ZAVOD ZA SIGURNOST
INFORMACIJSKIH SUSTAVA

Prilog B – Okvir za evaluaciju mjera upravljanja kibernetičkim sigurnosnim rizicima

Verzija: 1.0

Sadržaj

Uvod

Ovaj dokument pruža sustavni okvir za provođenje postupka samoprocjene sukladno članku 51. Uredbe o kibernetičkoj sigurnosti („Narodne novine“, broj: 135/24, u daljnjem tekstu Uredba), te čini sastavni dio Smjernica za provedbu samoprocjene kibernetičke sigurnosti.

Svrha ovog dokumenta je definiranje uvjeta za provođenje samoprocjene i utvrđivanje stupnja usklađenosti pojedinih mjera kao i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta, a sve sukladno člancima od 51. do 54. Uredbe, te Prilogu II. Uredbe.

Svaka kontrola koncipirana je da obuhvati specifične aspekte pojedine mjere, čime se osigurava visoka razina preglednosti i jasnoće pri procjeni usklađenosti subjekta s propisanim mjerama upravljanja kibernetičkim sigurnosnim rizicima koje su definirane člankom 42. i Prilogom II. Uredbe.

Kontrole su strukturirane kako bi omogućile sustavan i dosljedan pristup pri procjeni ispunjavanja zahtjeva na različitim razinama implementacije: osnovnoj, srednjoj i naprednoj - u skladu s odredbama članka 42. i Priloga II. Uredbe.

Metode ocjenjivanja

Svaka mjera sastoji se od više mjera iz podskupa mjere (u daljnjem tekstu podmjera), a za svaku podmjeru propisanu Uredbom sastavljen je odgovarajući set kontrola. Setovi kontrola uključuju nazive kontrola detaljno opisanih u Prilogu C - Katalog kontrola, kao i razine mjera. Svaka razina mjere (osnovna, srednja i napredna) ima propisanu minimalnu ocjenu koju subjekt mora zadovoljiti kako bi se mogla uzimati u prosjek.

Sustav ocjenjivanja podmjera temelji se na ispunjavanju uvjeta pojedinačnih kontrola i ukupne ocjene podmjere za odgovarajuću razinu. Svaka kontrola ima postavljen minimalni bodovni prag ocjene (P_i) koji mora biti ispunjen kako bi se smatrala zadovoljenom. Na primjer, ako je bodovni prag za određenu kontrolu definiran kao „≥2“, subjekt mora ostvariti ocjenu (O_i) jednaku ili veću od 2 kako bi zadovoljio taj kriterij i prošao pojedinačnu kontrolu. Ocjena se dodjeljuje sukladno smjernicama za ocjenjivanje propisanim u Prilogu C - Katalog kontrola.

Za prolazak podmjere nije dovoljno ispuniti samo pojedinačne bodovne pragove ocjena kontrola, već prosječna ocjena svih kontrola također mora zadovoljiti unaprijed definirani ukupni bodovni prag (T). Ako prosječna ocjena svih kontrola ne ispunjava ukupni bodovni prag, smatra se da podmjera nije ispunila kriterije za prolaz, bez obzira na pojedinačne rezultate kontrola.

Iako pojedinačne ocjene za sve kontrole mogu biti zadovoljene, dodatni bodovni prag uveden je kako bi se osiguralo da subjekt u praksi postiže odgovarajuću razinu kibernetičke sigurnosti, a ne samo formalno zadovoljava pojedinačne kriterije. Dodatni bodovni prag stoga služi kao završna provjera koja omogućava procjenu stvarne primjene i integracije svih kontrola u svrhu postizanja cilja mjere. Ako se utvrdi da, unatoč formalnom ispunjavanju uvjeta pojedinačnih kontrola mjera u svojoj suštini nije djelotvorna ili nije dovoljno integrirana u sustav upravljanja rizicima subjekta, takva mjera se može ocijeniti kao nezadovoljavajuća.

