nestabilnosti koje su rizičnije od izvornog razloga za primjenu zakrpe

– dokumentiraju se razlozi za neprimjenjivanje raspoloživih sigurnosnih zakrpa

– u slučajevima kada sigurnosna zakrpa nije raspoloživa, provode se dodatne mjere upravljanja kibernetičkim sigurnosnim rizicima i prihvaćaju se preostali rizici

– upravljanje sigurnosnim zakrpama treba biti usklađeno s kontrolnim procedurama za upravljanje promjenama i održavanje mrežnih i informacijskih sustava

5.6. osigurati, ukoliko je tehnički izvedivo, stvaranje zapisa o svakoj prijavi i aktivnosti na kritičnom mrežnom i informacijskom sustavu radi osiguravanja forenzičkog traga, a pri tome treba koristiti alate i procese za praćenje i bilježenje aktivnosti na mrežnom i informacijskom sustavu subjekta u svrhu otkrivanja sumnjivih događaja koji bi mogli predstavljati incident te postupanja kojim će se umanjiti potencijalni učinak incidenta. Dnevničke zapise je potrebno čuvati pohranjene najmanje zadnjih 90 dana (ne nužno u sustavu koji ih je stvorio). Iznimno od toga, pojedine vrste dnevničkih zapisa dopušteno je čuvati i kraće, ako količina tih zapisa predstavlja ograničenje za pohranu i ako nije moguće filtrirati i/ili komprimirati te dnevničke zapise kako bi se zadržale ključne informacije, a smanjila količina zapisa. U okviru uređenja procesa bilježenja dnevničkih zapisa (opseg i period čuvanja), treba uzimati u obzir procjenu rizika kako bi se omogućila detekcija i istraga incidenata sukladno procijenjenim scenarijima rizika. Subjekt mora osigurati da svi sustavi imaju sinkronizirano vrijeme kako bi se moglo korelirati dnevničke zapise između različitih mrežnih i informacijskih sustava. Tijekom projektiranja mrežnog i informacijskog sustava minimalno treba uključiti sljedeće vrste dnevničkih zapisa:

– metapodatke odlaznog i dolaznog mrežnog prometa

– pristup mrežnim i informacijskim sustavima, aplikacijama, mrežnoj opremi i uređajima

– stvaranje, izmjenu i brisanje korisničkih računa i proširivanje prava

– izmjene na pričuvnim kopijama

– zapisi iz sigurnosnih alata, primjerice antivirusnog sustava, sustav za otkrivanje napada ili vatrozida

5.7. definirati i dokumentirati proces identifikacije i upravljanja ranjivostima na kritičnim mrežnim i informacijskim sustavima koje samostalno razvija. U tu svrhu, subjekt mora osigurati mehanizam identifikacije mogućih ranjivosti na mrežnim i informacijskim sustavima koje samostalno razvija. Sukladno vlastitoj procjeni rizika, mehanizmi mogu uključivati alate za statičku analizu kôda (SAST), alate za dinamičku analizu aplikacija (DAST), provjeru komponenti trećih strana (SCA), interne ili vanjske penetracijske testove, uključivanje u nagradne programe (*bug bounty*) ili slično. Preporuča se primjena načela pomaka sigurnosnih provjera »na lijevo« tj. na ranije faze softverskog razvoja. Ukoliko subjekt ne primjenjuje navedena načela pomaka sigurnosnih provjera »na lijevo«, onda je prije puštanja novoga ili promijenjenog mrežnog i informacijskog sustava u produkcijski rad potrebno provesti adekvatno sigurnosno testiranje

UVJET: Mjera 5.7. je obvezujuća ako subjekt koristi programska rješenja koja samostalno razvija.

5.8. implementirati mehanizme za periodičnu ili redovitu provjeru ranjivosti svih mrežnih i informacijskih sustava kako bi se pravovremeno otkrio manjak primjene sigurnosnih zakrpi ili nepravilna konfiguracija sustava. Subjekti su dužni, na temelju procjene rizika, utvrditi potrebu i učestalost te vrste sigurnosnog testiranja (penetracijski testovi, *red teaming*, *purple teaming*, i dr.) kako bi otkrili ranjivosti u implementaciji mrežnog i informacijskog sustava. Rezultati sigurnosnog testiranja i provjere ranjivosti trebaju se prioritizirati, koristiti za unaprjeđenje sigurnosti mrežnog i informacijskog sustava te pratiti do njihovoga rješavanja. Prema potrebi treba provesti ažuriranje politika i procedura. Subjekt može ovu mjeru ograničiti na kritičnu programsku i sklopovsku imovinu iz mjere 2.1.

5.9. osigurati središnju pohranu sigurnosno relevantnih događaja kopijom dnevničkih zapisa, kontinuirano ili u vremenskim intervalima ne duljima od 24 sata, s mjesta gdje su generirani na centralizirani sustav koji omogućava pohranu i pretragu te gdje su isti zaštićeni od neautoriziranog pristupa i izmjena (ukoliko je moguće administrator izvorišnog sustava ne bi trebao biti administrator ovoga centraliziranog sustava). Osigurati da središnji sustav ima mogućnosti prepoznavanja anomalija i mogućih incidenata te generiranje upozorenja o sumnjivim događajima. Praćenje dnevničkih zapisa treba uzimati u obzir važnost programske i sklopovske imovine i procjenu rizika – potrebno je generirati veći, odnosno dopušteno je generirati manji broj različitih vrsta upozorenja o sumnjivim događajima uzimajući u obzir scenarije rizika i procijenjene rizike. Subjekt mora u unaprijed planiranim intervalima provjeravati bilježe li se dnevnički zapisi ispravno kroz provođenje ili simulaciju radnje koja bi trebala rezultirati bilježenjem odgovarajućeg dnevničkog zapisa. Subjekt mora voditi brigu da se praćenje implementira i na način kojim bi se minimaliziralo postojanje lažno pozitivnih i lažno negativnih događaja

5.10. osigurati primjenu kontrola koje sprječavaju ili otkrivaju korištenje poznatih ili sumnjivih zlonamjernih web-stranica. Filter je moguće ostvariti primjenom liste zabranjenih kategorija ili imena domena, ili primjenom liste dozvoljenih kategorija ili imena domena, ovisno o apetitu subjekta za rizik te poslovnim potrebama

5.11. smanjiti potencijalnu površinu izloženosti subjekta kibernetičkim napadima:

– identifikacijom i ograničavanjem servisa koji su javno izloženi/dostupni putem Interneta (primjerice web-stranice, e-pošta, VPN ulazne točke, nadzorne konzole, RDP ili SSH servisi za udaljenu administraciju, SFTP, SMB i sličnih servisa za razmjenu datoteka i dr.)

– smanjenjem broja administratorskih i visoko privilegiranih korisničkih računa

– blokiranjem pristupa javno dostupnim servisima s TOR mreže i poznatih anonimizacijskih VPN servisa

– ograničavanjem izravnog pristupa Internet poslužiteljima, ukoliko je moguće.

Mjere 5.1 do 5.11. primjenjuju se u cijelosti na IT dio mrežnih i informacijskih sustava subjekta. Na OT sustave primjenjuju se gornje točke 5.1., 5.2., 5.3., 5.5., 5.6., 5.7., 5.8., 5.9., 5.10. i 5.11., dok se gornja točka 5.4. primjenjuje, ovisno o procjeni rizika implementacije takve mjere na OT sustave.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere										
	5.1.	5.2.	5.3.	5.4.	5.5.	5.6.	5.7.	5.8.	5.9.	5.10.	5.11.
osnovna	A	A	A	A	A	A	C	A	C	C	C
srednja	A	A	A	A	A	A	B	A	A	A	A
napredna	A	A	A	A	A	A	B	A	A	A	A

6. Osiguravanje kibernetičke sigurnosti mreže

Cilj: Cilj mjere je osigurati cjelovitost, povjerljivost i dostupnost mrežnih resursa subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

6.1. definirati i uspostaviti, sukladno svojoj mrežnoj arhitekturi i izloženosti javnim mrežama, obavezne mjere zaštite mreže te pritom razmotriti adekvatne mjere poput korištenje vatrozida, virtualne privatne mreže (VPN), mrežnog pristupa uz stalnu primjenu principa nultog povjerenja (*zero trust* – »svi su nepouzdani«), sigurnih mrežnih protokola za bežičnu mrežu, odvajanje mreža različitih namjena, sukladno kritičnosti podataka ili prioritetu pojedinih mrežnih segmenata (primjerice uredska mreža, nadzorna mreža, produkcija, proizvodnja, gosti itd.)

