REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Ključne politike EU na področju kibernetske varnosti

URSIV

KLJUČNE POLITIKE EU NA PODROČJU KIBERNETSKE VARNOSTI

Politike – Zakonodaja – Mehanizmi

KAZALO

I. KROVNI EVROPSKI PRAVNI OKVIR

Krovni evropski pravni okvir za kibernetsko varnost (Direktiva NIS2, Akt o kibernetski varnosti, Akt o kibernetski odpornosti, Akt o kibernetski solidarnosti) določa splošna horizontalna pravila, ki veljajo za vse države članice in širok krog zavezancev.

Akt o kibernetski varnosti

- *Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013*

Ta uredba, z namenom, da bi zagotovili pravilno delovanje notranjega trga in obenem dosegli visoko raven kibernetske varnosti, kibernetske odpornosti in zaupanja v Uniji, določa cilje, naloge in organizacijske zadeve, povezane z Agencijo Evropske unije za kibernetsko varnost (agencija ENISA), ter okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za namene zagotavljanja ustrezne ravni kibernetske varnosti za proizvode IKT, storitve IKT in postopke IKT v Uniji, pa tudi za namene preprečevanja razdrobljenosti notranjega trga v zvezi s certifikacijskimi shemami za kibernetsko varnost v Uniji.

- Glej: Zakon o informacijski varnosti (ZInfV-1)

Uredba za vzpostavitev Evropskega kompetenčnega centra

- *Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov*

Ta uredba vzpostavlja Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost ter Mrežo nacionalnih koordinacijskih centrov. Določa pravila za imenovanje nacionalnih koordinacijskih centrov in pravila za vzpostavitev kompetenčne skupnosti za kibernetsko varnost.

- Glej: Zakon o informacijski varnosti (ZInfV-1)

Direktiva NIS2

- *Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2)*

Ta direktiva določa ukrepe, katerih cilj je zagotoviti visoko skupno raven kibernetske varnosti v Uniji, da bi se izboljšalo delovanje notranjega trga. V ta namen ta direktiva določa: obveznosti, ki od držav članic zahtevajo, da sprejmejo nacionalne strategije za kibernetsko varnost in imenujejo ali ustanovijo pristojne organe, organe za obvladovanje kibernetskih kriz, enotne kontaktne točke za kibernetsko varnost in skupine za odzivanje na incidente na področju računalniške varnosti, ukrepe za obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja za subjekte vrste iz Priloge I ali II, kot tudi za subjekte, ki so identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557, pravila in obveznosti glede izmenjave informacij o kibernetski varnosti, obveznosti nadzora in izvrševanja za države članice.

Direktiva NIS2 si prizadeva za standardizacijo kibernetske varnosti po vsej Evropski uniji. Uporablja se za 18 kritičnih sektorjev. Njen glavni cilj je zaščititi bistveno infrastrukturo pred kibernetskimi grožnjami z uvedbo ukrepov za obvladovanje tveganj za bistvene in pomembne subjekte.

- Glej: Zakon o informacijski varnosti (ZInfV-1)

Uredba EUIBAs

- *Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije*

Ta uredba določa ukrepe, katerih cilj je doseči visoko skupno raven kibernetske varnosti v subjektih Unije v zvezi z: notranjim okvirom za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti na podlagi člena 6, ki ga vzpostavi vsak subjekt Unije; obvladovanjem tveganj za kibernetsko varnost, poročanjem in izmenjavo informacij; organizacijo in delovanjem Medinstitucionalnega odbora za kibernetsko varnost, ustanovljenega na podlagi člena 10, ter organizacijo in delovanjem Službe za kibernetsko varnost za institucije, organe, urade in agencije Unije; spremljanjem izvajanja te uredbe.

