DEN EUROPÆISKE UNION

EUROPA-PARLAMENTET **RÅDET**

Strasbourg, den 13. december 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM FORANSTALTNINGER TIL SIKRING AF ET HØJT FÆLLES CYBERSIKKERHEDSNIVEAU I UNIONENS INSTITUTIONER, ORGANER, KONTORER OG AGENTURER

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU, Euratom) 2023/…

af 13. december 2023

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 298,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 106a,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

efter den almindelige lovgivningsprocedure[1], og

ud fra følgende betragtninger:

[1] Europa-Parlamentets holdning af 21.11.2023 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 8.12.2023.

(1) I den digitale tidsalder er informations- og kommunikationsteknologi en hjørnesten i en åben, effektiv og uafhængig europæisk forvaltning. Ny teknologi og de digitale systemers øgede kompleksitet og indbyrdes forbundethed øger cybersikkerhedsrisiciene og gør EU-enheder mere sårbare over for cybertrusler og hændelser, hvilket udgør en trussel mod deres driftskontinuitet og evne til at sikre deres data. Selv om øget brug af cloudtjenester, den allestedsnærværende brug af informations- og kommunikationsteknologi (IKT), den høje grad af digitalisering, fjernarbejde, ny teknologi og konnektivitet i dag er centrale elementer i alle aktiviteter i EU-enhederne, er digital modstandsdygtighed endnu ikke tilstrækkelig indarbejdet.

(2) Det trusselsbillede for cybersikkerheden, som EU-enhederne står over for, udvikler sig konstant. De taktikker, teknikker og fremgangsmåder, som trusselsaktørerne benytter sig af, udvikler sig konstant, men de primære bevæggrunde for sådanne angreb – fra at stjæle værdifulde fortrolige oplysninger til at tjene penge, manipulere den offentlige mening eller underminere digital infrastruktur – ændrer sig kun lidt. Hastigheden, hvormed trusselsaktørerne gennemfører deres cyberangreb, øges hele tiden, og deres kampagner bliver mere og mere avancerede og automatiserede med angreb på eksponerede angrebsflader, der hele tiden udvides, og sårbarheder udnyttes hurtigt.

(3) EU-enhedernes IKT-miljøer har indbyrdes afhængige elementer og integrerede datastrømme, og brugerne arbejder tæt sammen. Denne sammenkobling betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én EU-enhed, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for andre EU-enheder. Derudover er visse EU-enheders IKT-miljøer sammenkoblet med medlemsstaternes IKT-miljøer, hvilket betyder, at en hændelse i en EU-enhed udgør en cybersikkerhedsrisiko for medlemsstaternes IKT-miljøer og omvendt. Udvekslingen af hændelsesspecifikke oplysninger kan fremme opdagelsen af lignende cybertrusler eller hændelser, som påvirker medlemsstaterne.

(4) EU-enheder er attraktive mål, der er oppe mod højt kvalificerede trusselsaktører med adgang til mange ressourcer samt andre trusler. Samtidig varierer graden og modenheden af cyberrobusthed samt evnen til at reagere på ondsindede cyberaktiviteter betydeligt fra den ene enhed til den anden. Det er derfor nødvendigt for EU-enhedernes funktionsdygtighed, at de opnår et højt fælles cybersikkerhedsniveau ved at gennemføre cybersikkerhedsforanstaltninger, der står i et rimeligt forhold til de identificerede cybersikkerhedsrisici, udveksling af oplysninger og samarbejde.

(5) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[1] har til formål at forbedre offentlige og private enheders, kompetente myndigheders og organers samt Unionens samlede cyberrobusthed og kapacitet til at reagere på hændelser. Det er derfor nødvendigt at sikre, at EU-enhederne følger trop ved at tilvejebringe regler, der er i overensstemmelse med direktiv (EU) 2022/2555 og afspejler ambitionsniveauet heri.

(6) For at opnå et højt fælles cybersikkerhedsniveau er det nødvendigt, at hver EU-enhed fastlægger en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici ("rammen"), som sikrer en effektiv og fornuftig styring af alle cybersikkerhedsrisici og tager hensyn til driftskontinuitet og krisestyring. Rammen bør fastlægge cybersikkerhedspolitikker, herunder mål og prioriteter, for sikkerheden i net- og informationssystemer, der omfatter hele det uklassificerede IKT-miljø. Rammen bør bygge på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod enhver begivenhed såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en EU-enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data, der lagres, overføres, behandles eller er tilgængelige via net- og informationssystemer.

---

[1] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

(7) Med henblik på styring af de cybersikkerhedsrisici, der konstateres inden for rammen, bør hver EU-enhed træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger. Disse foranstaltninger bør omfatte de områder og foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i denne forordning, for at styrke cybersikkerheden i hver EU-enhed.

(8) De aktiver og cybersikkerhedsrisici, der er konstateret inden for rammen, samt de konklusioner, der drages af regelmæssige modenhedsvurderinger af cybersikkerheden, bør afspejles i en cybersikkerhedsplan, der udarbejdes af hver EU-enhed. Cybersikkerhedsplanen bør omfatte de vedtagne foranstaltninger til styring af cybersikkerhedsrisici.

(9) Da sikring af cybersikkerhed er en kontinuerlig proces, bør egnetheden og effektiviteten af de foranstaltninger, der træffes i henhold til denne forordning, revideres regelmæssigt i lyset af EU-enhedernes skiftende cybersikkerhedsrisici, aktiver og modenhed inden for cybersikkerhed. Rammen bør revideres regelmæssigt og mindst hvert fjerde år, mens cybersikkerhedsplanen bør revideres hvert andet år eller hyppigere, hvis det er nødvendigt, efter modenhedsvurderingerne af cybersikkerheden eller en eventuel betydelig revision af rammen.

(10) De foranstaltninger til styring af cybersikkerhedsrisici, som EU-enhederne indfører, bør, hvor det er muligt, omfatte politikker, der tilstræber at gøre kildekoden gennemsigtig under hensyntagen til garantier for beskyttelse af tredjeparters eller EU-enheders rettigheder. Disse politikker bør stå i et rimeligt forhold til cybersikkerhedsrisikoen og har til formål at lette analysen af cybertrusler uden at skabe forpligtelser til at offentliggøre eller give adgang til tredjepartskoder ud over de gældende kontraktvilkår.

(11) Open source-cybersikkerhedsværktøjer og -applikationer kan bidrage til en højere grad af åbenhed. Åbne standarder fremmer interoperabiliteten mellem sikkerhedsværktøjer, hvilket gavner interessenternes sikkerhed. Open source-cybersikkerhedsværktøjer og -applikationer kan fungere som en løftestang for det bredere udviklersamfund og give mulighed for leverandørdiversificering. Open source kan føre til en mere gennemsigtig proces for kontrol af cybersikkerhedsrelaterede værktøjer og en brugerdrevet proces for opdagelse af sårbarheder. EU-enheder bør derfor kunne fremme anvendelsen af open source-software og åbne standarder ved at føre politikker vedrørende brugen af åbne data og open source som en del af konceptet "sikkerhed gennem gennemsigtighed".

(12) EU-enhedernes forskelligheder kræver fleksibilitet i gennemførelsen af denne forordning. Foranstaltningerne til sikring af et højt fælles cybersikkerhedsniveau, som er fastsat i denne forordning, bør ikke omfatte forpligtelser, der direkte griber ind i gennemførelsen af EU-enhedernes opgaver eller deres institutionelle autonomi. Derfor bør disse enheder fastlægge deres egne rammer og vedtage deres egne foranstaltninger til styring af cybersikkerhedsrisici og cybersikkerhedsplaner. Ved gennemførelsen af sådanne foranstaltninger bør der tages behørigt hensyn til eksisterende synergier mellem EU-enheder med henblik på korrekt forvaltning af ressourcer og omkostningsoptimering. Der bør også tages behørigt hensyn til, at foranstaltningerne ikke har en negativ indvirkning på den effektive informationsudveksling og det effektive samarbejde blandt EU-enhederne og mellem EU-enhederne og medlemsstatsmodparterne.

(13) For at optimere anvendelsen af ressourcer bør denne forordning give mulighed for, at to eller flere EU-enheder med ensartede strukturer samarbejder om at foretage modenhedsvurderingerne af cybersikkerheden for deres respektive enheder.

(14) Med henblik på at undgå at EU-enhederne pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, bør kravene til styring af cybersikkerhedsrisici stå i et rimeligt forhold til cybersikkerhedsrisikoen fra de pågældende net- og informationssystemer under hensyntagen til sådanne foranstaltningers aktuelle tekniske niveau. Hver EU-enhed bør sigte mod at tildele en passende procentdel af sit IKT-budget til forbedring af cybersikkerhedsniveauet. På længere sigt bør de forfølge et vejledende mål på mindst 10 %. Modenhedsvurderingen af cybersikkerheden bør evaluere, om EU-enhedens udgifter til cybersikkerhed står i et rimeligt forhold til de cybersikkerhedsrisici, som den er udsat for. Med forbehold af reglerne vedrørende Unionens årlige budget i henhold til traktaterne bør Kommissionen i sit forslag til det første årlige budget, der skal vedtages efter denne forordnings ikrafttræden, tage hensyn til de forpligtelser, der følger af denne forordning, når den vurderer EU-enhedernes budget- og personalebehov på baggrund af deres overslag over udgifter.

(15) Et højt fælles cybersikkerhedsniveau kræver, at cybersikkerhed bliver lagt ind under hver EU-enheds øverste ledelses tilsyn. EU-enhedens øverste ledelse bør være ansvarlig for gennemførelsen af denne forordning, herunder for at fastlægge rammen, træffe foranstaltninger til styring af cybersikkerhedsrisici og godkende cybersikkerhedsplanen. Cybersikkerhedskulturen, nemlig den daglige praksis for cybersikkerhed, er en integreret del af rammen og de tilsvarende foranstaltninger til styring af cybersikkerhedsrisici i alle EU-enheder.

(16) Sikkerheden i net- og informationssystemer, der håndterer EU's klassificerede informationer (EUCI), er helt afgørende. EU-enheder, der håndterer EUCI, skal anvende de omfattende lovgivningsmæssige rammer, der er indført for at beskytte sådanne informationer, herunder specifik forvaltning og specifikke politikker og risikostyringsprocedurer. Det er nødvendigt, at net- og informationssystemer, der håndterer EUCI, overholder strengere sikkerhedsstandarder end uklassificerede net- og informationssystemer. Net- og informationssystemer, der håndterer EUCI, er derfor mere modstandsdygtige over for cybertrusler og hændelser. Selv om det anerkendes, at der er behov for en fælles ramme i denne henseende, bør denne forordning derfor ikke finde anvendelse på net- og informationssystemer, der håndterer EUCI. Hvis en EU-enhed udtrykkeligt anmoder herom, bør IT-Beredskabsenheden for EU's Institutioner, Organer og Agenturer (CERT-EU) imidlertid kunne yde bistand til den pågældende EU-enhed i forbindelse med hændelser i klassificerede IKT-miljøer.

(17) EU-enhederne bør vurdere cybersikkerhedsrisici vedrørende forholdet til leverandører og tjenesteudbydere, herunder leverandører af datalagrings- og databehandlingstjenester eller administrerede sikkerhedstjenester, og træffe foranstaltninger til at håndtere dem. Cybersikkerhedsforanstaltninger bør specificeres nærmere i retningslinjer eller henstillinger udstedt af CERT-EU. Når der udarbejdes foranstaltninger og retningslinjer bør der tages behørigt hensyn til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt relevant EU-ret og relevante EU-politikker, herunder cybersikkerhedsrisikovurderinger og henstillinger fra den samarbejdsgruppe, der er nedsat i henhold til artikel 14 i direktiv (EU) 2022/2555, såsom EU's koordinerede risikovurdering af cybersikkerheden i 5G-net og EU-værktøjskassen til cybersikkerhed i 5G-net. I betragtning af cybertrusselsbilledet og vigtigheden af at opbygge cyberrobusthed for EU-enhederne kan der desuden kræves certificering af relevante IKT-produkter, IKT-tjenester og IKT-processer i overensstemmelse med specifikke europæiske cybersikkerhedscertificeringsordninger vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881[1].

