Svet
Evropske unije

Bruselj, 31. oktober 2022
(OR. en)

14128/22

Medinstitucionalna zadeva:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

DOPIS O TOČKI POD „I/A“

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	Odbor stalnih predstavnikov (2. del)/Svet
Št. predh. dok.:	10097/5/22 REV 5
Št. dok. Kom.:	7474/22 + ADD 1
Zadeva:	Predlog uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije – splošni pristop

UVOD

1. Komisija je 22. marca 2022 sprejela Predlog uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije. Predlog je bil eden od ukrepov, predvidenih v strategiji EU za kibernetsko varnost v digitalnem desetletju[1], katere cilj je okrepiti skupno odpornost Unije proti kibernetskim grožnjam.

[1] 14133/20.

Svet je v sklepih z dne 22. marca 2021 o tej strategiji[2] poudaril, da je kibernetska varnost bistvena za delovanje javne uprave in institucij na nacionalni ravni in ravni EU ter za našo družbo in gospodarstvo kot celoto.

2. Cilj predloga Komisije, ki temelji na členu 298 Pogodbe o delovanju Evropske unije, je z vzpostavitvijo skupnega okvira, ki bo ustrezno upošteval avtonomijo vsakega subjekta Unije, izboljšati raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije. Cilji predloga so zlasti:

   – okrepiti mandat in financiranje CERT-EU (avtonomna medinstitucionalna skupina za odzivanje na računalniške grožnje za subjekte Unije);

   – vzpostaviti medinstitucionalno strukturo (Medinstitucionalni odbor za kibernetsko varnost – IICB), ki bo združevala predstavnike vseh subjektov Unije, da se zagotovi ustrezno izvajanje uredbe;

   – uvesti obveznost za subjekte Unije, da izmenjujejo (netajne) informacije o incidentih s CERT-EU ter poročajo o pomembnih grožnjah, ranljivostih in incidentih, ter

   – spodbujati usklajevanje in sodelovanje pri odzivanju na večje incidente.

3. Evropski parlament je za poročevalko pristojnega odbora, tj. odbora ITRE, imenoval Henno Virkkunen (EPP). Osnutek poročila je bil objavljen 7. oktobra 2022.

4. Evropski nadzornik za varstvo podatkov je mnenje predložil 17. maja 2022[3].

[2] 6722/21.
[3] 9252/22.

5. V Svetu je Horizontalna delovna skupina za kibernetska vprašanja predlog začela preučevati med francoskim predsedovanjem 29. marca 2022. Francosko predsedstvo je pripravilo prvo kompromisno besedilo, o katerem je zadevna delovna skupina razpravljala v juniju 2022, in nato 21. junija 2022 Svetu predložilo poročilo o napredku[4].

6. Med češkim predsedovanjem je Horizontalna delovna skupina za kibernetska vprašanja o predlogu in nadaljnjih kompromisnih besedilih razpravljala na osmih sejah[5].

7. Predsedstvo je 23. maja 2022 Varnostni odbor Sveta zaprosilo za mnenje o vidikih predloga, povezanih z varnostjo informacij in zlasti s tajnimi podatki. Varnostni odbor Sveta je mnenje dal 19. septembra 2022[6]. Kot je predlagal Varnostni odbor Sveta, so bili tajni podatki EU izrecno izključeni iz področja uporabe Uredbe. Določbe o izvzetju iz obveznosti izmenjave informacij in poročanja v zvezi s prejetimi informacijami, ki ne izhajajo iz subjektov Unije, so bile ustrezno spremenjene.

8. Horizontalna delovna skupina za kibernetska vprašanja je 28. oktobra 2022 dosegla dogovor o kompromisnem predlogu predsedstva iz priloge.

---

4 9719/22.
5 6. in 20. julija, 13., 21. in 28. septembra ter 5., 19. in 28. oktobra 2022.
6 12603/22 + COR 1.

GLAVNA VPRAŠANJA

9. Države članice so pozdravile predlog, ki je po njihovem mnenju pravočasen in dopolnjuje prihodnjo direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (revidirana direktiva o varnosti omrežij in informacij), ter podprle njegove splošne cilje. Vendar so pozvale k nadaljnjemu usklajevanju z revidirano direktivo o varnosti omrežij in informacij in k večji vzajemnosti pri izmenjavi informacij med subjekti Unije in državami članicami ter opozorile na pretirano prostovoljno naravo nekaterih predlaganih ukrepov. Zavzele so se tudi za črtanje sklicevanja na skupno kibernetsko enoto, katere mandat in sestava še nista opredeljena.

10. Na podlagi razprav Horizontalne delovne skupine za kibernetska vprašanja so bile kot glavna politična vprašanja opredeljene naslednje točke:

a) Uskladitev s prihodnjo revidirano direktivo o varnosti omrežij in informacij

Na zahtevo držav članic je bilo besedilo dodatno usklajeno s prihodnjo direktivo o varnosti omrežij in informacij, in sicer:

- več opredelitev pojmov (člen 3) je bilo usklajenih z opredelitvami iz revidirane direktive o varnosti omrežij in informacij;
- vstavljen je bil nov člen 7a o prostovoljnih medsebojnih strokovnih pregledih v skladu z revidirano direktivo o varnosti omrežij in informacij, prilagojen potrebam subjektov Unije;
- obveznosti poročanja iz člena 20 so bile usklajene z obveznostmi iz revidirane direktive o varnosti omrežij in informacij.

b) Sestava Medinstitucionalnega odbora za kibernetsko varnost (IICB) (člen 9)

Po razpravah o ustrezni vključitvi predstavnikov držav članic v delo IICB je bil dosežen kompromis v obliki izjave Sveta za zapisnik.

c) Institucionalna avtonomija

Dosežen je bil uravnotežen pristop med namenom držav članic, da okrepijo mehanizme skladnosti, in potrebo po spoštovanju načela institucionalne avtonomije, zlasti v zvezi z revizijami in disciplinskimi ukrepi (člen 11).

Nazadnje – iz uvodne izjave 8 je bilo črtano sklicevanje na določen odstotek proračuna za informacijsko tehnologijo, namenjenega kibernetski varnosti.

ZAKLJUČEK

11. Odbor stalnih predstavnikov naj:

(a) odobri kompromisno besedilo iz priloge, ki bo nato podlaga mandatu za pogajanja z Evropskim parlamentom;

(b) pozove Svet, naj na seji 18. novembra 2022 odobri priloženo kompromisno besedilo in v zapisnik vključi izjavo Sveta iz dodatka k temu dokumentu.

PRILOGA

2022/0085 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 298 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo in zlasti člena 106a Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) V digitalni dobi je informacijska in komunikacijska tehnologija temelj odprte, učinkovite in neodvisne uprave Unije. Razvijajoča se tehnologija ter vse večja kompleksnost in medsebojna povezanost digitalnih sistemov povečujejo tveganja za kibernetsko varnost, zaradi česar je uprava Unije ranljivejša za kibernetske grožnje in incidente, kar posledično ogroža neprekinjeno poslovanje uprave in zmogljivost zaščite podatkov. Večja uporaba storitev v oblaku, vsesplošna uporaba informacijskih tehnologij, visoka stopnja digitalizacije, delo na daljavo ter razvijajoča se tehnologija in povezljivost so danes ključne značilnosti vseh dejavnosti subjektov uprave Unije, vendar digitalna odpornost še ni zadostno vgrajena.

(2) Okolje kibernetskih groženj, ki so mu izpostavljeni [...] **subjekti** Unije, se nenehno razvija. Taktike, tehnike in postopki, ki jih uporabljajo akterji groženj, se nenehno razvijajo, očitni motivi za take napade pa se le malo spreminjajo in zajemajo krajo dragocenih nerazkritih informacij, služenje denarja, manipulacijo z javnim mnenjem ali ogrožanje digitalne infrastrukture. Akterji kibernetske napade izvajajo vse pogosteje, njihove kampanje pa so vse bolj izpopolnjene in avtomatizirane, usmerjene v izpostavljene napadne površine, ki se širijo, ter hitro izkoriščajo ranljivosti.

(3) Okolja IT [...] **subjektov** Unije so medsebojno povezana in imajo vgrajene podatkovne tokove, njihovi uporabniki pa tesno sodelujejo. Ta medsebojna povezava pomeni, da lahko ima vsaka motnja, tudi če je sprva omejena na en [...] **subjekt** Unije, širše kaskadne učinke, ki lahko imajo daljnosežne in dolgotrajne negativne posledice za druge. Poleg tega so okolja IT nekaterih [...]**subjektov Unije** povezana z okolji IT držav članic, kar pomeni, da incident v enem subjektu Unije ogroža kibernetsko varnost okolij IT držav članic in obratno. **Poleg tega subjekti Unije obdelujejo velike količine pogosto občutljivih informacij iz držav članic, zato bi lahko incidenti negativno vplivali tudi na države članice. Zato je kibernetska varnost subjektov Unije zelo pomembna tudi za države članice. Informacije o posameznih incidentih lahko poleg tega pomagajo pri odkrivanju podobnih kibernetskih groženj ali incidentov, ki zadevajo države članice.**

(4) [...] **Subjekti** Unije so privlačne tarče, ki jih ogrožajo visoko usposobljeni in dobro podprti akterji groženj in tudi druge grožnje. Hkrati pa se raven in zrelost kibernetske odpornosti ter sposobnost odkrivanja zlonamernih kibernetskih dejavnosti in odzivanja nanje med navedenimi subjekti močno razlikujejo. Zato je za delovanje evropske uprave nujno, da [...] **subjekti** Unije z **izvajanjem ukrepov za kibernetsko varnost,** [...] izmenjavo informacij in sodelovanjem dosežejo visoko skupno raven kibernetske varnosti.

(5) Cilj Direktive [predlog revidirane direktive o varnosti omrežij in informacij] o ukrepih za visoko skupno raven kibernetske varnosti v Uniji je nadalje izboljšati kibernetsko odpornost in zmogljivosti za odzivanje na incidente javnih in zasebnih subjektov, nacionalnih pristojnih organov in teles ter Unije kot celote. Zato morajo [...] **subjekti** Unije temu slediti, tako da zagotovijo pravila, ki so skladna z Direktivo [predlog revidirane direktive o varnosti omrežij in informacij] in odražajo njeno raven ambicij.

(6) Za doseganje visoke skupne ravni kibernetske varnosti je nujno, da vsak [...] **subjekt** Unije vzpostavi notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, ki zagotavlja učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost [...]. **Okvir bi moral določati politike kibernetske varnosti, vključno s postopki za oceno učinkovitosti izvedenih ukrepov za kibernetsko varnost. Okvir bi moral temeljiti na pristopu, ki upošteva vse nevarnosti in katerega cilj je zaščititi omrežje in informacijske sisteme ter njihovo fizično okolje pred dogodki, kot so kraja, požar, poplave, izpadi telekomunikacij ali električne energije, ali pred nepooblaščenim fizičnim dostopom in poškodbami ali poseganjem v informacije subjekta Unije in njegovo opremo za obdelavo informacij, ki bi lahko ogrozili razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov, ki se shranjujejo, prenašajo, obdelujejo ali so dostopni prek omrežja in informacijskih sistemov. Okvir bi moral odražati ugotovitve analize tveganja in pri tem upoštevati vsa zadevna tehnična, operativna in organizacijska tveganja za kibernetsko varnost zadevnega subjekta Unije.**

(6a) Za obvladovanje v tem okviru opredeljenih tveganj bi moral vsak subjekt Unije zagotoviti, da se sprejmejo ustrezni in sorazmerni tehnični, operativni in organizacijski ukrepi. Ti bi morali obravnavati področja, opredeljena v tej uredbi, vključno z ukrepi za kibernetsko varnost, da bi se okrepila kibernetska varnost vsakega subjekta Unije.