Akt o kibernetski odpornosti

- *Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (Besedilo velja za EGP)*

Ta uredba ima dva glavna cilja za zagotovitev ustreznega delovanja notranjega trga: (1) ustvariti pogoje za razvoj varnih izdelkov z digitalnimi elementi z zagotavljanjem, da se na trg dajejo izdelki strojne in programske opreme z manj ranljivostmi in da proizvajalci v celotnem življenjskem ciklu izdelka resno obravnavajo vprašanje varnosti, ter (2) ustvariti pogoje, ki uporabnikom omogočajo upoštevanje kibernetske varnosti pri izbiri in uporabi izdelkov z digitalnimi elementi. Oblikovani so bili štirje specifični cilji: (i) zagotoviti, da proizvajalci izboljšujejo varnost izdelkov z digitalnimi elementi že od faze zasnove in razvoja ter v celotnem življenjskem ciklu izdelka; (ii) zagotoviti skladen okvir kibernetske varnosti, s čimer se olajša zagotavljanje skladnosti za proizvajalce strojne in programske opreme; (iii) izboljšati preglednost varnostnih lastnosti izdelkov z digitalnimi elementi ter (iv) podjetjem in potrošnikom omogočiti varno uporabo izdelkov z digitalnimi elementi.

Akt o kibernetski solidarnosti

- *Uredba (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov er pripravo in odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti)*

Uredba ima cilj okrepiti skupno odkrivanje kibernetskih groženj in incidentov v EU in situacijsko zavedanje o njih ter tako prispevati k evropski tehnološki suverenosti na področju kibernetske varnosti; okrepiti pripravljenost kritičnih subjektov po vsej EU in solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetsko varnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore pri odzivanju na incidente tretjim državam, pridruženim programu Digitalna Evropa; povečati odpornost Unije in prispevati k učinkovitemu odzivu s pregledovanjem in ocenjevanjem pomembnih incidentov ali incidentov velikih razsežnosti, med drugim z uporabo pridobljenih spoznanj in po potrebi priporočil. Ti cilji se uresničujejo z naslednjimi ukrepi: vzpostavitvijo vseevropske infrastrukture centrov za varnostne operacije (Evropski sistem za opozarjanje glede kibernetske varnosti) za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje; vzpostavitvijo mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetsko varnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih. Podpora za odzivanje na incidente se omogoči tudi evropskim institucijam, organom, uradom in agencijam Unije; vzpostavitvijo evropskega mehanizma za pregledovanje kibernetsko varnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih incidentov ali incidentov velikih razsežnosti.

- Glej: Zakon o informacijski varnosti (ZInfV-1)

II. SEKTORSKI EU AKTI

Poleg krovnega evropskega pravnega okvira za kibernetsko varnost EU sprejema sektorske pravne akte, saj imajo številni sektorji, zaradi posebnih tveganj, infrastrukture ali reguliranih storitev, dodatne zahteve. EU s sektorskimi pravnimi akti dopolnjuje krovno zakonodajo in določa konkretne organizacijske, tehnične ter varnostne standarde za posamezna področja. Sektorski akti zagotavljajo, da se splošni okvir EU na področju kibernetske varnosti dejansko prilagodi posebnostim posameznih panog.
Za Slovenijo to pomeni, da mora URSIV kot nacionalni organ za kibernetsko varnost zagotoviti učinkovito usklajevanje z drugimi resorji (MOPE, MF, MZ, MGRT, MGTŠ ipd.).

Primeri sektorskih EU aktov, ki dopolnjujejo krovne akte:

1. Omrežni kodeks za elektroenergetska podjetja
   - *Delegirana uredba Komisije (EU) 2024/1366 vzpostavlja sektorska pravila za kibernetsko varnost čezmejnih pretokov električne energije.*
   - *Delegirana uredba - EU - 2024/1366 - SL - EUR-Lex*

Uredba podrobno določa organizacijske in tehnične ukrepe za obravnavo incidentov v elektroenergetskem sektorju. Gre za sektorska pravila za vidike kibernetske varnosti čezmejnih pretokov električne energije, vključno s pravili o skupnih minimalnih zahtevah, načrtovanju, spremljanju, poročanju in obvladovanju kriz.

