EUROPEISKA UNIONEN

EUROPAPARLAMENTET **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

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM ÅTGÄRDER FÖR EN HÖG GEMENSAM CYBERSÄKERHETSNIVÅ VID UNIONENS INSTITUTIONER, ORGAN OCH BYRÅER

EUROPAPARLAMENTETS OCH RÅDETS
FÖRORDNING (EU, Euratom) 2023/…

av den 13 december 2023

om åtgärder för en hög gemensam cybersäkerhetsnivå
vid unionens institutioner,
organ och byråer

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 298,

med beaktande av fördraget om upprättandet av Europeiska atomenergigemenskapen, särskilt artikel 106a,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

i enlighet med det ordinarie lagstiftningsförfarandet[1], och

[1] Europaparlamentets ståndpunkt av den 21 november 2023 (ännu ej offentliggjord i EUT) och rådets beslut av den 8 december 2023.

av följande skäl:

(1) I den digitala tidsåldern är informations- och kommunikationsteknik en hörnsten i en öppen, effektiv och oberoende europeisk förvaltning. Ny teknik och de digitala systemens ökade komplexitet och sammankopplingar förstärker cybersäkerhetsriskerna och gör unionens entiteter mer sårbara för cyberhot och incidenter, vilket utgör ett hot mot deras driftskontinuitet och kapacitet att säkra sina data. Ökad användning av molntjänster, allmänt utbredd användning av informations- och kommunikationsteknik (IKT), en hög digitaliseringsnivå, distansarbete och framväxande teknik och konnektivitet är centrala inslag i all verksamhet inom unionens entiteter, men den digitala resiliensen är ännu inte tillräckligt inbyggd.

(2) Unionens entiteter konfronteras med en cyberbild i ständig utveckling. Hotaktörernas taktik, metoder och förfaranden utvecklas hela tiden, samtidigt som de främsta motiven bakom angrepp förändras föga, från att stjäla värdefull icke-offentlig information till att tjäna pengar, manipulera den allmänna opinionen eller undergräva digital infrastruktur. Hotaktörerna utför sina cyberangrepp i en allt snabbare takt med alltmer sofistikerade och automatiserade kampanjer, riktar in sig på exponerade attackytor som bara blir större och är snabba att utnyttja sårbarheter.

(3) Unionens entiteter har sammankopplade IKT-miljöer och integrerade dataflöden, och deras användare har ett nära samarbete. Denna sammankoppling innebär att alla störningar, även om de inledningsvis endast berör en enda unionsentitet, kan få större kaskadeffekter med långtgående och långvariga negativa konsekvenser för unionens andra entiteter. Dessutom är vissa unionsentiteters IKT-miljöer sammankopplade med medlemsstaternas IKT-miljöer, så att en incident hos en unionsentitet kan utgöra en cybersäkerhetsrisk för medlemsstaternas IKT-miljöer och vice versa. Ett utbyte av incidentspecifik information kan underlätta upptäckt av liknande cyberhot eller incidenter som berör medlemsstaterna.

(4) Unionens entiteter är attraktiva mål som konfronteras med mycket avancerade och resursstarka hotaktörer, liksom även andra hot. Samtidigt varierar cyberresiliensens nivå och mognad och förmågan att upptäcka och hantera skadlig cyberverksamhet avsevärt mellan dessa entiteter. För att unionens entiteter ska fungera är det därför nödvändigt att de uppnår en hög gemensam cybersäkerhetsnivå genom tillämpning av cybersäkerhetsåtgärder som står i proportion till de cybersäkerhetsrisker som identifierats, samt informationsutbyte och samarbete.

(5) Europaparlamentets och rådets direktiv (EU) 2022/2555[1] syftar till att ytterligare förbättra cyberresiliensen och incidenthanteringskapaciteten hos offentliga och privata entiteter, behöriga myndigheter och organ samt unionen som helhet. Det är därför nödvändigt att säkerställa att unionens entiteter följer detta genom att föreskriva regler som är förenliga med direktiv (EU) 2022/2555 och som återspeglar dess ambitionsnivå.

(6) För att uppnå en hög gemensam cybersäkerhetsnivå är det nödvändigt att varje unionsentitet inrättar en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker (ramen) som säkerställer en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker och tar hänsyn till driftskontinuitet och krishantering. Ramen bör fastställa strategier på cybersäkerhetsområdet, inbegripet mål och prioriteringar för säkerheten i nätverks- och informationssystemen som omfattar hela den icke-säkerhetsskyddsklassificerade IKT-miljön. Ramen bör bygga på en allriskstrategi som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en unionsentitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, äktheten, integriteten eller konfidentialiteten hos uppgifter som lagras, överförs, behandlas eller är tillgängliga via nätverks- och informationssystem.