6.2. osigurati da obavezne mjere zaštite mreže osiguravaju zaštićeni prijenos kritičnih podataka te autorizaciju i kontrolu korištenja mreža i mrežno dostupnih resursa. Primjerice, subjekt će osigurati korištenje sigurnih inačica protokola kao što su HTTPS i sFTP, pristup mreži samo za ovlaštene pojedince ili uređaje (autorizacija može biti utemeljena na provjerenom digitalnom identitetu pojedinca, provjerenom digitalnom identitetu uređaja, oboje ili

gdje drugačije nije moguće lokacijom spajanja ukoliko se provodi autorizacija pristupa lokaciji, primjerice čuvani uredski prostor ili podatkovni centar)

6.3. svake godine provesti sveobuhvatan pregled svih definiranih mjera zaštite mreže kako bi se osiguralo da su one i dalje učinkovite i relevantne. Ovaj pregled uključuje procjenu trenutnih kibernetičkih prijetnji, ranjivosti i promjena u poslovnom okruženju koje bi mogle utjecati na uspostavljene mjere zaštite. Na temelju rezultata pregleda, provodi se ažuriranje tehničkih mjera zaštite kako bi se odgovorilo na nove izazove i rizike, osiguravajući stalnu usklađenost s najboljim praksama i zahtjevima. Svi rezultati i promjene koje se predlažu moraju se dokumentirati i odobriti od strane osoba odgovornih za provedbu mjera

6.4. implementirati mehanizme praćenja odlaznog i dolaznog mrežnog prometa u svrhu smanjenja rizika od kibernetičkog napada te definirati metode filtriranja nepoželjnog mrežnog prometa u smislu prepoznavanja potencijalnih indikatora kompromitacije. Ovo uključuje postavljanje odgovarajućih alata za praćenje i analizu mrežnog prometa koji omogućuju identifikaciju i automatsko blokiranje potencijalno opasnih aktivnosti. Također, subjekt mora definirati i primijeniti metode filtriranja nepoželjnog mrežnog prometa, poput upotrebe sustava za otkrivanje i sprječavanje napada (IDS/IPS) i drugih sigurnosnih rješenja. Svi implementirani mehanizmi i metode filtriranja moraju biti redovito revidirani i ažurirani kako bi se održala visoka razina sigurnosti mreže. Ova mjera ne utječe na zabranu nadzora elektroničkih komunikacija reguliranu zakonom koji uređuje elektroničke komunikacije

6.5. implementirati tehničke mehanizme detekcije anomalija u mreži temeljene ili na odstupanju od tipičnog mrežnog prometa ili na odstupanju od interno definiranih pravila.

Mjere 6.1. do 6.5. primjenjuju se u cijelosti na IT dio mrežnih i informacijskih sustava subjekta. Na OT sustave subjekta primjenjuju se u cijelosti mjere pod gornjim točkama 6.1., 6.3. i 6.5.

Na OT dio mrežnih i informacijskih sustava subjekta je primjenjiva i gornja točka 6.2., ovisno o dodatnoj procjeni kritičnosti podataka subjekta u okruženju OT sustava, dok je gornja točka 6.4. primjenjiva, ovisno o procjeni mogućeg negativnog učinka automatskog blokiranja potencijalno opasnih aktivnosti na operativni učinak i sigurnost OT sustava.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere				
	6.1.	6.2.	6.3.	6.4.	6.5.
osnovna	A	A	A	C	C
srednja	A	A	A	A	C
napredna	A	A	A	A	A

7. Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima

Cilj: Cilj mjere je uspostaviti sveobuhvatan sustav politika i procedura za kontrolu fizičkog i logičkog pristupa mrežnim i informacijskim sustavima subjekta, kako bi se spriječio neovlašteni pristup programskoj i sklopovskoj imovini te podacima subjekta.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

7.1. razviti, dokumentirati održavati i implementirati pravila kontrole pristupa mrežnom i informacijskom sustavu. Kontrola pristupa se odnosi na sve osobe i vanjske sustave koji pristupaju mrežnim i informacijskim sustavima subjekta. Politika i pravila kontrole pristupa trebaju obuhvaćati razradu kontrole pristupa za:

– zaposlenike i osoblje drugih subjekata koji predstavljaju izravne dobavljače ili pružatelje usluga

– procese u okviru mrežnog i informacijskog sustava subjekta, kojima je omogućeno povezivanje s nekim drugim procesom izvan mrežnog i informacijskog sustava subjekta.

Subjekt ne mora dokumentirati pravila kontrole pristupa ako koristi isključivo usluge računalstva u oblaku, ali i u tom slučaju mora osigurati upravljanje životnim ciklusom digitalnih identiteta svih svojih korisnika sukladno mjeri 4.6.

7.2. osigurati definiranje uloga vlasnika na aplikacijama koje odobravaju pridruživanje korisničkih prava te osigurati zapise o tome tko je odobrio dodjelu prava. Prava pristupa mrežnim i informacijskim sustavima moraju biti dodijeljena, izmijenjena, ukinuta i dokumentirana u skladu s politikom kontrole pristupa subjekta. Ukoliko se prava pristupa definiraju kroz uloge, svakoj ulozi se mora pridružiti vlasnik. Vlasnik uloge odgovoran je za dodjelu prava. Subjekt mora osigurati zapise o odobrenju dodjele uloga sukladno politici bilježenja i praćenja dnevničkih zapisa. Subjekt može odlučiti u svojem sustavu za dodjelu prava korisnicima dokumentirati ili implementirati mapiranje radnih uloga na funkcionalne uloge u pojedinim mrežnim i informacijskim sustavima u cilju bržeg i učinkovitijeg upravljanje digitalnim identitetima

7.3. provoditi redovite kontrole korisničkih prava pristupa. Prava pristupa revidiraju se i dokumentiraju u planiranim intervalima, najmanje jednom godišnje te se prilagođavaju organizacijsko-poslovnim promjenama subjekta i dokumentiraju se s odgovarajućim praćenjem promjena. Subjekt može ovu mjeru ograničiti na kritičnu programsku i sklopovsku imovinu iz mjere 2.1.

7.4. osigurati nadzor i kontrolu pristupa kritičnim mrežnim i informacijskim sustavima za privilegirane korisnike. Subjekt mora donijeti i primjenjivati politike tj. pravila za upravljanje privilegiranim računima i računima administratora sustava. Pravila moraju uključivati:

– kreiranje specifičnih računa koji će se koristiti isključivo za aktivnosti administracije sustava, kao što su instalacija, konfiguracija, upravljanje i održavanje

– individualizaciju i ograničavanje administratorskih privilegija koliko god je to moguće

– korištenje privilegiranih i administratorskih računa isključivo za spajanje na sustave za administraciju, a ne za korištenje u ostalim poslovnim aktivnostima subjekta

– korištenje identifikacije, snažnu provjeru autentičnosti (primjerice metoda višefaktorske autentifikacije) i autorizacijske procedure za privilegirane i administratorske račune

7.5. primijeniti dinamičku kontrolu pristupa temeljenu na riziku u stvarnom vremenu gdje je to moguće i izvedivo korištenjem naprednih alata

7.6. koristiti naprednu analizu ponašanja korisnika mrežnih i informacijskih sustava (UEBA) koja prepoznaje neobično ili sumnjivo ponašanje korisnika, odnosno slučajeve u kojima postoje nepravilnosti koje izlaze izvan okvira uobičajenih svakodnevnih obrazaca ili korištenja.

