Uradni list
Evropske unije

SL
Serija L

2023/2841

18.12.2023

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

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 ([1]),

ob upoštevanju naslednjega:

(1) V digitalni dobi je informacijska in komunikacijska tehnologija temelj odprte, učinkovite in neodvisne evropske uprave. Razvijajoča se tehnologija ter vse večja kompleksnost in medsebojna povezanost digitalnih sistemov povečujejo tveganja za kibernetsko varnost, zaradi česar so subjekti Unije ranljivejši za kibernetske grožnje in incidente, kar ogroža njihovo neprekinjeno poslovanje in zmogljivost zaščite njihovih podatkov. Medtem ko so večja uporaba storitev v oblaku, vsesplošna uporaba informacijske in komunikacijske tehnologije (IKT), visoka stopnja digitalizacije, delo na daljavo ter razvijajoča se tehnologija in povezljivost ključne značilnosti vseh dejavnosti subjektov Unije, 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, ključni 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 groženj svoje 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 IKT subjektov Unije so soodvisna in imajo vgrajene podatkovne tokove, njihovi uporabniki pa tesno sodelujejo. Ta medsebojna povezava pomeni, da ima lahko vsaka motnja, tudi če je sprva omejena na en subjekt Unije, širše kaskadne učinke, ki imajo lahko daljnosežne in dolgotrajne negativne učinke na druge subjekte Unije. Poleg tega so okolja IKT nekaterih subjektov Unije povezana z okolji IKT držav članic, zaradi česar incident v subjektu Unije predstavlja tveganje za kibernetsko varnost okolij IKT držav članic in obratno. Izmenjava informacij o posameznem incidentu lahko olajša odkrivanje 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 subjektov Unije potrebno, da z izvajanjem ukrepov za kibernetsko varnost, ki so sorazmerni z ugotovljenimi tveganji za kibernetsko varnost, izmenjavo informacij in sodelovanjem dosežejo visoko skupno raven kibernetske varnosti.

([1]) Stališče Evropskega parlamenta z dne 21. novembra 2023 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 8. decembra 2023.

(5) Cilj Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta ([2]) je nadalje izboljšati kibernetsko odpornost in zmogljivosti za odzivanje na incidente javnih in zasebnih subjektov, pristojnih organov ter Unije kot celote. Zato je potrebno zagotoviti, da subjekti Unije temu sledijo in zagotovijo pravila, ki so skladna z Direktivo (EU) 2022/2555 in izražajo njeno raven ambicij.

(6) Za doseganje visoke skupne ravni kibernetske varnosti je potrebno, da vsak subjekt Unije vzpostavi notranji okvir za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti (v nadaljnjem besedilu: okvir), ki zagotavlja učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost ter upošteva neprekinjeno poslovanje in krizno upravljanje. Z okvirom bi bilo treba oblikovati politike kibernetske varnosti, vključno s cilji in prednostnimi nalogami, za varnost omrežnih in informacijskih sistemov, ki zajemajo celotno netajno okolje IKT. Okvir bi moral temeljiti na pristopu, ki upošteva vse nevarnosti in katerega cilj je zaščititi omrežne 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 ter 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 omrežnih in informacijskih sistemov.

(7) Za obvladovanje tveganj za kibernetsko varnost, opredeljenih v okviru, bi moral vsak subjekt Unije sprejeti ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe. Ti ukrepi bi morali obravnavati področja in ukrepe za obvladovanje tveganj za kibernetsko varnost, določene v tej uredbi, da se okrepi kibernetska varnost vsakega subjekta Unije.

(8) Načrt za kibernetsko varnost, ki ga pripravi vsak subjekt Unije, bi moral odražati sredstva in tveganja za kibernetsko varnost, opredeljena v okviru, ter ugotovitve, ki izhajajo iz rednih ocen kibernetskovarnostne zrelosti. Načrt za kibernetsko varnost bi moral vključevati sprejete ukrepe za obvladovanje tveganj za kibernetsko varnost.

(9) Ker je zagotavljanje kibernetske varnosti neprekinjen proces, bi bilo treba ustreznost in učinkovitost ukrepov, sprejetih na podlagi te uredbe, redno pregledovati glede na spreminjajoča se tveganja za kibernetsko varnost, sredstva in kibernetskovarnostno zrelost subjektov Unije. Okvir bi bilo treba pregledovati redno in vsaj vsaka štiri leta, načrt za kibernetsko varnost pa bi bilo treba revidirati vsaki dve leti ali bolj pogosto, kadar je to potrebno, in sicer na podlagi ocen kibernetskovarnostne zrelosti ali morebitnega vsebinskega pregleda okvira.

(10) Ukrepi za obvladovanje tveganj za kibernetsko varnost, ki jih uvedejo subjekti Unije, bi morali vključevati politike, katerih cilj je, kadar je mogoče, da zagotovijo preglednost izvorne kode, pri tem pa upoštevajo zaščitne ukrepe za pravice tretjih oseb ali subjektov Unije. Te politike bi morale biti sorazmerne s tveganjem za kibernetsko varnost, njihov namen pa je olajšati analizo kibernetskih groženj, pri čemer pa ne ustvarjajo obveznosti razkritja ali pravic do dostopa do kod tretjih oseb, ki bi presegale veljavne pogodbene pogoje.

(11) Odprtokodna orodja in aplikacije za kibernetsko varnost lahko prispevajo k večji odprtosti. Odprti standardi omogočajo interoperabilnost med orodji za varnost in koristijo varnosti deležnikov. Odprtokodna orodja in aplikacije za kibernetsko varnost lahko spodbudijo širšo skupnost razvijalcev, kar omogoča diverzifikacijo dobaviteljev. Odprta koda lahko vodi k preglednejšemu postopku preverjanja orodij, povezanih s kibernetsko varnostjo, in k procesu odkrivanja ranljivosti, ki ga vodi skupnost. Subjekti Unije bi zato morali imeti možnost, da spodbujajo uporabo odprtokodne programske opreme in odprtih standardov z izvajanjem politik v zvezi z uporabo odprtih podatkov in odprte kode kot dela varnosti prek preglednosti.

([2]) 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) (UL L 333, 27.12.2022, str. 80).

(12) Zaradi razlik med subjekti Unije je potrebna prožnost v izvajanju te uredbe. Ukrepi za visoko skupno raven kibernetske varnosti, določeno v tej uredbi, ne bi smeli vključevati obveznosti, ki bi neposredno posegale v opravljanje nalog subjektov Unije ali posegale v njihovo institucionalno avtonomijo. Zato bi ti subjekti morali vzpostaviti lastne okvire ter sprejeti lastne ukrepe za obvladovanje tveganj za kibernetsko varnost in načrte 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. Ustrezno pozornost bi bilo treba nameniti tudi temu, da ukrepi ne bodo negativno vplivali na učinkovito izmenjavo informacij med subjekti Unije in njihovo sodelovanje ter izmenjavo informacij med subjekti Unije in sorodnimi organi držav članic in njihovo sodelovanje.

(13) Zaradi optimizacije uporabe virov bi morala ta uredba omogočati, da dva ali več subjektov Unije s podobnimi strukturami sodeluje pri ocenjevanju kibernetskovarnostne zrelosti za svoje zadevne subjekte.

(14) 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 za kibernetsko varnost zadevnih omrežnih in informacijskih sistemov, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. Vsak subjekt Unije bi moral za izboljšanje ravni kibernetske varnosti skušati dodeliti ustrezen delež svojega proračuna za IKT. Dolgoročno bi si bilo treba prizadevati za okvirni cilj v višini najmanj 10 %. Pri oceni kibernetskovarnostne zrelosti bi bilo treba oceniti, ali je izdatek, ki ga subjekt Unije nameni za kibernetsko varnost, sorazmeren s tveganji za kibernetsko varnost, s katerimi se sooča. Brez poseganja v pravila, ki se nanašajo na letni proračun Unije na podlagi Pogodb, bi morala Komisija v svojem predlogu prvega letnega proračuna, ki se sprejme po začetku veljavnosti te uredbe, pri oceni proračunskih in kadrovskih potreb subjektov Unije, ki izhajajo iz njihovih ocen odhodkov, upoštevati obveznosti, ki izhajajo iz te uredbe.

(15) Za visoko skupno raven kibernetske varnosti mora imeti nadzor nad kibernetsko varnostjo najvišja raven vodenja vsakega subjekta Unije. Najvišja raven vodenja subjekta Unije bi morala biti odgovorna za izvajanje te uredbe, tudi za vzpostavitev okvira, sprejetje ukrepov za obvladovanje tveganj za kibernetsko varnost in odobritev načrta za kibernetsko varnost. Obravnava kulture kibernetske varnosti, in sicer dnevno izvajanje kibernetske varnosti, je sestavni del okvira in ustreznih ukrepov za obvladovanje tveganj za kibernetsko varnost v vseh subjektih Unije.

(16) Varnost omrežnih in informacijskih sistemov, ki obravnavajo tajne podatki EU (EUCI), je bistvenega pomena. Subjekti Unije, ki ravnajo s tajnimi podatki EU, morajo uporabljati celovite regulativne okvire, vzpostavljene za varovanje takih informacij, vključno s posebnim upravljanjem, politikami in postopki za obvladovanje tveganj. Omrežni in informacijski sistemi, ki obravnavajo tajne podatke EU, morajo izpolnjevati strožje varnostne standarde kot netajni omrežni in informacijski sistemi. Zato so omrežni in informacijski sistemi, ki obravnavajo tajne podatke EU, odpornejši na kibernetske grožnje in incidente. Čeprav ta uredba priznava potrebo po skupnem okviru v zvezi s tem, se ne bi smela uporabljati za omrežne in informacijske sisteme, ki obravnavajo tajne podatke EU. Skupina za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (CERT-EU) pa bi morala imeti možnost, da subjektu Unije, če slednji to izrecno zahteva, zagotovi pomoč v zvezi z incidenti v tajnih okoljih IKT.

(17) Subjekti Unije bi morali oceniti tveganja za kibernetsko varnost, povezana z odnosi z dobavitelji in ponudniki storitev, vključno s ponudniki shranjevanja in obdelave podatkov ali upravljanih varnostnih storitev, ter sprejeti ustrezne ukrepe za njihovo obravnavo. Ukrepi za kibernetsko varnost bi morali biti podrobneje opredeljeni v smernicah ali priporočilih, ki jih izda CERT-EU. Pri pripravi ukrepov in smernic bi bilo treba ustrezno upoštevati najsodobnejše in po potrebi ustrezne evropske in mednarodne standarde ter ustrezno pravo in politike Unije, vključno z ocenami tveganja in priporočili skupine za sodelovanje, ustanovljene na podlagi člena 14 Direktive (EU) 2022/2555, kot sta usklajena ocena tveganja v EU za kibernetsko varnost omrežij 5G in nabor orodij EU za

kibernetsko varnost omrežij 5G. Ob upoštevanju okolja kibernetskih groženj in pomena krepitve kibernetske odpornosti subjektov Unije bi lahko bilo poleg tega potrebno certificiranje ustreznih proizvodov IKT, storitev IKT in postopkov IKT, na podlagi specifičnih evropskih certifikacijskih shem za kibernetsko varnost EU, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta ([3]).

(18) Generalni sekretarji institucij in organov Unije so maja 2011 sklenili, da bodo ustanovili predkonfiguracijsko skupino 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 Komisije z medinstitucionalnimi pristojnostmi. Institucije in organi Unije so decembra 2017 sklenili medinstitucionalni dogovor o organizaciji in delovanju CERT-EU ([4]). 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.