---

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

(7) För att hantera de cybersäkerhetsrisker som identifierats inom ramen bör varje unionsentitet vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder. Dessa åtgärder bör omfatta de områden och riskhanteringsåtgärder för cybersäkerhet som föreskrivs i denna förordning för att stärka varje unionsentitets cybersäkerhet.

(8) De tillgångar och cybersäkerhetsrisker som identifierats inom ramen samt slutsatserna från regelbundna mognadsbedömningar av cybersäkerheten bör återspeglas i en cybersäkerhetsplan som upprättas av varje unionsentitet. Cybersäkerhetsplanen bör omfatta de antagna riskhanteringsåtgärderna för cybersäkerhet.

(9) Säkerställandet av cybersäkerhet är en kontinuerlig process, och således bör lämpligheten och ändamålsenligheten i de åtgärder som vidtas i enlighet med denna förordning regelbundet ses över mot bakgrund av de föränderliga cybersäkerhetsriskerna, tillgångarna och unionsentiteternas mognad i fråga om cybersäkerhet. Ramen bör ses över med jämna mellanrum och åtminstone vart fjärde år, medan cybersäkerhetsplanen bör ses över vartannat år, eller mer frekvent vid behov enligt mognadsbedömningarna av cybersäkerheten eller en betydande översyn av ramen.

(10) De riskhanteringsåtgärder för cybersäkerhet som införs av unionens entiteter bör omfatta strategier som, när så är möjligt, syftar till att göra källkoden transparent, med beaktande av skyddsåtgärder för tredje parters eller unionsentiteters rättigheter. Dessa strategier bör stå i proportion till cybersäkerhetsrisken och vara avsedda att underlätta analysen av cyberhot, men inte medföra skyldigheter att offentliggöra eller en rätt att få tillgång till tredjepartskoden utöver de tillämpliga avtalsvillkoren.

(11) Cybersäkerhetsverktyg och applikationer med öppen källkod kan bidra till en högre grad av öppenhet. Öppna standarder främjar interoperabilitet mellan säkerhetsverktyg, vilket gynnar säkerheten för berörda parter. Cybersäkerhetsverktyg och applikationer med öppen källkod kan dra nytta av utvecklargemenskapen i stort och möjliggöra diversifiering av leverantörer. Öppen källkod kan leda till en mer transparent verifieringsprocess för cybersäkerhetsrelaterade verktyg och till en gemenskapsdriven process för att upptäcka sårbarheter. Unionens entiteter bör därför kunna främja användningen av programvara med öppen källkod och öppna standarder genom att satsa på strategier för användning av öppna data och öppen källkod som ett led i säkerhet genom transparens.

(12) Skillnaderna mellan unionens entiteter kräver flexibilitet i genomförandet av denna förordning. De åtgärder för en hög gemensam cybersäkerhetsnivå som föreskrivs i denna förordning bör inte omfatta några skyldigheter som direkt inkräktar på unionsentiteternas utövande av sitt uppdrag eller deras institutionella autonomi. Därför bör dessa entiteter fastställa sina egna ramar och anta sina egna riskhanteringsåtgärder för cybersäkerhet och cybersäkerhetsplaner. Vid genomförandet av sådana åtgärder bör vederbörlig hänsyn tas till befintliga synergier mellan unionens entiteter så att resurserna hanteras på ett korrekt sätt och kostnader optimeras. Det bör också vederbörligen beaktas att åtgärderna inte på ett negativt sätt inverkar på effektivt informationsutbyte och samarbete mellan unionsentiteter och mellan unionsentiteter och motparter i medlemsstaterna.

(13) För att optimera användningen av resurser bör denna förordning ge två eller flera unionsentiteter med liknande strukturer möjlighet att samarbeta när mognadsbedömningar av cybersäkerheten för deras respektive entiteter görs.