U nastavku je prikazana univerzalna formula koja opisuje uvjete za prolaz subjekta uzimajući u obzir pojedinačne bodovne pragove (P_i) za svaku kontrolu (O_i) i dodatni bodovni prag prosječne ocjene (T):

$$(O_i \geq P_i, \forall i) \ \wedge \left(\frac{\sum_{i=0}^{n} O_i}{n} \geq T\right)$$

O_i – ocjena subjekta za *i*-tu kontrolu
P_i – bodovni prag za prolaz za *i*-tu kontrolu
T – dodatni bodovni prag za prosjek svih ocjena
n – ukupan broj kontrola

Mjera 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.

tbl 1.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-001	≥3	≥4	≥4
ORG-001	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	> 3.5	≥ 4.0

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.

tbl 2.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-001	≥2	≥3	≥4
EDU-002	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.5	> 4.0

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.

tbl 3.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RES-001	≥2	≥4	5
RES-003	≥3	≥4	5
EDU-006	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	> 4.0	> 4.5

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.

tbl 4.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
ORG-001	≥3	≥4	≥4
ORG-002	-	≥3	5
BODOVNI PRAG	≥ 3.0	≥ 3.5	≥ 4.5

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).

tbl 5.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
POL-002	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 6.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
ORG-003	≥2	≥4	5
BODOVNI PRAG	≥2.0	≥4.0	5.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 7.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-012	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

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.

tbl 8.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-001	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 9.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
EDU-001	≥2	≥4	5
EDU-003	≥2	≥3	5
EDU-004	-	≥2	≥3
BODOVNI PRAG	> 2.0	> 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 10.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
UPR-001	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 11.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
NAD-002	≥2	≥4	≥4
NAD-003	≥2	≥3	≥4
NAD-004	≥2	≥2	≥3
BODOVNI PRAG	> 2.0	> 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 12.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
INV-001	≥2	≥4	≥4
INV-002	≥2	≥3	≥4
INV-003	≥2	≥3	≥4
INV-004	≥3	≥4	≥4
BODOVNI PRAG	≥ 2.5	≥ 4.0	> 4.0

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.

tbl 13.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
INV-004	≥3	≥4	≥4
INV-005	≥3	≥3	≥4
BODOVNI PRAG	> 3.0	> 3.5	≥ 4.0

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).

tbl 14.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POD-001	≥2	≥3	≥4
INV-002	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.5	≥ 4.0

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.

tbl 15.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POD-003	≥3	≥3	≥4
POD-004	≥2	≥3	≥4
KRIP-004	-	≥2	≥4
BODOVNI PRAG	> 2.5	≥ 3.0	> 4.0

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.

tbl 16.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
INV-006	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

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).

tbl 17.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
INV-007	≥2	≥3	≥4
RIZ-008	-	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.5

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 18.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
INV-004	≥3	≥4	≥4
INV-008	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	≥ 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 19.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
POD-005	≥3	≥3	≥4
POD-006	≥2	≥4	≥4
POD-007	≥3	≥4	5
BODOVNI PRAG	≥ 3.0	≥ 4.0	≥ 4.3

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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*).

tbl 20.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
INV-009	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 21.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-006	≥2	≥4	≥4
EDU-005	-	≥2	≥4
BODOVNI PRAG	≥ 2.0	> 3.0	> 4.0

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*).

tbl 22.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
INV-004	≥3	≥3	≥4
RIZ-001	≥2	≥4	≥4
RIZ-002	≥2	≥4	≥4
RIZ-003	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	> 3.5	> 4.0

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.

tbl 23.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-004	≥2	≥3	≥4
RIZ-005	-	≥2	≥4
BODOVNI PRAG	≥ 2.0	≥ 2.5	≥ 4.0

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.

tbl 24.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-006	-	≥3	≥4
RIZ-007	≥3	≥3	≥4
POL-001	-	≥4	≥4
BODOVNI PRAG	≥ 3.0	> 3.5	> 4.0

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.

tbl 25.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-009	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

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.

tbl 26.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
RIZ-004	≥3	≥3	≥4
RIZ-007	≥2	≥3	≥4
RIZ-010	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	> 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 27.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
RIZ-011	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 28.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-012	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	≥ 4.0	≥ 4.0

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

Mjera 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.

tbl 29.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-001	≥2	≥3	≥4
EDU-002	-	≥2	≥3
ORG-001	≥3	≥4	≥4
ORG-002	-	≥4	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.0

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.

tbl 30.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RES-004	≥2	≥3	≥4
ORG-001	≥3	≥4	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.0

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.

tbl 31.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-001	≥2	≥3	5
EDU-003	≥2	≥3	≥4
EDU-006	-	≥2	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.0	≥ 4.5