[1] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

(18) I maj 2011 besluttede generalsekretærerne for Unionens institutioner og organer at etablere et første hold for CERT-EU under tilsyn af et interinstitutionelt styrelsesråd. Generalsekretærerne bekræftede i juli 2012 de praktiske ordninger og nåede til enighed om at bevare CERT-EU som en permanent enhed for fortsat at hjælpe med at forbedre det generelle IT-sikkerhedsniveau i Unionens institutioner, organer og agenturer som et eksempel på synligt interinstitutionelt samarbejde inden for cybersikkerhed. I september 2012 blev CERT-EU oprettet som en taskforce under Kommissionen med et interinstitutionelt mandat. I december 2017 indgik Unionens institutioner og organer en interinstitutionel aftale om CERT-EU's organisation og drift[1]. Denne forordning bør fastlægge et omfattende regelsæt for CERT-EU's organisation, funktion og drift. Bestemmelserne i denne forordning har forrang for bestemmelserne i den interinstitutionelle aftale om CERT-EU's organisation og drift, der blev indgået i december 2017.

(19) CERT-EU bør omdøbes til cybersikkerhedstjenesten for Unionens institutioner, organer, kontorer og agenturer, men kortformen CERT-EU bør bibeholdes af hensyn til navnets genkendelighed.

---

1 Aftale mellem Europa-Parlamentet, Det Europæiske Råd, Rådet for Den Europæiske Union, Europa-Kommissionen, Den Europæiske Unions Domstol, Den Europæiske Centralbank, Den Europæiske Revisionsret, Tjenesten for EU's Optræden Udadtil, Det Europæiske Økonomiske og Sociale Udvalg, Det Europæiske Regionsudvalg og Den Europæiske Investeringsbank om organisation og drift af en IT-beredskabsenhed for Unionens institutioner, organer og agenturer (CERT-EU) (EUT C 12 af 13.1.2018, s. 1).

(20) Udover at give CERT-EU flere opgaver og udvide dets rolle oprettes Det Interinstitutionelle Råd for Cybersikkerhed (IICB) ved denne forordning, med henblik på at fremme et højt fælles cybersikkerhedsniveau i EU-enhederne. IICB bør have enekompetence til at overvåge og støtte EU-enhedernes gennemførelse af denne forordning og til at føre tilsyn med CERT-EU's gennemførelse af de generelle prioriteter og mål og udstikke den strategiske retning for CERT-EU. IICB bør derfor sikre, at EU-institutionerne er repræsenteret og bør inddrage repræsentanter for Unionens organer, kontorer og agenturer gennem netværket af EU-agenturer (EUAN). IICB's organisation og funktion bør yderligere reguleres ved hjælp af en intern forretningsorden, som kan omfatte en nærmere præcisering af regelmæssige møder i IICB, herunder årlige forsamlinger på politisk plan, hvor repræsentanter fra den øverste ledelse i hvert medlem af IICB vil give IICB mulighed for at føre strategiske drøftelser og udstikke strategiske retningslinjer for IICB. IICB bør desuden have mulighed for at nedsætte et forretningsudvalg til at bistå IICB i dets arbejde og delegere nogle af sine opgaver og beføjelser til samme, navnlig for så vidt angår opgaver, der kræver specifik ekspertise hos dets medlemmer, f.eks. godkendelse af tjenestekataloget og eventuelle efterfølgende ajourføringer heraf, ordninger for serviceleveranceaftaler, vurderinger af dokumenter og rapporter, som EU-enhederne forelægger IICB i henhold til denne forordning, eller opgaver vedrørende udarbejdelse af afgørelser om overholdelsesforanstaltninger udstedt af IICB og overvågning af gennemførelsen heraf. IICB bør fastlægge forretningsudvalgets forretningsorden, inklusive dets opgaver og beføjelser.

(21) IICB har til formål at støtte EU-enhederne i at løfte deres cybersikkerhedstilstand til et højere niveau via gennemførslen af denne forordning. For at støtte EU-enhederne bør IICB yde vejledning til CERT-EU's chef, vedtage en flerårig strategi for forøgelse af cybersikkerhedsniveauet i EU-enhederne, fastlægge metoden for og andre aspekter af frivillige peerevalueringer og fremme oprettelsen af en uformel gruppe af lokale cybersikkerhedsansvarlige med støtte fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) med henblik på at udveksle bedste praksis og oplysninger i forbindelse med gennemførelsen af denne forordning.

(22) For at opnå et højt niveau af cybersikkerhed i alle EU-enheder bør interesserne for de af Unionens organer, kontorer og agenturer, der driver deres eget IKT-miljø, repræsenteres i IICB af tre repræsentanter udpeget af EUAN. Sikkerheden i forbindelse med behandling af personoplysninger og dermed også cybersikkerheden heraf er en hjørnesten i databeskyttelsen. I lyset af synergierne mellem databeskyttelse og cybersikkerhed bør Den Europæiske Tilsynsførende for Databeskyttelse være repræsenteret i IICB som en EU-enhed, der er omfattet af denne forordning, med særlig ekspertise inden for databeskyttelse, herunder sikkerhed i elektroniske kommunikationsnet. I betragtning af betydningen af innovation og konkurrenceevne inden for cybersikkerhed bør Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed være repræsenteret i IICB. I betragtning af ENISA's rolle som ekspertisecenter inden for cybersikkerhed og den støtte, som ENISA yder, og i betragtning af betydningen af cybersikkerhed i Unionens ruminfrastruktur og -tjenester bør ENISA og Den Europæiske Unions Agentur for Rumprogrammet være repræsenteret i IICB. I lyset af den rolle, som CERT-EU tildeles i henhold til denne forordning, bør IICB's formand indbyde CERT-EU's chef til alle IICB's møder, undtagen når IICB drøfter spørgsmål, der direkte vedrører CERT-EU's chef.

(23) IICB bør overvåge overholdelsen af denne forordning og gennemførelsen af retningslinjer og henstillinger og opfordringer til tiltag. IICB bør i tekniske spørgsmål støttes af tekniske rådgivende grupper, der sammensættes, som IICB finder passende. Disse tekniske rådgivende grupper bør arbejde tæt sammen med CERT-EU, EU-enhederne og andre interessenter efter behov.

(24) Hvis IICB finder, at en EU-enhed ikke på effektiv vis har gennemført denne forordning eller de retningslinjer, henstillinger eller opfordringer til tiltag, som er udstedt i medfør heraf, bør IICB kunne iværksætte overholdelsesforanstaltninger, uden at dette berører den pågældende EU-enheds interne procedurer. IICB bør anvende overholdelsesforanstaltninger gradvist – med andre ord bør IICB først vedtage den mindst strenge foranstaltning, nemlig en begrundet udtalelse og kun om nødvendigt stadig strengere foranstaltninger, der fører til den strengeste foranstaltning, nemlig en henstilling om midlertidig afbrydelse af dataoverførslen til den pågældende EU-enhed. En sådan henstilling bør kun anvendes i ekstraordinære tilfælde ved den pågældende EU-enheds langvarige, forsætlige, gentagne eller alvorlige overtrædelser af denne forordning.

(25) Den begrundede udtalelse udgør den mindst alvorlige overholdelsesforanstaltning til imødegåelse af konstaterede mangler i gennemførelsen af denne forordning. IICB bør kunne følge op på en begrundet udtalelse med vejledning for at bistå EU-enheden med at sikre, at dens ramme, foranstaltninger til styring af cybersikkerhedsrisici, cybersikkerhedsplan og rapportering er i overensstemmelse med denne forordning, og derefter med en advarsel for at afhjælpe konstaterede mangler i EU-enheden inden for en nærmere angivet periode. Hvis de mangler, der er konstateret i advarslen, ikke er blevet afhjulpet i tilstrækkelig grad, bør IICB kunne udstede en begrundet meddelelse.

(26) IICB bør kunne henstille, at der foretages en revision af en EU-enhed. EU-enheden bør kunne anvende sin interne revisionsfunktion til dette formål. IICB bør også kunne anmode om, at en tredjepartsrevisionstjeneste foretager en revision, herunder af en gensidigt aftalt tjenesteudbyder i den private sektor.

(27) I ekstraordinære tilfælde, hvor en EU-enheds overtrædelser af denne forordning er langvarige, forsætlige, gentagne eller alvorlige, bør IICB som en sidste udvej kunne henstille til alle medlemsstater og EU-enheder at foretage en midlertidig afbrydelse af datastrømmene til EU-enheden, indtil EU-enheden har bragt overtrædelsen til ophør. En sådan henstilling bør formidles ved hjælp af passende og sikre kommunikationskanaler.

(28) For at sikre en korrekt gennemførelse af denne forordning bør IICB, hvis det mener, at en EU-enheds vedholdende overtrædelse af denne forordning direkte skyldes en medarbejders handlinger eller undladelser, herunder i den øverste ledelse, anmode den pågældende EU-enhed om at træffe passende tiltag, herunder anmode den om at overveje at iværksætte tiltag af disciplinær karakter i overensstemmelse med de regler og procedurer, der er fastsat i vedtægten for tjenestemænd i Den Europæiske Union og ansættelsesvilkårene for de øvrige ansatte i Unionen, fastsat ved Rådets forordning (EØF, Euratom, EKSF) nr. 259/68[1] ("vedtægten for tjenestemænd") og eventuelle andre gældende regler og procedurer.

(29) CERT-EU bør bidrage til IKT-miljøets sikkerhed i alle EU-enheder. Når CERT-EU overvejer at yde teknisk rådgivning eller input om relevante politiske spørgsmål efter anmodning fra en EU-enhed, bør CERT-EU sikre, at dette ikke er til hinder for udførelsen af de andre opgaver, det er pålagt i medfør af denne forordning. CERT-EU bør agere på vegne af EU-enhederne som ækvivalent med den koordinator, der er udpeget med henblik på koordineret offentliggørelse af sårbarheder, jf. artikel 12, stk. 1, i direktiv (EU) 2022/2555.

[1] Rådets forordning (EØF, Euratom, EKSF) nr. 259/68 af 29. februar 1968 om vedtægten for tjenestemænd i De Europæiske Fællesskaber og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber samt om særlige midlertidige foranstaltninger for tjenestemænd i Kommissionen (EFT L 56 af 4.3.1968, s. 1).

(30) CERT-EU bør støtte gennemførelsen af foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau ved hjælp af forslag til retningslinjer og henstillinger til IICB eller ved at udstede opfordringer til tiltag. Sådanne retningslinjer og henstillinger bør godkendes af IICB. Når det er nødvendigt, bør CERT-EU udstede opfordringer til tiltag, der beskriver hastende sikkerhedsforanstaltninger, som EU-enhederne kraftigt opfordres til at træffe inden for en fastsat frist. IICB bør instruere CERT-EU i at udstede, tilbagekalde eller ændre et forslag til retningslinjer eller til en henstilling eller en opfordring til tiltag.

(31) CERT-EU bør også udfylde den rolle, der er fastsat i direktiv (EU) 2022/2555 for så vidt angår samarbejde og udveksling af oplysninger med netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), som er oprettet i henhold til artikel 15 i nævnte direktiv. I overensstemmelse med Kommissionens henstilling (EU) 2017/1584[1] bør CERT-EU samarbejde og koordinere en reaktion med de relevante interessenter. Med henblik på at bidrage til et højt cybersikkerhedsniveau i hele Unionen bør CERT-EU dele hændelsesspecifikke oplysninger med medlemsstatsmodparter. CERT-EU bør også samarbejde med andre offentlige såvel som private modparter, herunder Den Nordatlantiske Traktats Organisation, efter IICB's forudgående godkendelse.

---

[1] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

(32) I forbindelse med støtte til den operationelle cybersikkerhed bør CERT-EU gøre brug af ENISA's tilgængelige ekspertise i form af et struktureret samarbejde, jf. Europa-Parlamentets og Rådets forordning (EU) 2019/881. Hvor det er relevant, bør der indføres særlige ordninger mellem de to enheder med henblik på at fastlægge den praktiske gennemførelse af et sådant samarbejde og undgå overlap af aktiviteter. CERT-EU bør samarbejde med ENISA om cybertrusselsanalyser og regelmæssigt dele sin rapport om trusselsbilledet med ENISA.

(33) CERT-EU bør have mulighed for at samarbejde og udveksle oplysninger med relevante cybersikkerhedsfællesskaber i Unionen og dens medlemsstater med henblik på at fremme operationelt samarbejde og sætte de eksisterende netværk i stand til at udnytte deres fulde potentiale til at beskytte Unionen.

(34) Eftersom CERT-EU's tjenester og opgaver er i EU-enhedernes interesse, bør hver EU-enhed, der afholder udgifter til IKT, bidrage med en fair andel til disse tjenester og opgaver. Disse bidrag berører ikke EU-enhedernes budgetautonomi.