(6b) **Načrt za kibernetsko varnost, ki ga pripravi vsak subjekt Unije, bi moral upoštevati sredstva in tveganja, opredeljena v tem okviru, ter ugotovitve, ki izhajajo iz rednih ocen zrelosti. Načrt za kibernetsko varnost bi moral vključevati sprejete ukrepe za kibernetsko varnost, da bi se povečala splošna kibernetska varnost zadevnega subjekta Unije.**

(6c) **Ker je zagotavljanje kibernetske varnosti neprekinjen proces, bi bilo treba ustreznost in učinkovitost vseh ukrepov redno pregledovati glede na spreminjajoča se tveganja, sredstva in zrelost subjektov Unije. Okvir bi bilo treba pregledovati redno in vsaj vsaka tri leta, načrt za kibernetsko varnost pa bi bilo treba revidirati vsaj vsaki dve leti ali po vsaki oceni zrelosti ali vsakem pregledu okvira.**

(6d) **Subjekti Unije bi si morali redno izmenjevati ustrezne informacije, tudi v zvezi z zadevnimi incidenti in kibernetskimi grožnjami, pri tem pa zagotavljati zaupnost in ustrezno varstvo informacij, ki jih predloži subjekt Unije, ki poroča.**

(6e) **Uvesti bi bilo treba mehanizem za zagotavljanje učinkovite izmenjave informacij, usklajevanja in sodelovanja subjektov Unije v primeru večjih incidentov, vključno z jasno opredelitvijo vlog in odgovornosti vključenih subjektov Unije. Izmenjane informacije bi morala imenovana kontaktna točka za EU-CyCLONe upoštevati v okviru zadevnih informacij, ki se posredujejo mreži EU-CyCLONe kot prispevek k skupnemu situacijskemu zavedanju.**

(7) Zaradi razlik med [...] **subjekti** Unije je potrebna prožnost v izvajanju, saj ena rešitev ne bo primerna za vse. Ukrepi za visoko skupno raven kibernetske varnosti ne bi smeli vključevati obveznosti, ki bi neposredno posegale v opravljanje nalog [...] **subjektov** Unije ali posegale v njihovo institucionalno avtonomijo. Zato bi morali [...] **subjekti Unije** vzpostaviti lastne okvire za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost **ter načrte za kibernetsko varnost** in sprejeti [...] **ukrepe** [...] za kibernetsko varnost. **Pri izvajanju takih ukrepov bi bilo treba ustrezno upoštevati obstoječe sinergije med subjekti Unije, da bi zagotovili ustrezno upravljanje virov in optimizacijo stroškov. Pozornost bi bilo treba nameniti tudi temu, da ukrepi ne bodo negativno vplivali na učinkovito izmenjavo informacij in delovanje subjektov Unije z drugimi subjekti Unije in pristojnimi nacionalnimi organi.**

(8) Da [...] **subjektom** Unije ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetsko varnost sorazmerne s tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. Vsak [...] **subjekt** Unije bi si moral zaradi izboljšanja ravni kibernetske varnosti prizadevati, da se ustrezen delež proračuna dodeli za IT [...]. **Pri oceni zrelosti bi bilo treba oceniti tudi, ali je izdatek, ki ga subjekt Unije nameni za kibernetsko varnost, sorazmeren s tveganji, s katerimi se sooča.**

(9) Za visoko skupno raven kibernetske varnosti mora imeti nadzor nad kibernetsko varnostjo najvišja raven vodenja vsakega [...] **subjekta** Unije [...] **Najvišja raven vodenja bi morala nadzorovati izvajanje te uredbe, tudi vzpostavitev okvira za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost in načrtov za kibernetsko varnost, ki zajemajo ukrepe za kibernetsko varnost**. Obravnava kulture kibernetske varnosti, tj. dnevno izvajanje kibernetske varnosti, je sestavni del **okvira** kibernetske varnosti [...] v vseh [...] **subjektih** Unije.

(10) [...][...] Ukrepi **za kibernetsko varnost** bi morali biti del [...] **načrta** za kibernetsko varnost in podrobneje opredeljeni v smernicah ali priporočilih, ki jih izda CERT-EU. Pri pripravi ukrepov in smernic bi bilo treba ustrezno upoštevati **najnovejše in, kjer je ustrezno, zadevne evropske in mednarodne standarde ter** zadevno zakonodajo in politike EU, vključno z ocenami tveganja in priporočili skupine za sodelovanje na področju varnosti omrežij in informacij, kot sta usklajena ocena tveganja v EU in nabor orodij EU za kibernetsko varnost omrežij 5G. Poleg tega bi lahko bilo potrebno certificiranje ustreznih proizvodov, storitev in postopkov IKT, na podlagi specifičnih certifikacijskih shem za kibernetsko varnost EU, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881. **CERT-EU bi moral po potrebi sodelovati z agencijo ENISA.**

(11) Generalni sekretarji institucij in organov Unije so maja 2011 sklenili, da bodo ustanovili predkonfiguracijsko skupino za skupino za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (CERT-EU), ki jo bo nadziral medinstitucionalni usmerjevalni odbor. Julija 2012 so generalni sekretarji potrdili praktično ureditev in se dogovorili, da ohranijo CERT-EU kot stalno enoto, ki naj še naprej pomaga izboljševati splošno stopnjo varnosti informacijske tehnologije v institucijah, organih in agencijah Unije kot primer vidnega medinstitucionalnega sodelovanja na področju kibernetske varnosti. CERT-EU je bil septembra 2012 vzpostavljen kot projektna skupina Evropske komisije z medinstitucionalnimi pooblastili. Institucije in organi Unije so decembra 2017 sklenili medinstitucionalni dogovor o organizaciji in delovanju CERT-EU[7]. [...] Ta **uredba** bi morala [...] **zagotoviti celovit sklop pravil o organizaciji in delovanju CERT-EU. Določbe te uredbe prevladajo nad določbami medinstitucionalnega dogovora o organizaciji in delovanju CERT-EU, ki je bil sklenjen decembra 2017.**

[...]

[7] UL C 12, 13.1.2018, str. 1–11.

(13) Veliko kibernetskih napadov je del širših kampanj, usmerjenih v skupine [...] **subjektov** Unije ali interesne skupnosti, ki vključujejo [...] **subjekte** Unije. Da bi omogočili proaktivno odkrivanje, odzivanje na incidente ali blažilne ukrepe, bi morali [...] **subjekti** Unije CERT-EU uradno obvestiti o [...] kibernetskih grožnjah, [...] ranljivostih, **skorajšnjih dogodkih in** [...] incidentih ter deliti ustrezne tehnične podrobnosti, ki omogočajo odkrivanje ali blaženje podobnih kibernetskih groženj, **ranljivosti, skorajšnjih dogodkov in** incidentov ter odzivanje nanje v drugih **subjektih** [...] Unije. V skladu s pristopom, enakim tistemu, ki je predviden v Direktivi [predlog revidirane direktive o varnosti omrežij in informacij], bi morali subjekti **Unije**, ko se seznanijo s pomembnim incidentom, v 24 urah CERT-EU posredovati [...] **zgodnje opozorilo**. Taka izmenjava informacij bi morala CERT-EU omogočiti, da informacije posreduje drugim [...] **subjektom** Unije ter ustreznim sorodnim organom in tako prispeva k zaščiti okolij IT Unije in okolij IT sorodnih organov Unije pred podobnimi incidenti [...].

(13a) **Ta uredba določa večstopenjski pristop k poročanju o pomembnih incidentih, da bi se vzpostavilo ustrezno ravnovesje med – na eni strani – hitrim poročanjem, ki pomaga zajeziti morebitno širjenje pomembnih incidentov in omogoča subjektom Unije, da zaprosijo za pomoč, ter – na drugi strani – podrobnim poročanjem, ki omogoča pridobivanje dragocenih izkušenj iz posameznih incidentov ter sčasoma poveča kibernetsko odpornost posameznih subjektov Unije. V zvezi s tem bi morala ta uredba vključevati poročanje o incidentih, ki bi lahko na podlagi začetne ocene, ki jo izvede subjekt Unije, povzročili resne operativne motnje v delovanju subjekta Unije ali finančno izgubo za zadevni subjekt Unije ali povzročili znatno premoženjsko ali nepremoženjsko škodo drugim fizičnim ali pravnim osebam. Pri taki začetni oceni bi bilo treba med drugim upoštevati prizadeta omrežje in informacijske sisteme, zlasti njihov pomen za delovanje subjekta Unije, resnost in tehnične značilnosti kibernetske grožnje in vse ranljivosti, ki se izkoriščajo, ter izkušnje subjekta Unije s podobnimi incidenti. Kazalniki, kot so obseg tega, koliko je prizadeto delovanje subjekta Unije, trajanje incidenta ali število prizadetih fizičnih ali pravnih oseb, bi lahko imeli pomembno vlogo pri ugotavljanju, ali je operativna motnja resna.**

(13b) **Ker so infrastruktura in omrežja zadevnega subjekta Unije in države članice, v kateri se ta subjekt Unije nahaja, med seboj povezani, je bistveno, da je ta država članica nemudoma obveščena o pomembnem incidentu znotraj tega subjekta Unije. V ta namen bi moral prizadeti subjekt Unije uradno obvestiti nacionalni organ, ki je sorodni organ skupini CERT-EU in ga država članica imenuje v skladu z Direktivo [predlog revidirane direktive o varnosti omrežij in informacij], in sicer v enakem časovnem okviru, kot bi moral o pomembnem incidentu poročati skupini CERT-EU. CERT-EU bi moral ta nacionalni sorodni organ obvestiti tudi, ko izve za pomemben incident v državi članici, razen če je o njem že poročal prizadeti subjekt Unije.**