(19) CERT-EU bi bilo treba preimenovati v službo za kibernetsko varnost za institucije, organe, urade in agencije Unije, vendar bi bilo treba kratico CERT-EU zaradi prepoznavnosti imena ohraniti.

(20) Poleg tega, da se CERT-EU dodeli več nalog in razširjena vloga, ta uredba ustanavlja Medinstitucionalni odbor za kibernetsko varnost (IICB), da bi se olajšalo doseganje visoke skupne ravni kibernetske varnosti med subjekti Unije. IICB bi moral imeti izključno vlogo pri spremljanju in podpiranju izvajanja te uredbe s strani subjektov Unije ter pri nadzorovanju izvajanja splošnih prednostnih nalog in ciljev s strani CERT-EU in pri zagotavljanju njegovih strateških usmeritev. IICB bi zato moral zagotoviti zastopanost institucij Unije ter vključevati predstavnike organov, uradov in agencij Unije prek mreže agencij EU (EUAN). 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 usmeritve za IICB. Poleg tega bi moral imeti IICB možnost, da 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, ureditve izvajanja sporazumov o ravni storitev, ocene dokumentov in poročil, ki jih subjekti Unije predložijo IICB na podlagi te uredbe, 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.

(21) IICB si prizadeva, da z izvajanjem te uredbe podpira subjekte Unije pri izboljšanju njihovega odnosa do kibernetske varnosti. Da bi podpiral subjekte Unije, bi moral IICB vodji CERT-EU zagotoviti usmeritve, sprejeti večletno strategijo za dvig ravni kibernetske varnosti v subjektih Unije, določiti metodologijo za prostovoljne medsebojne strokovne preglede in druge vidike teh pregledov ter spodbuditi ustanovitev neformalne skupine lokalnih uradnikov za kibernetsko varnost, ki bi jo podpirala Agencija Evropske unije za kibernetsko varnost (ENISA), namenjena pa bi bila izmenjavi dobrih praks in informacij v zvezi z izvajanjem te uredbe.

([3]) 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).

([4]) Dogovor med Evropskim parlamentom, Evropskim svetom, Svetom Evropske unije, Evropsko komisijo, Sodiščem Evropske unije, Evropsko centralno banko, Evropskim računskim sodiščem, Evropsko službo za zunanje delovanje, Evropskim ekonomsko-socialnim odborom, Evropskim odborom regij in Evropsko investicijsko banko o organizaciji in delovanju skupine za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (CERT-EU) (UL C 12, 13.1.2018, str. 1).

(22) Da bi dosegli visoko raven kibernetske varnosti v vseh subjektih Unije, bi morali interese organov, uradov in agencij Unije, ki upravljajo svoja okolja IKT, v IICB zastopati trije predstavniki, ki jih imenuje mreža agencij EU. Varnost obdelave osebnih podatkov in s tem tudi njena kibernetska varnost je temelj varstva podatkov. Glede na sinergije med varstvom podatkov in kibernetsko varnostjo bi moral biti Evropski nadzornik za varstvo podatkov v IICB zastopan kot subjekt Unije, za katerega se uporablja ta uredba, s posebnim strokovnim znanjem na področju varstva podatkov, vključno z varnostjo elektronskih komunikacijskih omrežij. Zaradi pomena inovacij in konkurenčnosti na področju kibernetske varnosti bi moral biti v IICB zastopan Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost. Glede na vlogo ENISA kot središča strokovnega znanja na področju kibernetske varnosti in podporo, ki jo ENISA zagotavlja, ter glede na pomen kibernetske varnosti vesoljske infrastrukture in storitev Unije bi morali biti v IICB zastopani ENISA in Agencija Evropske unije za vesoljski program. Glede na vlogo, ki jo ima na podlagi te uredbe CERT-EU, bi moral predsednik IICB povabiti vodjo CERT-EU na vse sestanke IICB, razen kadar IICB razpravlja o zadevah, ki se neposredno nanašajo na vodjo CERT-EU.

(23) IICB bi moral spremljati skladnost s to uredbo ter izvajanje smernic in priporočil ter 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. Te tehnične svetovalne skupine bi morale tesno sodelovati s CERT-EU, subjekti Unije ter po potrebi z drugimi deležniki.

(24) Kadar IICB ugotovi, da subjekt Unije ni učinkovito izvajal te uredbe ali smernic, priporočil ali pozivov k ukrepanju, izdanih na podlagi te uredbe, bi moral imeti možnost, da brez poseganja v notranje postopke zadevnega subjekta Unije sprejme ukrepe za skladnost. IICB bi moral ukrepe za skladnost uporabljati postopoma, kar pomeni, da bi moral najprej sprejeti najmanj strog ukrep, in sicer obrazloženo mnenje, ter le, če je potrebno, sprejemati vse strožje ukrepe, dokler ne pride do najstrožjega ukrepa, in sicer priporočila za začasno prekinitev prenosov podatkov zadevnemu subjektu Unije. Tako priporočilo bi bilo treba uporabiti le v izjemnih primerih, ko zadevni subjekt Unije dolgotrajno, namerno, ponavljajoče ali resno krši to uredbo.

(25) Obrazloženo mnenje je najmanj strog ukrep za skladnost, s katerim se obravnavajo opažene vrzeli pri izvajanju te uredbe. IICB bi moral imeti možnost, da po izdaji obrazloženega mnenja sprejme usmeritve, s katerimi subjektu Unije pomaga zagotoviti, da so njegov okvir, ukrepi za obvladovanje tveganj za kibernetsko varnost, načrt za kibernetsko varnost in poročanje v skladu s to uredbo, ter nato izda opozorilo, da je treba ugotovljene pomanjkljivosti subjekta Unije v določenem roku odpraviti. Če pomanjkljivosti, ugotovljene v opozorilu, niso bile ustrezno odpravljene, bi moral imeti IICB možnost, da izda utemeljeno uradno obvestilo.

(26) IICB bi moral imeti možnost, da priporoči izvedbo revizije subjekta Unije. Subjekt Unije bi moral imeti možnost, da v ta namen uporabi svojo funkcijo notranje revizije. IICB bi moral imeti tudi možnost, da zahteva, da revizijo izvede neodvisna revizijska služba, kar zajema tudi vzajemno dogovorjenega ponudnika storitev iz zasebnega sektorja.

(27) V izrednih primerih dolgotrajnih, namernih, ponavljajočih se ali resnih kršitev te uredbe s strani subjekta Unije bi moral imeti IICB možnost, da kot skrajni ukrep priporoči vsem državam članicam in subjektom Unije, naj začasno prekinejo prenose podatkov subjektu Unije, kar ostane v veljavi, dokler subjekt Unije ne preneha s kršitvijo. Tako priporočilo bi bilo treba posredovati po ustreznih in varnih komunikacijskih kanalih.

(28) Za zagotovitev pravilnega izvajanja te uredbe bi moral IICB, če meni, da je vztrajno kršenje te uredbe s strani subjekta Unije neposredna posledica dejanj ali opustitev dejanj člana njegovega osebja, tudi na najvišji ravni vodenja, od zadevnega subjekta Unije zahtevati, da sprejme ustrezne ukrepe, vključno z zahtevo, naj preuči možnost sprejetja disciplinskih ukrepov v skladu s pravili in postopki iz Kadrovskih predpisov za uradnike Evropske unije in pogojev za zaposlitev drugih uslužbencev Unije, določenih v Uredbi Sveta (EGS, Euratom, ESPJ) št. 259/68 ([5]) (v nadaljnjem besedilu: kadrovski predpisi), ter vsemi drugimi veljavnimi pravili in postopki.

(29) CERT-EU bi moral prispevati k varnosti okolja IKT vseh subjektov Unije. CERT-EU bi moral pri odločanju, ali naj na prošnjo subjekta Unije zagotovi tehnično svetovanje ali prispevek o ustreznih zadevah politike, poskrbeti za to, da to ne bo oviralo izpolnjevanja drugih nalog, ki so mu bile dodeljene na podlagi te uredbe. CERT-EU bi moral delovati na strani subjektov Unije kot enakovreden koordinatorju, imenovanemu za usklajeno razkrivanje ranljivosti na podlagi člena 12(1) Direktive (EU) 2022/2555.

(30) 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, kadar bi bilo potrebno, izdati pozive k ukrepanju, ki opisujejo nujne varnostne ukrepe, ki naj bi jih subjekti Unije nujno sprejeli v določenem časovnem obdobju. IICB bi moral naročiti CERT-EU, da izda, umakne ali spremeni predlog za smernice ali priporočilo ali poziv k ukrepanju.

(31) CERT-EU bi moral tudi izpolnjevati vlogo, ki je zanj predvidena v Direktivi (EU) 2022/2555, v zvezi s sodelovanjem in izmenjavo informacij z mrežo skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT), ustanovljeno na podlagi člena 15 navedene direktive. Poleg tega bi moral CERT-EU v skladu s Priporočilom Komisije (EU) 2017/1584 ([6]) sodelovati z zadevnimi deležniki in se z njimi usklajevati glede odzivanja. Za prispevanje k visoki ravni kibernetske varnosti v Uniji bi CERT-EU moral s sorodnimi organi držav članic deliti informacije, povezane z incidenti. Prav tako bi CERT-EU moral sodelovati z drugimi javnimi in zasebnimi sorodnimi organi, vključno z Natom, pri čemer sodelovanje predhodno odobri IICB.

(32) Pri podpori operativni kibernetski varnosti bi moral CERT-EU prek strukturiranega sodelovanja izkoriščati razpoložljivo strokovno znanje ENISA, kot je predvideno v Uredbi (EU) 2019/881. Kadar je potrebno, bi bilo treba sprejeti posebne dogovore med tema dvema subjektoma, s katerimi bi opredelili praktično izvajanje takega sodelovanja in se izogibali podvajanju dejavnosti. CERT-EU bi moral z ENISA sodelovati v zvezi z analizo kibernetskih groženj in ENISA redno posredovati svoje poročilo o grožnjah.

(33) CERT-EU bi moral imeti možnost sodelovanja in izmenjave informacij z ustreznimi skupnostmi za kibernetsko varnost v Uniji in njenih državah članicah, da bi se olajšalo operativno sodelovanje in se obstoječim mrežam omogočilo, da pri varovanju Unije uresničijo ves svoj potencial.

(34) Ker so storitve in naloge CERT-EU v interesu subjektov Unije, bi moral vsak subjekt Unije, ki ima izdatke za IKT, prispevati pravičen delež k tem storitvam in nalogam. Ti prispevki ne posegajo v proračunsko avtonomijo subjektov Unije.

([5]) Uredba Sveta (EGS, Euratom, ESPJ) št. 259/68 z dne 29. februarja 1968 o kadrovskih predpisih za uradnike in pogojih za zaposlitev drugih uslužbencev Evropskih skupnosti in o posebnih ukrepih, ki se začasno uporabljajo za uradnike Komisije (UL L 56, 4.3.1968, str. 1).

([6]) 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).