(35) Mange cyberangreb er en del af bredere kampagner rettet mod grupper af EU-enheder eller interessefællesskaber, der omfatter EU-enheder. Med henblik på at muliggøre proaktiv opdagelse, reaktion på hændelser eller afhjælpende foranstaltninger og genopretning efter hændelser bør EU-enhederne kunne underrette CERT-EU om hændelser, cybertrusler, sårbarheder og nærvedhændelser og dele relevante tekniske detaljer, der muliggør proaktiv opdagelse eller afhjælpning af samt reaktion på lignende hændelser, cybertrusler, sårbarheder og nærvedhændelser i andre EU-enheder. Efter den samme tilgang som i direktiv (EU) 2022/2555 bør EU-enheder være forpligtet til at indsende en tidlig varsling til CERT-EU senest 24 timer efter, at de er blevet opmærksomme på en væsentlig hændelse. En sådan udveksling af oplysninger vil gøre det muligt for CERT-EU at formidle oplysningerne til andre EU-enheder samt relevante modparter med henblik på at beskytte EU-enhedernes og deres modparters IKT-miljøer mod lignende hændelser.

(36) I denne forordning fastlægges en flertrinstilgang for underretning om væsentlige hændelser med henblik på at finde den rette balance mellem på den ene side hurtig underretning, der bidrager til at afbøde den potentielle spredning af væsentlige hændelser og giver EU-enhederne mulighed for at søge assistance, og på den anden side dybdegående underretning, der gør det muligt at høste værdifulde erfaringer fra individuelle hændelser og over tid forbedre individuelle EU-enheders cyberrobusthed og bidrager til at øge deres samlede cybersikkerhedstilstand. Forordningen bør i den henseende omfatte underretning om hændelser, der på grundlag af en indledende vurdering foretaget af den berørte EU-enhed kunne forårsage alvorlige driftsmæssige forstyrrelser i den pågældende EU-enhedsfunktionsdygtighed eller økonomiske tab for denne, eller forvolde betydelig materiel eller immateriel skade for andre fysiske eller juridiske personer. En sådan indledende vurdering bør bl.a. tage i betragtning de berørte net- og informationssystemer, navnlig deres betydning for EU-enhedens funktionsdygtighed, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt EU-enhedens erfaring med lignende hændelser. Indikatorer såsom graden af påvirkning af EU-enhedens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte fysiske eller juridiske personer, vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse er alvorlig.

(37) Da infrastrukturen og net- og informationssystemerne i den relevante EU-enhed og den medlemsstat, hvor den pågældende EU-enhed er beliggende, er indbyrdes forbundne, er det afgørende, at den pågældende medlemsstat uden unødigt ophold underrettes om en væsentlig hændelse i den pågældende EU-enhed. Med henblik herpå bør den berørte EU-enhed underrette alle relevante medlemsstatsmodparter, der er udpeget eller oprettet i henhold til artikel 8 og 10 i direktiv (EU) 2022/2555, om forekomsten af en væsentlig hændelse, som den indberetter til CERT-EU. Hvis CERT-EU bliver opmærksomt på en væsentlig hændelse i den pågældende medlemsstat, bør det underrette den relevante medlemsstatsmodpart.

(38) Der bør indføres en mekanisme til at sikre effektiv udveksling af oplysninger, koordinering og samarbejde mellem EU-enhederne i tilfælde af større hændelser, herunder en klar fastlæggelse af de involverede EU-enheders roller og ansvarsområder. Kommissionens repræsentant i IICB bør, med forbehold af cyberkrisestyringsplanen, være kontaktpunktet for at lette IICB's udveksling af relevante oplysninger i relation til større hændelser med det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) som et bidrag til den fælles situationsbevidsthed. Kommissionens repræsentants rolle i IICB som kontaktpunkt bør ikke berøre Kommissionens særskilte og klart fremhævede rolle i EU-CyCLONe i henhold til artikel 16, stk. 2, i direktiv (EU) 2022/2555.

(39) Europa-Parlamentets og Rådets forordning (EU) 2018/1725[1] finder anvendelse på enhver behandling af personoplysninger i medfør af nærværende forordning. Behandlingen af personoplysninger kan finde sted i tilknytning til foranstaltninger, der er vedtaget i forbindelse med styring af cybersikkerhedsrisici, håndtering af sårbarheder og hændelser, udveksling af oplysninger om hændelser, cybertrusler og sårbarheder samt koordinering af og samarbejde om reaktion på hændelser. Sådanne foranstaltninger kan kræve behandling af visse kategorier af personoplysninger såsom IP-adresser, URL'er, domænenavne, e-mailadresser, den registreredes organisatoriske roller, tidsstempler, e-mail-overskrifter eller filnavne. Alle foranstaltninger, der træffes i henhold til nærværende forordning, bør være i overensstemmelse med rammen for databeskyttelse og privatlivets fred, og EU-enhederne, CERT-EU og, hvor det er relevant, IICB bør træffe alle relevante tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre denne overensstemmelse på en ansvarlig måde.

(40) Denne forordning fastsætter retsgrundlaget for EU-enhedernes, CERT-EU's og, hvor det er relevant, IICB's behandling af personoplysninger med henblik på at udføre deres opgaver og opfylde deres forpligtelser i henhold til denne forordning i overensstemmelse med artikel 5, stk. 1, litra b), i forordning (EU) 2018/1725. CERT-EU kan fungere som databehandler eller dataansvarlig afhængigt af den opgave, det udfører i henhold til forordning (EU) 2018/1725.

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

(41) I visse tilfælde kan det med henblik på at opfylde deres forpligtelser i henhold til denne forordning til at sikre et højt cybersikkerhedsniveau og navnlig i forbindelse med håndtering af sårbarheder og hændelser være nødvendigt for EU-enheder og CERT-EU at behandle særlige kategorier af personoplysninger som omhandlet i artikel 10, stk. 1, i forordning (EU) 2018/1725. Nærværende forordning fastsætter retsgrundlaget for EU-enhedernes og CERT-EU's behandling af særlige kategorier af personoplysninger i overensstemmelse med artikel 10, stk. 2, litra g), i forordning (EU) 2018/1725. Behandlingen af særlige kategorier af personoplysninger i henhold til nærværende forordning bør absolut stå i et rimeligt forhold til det mål, der forfølges. Med forbehold af betingelserne i artikel 10, stk. 2, litra g), i nævnte forordning bør EU-enhederne og CERT-EU kun kunne behandle sådanne oplysninger i det omfang, det er nødvendigt, og hvis det udtrykkeligt er fastsat i nærværende forordning. EU-enhederne og CERT-EU bør, når de behandler særlige kategorier af personoplysninger, respektere selve kernen i retten til databeskyttelse og sørge for passende og specifikke foranstaltninger til beskyttelse af de registreredes grundlæggende rettigheder og interesser.

(42) I henhold til artikel 33 i forordning (EU) 2018/1725 bør EU-enheder og CERT-EU under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et passende niveau af sikkerhed for personoplysninger, såsom tilvejebringelse af begrænsede adgangsrettigheder på need-to-know-basis, anvendelse af principperne for revisionsspor, indførelse af en sporbarhedskæde, opbevaring af data i hvile i et kontrolleret og kontrollerbart miljø, standardiserede operationelle procedurer og foranstaltninger til beskyttelse af privatlivets fred såsom pseudonymisering eller kryptering. Disse foranstaltninger bør ikke gennemføres på en måde, der påvirker formålene, nemlig håndtering af hændelser og bevismateriales integritet. Hvis en EU-enhed eller CERT-EU overfører personoplysninger vedrørende en hændelse, herunder særlige kategorier af personoplysninger, til en modpart eller partner med henblik på nærværende forordning, bør sådanne overførsler ske i overensstemmelse med forordning (EU) 2018/1725. Hvis særlige kategorier af personoplysninger overføres til en tredjepart, bør EU-enhederne og CERT-EU sikre, at tredjeparten anvender foranstaltninger vedrørende beskyttelse af personoplysninger på et niveau, der svarer til forordning (EU) 2018/1725.

(43) Personoplysninger, der behandles med henblik på denne forordning, bør kun opbevares, så længe det er nødvendigt, i overensstemmelse med forordning (EU) 2018/1725. EU-enheder og, hvor det er relevant, CERT-EU, der fungerer som dataansvarlig, bør fastsætte opbevaringsperioder, som er begrænsede til, hvad der er nødvendigt for at opfylde de angivne formål. Navnlig i forbindelse med personoplysninger, der indsamles med henblik på håndtering af hændelser, bør EU-enheder og CERT-EU skelne mellem personoplysninger, der indsamles med henblik på optagelse af en cybertrussel i deres IKT-miljøer for at forebygge en hændelse, og personoplysninger, der indsamles med henblik på afbødning af, reaktion på og genopretning efter en hændelse. Med henblik på opdagelse af en cybertrussel er det vigtigt at tage med i betragtning, hvor lang tid en trusselsaktør kan forblive uopdaget i et system. Med henblik på afbødning af, reaktion på og genopretning efter en hændelse er det vigtigt at overveje, om personoplysningerne er nødvendige for at spore og håndtere en tilbagevendende hændelse eller en hændelse af lignende art, med hvilken der kan påvises et sammenfald.

(44) EU-enhedernes og CERT-EU's håndtering af oplysninger bør overholde de gældende regler om informationssikkerhed. Medtagelsen af personalesikkerhed som en foranstaltning til styring af cybersikkerhedsrisici bør også overholde de gældende regler.

(45) Med henblik på udveksling af oplysninger anvendes synlige markeringer til at angive, at modtagerne af oplysninger skal anvende delingsbegrænsninger på grundlag af især aftaler om fortrolighed eller uformelle aftaler om fortrolighed såsom Traffic Light Protocol eller andre tydelige angivelser fra kilden. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger for så vidt angår den videre spredning af oplysninger. Den anvendes i næsten alle CSIRT'er og i nogle informationsanalyse- og informationsdelingscentre.

(46) Denne forordning bør evalueres regelmæssigt i lyset af fremtidige forhandlinger om flerårige finansielle rammer, som gør det muligt at træffe yderligere afgørelser med hensyn til CERT-EU's funktion og institutionelle rolle, herunder den eventuelle oprettelse af CERT-EU som et EU-kontor.

(47) IICB bør med bistand fra CERT-EU gennemgå og evaluere gennemførelsen af denne forordning og rapportere sine konklusioner til Kommissionen herom. På baggrund af denne rapportering bør Kommissionen rapportere til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget. Denne rapport bør med input fra IICB evaluere, om det er hensigtsmæssigt at medtage net- og informationssystemer, der håndterer EUCI inden for denne forordnings anvendelsesområde, navnlig i mangel af fælles informationssikkerhedsregler for EU-enhederne.

(48) I overensstemmelse med proportionalitetsprincippet er det for at virkeliggøre det grundlæggende mål, nemlig at opnå et højt fælles cybersikkerhedsniveau i EU-enhederne, nødvendigt og hensigtsmæssigt at fastsætte bestemmelser om cybersikkerhed for EU-enhederne. Denne forordning går ikke videre, end hvad der er nødvendigt for at nå det tilstræbte mål, i overensstemmelse med artikel 5, stk. 4, i traktaten om Den Europæiske Union.

(49) Denne forordning afspejler det forhold, at EU-enhederne er forskellige med hensyn til størrelse og kapacitet, herunder med hensyn til finansielle og menneskelige ressourcer.

(50) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav en udtalelse den 17. maj 2022[1] —

VEDTAGET DENNE FORORDNING:

[1] EUT C 258 af 5.7.2022, s. 10.

Kapitel I
Almindelige bestemmelser

Artikel 1

Genstand

Ved denne forordning fastsættes foranstaltninger, der har til formål at opnå et højt fælles cybersikkerhedsniveau i EU-enhederne for så vidt angår:

a) hver EU-enheds fastlæggelse af en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici i henhold til artikel 6

b) risikostyring, rapportering og udveksling af oplysninger i forbindelse med cybersikkerhedsrisici

c) organiseringen, funktionen og driften af Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, samt organiseringen, funktionen og driften af cybersikkerhedstjenesten for Unionens institutioner, organer, kontorer og agenturer (CERT-EU)

d) overvågningen af denne forordnings gennemførelse.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på EU-enheder, på Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, og på CERT-EU.

2. Denne forordning finder anvendelse, uden at det berører den institutionelle autonomi i henhold til traktaterne.

3. Med undtagelse af artikel 13, stk. 8, finder denne forordning ikke anvendelse på net- og informationssystemer, der håndterer EU's klassificerede informationer (EUCI).