(14) Poleg tega, da se CERT-EU dodeli več nalog in razširjena vloga, bi moral biti ustanovljen tudi Medinstitucionalni odbor za kibernetsko varnost (IICB), ki bi moral **za namene lažjega doseganja visoke skupne ravni kibernetske varnosti med subjekti Unije** imeti **izključno vlogo** [...] [...] pri spremljanju, kako [...] **subjekti** Unije izvajajo to uredbo, in pri nadzorovanju tega, kako se izvajajo splošne prednostne naloge in cilji s strani CERT-EU in CERT-EU, ter pri zagotavljanju strateških usmeritev. IICB bi **zato** moral zagotoviti zastopanost institucij ter vključevati predstavnike agencij in organov prek mreže agencij Unije. **Organizacijo in delovanje IICB bi bilo treba dodatno urediti z notranjim poslovnikom, ki lahko vključuje podrobnejšo opredelitev rednih srečanj IICB, vključno z letnimi srečanji na politični ravni, na katerih bi predstavniki najvišje ravni vodenja vsakega člana IICB slednjemu omogočili, da opravi strateško razpravo in zagotovi strateške smernice za IICB. Poleg tega lahko IICB ustanovi izvršni odbor, ki mu pomaga pri delu, ter nanj prenese nekatere naloge in pooblastila, zlasti v zvezi z nalogami, ki zahtevajo [...] posebno strokovno znanje njegovih članov, na primer kar zadeva odobritev kataloga storitev in njegovih naknadnih posodobitev, načine izvajanja sporazumov o ravni storitev, ocene dokumentov in poročil, ki jih subjekti Unije predložijo IICB v skladu s to uredbo, ali naloge, povezane s pripravo odločitev o ukrepih za skladnost, ki jih izda IICB, in spremljanjem njihovega izvajanja. IICB bi moral določiti poslovnik izvršnega odbora, vključno z njegovimi nalogami in pooblastili.**

(15) CERT-EU bi moral izvajanje ukrepov za visoko skupno raven kibernetske varnosti podpirati s predlogi za smernice in priporočila, naslovljenimi na IICB, ali z izdajo pozivov k ukrepanju. Take smernice in priporočila bi moral odobriti IICB. CERT-EU bi moral po potrebi izdati pozive k ukrepanju, ki opisujejo nujne varnostne ukrepe, ki naj bi jih [...] **subjekti** Unije nujno sprejeli v določenem časovnem obdobju. **IICB lahko CERT-EU naroči izdajo, umik ali spremembo predloga za smernice ali priporočilo ali poziv k ukrepanju.**

(16) IICB bi moral spremljati skladnost s to uredbo ter nadaljnje ukrepanje na podlagi smernic, priporočil in pozivov k ukrepanju [...]. V zvezi s tehničnimi vprašanji bi ga bilo treba podpreti s tehničnimi svetovalnimi skupinami, ki so sestavljene, kot se IICB zdi ustrezno, in ki bi morale tesno sodelovati s CERT-EU, [...] **subjekti** Unije ter po potrebi z drugimi deležniki. [...] **Kadar IICB ugotovi, da subjekti Unije niso uporabljali ali izvajali te uredbe, vključno s smernicami, priporočili ali pozivi k ukrepanju, izdanimi na podlagi te uredbe, lahko brez poseganja v notranje postopke zadevnega subjekta Unije sprejme ukrepe za skladnost. Sistem ukrepov za skladnost bi bilo treba uporabljati s stopnjujočo se strogostjo ukrepov, kar pomeni, da bi moral IICB, ko sprejme ukrepe za skladnost, začeti z opozorilom kot najmanj strogim ukrepom in po potrebi ukrepe zaostrovati vse do najstrožjega ukrepa izdaje svetovalnega mnenja, s katerim se priporoči začasna prekinitev prenosa podatkov zadevnemu subjektu Unije, kar bi se uporabilo v izrednih primerih dolgoročnega, namernega in/ali resnega neizpolnjevanja obveznosti iz te uredbe s strani zadevnega subjekta.**

(16a) Opozorilo je najmanj strog ukrep za skladnost, ki odpravlja ugotovljene pomanjkljivosti subjekta Unije in vsebuje priporočila za spremembo njegovih dokumentov o kibernetski varnosti v določenem časovnem okviru. Opozorilo bi moralo biti dostopno vsem subjektom Unije, razen če je ustrezno omejeno v skladu s to uredbo.

(16b) IICB lahko poleg tega priporoča, da se izvede revizija subjekta Unije. Subjekt Unije lahko v ta namen uporabi funkcijo notranje revizije. IICB bi lahko zahteval tudi, da revizijo izvede neodvisna revizijska služba, tudi vzajemno dogovorjen ponudnik storitev iz zasebnega sektorja.

(16c) Na podlagi rezultatov revizije, izvedene na priporočilo ali zahtevo IICB, lahko IICB od subjekta Unije nadalje zahteva, da obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost uskladi z določbami te uredbe.

(16d) Ker države članice z ustreznimi subjekti Unije izmenjujejo informacije, ki so lahko občutljive narave, je kibernetska varnost naslovnika takih informacij ključnega pomena za države članice. Zato lahko IICB v izrednih primerih dolgoročnega, namernega, ponavljajočega se in/ali resnega neizpolnjevanja obveznosti subjekta Unije kot skrajni ukrep izda svetovalno mnenje, naslovljeno na vse države članice in subjekte Unije, s katerim priporoči začasno prekinitev prenosa podatkov subjektu Unije, ki bi morala trajati do izboljšanja stanja kibernetske varnosti tega subjekta. To svetovalno mnenje bi bilo treba sporočiti vsem državam članicam in subjektom Unije prek ustreznih varnih komunikacijskih kanalov.

(16e) **Za zagotovitev pravilnega izvajanja te uredbe bi moral IICB, če meni, da je subjekt Unije nadaljeval kršitve te uredbe neposredno zaradi dejanj ali opustitve dejanj člana njegovega osebja, tudi na najvišji ravni vodenja, od zadevnega subjekta Unije zahtevati, da sprejme ustrezne ukrepe proti temu članu osebja v skladu s kadrovskimi predpisi in drugimi enakovrednimi pravili, ki se uporabljajo v nekaterih subjektih Unije. Ti ukrepi lahko na primer vključujejo disciplinske postopke in po potrebi v posebnem primeru agencij Unije zahtevo pristojnemu organu, da sprejme potrebne ukrepe v zvezi z morebitno razrešitvijo osebe, ki bi lahko bila odgovorna za trajajočo kršitev te uredbe.**

(17) CERT-EU bi moral imeti nalogo prispevati k varnosti okolja IT vseh [...] **subjektov** Unije. **CERT-EU bi moral pri odločanju, ali naj na zahtevo subjekta Unije zagotovi tehnično svetovanje ali prispevek o ustreznih zadevah politike, zagotoviti, da to ne ovira izpolnjevanja njegovih drugih nalog iz te uredbe.**

(17a) CERT-EU bi moral imeti vlogo, enakovredno imenovanemu koordinatorju za [...] **subjekte** Unije, za namene usklajenega razkrivanja ranljivosti evropskemu registru ranljivosti iz člena 6 Direktive [predlog revidirane direktive o varnosti omrežij in informacij] **in bi moral oblikovati politiko o obvladovanju ranljivosti, ki bi zajemala spodbujanje in lajšanje prostovoljnega usklajenega razkrivanja ranljivosti.**

[...]

(19) CERT-EU bi moral tudi izpolnjevati vlogo, ki je zanj predvidena v Direktivi [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], v zvezi s sodelovanjem in izmenjavo informacij z mrežo skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT). Poleg tega bi moral CERT-EU v skladu s Priporočilom Komisije (EU) 2017/1584[8] sodelovati z zadevnimi deležniki in se z njimi usklajevati glede odzivanja. Za prispevanje k visoki ravni kibernetske varnosti v Uniji bi moral z nacionalnimi sorodnimi organi deliti informacije, povezane z incidenti. Prav tako bi moral sodelovati z drugimi javnimi in zasebnimi sorodnimi organi, tudi pri Natu, pri čemer sodelovanje predhodno odobri IICB.

[8] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

(20) Pri podpori operativni kibernetski varnosti bi moral CERT-EU prek strukturiranega sodelovanja izkoriščati razpoložljivo strokovno znanje Agencije Evropske unije za kibernetsko varnost **(ENISA)**, kot je predvideno v Uredbi (EU) 2019/881 Evropskega parlamenta in Sveta[9]. Po potrebi bi bilo treba sprejeti posebne dogovore med tema dvema subjektoma, s katerimi bi določili praktično izvajanje takega sodelovanja in se izogibali podvajanju dejavnosti. CERT-EU bi moral sodelovati [...] z agencijo **ENISA** v zvezi z analizo groženj in ji redno posredovati svoje poročilo o grožnjah.

[...]

(22) **Dejavnosti CERT-EU in njegovo ravnanje z informacijami v skladu s to uredbo lahko vključujejo obdelavo osebnih podatkov.** Vsi osebni podatki, obdelani na podlagi te uredbe, bi se morali obdelovati v skladu z zakonodajo o varstvu podatkov, vključno z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta[10]. **Kadar se osebni podatki v skladu s to uredbo posredujejo prejemnikom s sedežem v Uniji, ki niso subjekti Unije, bi bilo treba to storiti v skladu s členom 9 Uredbe (EU) 2018/1725.**

---

9 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 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

10 Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

(23) CERT-EU ter **subjekti** [...] Unije bi morali z informacijami ravnati v skladu z **veljavnimi** pravili [...] o informacijski varnosti.

(23a) Za izmenjavo informacij se uporabljajo vidne oznake, ki označujejo, da morajo prejemniki informacij zlasti na podlagi sporazumov o nerazkritju informacij ali neformalnih dogovorov o nerazkritju, kot je semaforski protokol, ali na podlagi drugih jasnih navedb s strani vira, upoštevati omejitve pri nadaljnjem širjenju informacij. Semaforski protokol je treba razumeti kot sredstvo za zagotavljanje informacij o morebitnih omejitvah v zvezi z nadaljnjim širjenjem informacij. Uporablja se v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (CSIRT) ter v nekaterih centrih za analizo in izmenjavo informacij.

(24) **Ta uredba in nove naloge, dodeljene CERT-EU, ne bodo vplivale na skupne odhodke v večletnem finančnem okviru.** Ker so storitve in naloge CERT-EU v interesu vseh [...] **subjektov** Unije, bi moral vsak [...] **subjekt** Unije z izdatki za IT prispevati pravičen delež k tem storitvam in nalogam. Taki prispevki ne posegajo v proračunsko avtonomijo [...] **subjektov** Unije. **Vsi subjekti Unije in njihove uprave bi morali zagotoviti optimizacijo svojih virov na sedanji ravni in še povečati učinkovitost, vključno s poglobitvijo medinstitucionalnega sodelovanja na področju kibernetske varnosti. Zato bi bilo treba namesto individualiziranim izdatkom s strani subjektov Unije prednost dati skupnemu pristopu k združevanju upravnih odhodkov.**

(25) IICB bi moral ob pomoči CERT-EU pregledati in oceniti izvajanje te uredbe ter Komisiji poročati o svojih ugotovitvah. Na podlagi tega prispevka bi morala Komisija poročati Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij. **Poleg tega je Evropsko računsko sodišče pozvano, naj redno ocenjuje delovanje CERT-EU –**

SPREJELA NASLEDNJO UREDBO:

Poglavje I
SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

1. Ta uredba določa **ukrepe, katerih cilj je doseči visoko skupno raven kibernetske varnosti v subjektih Unije** [...].

2. V ta namen ta uredba opredeljuje:

(c) obveznosti za **vsak subjekt** [...] Unije, v skladu s katerimi mora vzpostaviti okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost;

(d) obveznosti za **subjekte** [...] Unije glede obvladovanja tveganj za kibernetsko varnost, poročanja **in izmenjave informacij**;

(e) pravila o organizaciji in delovanju [...] **avtonomne medinstitucionalne skupine za odzivanje na računalniške grožnje** za **subjekte** [...] Unije (CERT-EU) ter o organizaciji in delovanju Medinstitucionalnega odbora za kibernetsko varnost **(IICB)**;

(f) pravila v zvezi s spremljanjem izvajanja te uredbe.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za [...] vse [...] **subjekte** Unije in za [...] [...] CERT-EU ter **IICB** [...].