(35) 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 in okrevanje po incidentih, bi morali imeti subjekti Unije možnost uradno obvestiti CERT-EU o incidentih, kibernetskih grožnjah, ranljivostih in skorajšnjih incidentih ter deliti ustrezne tehnične podrobnosti, ki omogočajo odkrivanje ali blaženje podobnih kibernetskih groženj, ranljivosti in skorajšnjih incidentov ter odzivanje nanje v drugih subjektih Unije. V skladu z enakim pristopom, kot je predviden v Direktivi (EU) 2022/2555, bi morali subjekti Unije v 24 urah po tem, ko se seznanijo s pomembnim incidentom, CERT-EU posredovati zgodnje opozorilo. Taka izmenjava informacij bi morala CERT-EU omogočiti, da informacije razširja drugim subjektom Unije ter ustreznim sorodnim organom in tako prispeva k zaščiti okolij IKT subjektov Unije in okolij IKT sorodnih organov subjektov Unije pred podobnimi incidenti.

(36) Ta uredba določa večstopenjski pristop k poročanju o pomembnih incidentih, da bi se na eni strani vzpostavilo ustrezno ravnovesje med 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 in prispeva k izboljšanju njihovega splošnega odnosa do kibernetske varnosti. V zvezi s tem bi morala ta uredba vključevati poročanje o incidentih, ki bi na podlagi začetne ocene, ki jo izvede zadevni subjekt Unije, lahko povzročili resne operativne motnje v delovanju 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 prizadete omrežne in informacijske sisteme, zlasti njihov pomen za delovanje subjekta Unije, resnost in tehnične značilnosti kibernetske grožnje in vse s tem povezane ranljivosti, ki se izkoriščajo, ter izkušnje subjekta Unije s podobnimi incidenti. Kazalniki, kot so obseg prizadetosti delovanja subjekta Unije, trajanje incidenta ali število prizadetih fizičnih ali pravnih oseb, bi lahko imeli pomembno vlogo pri ugotavljanju, ali je operativna motnja resna.

(37) Ker so infrastruktura ter omrežni in informacijski sistemi zadevnega subjekta Unije in države članice, v kateri se ta subjekt Unije nahaja, med seboj povezani, je bistveno, da je ta država članica brez nepotrebnega odlašanja obveščena o pomembnem incidentu znotraj tega subjekta Unije. V ta namen bi moral prizadeti subjekt Unije obvestiti vse ustrezne sorodne organe iz držav članic, imenovane ali ustanovljene na podlagi členov 8 in 10 Direktive (EU) 2022/2555, o pojavu pomembnega incidenta, o katerem poroča CERT-EU. Ko CERT-EU izve, da se je zgodil pomemben incident v državi članici, bi moral uradno obvestiti vsak ustrezni sorodni organ v tej državi članici.

(38) 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. Predstavnik Komisije v IICB bi moral biti v skladu z načrtom za obvladovanje kibernetskih kriz kontaktna točka, da se IICB olajša izmenjavo ustreznih informacij v zvezi z večjimi incidenti z evropsko organizacijsko mrežo za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kar bi prispevalo k skupnemu situacijskemu zavedanju. Vloga predstavnika Komisije v IICB kot kontaktne točke ne bi smela posegati v ločeno in posebno vlogo Komisije v mreži EU-CyCLONe na podlagi člena 16(2) Direktive (EU) 2022/2555.

(39) Za vsako obdelavo osebnih podatkov, ki se izvaja na podlagi te uredbe, se uporablja Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta ([7]). Obdelava osebnih podatkov bi lahko potekala v zvezi z ukrepi, sprejetimi v okviru obvladovanja tveganj za kibernetsko varnost, obvladovanja ranljivosti in incidentov, izmenjave informacij o incidentih, kibernetskih grožnjah in ranljivostih ter usklajevanja in sodelovanja pri odzivanju na incidente. Taki ukrepi bi lahko zahtevali obdelavo nekaterih kategorij osebnih podatkov, kot so naslovi IP, enotni naslovi virov (URL), domenska imena, elektronski naslovi, organizacijske vloge posameznika, na katerega se nanašajo osebni

([7]) 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).

podatki, časovni žigi, zadeve elektronske pošte ali imena datotek. Vsi ukrepi, sprejeti na podlagi te uredbe, bi morali biti skladni z okvirom za varstvo podatkov in zasebnosti, subjekti Unije, CERT-EU in po potrebi IICB, pa bi morali sprejeti vse ustrezne tehnične in organizacijske zaščitne ukrepe za zagotovitev takšne skladnosti na odgovoren način.

(40) Ta uredba določa pravno podlago za obdelavo osebnih podatkov, ki jo izvajajo subjekti Unije, CERT-EU in, kadar je ustrezno, IICB, za namene opravljanja njihovih nalog in izpolnjevanja obveznosti iz te uredbe v skladu s členom 5(1), točka (b), Uredbe (EU) 2018/1725. CERT-EU lahko deluje kot obdelovalec ali upravljavec glede na nalogo, ki jo opravlja na podlagi Uredbe (EU) 2018/1725.

(41) V nekaterih primerih bodo subjekti Unije in CERT-EU zaradi izpolnjevanja svojih obveznosti iz te uredbe za zagotovitev visoke ravni kibernetske varnosti ter zlasti v okviru obvladovanja ranljivosti in incidentov morda morali obdelati posebne kategorije osebnih podatkov iz člena 10(1) Uredbe (EU) 2018/1725. Ta uredba določa pravno podlago za obdelavo posebnih vrst osebnih podatkov, ki jo izvajajo subjekti Unije in CERT-EU v skladu s členom 10(2), točka (g), Uredbe (EU) 2018/1725. Obdelava posebnih kategorij osebnih podatkov na podlagi te uredbe bi morala biti strogo sorazmerna z zastavljenim ciljem. Pod pogoji iz člena 10(2), točka (g), navedene uredbe bi morali imeti subjekti Unije in CERT-EU možnost obdelave takih podatkov le v obsegu, ki je potreben in kadar je to izrecno določeno v tej uredbi. Pri obdelavi posebnih kategorij osebnih podatkov bi morali subjekti Unije in CERT-EU spoštovati bistvo pravice do varstva podatkov ter določati ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznikov, na katere se podatki nanašajo.

(42) Na podlagi člena 33 Uredbe (EU) 2018/1725 bi morali subjekti Unije in CERT-EU ob upoštevanju najnovejšega tehnološkega razvoja, stroškov izvajanja, narave, obsega, okoliščin in namenov obdelave ter tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, izvesti ustrezne tehnične in organizacijske ukrepe za zagotovitev ustrezne ravni varnosti osebnih podatkov, kot so zagotavljanje omejenih pravic dostopa na podlagi potrebe po seznanitvi, uporaba načel revizijske sledi, sprejetje nadzorne verige, shranjevanje podatkov v mirovanju v nadzorovanem in revidiranem okolju, standardizirani operativni postopki in ukrepi za ohranjanje zasebnosti, kot so psevdonimizacija ali šifriranje. Ti ukrepi se ne bi smeli izvajati na način, ki bi vplival na namene obvladovanja incidentov in celovitosti dokazov. Kadar subjekt Unije ali CERT-EU prenese osebne podatke, povezane z incidentom, vključno s posebnimi kategorijami osebnih podatkov, sorodnemu organu ali partnerju za namene te uredbe, bi morali biti taki prenosi skladni z Uredbo (EU) 2018/1725. Kadar se posebne vrste osebnih podatkov prenesejo tretji osebi, bi morali subjekti Unije in CERT-EU zagotoviti, da tretja oseba uporablja ukrepe v zvezi z varstvom osebnih podatkov na ravni, enakovredni Uredbi (EU) 2018/1725.

(43) Osebne podatke, ki se obdelujejo za namene te uredbe, bi bilo treba hraniti le toliko časa, kolikor je potrebno v skladu z Uredbo (EU) 2018/1725. Subjekti Unije in po potrebi CERT-EU, ki delujejo kot upravljavec, bi morali določiti obdobja hrambe, ki so omejena na tisto, kar je potrebno za doseganje določenih namenov. Zlasti v zvezi z osebnimi podatki, zbranimi za obvladovanje incidentov, bi morali subjekti Unije in CERT-EU razlikovati med osebnimi podatki, ki se zbirajo za odkrivanje kibernetske grožnje v njihovih okoljih IKT, da bi preprečili incident, in osebnimi podatki, ki se zbirajo za ublažitev incidenta, odzivanje nanj in okrevanje po njem. Za odkrivanje kibernetskih groženj je pomembno upoštevati čas, v katerem lahko akter grožnje v sistemu ostane neodkrit. Za ublažitev incidenta, odziv nanj in okrevanje po njem je pomembno proučiti, ali so osebni podatki potrebni za sledenje in obravnavanje ponavljajočega se incidenta ali incidenta podobne narave, za katerega bi bilo mogoče dokazati korelacijo.

(44) Subjekti Unije in CERT-EU bi morali pri ravnanju z informacijami upoštevati veljavna pravila o informacijski varnosti. Vključitev varnosti človeških virov kot ukrepa za obvladovanje tveganj za kibernetsko varnost bi tudi morala biti skladna z veljavnimi pravili.

(45) Za izmenjavo informacij se uporabljajo vidne oznake, ki označujejo, da morajo prejemniki informacij zlasti na podlagi sporazumov o zaupnosti ali neformalnih sporazumov o zaupnosti, kot je semaforski protokol, ali na podlagi drugih jasnih navedb s strani vira, upoštevati omejitve pri izmenjavi informacij. Semaforski protokol je treba razumeti kot sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij. Uporablja se v skoraj vseh skupinah CSIRT ter v nekaterih centrih za analizo in izmenjavo informacij.

(46) To uredbo bi bilo treba redno ocenjevati glede na prihodnja pogajanja o večletnih finančnih okvirih, ki bodo omogočila nadaljnje odločitve glede delovanja in institucionalne vloge CERT-EU, vključno z morebitno ustanovitvijo CERT-EU kot urada Unije.

(47) 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. V tem poročilu bi bilo treba ob prispevku IICB oceniti ustreznost vključitve omrežnih in informacijskih sistemov, ki obravnavajo tajne podatke EU, v področje uporabe te uredbe, zlasti ob odsotnosti pravil o informacijski varnosti, ki bi bila skupna subjektom Unije.

(48) V skladu z načelom sorazmernosti je potrebno in primerno, da se za doseganje osnovnega cilja zagotovitve visoke skupne ravni kibernetske varnosti v subjektih Unije določijo pravila o kibernetski varnosti za subjekte Unije. V skladu s členom 5(4) Pogodbe o Evropski uniji ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(49) Ta uredba odraža dejstvo, da se subjekti Unije razlikujejo po velikosti in zmogljivostih, tudi v smislu finančnih in človeških virov.

(50) V skladu s členom 42(1) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 17. maja 2022 ([8]) –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

Ta uredba določa ukrepe, katerih cilj je doseči visoko skupno raven kibernetske varnosti v subjektih Unije v zvezi z:

(a) notranjim okvirom za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti na podlagi člena 6, ki ga vzpostavi vsak subjekt Unije;

(b) obvladovanjem tveganj za kibernetsko varnost, poročanjem in izmenjavo informacij;

(c) 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;

(d) spremljanjem izvajanja te uredbe;

([8]) UL C 258, 5.7.2022, str. 10.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za subjekte Unije, Medinstitucionalni odbor za kibernetsko varnost, ustanovljen na podlagi člena 10, in CERT-EU.