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.

tbl 32.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-001	≥2	≥4	≥4
EDU-003	≥2	≥3	≥4
EDU-006	-	≥2	≥4
EDU-007	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.5	≥ 4.0

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.

tbl 33.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
ORG-001	≥3	≥4	≥4
ORG-004	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.0

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.

tbl 34.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-001	≥2	≥3	≥4
DID-002	-	≥3	≥4
BODOVNI PRAG	≥ 2.0	> 3.0	> 4.0

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 „poslovne potrebe" (*need-to-know*), „minimalno potrebnih ovlaštenja za provedbu zadaća" (*least privilege*) te „razdvajanja nadležnosti" (*segregation of duties*).

tbl 35.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
ORG-001	≥3	≥4	≥4
ORG-002	≥2	≥3	≥4
ORG-005	≥3	≥4	≥4
POL-002	-	≥3	≥4
BODOVNI PRAG	≥ 3.0	> 3.5	> 4.0

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.

tbl 36.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-001	≥2	≥3	≥4
DID-003	≥3	≥4	5
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.5

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.

tbl 37.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
EDU-006	≥2	≥3	≥4
EDU-008	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	> 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 38.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
EDU-003	≥3	≥3	≥4
EDU-009	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 39.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
EDU-003	≥3	≥4	5
EDU-007	≥2	≥3	≥4
EDU-010	-	≥3	≥4
BODOVNI PRAG	≥ 2.5	> 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 40.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
DID-003	≥2	≥3	≥4
DID-004	≥2	≥3	5
DID-005	≥2	≥3	≥4
DID-006	-	≥3	≥4
POL-002	-	≥4	≥4
BODOVNI PRAG	> 2.0	≥ 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 41.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-007	≥2	≥3	≥4
POL-008	≥3	≥3	≥4
BODOVNI PRAG	≥ 2.5	> 3.0	≥ 4.0

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 zaštite, 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.

tbl 42.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-004	≥2	≥3	≥4
POL-005	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	≥ 3.0	≥ 4.0

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.

tbl 43.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-007	≥2	≥4	≥4
POL-004	≥2	≥3	≥4
POL-005	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	> 3.5	> 4.5

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.

tbl 44.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RES-002	≥3	≥4	5
NAD-002	-	≥2	≥4
SKM-001	-	≥3	≥3
SKM-002	≥2	≥3	≥4
RIZ-003	-	≥3	≥4
RIZ-010	-	≥2	≥3
BODOVNI PRAG	> 2.0	≥ 3.0	> 4.0

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.

tbl 45.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-010	-	≥2	≥4
RIZ-013	≥2	≥3	≥4
SKM-003	≥2	≥4	5
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.5

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.

tbl 46.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
NAD-002	-	≥3	≥4
NAD-012	≥2	≥3	≥4
NAD-013	≥2	≥3	5
EDU-011	-	≥2	≥3
DID-006	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

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.

tbl 47.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
SRZ-001	≥2	≥3	≥4
SKM-005	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 48.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-004	≥2	≥3	≥4
SKM-004	≥3	≥4	5
SKM-005	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	≥ 3.5	> 4.0

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.

tbl 49.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-015	≥2	≥3	≥4
NAD-016	≥2	≥3	≥4
RIZ-002	≥2	≥3	≥4
DID-006	≥3	≥4	≥4
BODOVNI PRAG	≥ 2.5	> 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 50.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-005	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 51.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-006	≥3	≥3	5
SKM-008	-	≥2	≥4
ORG-005	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.).

tbl 52.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-007	≥2	≥4	5
BODOVNI PRAG	≥ 2.0	≥ 4.0	5.0

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).

tbl 53.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
NAD-008	≥2	≥3	≥4
DID-008	≥3	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.0	≥ 4.0

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.

tbl 54.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
NAD-014	≥2	≥3	≥4
RIZ-004	≥2	≥3	5
BODOVNI PRAG	> 2.0	≥ 3.0	≥ 4.5

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.

tbl 55.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-003	-	≥2	≥3
NAD-004	-	≥2	≥3
NAD-009	≥2	≥4	5
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

tbl 56.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
NAD-002	≥2	≥3	≥4
NAD-003	-	≥3	≥4
NAD-009	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	> 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 57.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-001	-	≥2	≥4
DID-003	-	≥3	≥4
DID-005	≥2	≥3	≥4
ORG-005	≥2	≥3	≥4
RIZ-001	≥2	≥4	5
RIZ-003	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	> 4.0