2. Ta uredba se uporablja brez poseganja v institucionalno avtonomijo v skladu s Pogodbama.

3. Z izjemo člena 12(7) se ta uredba ne uporablja za omrežje in informacijske sisteme, s katerimi se obdelujejo tajni podatki EU (EUCI).

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „**subjekti** [...] Unije“ pomeni institucije, organe**, urade** in agencije Unije, ustanovljene s Pogodbo o Evropski uniji, Pogodbo o delovanju Evropske unije ali Pogodbo o ustanovitvi Evropske skupnosti za atomsko energijo ali na njihovi podlagi;

(2) „omrežje in informacijski sistem“ pomeni omrežje in informacijski sistem, [...] **kot sta opredeljena v** členu 4(1) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

(3) „varnost omrežij in informacijskih sistemov“ pomeni varnost omrežij in informacijskih sistemov, [...] **kot je opredeljeno v** členu 4(2) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

(4) „kibernetska varnost“ pomeni kibernetsko varnost, [...] **kot je opredeljena v členu 2, točka (1), Uredbe (EU) št. 2019/881;**

(5) „najvišja raven vodenja“ pomeni vodjo, vodstvo ali organ za usklajevanje in nadzor na najvišji upravni ravni, **ki lahko sprejema odločitve**, ob upoštevanju ureditev upravljanja na visoki ravni v vsakem [...] **subjektu** Unije;

(5a) „skorajšnji dogodek“ pomeni skorajšnji dogodek, kot je opredeljen v členu 4(4a) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

(6) „incident“ pomeni incident, [...] **kot je opredeljen v** členu 4(5) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

[...]

(8) „večji **incident** [...]“ pomeni vsak incident, **ki povzroči stopnjo motenj, ki presega zmogljivost subjekta Unije in CERT-EU, da se nanj odzoveta, ali ki pomembno vpliva na vsaj dva subjekta Unije;** [...]

(9) „obvladovanje incidenta“ pomeni obvladovanje incidenta, [...] **kot je opredeljeno v** členu 4(6) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

(10) „kibernetska grožnja“ pomeni kibernetsko grožnjo, [...] **kot je opredeljena v** členu 2(8) Uredbe (EU) 2019/881;

[...]

(12) „ranljivost“ pomeni šibko točko v smislu člena 4(8) Direktive [predlog revidirane direktive o varnosti omrežij in informacij];

[...]

(14) „[...] tveganje“ pomeni **tveganje v smislu člena 4(7b) Direktive [predlog revidirane direktive o varnosti omrežij in informacij]** [...].

[...]

[...]

Člen 3a

Obdelava osebnih podatkov

1) CERT-EU, IICB ali subjekti Unije osebne podatke na podlagi te uredbe obdelujejo v skladu z Uredbo (EU) 2018/1725.

2) CERT-EU, IICB in subjekti Unije obdelujejo in si izmenjujejo osebne podatke v obsegu, ki je potreben, in izključno za izpolnjevanje svojih obveznosti iz te uredbe.

Poglavje II
UKREPI ZA VISOKO SKUPNO RAVEN KIBERNETSKE VARNOSTI

Člen 4

Obvladovanje, upravljanje in nadzor tveganj

1. Vsak [...] **subjekt** Unije vzpostavi lasten [...] okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost (v nadaljnjem besedilu: okvir) v podporo poslanstvu subjekta [...]. **Okvir** nadzoruje najvišja raven vodenja subjekta, da se zagotovi učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost. Okvir se vzpostavi najpozneje do …. [15 mesecev po začetku veljavnosti te uredbe].

2. Okvir zajema celotno netajno okolje IT zadevnega [...] **subjekta Unije**, vključno z morebitnim okoljem IT v njegovih prostorih, **operativnim tehnološkim omrežjem, sr**edstvi in storitvami v okoljih računalništva v oblaku, ki jih upravlja zunanji izvajalec ali gostijo tretje osebe, mobilnimi napravami, korporativnimi omrežji, poslovnimi omrežji, ki niso povezana z internetom, in vsemi napravami, povezanimi z okoljem IT. Okvir **temelji na pristopu, ki upošteva vse nevarnosti, in na oceni zrelosti v skladu s členom 6, ki zajema vsa zadevna tehnična, operativna in organizacijska tveganja, ki bi lahko vplivala na kibernetsko varnost zadevnega subjekta Unije** [...].

2a. **Okvir določa politike kibernetske varnosti, vključno s cilji in prednostnimi nalogami za varnost omrežja in informacijskih sistemov, ter politike in postopke za ocenjevanje učinkovitosti izvedenih ukrepov za obvladovanje tveganj za kibernetsko varnost, ter opredeljuje vloge in odgovornosti članov osebja.**

2b. Okvir se pregleduje redno in vsaj vsaka tri leta glede na spreminjajoča se tveganja, vire in zrelost subjekta Unije.

3. Najvišja raven vodenja vsakega [...]**subjekta** Unije **nadzoruje** [...] skladnost [...] **svoje** organizacije z obveznostmi, povezanimi z obvladovanjem, upravljanjem in nadzorom tveganj za kibernetsko varnost, brez poseganja v dolžnosti drugih ravni vodenja glede skladnosti in obvladovanja tveganja na njihovih področjih pristojnosti.

3a. **Kadar je to primerno in brez poseganja v lastno odgovornost za izvajanje te uredbe, lahko najvišja raven vodenja vsakega subjekta Unije na druge visoke uradnike znotraj zadevnega subjekta prenese posamezno obveznost iz te uredbe. Ne glede na morebiten prenos posebne obveznosti lahko najvišja raven vodenja odgovarja za neizpolnjevanje obveznosti iz te uredbe s strani subjektov.**

3b. Najvišja raven vodenja vsakega subjekta Unije zagotovi, da subjekti Unije odobrijo načrt za kibernetsko varnost, ki vključuje ukrepe za obvladovanje tveganj za kibernetsko varnost, v skladu s svojo analizo tveganja, tako da se okvir izvaja v skladu s to uredbo.

[...]

5. Vsak [...] **subjekt** Unije imenuje lokalnega uradnika za kibernetsko varnost ali enakovredno funkcijo, ki deluje kot njegova enotna kontaktna točka v zvezi z vsemi vidiki kibernetske varnosti.

   Lokalni uradnik za kibernetsko varnost olajša izvajanje te uredbe in neposredno redno poroča najvišji ravni vodenja o stanju izvajanja.

   Brez poseganja v to, da je lokalni uradnik za kibernetsko varnost enotna kontaktna točka v vsakem subjektu Unije, lahko subjekt Unije nekatere naloge lokalnega uradnika za kibernetsko varnost v zvezi z izvajanjem te uredbe prenese na CERT-EU na podlagi sporazuma o ravni storitve, sklenjenega med tem subjektom Unije in CERT-EU. IICB odloči, ali bo opravljanje te storitve del osnovnih storitev CERT-EU, pri čemer upošteva človeške in finančne vire zadevnega subjekta Unije. Vsak subjekt Unije brez nepotrebnega odlašanja obvesti CERT-EU o imenovanih lokalnih uradnikih za kibernetsko varnost in vseh naknadnih spremembah. CERT-EU redno posodablja seznam imenovanih lokalnih uradnikov za kibernetsko varnost.

6. Višji uradniki v smislu člena 29(2) Kadrovskih predpisov[11] ali drugi uslužbenci na enaki ravni subjekta Unije redno opravljajo posebno usposabljanje, da bi pridobili dovolj znanja in spretnosti za razumevanje in oceno tveganj za kibernetsko varnost in praks obvladovanja ter njihovega vpliva na delovanje organizacije.

---

11 Uredba Sveta št. 259/68 z dne 29. februarja 1968 o določitvi Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev Evropskih skupnosti (UL L 56, 4.3.1968).

7. Vsi subjekti Unije morajo imeti vzpostavljene učinkovite mehanizme za zagotavljanje, da se za kibernetsko varnost nameni ustrezen delež proračuna za IT. Pri določanju tega odstotka se ustrezno upošteva okvir.

Člen 5

Ukrepi za obvladovanje tveganj za kibernetsko varnost [...]

1. [...] **Vsak subjekt Unije pod nadzorom** najvišje ravni vodenja [...] **zagotovi, da se sprejmejo ustrezni in sorazmerni tehnični, operativni in organizacijski ukrepi za obvladovanje tveganj, opredeljenih v okviru iz člena 4(1), in se prepreči in/ali minimizira učinek incidentov. Ob upoštevanju najnovejšega tehnološkega razvoja in po potrebi zadevnih evropskih in mednarodnih standardov ter stroškov izvajanja ti ukrepi zagotovijo raven varnosti omrežja in informacijskih sistemov, ki ustreza nastalim tveganjem. Pri ocenjevanju sorazmernosti teh ukrepov se ustrezno upoštevajo stopnja izpostavljenosti subjekta tveganjem, njegova velikost, verjetnost pojava incidentov in njihova resnost, vključno z njihovim družbenim in gospodarskim vplivom.**

[...]

3. Subjekti Unije pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost v svojih načrtih za kibernetsko varnost v skladu s smernicami in priporočili IICB obravnavajo vsaj naslednja specifična področja:

(a) politiko kibernetske varnosti v smislu opredelitve orodij in ukrepov, potrebnih za doseganje ciljev in prednostnih nalog iz člena 4 in člena 5(4);

(b) analizo tveganja in varnostna pravila za informacijske sisteme;

(c) organizacijo kibernetske varnosti, vključno z opredelitvijo vlog in odgovornosti;

(d) upravljanje sredstev, vključno s popisom sredstev IT in kartografijo omrežja IT;

(e) varnost človeških virov in nadzor dostopa;

(f) varnost operacij;

(g) varnost komunikacij;

(h) pridobivanje, razvoj in vzdrževanje sistema, vključno z obravnavanjem in razkrivanjem ranljivosti;

(i) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki zadevajo odnose med vsakim subjektom Unije in njegovimi neposrednimi dobavitelji ali ponudniki storitev. Subjekti Unije upoštevajo ranljivosti, značilne za vsakega neposrednega dobavitelja in ponudnika storitev, ter splošno kakovost proizvodov in praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi postopki varnega razvoja;

(j) obvladovanje incidentov in sodelovanje s CERT-EU, kot je vzdrževanje varnostnega spremljanja in vodenja dnevnikov;

(k) upravljanje neprekinjenega poslovanja, kot sta upravljanje varnostnih kopij in obnovitev po nesreči, ter krizno upravljanje, in

(l) spodbujanje in razvijanje izobraževanja, spretnosti, ozaveščanja, vaj in programov usposabljanja na področju kibernetske varnosti.