2. Evropski odbor za sistemska tveganja (finance)
   - *Priporočilo Odbora za sistemska tveganja z dne 2. decembra 2021 o vseevropskem okviru za usklajevanje v primeru sistemskih kibernetskih incidentov za ustrezne organe*
   - *C_2022134SL.01000101.xml*

Priporočilo odbora za sistemska tveganja predvideva vzpostavitev okvira vseevropskega okvira za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF) za usklajevanje ob sistemskih kibernetskih incidentih v finančnem sektorju. ESRB priporočilo (2021) je opozorilo na potrebo po vseevropskem okviru za krizno usklajevanje, DORA (2022) pa je to potrebo pravno uresničila z vzpostavitvijo zavezujočega okvira za digitalno odpornost in krizno koordinacijo v finančnem sektorju EU.

3. Evropski zdravstveni podatkovni prostor (EHDS)
   - *Mnenje Evropskega ekonomsko-socialnega odbora – Sporočilo Komisije Evropskemu parlamentu in Svetu – Evropski zdravstveni podatkovni prostor: izkoriščanje moči zdravstvenih podatkov za ljudi, paciente in inovacije (COM(2022) 196 final) – Predlog uredbe Evropskega parlamenta in Sveta o evropskem zdravstvenem podatkovnem prostoru (COM(2022) 197 final – 2022/0140 (COD))*
   - *https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX:52022AE2531*

Evropski zdravstveni podatkovni prostor (EHDS), ki ga je Komisija predstavila leta 2022, je osrednja pobuda Evropske zdravstvene unije in prvi sektorski podatkovni prostor v okviru širše EU strategije za podatke. Njegov namen je omogočiti ljudem večji nadzor nad lastnimi zdravstvenimi podatki, zagotoviti njihovo varno primarno uporabo (za zdravstveno oskrbo) in sekundarno uporabo (za raziskave, inovacije, oblikovanje politik), ter pospešiti interoperabilnost in digitalizacijo zdravstvenih sistemov. Predlog uredbe (COM(2022) 197) določa pravni in tehnični okvir, vključno z vzpostavitvijo evropskih in nacionalnih organov za dostop do podatkov. EHDS je tesno povezan z obstoječimi pravnimi in političnimi instrumenti, kot so GDPR, Data Governance Act, Data Act, NIS2, program EU4Health in pobuda DARWIN EU, ter s tem krepi digitalno odpornost in inovacije v evropskem zdravstvenem prostoru. Organi za kibernetsko varnost so neposredno vključeni v koordinacijo varstva podatkov in odpornosti

zdravstvenih informacijskih sistemov. Za Slovenijo je odgovorno MZ, pri čemer je URSIV predviden v koordinacijski funkciji.

4. Notranji trg za plin in vodik (ENNOH)
    - *Uredba (EU) 2024/1789 Evropskega parlamenta in Sveta z dne 13. junija 2024 o notranjem trgu plina iz obnovljivih virov, zemeljskega plina in vodika, spremembi uredb (EU) št. 1227/2011, (EU) 2017/1938, (EU) 2019/942 in (EU) 2022/869 ter Sklepa (EU) 2017/684 in razveljavitvi Uredbe (ES) št. 715/2009 (prenovitev)*
    - *https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32024R1789*

Uredba (EU) 2024/1789 vzpostavlja Evropsko mrežo operaterjev vodikove infrastrukture (ENNOH), ki bo usklajevala razvoj in upravljanje čezmejne vodikove infrastrukture v EU. Njena naloga je priprava desetletnih razvojnih načrtov, oblikovanje tehničnih pravil ter sodelovanje z obstoječimi energetskimi omrežji (ENTSO-E, ENTSOG) za integrirano načrtovanje. Posebno mesto imajo tudi kibernetski vidiki, saj je varnost in odpornost vodikove infrastrukture proti kibernetskim grožnjam ključna za zanesljivo delovanje energetskega sistema.