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.

tbl 58.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
ORG-005	≥3	≥3	≥4
DID-003	-	≥4	5
DID-009	≥2	≥3	5
NAD-012	-	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.5

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.

tbl 59.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-003	≥3	≥4	5
BODOVNI PRAG	≥ 3.0	≥ 4.0	5.0

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.

tbl 60.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
DID-010	≥3	≥4	5
ORG-005	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	≥ 4.0	≥ 4.5

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

tbl 61.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
DID-011	≥2	≥3	5
RIZ-001	≥2	≥3	≥4
RIZ-002	-	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 62.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
NAD-002	≥2	≥3	≥4
NAD-010	≥2	≥3	≥4
NAD-013	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 63.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-003	-	≥3	≥4
RIZ-014	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.5	≥ 4.0

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.

tbl 64.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-003	≥2	≥3	≥4
RIZ-015	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

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.

tbl 65.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-016	≥2	≥3	5
BODOVNI PRAG	≥ 2.0	≥ 3.0	5.0

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.

tbl 66.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
RIZ-014	≥3	≥4	≥4
RIZ-017	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	≥ 4.0	≥ 4.0

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.

tbl 67.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
RIZ-004	≥2	≥3	≥4
RIZ-014	≥3	≥4	≥4
RIZ-018	≥2	≥4	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 68.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
POL-009	≥2	≥3	≥4
RIZ-015	-	≥3	≥4
EDU-008	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 69.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
SRZ-002	≥2	≥3	≥4
SRZ-003	≥2	≥3	≥4
RIZ-010	-	≥2	≥3
BODOVNI PRAG	≥ 2.5	> 2.5	> 3.5

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.

tbl 70.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
SKM-006	≥3	≥3	≥4
BODOVNI PRAG	≥ 3.0	≥ 3.0	≥ 4.0

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.

tbl 71.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
SKM-006	≥3	≥3	≥4
SKM-007	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.0	≥ 4.0

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.

tbl 72.

	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
SRZ-001	≥2	≥3	≥4
SRZ-002	-	≥3	≥4
SRZ-003	≥2	≥3	≥4
NAD-007	≥2	≥3	≥4
SKM-005	≥2	≥3	≥3
BODOVNI PRAG	≥ 2.0	> 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 73.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
SRZ-001	≥2	≥3	≥4
SRZ-003	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 74.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
SRZ-001	≥2	≥4	5
SRZ-003	≥2	≥4	5
SKM-006	≥3	≥4	≥4
SKM-007	≥3	≥4	≥4
BODOVNI PRAG	≥ 2.5	≥ 4.0	≥ 4.5

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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 mjere					
	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

Mjera 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.

tbl 75.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
KRIP-001	≥2	≥3	≥4
RIZ-004	≥3	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.0	≥ 4.0

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.

tbl 76.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
KRIP-002	≥2	≥3	≥4
RIZ-004	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.0

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.

tbl 77.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
KRIP-003	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.0	≥ 3.0	≥ 4.0

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.

tbl 78.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
KRIP-004	≥2	≥3	≥4
RIZ-004	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.0

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.

tbl 79.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
KRIP-001	≥4	≥4	≥4
BODOVNI PRAG	≥ 4.0	≥ 4.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

tbl 80.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA***
KRIP-005	≥2	≥3	≥4
RIZ-004	≥3	≥4	5
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.5

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 81.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-009	≥2	≥3	≥4
POL-010	≥3	≥3	≥4
ORG-001	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.0

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.

tbl 82.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-010	≥3	≥4	≥4
POL-011	≥2	≥3	5
UPR-003	≥2	≥3	≥4
UPR-004	≥2	≥3	5
UPR-005	≥2	≥3	5
UPR-006	≥2	≥3	≥4
UPR-007	≥3	≥4	≥4
UPR-008	≥2	≥3	≥4
UPR-009	≥2	≥4	≥4
UPR-010	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.2	≥ 3.3	≥ 4.3

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.

tbl 83.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
EDU-007	≥3	≥4	5
EDU-008	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.5

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.