4. Subjekti Unije pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost v svojih načrtih za kibernetsko varnost v skladu s smernicami in priporočili IICB obravnavajo vsaj naslednje specifične ukrepe za obvladovanje tveganj za kibernetsko varnost:

(a) cilje in prednostne naloge v zvezi z uporabo storitev računalništva v oblaku v smislu člena 4(19) Direktive [predlog revidirane direktive o varnosti omrežij in informacij] in tehničnimi ureditvami za omogočanje dela na daljavo;

(b) konkretne ukrepe za prihodnjo uporabo načel ničelnega zaupanja, vključno z varnostnim modelom, ter usklajeno strategijo za kibernetsko varnost in upravljanje sistema na podlagi zavedanja, da grožnje obstajajo znotraj tradicionalnih meja omrežja in zunaj njih;

(c) uvedbo večfaktorske avtentifikacije kot norme v omrežjih in informacijskih sistemih;

(d) vzpostavitev varnosti dobavne verige programske opreme z merili za varni razvoj in oceno programske opreme;

(e) okrepitev pravil o javnem naročanju za omogočanje visoke skupne ravni kibernetske varnosti z:

(i) odpravo pogodbenih ovir, ki omejujejo izmenjavo informacij med ponudniki storitev IT in CERT-EU o incidentih, ranljivostih in kibernetskih grožnjah;

(ii) pogodbenimi obveznostmi glede poročanja o incidentih, ranljivostih in kibernetskih grožnjah ter glede vzpostavitve ustreznega odzivanja na incidente in njihovega spremljanja;

(f) uporabo kriptografije in šifriranja, zlasti šifriranja med koncema;

(g) varne komunikacijske sisteme znotraj organizacije.

Člen 6

Ocene zrelosti

1. Vsak [...] **subjekt** Unije, **po potrebi s pomočjo specializirane neodvisne strani**, najmanj vsaka tri leta izvede oceno kibernetskovarnostne zrelosti, ki vključuje vse elemente njegovega okolja IT, kot je opisano v členu 4, ob upoštevanju ustreznih smernic in priporočil, sprejetih v skladu s členom 13.

2. IICB na priporočilo CERT-EU in po posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA) v štirih mesecih po začetku veljavnosti te uredbe sprejme metodološke smernice za izvajanje ocen zrelosti.

3. [...] **Subjekt Unije po zaključku ocene zrelosti to predloži IICB. Prva ocena zrelosti se izvede najpozneje [12 mesecev po začetku veljavnosti te uredbe].**

Člen 7

Načrti za kibernetsko varnost

1. Najvišja raven vodenja vsakega **subjekta** [...] Unije na podlagi sklepov ocene zrelosti in ob upoštevanju sredstev in tveganj, opredeljenih v skladu s členom 4, po vzpostavitvi okvira [...], **sprejetju** [...] **ukrepov za obvladovanje tveganj** za kibernetsko varnost [...] **in izvedbi ocene zrelosti, najpozneje pa 21 mesecev po začetku veljavnosti te uredbe,** brez nepotrebnega odlašanja odobri načrt za kibernetsko varnost. Cilj načrta **za kibernetsko varnost** je izboljšati splošno kibernetsko varnost [...] **zadevnega** subjekta **Unije**, s tem pa prispeva k [...] zvišanju visoke skupne ravni kibernetske varnosti vseh [...] **subjektov** Unije. [...] Načrt **za kibernetsko varnost** vključuje najmanj **ukrepe za obvladovanje tveganj za kibernetsko varnost iz člena 5** [...]. Načrt **za kibernetsko varnost** se pregleda najmanj vsaki [...] **dve** leti **ali** po [...] **posamezni** oceni zrelosti [...], izvedeni v skladu s členom 6, **ali vsakem pregledu okvira iz člena 4**.

2. [...]

3. Načrt za kibernetsko varnost **upošteva** [...] vse veljavne smernice in priporočila, izdane **v skladu s členom 13** [...].

4. **Subjekt Unije po dokončanju načrta za kibernetsko varnost tega predloži IICB**.

Člen 7a

Medsebojni strokovni pregled

1. IICB na priporočilo CERT-EU in po posvetovanju z agencijo ENISA najpozneje do ... [24 mesecev po začetku veljavnosti te uredbe] z uporabo metodologije medsebojnih strokovnih pregledov in metodologije samoocenjevanja v skladu s členom 16 Direktive [predlog revidirane direktive o varnosti omrežij in informacij], po potrebi prilagojene potrebam subjektov Unije, vzpostavi metodologijo in organizacijske vidike medsebojnega strokovnega pregleda, da bi se učili iz skupnih izkušenj, okrepili medsebojno zaupanje, dosegli visoko skupno raven kibernetske varnosti ter okrepili zmogljivosti in politike subjektov Unije na področju kibernetske varnosti, potrebne za izvajanje te uredbe. Sodelovanje pri medsebojnem strokovnem pregledu je prostovoljno. Pri medsebojnem strokovnem pregledu lahko kot opazovalci sodelujejo predstavniki držav članic. Medsebojne strokovne preglede izvajajo strokovnjaki za kibernetsko varnost, ki jih imenujeta vsaj dva subjekta Unije, ki nista med subjekti Unije, ki se pregledujejo; ti pregledi zajemajo vsaj eno od naslednjega:

(i) raven izvajanja ukrepov za obvladovanje tveganj za kibernetsko varnost ter obveznosti poročanja iz členov 5 in 20;

(ii) raven zmogljivosti, vključno z razpoložljivimi finančnimi, tehničnimi in človeškimi

viri;

(iii) raven izvajanja okvira za izmenjavo informacij iz člena 19;

(iv) posebna medsektorska vprašanja.

2. Subjekti Unije lahko opredelijo posebna vprašanja iz odstavka 1, točka (iv), ki jih je treba pregledati. Obseg pregleda, vključno z opredeljenimi vprašanji, se sporoči sodelujočim subjektom Unije pred začetkom medsebojnega strokovnega pregleda.

3. Subjekti Unije lahko pred začetkom medsebojnega strokovnega pregleda izvedejo samooceno vidikov, ki se pregledujejo, in to samooceno predložijo imenovanim strokovnjakom.

4. Medsebojni strokovni pregledi vključujejo fizične ali virtualne obiske na kraju samem in izmenjave na daljavo. Ob upoštevanju načela dobrega sodelovanja subjekti Unije, ki so predmet medsebojnega strokovnega pregleda, imenovanim strokovnjakom zagotovijo informacije, potrebne za oceno, brez poseganja v nacionalno zakonodajo ali zakonodajo Unije o varstvu občutljivih ali tajnih podatkov. Vse informacije, pridobljene v okviru postopka medsebojnega strokovnega pregleda, se uporabljajo izključno v ta namen. Strokovnjaki, ki sodelujejo pri medsebojnem strokovnem pregledu, občutljivih ali tajnih informacij, pridobljenih med zadevnim pregledom, ne razkrijejo tretjim osebam.

5. Vidiki, ki so predmet medsebojnega strokovnega pregleda v subjektih Unije, dve leti po zaključku tega pregleda niso predmet ponovnega medsebojnega strokovnega pregleda v zadevnih subjektih Unije, razen če subjekti Unije ne zahtevajo drugače ali pristanejo na predlog IICB.

6. Subjekti Unije zagotovijo, da se vsako tveganje navzkrižja interesov v zvezi z imenovanimi strokovnjaki razkrije drugim subjektom Unije in IICB pred začetkom medsebojnega strokovnega pregleda. Subjekti Unije, ki so predmet medsebojnega strokovnega pregleda, lahko nasprotujejo imenovanju posameznih strokovnjakov iz ustrezno utemeljenih razlogov, o katerih se obvestijo subjekti Unije, ki jih imenujejo.

7. Strokovnjaki, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah in sklepih pregledov. Subjekti Unije lahko predložijo pripombe na osnutke poročil, ki jih zadevajo, in te pripombe se priložijo poročilom. Poročila vključujejo priporočila, da se omogoči izboljšanje vidikov, ki jih zajema medsebojni strokovni pregled. Poročila se po potrebi predložijo IICB in mreži skupin CSIRT. Subjekti Unije, ki se pregledujejo, se lahko odločijo, da poročilo, ki jih zadeva, ali njegovo redigirano različico javno objavijo.

Člen 8

Izvajanje

1. [...]

2. Smernice in priporočila, izdani v skladu s členom 13, podpirajo izvajanje določb iz tega poglavja.

3. Subjekti Unije na zahtevo IICB poročajo o posameznih vidikih tega poglavja.

Poglavje III
MEDINSTITUCIONALNI ODBOR ZA KIBERNETSKO VARNOST

Člen 9

Medinstitucionalni odbor za kibernetsko varnost

1. Vzpostavi se Medinstitucionalni odbor za kibernetsko varnost (IICB).

2. IICB je odgovoren za:

   (a) spremljanje, kako **subjekti** [...] **Unije** izvajajo to uredbo;

   (b) nadzor nad tem, kako CERT-EU izvaja splošne prednostne naloge in cilje, pri čemer IICB CERT-EU zagotavlja strateške usmeritve.

3. IICB sestavljajo:

   (a) po en predstavnik, ki ga imenuje vsak od spodaj navedenih:

   (i) Evropski parlament;

   (ii) Evropski svet;

   (iii) Svet Evropske unije;

   (iv) Evropska komisija;

   (v) Sodišče Evropske unije;

   (vi) Evropska centralna banka;

(vii) Evropsko računsko sodišče;

(viii) Evropska služba za zunanje delovanje;

(ix) Evropski ekonomsko-socialni odbor;

(x) Evropski odbor regij;

(xi) Evropska investicijska banka;

(xii) Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost ter

(xiii) Agencija Evropske unije za kibernetsko varnost;

(b) trije predstavniki, ki jih [...] **imenuje** mreža agencij Unije (EUAN) na predlog svojega svetovalnega odbora za IKT in ki zastopajo interese agencij in organov, ki upravljajo svoje okolje IT. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. Članom lahko pomaga namestnik. Predsednik lahko povabi druge predstavnike zgoraj navedenih [...] **subjektov** ali drugih **subjektov** [...] Unije, da se udeležijo sestankov IICB brez pravice do glasovanja.

4. IICB sprejme svoj notranji poslovnik.

5. IICB v skladu z notranjim poslovnikom med svojimi člani imenuje predsednika za obdobje [...] **dveh** let. Njegov namestnik postane polnopravni član IICB za enako obdobje.

6. IICB se **vsaj trikrat na leto** sestane na pobudo predsednika **in/ali** na zahtevo CERT-EU **in**/ali na zahtevo katerega koli člana.

7. Vsak član IICB ima en glas. IICB odločitve sprejema z navadno večino, razen če je v tej uredbi določeno drugače. Predsednik ne glasuje, razen v primeru neodločenega izida glasovanja, ko ima odločilni glas.

8. IICB lahko deluje po poenostavljenem pisnem postopku, ki se začne v skladu z notranjim poslovnikom IICB. V skladu s tem postopkom se zadevna odločitev šteje za odobreno v roku, ki ga določi predsednik, razen v primeru ugovora člana.

9. Vodja CERT-EU, **predsednik Skupine za sodelovanje na področju varnosti omrežij in informacij, predsednik mreže EU-CyCLONe in predsednik mreže skupin CSIRT** ali **njihovi** [...] namestniki [...] se **lahko kot opazovalci** udeležujejo sestankov IICB, razen če IICB odloči drugače.