Artikel 3

Definitioner

I denne forordning forstås ved:

1) "EU-enheder": Unionens institutioner, organer, kontorer og agenturer, der er oprettet ved eller i medfør af traktaten om Den Europæiske Union, traktaten om Den Europæiske Unions funktionsmåde (TEUF) eller traktaten om oprettelse af Det Europæiske Atomenergifællesskab

2) "net- og informationssystem": et net- og informationssystem som defineret i artikel 6, nr. 1), i direktiv (EU) 2022/2555

3) "sikkerhed i net- og informationssystemer": sikkerhed i net- og informationssystemer som defineret i artikel 6, nr. 2), i direktiv (EU) 2022/2555

4) "cybersikkerhed ": cybersikkerhed som defineret i artikel 2, nr. 1), i forordning (EU) 2019/881

5) "øverste ledelse": en leder, et ledelsesorgan eller et koordinerings- eller tilsynsorgan, der er ansvarlig for en EU-enheds funktionsdygtighed, på højeste administrative niveau med et mandat til at træffe eller godkende beslutninger på linje med ledelsesordningerne på højt niveau i den pågældende EU-enhed, uden at dette berører det formelle ansvar for overholdelse og cybersikkerhedsrisikostyring på andre ledelsesniveauer inden for deres respektive ansvarsområder

6) "nærvedhændelse": en nærvedhændelse som defineret i artikel 6, nr. 5), i direktiv (EU) 2022/2555

7) "hændelse": en hændelse som defineret i artikel 6, nr. 6), i direktiv (EU) 2022/2555

8) "større hændelse": en hændelse, der forårsager en forstyrrelse på et niveau, som overstiger en EU-enheds og CERT-EU's kapacitet til at reagere på den, eller som har en betydelig virkning for mindst to EU-enheder

9) "omfattende cybersikkerhedshændelse": en omfattende cybersikkerhedshændelse som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555

10) "håndtering af hændelser": håndtering af hændelser som defineret i artikel 6, nr. 8), i direktiv (EU) 2022/2555

11) "cybertrussel": en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

12) "væsentlig cybertrussel": en væsentlig cybertrussel som defineret i artikel 6, nr. 11), i direktiv (EU) 2022/2555

13) "sårbarhed": en sårbarhed som defineret i artikel 6, nr. 15), i direktiv (EU) 2022/2555

14) "cybersikkerhedsrisiko": en risiko som defineret i artikel 6, nr. 9), i direktiv (EU) 2022/2555

15) "cloudcomputingtjeneste": en cloudcomputingtjeneste som defineret i artikel 6, nr. 30), i direktiv (EU) 2022/2555.

Artikel 4

Behandling af personoplysninger

1. CERT-EU, Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, og EU-enhederne behandler personoplysninger i henhold til denne forordning i overensstemmelse med forordning (EU) 2018/1725.

2. Når de udfører opgaver eller opfylder forpligtelser i henhold til denne forordning, behandler og udveksler CERT-EU, Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, og EU-enhederne kun personoplysninger i det omfang, det er nødvendigt og udelukkende med henblik på at udføre disse opgaver eller opfylde disse forpligtelser.

3. Behandling af særlige kategorier af personoplysninger som omhandlet i artikel 10, stk. 1, i forordning (EU) 2018/1725 skal anses for at være nødvendig af hensyn til væsentlige samfundsinteresser i henhold til artikel 10, stk. 2, litra g), i nævnte forordning. Sådanne oplysninger må kun behandles i det omfang, det er nødvendigt for gennemførelsen af de foranstaltninger til styring af cybersikkerhedsrisici, som er omhandlet i artikel 6 og 8, for CERT-EU's levering af tjenester i henhold til artikel 13, for udveksling af hændelsesspecifikke oplysninger i henhold til artikel 17, stk. 3, og artikel 18, stk. 3, for udveksling af oplysninger i henhold til artikel 20, for rapporteringsforpligtelserne i henhold til artikel 21, for koordinering af og samarbejde om reaktion på hændelser i henhold til artikel 22 og for håndtering af større hændelser i henhold til artikel 23 i nærværende forordning. Når EU-enhederne og CERT-EU fungerer som dataansvarlige, anvender de tekniske foranstaltninger for at forhindre behandling af særlige kategorier af personoplysninger til andre formål og sørger for egnede og særlige foranstaltninger til beskyttelse af de registreredes grundlæggende rettigheder og interesser.

Kapitel II

Foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau

Artikel 5

Gennemførelse af foranstaltninger

1. Senest den … [otte måneder fra datoen for denne forordnings ikrafttræden] udsteder Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, efter høring af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og efter at have modtaget vejledning fra CERT-EU retningslinjer til EU-enhederne med henblik på at foretage en indledende cybersikkerhedsrevision og fastlægge en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici i henhold til artikel 6, foretage modenhedsvurderinger af cybersikkerheden i henhold til artikel 7, træffe foranstaltninger til styring af cybersikkerhedsrisici i henhold til artikel 8 og vedtage cybersikkerhedsplanen i henhold til artikel 9.

2. Ved gennemførelsen af artikel 6-9 tager EU-enhederne hensyn til de retningslinjer, der er omhandlet i nærværende artikels stk. 1, samt relevante retningslinjer og henstillinger vedtaget i henhold til artikel 11 og 14.

Artikel 6

Ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici

1. Senest den … [15 måneder fra datoen for denne forordnings ikrafttræden] fastlægger hver EU-enhed efter at have foretaget en indledende cybersikkerhedsgennemgang, såsom en revision, en intern ramme for styring, forvaltning og kontrol af cybersikkerhedsrisici ("rammen"). Fastlæggelsen af rammen overvåges af og under ansvar af EU-enhedens øverste ledelse.

2. Rammen skal dække hele den pågældende EU-enheds uklassificerede IKT-miljø, herunder lokale IKT-miljøer, lokale driftsteknologinet, udliciterede aktiver og tjenester i cloudcomputingmiljøer eller som hostes af tredjeparter, bærbare enheder, interne netværk, forretningsnetværk, der ikke er forbundet til internettet, og andre enheder, der er forbundet til disse miljøer ("IKT-miljøet"). Rammen skal være baseret på en tilgang, der omfatter alle farer.

3. Rammen skal sikre et højt cybersikkerhedsniveau. Rammen fastlægger interne cybersikkerhedspolitikker, herunder mål og prioriteter for sikkerheden i net- og informationssystemer og rollerne og ansvarsområderne for EU-enhedens personale, der har til opgave at sikre en effektiv gennemførelse af denne forordning. Rammen omfatter også mekanismer til måling af effektiviteten af gennemførelsen.

4. Rammen revideres regelmæssigt i lyset af cybersikkerhedsrisiciene, som hele tiden ændrer sig, og mindst hvert fjerde år. Hvor det er relevant, og efter anmodning fra Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, kan en EU-enheds ramme ajourføres på grundlag af vejledning fra CERT-EU om påviste hændelser eller mulige mangler i gennemførelsen af denne forordning, som er konstateret.

5. Den øverste ledelse i hver EU-enhed er ansvarlig for gennemførelsen af denne forordning og fører tilsyn med sin organisations overholdelse af forpligtelserne i forbindelse med rammen.

6. Hvor det er relevant, og uden at det berører dens ansvar for gennemførelsen af denne forordning, kan den øverste ledelse i hver EU-enhed uddelegere specifikke forpligtelser i henhold til denne forordning til seniormanagere som omhandlet i artikel 29, stk. 2, i vedtægten for tjenestemænd eller andre tjenestemænd på tilsvarende niveau i den pågældende EU-enhed. Uanset en sådan delegering kan den øverste ledelse holdes ansvarlig for den pågældende EU-enheds overtrædelser af denne forordning.

7. Hver EU-enhed indfører effektive mekanismer til sikring af, at en passende procentdel af IKT-budgettet bruges på cybersikkerhed. Der skal tages behørigt hensyn til rammen ved fastlæggelsen af denne procentdel.

8. Hver EU-enhed udpeger en lokal cybersikkerhedsansvarlig eller en ækvivalent funktion, der fungerer som det centrale kontaktpunkt vedrørende alle aspekter af cybersikkerhed. Den lokale cybersikkerhedsansvarlige fremmer gennemførelsen af denne forordning og aflægger regelmæssigt rapport direkte til den øverste ledelse om status for gennemførelsen. Uden at det berører den omstændighed, at den lokale cybersikkerhedsansvarlige er det centrale kontaktpunkt i hver EU-enhed, kan en EU-enhed uddelegere visse af den lokale cybersikkerhedsansvarliges opgaver i relation til gennemførelsen af denne forordning til CERT-EU på grundlag af en serviceleveranceaftale, som indgås mellem den pågældende EU-enhed og CERT-EU, eller disse opgaver kan deles af flere EU-enheder. Hvis disse opgaver uddelegeres til CERT-EU, træffer Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, afgørelse om, hvorvidt leveringen af denne tjeneste skal være en del af CERT-EU's basistjenester, under hensyntagen til den pågældende EU-enheds menneskelige og finansielle ressourcer. Hver EU-enhed underretter uden unødigt ophold CERT-EU om de udpegede lokale cybersikkerhedsansvarlige og alle senere ændringer af disse.

CERT-EU opretter en liste over udpegede lokale cybersikkerhedsansvarlige og holder den ajour.

9. Seniormanagere som omhandlet i artikel 29, stk. 2, i vedtægten for tjenestemænd eller andre tjenestemænd på tilsvarende niveau i hver EU-enhed samt alle relevante medarbejdere, der har til opgave at gennemføre foranstaltningerne for styring af cybersikkerhedsrisici og at opfylde forpligtelserne fastsat i denne forordning, følger regelmæssigt specifikke kurser for at tilegne sig tilstrækkelig viden og tilstrækkelige færdigheder til at forstå og vurdere cybersikkerhedsrisici- og cybersikkerhedsstyringspraksis samt virkningen heraf for EU-enhedens drift.

Artikel 7

Modenhedsvurderinger af cybersikkerheden

1. Senest den … [18 måneder fra datoen for denne forordnings ikrafttræden] og mindst hvert andet år derefter foretager hver EU-enhed en modenhedsvurdering af cybersikkerheden, der omfatter alle elementerne i dens IKT-miljø.

2. Modenhedsvurderingerne af cybersikkerheden foretages, hvor det er relevant, med bistand fra en specialiseret tredjepart.

3. EU-enheder med ensartede strukturer kan samarbejde om at foretage modenhedsvurderinger af cybersikkerheden for deres respektive enheder.

4. På grundlag af en anmodning fra Det Interinstitutionelle Råd for Cybersikkerhed, der er oprettet i henhold til artikel 10, og med den pågældende EU-enheds udtrykkelige samtykke kan resultaterne af en modenhedsvurdering af cybersikkerheden drøftes i ovennævnte råd eller i den uformelle gruppe af lokale cybersikkerhedsansvarlige med henblik på at lære af erfaringerne og udveksle bedste praksis.

Artikel 8

Foranstaltninger til styring af cybersikkerhedsrisici

1. Uden unødigt ophold og under alle omstændigheder senest den … [20 måneder fra datoen for denne forordnings ikrafttræden] træffer hver EU-enhed under tilsyn af sin øverste ledelse passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre de cybersikkerhedsrisici, der konstateres inden for rammen, og for at forebygge eller minimere virkningerne af hændelser. Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder skal disse foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer i hele IKT-miljøet, som står mål med de cybersikkerhedsrisici, der truer dem. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af EU-enhedens eksponering for cybersikkerhedsrisici, dens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige, økonomiske og interinstitutionelle indvirkning.

2. EU-enheder tager som minimum fat på følgende områder i gennemførelsen af foranstaltningerne til styring af cybersikkerhedsrisici:

a) cybersikkerhedspolitikken, herunder foranstaltninger, der er nødvendige for at nå de mål og prioriteter, der er omhandlet i artikel 6 og nærværende artikels stk. 3

b) politikker for cybersikkerhedsrisikoanalyse og informationssystemsikkerhed

c) politikmål for brugen af cloudcomputingtjenester

d) cybersikkerhedsrevision, hvor det er relevant, som kan omfatte en cybersikkerhedsrisiko-, sårbarheds- og cybertrusselsvurdering og en penetrationstest, der udføres regelmæssigt af en betroet privat udbyder

e) gennemførelse af henstillinger som følge af cybersikkerhedsrevisioner, jf. litra d), gennem cybersikkerheds- og politikopdateringer

f) organisering af cybersikkerheden, herunder fastlæggelse af roller og ansvarsområder

g) forvaltning af aktiver, herunder en liste over IKT-aktiver og en kortlægning af IKT-netværket

h) personalesikkerhed og adgangskontrol

i) driftssikkerhed

j) kommunikationssikkerhed

k) erhvervelse, udvikling og vedligeholdelse af systemer, herunder politikker for håndtering og offentliggørelse af sårbarheder

l) hvor det er muligt, politikker for kildekodens gennemsigtighed

m) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte EU-enhed og dens direkte leverandører eller tjenesteudbydere

n) håndtering af hændelser og samarbejde med CERT-EU, såsom vedligeholdelse af sikkerhedsovervågning og -logning

o) styring af driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring, og

p) fremme og udvikling af uddannelse, færdigheder, bevidstgørelse, øvelses- og undervisningsprogrammer i forbindelse med cybersikkerhed.