2. Ta uredba se uporablja brez poseganja v institucionalno avtonomijo na podlagi Pogodb.

3. Z izjemo člena 13(8) se ta uredba ne uporablja za omrežne in informacijske sisteme, s katerimi se obravnavajo 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 (PDEU) ali Pogodbo o ustanovitvi Evropske skupnosti za atomsko energijo ali na njihovi podlagi;

(2) „omrežni in informacijski sistem“ pomeni omrežni in informacijski sistem, kakor je opredeljen v členu 6, točka 1, Direktive (EU) 2022/2555;

(3) „varnost omrežnih in informacijskih sistemov“ pomeni varnost omrežnih in informacijskih sistemov, kakor je opredeljena v členu 6, točka 2, Direktive (EU) 2022/2555;

(4) „kibernetska varnost“ pomeni kibernetsko varnost, kakor je opredeljena v členu 2, točka 1, Uredbe (EU) 2019/881;

(5) „najvišja raven vodenja“ pomeni vodjo, vodstveni organ ali organ za usklajevanje in nadzor, pristojen za delovanje subjekta Unije, na najvišji upravni ravni, ki ima pristojnost za sprejemanje ali odobritev odločitev v skladu z ureditvijo upravljanja na visoki ravni tega subjekta Unije, brez poseganja v formalno odgovornost drugih ravni vodstva za skladnost in upravljanje kibernetskih tveganj na njihovih področjih odgovornosti;

(6) „skorajšnji incident“ pomeni skorajšnji incident, kakor je opredeljen v členu 6, točka 5, Direktive (EU) 2022/2555;

(7) „incident“ pomeni incident, kakor je opredeljen v členu 6, točka 6, Direktive (EU) 2022/2555;

(8) „večji incident“ pomeni incident, ki povzroči stopnjo motnje, ki presega zmogljivost subjekta Unije in CERT-EU, da se nanjo odzoveta, ali ki pomembno vpliva na vsaj dva subjekta Unije;

(9) „kibernetski incident velikih razsežnosti“ pomeni kibernetski incident velikih razsežnosti, kakor je opredeljen v členu 6, točka 7, Direktive (EU) 2022/2555;

(10) „obvladovanje incidentov“ pomeni obvladovanje incidentov, kakor je opredeljeno v členu 6, točka 8, Direktive (EU) 2022/2555;

(11) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kakor je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(12) „pomembna kibernetska grožnja“ pomeni pomembno kibernetsko grožnjo, kakor je opredeljena v členu 6, točka 11, Uredbe (EU) 2022/2555;

(13) „ranljivost“ pomeni ranljivost, kakor je opredeljena v členu 6, točka 15, Direktive (EU) 2022/2555;

(14) „kibernetsko tveganje“ pomeni tveganje, kakor je opredeljeno v členu 6, točka 9, Direktive (EU) 2022/2555;

(15) „storitev računalništva v oblaku“ pomeni storitev v oblaku, kakor je opredeljena v členu 6, točka 30, Direktive (EU) 2022/2555;

Člen 4

Obdelava osebnih podatkov

1. CERT-EU, Medinstitucionalni odbor za kibernetsko varnost, ustanovljen na podlagi člena 10, in subjekti Unije osebne podatke na podlagi te uredbe obdelujejo v skladu z Uredbo (EU) 2018/1725.

2. Kadar opravljajo naloge ali izpolnjujejo obveznosti na podlagi te uredbe, CERT-EU, Medinstitucionalni odbor za kibernetsko varnost, ustanovljen na podlagi člena 10, in subjekti Unije obdelujejo in izmenjujejo osebne podatke le v obsegu, ki je potreben in izključno za namen opravljanja teh nalog ali izpolnjevanja teh obveznosti.

3. Obdelava posebnih kategorij osebnih podatkov iz člena 10(1) Uredbe (EU) 2018/1725 se šteje za potrebno iz razlogov bistvenega javnega interesa na podlagi člena 10(2), točka (g), navedene uredbe. Taki podatki se lahko obdelujejo le v obsegu, ki je potreben za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost iz členov 6 in 8, zagotavljanje storitev CERT-EU na podlagi člena 13, izmenjavo informacij o incidentih na podlagi člena 17(3) in člena 18(3), izmenjavo informacij na podlagi člena 20, obveznosti poročanja na podlagi člena 21, usklajevanje in sodelovanje pri odzivanju na incidente na podlagi člena 22 ter obvladovanje večjih incidentov na podlagi člena 23 te uredbe. Subjekti Unije in CERT-EU, kadar delujejo kot upravljavci podatkov, uporabijo tehnične ukrepe, s katerimi preprečijo obdelavo posebnih kategorij osebnih podatkov za druge namene, ter zagotovijo ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznikov, na katere se nanašajo osebni podatki.

POGLAVJE II

UKREPI ZA VISOKO SKUPNO RAVEN KIBERNETSKE VARNOSTI

Člen 5

Izvajanje ukrepov

1. Medinstitucionalni odbor za kibernetsko varnost, ustanovljen na podlagi člena 10, do 8. septembra 2024 po posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA) in po prejetju usmeritev s strani CERT-EU izda smernice za subjekte Unije za namene izvajanja začetnega pregleda kibernetske varnosti in vzpostavitve notranjega okvira za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti na podlagi člena 6, izvajanja ocene kibernetsko-varnostne zrelosti na podlagi člena 7, uvedbe ukrepov za obvladovanje tveganj za kibernetsko varnost na podlagi člena 8 in sprejetja načrta za kibernetsko varnost na podlagi člena 9.

2. Subjekti Unije pri izvajanju členov 6 do 9 upoštevajo smernice iz odstavka 1 tega člena ter ustrezne smernice in priporočila, sprejeta na podlagi členov 11 in 14.

Člen 6

Okvir za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti

1. Vsak subjekt Unije do 8. aprila 2025 po opravljenem začetnem pregledu kibernetske varnosti, kot je revizija, vzpostavi notranji okvir za obvladovanje tveganj, upravljanje in nadzor kibernetske varnosti (v nadaljnjem besedilu: okvir). Vzpostavitev okvira nadzoruje ter je zanjo odgovorna najvišja raven vodenja subjekta Unije.

2. Okvir zajema celotno netajno okolje IKT zadevnega subjekta Unije, vključno z vsem lokalnim okoljem IKT in lokalnim operativnim tehnološkim omrežjem, sredstvi in storitvami v okoljih storitev 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 s temi okolji (v nadaljnjem besedilu: okolje IKT). Okvir temelji na pristopu, ki upošteva vse nevarnosti.

3. Okvir zagotavlja visoko raven kibernetske varnosti. V okviru so določene notranje politike kibernetske varnosti skupaj s cilji in prednostnimi nalogami za varnost omrežnih in informacijskih sistemov ter vloge in odgovornosti osebja subjekta Unije, zadolženega za uspešno izvajanje te uredbe. Okvir vključuje tudi mehanizme za merjenje učinkovitosti izvajanja.

4. Okvir se pregleduje redno in vsaj vsaka štiri leta glede na spreminjajoča se tveganja za kibernetsko varnost. Po potrebi in na zaprosilo Medinstitucionalnega odbora za kibernetsko varnost, ustanovljenega na podlagi člena 10, se lahko okvir subjekta Unije posodobi na podlagi usmeritev CERT-EU o ugotovljenih incidentih ali morebitnih opaženih vrzelih pri izvajanju te uredbe.

5. Najvišja raven vodenja vsakega subjekta Unije je odgovorna za izvajanje te uredbe in nadzira skladnost svoje organizacije z obveznostmi, povezanimi z okvirom.

6. Kadar je to primerno in brez poseganja v svojo odgovornost za izvajanje te uredbe, lahko najvišja raven vodenja vsakega subjekta Unije prenese na visoke uradnike v smislu člena 29(2) kadrovskih predpisov ali druge uradnike na enakovredni ravni znotraj zadevnega subjekta Unije posebne obveznosti iz te uredbe. Ne glede na tak morebiten prenos lahko najvišja raven vodenja odgovarja za kršitve te uredbe s strani zadevnega subjekta Unije.

7. Vsak subjekt Unije ima vzpostavljene učinkovite mehanizme za zagotavljanje, da se za kibernetsko varnost nameni ustrezen delež proračuna za IKT. Pri določanju navedenega odstotka se ustrezno upošteva okvir.

8. 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, ali se te naloge razdelijo med več subjektov Unije. Kadar se te naloge prenesejo na CERT-EU, Medinstitucionalni odbor za kibernetsko varnost, ustanovljen na podlagi člena 10, 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 odlašanja uradno obvesti CERT-EU o imenovanem lokalnem uradniku za kibernetsko varnost in vseh naknadnih spremembah v zvezi s tem.

CERT-EU vzpostavi in redno posodablja seznam imenovanih lokalnih uradnikov za kibernetsko varnost.

9. Višji uradniki v smislu člena 29(2) kadrovskih predpisov ali drugi uradniki na enakovredni ravni vsakega subjekta Unije ter vsi ustrezni člani osebja, ki je zadolženo za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost in izpolnjevanje obveznosti iz te uredbe, redno opravljajo posebno usposabljanje, da pridobijo dovolj znanja in spretnosti za razumevanje in oceno tveganj za kibernetsko varnost in praks njihovega obvladovanja ter njihovega vpliva na delovanje subjekta Unije.

Člen 7

Ocene kibernetskovarnostne zrelosti

1. Vsak subjekt Unije do 8. julija 2025 in nato najmanj vsaki dve leti izvede oceno kibernetskovarnostne zrelosti, ki vključuje vse elemente njegovega okolja IKT.

2. Kadar je primerno, se ocene kibernetskovarnostne zrelosti izvedejo s pomočjo specializirane tretje strani.

3. Subjekti Unije s podobno strukturo lahko sodelujejo pri izvajanju ocen kibernetskovarnostne zrelosti za svoje ustrezne subjekte.

4. Na zaprosilo Medinstitucionalnega odbora za kibernetsko varnost, ustanovljenega na podlagi člena 10, in z izrecnim soglasjem zadevnega subjekta Unije se lahko o rezultatih ocene kibernetskovarnostne zrelosti razpravlja v okviru navedenega odbora ali neformalne skupine lokalnih uradnikov za kibernetsko varnost, da bi se učili iz izkušenj ter izmenjali dobre prakse.

Člen 8

Ukrepi za obvladovanje tveganj za kibernetsko varnost

1. Brez nepotrebnega odlašanja in v vsakem primeru 8. septembra 2025 vsak subjekt Unije pod nadzorom svoje najvišje ravni vodenja sprejme ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za kibernetsko varnost, opredeljene v okviru, in da se prepreči ali čim bolj zmanjša učinek incidentov. Ob upoštevanju najsodobnejših in po potrebi ustreznih evropskih in mednarodnih standardov ti ukrepi zagotavljajo raven varnosti omrežnih in informacijskih sistemov v celotnem okolju IKT, ki je sorazmerna s tveganji za kibernetsko varnost. Pri ocenjevanju sorazmernosti teh ukrepov se ustrezno upoštevajo stopnja izpostavljenosti subjekta Unije tveganjem za kibernetsko varnost, njegova velikost ter verjetnost pojava incidentov in njihova resnost, vključno z njihovim družbenim, gospodarskim in medinstitucionalnim vplivom.