10. Sekretariat IICB zagotavlja **agencija ENISA** [...] **in odgovarja predsedniku IICB**.

11. Predstavniki, ki jih mreža agencij Unije imenuje na predlog svetovalnega odbora za IKT, odločitve IICB posredujejo **članom mreže agencij Unije** [...]. Vsaka agencija in organ Unije ima pravico, da na predstavnike ali predsednika IICB naslovi katero koli vprašanje, za katero meni, da bi ga IICB moral obravnavati.

12. [...]

13. IICB lahko **ustanovi** [...] izvršni odbor, ki mu pomaga pri delu ter na katerega prenese nekaj svojih nalog in pooblastil**, zlasti tiste iz člena 10, točki (c) in (e)**. IICB določi poslovnik izvršnega odbora, vključno z njegovimi nalogami in pooblastili, ter mandat njegovih članov.

14. IICB Svetu vsakih 12 mesecev predloži poročilo, v katerem podrobno opiše napredek pri izvajanju te uredbe in navede zlasti obseg sodelovanja CERT-EU z nacionalnimi sorodnimi organi v vsaki državi članici. To poročilo je prispevek k dvoletnemu poročilu o stanju kibernetske varnosti v Uniji v istem obdobju v skladu s členom 15 Direktive [predlog revidirane direktive o varnosti omrežij in informacij].

Člen 10

Naloge IICB

IICB pri izvrševanju svojih obveznosti zlasti:

(a) [...] **učinkovito spremlja in nadzoruje uporabo** te uredbe [...] **ter podpira subjekte** Unije [...] **pri izboljšanju njihove kibernetske varnosti**; **v ta namen lahko IICB od CERT-EU in subjektov Unije zahteva *ad hoc* poročila;**

(**aa**) **po strateški razpravi sprejme večletno strategijo za dvig ravni kibernetske varnosti v subjektih Unije in jo redno ocenjuje, in sicer vsaj vsakih pet let, ter po potrebi spremeni;**

(b) na podlagi predloga**, ki ga predloži** [...] vodja CERT-EU, odobri letni delovni program za CERT-EU in spremlja njegovo izvajanje;

(c) na podlagi predloga vodje CERT-EU odobri katalog storitev CERT-EU **in njegovo vsako naslednjo posodobitev**;

(d) na podlagi predloga, ki ga predloži vodja CERT-EU, odobri letno finančno načrtovanje prihodkov in izdatkov, vključno z osebjem, za dejavnosti CERT-EU;

(e) na podlagi predloga vodje CERT-EU odobri načine izvajanja sporazumov o ravni storitev;

(f) preveri in odobri letno poročilo, ki ga pripravi vodja CERT-EU ter zajema dejavnosti CERT-EU in upravljanje njegovih sredstev;

(g) odobri in spremlja ključne kazalnike uspešnosti za CERT-EU, opredeljene na predlog vodje CERT-EU;

(h) odobri dogovore o sodelovanju ter ureditve ali **sporazume** [...] o ravni storitev med CERT-EU in drugimi subjekti v skladu s členom 17;

(i) vzpostavi [...] tehnične svetovalne skupine [...] za pomoč IICB pri njegovem delu, odobri njihov mandat in imenuje njihove predsednike;

(j) **sprejme smernice in priporočila na podlagi predloga CERT-EU v skladu s členom 13 ter CERT-EU naroči izdajo, umik ali spremembo predloga smernic ali priporočil ali poziva k ukrepanju;**

(k) prejema in ocenjuje dokumente in poročila, ki jih v skladu s to uredbo predložijo subjekti Unije;

(l) podpira ustanovitev neformalne skupine lokalnih uradnikov za kibernetsko varnost vseh subjektov ter s tem olajšuje izmenjavo dobrih praks in informacij v zvezi z izvajanjem te uredbe;

(m) pripravi načrt za krizno upravljanje na področju kibernetske varnosti v podporo usklajenemu obvladovanju večjih incidentov na operativni ravni, ki vplivajo na subjekte Unije, in prispeva k redni izmenjavi relevantnih informacij, zlasti o vplivih in resnosti večjih incidentov ter možnih načinih blaženja.

Člen 11

Skladnost

1. IICB **v skladu s členom 9(2) in členom 10 učinkovito** spremlja, kako **subjekti** [...] Unije izvajajo to uredbo ter sprejete smernice, priporočila in pozive k ukrepanju. **V ta namen lahko IICB zahteva informacije ali dokumentacijo, potrebne za oceno pravilne uporabe določb Uredbe s strani subjektov Unije. Za namene sprejetja ukrepov za skladnost v skladu s tem členom zadevni subjekt Unije nima glasovalnih pravic.**

2. Kadar IICB ugotovi, da **subjekti** [...] Unije niso učinkovito uporabljali ali izvajali te uredbe ali smernic, priporočil in pozivov k ukrepanju, izdanih na podlagi te uredbe, lahko brez poseganja v notranje postopke zadevnega **subjekta** [...] Unije **ter po tem, ko zadevnemu subjektu ali osebi da možnost, da predstavi svoje stališče**:

(a) izda opozorilo **za odpravo ugotovljenih pomanjkljivosti v določenem časovnem okviru, vključno s priporočili za spremembo dokumentov o kibernetski varnosti, ki so jih sprejeli subjekti Unije na podlagi te uredbe**; po potrebi zaradi velikega tveganja za kibernetsko varnost je krog prejemnikov opozorila ustrezno omejen;

(aa) izda utemeljeno uradno obvestilo subjektu Unije, če pomanjkljivosti, ugotovljene v predhodno izdanem opozorilu, niso bile ustrezno odpravljene v določenem roku, ter o tem mnenju uradno obvesti Svet, Evropski parlament in Komisijo;

(b) **izda zlasti:** [...]

i. priporočilo, da se izvede revizija subjekta Unije;

ii. zahtevo, da revizijo izvede neodvisna revizijska služba;

(c) od subjekta Unije zahteva, da obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, če je to ustrezno, na določen način in v določenem roku uskladi z določbami te uredbe;

(d) za vse države članice in subjekte Unije izda svetovalno mnenje, v katerem priporoči začasno prekinitev prenosa podatkov subjektu Unije.

3. Kadar IICB sprejme ukrepe v skladu z odstavkom 2, točke (a) do (d), zadevni subjekt Unije zagotovi podroben opis ukrepov in dejavnosti, sprejetih za odpravo domnevnih pomanjkljivosti, ki jih je ugotovil IICB. Subjekt Unije ta opis predloži v razumnem roku, o katerem se dogovori z IICB.

4. Kadar IICB meni, da subjekt Unije nenehno krši določbe te uredbe neposredno zaradi dejanj ali opustitev dejanj s strani uradnika ali drugega uslužbenca Unije, tudi na najvišji ravni vodenja, IICB od zadevnega subjekta zahteva, da sprejme ustrezne ukrepe, vključno z disciplinskimi ukrepi, zlasti v skladu s pravili iz Kadrovskih predpisov in Pogojev za zaposlitev drugih uslužbencev Evropske unije. V ta namen IICB zadevnemu subjektu pošlje potrebne informacije.

Poglavje IV
CERT-EU

Člen 12

Poslanstvo in naloge CERT-EU

1. [...] **Poslanstvo CERT-EU** [...] je prispevati k varnosti netajnega okolja IT vseh **subjektov** [...] Unije, tako da jim svetuje glede kibernetske varnosti ter jim pomaga preprečiti, odkriti in ublažiti incidente ter se odzivati nanje, deluje pa tudi kot njihovo vozlišče za izmenjavo informacij o kibernetski varnosti in za usklajevanje odzivanja na incidente.

1a. CERT-EU zbira, upravlja, analizira in izmenjuje informacije s subjekti Unije o grožnjah, šibkih točkah ter incidentih na netajni infrastrukturi IT. Usklajuje odzive na incidente na medinstitucionalni ravni in na ravni subjektov Unije, vključno z zagotavljanjem ali usklajevanjem zagotavljanja specializirane operativne pomoči.

2. CERT-EU za **subjekte** [...] Unije izvaja naslednje naloge:

(a) podpira jih pri izvajanju te uredbe in prispeva k usklajevanju uporabe te uredbe z **določbami** [...] iz člena 13(1) ali *ad hoc* poročili, ki jih zahteva IICB;

(b) [...] s svežnjem storitev za kibernetsko varnost, opisanih v katalogu storitev CERT-EU, **vsem subjektom Unije ponuja standardne storitve CSIRT** (v nadaljnjem besedilu: osnovne storitve);

(c) vzdržuje mrežo podobnih institucij, organov in agencij ter partnerjev za podporo storitev, kot so navedene v členih 16 in 17;

(d) IICB opozori na katero koli vprašanje, ki se nanaša na izvajanje te uredbe ali smernic, priporočil in pozivov k ukrepanju;

(e) **na podlagi informacij iz odstavka 1a in v tesnem sodelovanju z agencijo ENISA** [...] prispeva k situacijskemu zavedanju na področju kibernetske varnosti v EU**. Te informacije se delijo z IICB, mrežo skupin CSIRT in EU-INTCEN;**

(f) deluje kot enakovreden koordinatorju, imenovanemu za subjekte Unije, kot je navedeno v členu 6 Direktive [predlog revidirane direktive o varnosti omrežij in informacij].

[...]

[...]

[...]

[...]

[...]

4. CERT-EU **v okviru kompetenc** strukturirano sodeluje z [...] **ENISA** pri krepitvi zmogljivosti, operativnem sodelovanju in dolgoročnih strateških analizah kibernetskih groženj v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta.

5. CERT-EU lahko zagotavlja naslednje storitve, ki niso opisane v njegovem katalogu storitev (v nadaljnjem besedilu: storitve, ki se zaračunajo):

   (a) storitve, ki podpirajo kibernetsko varnost okolja IT **subjektov** [...] Unije, razen storitev iz odstavka 2, in sicer na podlagi sporazumov o ravni storitev in glede na razpoložljive vire;

   (b) storitve, ki podpirajo operacije ali projekte **subjektov** [...] Unije v zvezi s kibernetsko varnostjo, razen tistih za zaščito njihovih okolij IT, in sicer na podlagi pisnih dogovorov in s predhodno odobritvijo IICB;

   (c) storitve, ki podpirajo varnost okolja IT organizacij, ki niso **subjekti** [...] Unije in ki tesno sodelujejo s **subjekti** [...] Unije, ki so jim na primer bile dodeljene naloge ali odgovornosti v skladu s pravom Unije, na podlagi pisnih sporazumov in s predhodno odobritvijo IICB.

6. CERT-EU lahko po potrebi v tesnem sodelovanju z agencijo [...] **ENISA** organizira vaje na področju kibernetske varnosti ali priporoča udeležbo na že obstoječih vajah, da preizkusi raven kibernetske varnosti **subjektov** [...] Unije**, ali v teh vajah sodeluje**.