tbl 84.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-010	≥3	≥4	≥4
UPR-003	≥2	≥3	≥4
UPR-008	≥2	≥3	≥4
UPR-010	≥3	≥4	5
UPR-011	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	> 4.0

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.

tbl 85.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
POL-010	≥3	≥4	≥4
UPR-009	≥2	≥4	≥4
UPR-012	≥3	≥4	5
EDU-008	≥3	≥4	5
BODOVNI PRAG	> 3.5	≥ 4.0	≥ 4.5

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 86.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
NAD-002	≥2	≥3	≥4
NAD-003	-	≥3	≥4
NAD-011	≥3	≥3	≥4
NAD-012	-	≥3	≥4
UPR-011	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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 identificira ti 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.

tbl 87.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
ORG-001	≥2	≥4	≥4
EDU-008	-	≥2	≥3
UPR-002	≥2	≥3	≥4
UPR-018	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	≥ 4.0

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.

tbl 88.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
UPR-004	≥2	≥3	≥4
ORG-006	≥2	≥3	≥4
RIZ-004	≥2	≥3	5
BODOVNI PRAG	> 2.0	> 3.0	> 4.0

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.

tbl 89.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
UPR-008	≥2	≥3	≥4
UPR-014	≥2	≥3	≥4
UPR-015	-	≥3	≥4
ORG-001	≥2	≥3	≥4
EDU-008	-	≥2	≥3
BODOVNI PRAG	> 2.0	≥ 3.0	≥ 4.0

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.

tbl 90.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
UPR-016	≥2	≥3	≥4
UPR-017	≥2	≥3	≥4
ORG-006	≥2	≥3	≥4
RIZ-004	-	≥3	5
POD-002	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.0	> 4.0

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.

tbl 91.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
UPR-005	-	≥3	≥4
UPR-008	≥2	≥3	≥4
UPR-013	≥3	≥4	5
ORG-007	≥3	≥4	≥4
POD-002	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	≥ 3.5	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 92.

	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
UPR-006	≥2	≥3	≥4
UPR-013	-	≥3	≥4
UPR-014	≥2	≥3	≥4
UPR-015	≥2	≥3	≥4
POL-011	≥3	≥4	≥4
EDU-008	-	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.2	> 4.0

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.

tbl 93.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
ORG-003	-	≥3	≥4
RES-005	≥2	≥3	≥4
RES-006	≥2	≥3	≥4
RES-007	-	≥3	≥4
RES-008	≥3	≥4	≥4
RES-009	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	> 3.0	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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.

tbl 94.	**RAZINE MJERE**		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
RIZ-010	-	≥3	≥4
RIZ-019	≥2	≥3	≥4
RES-005	≥2	≥4	≥4
RES-006	≥2	≥3	≥4
BODOVNI PRAG	> 2.0	≥ 3.5	> 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

Mjera 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.

tbl 95.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-003	≥3	≥4	≥4
ORG-001	≥2	≥3	≥4
BODOVNI PRAG	≥ 2.5	≥ 3.5	≥ 4.0

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.

tbl 96.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-003	≥3	≥4	≥4
RIZ-001	≥3	≥4	≥4
FIZ-001	≥2	≥3	≥4
BODOVNI PRAG	> 2.5	> 3.5	> 4.0

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.

tbl 97.	RAZINE MJERE		
KONTROLA	**OSNOVNA**	**SREDNJA**	**NAPREDNA**
POL-003	≥3	≥4	≥4
RIZ-001	≥3	≥4	≥4
FIZ-002	≥4	≥4	5
BODOVNI PRAG	> 3.0	≥ 4.0	> 4.0

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.

tbl 98.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA**	**NAPREDNA**
POL-003	≥3	≥4	≥4
RIZ-001	≥3	≥4	≥4
FIZ-003	≥2	≥3	≥3
NAD-012	-	≥3	≥4
BODOVNI PRAG	> 2.5	≥ 3.5	> 3.5

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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

tbl 99.	RAZINE MJERE		
KONTROLA	**OSNOVNA***	**SREDNJA***	**NAPREDNA**
RIZ-001	≥3	≥4	≥4
FIZ-004	≥3	≥4	≥4
BODOVNI PRAG	≥ 3.0	≥ 4.0	≥ 4.0

* kontrole podmjera se ocjenjuju samo u slučaju kada je podmjera dobrovoljno uključena sukladno lokalnoj procjeni rizika

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