Mjere 7.1 do 7.6. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere					
	7.1.	7.2.	7.3.	7.4.	7.5.	7.6.
osnovna	A	A	A	A	C	C
srednja	A	A	A	A	C	C
napredna	A	A	A	A	C	C

8. Sigurnost lanca opskrbe

Cilj: Cilj mjere je uspostaviti jasnu i sveobuhvatnu politiku za izravne dobavljače ili pružatelje usluga, osobito ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, u svrhu smanjenja identificiranih rizika i minimiziranja ranjivosti te optimiziranja lanca opskrbe subjekta, što će rezultirati stabilnijim poslovanjem i većom pouzdanosti isporuke svojih proizvoda i usluga.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

8.1. razvijati, održavati, dokumentirati i implementirati pravila sigurnosti lanca opskrbe koja uključuju minimalne zahtjeve za pojedine vrste svojih izravnih dobavljača i pružatelja usluga, a posebno onih koji subjekte opskrbljuju IKT uslugama, IKT sustavima ili IKT proizvodima te proces provjere sigurnosti svojih izravnih dobavljača i ponuđenih usluga koje se tiču kritičnih mrežnih i informacijskih sustava. Subjekt mora uspostaviti ova pravila za svoje izravne dobavljače i pružatelje usluga, uključujući lanac opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima. Pravila sigurnosti lanca opskrbe sadržavaju uloge, odgovornosti i ovlasti uključujući sigurnosne aspekte u pogledu odnosa između subjekta i njegovih izravnih dobavljača ili pružatelja usluga. Preporuča se da subjekt definira pravila za različite dobavljače ukoliko se sigurnosni aspekti razlikuju, primjerice različita pravila za dobavljače opreme i softvera u komercijalnoj ponudi od pravila za dobavljače softvera po narudžbi ili pružatelje usluga računalstva u oblaku (primjerice obavezni SSO) odnosno pružatelje usluge održavanja mrežnog i informacijskog sustava

8.2. identificirati sve svoje izravne dobavljače i pružatelje usluga, uključujući one u lancu opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, te procijeniti potencijalne rizike za mrežne i informacijske sustave subjekta, koji proizlaze iz tih poslovnih odnosa i temeljem toga uspostaviti i održavati registar izravnih dobavljača i pružatelja usluga koji uključuje:

– kontaktne točke za svakog od njih, a posebno za one koje imaju pristup ili upravljaju kritičnom programskom ili sklopovskom imovinom subjekta

– popis usluga, sustava ili proizvoda koje subjekt izravno nabavlja od identificiranih izravnih dobavljača i pružatelja usluga

8.3. u ugovorima o poslovnoj suradnji odnosno nabavi ili pružanju usluga (*Service Level Agreement – SLA*) definirati sigurnosne zahtjeve za svoje izravne dobavljače i pružatelje usluga, koji su usklađeni s kibernetičkim sigurnosnim politikama subjekta.

Sigurnosni zahtjevi trebaju uključivati sljedeće:

– sigurnosne klauzule u ugovorima (primjerice odredbe o povjerljivosti)

– u slučaju sklapanja ugovora o pružanju upravljanih usluga i upravljanih sigurnosnih usluga, ugovori o pružanju takvih usluga moraju se sklapati isključivo sa pružateljima takvih usluga koji su kategorizirani kao ključni ili važni subjekti sukladno Zakonu (provjera statusa kategorizacije pružatelja upravljanih usluga i pružatelja upravljanih sigurnosnih usluga provodi se preko središnjeg državnog tijela za kibernetičku sigurnost)

– odredbe o obvezi izravnog dobavljača ili pružatelja usluga da odmah po saznanju obavijesti subjekta o incidentima koji mogu utjecati na subjekta

– odredbe o pravu na zahtijevanje provedbe revizije kibernetičke sigurnosti i/ili pravu na dokaz o provedenoj reviziji kibernetičke sigurnosti, odnosno posjedovanju odgovarajućih jednakovrijednih certifikata izravnog dobavljača

– odredbe o obvezi upravljanja ranjivostima koja uključuje otkrivanje ranjivosti i njihovo otklanjanje, kao i obavještavanje subjekta o ranjivostima koje mogu utjecati na subjekta

– odredbe o mogućem podugovaranju i sigurnosnim zahtjevima za podugovaratelje

– odredbe o obvezama izravnog dobavljača ili pružatelja usluga pri isteku ili raskidu ugovornog odnosa (primjerice pronalaženje i uklanjanje/uništavanje/zbrinjavanje podataka).

Sigurnosni zahtjevi mogu uključivati sljedeće:

– odredbe o vještinama i osposobljavanju koje se zahtijevaju u odnosu na zaposlenike izravnog dobavljača ili pružatelja usluga

– odredbe o certifikatima ili drugim ovlaštenjima koji se zahtijevaju za zaposlenike izravnog dobavljača ili pružatelja usluga.

8.4. nadzirati, revidirati, evaluirati i ponavljati proces provjere sigurnosti ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima i to prilikom svakog novoga ugovaranja ili minimalno svake dvije godine ili nakon incidenta povezanog s predmetnom uslugom, sustavom ili proizvodom ili nakon značajnih promjena u sigurnosnim zahtjevima ili stanju kibernetičke sigurnosti. Sva utvrđena odstupanja tijekom revidiranja i evaluacije trebaju se obraditi kroz procjenu rizika. Kontrola sigurnosnih zahtjeva trebala bi obuhvatiti sve ugovorima definirane sigurnosne zahtjeve

8.5. definirati kriterije i sigurnosne zahtjeve za odabir i sklapanje ugovora s izravnim dobavljačima ili pružateljima usluga kao i kriterije za evaluaciju i praćenje sigurnosti pojedinih dobavljača i pružatelja usluga, osobito onih koji pripadaju ključnom lancu opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima. Subjekt treba nastojati diversificirati svoje izvore opskrbe, kako bi ograničio ovisnost o pojedinom dobavljaču odnosno pružatelju usluga te uzeti u obzir rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, koje provodi Skupina za suradnju zajedno s Europskom komisijom i ENISA-om, ukoliko su dostupni. Subjekt je dužan pri definiranju kriterija i sigurnosnih zahtjeva odabira i sklapanja ugovora uzeti u obzir:

– sposobnost dobavljača i pružatelja usluge da osigura provedbu sigurnosnih zahtjeva subjekta

– vlastite rizike i razinu kritičnosti pojedinih IKT usluga, IKT sustava ili IKT proizvoda koje nabavlja, uključujući toleranciju rizika dobavljača odnosno pružatelja usluga

8.6. razviti planove za odgovor na incidente koji uključuju ključne dobavljače i pružatelje usluga, osobito one koji pripadaju ključnom lancu opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima. Subjekt mora razviti planove odgovora na incidente u skladu s dokumentiranim procedurama i u razumnom vremenskom razdoblju. Odgovor na incidente mora uključivati i aktivnosti ključnih dobavljača i pružatelja usluga.