2. Subjekti Unije pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost obravnavajo vsaj naslednja področja:

(a) politiko na področju kibernetske varnosti, vključno z ukrepi, potrebnimi za uresničevanje ciljev in prednostnih nalog iz člena 6 in odstavka 3 tega člena;

(b) politike o analizi tveganj za kibernetsko varnost in o varnosti informacijskih sistemov;

(c) cilje politike glede uporabe storitev računalništva v oblaku;

(d) po potrebi revizijo kibernetske varnosti, ki lahko vključuje oceno tveganj za kibernetsko varnost, ranljivosti in kibernetskih groženj ter penetracijsko testiranje, ki ga redno izvaja zaupanja vreden zasebni ponudnik;

(e) izvajanje priporočil, pripravljenih na podlagi revizij kibernetske varnosti iz točke (d), in sicer s posodobitvijo kibernetske varnosti in politik;

(f) organizacijo kibernetske varnosti, vključno z določitvijo vlog in odgovornosti;

(g) upravljanje sredstev, vključno s popisom sredstev IKT in kartografijo omrežja IKT;

(h) varnost človeških virov in nadzor dostopa;

(i) varnost operacij;

(j) varnost komunikacij;

(k) pridobivanje, razvoj in vzdrževanje sistema, vključno s politikami o obravnavi in razkrivanju ranljivosti;

(l) po možnosti politike o preglednosti izvorne kode;

(m) varnost dobavne verige, vključno z varnostnimi vidiki odnosov med vsakim subjektom Unije in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

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

(o) upravljanje neprekinjenega poslovanja, kot je upravljanje varnostnih kopij in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih, ter obvladovanje kriz ter

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

Za namene prvega pododstavka, točka (m), 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.

3. Subjekti Unije sprejmejo vsaj naslednje posebne ukrepe za obvladovanje tveganj za kibernetsko varnost:

(a) tehnične ureditve za omogočanje in ohranjanje dela na daljavo;

(b) konkretne ukrepe za prehod na načela ničelnega zaupanja;

(c) uporabo večfaktorske avtentifikacije kot norme v omrežnih in informacijskih sistemih;

(d) uporabo kriptografije in šifriranja, zlasti šifriranja od konca do konca ter varnega digitalnega podpisovanja;

(e) kadar je primerno, vzpostavitev varnega glasovnega, video- in besedilnega sporočanja ter varnih sistemov za komunikacijo v sili znotraj subjekta Unije;

(f) proaktivne ukrepe za odkrivanje in odstranjevanje zlonamerne in vohunske programske opreme;

(g) vzpostavitev varnosti dobavne verige programske opreme z merili za razvoj in oceno varne programske opreme;

(h) vzpostavitev in sprejetje programov za usposabljanje o kibernetski varnosti, ki so sorazmerni s predpisanimi nalogami in pričakovanimi zmogljivostmi najvišje ravni vodenja ter članov osebja subjekta Unije, ki je zadolženo za zagotavljanje učinkovitega izvajanja te uredbe;

(i) redno usposabljanje zaposlenih na področju kibernetske varnosti;

(j) kadar je ustrezno, udeležbo pri analizah tveganja medsebojne povezljivosti med subjekti Unije;

(k) krepitev pravil o javnem naročanju, da se omogoči visoka skupna raven kibernetske varnosti, in sicer:

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

   (ii) s pogodbenimi obveznostmi glede poročanja o incidentih, ranljivostih in kibernetskih grožnjah ter glede vzpostavitve ustreznih mehanizmov odzivanja na incidente in njihovega spremljanja.

Člen 9

Načrti za kibernetsko varnost

1. Najvišja raven vodenja vsakega subjekta Unije na podlagi ocene kibernetskovarnostne zrelosti, opravljene na podlagi člena 7, in ob upoštevanju sredstev in tveganj za kibernetsko varnost, opredeljenih v okviru, ter ukrepov za obvladovanje tveganj za kibernetsko varnost, sprejetih na podlagi člena 8, brez nepotrebnega odlašanja in v vsakem primeru do 8. januarja 2026 odobri načrt za kibernetsko varnost. Cilj načrta za kibernetsko varnost je izboljšati splošno kibernetsko varnost subjekta Unije, s tem pa prispevati k zvišanju visoke skupne ravni kibernetske varnosti v subjektih Unije. Načrt za kibernetsko varnost vključuje najmanj ukrepe za obvladovanje tveganj za kibernetsko varnost, sprejete na podlagi člena 8. Načrt za kibernetsko varnost se pregleda vsaki dve leti ali bolj pogosto, kadar je to potrebno, in sicer na podlagi ocen kibernetskovarnostne zrelosti, izvedenih na podlagi člena 7, ali morebitnega vsebinskega pregledu okvira.

2. Načrt za kibernetsko varnost vključuje načrt subjekta Unije za obvladovanje kibernetskih kriz za večje incidente.

3. Subjekt Unije svoj dokončan načrt za kibernetsko varnost predloži Medinstitucionalnemu odboru za kibernetsko varnost, ustanovljenemu na podlagi člena 10.

POGLAVJE III

MEDINSTITUCIONALNI ODBOR ZA KIBERNETSKO VARNOST

Člen 10

Medinstitucionalni odbor za kibernetsko varnost

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

2. IICB je odgovoren za:

(a) spremljanje in podpiranje izvajanja te uredbe s strani subjektov Unije;

(b) nadzor nad izvajanjem splošnih prednostnih nalog in ciljev CERT-EU ter zagotavljanje strateških usmeritev za CERT-EU.

3. IICB sestavljajo:

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

(i) Evropski parlament;

(ii) Evropski svet;

(iii) Svet Evropske unije;

(iv) 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 kompetenčni center za kibernetsko varnost;

(xiii) ENISA;

(xiv) Evropski nadzornik za varstvo podatkov (ENVP);

(xv) Agencija Evropske unije za vesoljski program;

(b) trije predstavniki, ki jih imenuje mreža agencij EU (EUAN) na predlog svojega svetovalnega odbora za IKT in ki zastopajo interese organov, uradov in agencij Unije, ki upravljajo svoje lastno okolje IKT, razen tistih iz točke (a).

Subjekti Unije, zastopani v IICB, si prizadevajo za uravnoteženo zastopanost spolov med imenovanimi predstavniki.

4. Članom IICB lahko pomaga namestnik. Predsednik lahko povabi druge predstavnike subjektov Unije iz odstavka 3 ali drugih subjektov Unije, da se udeležijo sestankov IICB brez pravice do glasovanja.

5. Vodja CERT-EU ter predsedniki skupine za sodelovanje, mreže skupin CSIRT in mreže EU-CyCLONe, ustanovljenih na podlagi členov 14, 15 in 16 Direktive (EU) 2022/2555, ali njihovi namestniki lahko sodelujejo na sestankih IICB kot opazovalci. V izjemnih primerih lahko IICB v skladu s svojim notranjim poslovnikom odloči drugače.

6. IICB sprejme svoj notranji poslovnik.

7. IICB v skladu s svojim notranjim poslovnikom med svojimi člani imenuje predsednika za obdobje treh let. Predsednikov namestnik postane polnopravni član IICB za enako obdobje.

8. IICB se vsaj trikrat na leto sestane na pobudo svojega predsednika, na zahtevo CERT-EU ali na zahtevo katerega koli svojega člana.

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

10. IICB lahko deluje po poenostavljenem pisnem postopku, ki se začne v skladu z njegovim notranjim poslovnikom. Na podlagi tega postopka se zadevna odločitev šteje za odobreno v roku, ki ga določi predsednik, razen v primeru ugovora člana.

11. Sekretariat IICB zagotavlja Komisija in je odgovoren predsedniku IICB.

12. Predstavniki, ki jih imenuje mreža agencij EU, odločitve IICB posredujejo članom te mreže. Vsak član mreže agencij EU ima pravico, da na te predstavnike ali predsednika IICB naslovi katero koli vprašanje, za katero meni, da bi ga IICB moral obravnavati.

13. IICB lahko ustanovi izvršni odbor, ki mu pomaga pri delu ter na katerega prenese nekaj svojih nalog in pooblastil. IICB določi poslovnik izvršnega odbora, vključno z njegovimi nalogami in pooblastili, ter mandati njegovih članov.

14. IICB do 8. januarja 2025 in nato vsako leto Evropskemu parlamentu in Svetu predloži poročilo, v katerem podrobno opiše napredek pri izvajanju te uredbe in navede zlasti obseg sodelovanja CERT-EU s sorodnimi organi držav članic v vsaki državi članici. Poročilo je prispevek k dvoletnemu poročilu o stanju kibernetske varnosti v Uniji, sprejetem na podlagi člena 18 Direktive (EU) 2022/2555.

Člen 11

Naloge IICB

IICB pri izvrševanju svojih dolžnosti zlasti:

(a) zagotavlja usmeritve vodji CERT-EU;

(b) učinkovito spremlja in nadzoruje izvajanje te uredbe ter subjekte Unije podpira pri izboljševanju njihove kibernetske varnosti, po potrebi tudi tako, da od subjektov Unije in CERT-EU zahteva ad hoc poročila;

(c) po strateški razpravi sprejme večletno strategijo za dvig ravni kibernetske varnosti v subjektih Unije, to strategijo redno ocenjuje, in v vsakem primeru vsakih pet let, ter jo po potrebi spremeni;

(d) pripravi metodologijo in organizacijske vidike za izvajanje prostovoljnih medsebojnih strokovnih pregledov s strani subjektov Unije, da bi se učili iz skupnih izkušenj, okrepili medsebojno zaupanje, dosegli visoko skupno raven kibernetske varnosti ter okrepili zmogljivosti subjektov Unije na področju kibernetske varnosti, pri čemer te medsebojne strokovne preglede izvajajo strokovnjaki za kibernetsko varnost, ki jih imenuje subjekt Unije, ki ni subjekt Unije, ki se pregleduje, metodologija pa temelji na členu 19 Direktive (EU) 2022/2555 in je po potrebi prilagojena subjektom Unije;

(e) na podlagi predloga vodje CERT-EU odobri letni delovni program CERT-EU in spremlja njegovo izvajanje;

(f) na podlagi predloga vodje CERT-EU odobri katalog storitev CERT-EU in vse posodobitve tega kataloga;

(g) na podlagi predloga vodje CERT-EU odobri letno finančno načrtovanje prihodkov in izdatkov, vključno z osebjem, za dejavnosti CERT-EU;

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

(i) preuči in odobri letno poročilo, ki ga pripravi vodja CERT-EU in ki zajema dejavnosti in upravljanje sredstev CERT-EU;

(j) odobri in spremlja ključne kazalnike uspešnosti za CERT-EU, določene na podlagi predloga vodje CERT-EU;

(k) odobri dogovore o sodelovanju ter sporazume ali pogodbe o ravni storitev med CERT-EU in drugimi subjekti na podlagi člena 18;

(l) sprejme smernice in priporočila na podlagi predloga CERT-EU v skladu s členom 14 ter CERT-EU naroči izdajo, umik ali spremembo predloga smernic ali priporočil ali poziva k ukrepanju;

(m) vzpostavi tehnične svetovalne skupine s posebnimi nalogami za pomoč IICB pri njegovem delu, odobri njihove mandate in imenuje njihove predsednike;

(n) prejema in ocenjuje dokumente in poročila, ki jih na podlagi te uredbe predložijo subjekti Unije, kot so ocene kibernetskovarnostne zrelosti;

(o) podpira ustanovitev neformalne skupine lokalnih uradnikov za kibernetsko varnost subjektov Unije ob podpori ENISA, da bi olajšali izmenjavo dobrih praks in informacij v zvezi z izvajanjem te uredbe;

(p) ob upoštevanju informacij o ugotovljenih tveganjih za kibernetsko varnost in pridobljenih izkušnjah, ki jih posreduje CERT-EU, spremlja ustreznost ureditev medsebojne povezljivosti med okolji IKT subjektov Unije ter svetuje o možnih izboljšavah;

(q) pripravi načrt za obvladovanje kibernetskih kriz, da se na operativni ravni podpre usklajeno obvladovanje večjih incidentov, ki vplivajo na subjekte Unije, in prispeva k redni izmenjavi ustreznih informacij, zlasti o vplivu in resnosti večjih incidentov ter možnih načinih za blažitev njihovih posledic;

(r) usklajuje sprejemanje načrtov za obvladovanje kibernetskih kriz iz člena 9(2) za posamezne subjekte Unije;

(s) sprejme priporočila o varnosti dobavne verige iz člena 8(2), prvi pododstavek, točka (m), pri čemer upošteva rezultate usklajenih ocen varnostnih tveganj na ravni Unije za kritične dobavne verige iz člena 22 Direktive (EU) 2022/2555 v podporo subjektom Unije pri sprejemanju učinkovitih in sorazmernih ukrepov za obvladovanje tveganj za kibernetsko varnost.