7. CERT-EU lahko **subjektom** [...] Unije pomaga v primeru incidentov, do katerih pride v tajnih okoljih IT, če to izrecno **v skladu s svojimi postopki** zahtevajo zadevni **subjekti** [...] **Unije**. **V tem primeru se določbe iz členov 19 do 21 te uredbe ne uporabljajo. Zagotavljanje pomoči s strani CERT-EU v skladu s tem odstavkom ne posega v veljavna pravila države članice ali Unije v zvezi z varstvom občutljivih ali tajnih podatkov.**

8. CERT-EU obvesti subjekte Unije o svojih postopkih in procesih obvladovanja incidentov.

9. CERT-EU lahko s privolitvijo zadevnega subjekta Unije spremlja omrežni promet subjektov Unije.

10. CERT-EU lahko, če to izrecno zahtevajo službe subjektov Unije, ki skrbijo za vprašanja politike, zagotavlja tehnične nasvete ali informacije o zadevnih vprašanjih politike.

11. CERT-EU v sodelovanju z Evropskim nadzornikom za varstvo podatkov podpira zadevne subjekte Unije pri obravnavanju incidentov, ki povzročijo kršitve varstva osebnih podatkov.

Člen 13

Smernice, priporočila in pozivi k ukrepanju

1. CERT-EU podpira izvajanje te uredbe z izdajo:

   (a) pozivov k ukrepanju, ki opisujejo nujne varnostne ukrepe, ki naj bi jih subjekti [...] Unije nujno sprejeli v določenem časovnem obdobju. Zadevni subjekt Unije po prejemu poziva k ukrepanju brez nepotrebnega odlašanja obvesti CERT-EU o tem, kako so bili ti ukrepi uporabljeni;

   (b) predlogov za IICB za smernice, naslovljene na vse ali podskupino subjektov [...] **Unije**;

   (c) predlogov za IICB za priporočila, naslovljena na posamezne subjekte [...] **Unije**.

2. Smernice in priporočila lahko vključujejo:

   (a) načine obvladovanja tveganj za kibernetsko varnost in [...] **ukrepov za obvladovanje tveganj** za kibernetsko varnost ali njihove izboljšave;

   (b) načine izvajanja ocen zrelosti in načrtov za kibernetsko varnost ter

   (c) kadar je primerno, uporabo skupne tehnologije, arhitekture in povezanih dobrih praks s ciljem doseganja interoperabilnosti in skupnih standardov**, tudi usklajenega pristopa k zagotavljanju varnosti dobavne verige** [...]**.**

[...]

[...]

Člen 14

Vodja CERT-EU

1. Komisija po pridobitvi odobritve dveh tretjin članov IICB imenuje vodjo CERT-EU. Posvetovanje z IICB se izvede v vseh fazah postopka pred imenovanjem vodje CERT-EU, zlasti pri pripravi razpisov prostega delovnega mesta, pregledovanju prijav in imenovanju izbirnih komisij v zvezi s tem delovnim mestom.

2. Vodja CERT-EU je odgovoren za ustrezno delovanje CERT-EU v okviru svojih pristojnosti pod vodstvom IICB. Odgovoren je za izvajanje strateške usmeritve, smernic, ciljev in prednostnih nalog, ki jih določi IICB, ter za upravljanje CERT-EU, vključno s finančnimi in človeškimi viri. Redno poroča predsedniku IICB.

3. Vodja CERT-EU pomaga odgovornemu odredbodajalcu na podlagi prenosa pooblastil pri pripravi letnega poročila o dejavnostih, ki vsebuje finančne in upravljavske informacije, med drugim o rezultatih kontrol, pripravljenega v skladu s členom 66(9) finančne uredbe, ter mu redno poroča o izvajanju ukrepov, v zvezi s katerimi so bila pooblastila prenesena na vodjo CERT-EU.

4. Vodja CERT-EU vsako leto pripravi finančno načrtovanje upravnih prihodkov in odhodkov za svoje dejavnosti, predlog letnega delovnega programa, predlog kataloga storitev CERT-EU in njegovo revizijo, predlog načinov izvajanja sporazumov o ravni storitev in predlog ključnih kazalnikov uspešnosti za CERT-EU, ki ga odobri IICB v skladu s členom 10.

Pri reviziji seznama storitev v katalogu storitev CERT-EU vodja CERT-EU upošteva vire, dodeljene CERT-EU.

5. Vodja CERT-EU IICB [...] [...] predloži **letna** poročila o delovanju CERT-EU, finančnem načrtovanju, prihodkih, izvrševanju proračuna, sporazumih o ravni storitev in sklenjenih pisnih sporazumih, sodelovanju s sorodnimi organi in partnerji ter službenih potovanjih osebja, vključno s poročili iz člena 10([...]**a**).

Člen 15

Finančne in kadrovske zadeve

[...]

1a. CERT-EU je sicer ustanovljen kot ločen medinstitucionalni ponudnik storitev za vse subjekte Unije, vendar je vključen v upravno strukturo generalnega direktorata Komisije, da lahko uporablja upravne, finančne, upravljavske in računovodske podporne strukture Komisije. Komisija obvesti IICB o upravnem sedežu CERT-EU in o vseh spremembah v zvezi z njim. Ta pristop se redno ocenjuje, najpozneje pred koncem vsakega večletnega finančnega okvira, sprejetega v skladu s členom 312 PDEU, da se lahko sprejmejo ustrezni ukrepi.

2. Pri uporabi upravnih in finančnih postopkov vodja CERT-EU deluje pod nadzorom Komisije.

3. Naloge in dejavnosti CERT-EU, vključno s storitvami, ki jih CERT-EU **subjektom** [...] Unije zagotavlja v skladu s členom 12(2), [...] (4) in (6) ter členom 13(1) in so financirane iz razdelka večletnega finančnega okvira, namenjenega evropski javni upravi, se financirajo iz posebne proračunske vrstice proračuna Komisije. Delovna mesta, rezervirana za CERT-EU, se podrobneje opredelijo v opombi h kadrovskemu načrtu Komisije.

4. **Subjekti** [...] Unije, razen tistih iz odstavka 3, CERT-EU zagotovijo letni finančni prispevek za kritje storitev, ki jih CERT-EU zagotavlja v skladu z odstavkom 3. Ustrezni prispevki temeljijo na usmeritvah IICB, o njih pa se vsak subjekt in CERT-EU dogovorita v sporazumih o ravni storitev. Prispevki pomenijo pravičen in sorazmeren delež skupnih stroškov zagotovljenih storitev. Zbirajo se na posebni proračunski vrstici iz odstavka 3 kot namenski prejemki, kot je določeno v členu 21(3), točka (c), Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta[12].

5. Stroške nalog, opredeljenih v členu 12(5), krijejo **subjekti** [...] Unije, ki prejemajo storitve CERT-EU. Prihodki se dodelijo proračunskim vrsticam, ki krijejo stroške.

[12] Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 (UL L 193, 30.7.2018, str. 1).

Člen 16

Sodelovanje CERT-EU s sorodnimi organi iz držav članic

1. CERT-EU **brez nepotrebnega odlašanja** sodeluje in si izmenjuje informacije z nacionalnimi sorodnimi organi v državah članicah, **zlasti** [...] [...] [...] s skupinami CSIRT **iz člena 9 Direktive [predlog revidirane direktive o varnosti omrežij in informacij] in/ali po potrebi pristojnimi nacionalnimi organi** ter enotnimi kontaktnimi točkami iz člena 8 Direktive [predlog revidirane direktive o varnosti omrežij in informacij], v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti, možnimi protiukrepi ter vsemi zadevami, pomembnimi za izboljšanje zaščite okolij IT **subjektov** [...] Unije, vključno prek mreže skupin CSIRT iz člena 13 Direktive [predlog revidirane direktive o varnosti omrežij in informacij].

1a. CERT-EU nemudoma uradno obvesti vse ustrezne nacionalne sorodne organe iz odstavka 1 v državi članici, ko izve za pomembne incidente, ki se zgodijo na ozemlju te države članice, razen če ima CERT-EU informacije, da je prizadeti subjekt Unije tak incident že prijavil v skladu s členom 20(2a).

2. CERT-EU si **brez nepotrebnega odlašanja** [...] za olajšanje odkrivanja podobnih kibernetskih groženj in incidentov **ali prispevek k analizi incidenta** z nacionalnimi sorodnimi organi v državah članicah izmenjuje z incidenti povezane informacije, ne da bi za to **potreboval** soglasje prizadetega **subjekta Unije** [...]. CERT-EU [...] z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le:

(a) s soglasjem prizadetega subjekta Unije;

(b) v primeru, da je prizadeti subjekt Unije že objavil, da je bil prizadet;

(c) če bi objava identitete prizadetega subjekta Unije povečala verjetnost, da se bodo incidenti drugje preprečili ali ublažili, četudi brez soglasja prizadetega subjekta Unije. Take odločitve mora odobriti vodja CERT-EU. Prizadeti subjekt Unije se obvesti pred objavo.

Člen 17

Sodelovanje CERT-EU z [...] ***drugimi sorodnimi organi***

1. CERT-EU lahko s sorodnimi organi [...] **v Evropski uniji, razen tistimi iz člena 16**, vključno s sorodnimi organi iz posameznih industrijskih sektorjev, sodeluje v zvezi z orodji in metodami, kot so tehnike, taktike, postopki in dobre prakse, ter v zvezi s kibernetskimi grožnjami in ranljivostmi. Za vsako sodelovanje s takimi sorodnimi organi [...] CERT-EU pridobi predhodno soglasje IICB **za vsak primer posebej**. **Kadar CERT-EU vzpostavi sodelovanje s takimi sorodnimi organi, obvesti vse ustrezne nacionalne sorodne organe iz člena 16(1) v državi članici, v kateri ima sorodni organ sedež.**

2. CERT-EU lahko za zbiranje informacij o splošnih in specifičnih kibernetskih grožnjah, ranljivostih in možnih protiukrepih sodeluje z drugimi partnerji, kot so komercialni subjekti, mednarodne organizacije, nacionalni subjekti, ki ne prihajajo iz Evropske unije, ali posamezni strokovnjaki. Za širše sodelovanje s takimi partnerji CERT-EU pridobi predhodno soglasje IICB **za vsak primer posebej**.

3. CERT-EU lahko, **če je z zadevnim partnerjem sklenjen sporazum ali pogodba o nerazkritju,** s soglasjem **subjekta Unije** [...], ki ga je incident prizadel, partnerjem **iz odstavkov 1 in 2** zagotovi s **posameznim** incidentom povezane informacije, **izključno z namenom, da lahko ti prispevajo k njegovi analizi** [...]. **Takšni sporazumi ali pogodbe o nerazkritju se zakonito preverijo v skladu z ustreznimi notranjimi postopki Komisije. Za sporazume ali pogodbe o nerazkritju ni potrebna predhodna odobritev IICB, vendar je o njih obveščen njegov predsednik.**

4. **CERT-EU lahko s predhodno odobritvijo IICB izjemoma sklene sporazume o ravni storitev s subjekti, ki niso subjekti Unije.**

Poglavje V
OBVEZNOSTI SODELOVANJA IN POROČANJA

Člen 18

Ravnanje z informacijami

1. CERT-EU in **subjekti** [...] Unije spoštujejo obveznost varovanja poslovne skrivnosti v skladu s členom 339 Pogodbe o delovanju Evropske unije ali enakovrednimi veljavnimi okviri.