Komisija je pooblaščena za sprejem delegiranih aktov, ki določajo **minimalne zahteve za kibernetsko varnost čezmejnih tokov plina in vodika**. Vključujejo se načrti za krizno upravljanje in zaveze držav članic, da vključujejo kibernetsko varnost v akcijske načrte.

5. Letalstvo
    - *Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (Besedilo velja za EGP)*
    - *https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=celex:32008R0300*

Skupna pravila za varovanje civilnega letalstva: Uredba (ES) 300/2008 vzpostavlja skupne osnovne standarde varnosti za civilno letalstvo, ki jih morajo upoštevati vsi civilni letališki objekti, letalske družbe ter povezani subjekti in storitve v EU. Ta pravilnik določa postopke za nadzor izvajanja varnostnih ukrepov, kot so pregled potnikov in prtljage, nadzor dostopa, pregled vozil in osebja, ter nadzor prometa z namenom preprečevanja nedovoljenega vstopa in sabotaže.

- *Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (Besedilo velja za EGP.)*
- *https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:32018R1139*

Osnovni pravilnik za letalstvo in vzpostavitev EASA: Uredba (EU) 2018/1139 določa visoko in enotno ravnijo varnosti v civilnem letalstvu po vsej EU. Uredba vzpostavlja Agencijo Evropske unije za varnost v letalstvu (EASA), ki koordinira tehnična pravila, nadzoruje skladnost in zagotavlja enotno izvajanje zakonodaje v letalskih operacijah, upravljanju zrakoplovov, usposabljanju osebja, sistemih nadzora zračnega prometa ter varnosti zaščite okolja in odziva v kriznih razmerah.

6. RED Direktiva (Telekomunikacije, radijska oprema)
    - *Delegirana uredba Komisije (EU) 2022/30 z dne 29. oktobra 2021 o dopolnitvi Direktive 2014/53/EU Evropskega parlamenta in Sveta v zvezi z uporabo bistvenih zahtev iz člena 3(3), točke (d), (e) in (f), navedene direktive*
    - *https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A02022R0030-20231027*

Uredba (EU) 2022/30 nadgrajuje **RED direktivo** z jasnimi **kibernetskimi zahtevami** za radijsko opremo, ki se povezuje na internet ali obdeluje osebne podatke ali omogoča finančne transakcije. Delegirana uredba je namenjena okrepitvi kibernetske varnosti in zasebnosti v okviru RED direktive. S tem uvaja posebno pozornost zaščiti omrežij, uporabnikovih osebnih podatkov in finančnih transakcij preko radijske opreme.

Sektorska zakonodaja, ki izključuje uporabo Direktive NIS2

Akt o digitalni operativni odpornosti

- *UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011*
- *https://eur-lex.europa.eu/legal-content/sl/ALL/?uri=CELEX:32022R2554*

Uredba DORA uvaja enoten okvir za digitalno operativno odpornost finančnih subjektov in njihovih ICT-storitev. Uredba določa enotne zahteve za varnost omrežij in informacijskih sistemov podjetij in organizacij, ki delujejo v finančnem sektorju, ter ključnih tretjih strani, ki jim zagotavljajo storitve, povezane z IKT (informacijske komunikacijske tehnologije), kot so platforme v oblaku ali storitve podatkovne analitike. Vzpostavlja regulativni okvir za digitalno operativno odpornost, pri čemer morajo vsa podjetja zagotoviti, da lahko vzdržijo vse vrste motenj in groženj, povezane z IKT, ter se nanje odzovejo in si opomorejo. Te zahteve so enotne v vseh državah članicah EU. Glavni cilj je preprečiti in ublažiti kibernetske grožnje. Akt je v pristojnosti MF, ki je pripravil Uredbo o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor.