(14) För att inte ålägga unionens entiteter oproportionella finansiella och administrativa bördor bör riskhanteringskraven för cybersäkerhet stå i proportion till cybersäkerhetsrisken för de berörda nätverks- och informationssystemen, med beaktande av den senaste utvecklingen i fråga om sådana åtgärder. Varje unionsentitet bör sträva efter att anslå en tillräcklig procentandel av sin IKT-budget för att förbättra sin cybersäkerhetsnivå. På längre sikt bör man eftersträva ett vägledande mål i en storleksordning på minst 10 %. Mognadsbedömningen av cybersäkerheten bör också utvärdera huruvida unionsentitetens cybersäkerhetsutgifter står i proportion till de cybersäkerhetsrisker som entiteten utsätts för. Utan att det påverkar tillämpningen av bestämmelserna om unionens årliga budget enligt fördragen bör kommissionen i sitt förslag till den första årliga budget som ska antas efter denna förordnings ikraftträdande ta hänsyn till de skyldigheter som följer av denna förordning när den bedömer unionsentiteternas budget- och personalbehov enligt deras utgiftsberäkningar.

(15) En hög gemensam cybersäkerhetsnivå kräver att cybersäkerheten övervakas av den högsta ledningsnivån för varje unionsentitet. Unionsentitetens högsta ledningsnivå bör ansvara för genomförandet av denna förordning, bland annat att inrätta ramen, vidta riskhanteringsåtgärder för cybersäkerhet och godkänna cybersäkerhetsplanen. Att etablera en cybersäkerhetskultur, dvs. dagliga cybersäkerhetsrutiner, är en viktig del av ramen och tillhörande riskhanteringsåtgärder för cybersäkerhet vid alla unionens entiteter.

(16) Säkerheten i de nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter är av avgörande betydelse. Unionsentiteter som hanterar säkerhetsskyddsklassificerade EU-uppgifter är skyldiga att tillämpa de övergripande regelverk som finns för att skydda sådana uppgifter, inbegripet särskild styrning, strategier och riskhanteringsförfaranden. Nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter måste uppfylla strängare säkerhetsstandarder än icke-säkerhetsskyddsklassificerade nätverks- och informationssystem. Därför är nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter mer motståndskraftiga mot cyberhot och incidenter. Följaktligen bör denna förordning, samtidigt som den erkänner behovet av en gemensam ram i detta avseende, inte tillämpas på nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter. Om en unionsentitet uttryckligen begär detta bör dock incidenthanteringsorganisationen för EU:s institutioner, organ och byråer (CERT-EU) kunna bistå den unionsentiteten när det gäller incidenter i säkerhetsskyddsklassificerade IKT-miljöer.

(17) Unionens entiteter bör bedöma cybersäkerhetsrisker som rör förbindelser med leverantörer och tjänsteleverantörer, inbegripet leverantörer av datalagrings- och databehandlingstjänster eller hanterade säkerhetstjänster, och vidta lämpliga åtgärder för att hantera dem. Cybersäkerhetsåtgärderna bör specificeras ytterligare i vägledningar eller rekommendationer som utfärdas av CERT-EU. Vid fastställandet av åtgärder och riktlinjer bör vederbörlig hänsyn tas till den senaste utvecklingen och, i förekommande fall, relevanta europeiska och internationella standarder samt relevant unionsrätt och unionspolitik, inbegripet riskbedömningar av cybersäkerhet och rekommendationer som utfärdats av den samarbetsgrupp som inrättats i enlighet med artikel 14 i direktiv (EU) 2022/2555, såsom EU:s samordnade riskbedömning och EU:s verktygslåda för 5G-cybersäkerhet. Med beaktande av cyberhotbilden och vikten av att bygga upp cyberresiliens för unionens entiteter kan dessutom certifiering av relevanta IKT-produkter, IKT-tjänster och IKT-processer krävas enligt särskilda europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i Europaparlamentets och rådets förordning (EU) 2019/881[1].

[1] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

(18) I maj 2011 beslutade generalsekreterarna för unionens institutioner och organ att inrätta en förkonfigurationsgrupp för CERT-EU, som övervakas av en interinstitutionell styrelse. I juli 2012 bekräftade generalsekreterarna de praktiska arrangemangen och enades om att behålla CERT-EU som en permanent entitet för att fortsätta att förbättra den övergripande it-säkerheten vid unionens institutioner, organ och byråer som ett exempel på synligt interinstitutionellt samarbete inom cybersäkerhet. I september 2012 inrättades CERT-EU som en kommissionsarbetsgrupp med ett interinstitutionellt mandat. I december 2017 ingick unionens institutioner och organ ett interinstitutionellt avtal om organisationen och driften av CERT-EU[1]. Denna förordning bör fastställa en omfattande uppsättning regler för organisationen, funktionssättet och driften av CERT-EU. Bestämmelserna i denna förordning har företräde framför bestämmelserna i det interinstitutionella avtalet om organisationen och driften av CERT-EU som ingicks i december 2017.