Med henblik på første afsnit, litra m), tager EU-enheder hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den samlede kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

3. EU-enhederne træffer som minimum følgende foranstaltninger til styring af cybersikkerhedsrisici:

a) tekniske konfigurationer med henblik på at muliggøre og opretholde telearbejde

b) konkrete skridt til at bevæge sig i retning af "zero trust"-principper

c) anvendelse af multifaktorgodkendelse som standard for alle net- og informationssystemer

d) anvendelse af kryptografi og kryptering, navnlig end-to-end-kryptering, og sikker digital underskrift

e) hvor det er relevant, anvendelse af sikker tale-, video- og tekstkommunikation og sikre nødkommunikationssystemer internt i EU-enheden

f) proaktive foranstaltninger til opdagelse og fjernelse af malware og spyware

g) etablering af forsyningskædesikkerhed for så vidt angår software ved hjælp af kriterier for sikker udvikling og evaluering af software

h) fastlæggelse og indførelse af uddannelsesprogrammer om cybersikkerhed, som svarer til de foreskrevne opgaver og den forventede kapacitet, for den øverste ledelse og medarbejdere i EU-enheden, der har til opgave at sikre den effektive gennemførelse af denne forordning

i) regelmæssig uddannelse af medarbejdere i cybersikkerhed

j) hvor det er relevant, deltagelse i risikoanalyser af sammenkoblingsordningerne mellem EU-enhederne

k) forbedring af indkøbsprocedurerne med henblik på at fremme et højt fælles cybersikkerhedsniveau ved hjælp af:

   i) fjernelse af kontraktmæssige hindringer, der begrænser IKT-tjenesteudbydernes udveksling af oplysninger om cybertrusler, sårbarheder og hændelser med CERT-EU

   ii) kontraktmæssige forpligtelser til at indberette hændelser, sårbarheder og cybertrusler samt til at have passende mekanismer for reaktion på og overvågning af hændelser.

Artikel 9

Cybersikkerhedsplaner

1. Efter færdiggørelsen af den modenhedsvurdering af cybersikkerheden, der er foretaget i henhold til artikel 7, og under hensyntagen til de aktiver og cybersikkerhedsrisici, der er konstateret inden for rammen og de foranstaltninger til styring af cybersikkerhedsrisici, der er truffet i henhold til artikel 8, godkender den øverste ledelse i hver EU-enhed en cybersikkerhedsplan uden unødigt ophold og under alle omstændigheder senest den … [24 måneder fra datoen for denne forordnings ikrafttræden]. Cybersikkerhedsplanen skal tage sigte på at øge EU-enhedens overordnede cybersikkerhed og derved bidrage til forbedringen af et højt fælles cybersikkerhedsniveau i EU-enhederne. Cybersikkerhedsplanen skal som minimum omfatte de foranstaltninger til styring af cybersikkerhedsrisiciene, der er truffet i henhold til artikel 8. Cybersikkerhedsplanen revideres hvert andet år eller hyppigere, hvis det er nødvendigt, efter de modenhedsvurderinger af cybersikkerheden, der er foretaget i henhold til artikel 7, eller en eventuel betydelig revision af rammen.

2. Cybersikkerhedsplanen skal omfatte EU-enhedens plan for cyberkrisestyring i tilfælde af større hændelser.

3. EU-enheden forelægger den fuldstændige cybersikkerhedsplan for Det Interinstitutionelle Råd for Cybersikkerhed, som er oprettet i henhold til artikel 10.

Kapitel III

Det Interinstitutionelle Råd for Cybersikkerhed

Artikel 10

Det Interinstitutionelle Råd for Cybersikkerhed

1. Det Interinstitutionelle Råd for Cybersikkerhed (IICB) oprettes herved.

2. IICB er ansvarligt for:

   a) at overvåge og støtte EU-enhedernes gennemførelse af denne forordning

   b) at føre tilsyn med CERT-EU's gennemførelse af de generelle prioriteter og mål og udstikke den strategiske retning for CERT-EU.

3. IICB sammensættes af:

   a) én repræsentant udpeget af hver af følgende:

      i) Europa-Parlamentet

      ii) Det Europæiske Råd

iii) Rådet for Den Europæiske Union

iv) Kommissionen

v) Den Europæiske Unions Domstol

vi) Den Europæiske Centralbank

vii) Revisionsretten

viii) Tjenesten for EU's Optræden Udadtil

ix) Det Europæiske Økonomiske og Sociale Udvalg

x) Regionsudvalget

xi) Den Europæiske Investeringsbank

xii) Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed

xiii) ENISA

xiv) Den Europæiske Tilsynsførende for Databeskyttelse (EDPS)

xv) Den Europæiske Unions Agentur for Rumprogrammet.

b) tre repræsentanter udpeget af EU-agenturernes netværk (EUAN) på grundlag af et forslag fra netværkets rådgivende IKT-udvalg til at repræsentere interesserne for Unionens organer, kontorer og agenturer, der har deres eget IKT-miljø, bortset fra dem, der er omhandlet i litra a).

De EU-enheder, der er repræsenteret i IICB, tilstræber at opnå en ligelig kønsfordeling blandt de udpegede repræsentanter.

4. Medlemmerne af IICB kan bistås af en suppleant. Formanden kan invitere andre repræsentanter for de i stk. 3 omhandlede EU-enheder eller for andre EU-enheder til at deltage i IICB's møder uden stemmeret.

5. Chefen for CERT-EU samt formændene for samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe, der er oprettet i henhold til henholdsvis artikel 14, 15 og 16 i direktiv (EU) 2022/2555, eller deres suppleanter kan deltage i IICB's møder som observatører. I undtagelsestilfælde kan IICB i overensstemmelse med dets forretningsorden træffe en anden afgørelse.

6. IICB vedtager sin egen forretningsorden.

7. IICB udpeger en formand blandt medlemmerne i overensstemmelse med sin forretningsorden og for en periode på tre år. Formandens suppleant bliver fuldgyldigt medlem af IICB for samme periode.

8. IICB mødes mindst tre gange årligt på formandens initiativ, efter anmodning fra CERT-EU, eller efter anmodning fra et af medlemmerne.

9. Hvert medlem af IICB har én stemme. IICB's afgørelser træffes med simpelt flertal, såfremt intet andet er fastsat i denne forordning. Formanden for IICB har ikke stemmeret, undtagen i tilfælde af stemmelighed, hvor formanden kan afgive den afgørende stemme.

10. IICB kan handle ved hjælp af en forenklet skriftlig procedure, som indledes i overensstemmelse med dets forretningsorden. I henhold til denne procedure anses den relevante afgørelse for at være godkendt inden for den tidsfrist, som formanden har fastsat, medmindre et medlem gør indsigelse.

11. IICB's sekretariat stilles til rådighed af Kommissionen og refererer til IICB's formand.

12. De repræsentanter, der er udpeget af EUAN, formidler IICB's afgørelser til EUAN's medlemmer. Ethvert medlem af EUAN har ret til over for disse repræsentanter eller IICB's formand at rejse ethvert spørgsmål, som medlemmet mener, IICB bør gøres opmærksom på.

13. IICB kan nedsætte et forretningsudvalg til at bistå IICB i dets arbejde og delegere nogle af sine opgaver og beføjelser til samme. IICB fastsætter forretningsudvalgets forretningsorden, herunder dets opgaver og beføjelser, og dets medlemmers mandatperiode.

14. Senest den … [12 måneder fra datoen for denne forordnings ikrafttræden] og derefter hvert år forelægger IICB en rapport for Europa-Parlamentet og Rådet, som indeholder en detaljeret beskrivelse af de fremskridt, der er gjort med gennemførelsen af denne forordning, og som navnlig præciserer omfanget af CERT-EU's samarbejde med medlemsstatsmodparter i hver af medlemsstaterne. Rapporten udgør et input til den rapport, der kommer hvert andet år, om cybersikkerhedssituationen i Unionen, som vedtages i henhold til artikel 18 i direktiv (EU) 2022/2555.

Artikel 11

IICB's opgaver

Når det udfører sine forpligtelser, skal IICB navnlig:

a) yde vejledning til CERT-EU's chef

b) effektivt overvåge og føre tilsyn med gennemførelsen af denne forordning og støtte EU-enhederne i at styrke deres cybersikkerhed, herunder, hvor det er relevant, anmode om ad hoc-rapporter fra EU-enhederne og CERT-EU

c) efter en strategisk drøftelse vedtage en flerårig strategi for forøgelse af cybersikkerhedsniveauet i EU-enhederne, vurdere denne strategi regelmæssigt og under alle omstændigheder hvert femte år og, hvor det er nødvendigt, ændre strategien

d) fastlægge metoden for og de organisatoriske aspekter af EU-enhedernes gennemførelse af frivillige peerevalueringer med henblik på at lære af fælles erfaringer, styrke den gensidige tillid, opnå et højt fælles cybersikkerhedsniveau og styrke EU-enhedernes cybersikkerhedskapacitet, idet det sikres, at sådanne peerevalueringer foretages af cybersikkerhedseksperter udpeget af en anden EU-enhed end den EU-enhed, der evalueres, og at metoden er baseret på artikel 19 i direktiv (EU) 2022/2555 og, hvor det er relevant, er tilpasset EU-enhederne

e) godkende CERT-EU's årlige arbejdsprogram på grundlag af et forslag fra CERT-EU's chef og overvåge gennemførelsen heraf

f) godkende CERT-EU's tjenestekatalog og eventuelle senere ajourføringer heraf på grundlag af et forslag fra CERT-EU's chef

g) på grundlag af et forslag fra CERT-EU's chef godkende den årlige finansielle planlægning af indtægter og udgifter, herunder personale, i forbindelse med CERT-EU's aktiviteter

h) godkende ordningerne for serviceleveranceaftaler på grundlag af et forslag fra CERT-EU's chef

i) behandle og godkende den årsrapport, som udarbejdes af CERT-EU's chef, og som omfatter CERT-EU's aktiviteter og forvaltning af midler

j) godkende og overvåge nøgleresultatindikatorer (KPI'er) for CERT-EU, der fastsættes på grundlag af et forslag fra CERT-EU's chef

k) godkende samarbejdsaftaler, serviceleveranceaftaler eller kontrakter mellem CERT-EU og andre enheder, der indgås i medfør af artikel 18

l) vedtage retningslinjer og henstillinger på grundlag af et forslag fra CERT-EU i overensstemmelse med artikel 14 og pålægge CERT-EU at udstede, tilbagekalde eller ændre et forslag til retningslinjer eller henstillinger eller en opfordring til tiltag

m) nedsætte tekniske rådgivende grupper med specifikke opgaver til at bistå IICB i dets arbejde, godkende deres mandat og udpege deres respektive formænd

n) modtage og vurdere dokumenter og rapporter, der forelægges af EU-enhederne i henhold til denne forordning, såsom modenhedsvurderinger af cybersikkerheden

o) fremme nedsættelsen af en uformel gruppe bestående af EU-enhedernes lokale cybersikkerhedsansvarlige med støtte fra ENISA med henblik på udveksling af bedste praksis og oplysninger i forbindelse med gennemførelsen af denne forordning

p) under hensyntagen til oplysningerne om de udpegede cybersikkerhedsrisici og de indhøstede erfaringer, der kommer fra CERT-EU, overvåge, om sammenkoblingsordningerne mellem EU-enhedernes IKT-miljøer er tilstrækkelige, og rådgive om mulige forbedringer

q) fastlægge en plan for cyberkrisestyring for på operationelt plan at støtte den koordinerede håndtering af større hændelser, der påvirker EU-enheder, og bidrage til regelmæssig udveksling af relevante oplysninger, navnlig med hensyn til virkningerne og alvoren af større hændelser og de mulige metoder til at afbøde virkningerne heraf

r) koordinere vedtagelsen af de enkelte EU-enheders cyberkrisestyringsplaner, jf. artikel 9, stk. 2

s) vedtage henstillinger vedrørende forsyningskædesikkerhed som omhandlet i artikel 8, stk. 2, første afsnit, litra m), under hensyntagen til resultaterne af sikkerhedsrisikovurderinger koordineret på EU-niveau af kritiske forsyningskæder, jf. artikel 22 i direktiv (EU) 2022/2555, for at støtte EU-enhederne i at vedtage effektive og forholdsmæssige foranstaltninger til styring af cybersikkerhedsrisici.