Mjere 8.1 do 8.6. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere					
	8.1.	8.2.	8.3.	8.4.	8.5.	8.6.
osnovna	A	A	A	A	C	C
srednja	A	A	A	A	A	A
napredna	A	A	A	A	A	A

9. Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava

Cilj: Cilj mjere je osigurati da subjekti uspostave, dokumentiraju, provode i kontinuirano nadziru konfiguraciju svojih mrežnih i informacijskih sustava, uključujući sigurnosne postavke sklopovske i programske imovine, kao i vanjske usluge i mreže koje koriste.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

9.1. provoditi analizu sigurnosnih zahtjeva u fazama izrade tehničke specifikacije, projektiranja ili nabave mrežnih i informacijskih sustava te definirati kriterije za prihvaćanje rješenja sukladno definiranim sigurnosnim zahtjevima

9.2. uspostaviti, dokumentirati, provesti i kontinuirano nadzirati konfiguraciju svojih mrežnih i informacijskih sustava, uključujući sigurnosne konfiguracijske postavke za svu sklopovsku i programsku imovinu, kao i za sve korištene vanjske usluge i mreže, tijekom njihova životnog ciklusa

9.3. propisati procedure za upravljanje promjenama u okviru održavanja mrežnih i informacijskih sustava, koje moraju uključivati svu korištenu programsku i sklopovsku podršku te promjene njihove konfiguracije. Procedure se primjenjuju prilikom puštanja u produkcijsku okolinu, prilikom svih planiranih ili neplaniranih promjena programske i sklopovske imovine koja se koristi ili prilikom bilo koje značajnije promjene konfiguracije mrežnih i informacijskih sustava, kao i u slučaju njihova razvoja. Kontrolne procedure moraju biti propisane u okviru kibernetičkih sigurnosnih politika subjekta te s njima trebaju biti upoznati svi relevantni zaposlenici subjekta. U slučaju hitnih promjena, potrebno je dokumentirati rezultate promjene, ali i dati objašnjenje zašto se nije mogao provesti redovni postupak promjene i koje bi bile posljedice kašnjenja da je došlo do provedbe redovnog postupka promjene. Testiranja koja nisu provedena zbog hitnih promjena, trebaju biti naknadno provedena. Kad god je to moguće, promjene trebaju biti testirane i potvrđene prije nego što se uvedu u produkcijsku okolinu. Kontrolne procedure trebaju uključivati:

– zahtjev za promjenu

– procjenu rizika koju promjena unosi

– kriterije za kategorizaciju i određivanje prioriteta promjena i pridružene zahtjeve za vrstu i opseg testiranja koje je potrebno provesti te odobrenja koja je potrebno dobiti

– zahtjeve za provedbu reverznog postupka za povratak na prijašnje stanje

– dokumentaciju o promjeni i odobrenju promjene, uključujući i podatke o odgovornim osobama za pojedini segment mrežnog i informacijskog sustava

9.4. razviti, održavati i implementirati pravila za sigurnost u procesima razvoja i održavanja mrežnih i informacijskih sustava. Subjekt mora osigurati mehanizme za osiguravanje sigurnog dizajna (*secure by design* and *by default*) i arhitekturu nultog povjerenja, identifikaciju mogućih ranjivosti na mrežnim i informacijskim sustavima koje samostalno razvija, integrira ili implementira te definirati sigurnosne zahtjeve za razvojna okruženja. Identifikaciju mogućih ranjivosti je moguće postići tijekom ranih faza dizajna primjenom metoda modeliranja prijetnji (*Threat modelling*), tijekom razvoja raznim tehnikama statičkog (*SAST*) i dinamičkog (*DAST*) testiranja ili nakon završetka razvoja raznim vrstama testiranja konačnog produkta ili sustava (*primjerice penetration testing*). Preporuča se primjena načela pomaka sigurnosnih provjera na lijevo tj. na ranije faze softverskog razvoja. Rezultatima provedenog sigurnosnog testiranja treba odgovarajuće upravljati kao sa svim drugim rizicima

UVJET: Mjera 9.4. je obvezujuća za subjekte koji samostalno razvijaju ili održavaju mrežne i informacijske sustave.

9.5. zaposlenicima koji su uključeni u razvoj mrežnih i informacijskih sustava omogućiti kontinuirano osposobljavanje, definirati interne standarde za sigurni razvoj mrežnih i informacijskih sustava te provoditi redovne sigurnosne preglede kôda. Mjeru je moguće provesti primjenom nekih od kolaborativnih metoda razvoja (programiranje u paru, dva para očiju prilikom prihvaćanje promjena kôda, razvoj temeljen na testiranju itd.), primjenom alata za statičku analizu kôda (SAST) i slično, a osposobljavanje zaposlenika koji su uključeni u razvoj mrežnih i informacijskih sustava mora minimalno uključiti:

– analizu sigurnosnih zahtjeva u fazama izrade tehničke specifikacije i projektiranja ili nabave mrežnih i informacijskih sustava

– načela za projektiranje sigurnih sustava i načela sigurnog programskog kôdiranja, kao što je primjerice ugradnja mjera sigurnosti sustava u fazi projektiranja (*security-by-design*) modeliranje prijetnji ili arhitektura nultog povjerenja

– pridržavanje sigurnosnih zahtjeva za razvojna okruženja

– korištenje sigurnosnog testiranja u okviru životnog ciklusa razvoja

UVJET: Mjera 9.5. je obvezujuća za subjekte koji samostalno razvijaju ili održavaju mrežne i informacijske sustave.

9.6. integrirati sigurnosne alate i procese u razvojne operacije i prakse (*DevOps, DevSecOps*) tj. osigurati provjeru sigurnosti unutar procesa kontinuirane integracije i isporuke (*CI/CD*). Subjekti moraju uspostaviti, dokumentirati, provesti i kontinuirano nadzirati konfiguraciju svojih mrežnih i informacijskih sustava, uključujući sigurnosne konfiguracijske postavke sklopovske i programske imovine što uključuje i primjenu unutar metodologije procesa kontinuirane integracije i kontinuirane isporuke, a sukladno odabranoj praksi.

Mjere 9.1 do 9.6. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjera					
	9.1.	9.2.	9.3.	9.4.	9.5.	9.6.
osnovna	A	A	A	C	C	C
srednja	A	A	A	B	B	C
napredna	A	A	A	B	B	C

10. Kriptografija

Cilj: Cilj mjere je da subjekti, sukladno vlastitim poslovnim potrebama, uspostave sveobuhvatne kriptografske politike i postupke kako bi osigurali zaštitu podataka u prijenosu i mirovanju. Implementacija kriptografskih politika treba osigurati primjenu prikladne kriptografske tehnike i algoritama, u skladu s najboljim praksama i regulatornim zahtjevima.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

10.1. razviti, dokumentirati, održavati i implementirati pravila primjene kriptografije u subjektu, s ciljem osiguravanja odgovarajućeg i učinkovitog korištenja kriptografije za zaštitu dostupnosti, autentičnosti, cjelovitosti i povjerljivosti kritičnih podataka sukladno vrsti podataka i rezultatima procjene rizika

10.2. koristiti metode kriptiranja za zaštitu kritičnih podataka u prijenosu. Kriptografske algoritme, metode nadopune prije kriptiranja (*padding*) te veličine ključeva za pojedine algoritme treba prilagođavati trenutnim dobrim praksama te moraju biti proporcionalni riziku i potrebi zaštite subjekta

10.3. osigurati sigurno upravljanje kriptografskim ključevima što uključuje osiguravanje da kriptografski ključevi budu zaštićeni od neovlaštenog pristupa. Subjekt mora definirati i dokumentirati pravila pristupa upravljanju kriptografskim ključevima, uključujući metode za:

– generiranje ključeva za različite kriptografske sustave i aplikacije

– izdavanje i pribavljanje certifikata s javnim ključevima

– distribuciju ključeva do krajnjih korisnika, uključujući pravila aktivacije zaprimljenih ključeva

– pohranjivanje ključeva, uključujući pravila pristupa ključevima od strane ovlaštenih korisnika

– zamjenu ili ažuriranje ključeva, uključujući pravila o načinu i vremenskim periodima zamjene ključeva

– postupanje s kompromitiranim ključevima

– opoziv ključeva, uključujući pravila o načinu povlačenja ili deaktivaciji ključeva

– oporavak ključeva koji su izgubljeni ili oštećeni

– sigurnosno pohranjivanje ili arhiviranje ključeva

– uništavanje ključeva

– evidentiranje i nadziranje aktivnosti vezanih uz upravljanje ključevima

– određivanje razdoblja valjanosti ključeva

10.4. implementirati metode kriptiranja za zaštitu kritičnih podataka u mirovanju. Subjekt će sukladno kritičnosti podatka implementirati metode zaštite kritičnih podataka u mirovanju. Metode moraju obuhvatiti sve medije na kojima su pohranjeni dotični podaci u mirovanju. Kriptografski algoritmi, metode nadopune prije kriptiranja (engl. *padding*) te veličine ključeva za pojedine algoritme treba prilagođavati trenutnim dobrih praksama te moraju biti proporcionalni procijenjenom riziku subjekta i potrebi subjekta za zaštitom

10.5. provoditi redovite revizije i ažuriranja kriptografskih politika i procedura. Pravila kriptografske politike i procedura obveznici su dužni ažurirati u planiranim intervalima i sukladno najnovijim dostignućima u kriptografiji

10.6. sukladno procijenjenom riziku, koristiti kvantno otpornu kriptografiju za zaštitu protiv budućih prijetnji u slučajevima gdje je to moguće.