Člen 12

Skladnost

1. IICB na podlagi člena 10(2) in člena 11 učinkovito spremlja izvajanje te uredbe ter sprejetih smernic, priporočil in pozivov k ukrepanju s strani subjektov Unije. IICB lahko od subjektov Unije zahteva informacije ali dokumentacijo, potrebne za ta namen. Za namen sprejetja ukrepov za skladnost na podlagi tega člena zadevni subjekt Unije, kadar je neposredno zastopan v IICB, nima glasovalnih pravic.

2. Kadar IICB ugotovi, da subjekt Unije ni učinkovito izvajal te uredbe ali smernic, priporočil ali pozivov k ukrepanju, izdanih na podlagi te uredbe, lahko brez poseganja v notranje postopke zadevnega subjekta Unije in po tem, ko je zadevnemu subjektu Unije dal možnost, da predloži svoja opažanja:

(a) subjektu Unije, pri katerem so bile opažene vrzeli pri izvajanju te uredbe, sporoči obrazloženo mnenje;

(b) po posvetovanju s CERT-EU zadevnemu subjektu Unije zagotovi smernice za zagotovitev, da so njegov okvir, ukrepi za obvladovanje tveganj za kibernetsko varnost, načrt za kibernetsko varnost in poročanje skladni s to uredbo v določenem obdobju;

(c) izda opozorilo za odpravo ugotovljenih pomanjkljivosti v določenem obdobju, vključno s priporočili za spremembo ukrepov, ki jih je zadevni subjekt Unije sprejel na podlagi te uredbe;

(d) zadevnemu subjektu Unije izda utemeljeno uradno obvestilo, v primeru, da pomanjkljivosti, ugotovljene v opozorilu, izdanem na podlagi točke (c), niso bile ustrezno odpravljene v določenem roku;

(e) izda:

(i) priporočilo za izvedbo revizije ali

(ii) zahtevo, da revizijo izvede neodvisna revizijska služba;

(f) če je ustrezno, obvesti Računsko sodišče v okviru svojih pristojnosti o domnevni neskladnosti;

(g) izda priporočilo, naj vse države članice in subjekti Unije začasno prekinejo prenose podatkov zadevnemu subjektu Unije.

Za namene prvega pododstavka, točka (c), je krog prejemnikov opozorila ustrezno omejen, kadar je to potrebno zaradi tveganja za kibernetsko varnost.

Opozorila in priporočila, izdana na podlagi prvega pododstavka, se naslovijo na najvišjo raven vodenja zadevnega subjekta Unije.

3. Kadar IICB sprejme ukrepe na podlagi odstavka 2, prvi pododstavek, točke (a) do (g), zadevni subjekt Unije zagotovi podrobnosti ukrepov in dejavnosti, sprejetih za odpravo domnevnih pomanjkljivosti, ki jih je ugotovil IICB. Subjekt Unije te podrobnosti predloži v razumnem roku, o katerem se dogovori z IICB.

4. Kadar IICB meni, da subjekt Unije vztrajno krši to uredbo neposredno zaradi dejanj ali opustitev dejanj uradnika ali drugega uslužbenca Unije, tudi na najvišji ravni vodenja, IICB zahteva, da zadevni subjekt Unije sprejme ustrezne ukrepe, vključno z zahtevo, da razmisli o sprejetju disciplinskih ukrepov v skladu s pravili in postopki, določenimi v kadrovskih predpisih in vseh drugih veljavnih pravilih in postopkih. V ta namen IICB zadevnemu subjektu Unije posreduje potrebne informacije.

5. Kadar subjekti Unije uradno obvestijo, da ne morejo spoštovati rokov iz člena 6(1) in člena 8(1), lahko IICB v ustrezno utemeljenih primerih in ob upoštevanju velikosti subjekta Unije odobri podaljšanje teh rokov.

POGLAVJE IV

CERT-EU

Člen 13

Poslanstvo in naloge CERT-EU

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

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

3. CERT-EU za pomoč subjektom Unije izvaja naslednje naloge:

(a) podpira jih pri izvajanju te uredbe in prispeva k usklajevanju izvajanja te uredbe z ukrepi iz člena 14(1) ali ad hoc poročili, ki jih zahteva IICB;

(b) ponuja standardne storitve skupine CSIRT subjektom Unije s svežnjem storitev za kibernetsko varnost, opisanih v katalogu storitev (osnovne storitve);

(c) vzdržuje mrežo podobnih institucij, organov in agencij ter partnerjev za podporo storitev, kot so navedene v členih 17 in 18;

(d) IICB opozori na vse težave, ki se nanašajo na izvajanje te uredbe ter izvajanje smernic, priporočil in pozivov k ukrepanju;

(e) na podlagi informacij iz odstavka 2 in v tesnem sodelovanju z ENISA prispeva k situacijskem zavedanju na področju kibernetske varnosti v Uniji;

(f) usklajuje obvladovanje večjih incidentov;

(g) deluje na strani subjektov Unije kot enakovreden koordinatorju, imenovanemu za usklajeno razkrivanje ranljivosti na podlagi člena 12(1) Direktive (EU) 2022/2555;

(h) na zahtevo subjekta Unije zagotovi proaktivno neinvazivno pregledovanje javno dostopnih omrežnih in informacijskih sistemov tega subjekta Unije.

Informacije iz prvega pododstavka, točka (e), se po potrebi in kadar je to ustrezno ter ob upoštevanju ustreznih pogojev zaupnosti izmenjujejo z IICB, mrežo skupin CSIRT ter Obveščevalnim in situacijskim centrom Evropske unije (EU INTCEN).

4. CERT-EU lahko v skladu s členom 17 ali 18, kot je ustrezno, sodeluje z ustreznimi skupnostmi za kibernetsko varnost v Uniji in njenih državah članicah, vključno na naslednjih področjih:

(a) pripravljenost, obvladovanje incidentov, izmenjava informacij in odzivanje na krize na tehnični ravni v zvezi s primeri, povezanimi s subjekti Unije;

(b) operativno sodelovanje v zvezi z mrežo skupin CSIRT, vključno z vzajemno pomočjo;

(c) obveščevalni podatki o kibernetskih grožnjah, vključno s situacijskim zavedanjem;

(d) vsaka tema, ki zahteva tehnično strokovno znanje CERT-EU na področju kibernetske varnosti.

5. CERT-EU v okviru svoje pristojnosti strukturirano sodeluje z ENISA pri krepitvi zmogljivosti, operativnem sodelovanju in dolgoročnih strateških analizah kibernetskih groženj v skladu z Uredbo (EU) 2019/881. CERT-EU lahko sodeluje in izmenjuje informacije z Europolovim Evropskim centrom za boj proti kibernetski kriminaliteti.

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

(a) storitve, ki podpirajo kibernetsko varnost okolja IKT subjektov Unije, razen storitev iz odstavka 3, in sicer na podlagi sporazumov o ravni storitev in glede na razpoložljive vire, zlasti spremljanje mreže širokega spektra, vključno s primarnim spremljanjem 24 ur na dan sedem dni v tednu za zelo resne kibernetske grožnje;

(b) storitve, ki podpirajo operacije ali projekte subjektov Unije za kibernetsko varnost, razen tistih za zaščito njihovih okolij IKT, in sicer na podlagi pisnih sporazumov in s predhodno odobritvijo IICB;

(c) na zahtevo proaktivno pregledovanje omrežnih in informacijskih sistemov zadevnega subjekta Unije, da se odkrijejo ranljivosti, ki bi lahko imele pomemben vpliv;

(d) storitve, ki podpirajo varnost okolja IKT organizacij, ki niso subjekti Unije, ki tesno sodelujejo s subjekti Unije, ker so jim na primer bile dodeljene naloge ali odgovornosti na podlagi prava Unije, na podlagi pisnih sporazumov in s predhodno odobritvijo IICB.

V zvezi s prvim pododstavkom, točka (d), lahko CERT-EU s predhodno odobritvijo IICB izjemoma sklene sporazume o ravni storitev s subjekti, ki niso subjekti Unije.

7. CERT-EU organizira vaje na področju kibernetske varnosti in lahko v njih sodeluje ali priporoča udeležbo na obstoječih vajah, v tesnem sodelovanju z agencijo ENISA, kadar je to primerno, da preizkusi raven kibernetske varnosti subjektov Unije.

8. CERT-EU lahko subjektom Unije zagotovi pomoč v zvezi z incidenti v omrežnih in informacijskih sistemih, v katerih se obravnavajo tajni podatki EU, kadar zadevni subjekti Unije to izrecno zahtevajo v skladu s svojimi postopki. Zagotavljanje pomoči s strani CERT-EU na podlagi tega odstavka ne posega v veljavna pravila v zvezi z varstvom tajnih podatkov.

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

10. CERT-EU z visoko stopnjo zaupnosti in zanesljivosti prek ustreznih mehanizmov sodelovanja in linij poročanja prispeva ustrezne in anonimizirane informacije o večjih incidentih in načinu, kako se jih je obravnavalo. Te informacije se vključijo v poročilo iz člena 10(14).

11. CERT-EU v sodelovanju z ENVP podpira zadevne subjekte Unije pri obravnavanju incidentov, katerih posledica je kršitev varstva osebnih podatkov, pri čemer se ne posega v pristojnosti in naloge ENVP kot nadzornega organa na podlagi Uredbe (EU) 2018/1725.

12. CERT-EU lahko, če to izrecno zahtevajo službe subjektov Unije, ki skrbijo za vprašanja politike, zagotavlja tehnične nasvete ali prispevek o ustreznih zadevah politike.

Člen 14

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;

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

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

V zvezi s prvim pododstavkom, točka (a), zadevni subjekt Unije po prejemu poziva k ukrepanju brez nepotrebnega odlašanja obvesti CERT-EU o tem, kako so se nujni varnostni ukrepi izvajali.