(19) CERT-EU:s namn bör ändras till cybersäkerhetstjänsten för unionens institutioner, organ och byråer, men kortnamnet CERT-EU bör behållas eftersom det är inarbetat.

---

1 Avtal mellan Europaparlamentet, Europeiska rådet, Europeiska unionens råd, Europeiska kommissionen, Europeiska unionens domstol, Europeiska centralbanken, Europeiska revisionsrätten, Europeiska utrikestjänsten, Europeiska ekonomiska och sociala kommittén, Europeiska regionkommittén och Europeiska investeringsbanken om organiseringen och driften av incidenthanteringsorganisationen för unionens institutioner och byråer (CERT-EU) (EUT C 12, 13.1.2018, s. 1).

(20) Utöver att ge CERT-EU fler uppgifter och en utökad roll inrättas genom denna förordning interinstitutionella cybersäkerhetsstyrelsen (IICB), i syfte att främja en hög gemensam cybersäkerhetsnivå vid unionens entiteter. IICB bör ha en exklusiv roll när det gäller att övervaka och stödja unionsentiteternas genomförande av denna förordning och när det gäller att övervaka CERT-EU:s genomförande av allmänna prioriteringar och mål samt att tillhandahålla strategisk ledning för CERT-EU. IICB bör därför säkerställa att unionens institutioner företräds och bör inkludera företrädare för unionens organ och byråer genom EU-byråernas nätverk (EUAN). Organisationen och driften av IICB bör regleras ytterligare med hjälp av en intern arbetsordning som får innehålla närmare bestämmelser om IICB:s regelbundna möten, inbegripet årliga sammankomster på politisk nivå där företrädare för den högsta ledningsnivån för varje medlem i IICB skulle göra det möjligt för IICB att föra strategiska diskussioner och få strategisk vägledning. IICB bör också kunna inrätta en verkställande kommitté som bistår den i dess arbete och kunna delegera vissa av sina arbetsuppgifter och befogenheter till denna kommitté, i synnerhet arbetsuppgifter som kräver särskild kompetens av sina medlemmar, som t. ex. godkännande av tjänstekatalogen och eventuella senare uppdateringar av den, arrangemang för servicenivåavtal, bedömningar av dokument och rapporter som unionens entiteter lämnat till IICB enligt denna förordning eller arbetsuppgifter som rör utarbetande av beslut om efterlevnadsåtgärder som utfärdats av IICB och övervakning av deras genomförande. IICB bör fastställa den verkställande kommitténs arbetsordning, inbegripet dess arbetsuppgifter och befogenheter.

(21) IICB syftar till att hjälpa unionens entiteter att höja sin cybersäkerhetsstatus genom genomförandet av denna förordning. För att stödja unionens entiteter bör IICB ge vägledning till CERT-EU:s chef, anta en flerårig strategi för att höja cybersäkerhetsnivån i unionens entiteter, fastställa metoden för och andra aspekter av frivilliga inbördes utvärderingar och underlätta inrättandet av en informell grupp av lokala cybersäkerhetsansvariga, med stöd av Europeiska unionens cybersäkerhetsbyrå (Enisa), i syfte att utbyta bästa praxis och information i samband med genomförandet av denna förordning.

(22) För att uppnå en hög cybersäkerhetsnivå i alla unionens entiteter bör intressena hos de unionsorgan och unionsbyråer som driver sin egen IKT-miljö vara företrädda i IICB av tre företrädare som utsetts av EUAN. Säkerheten vid behandling av personuppgifter, och därmed även cybersäkerheten, är en hörnsten i dataskyddet. Mot bakgrund av synergierna mellan dataskydd och cybersäkerhet bör Europeiska datatillsynsmannen vara företrädd i IICB i egenskap av unionsentitet som omfattas av denna förordning, med särskild sakkunskap på dataskyddsområdet, inbegripet säkerhet i elektroniska kommunikationsnät. Med tanke på vikten av innovation och konkurrenskraft inom cybersäkerhet bör Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning vara representerat i IICB. Med tanke på Enisas roll som kompetenscentrum för cybersäkerhet och det stöd som Enisa tillhandahåller, och med tanke på vikten av cybersäkerhet i unionens rymdinfrastruktur och rymdtjänster, bör Enisa och Europeiska unionens rymdprogrambyrå vara företrädda i IICB. Mot bakgrund av den roll som CERT-EU tilldelas enligt denna förordning bör CERT-EU:s chef bjudas in av IICB:s ordförande till alla IICB:s möten, utom när IICB diskuterar frågor som direkt rör CERT-EU:s chef.