Mjere 10.1. do 10.6. primjenjuju se na kritične podatke subjekta iz mjere 2.3. i sukladno procjeni rizika subjekta, neovisno nalaze li se podaci na IT ili OT dijelu mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere					
	10.1.	10.2.	10.3.	10.4.	10.5.	10.6.
osnovna	A	A	A	A	C	C
srednja	A	A	A	A	A	C
napredna	A	A	A	A	A	C

11. Postupanje s incidentima

Cilj: Cilj mjere je uspostaviti sveobuhvatan okvir za utvrđivanje uloga, odgovornosti i procedura koje će omogućiti subjektu učinkovito sprječavanje, otkrivanje, analizu, zaustavljanje i odgovor na incidente te oporavak od incidenata.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

11.1. razviti i dokumentirati postupke za postupanje s incidentima, što uključuje definiranje uloga, odgovornosti i procedura za praćenje, sprječavanje, otkrivanje, analizu, zaustavljanje incidenta i odgovor na njega, oporavak od incidenta te evidentiranje i interno prijavljivanje incidenata u jasno definiranim vremenskim okvirima

11.2. uspostaviti osnovne procedure za postupanje s incidentima kojima subjekt mora minimalno osigurati sljedeće:

– utvrđivanje djelotvornih planova komunikacije, uključujući planova za razvrstavanje incidenata prema nacionalnoj taksonomiji, internu eskalaciju i prijavljivanje incidenata. Pri tome, subjekt će, sukladno procjeni rizika, u planove komunikacije uključiti pravila za korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima.

– dodjeljivanje uloga za otkrivanje i odgovor na incidente kompetentnim zaposlenicima

– pravila postupanja s dokumentacijom koja će biti korištena ili će nastati tijekom postupanja s incidentom, što može uključivati priručnike za odgovor na incidente, grafove eskalacije, kontaktne liste i obrasce koje je potrebno popunjavati i dostavljati nadležnim tijelima

– uvođenje jednostavnog mehanizma koji omogućuje zaposlenicima subjekta i njegovim izravnim dobavljačima i pružateljima usluga prijavu sumnjivih događaja koji bi mogli predstavljati incident

– potrebno je procjenjivati utjecaj svakog pojedinog incidenta na kontinuitet poslovanja subjekta i na odgovarajući način uspostaviti sučelje između postupanja s incidentima i upravljanja kontinuitetom poslovanja subjekta

– evidentiranje incidenata

– praćenje svih elemenata potrebnih za identificiranje i praćenje značajnih incidenata i pravovremeno obavještavanje o značajnim incidentima u nadležni CSIRT, u skladu s propisanim obvezama subjekta.

11.3. osigurati osnovnu obuku zaposlenika za prepoznavanje i prijavu sumnjivih događaja i incidenata koja se mora ponoviti najmanje jednom godišnje za sve zaposlenike. Provođenje obuke mora biti dokumentirano. Provođenje obuke mora se prilagoditi potrebama poslovanja subjekta

11.4. razviti i dokumentirati detaljne procedure za praćenje, analizu i odgovor na incidente, uzimajući u obzir definirani vremenski okvir za interno prijavljivanje incidenta. Subjekt je dužan definirati i dokumentirati pravila za trijažu sumnjivih događaja, koja određuju kojim će se redoslijedom procjenjivati i obrađivati takvi

događaji. U procesu trijaže prilikom procjene određenog sumnjivog događaja moguće je procijeniti da je određeni sumnjivi događaj vjerojatno lažno pozitivan događaj ili da je mogući učinak takvog događaja vjerojatno manji od očekivanog, na temelju čega se zatim može smanjiti prioritet za daljnju procjenu i obradu tog sumnjivog događaja, tj. može se prijeći na procjenu drugih sumnjivih događaja prije završetka konačne obrade i procjene tog događaja. Subjekt je dužan definirati procedure za zaustavljanje incidenta, odgovor na incident i oporavak od incidenta, u svrhu sprječavanja incidenta i njegove ponovne pojave te širenja i otklanjanja njegovih posljedica. Subjekt je dužan definirati procedure za obavještavanje nadležnog CSIRT-a o značajnim incidentima, kao i za izvještavanje relevantnih internih i vanjskih korisnika svojih mrežnih i informacijskih sustava, u skladu s definiranim planom komunikacije i propisanim obvezama subjekta

11.5. provoditi jednom godišnje vježbe postupanja sa simuliranim incidentima u svrhu provjeravanja djelotvornosti uspostavljenih procedura za praćenje, analizu i odgovor na incidente. Provođenje vježbi subjekt je dužan dokumentirati na isti način kao i stvarne incidente, uz jasnu napomenu u dokumentaciji koja nastaje u okviru provedbe vježbe da se ne radi o stvarnom incidentu već o vježbi. U pitanju mogu biti *red teaming* vježbe, *table top* simulacijske vježbe te *purple teaming/adversary emulation* & *detection engineering* vježbe

11.6. koristiti specijalizirane alate za automatizirano otkrivanje i odgovor na incidente (*IDR/EDR/XDR/NDR*). Navedene alate potrebno je adekvatno uključiti i povezati s drugim sigurnosnim kontrolama. Kako količina sumnjivih događaja može biti velika, bitno je da se subjekt ne nađe u situaciji da od velike količine sumnjivih događaja ne prepozna ključnu informaciju koja ukazuje na to da se dogodio značajan incident. Bitnije je da subjekt obradi i procijeni manji broj ključnih sumnjivih događaja, nego da obradi i procijeni veći broj svih ostalih sumnjivih događaja. Zato je nužno da svaki sumnjivi događaj ima odgovarajuću razinu prioriteta na temelju koje će se u procesu trijaže odrediti kojim će se redoslijedom obrađivati sumnjivi događaji.

Mjere 11.1 do 11.5. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta, dok je gornja točka 11.6. primjenjiva, ovisno o procjeni mogućeg negativnog učinka automatiziranog otkrivanja i odgovora na incidente s obzirom na operativni učinak i sigurnost OT sustava.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere					
	11.1.	11.2.	11.3.	11.4.	11.5.	11.6.
osnovna	A	A	A	A	C	C
srednja	A	A	A	A	A	A
napredna	A	A	A	A	A	A

12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama

Cilj: Cilj mjere je osigurati postojanje unaprijed pripremljenih planove za minimiziranje prekida u poslovanju i osiguravanje kontinuiteta ključnih poslovnih aktivnosti subjekta za slučajeve incidenata i kibernetičkih kriza.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

12.1. razviti, održavati i implementirati politike kontinuiteta poslovanja i upravljanja kibernetičkim krizama, koje će identificirati ključne poslovne aktivnosti subjekta te organizacijske i tehničke preduvjete za njihovu provedbu, kao podlogu za izradu planova mogućeg suženog opsega poslovanja tijekom oporavka od incidenata i povratka uobičajenom opsegu poslovanju u definiranom vremenskom okviru i opsegu poslovanja prihvatljivom za subjekt

12.2. provesti analizu utjecaja incidenata na poslovanje (*Business Impact Analysis – BIA*) kojom će se identificirati ključne poslovne funkcije i procjenu rizika kao preduvjet za razvoj planova za oporavak od incidenata. Na temelju rezultata te analize i procjene rizika, subjekt mora minimalno uspostaviti:

– ciljana vremena oporavka (*Recovery Time Objectives – RTOs*) kako bi se utvrdilo maksimalno dopušteno vrijeme koje može proteći za oporavak poslovnih resursa i funkcija nakon prekida u radu pojedinih segmenata mrežnih i informacijskih sustava

– vremenske točke oporavka (*Recovery Point Objectives – RPOs*) kako bi se utvrdilo koliko podataka se može izgubiti po pojedinoj poslovnoj aktivnosti koja se provodi pomoću mrežnog i informacijskog sustava, odnosno pomoću IKT usluga i IKT procesa koje mogu biti u prekidu

– ciljevi pružanja usluge (*Service Delivery Objectives – SDOs*) kako bi se utvrdila minimalna razina performansi koja se treba postići kako bi se omogućilo poslovanje za vrijeme alternativnog načina rada

– RPO, RTO i SDO se moraju uzeti u obzir kod utvrđivanja politika pričuvnih kopija i redundancija. Isto tako RPO, RTO, SDO se moraju uzeti u obzir kod upravljanja sigurnošću lanca opskrbe, kao i kod sigurnosti u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući otklanjanje ranjivosti i njihovo otkrivanje

– popis ključnih komunalnih usluga potrebnih za normalan rad mrežnih i informacijskih sustava

12.3. uspostaviti procese za upravljanje kibernetičkim krizama odnosno za slučajeve kibernetičkih sigurnosnih incidenata velikih razmjera, pri čemu će osigurati da procesi upravljanja kibernetičkim krizama adresiraju najmanje:

– uloge i odgovornosti zaposlenika subjekta, kako bi se osiguralo da svi zaposlenici budu upoznati sa svojim ulogama u kriznim situacijama, uključujući konkretne korake koje je potrebno pratiti

– primjerene mjere komunikacije između subjekta i relevantnih nadležnih tijela sukladno Nacionalnom programu upravljanja kibernetičkim krizama

– održavanje uspostavljene razine kibernetičke sigurnosti subjekta u kriznim situacija kroz primjenu primjerenih mjera, poput sustava i procesa za podršku i uspostavu možebitnih dodatnih kapaciteta

– provedbu procesa za upravljanje i korištenje informacija dobivenih od nadležnog CSIRT-a ili drugog nadležnog tijela vezano za incidente, ranjivosti, kibernetičke prijetnje i potrebne mjere upravljanja kibernetičkim sigurnosnim rizicima

12.4. razviti detaljne planove za oporavak od katastrofa (DRP) i kontinuitet poslovanja (BCP). Na osnovu rezultata procjene rizika i plana kontinuiteta poslovanja, plan subjekta za pričuvno kopiranje podataka i redundancije treba biti razvijen, održavan i dokumentiran, a mora uzeti u obzir najmanje:

– vrijeme oporavka

– osiguranje da su pričuvne kopije odnosno redundantni sustavi potpuni i ispravni, uključujući konfiguracijske podatke i podatke pohranjene u okruženju usluga računalstva u oblaku

– pohrana (mrežnih i izvan mrežnih) pričuvnih kopija te redundantnih sustava na sigurnoj lokaciji ili lokacijama, koji nisu na

istoj mreži kao i primarni sustav te su na dovoljnoj udaljenosti kako bi izbjegle bilo koju štetu uslijed katastrofe na glavnoj lokaciji

– primjena odgovarajućih fizičkih kontrola (kao što je ograničenje pristupa) i logičkih kontrola (kao što je enkripcija) za pričuvne kopije, u skladu s razinom kritičnosti podataka na tim kopijama

– ponovno uspostavljanje podataka iz pričuvnih kopija odnosno aktiviranje prebacivanja na redundantne sustave, uključujući proces odobrenja

– ovisnost o ključnim komunalnim uslugama

– hodogram aktivnosti oporavka koji se odnose na vremenski raspored i međuovisnosti pojedinih aktivnosti oporavka

12.5. provoditi testiranje planova kontinuiteta poslovanja najmanje jednom godišnje. Planovi kontinuiteta poslovanja se moraju testirati kroz vježbe i revidirati periodički, nakon incidenata, promjena u operacijama ili procijenjenim rizicima. Provođenje testiranja planova kontinuiteta poslovanja mora biti dokumentirano kako bi se nedvosmisleno utvrdilo potrebna unaprjeđenja uočena tijekom provedbe testiranja. Prilikom testiranja plana kontinuiteta poslovanja potrebno je testirati sljedeće:

– uloge i odgovornosti

– ključne kontakte tj. kontakte zaposlenika s potrebnim odgovornostima, ovlastima i sposobnostima

– unutarnje i vanjske komunikacije kanale

– uvjete aktivacije i deaktivacije plana

– redoslijed postupanja kod oporavka

– plan oporavka za specifične operacije

– potrebni resursi, uključujući pričuvne kopije i redundancije

– minimalno ponovno uspostavljanje (*Recovery*), a ovisno o planovima i ponovno pokretanje aktivnosti (*Restore*) nakon privremenih mjera

– povezanost s postupanjem s incidentima

– mrežne i informacijske sustave, primjerice hardver, softver, servise, podatke itd. (kao što su redundantni mrežni uređaji, poslužitelji koji se nalaze iza sustava za raspodjelu opterećenja, raid polja diskova, servisi za pričuvne kopije, više podatkovnih centara)

– imovina, uključujući objekte, opremu i zalihe

– korištenje alternativnih i redundantnih izvora napajanje električnom energijom

12.6. provoditi vježbe upravljanja kibernetičkim krizama kako bi se testirala otpornost subjekta na situacije koje nije moguće predvidjeti i planirati, a uzimajući u obzir:

– uloge i odgovornosti zaposlenika, kako bi se osiguralo da svi zaposlenici budu upoznati sa svojim ulogama u kriznim situacijama, uključujući konkretne korake koje je potrebno pratiti

– primjerene mjere komunikacije između subjekta i relevantnih nadležnih tijela

– održavanje uspostavljene razine kibernetičke sigurnosti u kriznim situacijama kroz primjenu primjerenih mjera, poput sustava i procesa za podršku i uspostavu dodatnog kapaciteta

UVJET: Mjera 12.6. se provodi kao obvezujuća na zahtjev nadležnih tijela u okviru provedbi vježbi kibernetičkog kriznog upravljanja.

12.7. implementirati redundanciju za kritične mrežne i informacijske sustave i kritične podatke. Prilikom implementacije subjekt mora razmotriti opcije ulaganja u vlastitu redundanciju ili angažman treće strane da pruži potrebnu redundanciju i to dokumentirati. Redundanciju je potrebno razmotriti djelomično ili u potpunosti za:

– mrežne i informacijske sustave, primjerice hardver, softver, servise, podatke itd. (kao što su redundantni mrežni uređaji, poslužitelji koji se nalaze iza sustava za raspodjelu opterećenja, raid polja diskova, servisi za pričuvne kopije, više podatkovnih centara)

– imovina, uključujući objekte, opremu i zalihe

– zaposlenike s nužnim odgovornostima, ovlastima i sposobnostima

– odgovarajuće komunikacijske kanale

– ključne komunalne usluge

12.8. koristiti redundantne podatkovne centre na lokacijama na kojima je vjerojatnost pojave istih ugroza geografske lokacije manji. Subjekt mora provesti procjenu rizika geografske lokacije koristeći se dostupnim podacima (primjerice potresnim zonama). Procjena rizika mora biti dokumentirana. Na osnovu procjene rizika potrebno je definirati i implementirati odabir i način korištenja različitih podatkovnih centara uzimajući u obzir pozitivne zakonske propise. Subjekt može provesti analizu je li trošak korištenja redundantnog podatkovnog centra veći od mogućih gubitaka u slučaju njegova nekorištenja. U tom slučaju osobe odgovorne za upravljanje mjerama mogu sukladno procesu upravljanja rizicima prihvatiti rizik.