2. Smernice in priporočila lahko vključujejo:

(a) skupne metodologije in model za oceno kibernetskovarnostne zrelosti subjektov Unije, vključno z ustreznimi lestvicami ali ključnimi kazalniki uspešnosti, ki služijo kot referenca v podporo stalnemu izboljševanju kibernetske varnosti v vseh subjektih Unije ter olajšujejo prednostno razvrščanje področij in ukrepov na področju kibernetske varnosti ob upoštevanju odnosa subjektov do kibernetske varnosti;

(b) ureditve obvladovanja tveganj za kibernetsko varnost ali njegove izboljšave in ukrepe za obvladovanje tveganj za kibernetsko varnost;

(c) ureditve ocen kibernetskovarnostne zrelosti in načrtov za kibernetsko varnost;

(d) kadar je primerno, uporabo skupne tehnologije, arhitekture, odprtokodnih in povezanih dobrih praks s ciljem doseganja interoperabilnosti in skupnih standardov, vključno z usklajenim pristopom k varnosti dobavne verige;

(e) po potrebi informacije za lažjo uporabo instrumentov za skupna javna naročila za nakup ustreznih storitev in izdelkov na področju kibernetske varnosti od tretjih dobaviteljev;

(f) dogovori o izmenjavi informacij na podlagi člena 20.

Člen 15

Vodja CERT-EU

1. Komisija na podlagi odobritve dveh tretjin članov IICB imenuje vodjo CERT-EU. Posvetovanje z IICB se izvede v vseh fazah postopka imenovanja, zlasti pri pripravi razpisov za prosto delovno mesto, pregledovanju prijav in imenovanju izbirnih komisij v zvezi z delovnim mestom. Izbirni postopek, vključno s končnim ožjim izborom kandidatov, iz katerega bo imenovan vodja CERT-EU, zagotavlja pravično zastopanost spolov, pri čemer se upoštevajo vložene prijave.

2. Vodja CERT-EU je odgovoren za pravilno delovanje CERT-EU ter deluje v okviru svoje vloge in pod vodstvom IICB. Vodja CERT-EU redno poroča predsedniku IICB in mu na njegovo zahtevo predloži ad hoc poročila.

3. Vodja CERT-EU pomaga odgovornemu odredbodajalcu na podlagi prenosa pooblastil pri pripravi letnega poročila o dejavnostih, ki vsebuje finančne in upravljavske informacije, vključno z rezultati kontrol, pripravljenega v skladu s členom 74(9) Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta ([9]), ter redno poroča odredbodajalcu na podlagi prenosa pooblastil o izvajanju ukrepov, v zvezi s katerimi so bila pooblastila nadaljnje prenesena na vodjo CERT-EU.

4. Vodja CERT-EU vsako leto pripravi finančno načrtovanje upravnih prihodkov in odhodkov za svoje dejavnosti, predlagan letni delovni program, predlagan katalog storitev za CERT-EU, predlagane revizije kataloga storitev, predlagane ureditve za sporazume o ravni storitev in predlagane ključne kazalnike uspešnosti za CERT-EU, ki jih odobri IICB v skladu s členom 11. Pri reviziji seznama storitev v katalogu storitev CERT-EU vodja CERT-EU upošteva vire, dodeljene CERT-EU.

5. Vodja CERT-EU predloži IICB in njegovemu predsedniku najmanj enkrat letno poročila o dejavnostih in uspešnosti CERT-EU v referenčnem obdobju, med drugim o izvrševanju proračuna, sporazumih o ravni storitev in sklenjenih pisnih sporazumih, sodelovanju s sorodnimi organi in partnerji ter misijah osebja, vključno s poročili iz člena 11. Ta poročila vključujejo delovni program za naslednje obdobje, finančno načrtovanje prihodkov in odhodkov, vključno z osebjem, načrtovane posodobitve kataloga storitev CERT-EU in oceno pričakovanega učinka, ki bi ga take posodobitve lahko imele na finančne in človeške vire.

Člen 16

Finančne in kadrovske zadeve

1. CERT-EU se vključi v upravno strukturo generalnega direktorata Komisije, da lahko uporablja upravne, finančne in računovodske podporne strukture Komisije, hkrati pa ohrani svoj status samostojnega medinstitucionalnega ponudnika storitev za vse subjekte Unije. Komisija obvesti IICB o upravnemu sedežu CERT-EU in o vseh spremembah v zvezi z njim. Komisija redno pregleduje upravne ureditve v zvezi s CERT-EU, v vsakem primeru pa pred vzpostavitvijo večletnega finančnega okvira na podlagi člena 312 PDEU, da se lahko sprejmejo ustrezni ukrepi. Pregled vključuje možnost ustanovitve CERT-EU kot urada Unije.

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

([9]) 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).

3. Naloge in dejavnosti CERT-EU, vključno s storitvami, ki jih subjektom Unije zagotavlja na podlagi člena 13(3), (4), (5) in (7) ter člena 14(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 tega člena, zagotovijo CERT-EU letni finančni prispevek za kritje storitev, ki jih CERT-EU zagotavlja na podlagi navedenega odstavka. Prispevki temeljijo na usmeritvah IICB, o njih pa se vsak subjekt Unije 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 tega člena kot notranji namenski prejemki, kot je določeno v členu 21(3), točka (c), Uredbe (EU, Euratom) 2018/1046.

5. Stroške storitev, opredeljenih v členu 13(6), krijejo subjekti Unije, ki prejemajo storitve CERT-EU. Prihodki se dodelijo proračunskim vrsticam, ki krijejo stroške.

Člen 17

Sodelovanje CERT-EU s sorodnimi organi iz držav članic

1. CERT-EU brez nepotrebnega odlašanja sodeluje in si izmenjuje informacije s sorodnimi organi iz držav članic, zlasti skupinami CSIRT, imenovanimi ali ustanovljenimi na podlagi člena 10 Direktive (EU) 2022/2555, ali, kadar je ustrezno, pristojnimi organi in enotnimi kontaktnimi točkami, imenovanimi ali ustanovljenimi na podlagi člena 8 navedene direktive, v zvezi z incidenti, kibernetskimi grožnjami, ranljivostmi, skorajšnjimi incidenti, možnimi protiukrepi in dobrimi praksami ter vsemi zadevami, pomembnimi za izboljšanje zaščite okolij IKT subjektov Unije, vključno prek mreže skupin CSIRT, vzpostavljene na podlagi člena 15 Direktive (EU) 2022/2555. CERT-EU podpira Komisijo v mreži EU-CyCLONe, ustanovljeni na podlagi člena 16 Direktive (EU) 2022/2555 za usklajeno obvladovanje kibernetskih incidentov velikih razsežnosti in kriz.

2. Kadar CERT-EU izve za pomembni incident na ozemlju države članice, brez odlašanja v skladu z odstavkom 1 uradno obvesti vse ustrezne sorodne organe v tej državi članici.

3. CERT-EU brez nepotrebnega odlašanja in pod pogojem, da so osebni podatki zaščiteni v skladu z veljavnim pravom Unije o varstvu podatkov, s sorodnimi organi v državah članicah izmenjuje ustrezne informacije o posameznem incidentu, da se lažje odkrivajo podobne kibernetske grožnje ali incidenti ali prispeva k analizi incidenta, brez dovoljenja prizadetega subjekta Unije. CERT-EU informacije o posameznem incidentu, ki razkrivajo identiteto tarče incidenta, izmenjuje le, če:

(a) prizadeti subjekt Unije da soglasje;

(b) prizadeti subjekt Unije ne soglaša, kot je določeno v točki (a), vendar bi razkritje identitete prizadetega subjekta Unije povečalo verjetnost, da bi se incidentom drugje izognili ali jih ublažili;

(c) je prizadeti subjekt Unije že javno objavil, da je bil prizadet.

Odločitve o izmenjavi informacij o posameznem incidentu, ki razkrivajo identiteto tarče incidenta na podlagi prvega pododstavka, točka (b), potrdi vodja CERT-EU. CERT-EU pred izdajo take odločitve pisno stopi v stik s prizadetim subjektom Unije in jasno pojasni, kako bi razkritje njegove identitete pomagalo preprečiti ali ublažiti incidente drugje. Vodja CERT-EU zagotovi pojasnilo in od subjekta Unije izrecno zahteva, da v določenem roku navede, ali soglaša. Vodja CERT-EU subjekt Unije tudi obvesti, da si glede na predloženo pojasnilo pridržuje pravico do razkritja informacij, tudi če soglasje ni bilo predloženo. Prizadeti subjekt Unije se obvesti pred razkritjem informacij.

Člen 18

Sodelovanje CERT-EU z drugimi sorodnimi organi

1. CERT-EU lahko sodeluje s sorodnimi organi v Uniji, razen tistih iz člena 17, za katere veljajo zahteve Unije glede kibernetske varnosti, vključno s sorodnimi organi iz posameznih industrijskih sektorjev, 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 sorodne organe držav članic iz člena 17(1) v državi članici, v kateri ima sorodni organ sedež. Tako sodelovanje in pogoji zanj, tudi v zvezi s kibernetsko varnostjo, varstvom podatkov in ravnanjem z informacijami, se po potrebi in, kadar je to ustrezno, določijo v posebnih dogovorih o zaupnosti, kot so pogodbe ali upravne ureditve. Za dogovore o zaupnosti ni potrebna predhodna odobritev IICB, vendar se o njih obvesti predsednika IICB. CERT-EU lahko v primeru nujne in neizbežne potrebe po izmenjavi informacij o kibernetski varnosti v interesu subjektov Unije ali druge strani izmenjuje informacije s subjektom, katerega posebna usposobljenost, zmogljivost in strokovno znanje so upravičeno potrebni za pomoč pri taki nujni in takojšnji potrebi, tudi če CERT-EU s tem subjektom nima sklenjenega dogovora o zaupnosti. V takih primerih CERT-EU nemudoma obvesti predsednika IICB in z rednimi poročili ali sestanki poroča IICB.

2. CERT-EU lahko za zbiranje informacij o splošnih in specifičnih kibernetskih grožnjah, skorajšnjih incidentih, ranljivostih in možnih protiukrepih sodeluje s partnerji, kot so komercialni subjekti, vključno s subjekti iz posameznih industrijskih sektorjev, mednarodne organizacije, nacionalni subjekti, ki ne prihajajo iz Unije, ali posamezni strokovnjaki. Za širše sodelovanje s takimi partnerji CERT-EU pridobi predhodno soglasje IICB za vsak primer posebej.

3. CERT-EU lahko s soglasjem subjekta Unije, ki ga je incident prizadel, in pod pogojem, da ima z zadevnim sorodnim organom ali partnerjem sklenjen dogovor ali pogodbo o nerazkritju, sorodnim organom ali partnerjem iz odstavkov 1 in 2 zagotovi informacije, povezane s posameznim incidentom, izključno za namene prispevanja k njegovi analizi.

POGLAVJE V

OBVEZNOSTI SODELOVANJA IN POROČANJA

Člen 19

Ravnanje z informacijami

1. Subjekti Unije in CERT-EU spoštujejo obveznost varovanja poslovne skrivnosti v skladu s členom 339 PDEU ali enakovrednimi veljavnimi okviri.

2. Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta ([10]) se uporablja v zvezi z zahtevami za dostop javnosti do dokumentov, ki jih ima CERT-EU, vključno z obveznostjo iz navedene uredbe, da se je treba posvetovati z drugimi subjekti Unije in po potrebi državami članicami, kadar se zahteva nanaša na njihove dokumente.