Artikel 12

Overholdelse

1. IICB overvåger i henhold til artikel 10, stk. 2, og artikel 11 effektivt EU-enhedernes gennemførelse af denne forordning og de vedtagne retningslinjer, henstillinger og opfordringer til tiltag. IICB kan anmode EU-enhederne om de oplysninger eller den dokumentation, der er behov for til dette formål. Med henblik på vedtagelse af overholdelsesforanstaltninger i henhold til nærværende artikel har den pågældende EU-enhed, såfremt den er direkte repræsenteret i IICB, ikke stemmeret.

2. Hvis IICB finder, at en EU-enhed ikke på effektiv vis har gennemført denne forordning eller retningslinjer, henstillinger eller opfordringer til tiltag, som er udstedt i medfør heraf, kan det, uden at dette berører den pågældende EU-enheds interne procedurer, og efter at have givet den pågældende EU-enhed mulighed for at fremsætte sine bemærkninger gøre følgende:

   a) sende en begrundet udtalelse til den pågældende EU-enhed med konstaterede mangler i gennemførelsen af denne forordning

   b) efter høring af CERT-EU udstede retningslinjer til den pågældende EU-enhed for at sikre, at dens ramme, foranstaltninger til styring af cybersikkerhedsrisici, cybersikkerhedsplan og rapportering er i overensstemmelse med denne forordning inden for en nærmere angivet periode

c) udstede en advarsel om, at konstaterede mangler skal afhjælpes inden for en nærmere angivet periode, herunder henstillinger om ændring af foranstaltninger vedtaget af den pågældende EU-enhed i henhold til denne forordning

d) udstede en begrundet meddelelse til den pågældende EU-enhed, hvis de mangler, der blev påpeget i en advarsel udstedt i henhold til litra c), ikke er blevet afhjulpet i tilstrækkelig grad inden for den fastsatte periode

e) udstede:

   i) en henstilling om, at der foretages en revision, eller

   ii) en anmodning om, at en tredjepartsrevisionstjeneste foretager en revision

f) hvor det er relevant, underrette Revisionsretten inden for rammerne af sit mandat om den påståede manglende overholdelse

g) udstede en henstilling om, at alle medlemsstater og EU-enheder foretager en midlertidig afbrydelse af datastrømmene til den pågældende EU-enhed.

Med henblik på litra c), første afsnit, begrænses advarslens læserskare på passende vis, hvis det er nødvendigt i lyset af cybersikkerhedsrisikoen.

Advarsler og henstillinger udstedt i henhold til første afsnit rettes til det øverste ledelsesniveau i den pågældende EU-enhed.

3. Hvis IICB har vedtaget foranstaltninger i henhold til stk. 2, første afsnit, litra a)-g), fremlægger den pågældende EU-enhed detaljer om de foranstaltninger og tiltag, der er iværksat for at afhjælpe de påståede mangler, som IICB har konstateret. EU-enheden indsender disse detaljer inden for en rimelig periode, der aftales med IICB.

4. Hvis IICB finder, at en EU-enhed vedholdende overtræder denne forordning som en direkte følge af en EU-tjenestemands eller anden EU-ansats handlinger eller undladelser, herunder i den øverste ledelse, anmoder IICB om, at den pågældende EU-enhed iværksætter passende tiltag, hvilket indbefatter en anmodning om at iværksætte tiltag af disciplinær karakter, i overensstemmelse med de regler og procedurer, der er fastsat i vedtægten for tjenestemænd, og eventuelle andre gældende regler og procedurer. Med henblik herpå videregiver IICB de nødvendige oplysninger til den pågældende EU-enhed.

5. Hvis EU-enheder meddeler, at de ikke er i stand til at overholde fristerne i artikel 6, stk. 1, og artikel 8, stk. 1, kan IICB i behørigt begrundede tilfælde under hensyntagen til EU-enhedens størrelse tillade en forlængelse af disse frister.

Kapitel IV
CERT-EU

Artikel 13

CERT-EU's mission og opgaver

1. CERT-EU's mission er at bidrage til det uklassificerede IKT-miljøs sikkerhed i alle EU-enheder ved at rådgive dem om cybersikkerhed, hjælpe dem med at forebygge, opdage, håndtere, afbøde, reagere på og reetablere sig efter hændelser og fungere som deres knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og for koordinering af reaktionen på hændelser.

2. CERT-EU indsamler, forvalter, analyserer og deler oplysninger med EU-enhederne om cybertrusler, sårbarheder og hændelser i uklassificeret IKT-infrastruktur. Det koordinerer beredskabet i forbindelse med hændelser på interinstitutionelt niveau og på EU-enhedsniveau, herunder ved at yde eller koordinere ydelsen af specialiseret operationel bistand.

3. CERT-EU udfører følgende opgaver for at bistå EU-enhederne:

   a) støtter dem i forbindelse med gennemførelsen af denne forordning og bidrager til koordineringen af gennemførelsen af denne forordning ved hjælp af de foranstaltninger, der er opført i artikel 14, stk. 1, eller ved hjælp af ad hoc-rapporter, som IICB har anmodet om

b) tilbyder standardiserede CSIRT-tjenester til EU-enheder i form af en pakke af cybersikkerhedstjenester beskrevet i dets tjenestekatalog ("basistjenester")

c) vedligeholder et netværk af ligestillede og partnere til støtte for tjenesterne, jf. artikel 17 og 18

d) gør IICB opmærksom på problemer, der vedrører gennemførelsen af denne forordning samt gennemførelsen af retningslinjer, henstillinger og opfordringer til tiltag

e) bidrager på grundlag af de oplysninger, der er omhandlet i stk. 2, til Unionens cybersituationsbevidsthed i tæt samarbejde med ENISA

f) koordinerer håndteringen af større hændelser

g) agerer på vegne af EU-enhederne som ækvivalent med den koordinator, der er udpeget med henblik på koordineret offentliggørelse af sårbarheder, jf. artikel 12, stk. 1, i direktiv (EU) 2022/2555

h) sørger efter anmodning fra en EU-enhed for en proaktiv, ikkeindgribende scanning af den pågældende EU-enheds offentligt tilgængelige net- og informationssystemer.

De oplysninger, der er omhandlet i første afsnit, litra e), deles med IICB, CSIRT-netværket og Den Europæiske Unions Efterretnings- og Situationscenter (EU INTCEN), hvor det er relevant og hensigtsmæssigt, og under overholdelse af passende fortrolighedsbetingelser.

4. CERT-EU kan i overensstemmelse med artikel 17 eller 18, alt efter hvad der er relevant, samarbejde med relevante cybersikkerhedsfællesskaber i Unionen og dens medlemsstater, herunder på følgende områder:

a) beredskab, koordinering i forbindelse med hændelser, udveksling af oplysninger og reaktion på kriser på teknisk plan i forbindelse med sager, der har tilknytning til EU-enhederne

b) operationelt samarbejde i forbindelse med CSIRT-netværket, herunder med hensyn til gensidig bistand

c) efterretninger om cybertrusler, herunder situationsbevidsthed

d) et hvilket som helst andet område, hvor CERT-EU's tekniske cybersikkerhedsekspertise er påkrævet.

5. CERT-EU indgår inden for sin kompetence i et struktureret samarbejde med ENISA om kapacitetsopbygning, operationelt samarbejde og langsigtede strategiske analyser af cybertrusler i overensstemmelse med forordning (EU) 2019/881. CERT-EU kan samarbejde og udveksle oplysninger med Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet.

6. CERT-EU kan levere følgende tjenester, der ikke er beskrevet i dets tjenestekatalog (betalingspligtige tjenester):

a) tjenester til støtte for cybersikkerheden i relation til EU-enhedernes IKT-miljø ud over dem, der er omhandlet i stk. 3, i henhold til serviceleveranceaftaler og under forudsætning af, at der er ressourcer til rådighed, navnlig bredspektret overvågning af netværk, herunder 24/7-frontlinjeovervågning af meget alvorlige cybertrusler

b) tjenester til støtte for EU-enhedernes cybersikkerhedsoperationer eller -projekter ud over dem, der beskytter deres IKT-miljø, i henhold til skriftlige aftaler og under forudsætning af forudgående godkendelse fra IICB

c) efter anmodning en proaktiv scanning af den pågældende EU-enheds net- og informationssystemer for at opdage sårbarheder med en potentiel væsentlig virkning

d) tjenester til støtte for IKT-miljøers sikkerhed i andre organisationer end EU-enhederne, som arbejder tæt sammen med EU-enhederne, f.eks. fordi de er tildelt opgaver eller ansvarsområder i henhold til EU-retten, i henhold til skriftlige aftaler og under forudsætning af forudgående godkendelse fra IICB.

For så vidt angår første afsnit, litra d), kan CERT-EU undtagelsesvis indgå serviceleveranceaftaler med andre enheder end EU-enheder med forudgående godkendelse fra IICB.

7. CERT-EU arrangerer og kan deltage i cybersikkerhedsøvelser eller opfordre til deltagelse i eksisterende øvelser, hvor det er relevant i tæt samarbejde med ENISA, med henblik på at teste cybersikkerhedsniveauet i EU-enhederne.

8. CERT-EU kan yde bistand til EU-enhederne vedrørende hændelser i net- og informationssystemer, der håndterer EUCI, hvis de pågældende EU-enheder udtrykkeligt anmoder herom i overensstemmelse med deres respektive procedurer. CERT-EU's ydelse af bistand i henhold til dette stykke berører ikke gældende regler om beskyttelse af klassificerede informationer.

9. CERT-EU underretter EU-enhederne om sine procedurer og processer for håndtering af hændelser.

10. CERT-EU bidrager med en høj grad af fortrolighed og pålidelighed via de behørige samarbejdsmekanismer og rapporteringsveje til relevante og anonymiserede oplysninger om større hændelser og måden, hvorpå de blev håndteret. Disse oplysninger medtages i den rapport, der er omhandlet i artikel 10, stk. 14.

11. CERT-EU støtter i samarbejde med EDPS de pågældende EU-enheder, når de håndterer hændelser, der medfører brud på persondatasikkerheden, uden at dette berører EDPS' kompetencer og opgaver som tilsynsmyndighed i henhold til forordning (EU) 2018/1725.

12. CERT-EU kan, hvis EU-enhedernes politiske afdelinger udtrykkeligt anmoder herom, yde teknisk rådgivning eller input om relevante politiske spørgsmål.

Artikel 14

Retningslinjer, henstillinger og opfordringer til tiltag

1. CERT-EU støtter gennemførelsen af denne forordning ved at udstede:

   a) opfordringer til tiltag, der beskriver hastende sikkerhedsforanstaltninger, som EU-enhederne kraftigt opfordres til at træffe inden udløbet af en fastsat frist

   b) forslag til IICB om retningslinjer rettet til alle eller en delgruppe af EU-enheder

   c) forslag til IICB om henstillinger rettet til individuelle EU-enheder.

   Med hensyn til første afsnit, litra a), underretter den pågældende EU-enhed uden unødigt ophold efter modtagelsen af opfordringen til tiltag CERT-EU om, hvordan de hastende sikkerhedsforanstaltninger er blevet anvendt.

2. Retningslinjer og henstillinger kan omfatte:

a) fælles metoder og en model for modenhedsvurdering af EU-enhedernes cybersikkerhed, herunder de tilhørende skalaer eller KPI'er, der tjener som reference til støtte for løbende forbedringer af cybersikkerheden i alle EU-enhederne og letter prioriteringen af cybersikkerhedsområder og -foranstaltninger under hensyntagen til enhedernes cybersikkerhedstilstand

b) ordninger for eller forbedringer af styringen af cybersikkerhedsrisici og foranstaltningerne til styring af cybersikkerhedsrisici

c) ordninger for modenhedsvurderinger af cybersikkerheden og cybersikkerhedsplaner

d) hvor det er relevant, brugen af fælles teknologi, arkitektur, open source og dertil knyttet bedste praksis med henblik på at opnå interoperabilitet og fælles standarder, herunder en koordineret tilgang til forsyningskædesikkerhed

e) hvor det er relevant, oplysninger med henblik på at lette anvendelsen af fælles udbudsinstrumenter til indkøb af relevante cybersikkerhedstjenester og -produkter fra tredjepartsleverandører

f) ordninger for udveksling af oplysninger i henhold til artikel 20.