Mjere 12.1 do 12.8. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere							
	12.1.	12.2.	12.3.	12.4.	12.5.	12.6.	12.7.	12.8.
osnovna	A	A	A	A	C	B	C	C
srednja	A	A	A	A	A	B	A	C
napredna	A	A	A	A	A	B	A	A

13. Fizička sigurnost

Cilj: Cilj je uspostaviti mjere za sprječavanje i nadziranje neovlaštenog fizičkog pristupa mrežnim i informacijskim sustavima subjekta, kako bi subjekt zaštitio te sustave od moguće štete i smetnji uzrokovanih fizičkim prijetnjama.

Subjekt će u okviru provedbe ove mjere provoditi sljedeće podskupove mjera:

13.1. sukladno rizicima unutar svog eko-sustava razviti i implementirati politiku fizičke sigurnosti. Politika minimalno treba odrediti opseg primjene, razine zaštite pojedinih prostora, načine primjene, odgovorne osobe i redovitost provjere djelotvornosti mjera. Politika, kao i promjene politike, moraju biti komunicirane sa svim zaposlenicima i relevantnim pravnim osobama s kojima subjekt ima poslovni odnos

13.2. osigurati osnovne fizičke mjere zaštite kao što su odgovarajuće fizičke barijere, brave, sigurnosne kamere i kontrole pristupa. Za definirane sigurnosne perimetre u kojima se nalaze mrežni i informacijski sustavi i druga povezana oprema, potrebno je postaviti tehničku zaštitu kako bi se osigurao pristup prostorima ovisno o procjeni rizika subjekta, uzimajući u obzir potencijalnu kritičnost mrežnog i informacijskog sustava i kritičnost programske i sklopovske imovine koja se u tom prostoru nalazi

13.3. redovito pregledavati i ažurirati sigurnosne protokole za fizičke lokacije. Sigurnosne protokole za sprečavanje neovlaštenog pristupa potrebno je uspostaviti za kritične mrežne i informacijske sustave s ciljem smanjenja rizika. Sigurnosni protokoli moraju pratiti kritičnost mrežnih i informacijskih sustava na koje se odnose

13.4. implementirati naprednije mjere fizičke zaštite koje osiguravaju jasnu evidenciju pristupa te mogu biti korištene za naknadnu digitalnu forenziku. Subjekt mora implementirati naprednije mjere fizičke zaštite sukladno svojoj procjeni rizika i u smislu omogućavanja razmjene podataka sa drugim sustavima za nadzor (sustav upravljanja zapisima) kako bi se jednoznačno mogli pohranjivati podaci o pristupima te omogućiti analizu tijekom nadzora ili incidenta

13.5. sukladno procjeni rizika subjekta, implementirati nadzor prostora s kritičnom programskom i sklopovskom imovinom u stvarnom vremenu.

Mjere 13.1 do 13.5. primjenjuju se u cijelosti i na IT i na OT dio mrežnih i informacijskih sustava subjekta.

Raspodjela podskupova mjere po razinama mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe:

Razina	Podskupovi mjere				
	13.1.	13.2.	13.3.	13.4.	13.5.
osnovna	A	A	A	C	C
srednja	A	A	A	A	C
napredna	A	A	A	A	A

PRILOG III.

POSEBNE MJERE FIZIČKE SIGURNOSTI ZA SUBJEKTE IZ SEKTORA DIGITALNE INFRASTRUKTURE

Cilj: Cilj ovih mjera je spriječiti i nadzirati mogućnost neovlaštenog fizičkog pristupa perimetru i objektima u kojima se nalaze mrežni i informacijski sustavi koje subjekti iz sektora digitalna infrastruktura iz Priloga I. Zakona koriste u svom poslovanju, kao i spriječiti moguću štetu i smetnje na njihovim mrežnim i informacijskim sustavima, uzrokovane namjernim, nenamjernim i prirodnim fizičkim prijetnjama.

Ključni i važni subjekti iz sektora digitalna infrastruktura iz Priloga I. Zakona dužni su provoditi sljedeće mjere fizičke sigurnosti:

1. Izraditi plan fizičke sigurnosti koji mora sadržavati:

– procjenu rizika fizičke sigurnosti kao dio procjene rizika koju subjekt provodi u okviru provedbe mjere naziva »Upravljanje rizicima« iz točke 3. Priloga II. ove Uredbe

– određivanje prostora subjekta koje je potrebno štititi i utvrđivanje razine fizičke sigurnosti koju je za svaki takav prostor potrebno osigurati, uvažavajući specifičnosti prostora za smještaj mrežnog i informacijskih sustava

– odabir mjera fizičke sigurnosti za vanjski perimetar, objekte i prostore u kojima su smješteni kritični mrežni i informacijski sustavi subjekta

– popis prava pristupa objektima i prostorima iz alineje 2. ove točke i obveze i odgovornosti zaposlenika subjekta, djelatnika osiguranja, vanjskih suradnika i posjetitelja

– plan provođenja periodičkog testiranja fizičke sigurnosti, vodeći računa da se ono mora provoditi najmanje jednom godišnje u sklopu procjene rizika iz alineje 1. ove točke

– način provedbe redovnog održavanja sustava fizičke sigurnosti.

Dodatno, u odnosu na svaki od prostora s različitom razinom potrebne fizičke sigurnosti, planom fizičke sigurnosti utvrđuju se sljedeći elementi fizičke sigurnosti:

– kontrola pristupa osoba, ovlaštenja pristupa zaposlenika, djelatnika osiguranja, vanjskih suradnika i posjetitelja pojedinom prostoru

– oprema za provedbu mjera fizičke sigurnosti koja se ugrađuje u pojedini prostor

– plan djelovanja djelatnika osiguranja ili vanjskih interventnih timova u odnosu na pojedini prostor.

2. Koristiti višestruke mjere fizičke sigurnosti na svakoj lokaciji koja se štiti. Uvođenjem višestrukih mjera fizičke sigurnosti potrebno je osigurati njihovo međusobno nadopunjavanje, pri čemu se može postaviti više sustava iste ili slične namjene, a sve u cilju smanjenja vjerojatnosti ostvarenja fizičkih prijetnji. Uspostava višestrukih mjera provodi se utvrđivanjem lokacije koju treba zaštititi, određivanjem vanjskog perimetra, perimetra objekta i perimetara pojedinih prostora unutar objekta s različitom razinom fizičke sigurnosti. Vanjske mjere fizičke sigurnosti primjenjuju se na vanjskom perimetru, njima se definiraju granice vanjskog prostora koji se štiti i te mjere moraju odvraćati od neovlaštenog pristupa. Mjerama fizičke sigurnosti koje se primjenjuju unutar prostora koji se štiti mora se osigurati utvrđivanje mogućih pokušaja neovlaštenog pristupa, o čemu se istovremeno obavještavaju djelatnici osiguranja te se pohranjuju zapisi o svim ostvarenim pristupima takvim prostorima. Mjerama fizičke sigurnosti koje se uspostavljaju najbliže prostorima s mrežnim i informacijskim sustavima subjekta mora se dodatno usporiti odnosno onemogućiti neovlašteni pristup do dolaska djelatnika osiguranja ili interventnih timova na mjesto, ali i osigurati zapise o boravku ovlaštenih osoba u pojedinom prostoru za slučaj istrage.

3. Potrebno je fizički jasno odvojiti prostor koji predstavlja vanjski perimetar pod kontrolom subjekta od javne površine ili druge površine s kojom graniči. Na vanjskom perimetru moraju se postaviti jasna upozorenja o zabrani ulaska za neovlaštene osobe. Subjekt mora osigurati pristup kroz vanjski perimetar za vozila i osobe, pri čemu mora utvrditi i prostor za isporuku opreme, kao i prostor za uvođenje vanjskih suradnika i drugih posjetitelja. Unutarnji prostori objekta u kojem subjekt ima smještene mrežne i informacijske sustave moraju biti odgovarajuće podijeljeni na prostore u kojima je moguć ulazak vanjskih suradnika i drugih posjetitelja i prostore koji su isključivo za korištenje zaposlenika ili samo za određenu kategoriju zaposlenika. Ulazak vozila, vanjskih suradnika i drugih posjetitelja mora biti obuhvaćen odgovarajućim mjerama kontrolnog pregleda i biti u skladu s pravilima subjekta o mogućnosti unosa tehničke opreme vanjskih suradnika i posjetitelja ili privatne tehničke opreme zaposlenika subjekta u pojedine prostore s različitom razinom fizičke sigurnosti.