3. Subjekti Unije in CERT-EU pri ravnanju z informacijami upoštevajo veljavna pravila o informacijski varnosti.

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

Člen 20

Dogovori o izmenjavi informacij o kibernetski varnosti

1. Subjekti Unije lahko CERT-EU prostovoljno priglasijo incidente, kibernetske grožnje, skorajšnje incidente in ranljivosti, ki vplivajo nanje, ter mu zagotovijo informacije o njih. CERT-EU poskrbi, da so na voljo učinkovita komunikacijska sredstva, in sicer z visoko ravnjo sledljivosti, zaupnosti in zanesljivosti, da se olajša izmenjava informacij s subjekti Unije. Pri obdelavi priglasitev lahko CERT-EU da prednost obdelavi obveznih priglasitev pred prostovoljnimi. Brez poseganja v člen 12 se zaradi prostovoljne priglasitve poročajočemu subjektu Unije ne nalagajo dodatne obveznosti, ki zanj ne bi veljale, če priglasitve ne bi opravil.

2. Da bi CERT-EU lahko izvajal svoje poslanstvo in naloge, podeljene na podlagi člena 13, lahko CERT-EU od subjektov Unije zahteva predložitev informacij iz njihovih zbirk sistemov ICT, kar vključuje informacije v zvezi s kibernetskimi grožnjami, skorajšnjimi incidenti, ranljivostmi, kazalniki ogroženosti, kibernetskovarnostnimi opozorili in priporočili glede konfiguracije kibernetskovarnostnih orodij za odkrivanje incidentov. Subjekt Unije brez nepotrebnega odlašanja posreduje zahtevane informacije in vse njihove naknadne posodobitve.

3. CERT-EU si lahko informacije o posameznem incidentu, ki razkrivajo identiteto subjekta Unije, ki ga je prizadel incident, izmenjuje s subjekti Unije, če prizadeti subjekt Unije s tem soglaša. Kadar subjekt Unije odkloni soglasje, predloži CERT-EU razloge, ki utemeljujejo to odločitev.

4. Subjekti Unije na zahtevo izmenjujejo informacije z Evropskim parlamentom in Svetom o dokončanju načrtov za kibernetsko varnost.

5. IICB ali CERT-EU, kot je ustrezno, posreduje smernice, priporočila in pozive k ukrepanju Evropskemu parlamentu in Svetu na njuno zahtevo.

6. Obveznosti izmenjave iz tega člena ne veljajo za:

(a) tajne podatke EU;

(b) informacije, katerih nadaljnja distribucija je bila izključena z vidno oznako, razen če je bila njihova izmenjava s CERT-EU izrecno dovoljena.

Člen 21

Obveznosti poročanja

1. Incident se šteje za pomembnega, če:

(a) je zadevnemu subjektu Unije povzročil ali bi mu lahko povzročil znatne operativne motnje pri delovanju ali finančno izgubo;

(b) je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

2. Subjekti Unije CERT-EU predložijo:

(a) brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po tem, ko izvejo za pomembni incident, zgodnje opozorilo, iz katerega je po možnosti razvidno, da je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali da bi lahko imel vpliv na druge subjekte ali čezmejni vpliv;

(b) brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po tem, ko izvejo za pomembni incident, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz točke (a) in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter kazalniki ogroženosti, kadar so ti na voljo;

(c) na zahtevo organa CERT-EU vmesno poročilo o ustreznih posodobitvah stanja;

(d) končno poročilo, najpozneje v enem mesecu po predložitvi priglasitve incidenta na podlagi točke (b), ki vključuje:

(i) podroben opis incidenta, vključno z njegovo resnostjo in učinkom;

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

(iii) izvedene blažilne ukrepe in take ukrepe v teku;

(iv) po potrebi čezmejni vpliv ali vpliv na druge subjekte incidenta;

(e) v primeru incidenta, ki je ob predložitvi končnega poročila iz točke (d) še vedno v teku, poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta.

3. Subjekt Unije brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po tem, ko izve za pomembni incident, obvesti vse ustrezne sorodne organe držav članic iz člena 17(1) v državi članici, v kateri se nahaja, da se je zgodil pomemben incident.

4. Subjekti Unije med drugim priglasijo vse informacije, na podlagi katerih lahko CERT-EU ugotovi morebitni učinek na druge subjekte, učinek na državo članico gostiteljico ali čezmejni učinek pomembnega incidenta. Brez poseganja v člen 12 samo dejanje priglasitve ne nalaga dodatne odgovornosti subjektu, ki tako priglasitev izvede.

5. Subjekti Unije po potrebi in brez nepotrebnega odlašanja sporočijo uporabnikom prizadetih omrežnih in informacijskih sistemov ali drugih komponent okolja IKT, na katere lahko vpliva pomemben incident ali pomembna kibernetska grožnja in ki morajo, kadar je to ustrezno, sprejeti blažilne ukrepe, o vseh ukrepih ali pravnih sredstvih, ki jih lahko sprejmejo v odziv na incident ali grožnjo. Kadar je primerno, subjekti Unije obvestijo te uporabnike o pomembni kibernetski grožnji kot taki.

6. Kadar pomemben incident ali pomembna kibernetska grožnja prizadene omrežni in informacijski sistem ali komponento okolja IKT subjekta Unije, ki je načrtno povezana z okoljem IKT drugega subjekta Unije, CERT-EU izda ustrezno kibernetskovarnostno opozorilo.

7. Subjekti Unije na zahtevo CERT-EU brez nepotrebnega odlašanja posredujejo CERT-EU digitalne informacije, ustvarjene z uporabo elektronskih naprav, ki so vpete v zadevne incidente. CERT-EU lahko dodatno pojasni vrste informacij, ki jih potrebuje za situacijsko zavedanje in odzivanje na incidente.

8. CERT-EU predloži IICB, ENISA, EU INTCEN in mreži skupin CSIRT vsake tri mesece zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o pomembnih incidentih, incidentih, kibernetskih grožnjah, skorajšnjih incidentih in ranljivostih na podlagi člena 20 ter pomembnih incidentih, priglašenih na podlagi odstavka 2 tega člena. Zbirno poročilo je prispevek k dveletnemu poročilu o stanju kibernetske varnosti v Uniji, ki se sprejme na podlagi člena 18 Direktive (EU) 2022/2555.

9. IICB do 8. julija 2024 izda smernice ali priporočila, v katerih podrobneje opredeli ureditve za poročanje ter obliko in vsebino poročanja na podlagi tega člena. IICB pri pripravi takih smernic ali priporočil upošteva vse izvedbene akte, sprejete na podlagi člena 23(11) Direktive (EU) 2022/2555, v katerih so določeni vrsta informacij, oblika in postopek priglasitve. CERT-EU razširja ustrezne tehnične podrobnosti, da se subjektom Unije omogočijo proaktivno odkrivanje, odzivanje na incidente ali blažilni ukrepi.

10. Obveznosti poročanja iz tega člena ne veljajo za:

(a) tajne podatke EU;

(b) informacije, katerih nadaljnja distribucija je bila izključena z vidno oznako, razen če je bila njihova izmenjava s CERT-EU izrecno dovoljena.

Člen 22

Usklajevanje odzivanja na incidente in sodelovanje

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

(a) subjekti Unije;

(b) sorodnimi organi iz členov 17 in 18.

2. CERT-EU po potrebi v tesnem sodelovanju z ENISA olajša usklajevanje med subjekti Unije v zvezi z odzivanjem na incidente, vključno s:

(a) prispevkom k doslednemu zunanjemu komuniciranju;

(b) medsebojno podporo, kot je izmenjava informacij, pomembnih za subjekte Unije, ali zagotavljanje pomoči, po potrebi neposredno na kraju samem;

(c) optimalno uporabo operativnih virov;

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

3. CERT-EU v tesnem sodelovanju z ENISA podpira subjekte Unije v zvezi s situacijskim zavedanjem o incidentih, kibernetskih grožnjah, ranljivostih, in skorajšnjih incidentih ter pri izmenjavi najnovejših dosežkov na področju kibernetske varnosti.

4. IICB do 8. januarja 2025 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 svetuje o tem, kako incident brez nepotrebnega odlašanja prijaviti organom kazenskega pregona.

5. CERT-EU lahko na posebno zahtevo države članice in z odobritvijo zadevnih subjektov Unije povabi strokovnjake s seznama iz člena 23(4), da prispevajo k odzivu na večji incident, ki vpliva na to državo članico, ali kibernetski incident velikih razsežnosti v skladu s členom 15(3), točka (g), Direktive (EU) 2022/2555. IICB na podlagi predloga CERT-EU odobri posebna pravila o dostopu do tehničnih strokovnjakov iz subjektov Unije ter njihovem sodelovanju.

Člen 23

Obvladovanje večjih incidentov

1. IICB na podlagi člena 11, točka (q), v tesnem sodelovanju s CERT-EU in ENISA pripravi načrt za obvladovanje kibernetskih kriz na podlagi dejavnosti iz člena 22(2), da bi na operativni ravni podprl usklajeno obvladovanje večjih incidentov, ki vplivajo na subjekte Unije, in prispeval k redni izmenjavi ustreznih informacij med subjekti Unije in državami članicami. Načrt za obvladovanje kibernetskih kriz vključuje vsaj naslednje elemente:

(a) ureditve glede 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.

2. Predstavnik Komisije v IICB je ob upoštevanju načrta za obvladovanje kibernetskih kriz, pripravljenega na podlagi odstavka 1 tega člena, in brez poseganja v člen 16(2), prvi pododstavek, Direktive (EU) 2022/2555, kontaktna točka za izmenjavo ustreznih informacij v zvezi z večjimi incidenti z mrežo EU-CyCLONe.

3. CERT-EU usklajuje subjekte Unije pri obvladovanju večjih incidentov. Vzdržuje zbirko razpoložljivega tehničnega strokovnega znanja, ki bi bilo potrebno za odzivanje v primeru večjih incidentov, in pomaga IICB pri usklajevanju načrtov subjektov Unije za obvladovanje kibernetskih kriz v primeru večjih incidentov iz člena 9(2).

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

POGLAVJE VI

KONČNE DOLOČBE

Člen 24

Začetna proračunska prerazporeditev

Komisija lahko za zagotovitev pravilnega in stabilnega delovanja CERT-EU predlaga prerazporeditev osebja in finančnih virov v proračun Komisije za uporabo v operacijah CERT-EU. Prerazporeditev se izvede hkrati s sprejetjem prvega letnega proračuna Unije po začetku veljavnosti te uredbe.

Člen 25

Pregled

1. IICB ob pomoči CERT-EU do 8. januarja 2025 ter nato vsako leto poroča Komisiji o izvajanju te uredbe. IICB lahko Komisiji izda tudi priporočila, naj pregleda to uredbo.

2. Komisija do 8. januarja 2027 ter nato vsaki dve leti oceni izvajanje te uredbe ter izkušnje, pridobljene na strateški in operativni ravni, ter o njih poroča Evropskemu parlamentu in Svetu.

V poročilo iz prvega pododstavka tega odstavka se vključi pregled iz člena 16(1) o možnosti ustanovitve CERT-EU kot urada Unije.

3. Komisija do 8. januarja 2029 oceni delovanje te uredbe ter Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij predloži poročilo. Komisija oceni tudi ustreznost vključitve omrežnih in informacijskih sistemov, ki obravnavajo tajne podatke EU, na področje uporabe te uredbe, pri čemer upošteva druge zakonodajne akte Unije, ki se uporabljajo za te sisteme. Poročilu se po potrebi priloži zakonodajni predlog.

Člen 26

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 Strasbourgu, 13. decembra 2023

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	P. NAVARRO RÍOS