Artikel 15

Chefen for CERT-EU

1. Kommissionen udnævner chefen for CERT-EU efter at have indhentet godkendelse fra to tredjedele af IICB's medlemmer. IICB høres i alle udvælgelsesprocedurens faser, navnlig i forbindelse med udarbejdelse af stillingsopslag, behandling af ansøgninger og udpegelse af udvælgelseskomitéer i forbindelse med denne stilling. Udvælgelsesproceduren, herunder den endelige liste over kandidater, blandt hvilke CERT-EU's chef skal udnævnes, skal sikre en retfærdig repræsentation af hvert køn under hensyntagen til de indgivne ansøgninger.

2. Chefen for CERT-EU er ansvarlig for, at CERT-EU fungerer korrekt, og handler inden for rammerne af sin rolle og under ledelse af IICB. Chefen for CERT-EU aflægger regelmæssigt rapport til formanden for IICB og forelægger ad hoc-rapporter for IICB på anmodning herfra.

3. Chefen for CERT-EU bistår den ved delegation bemyndigede ansvarlige anvisningsberettigede med udarbejdelsen af årsberetningen med oplysninger om de finansielle og forvaltningsmæssige forhold, herunder kontrolresultater, der udarbejdes i overensstemmelse med artikel 74, stk. 9, i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046[1], og aflægger regelmæssigt rapport til den ved delegation bemyndigede anvisningsberettigede om gennemførelsen af foranstaltninger, i forbindelse med hvilke der er videredelegeret beføjelser til chefen for CERT-EU.

4. Chefen for CERT-EU udarbejder årligt en finansiel planlægning af de administrative indtægter og udgifter i forbindelse med CERT-EU's aktiviteter, et forslag til det årlige arbejdsprogram, et forslag til CERT-EU's tjenestekatalog, foreslåede ændringer af tjenestekataloget, et forslag til ordninger for serviceleveranceaftaler og foreslåede KPI'er for CERT-EU, som IICB skal godkende i overensstemmelse med artikel 11. Ved revision af listen over tjenester i CERT-EU's tjenestekatalog tager CERT-EU's chef hensyn til de ressourcer, som CERT-EU har fået tildelt.

---

[1] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1).

5. Chefen for CERT-EU forelægger mindst en gang om året IICB og formanden for IICB rapporter om CERT-EU's aktiviteter og resultater i referenceperioden, herunder om gennemførelsen af budgettet, serviceleveranceaftaler og indgåede skriftlige aftaler, samarbejde med modparter og partnere og tjenesterejser, som personalet har foretaget, herunder de rapporter, der er omhandlet i artikel 11. Disse rapporter skal indeholde et arbejdsprogram for den efterfølgende periode, finansiel planlægning af indtægter og udgifter, herunder personale, planlagte ajourføringer af CERT-EU's tjenestekatalog og en vurdering af den forventede virkning, som sådanne ajourføringer kan have med hensyn til finansielle og menneskelige ressourcer.

Artikel 16

Finansielle og personalemæssige spørgsmål

1. CERT-EU integreres i den administrative struktur i et generaldirektorat i Kommissionen for at drage fordel af Kommissionens strukturer for administrativ, finansiel og regnskabsmæssig støtte, samtidig med at CERT-EU bevarer sin status som en uafhængig interinstitutionel tjenesteyder for alle EU-enheder. Kommissionen underretter IICB om CERT-EU's administrative placering og alle ændringer heraf. Kommissionen gennemgår de administrative ordninger vedrørende CERT-EU regelmæssigt og under alle omstændigheder inden fastlæggelsen af en flerårig finansiel ramme i henhold til artikel 312 i TEUF for at gøre det muligt at træffe passende tiltag. Gennemgangen skal omfatte muligheden for at oprette CERT-EU som et EU-kontor.

2. Med hensyn til anvendelsen af de administrative og finansielle procedurer handler CERT-EU's chef med referat til Kommissionen og under IICB's tilsyn.

3. CERT-EU's opgaver og aktiviteter, herunder tjenester, som CERT-EU yder i henhold til artikel 13, stk. 3, 4, 5 og 7, og artikel 14, stk. 1, til EU-enheder, og som finansieres under det udgiftsområde i den flerårige finansielle ramme, der vedrører europæisk offentlig forvaltning, finansieres over en særlig budgetpost på Kommissionens budget. De stillinger, der er øremærket til CERT-EU, beskrives nærmere i en fodnote til Kommissionens stillingsfortegnelse.

4. Andre EU-enheder end dem, der er omhandlet i denne artikels stk. 3, yder et årligt finansielt bidrag til CERT-EU til dækning af de tjenester, som CERT-EU yder i henhold til nævnte stykke. Bidragene baseres på retningslinjer, der er udstedt af IICB og aftalt mellem hver enkelt EU-enhed og CERT-EU i serviceleveranceaftaler. Bidragene afspejler en fair og forholdsmæssig andel af de samlede omkostninger ved de tjenester, der er ydet. De opføres på den særlige budgetpost, der er omhandlet i denne artikels stk. 3, som formålsbestemte indtægter, jf. artikel 21, stk. 3, litra c), i forordning (EU, Euratom) 2018/1046.

5. Omkostningerne ved de tjenester, der er fastsat i artikel 13, stk. 6, opkræves fra de EU-enheder, der har gjort brug af CERT-EU's tjenester. Indtægterne opføres på de budgetposter, der vedrører omkostningerne.

Artikel 17

CERT-EU's samarbejde med medlemsstatsmodparter

1. CERT-EU samarbejder og udveksler oplysninger uden unødigt ophold med modparter i medlemsstaterne, navnlig de CSIRT'er, der er udpeget eller oprettet i henhold til artikel 10 i direktiv (EU) 2022/2555, eller, hvor det er relevant, de kompetente myndigheder og centrale kontaktpunkter, der er udpeget eller oprettet i henhold til artikel 8 i nævnte direktiv, om hændelser, cybertrusler, sårbarheder, nærvedhændelser, eventuelle modforanstaltninger samt bedste praksis og om alle spørgsmål, der er relevante for at forbedre beskyttelsen af EU-enhedernes IKT-miljøer, herunder ved hjælp af det CSIRT-netværk, der er oprettet i henhold til artikel 15 i direktiv (EU) 2022/2555. CERT-EU støtter Kommissionen i EU-CyCLONe, som er oprettet i henhold til artikel 16 i direktiv (EU) 2022/2555 om koordineret forvaltning af omfattende cybersikkerhedshændelser og kriser.

2. Hvis CERT-EU bliver opmærksomt på en væsentlig hændelse, der indtræffer på en medlemsstats område, underretter det straks alle relevante medlemsstatsmodparter i den pågældende medlemsstat i overensstemmelse med stk. 1.

3. Forudsat at personoplysninger er beskyttet i overensstemmelse med gældende EU-databeskyttelsesret, udveksler CERT-EU uden unødigt ophold relevante hændelsesspecifikke oplysninger med medlemsstatsmodparter for at lette opdagelsen af lignende cybertrusler eller -hændelser eller for at bidrage til analysen af en hændelse uden tilladelse fra den berørte EU-enhed. CERT-EU udveksler kun hændelsesspecifikke oplysninger, der afslører identiteten på målet for hændelsen, i tilfælde af et af følgende:

a) den berørte EU-enhed giver samtykke

b) den berørte EU-enhed ikke giver samtykke som fastsat i litra a), men offentliggørelsen af den berørte EU-enheds identitet vil øge sandsynligheden for, at hændelser andre steder vil blive undgået eller afbødet

c) den berørte EU-enhed allerede har offentliggjort, at den var berørt.

Afgørelser om udveksling af hændelsesspecifikke oplysninger, der afslører identiteten af målet for hændelsen i henhold til første afsnit, litra b), skal godkendes af CERT-EU's chef. Inden offentliggørelsen af en sådan afgørelse, kontakter CERT-EU skriftligt den berørte EU-enhed og forklarer tydeligt, hvordan offentliggørelsen af dens identitet vil bidrage til at undgå eller afbøde hændelser andre steder. CERT-EU's chef giver denne forklaring og anmoder udtrykkeligt EU-enheden om at meddele, hvorvidt den giver samtykke, inden for en fastsat frist. CERT-EU's chef oplyser også EU-enheden om, at han eller hun i lyset af den fremlagte forklaring forbeholder sig ret til at videregive oplysningerne, selv om der ikke gives samtykke. Den berørte EU-enhed underrettes, inden oplysningerne videregives.

Artikel 18

CERT-EU's samarbejde med andre modparter

1. CERT-EU må samarbejde med andre modparter i Unionen end dem, der er omhandlet i artikel 17, som er underlagt EU-cybersikkerhedskrav, herunder branchespecifikke modparter, om værktøjer og metoder såsom teknikker, taktikker, procedurer og bedste praksis samt om cybertrusler og sårbarheder. CERT-EU indhenter med henblik på alt samarbejde med sådanne modparter forudgående godkendelse fra IICB i hvert enkelt tilfælde. Hvis CERT-EU etablerer et samarbejde med sådanne modparter, underretter den alle relevante medlemsstatsmodparter, jf. artikel 17, stk. 1, i den medlemsstat, hvor modparten befinder sig. Hvor det er relevant og hensigtsmæssigt, fastlægges et sådant samarbejde og betingelserne herfor, herunder vedrørende cybersikkerhed, databeskyttelse og håndtering af oplysninger, i særlige aftaler om fortrolighed, såsom kontrakter eller administrative ordninger. Aftalerne om fortrolighed kræver ikke forudgående godkendelse fra IICB, men IICB's formand skal underrettes. I tilfælde af et presserende og nært forestående behov for at udveksle cybersikkerhedsoplysninger i EU-enhedernes eller en anden parts interesse kan CERT-EU gøre dette med en enhed, hvis specifikke kompetence, kapacitet og ekspertise med god grund er nødvendig for at bistå med et sådant presserende og nært forestående behov, selv om CERT-EU ikke har indgået en aftale om fortrolighed med den pågældende enhed. I sådanne tilfælde underretter CERT-EU straks IICB's formand og aflægger rapport til IICB gennem regelmæssige rapporter eller møder.

2. CERT-EU må samarbejde med andre partnere såsom kommercielle enheder, herunder branche- og sektorspecifikke enheder, internationale organisationer, nationale ikke-EU-enheder eller individuelle eksperter med henblik på at indsamle oplysninger om generelle og specifikke cybertrusler, nærvedhændelser, sårbarheder og mulige modforanstaltninger. CERT-EU indhenter med henblik på at indlede et bredere samarbejde med sådanne partnere forudgående godkendelse fra IICB i hvert enkelt tilfælde.

3. CERT-EU må med samtykke fra den EU-enhed, der er berørt af en hændelse, og forudsat at der er indgået en aftale eller kontrakt om fortrolighed med den relevante modpart eller partner, give oplysninger om den specifikke hændelse til modparter eller partnere, der er omhandlet i stk. 1 og 2, udelukkende med henblik på at bidrage til analysen heraf.

Kapitel V

Samarbejde og rapporteringsforpligtelser

Artikel 19

Håndtering af oplysninger

1. EU-enhederne og CERT-EU overholder tavshedspligten i overensstemmelse med artikel 339 i TEUF eller tilsvarende gældende rammer.

2. Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001[1] finder anvendelse på anmodninger om aktindsigt i dokumenter, som CERT-EU er i besiddelse af, herunder forpligtelsen i nævnte forordning til at rådføre sig med andre EU-enheder eller, hvor det er relevant, medlemsstater, når en anmodning vedrører deres dokumenter.

3. EU-enhedernes og CERT-EU's håndtering af oplysninger sker i overensstemmelse med de gældende regler om informationssikkerhed.

Artikel 20

Ordninger for udveksling af cybersikkerhedsoplysninger

1. EU-enheder kan på frivillig basis underrette CERT-EU og give det oplysninger om hændelser, cybertrusler, nærvedhændelser og sårbarheder, der berører dem. CERT-EU sikrer, at der er adgang til effektive kommunikationsmidler med en høj grad af sporbarhed, fortrolighed og pålidelighed med henblik på at fremme udveksling af oplysninger med EU-enhederne. CERT-EU kan ved behandlingen af underretninger prioritere behandlingen af obligatoriske underretninger fremfor frivillige underretninger. Med forbehold af artikel 12 må frivillig underretning ikke medføre, at den rapporterende EU-enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde indgivet underretningen.