4. Provoditi kontrolu pristupa korištenjem mehaničkih, elektroničkih ili proceduralnih načina te korištenjem kombinacije tih načina. Mehaničku kontrolu pristupa potrebno je temeljiti na uporabi sigurnosnih brava i sigurnosnih ključeva na vratima štićenih prostora. Elektroničku kontrolu pristupa potrebno je temeljiti na uporabi automatskog sustava kontrole pristupa koji koristi neku vrstu digitalnih kartica i pina ili biometrije. Proceduralnu kontrolu pristupa potrebno je temeljiti na uspostavi kontrolnih točaka s djelatnicima osiguranja smještenima na pogodnim mjestima na prilazu vanjskom perimetru ili ulazu u objekt subjekta. Kontrolu pristupu potrebno je provoditi za sve prostore subjekta neposrednim uvidom u sigurnosne propusnice koji obavljaju djelatnici osiguranja ili drugim načinom jednoznačnog identificiranja osobe (automatski sustav kontrole pristupa), uz odgovarajući način vođenja evidencije o pristupu. Otkrivanje neovlaštenog pristupa potrebno je provoditi zbog omogućavanja učinkovite i pravovremene reakcije na pokušaj

neovlaštenog pristupa unutar vanjskog perimetra ili unutar objekata subjekta, kao i u svrhu naknadne analize u cilju utvrđivanja počinitelja takvih radnji. Otkrivanje neovlaštenog pristupa potrebno je provoditi na različite načine, ovisno o utvrđenoj razini fizičke sigurnosti pojedinog prostora. Otkrivanje neovlaštenog pristupa potrebno je provoditi korištenjem djelatnika osiguranja, vanjskim interventnim timovima ili uporabom različitih elektroničkih sustava, odnosno kombinacijom ovih mjera.

5. Na odgovarajući način zaštititi pohranu kritičnih podataka subjekta, koja obuhvaća podatke u fizičkom i elektroničkom obliku, vodeći računa da pohrana podataka vezanih za pružanje usluga iz sektora digitalne infrastrukture iz Priloga I. Zakona u pravilu obuhvaća podatke u elektroničkom obliku. Fizičku zaštitu kritičnih podataka u fizičkom obliku potrebno je provoditi korištenjem odgovarajućih sigurnosnih spremnika smještenih u prostorijama s odgovarajućom razinom mjera fizičke sigurnosti ili korištenjem prostora za otvorenu pohranu kritičnih podataka, bez sigurnosnih spremnika, ali s uspostavljenom odgovarajućom razinom mjera fizičke sigurnosti za takve prostorije. Fizičku zaštitu kritičnih podataka u elektroničkom obliku potrebno je provoditi fizičkom zaštitom prostora u kojima su smješteni mrežni i informacijski sustavi koje subjekti iz sektora digitalna infrastruktura iz Priloga I. Zakona koriste u svom poslovanju, a posebno u kojima je smještena osjetljiva klijentska računalna oprema. Subjekt je dužan utvrditi pravila pristupa osoba za sve prostore u kojima se pohranjuju kritični podaci, pravila unošenja tehničke opreme, kao i pravila unošenja i korištenja privatne tehničke opreme zaposlenika u pojedinim prostorima s različitim zahtjevima fizičke sigurnosti.

6. Prostore u kojima se nalaze poslužitelji i druga oprema za upravljanje mrežnim i informacijskim sustavima subjekta potrebno je organizirati kao posebno nadzirane prostore, u koje pravo pristupa imaju samo osobe nadležne za sigurnost i administriranje takvih sustava, odnosno osoblje za održavanje, ali isključivo kada je u stalnoj pratnji osoba nadležnih za sigurnost subjekta i administriranje takvih sustava. Pristup takvim prostorima mora se štititi odgovarajućim sustavom za kontrolu pristupa te sustavima za otkrivanje neovlaštenog pristupa. Klijentska računalna oprema koja je osjetljiva na neovlašteni fizički pristup smješta se u prostore koji imaju odgovarajuću razinu mjera fizičke sigurnosti te se ona mora i koristiti u takvim prostorima, odnosno pod kontrolom nadležnog zaposlenika subjekta. Za osobe odgovorne za upravljanje mjerama, kao i osobe odgovorne za sigurnost i administriranje mrežnih i informacijskih sustava subjekta, subjekt je dužan pribaviti podatke o nekažnjavanju tih osoba, odnosno odgovarajuću potvrdu o nekažnjavanju i dotične podatke periodično ažurirati, najmanje svakih pet godina.

PRILOG IV.

IZJAVA O SUKLADNOSTI
USPOSTAVLJENIH MJERA UPRAVLJANJA
KIBERNETIČKIM SIGURNOSNIM RIZICIMA

PODACI O SUBJEKTU	
NAZIV	
ADRESA	
SEKTOR PODSEKTOR VRSTA SUBJEKTA	
SEKTOR GLAVNA POSLOVNA DJELATNOST	

SAMOPROCJENA KIBERNETIČKE SIGURNOSTI	
UTVRĐENA RAZINA KIBERNETIČKIH SIGURNOSNIH RIZIKA	
RAZINA MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA KOJA JE UTVRĐENA OBVEZUJUĆOM	
UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	
UKUPNI BODOVI TRENDA PODIZANJA RAZINE ZRELOSTI	
POPIS DOKUMENTACIJE	
IME, PREZIME I POTPIS OSOBE KOJA JE PROVELA POSTUPAK SAMOPROCJENE	

IZJAVA O SUKLADNOSTI	
Rezultati provedene samoprocjene kibernetičke sigurnosti za subjekt pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti.	
IME, PREZIME I POTPIS OSOBE ODGOVORNE ZA UPRAVLJANJE MJERAMA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA	

2218

Na temelju članka 30. stavka 2. Zakona o Vladi Republike Hrvatske (»Narodne novine«, br. 150/11., 119/14., 93/16., 116/18., 80/22. i 78/24.), Vlada Republike Hrvatske je na sjednici održanoj 21. studenoga 2024. donijela

UREDBU

O MJERAMA RACIONALIZACIJE RADI UBRZANJA REALIZACIJE TRANSEUROPSKE PROMETNE MREŽE (TEN-T)

Članak 1.

Ovom Uredbom uređuju se postupci izdavanja dozvola koji su potrebni za odobravanje provedbe:

a) projekata koji su dio prethodno utvrđenih dionica osnovne mreže, kako je navedeno u Prilogu ove Uredbe i koji čini njezin sastavni dio

b) drugih projekata na koridorima osnovne mreže, kako je utvrđeno na temelju članka 11. stavka 1. Uredbe (EU) 2024/1679 Europskog parlamenta i Vijeća od 13. lipnja 2024. o smjernicama Unije za razvoj transeuropske prometne mreže, izmjeni Uredbe (EU) 2021/1153 i Uredbe (EU) br. 913/2010 te stavljanju izvan snage Uredbe (EU) br. 1315/2013 (SL L 2024/1679, 28. 6. 2024.) (u daljnjem tekstu: Uredba (EU) 2024/1679), čiji ukupni trošak prelazi iznos od 300.000.000,00 eura, uz iznimku projekata koji se odnose isključivo na telematske aplikacije, nove tehnologije i inovacije u smislu članaka 43. i 45. Uredbe (EU) 2024/1679.

Članak 2.

Ovom Uredbom u hrvatsko zakonodavstvo preuzima se Direktiva (EU) 2021/1187 Europskog parlamenta i Vijeća od 7. srpnja