(23) IICB bör övervaka efterlevnaden av denna förordning samt genomförandet av vägledningar och rekommendationer och uppmaningar till åtgärder. IICB bör i tekniska frågor stödjas av tekniska rådgivande grupper, i en sammansättning som IICB anser lämplig. Dessa tekniska rådgivande grupper bör arbeta i nära samarbete med CERT-EU, unionens entiteter och andra intressenter i enlighet med vad som är lämpligt.

(24) Om IICB konstaterar att en unionsentitet inte har genomfört denna förordning på effektivt sätt eller de vägledningar, rekommendationer eller uppmaningar till åtgärder i enlighet därmed, bör IICB kunna, utan att det påverkar de interna förfarandena för den berörda unionsentiteten, vidta efterlevnadsåtgärder. IICB bör tillämpa efterlevnadsåtgärder successivt. Med andra ord bör IICB först anta den minst ingripande åtgärden, nämligen ett motiverat yttrande och endast, vid behov, allt strängare åtgärder som kulminerar i den allra strängaste åtgärden, nämligen en rekommendation om ett tillfälligt stopp för dataflödena till den berörda unionsentiteten. En sådan rekommendation bör endast tillämpas i undantagsfall om den berörda unionsentiteten gör sig skyldig till långvariga, avsiktliga, återkommande eller allvarliga överträdelser av denna förordning.

(25) Det motiverade yttrandet utgör den minst ingripande efterlevnadsåtgärden och åtgärdar konstaterade brister i genomförandet av denna förordning. IICB bör kunna följa upp ett motiverat yttrande med vägledning för att hjälpa unionsentiteten att säkerställa att dess ram, riskhanteringsåtgärder för cybersäkerhet, cybersäkerhetsplan och rapportering är förenliga med denna förordning, och därefter genom en varning för att åtgärda identifierade brister hos unionsentiteten inom en angiven period. Om de brister som identifierats i varningen inte har åtgärdats i tillräcklig utsträckning bör IICB kunna utfärda ett motiverat meddelande.

(26) IICB bör också kunna rekommendera att en revision av en unionsentitet utförs. Unionsentiteten bör kunna använda sin interna revisionsfunktion i detta syfte. IICB bör också kunna begära att en revision utförs av en tredjeparts revisionstjänst, t. ex. en ömsesidigt överenskommen tjänsteleverantör från den privata sektorn.

(27) Som en sista utväg bör IICB i undantagsfall, om en unionsentitets överträdelse av denna förordning varit långvarig, avsiktlig, allvarlig eller upprepats, kunna rekommendera alla medlemsstater och unionsentiteter att införa ett tillfälligt stopp för dataflöden till unionsentiteten, som bör gälla till dess att unionsentiteten har upphört med överträdelsen. En sådan rekommendation bör meddelas med hjälp av lämpliga och säkra kommunikationskanaler.

(28) För att säkerställa ett korrekt genomförande av denna förordning bör IICB, om den anser att en unionsentitets ihållande överträdelse av denna förordning har orsakats direkt av en av dess anställdas handlingar eller försummelser, även på högsta ledningsnivå, begära att den berörda unionsentiteten vidtar lämpliga åtgärder, bland annat begära att den överväger disciplinära åtgärder, i enlighet med de regler och förfaranden som fastställs i tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i unionen, som fastställs i rådets förordning (EEG, Euratom, EKSG) nr 259/68[1] (*tjänsteföreskrifterna*) och andra tillämpliga regler och förfaranden.

(29) CERT-EU bör bidra till säkerheten i IKT-miljön för alla unionens entiteter. När CERT-EU överväger huruvida man ska ge teknisk rådgivning eller yttra sig om relevanta politiska frågor på begäran av en unionsentitet bör CERT-EU säkerställa att detta inte utgör något hinder för att utföra de övriga uppgifter som det tilldelats enligt denna förordning. CERT-EU bör agera för unionsentiteternas räkning och fungera som motsvarighet till den samordnare som utsetts för samordnad information om sårbarheter i enlighet med artikel 12.1 i direktiv (EU) 2022/2555.