Uredba DORA predstavlja specifičen sektorski akt, saj je posebej zasnovana za finančni sektor. Velja za 21 vrst finančnih subjektov, od bank in zavarovalnic do podjetij, ki zagotavljajo digitalne finančne storitve, pa tudi za ključne ponudnike storitev IKT, ki podpirajo ta sektor. Za razliko od Direktive NIS2 Uredba DORA uvaja podrobne zahteve za upravljanje tveganj IKT in testiranje operativne odpornosti. V bistvu zagotavlja, da lahko finančne institucije ohranijo poslovanje tudi v primeru sofisticiranih kibernetskih napadov.

Za razumevanje povezave med NIS2 in DORA je pomembno razumeti ključno pravno načelo: lex specialis. To se nanaša na zakon, ki ima prednost pred splošnejšim zakonom, kadar se oba uporabljata za isto področje. V tem primeru je DORA lex specialis glede na Direktivo NIS2 znotraj finančnega sektorja. Kljub temu dejstvo, da ima DORA prednost v finančnem sektorju, ne pomeni, da so obveznosti NIS2 za nekatere subjekte popolnoma nepomembne. Nekateri specifični vidiki NIS2 se lahko še vedno uporabljajo posredno – zlasti tisti, ki so povezani z zavarovanjem dobavnih verig ali kritične infrastrukture zunaj finančnega sektorja.

- Glej: Uredba o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor

III. EU MEHANIZMI IN AGENCIJE NA PODROČJU KIBERNETSKE VARNOSTI

1. **CERT-EU:** Računalniška odzivna enota za institucije EU. Odgovorna za odkrivanje, odzivanje in obveščanje glede incidentov v institucijah EU.

2. **Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost (Kompetenčni center) oz. t.i. European Cybersecurity Competence Centre (ECCC):** Glavno vozlišče za financiranje in koordinacijo raziskav ter inovacij. Povezano z mrežo nacionalnih koordinacijskih centrov.

3. **Agencija Evropske unije za kibernetsko varnost (ENISA):** Agencija EU za kibernetsko varnost. Podpira države članice, EK in zasebni sektor. Vodi pripravo analiz groženj, vaje (Cyber Europe) in razvoj politik.

4. **Evropski sistem za opozarjanje glede kibernetske varnosti:** To je vseevropska mreža infrastrukture, ki jo sestavljajo nacionalna kibernetska vozlišča in čezmejna kibernetska vozlišča, ki se prostovoljno pridružijo, imenovana evropski sistem za opozarjanje na področju kibernetske varnosti, da se podpre razvoj naprednih zmogljivosti Unije za okrepitev zmogljivosti odkrivanja, analiziranja in obdelave podatkov v zvezi s kibernetskimi grožnjami in preprečevanjem incidentov v Uniji. Vzpostavljena mreža nacionalnih in čezmejnih SOC-centrov omogoča zgodnje zaznavanje kibernetskih groženj ter skupno situacijsko zavedanje v EU. Sistem zagotavlja tudi sprotno opozarjanje držav in institucij o resnih incidentih. S tem se krepi odpornost EU proti čezmejnim grožnjam, omogoča hitrejši in usklajen odziv ter spodbuja solidarnost z izmenjavo informacij v enotnem opozorilnem okviru.

5. **Evropska certifikacijska skupina za kibernetsko varnost – European Cybersecurity Certification Group (ECCG):** Evropska certifikacijska skupina za kibernetsko varnost (ECCG) je skupina nacionalnih organov, pristojnih za certificiranje kibernetske varnosti, ustanovljena z Uredbo (EU) 2019/881. Namen skupine je usklajeno izvajanje evropskega certifikacijskega okvira: svetuje Evropski komisiji, podpira ENISA pri pripravi in vzdrževanju evropskih certifikacijskih shem ter skrbi, da se pravila uporabljajo enotno po vseh državah članicah.