2. Določbe Uredbe (ES) št. 1049/2001 Evropskega parlamenta in Sveta[13] se uporabljajo v zvezi z zahtevami za dostop javnosti do dokumentov, ki jih ima CERT-EU, vključno z obveznostmi iz navedene uredbe, da se je treba posvetovati z drugimi [...] **subjekti** Unije **ali po potrebi državami članicami**, kadar se zahteva nanaša na njihove dokumente.

[...]

4. CERT-EU ter **subjekti** [...] Unije pri ravnanju z informacijami upoštevajo **veljavna** pravila [...] o informacijski varnosti.

[...]

Člen 19

[...] ***Izmenjava informacij na področju kibernetske varnosti***

-1. Subjekti Unije lahko CERT-EU prostovoljno predložijo informacije o kibernetskih grožnjah, incidentih, skorajšnjih dogodkih in ranljivostih, ki so jih prizadeli. CERT-EU poskrbi, da so na voljo učinkovita komunikacijska sredstva, da se olajša izmenjava informacij s subjekti Unije. CERT-EU lahko pri obravnavi priglasitev daje prednost obveznim priglasitvam pred prostovoljnimi priglasitvami.

[13] Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

1. Da bi CERT-EU lahko [...] **izvajal svoje poslanstvo in naloge iz člena 12**, lahko **subjekte** [...] Unije zaprosi za predložitev informacij iz njihovih zbirk sistemov IT, **kar vključuje informacije v zvezi s kibernetskimi grožnjami, skorajšnjimi dogodki, ranljivostmi, kazalniki ogroženosti, kibernetskovarnostnimi opozorili in priporočili glede konfiguracije kibernetskovarnostnih orodij za odkrivanje incidentov na področju kibernetske varnosti** [...]. Zaprošeni **subjekt** [...] Unije zahtevane informacije in vse njihove naknadne posodobitve nemudoma posreduje.

2. **Subjekti** [...] Unije na zahtevo CERT-EU brez nepotrebnega odlašanja zagotovijo digitalne informacije, ustvarjene z elektronskimi napravami, uporabljenimi v zadevnih incidentih. CERT-EU lahko dodatno pojasni, katere vrste takih digitalnih informacij potrebuje za situacijsko zavedanje in odzivanje na incidente.

3. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto **subjekta** [...] Unije, ki ga je prizadel incident, izmenjuje **s subjekti Unije** le s soglasjem prizadetega subjekta. **Če se soglasje zavrne, zadevni subjekt CERT-EU predloži ustrezno utemeljene razloge.** [...]

4. Obveznosti izmenjave ne veljajo za tajne podatke EU in informacije, **razširjanje katerih zunaj subjekta Unije, ki je prejemnik informacij, je vir informacij prepovedal z vidno oznako, razen če vir informacij** [...] **izrecno dovoli izmenjavo informacij s CERT-EU.** [...]

Člen 20

[...] ***Obveznosti <u>poročanja</u>***

-1. Incident se šteje za pomembnega, če:

(a) je povzročil ali bi lahko povzročil resne operativne motnje v delovanju subjekta Unije ali finančno izgubo za zadevni subjekt Unije;

(b) je prizadel ali bi lahko prizadel druge fizične ali pravne osebe s povzročitvijo znatne premoženjske ali nepremoženjske škode.

1. Vsi **subjekti** [...] Unije **CERT-EU** [...] **predložijo:** [...]

[...].

(a) brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po seznanitvi s pomembnim incidentom, zgodnje opozorilo, iz katerega je, če je ustrezno, razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem in ali je oziroma bi lahko imel čezmejni vpliv;

(b) brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po seznanitvi s pomembnim incidentom, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz pododstavka (a) in navede začetna ocena pomembnega incidenta, njegova resnost in vpliv ter, če so na voljo, **kazalniki** ogroženosti;

(c) na zahtevo CERT-EU vmesno poročilo o zadevnih posodobitvah statusa;

(d) končno poročilo najpozneje v enem mesecu po predložitvi priglasitve pomembnega incidenta iz točke (b), ki vključuje vsaj naslednje:

(i) podroben opis pomembnega incidenta, njegove resnosti in vpliva;

(ii) vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil pomembni incident;

(iii) izvedene blažilne ukrepe in take ukrepe, ki se še izvajajo;

(iv) po potrebi čezmejni učinek pomembnega incidenta;

(e) v primerih, ko so v času predložitve končnega poročila iz točke (d) pomembni incidenti še vedno v teku, poročilo o napredku v tistem trenutku in končno poročilo v enem mesecu po razrešitvi incidenta.

[...]

(g) [...]

(h) [...]

(i) [...]

(j) [...]

2a. Vsi subjekti Unije si informacije, sporočene v skladu z odstavkom 1, v istem roku izmenjajo z vsemi ustreznimi nacionalnimi sorodnimi organi iz člena 16(1), kjer se nahajajo.

3. CERT-EU [...] **IICB, EU-INTCEN in mreži skupin CSIRT vsake tri mesece** [...] predloži zbirno poročilo, vključno z anonimiziranimi zbirnimi podatki o [...] kibernetskih grožnjah, [...] ranljivostih **v skladu s členom 19, odgovorih subjektov Unije na pozive k ukrepanju v skladu s členom 13(1), točka (a),** in pomembnih incidentih, priglašenih v skladu z odstavkom 1. **To poročilo je prispevek k dvoletnemu poročilu o stanju kibernetske varnosti v Uniji v skladu s členom 15 Direktive [predlog revidirane direktive o varnosti omrežij in informacij].**

4. IICB [...] **v [6 mesecih po začetku veljavnosti te uredbe]** izda smernice ali priporočila, **v katerih so podrobneje določeni** [...] načini izvajanja, **oblika** in vsebina **poročanja** [...]. **Smernice ali priporočila ustrezno upoštevajo določbe, ki se izvajajo s katerimi koli izvedbenimi akti v skladu s členom 20(11) Direktive [predlog revidirane direktive o varnosti omrežij in informacij]**. CERT-EU razširi ustrezne tehnične podrobnosti, da se **subjektom** [...] Unije omogočijo proaktivno odkrivanje, odzivanje na incidente ali blažilni ukrepi.

5. Obveznosti **poročanja** [...] ne veljajo za tajne podatke EU in informacije, **razširjanje katerih zunaj subjekta Unije, ki je prejemnik informacij, je vir informacij prepovedal z vidno oznako, razen če vir informacij** [...] **izrecno dovoli izmenjavo informacij s CERT-EU.** [...]

Člen 21

Usklajevanje odzivanja na incidente in sodelovanje v zvezi z incidenti [...]

1. CERT-EU, ki deluje kot vozlišče za izmenjavo informacij o kibernetski varnosti in usklajevanje odzivanja na incidente, olajša izmenjavo informacij v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti med:

   (a) **subjekti** [...] Unije;

   (b) sorodnimi organi iz členov 16 in 17.

2. CERT-EU**,** [...] **po potrebi v tesnem sodelovanju z agencijo ENISA v skladu s členom 7(7)(d) Akta o kibernetski varnosti[14],** olajša usklajevanje med **subjekti** [...] Unije v zvezi z odzivanjem na incidente, vključno s:

   (a) prispevkom k doslednemu zunanjemu komuniciranju;

   [...]

   (c) optimalno uporabo operativnih virov;

   (d) usklajevanjem z drugimi mehanizmi za odzivanje na krize na ravni Unije.

3. CERT-EU **v tesnem sodelovanju z agencijo ENISA** podpira **subjekte** [...] Unije v zvezi s situacijskim zavedanjem o kibernetskih grožnjah, ranljivostih in incidentih.

---

14 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 (Akt o kibernetski varnosti).

4. IICB **do [12 mesecev po začetku veljavnosti te uredbe] na podlagi predloga CERT-EU sprejme** [...] smernice **ali priporočila** o usklajevanju odzivanja na incidente in sodelovanju v zvezi s pomembnimi incidenti. Kadar obstaja sum, da je incident kaznivo dejanje, CERT-EU zagotovi smernice o tem, kako incident prijaviti organom kazenskega pregona.

Člen 22

Obvladovanje* *večjih* *incidentov [...]

-1. V podporo usklajenemu obvladovanju večjih incidentov na operativni ravni, ki vplivajo na subjekte Unije, in kot prispevek k redni izmenjavi relevantnih informacij med subjekti Unije in z državami članicami IICB v tesnem sodelovanju s skupino CERT-EU in agencijo ENISA pripravi načrt za krizno upravljanje na področju kibernetske varnosti na podlagi dejavnosti iz člena 21(2), ki vključuje vsaj naslednje elemente:

(a) načine usklajevanja in prenašanja informacij med subjekti Unije za obvladovanje večjih incidentov na operativni ravni;

(b) skupne standardne operativne postopke (SOP);

(c) skupno taksonomijo resnosti večjih incidentov in sprožilnih točk za krize;

(d) redne vaje;

(e) varne komunikacijske kanale, ki jih je treba uporabljati;

(f) kontaktno točko za EU-CyCLONe, ki izmenjuje ustrezne informacije z EU-CyCLONe kot prispevek k skupnemu situacijskemu zavedanju.

1. CERT-EU usklajuje odzive **subjektov** [...] Unije na večje **incidente** [...]. Vzdržuje zbirko tehničnega strokovnega znanja, ki bi bilo potrebno za odzivanje na incidente v primeru **večjih incidentov** [...].

2. **Subjekti** [...] Unije prispevajo v zbirko tehničnega strokovnega znanja, tako da zagotovijo letno posodobljen seznam strokovnjakov, ki so na voljo v njihovih organizacijah, z navedbo posebnih tehničnih znanj in spretnosti strokovnjakov.

3. CERT-EU lahko **na specifično zahtevo države članice, v kateri ima sedež prizadeti subjekt Unije, in z** [...] odobritvijo **prizadetega subjekta** [...] Unije strokovnjake, navedene na seznamu iz odstavka 2, pozove, naj prispevajo k odzivanju na večje **incidente** [...] **v** [...] **tem subjektu Unije** [...]**.**

Poglavje VI
KONČNE DOLOČBE

Člen 23

Začetne proračunske prerazporeditve

Komisija predlaga prerazporeditev osebja in finančnih virov iz zadevnih [...] **subjektov** Unije v proračun Komisije. Prerazporeditev se izvede hkrati s sprejetjem prvega proračuna po začetku veljavnosti te uredbe.

Člen 24

Pregled

1. IICB ob pomoči CERT-EU redno poroča Komisiji o izvajanju te uredbe. IICB lahko Komisiji izda tudi priporočila, naj **pregleda** [...] to uredbo.

2. Komisija poroča Evropskemu parlamentu in Svetu o izvajanju te uredbe najpozneje **36** [...] mesecev po začetku veljavnosti te uredbe in nato vsaka tri leta.

3. Komisija oceni delovanje te uredbe in poroča Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij **najpozneje** [...] pet let po datumu začetka veljavnosti. **Poročilu se po potrebi priloži zakonodajni predlog.**

Člen 25

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament	*Za Svet*
predsednik/predsednica	*predsednik/predsednica*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

PRILOGA II

[...]

[...]

[...]

[...]

[...]

[...]

[...]