[1] Rådets förordning (EEG, Euratom, EKSG) nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper samt om införande av särskilda tillfälliga åtgärder beträffande kommissionens tjänstemän (EGT L 56, 4.3.1968, s. 1).

(30) CERT-EU bör stödja genomförandet av åtgärder för en hög gemensam cybersäkerhetsnivå med hjälp av förslag till vägledningar och rekommendationer till IICB eller genom att utfärda uppmaningar till åtgärder. Sådana vägledningar och rekommendationer bör godkännas av IICB. Vid behov bör CERT-EU utfärda uppmaningar till åtgärder där man beskriver brådskande säkerhetsåtgärder som unionens entiteter uppmanas att vidta inom en fastställd tidsram. IICB bör ge CERT-EU i uppdrag att utfärda, dra tillbaka eller ändra ett förslag till vägledningar eller till en rekommendation, eller en uppmaning till åtgärder.

(31) CERT-EU bör också fullgöra den roll som föreskrivs i direktiv (EU) 2022/2555 när det gäller samarbete och informationsutbyte med nätverket av enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) som inrättats enligt artikel 15 i det direktivet. I enlighet med kommissionens rekommendation (EU) 2017/1584[1] bör CERT-EU dessutom samarbeta i samband med och samordna en insats med berörda parter. För att bidra till en hög cybersäkerhetsnivå i hela unionen bör CERT-EU utbyta incidentspecifik information med motparter i medlemsstaterna. CERT-EU bör också samarbeta med andra offentliga och privata motparter, även Nordatlantiska fördragsorganisationen, efter förhandsgodkännande från IICB.

---

[1] Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

(32) För att stödja operativ cybersäkerhet bör CERT-EU utnyttja tillgänglig expertis hos Enisa genom strukturerat samarbete i enlighet med förordning (EU) 2019/881. Vid behov bör särskilda arrangemang mellan de båda entiteterna inrättas för att definiera det praktiska genomförandet av detta samarbete och undvika dubbelarbete. CERT-EU bör samarbeta med Enisa när det gäller analys av cyberhot och regelbundet dela med sig av sin hotbildsrapport till Enisa.

(33) CERT-EU bör kunna samarbeta och utbyta information med relevanta cybersäkerhetsgrupper i unionen och dess medlemsstater för att främja operativt samarbete och göra det möjligt för de befintliga nätverken att förverkliga sin fulla potential när det gäller att skydda unionen.

(34) Eftersom CERT-EU:s tjänster och arbetsuppgifter ligger i unionsentiteternas intresse bör varje unionsentitet med IKT-utgifter bidra med en skälig andel till dessa tjänster och arbetsuppgifter. Dessa bidrag påverkar inte budgetautonomin för unionens entiteter.

(35) Många cyberangrepp är en del av bredare kampanjer som inriktas på grupper av unionsentiteter eller intressegrupper som inbegriper unionsentiteter. För att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder och återställning efter incidenter bör unionens entiteter kunna underrätta CERT-EU om incidenter, cyberhot, sårbarheter och tillbud och dela med sig av lämpliga tekniska detaljer som gör det möjligt att upptäcka eller begränsa samt vidta åtgärder mot liknande incidenter, cyberhot, sårbarheter och tillbud i unionens andra entiteter. Enligt samma tillvägagångssätt som i direktiv (EU) 2022/2555 bör unionsentiteter vara skyldiga att lämna en tidig varning till CERT-EU inom 24 timmar efter det att de blir medvetna om en betydande incident. Sådant informationsutbyte bör göra det möjligt för CERT-EU att sprida informationen till andra unionsentiteter samt till lämpliga motparter, för att bidra till att skydda unionens IKT-miljöer och unionsentiteters motparters IKT-miljöer mot liknande incidenter.

(36) I denna förordning fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, en snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för unionsentiteter att söka stöd och, å andra sidan, en ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och som över tid förbättrar cyberresiliensen hos enskilda unionsentiteter och bidrar till att höja deras övergripande cybersäkerhetsstatus. I detta avseende, bör denna förordning innefatta rapportering om incidenter som, på grundval av en första bedömning utförd av den berörda unionsentiteten, skulle kunna orsaka allvarliga driftstörningar i verksamheten för, eller ekonomiska förluster för, den berörda unionsentiteten eller ha en inverkan på andra fysiska eller juridiska personer genom att åsamka materiell eller immateriell skada. Denna första bedömning bör bland annat beakta de nätverks- och informationssystem som berörs, särskilt deras betydelse för unionsentitetens funktionssätt, cyberhotets allvar och tekniska egenskaper, eventuella underliggande sårbarheter som utnyttjas samt unionsentitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken omfattning unionsentitetens funktionssätt påverkas, hur länge en incident pågår eller hur många fysiska eller juridiska personer som berörs kan spela en viktig roll för att fastställa om driftsstörningen är allvarlig.