---

[1] Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

2. CERT-EU kan med henblik på at udføre sin mission og sine opgaver som omhandlet i artikel 13 anmode EU-enhederne om oplysninger fra deres respektive IKT-systemfortegnelser, herunder oplysninger vedrørende cybertrusler, nærvedhændelser, sårbarheder, kompromitteringsindikatorer, cybersikkerhedsadvarsler og henstillinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberhændelser. En EU-enhed, der modtager en sådan anmodning, overfører de oplysninger, der anmodes om, samt eventuelle efterfølgende ajourføringer heraf uden unødigt ophold.

3. CERT-EU må udveksle hændelsesspecifikke oplysninger med EU-enheder, der afslører identiteten på den EU-enhed, der er berørt af hændelsen, forudsat at den berørte EU-enhed giver sit samtykke. Hvis en EU-enhed nægter at give samtykke, giver den CERT-EU en begrundelse, der underbygger denne afgørelse.

4. EU-enheder udveksler på anmodning oplysninger med Europa-Parlamentet og Rådet om færdiggørelsen af cybersikkerhedsplanerne.

5. IICB eller CERT-EU, alt efter hvad der er relevant, deler på anmodning retningslinjer, henstillinger og opfordringer til tiltag med Europa-Parlamentet og Rådet.

6. De deleforpligtelser, der er fastsat i denne artikel, omfatter ikke:

   a) EUCI

b) oplysninger, hvis videre udbredelse er blevet udelukket ved hjælp af en synlig mærkning, medmindre det udtrykkeligt er tilladt at dele dem med CERT-EU.

Artikel 21

Rapporteringsforpligtelser

1. En hændelse anses for at være væsentlig, hvis:

a) den har forårsaget eller er i stand til at forårsage alvorlige driftsmæssige forstyrrelser i den pågældende EU-enheds funktionsdygtighed eller økonomiske tab for denne

b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

2. EU-enhederne fremsender til CERT-EU:

a) uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse et tidligt varsel, som i givet fald skal angive, at den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en virkning på tværs af enheder eller en grænseoverskridende virkning

b) uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse, en hændelsesunderretning, som i givet fald skal ajourføre de i litra a) omhandlede oplysninger og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og virkning samt kompromitteringsindikatorerne, hvor sådanne foreligger

c) på CERT-EU's anmodning en foreløbig rapport om relevante statusopdateringer

d) en endelig rapport senest en måned efter forelæggelsen af den i litra b) omhandlede hændelsesunderretning, som skal omfatte følgende:

   i) en detaljeret beskrivelse af hændelsen, herunder dens alvor og virkning

   ii) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen

   iii) anvendte og igangværende afbødende foranstaltninger

   iv) hvor det er relevant, virkninger på tværs af enheder eller grænseoverskridende virkninger af hændelsen

e) hvis en hændelse stadig pågår på tidspunktet for indgivelsen af den i litra d) omhandlede endelige rapport, en statusrapport på dette tidspunkt og en endelig rapport senest en måned efter deres håndtering af hændelsen.

3. En EU-enhed underretter uden unødigt ophold og under alle omstændigheder senest 24 timer efter at have fået kendskab til en væsentlig hændelse alle relevante medlemsstatsmodparter, jf. artikel 17, stk. 1, i den medlemsstat, hvor den befinder sig, om, at der er indtruffet en væsentlig hændelse.

4. EU-enhederne meddeler bl.a. alle oplysninger, der gør det muligt for CERT-EU at fastslå eventuelle virkninger på tværs af enheder, virkninger for værtsmedlemsstaten eller grænseoverskridende virkninger efter en væsentlig hændelse. Med forbehold af artikel 12 medfører underretningen i sig selv ikke øget ansvar for den underrettende EU-enhed.

5. Hvor det er relevant, kommunikerer EU-enhederne uden unødigt ophold med brugerne af de påvirkede net- og informationssystemer eller af andre komponenter i IKT-miljøet, som potentielt kan blive påvirket af en væsentlig hændelse eller en væsentlig cybertrussel, og som, hvor det er relevant, er nødt til at træffe afbødende foranstaltninger, om alle foranstaltninger eller modforholdsregler, de kan træffe som reaktion på den pågældende hændelse eller trussel. Hvor det er relevant, informerer EU-enhederne disse brugere om selve den væsentlige cybertrussel.

6. Hvis en væsentlig hændelse eller en væsentlig cybertrussel påvirker et net- og informationssystem eller en komponent i en EU-enheds IKT-miljø, som man ved er forbundet med en anden EU-enheds IKT-miljø, udsteder CERT-EU en relevant cybersikkerhedsadvarsel.

7. EU-enhederne giver på CERT-EU's anmodning og uden unødigt ophold CERT-EU digitale oplysninger, der er skabt ved brug af elektroniske enheder, som har været involveret i deres respektive hændelser. CERT-EU kan præcisere yderligere, hvilken type digitale oplysninger det har brug for med henblik på situationsbevidsthed og reaktion på hændelser.

8. CERT-EU forelægger hver tredje måned IICB, ENISA, EU INTCEN og CSIRT-netværket en sammenfattende rapport, herunder anonymiserede og aggregerede data om væsentlige hændelser, hændelser, cybertrusler, nærvedhændelser og sårbarheder i henhold til artikel 20 og væsentlige hændelser, der er indberettet i henhold til nærværende artikels stk. 2. Den sammenfattende rapport udgør et input til den rapport, der kommer hvert andet år, om cybersikkerhedssituationen i Unionen, som vedtages i henhold til artikel 18 i direktiv (EU) 2022/2555.

9. IICB udsteder senest den … [6 måneder fra datoen for denne forordnings ikrafttræden] retningslinjer eller henstillinger med en nærmere præcisering af ordningen og formatet for samt indholdet af rapporteringen i henhold til denne artikel. Ved udarbejdelsen af sådanne retningslinjer eller henstillinger tager IICB hensyn til eventuelle gennemførelsesretsakter vedtaget i henhold til artikel 23, stk. 11, i direktiv (EU) 2022/2555, der præciserer typen af oplysninger, formatet og proceduren for underretninger. CERT-EU formidler de relevante tekniske detaljer om cybertrusler for at gøre det muligt for EU-enhederne at foretage proaktiv opdagelse, reagere på hændelser eller træffe afhjælpende foranstaltninger.

10. Rapporteringsforpligtelserne, der er fastsat i denne artikel, gælder ikke:

a) EUCI

b) oplysninger, hvis videre udbredelse er blevet udelukket ved en synlig mærkning, medmindre det udtrykkeligt er tilladt at dele dem med CERT-EU.

Artikel 22

Koordinering af og samarbejde om reaktionen på hændelser

1. I sin funktion som knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og for koordinering af reaktionen på hændelser fremmer CERT-EU udvekslingen af oplysninger om hændelser, cybertrusler, sårbarheder og nærvedhændelser mellem:

a) EU-enheder

b) de i artikel 17 og 18 omhandlede modparter.

2. CERT-EU fremmer, hvor det er relevant i tæt samarbejde med ENISA, koordineringen mellem EU-enheder af reaktioner på hændelser, herunder:

a) bidrag til konsekvent ekstern kommunikation

b) gensidig støtte såsom udveksling af oplysninger, der er relevante for EU-enheder, eller ydelse af bistand direkte på stedet, hvor det er relevant

c) optimal udnyttelse af operationelle ressourcer

d) koordineringen med andre krisereaktionsmekanismer på EU-plan.

3. CERT-EU støtter, i tæt samarbejde med ENISA, EU-enhederne i relation til situationsbevidsthed i forbindelse med hændelser, cybertrusler, sårbarheder og nærvedhændelser og deler oplysninger om den seneste udvikling inden for cybersikkerhed.

4. IICB vedtager senest den … [12 måneder fra datoen for denne forordnings ikrafttræden] på grundlag af et forslag fra CERT-EU retningslinjer eller henstillinger om koordinering af reaktionen på hændelser og samarbejde om væsentlige hændelser. Hvis hændelsen mistænkes for at være af strafferetlig karakter, rådgiver CERT-EU også om, hvordan de retshåndhævende myndigheder underrettes om hændelsen, uden unødigt ophold.

5. Efter en specifik anmodning fra en medlemsstat og med de berørte EU-enheders godkendelse kan CERT-EU indkalde eksperter fra den liste, der er omhandlet i artikel 23, stk. 4, med henblik på at bidrage til reaktionen på en større hændelse, som har en virkning i den pågældende medlemsstat, eller en omfattende cybersikkerhedshændelse i overensstemmelse med artikel 15, stk. 3, litra g), i direktiv (EU) 2022/2555. Specifikke regler for adgangen til og brugen af tekniske eksperter fra EU-enheder skal godkendes af IICB på grundlag af et forslag fra CERT-EU.

Artikel 23

Håndtering af større hændelser

1. For på operationelt plan at støtte den koordinerede håndtering af større hændelser, der påvirker EU-enheder, og bidrage til regelmæssig udveksling af relevante oplysninger mellem EU-enheder og med medlemsstaterne udarbejder IICB i henhold til artikel 11, litra q), en cyberkrisestyringsplan baseret på de aktiviteter, der er omhandlet i artikel 22, stk. 2, i tæt samarbejde med CERT-EU og ENISA. Cyberkrisestyringsplanen skal mindst indeholde følgende elementer:

   a) ordninger for koordinering og informationsstrømme mellem EU-enhederne med henblik på håndtering af større hændelser på operationelt plan

   b) fælles operative standardprocedurer (SOP)

   c) en fælles taksonomi for alvorsgraden af større hændelser og kriseudløsende faktorer

   d) regelmæssige øvelser

   e) sikre kommunikationskanaler, der skal anvendes.

2. Kommissionens repræsentant i IICB er med forbehold af den cyberkrisestyringsplan, der er udarbejdet i henhold til denne artikels stk. 1, og uden at det berører artikel 16, stk. 2, første afsnit, i direktiv (EU) 2022/2555, kontaktpunktet for udveksling af relevante oplysninger i relation til større hændelser med EU-CyCLONe.

3. CERT-EU koordinerer håndteringen af større hændelser mellem EU-enhederne. CERT-EU fører en fortegnelse over disponibel teknisk ekspertise, der vil være brug for i forbindelse med reaktionen på større hændelser, og bistår IICB med at koordinere EU-enhedernes cyberkrisehåndteringsplaner for større hændelser, jf. artikel 9, stk. 2.

4. EU-enhederne bidrager til denne fortegnelse over teknisk ekspertise i form af en årlig ajourført liste over eksperter, der er til rådighed i deres respektive enheder, inkl. detaljerede beskrivelser af deres specifikke tekniske færdigheder.

Kapitel VI
Afsluttende bestemmelser

Artikel 24

Indledende budgetomfordeling

For at sikre, at CERT-EU fungerer korrekt og stabilt, kan Kommissionen foreslå en omfordeling af personale og finansielle ressourcer til Kommissionens budget til brug for CERT-EU's operationer. Omfordelingen træder i kraft samtidig med det første årlige EU-budget, der vedtages efter denne forordnings ikrafttræden.

Artikel 25

Evaluering

1. Senest den … [12 måneder fra datoen for denne forordnings ikrafttræden] og derefter hvert år rapporterer IICB med bistand fra CERT-EU til Kommissionen om gennemførelsen af denne forordning. IICB kan henstille til Kommissionen at evaluere denne forordning.

2. Senest den … [36 måneder fra datoen for denne forordnings ikrafttræden] og derefter hvert andet år foretager Kommissionen en vurdering og rapporterer til Europa-Parlamentet og Rådet om gennemførelsen af denne forordning og om de indhøstede erfaringer på strategisk og operationelt plan.

Den rapport, der er omhandlet i dette stykkes første afsnit, indeholder gennemgangen, jf. artikel 16, stk. 1, af muligheden for at oprette CERT-EU som et EU-kontor.

3. Senest den … [fem år fra datoen for denne forordnings ikrafttræden] evaluerer Kommissionen denne forordnings funktion og forelægger en rapport for Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget. Kommissionen vurderer også, om det er hensigtsmæssigt at medtage net- og informationssystemer, der håndterer EUCI, i denne forordnings anvendelsesområde, under hensyntagen til andre EU-retsakter, der finder anvendelse på disse systemer. Rapporten ledsages om nødvendigt af et lovgivningsmæssigt forslag.

Artikel 26

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Strasbourg, den …

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*