6. **Medinstitucionalni odbor za kibernetsko varnost – Interinstitutional Cybersecurity Board (IICB):** Medinstitucionalni odbor za kibernetsko varnost (IICB) je organ, ustanovljen z Uredbo (EU, Euratom) 2023/2841, ki združuje predstavnike institucij EU za usklajevanje področja kibernetske varnosti. Namen IICB je spremljati izvajanje uredbe, zagotavljati strateško usmeritev in koordinacijo med institucijami, spodbujati dosledno upravljanje kibernetskih tveganj ter pripravljati letna poročila o stanju kibernetske varnosti v institucijah EU.

7. **NIS Skupina za sodelovanje – NIS Cooperation group:** NIS Skupina za sodelovanje je platforma, ki povezuje države članice, Komisijo in ENISA za usklajevanje izvajanja Direktive NIS2. Namenjena je za svetovanje, izmenjavo praks, ocenjevanje tveganj, podporo pri zakonodaji in krepitev pripravljenosti EU na kibernetske grožnje.

8. **Mreža skupin CSIRT – CSIRTs Network:** Mreža skupin CSIRT je panevropsko telo, sestavljeno iz nacionalnih CSIRT-ov in CERT-EU, z ENISA kot tajništvom in Komisijo kot opazovalko. Namen Mreže skupin CSIRT je povečevanje zaupanja in koordinirane operativne odzivnosti med državami članicami skozi izmenjavo informacij, usklajevanje odzivov na incidente, obravnavanje ranljivosti ter krepitev skupne situacijske zavesti.

9. **Evropska organizacijska mreža za povezovanje v kibernetski krizi (mreža EU-CyCLONe) - Cyber Crises Liaison Organisation Network:** EU-CyCLONe je panevropska mreža predstavnikov nacionalnih organov, odgovornih za obvladovanje kibernetskih kriz. Formalno je ustanovljena z določbo člena 16 Direktive (EU) 2022/2555 (NIS2), z ENISA kot sekretariatom

in Komisijo kot opazovalko ali aktivnim udeležencem v primeru večjih incidentov. Namen EU-CyCLONe je usklajevanje operativnega odzivanje na velike čezmejne kibernetske incidente in krize. Ključne vloge vključujejo: dvig pripravljenosti za krizne razmere, vzpostavitev skupnega situacijskega zavedanja, oceno posledic incidentov in predlog ublažitvenih ukrepov, koordinacijo odziva in podporo političnim odločitvam, razpravo o nacionalnih načrtih odziva na kibernetske incidente po potrebi.
Omrežje redno poroča o svojem delu Evropskemu parlamentu in Svetu vsakih 18 mesecev.

10. **Nacionalni koordinacijski center (NCC):** Nacionalni koordinacijski center je javna institucija ali večinsko v državnem lastništvu delujoča organizacija, pooblaščena za povezovanje z Evropskim industrijskim, tehnološkim in raziskovalnim kompetenčnim centrom (ECCC) ter drugimi nacionalnimi centri. NCC ima dostop ali poseduje strokovno znanje na področju kibernetske varnosti in je sposobna učinkovito sodelovati z industrijo, javnim sektorjem, akademsko in raziskovalno skupnostjo ter državljani. Nacionalni koordinacijski centre (NCC) so vzpostavljeni z namenom:
    - Spodbujanja raziskav, inovacij in industrijskega razvoja na področju kibernetske varnosti, zlasti v okviru programov *Digitalna Evropa* in *Obzorje Evropa*.
    - Krepitev sodelovanja med nacionalnimi akterji (industrija, javni sektor, raziskovalna in akademska skupnost) znotraj posamezne države ter s povezanostjo na evropski ravni.
    - Podpora ECCC – z zagotavljanjem tehnične pomoči, dostopa do strokovnega znanja, organizacije ozaveščevalnih dejavnosti ter povezovanja deležnikov pri pripravi projektov.