(37) Eftersom infrastrukturen och nätverks- och informationssystemen i den relevanta unionsentiteten och den medlemsstat där unionsentiteten är belägen, är sammankopplade är det nödvändigt att denna medlemsstat utan oskäligt dröjsmål blir underrättad om en betydande incident inom denna unionsentitet. I detta syfte bör den berörda unionsentiteten informera alla relevanta motparter i medlemsstaterna som utsetts eller inrättats i enlighet med artiklarna 8 och 10 i direktiv (EU) 2022/2555 om förekomsten av en betydande incident som den rapporterar om till CERT-EU. När CERT-EU får kännedom om en betydande incident som inträffar i en medlemsstat bör den underrätta alla relevanta motparter i den medlemsstaten.

(38) En mekanism bör inrättas för att säkerställa informationsutbyte, samordning och samarbete på ett effektivt sätt mellan unionens entiteter vid större incidenter, och rollen och uppgifterna för de unionsentiteter som är inblandade bör tydligt framgå. Kommissionens företrädare i IICB bör, om inte annat följer av cyberkrishanteringsplanen, vara kontaktpunkt för att underlätta IICB:s utbyte av relevant information om större incidenter med Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som ett bidrag till den gemensamma situationsmedvetenheten. Kommissionens företrädare fungerar som kontaktpunkt i IICB, och denna roll bör inte påverka kommissionens separata och tydliga roll i EU-CyCLONe i enlighet med artikel 16.2 i direktiv (EU) 2022/2555.

(39) Europaparlamentets och rådets förordning (EU) 2018/1725[1] tillämpas på all behandling av personuppgifter enligt denna förordning. Personuppgifter kan behandlas i samband med åtgärder som antas inom ramen för hantering av cybersäkerhetsrisker, sårbarhetshantering och incidenthantering, informationsutbyte om incidenter, cyberhot och sårbarheter samt samordning och samarbete vid incidenthantering. Sådana åtgärder kan kräva behandling av vissa kategorier av personuppgifter, såsom IP-adresser, webbadresser (URL), domännamn, e-postadresser, den registrerades organisatoriska roller, tidsstämplar, e-postämnen eller filnamn. Alla åtgärder som vidtas i enlighet med denna förordning bör vara förenliga med ramverket för dataskydd och integritet, och unionens entiteter, CERT-EU och, i förekommande fall, IICB, bör vidta alla relevanta tekniska och organisatoriska skyddsåtgärder för att säkerställa sådan förenlighet på ett ansvarsfullt sätt.

(40) I denna förordning fastställs den rättsliga grunden för unionsentiteternas, CERT-EU:s och, i förekommande fall, IICB:s behandling av personuppgifter för att de ska kunna utföra sina arbetsuppgifter och fullgöra sina skyldigheter enligt denna förordning, i enlighet med artikel 5.1 b i förordning (EU) 2018/1725. CERT-EU får agera som personuppgiftsbiträde eller personuppgiftsansvarig beroende på vilken arbetsuppgift det utför i enlighet med förordning (EU) 2018/1725.

---

[1] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

(41) Det kan i vissa fall vara nödvändigt för unionens entiteter och CERT-EU, för att de ska kunna fullgöra sina skyldigheter enligt denna förordning i syfte att säkerställa en hög cybersäkerhetsnivå, särskilt i samband med sårbarhets- och incidenthantering, att behandla de särskilda kategorier av personuppgifter som avses i artikel 10.1 i förordning (EU) 2018/1725. I denna förordning fastställs den rättsliga grunden för unionsentiteters och CERT-EU:s behandling av särskilda kategorier av personuppgifter i enlighet med artikel 10.2 g i förordning (EU) 2018/1725. Behandlingen av särskilda kategorier av personuppgifter enligt denna förordning bör stå i strikt proportion till det eftersträvade målet. Med förbehåll för de villkor som anges i artikel 10.2 g i den förordningen bör unionens entiteter och CERT-EU endast få behandla sådana uppgifter i den mån som krävs och om det uttryckligen föreskrivs i den här förordningen. När unionens entiteter och CERT-EU behandlar särskilda kategorier av personuppgifter bör de respektera själva kärnan i rätten till dataskydd och föreskriva lämpliga och specifika åtgärder för att skydda de registrerades grundläggande rättigheter och intressen.

(42) I enlighet med artikel 33 i förordning (EU) 2018/1725 bör unionens entiteter och CERT-EU, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter, såsom tillhandahållande av begränsad åtkomsträtt på grundval av behovsenlig behörighet, tillämpning av principerna för verifieringskedja, antagande av spårbarhetskedja, lagring av uppgifter i vila i en kontrollerad och kontrollerbar miljö, standardiserade operativa förfaranden och integritetsbevarande åtgärder såsom pseudonymisering eller kryptering. Dessa åtgärder bör inte genomföras på ett sätt som påverkar incidenthanteringen och bevisens integritet. Om en unionsentitet eller CERT-EU överför personuppgifter som rör en incident, inbegripet särskilda kategorier av personuppgifter, till en motpart eller partner vid tillämpningen av denna förordning bör sådana överföringar vara förenliga med förordning (EU) 2018/1725. Om särskilda kategorier av personuppgifter överförs till en tredje part bör unionens entiteter och CERT-EU säkerställa att den tredje parten tillämpar åtgärder för skydd av personuppgifter på en nivå som motsvarar förordning (EU) 2018/1725.

(43) Personuppgifter som behandlas i enlighet med denna förordning bör endast bevaras så länge som krävs i enlighet med förordning (EU) 2018/1725. Unionens entiteter och, i tillämpliga fall, CERT-EU i egenskap av personuppgiftsansvarig bör fastställa lagringsperioder som är begränsade till vad som krävs för att uppnå de angivna syftena. I synnerhet när det gäller personuppgifter som samlas in för incidenthantering bör unionens entiteter och CERT-EU skilja mellan de personuppgifter som samlas in för upptäckt av ett cyberhot i sina IKT-miljöer för att förhindra en incident och de personuppgifter som samlas in för begränsning och hantering av samt återställning efter en incident. För att upptäcka ett cyberhot är det viktigt att ta hänsyn till den tid då en hotaktör kan förbli oupptäckt i ett system. För begränsning och hantering av, och återställning efter, en incident är det viktigt att överväga om personuppgifterna är nödvändiga för att spåra och hantera en återkommande incident eller en incident av liknande karaktär för vilken ett samband kan påvisas.

(44) Unionsentiteternas och CERT-EU:s hantering av information bör vara förenlig med tillämpliga regler om informationssäkerhet. Införandet av personalsäkerhet som en riskhanteringsåtgärd för cybersäkerhet bör också vara förenligt med tillämpliga regler.

(45) När information utbyts används synliga markeringar för att ange att mottagarna av informationen ska följa begränsningar när de delar den, särskilt på grundval av avtal om konfidentialitet, eller informella avtal om konfidentialitet såsom Traffic Light Protocol eller andra tydliga indikationer från avsändaren. Traffic Light Protocol ska betraktas som ett sätt att tillhandahålla information om eventuella begränsningar när det gäller ytterligare spridning av information. Protokollet används i nästan alla CSIRT-enheter och i vissa centrum för informationsutbyte och analys.

(46) Denna förordning bör utvärderas regelbundet mot bakgrund av framtida förhandlingar om fleråriga budgetramar som gör det möjligt att fatta ytterligare beslut om CERT-EU:s funktionssätt och institutionella roll, däribland ett eventuellt inrättande av CERT-EU som unionsbyrå.

(47) IICB bör, med CERT-EU:s hjälp, se över och utvärdera genomförandet av denna förordning och rapportera sina resultat till kommissionen. På grundval av dessa uppgifter bör kommissionen rapportera till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén. Den rapporten, med bidrag från IICB, bör utvärdera lämpligheten i att inkludera nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter inom ramen för denna förordning, särskilt i avsaknad av regler för informationssäkerhet som är gemensamma för unionens entiteter.

(48) Enligt proportionalitetsprincipen är det nödvändigt och lämpligt, för uppnåendet av det grundläggande målet att uppnå en hög gemensam cybersäkerhetsnivå inom unionens entiteter, att fastställa regler om cybersäkerhet för unionens entiteter. Denna förordning går inte utöver vad som är nödvändigt för att uppnå det eftersträvade målet, i enlighet med artikel 5.4 i fördraget om Europeiska unionen.

(49) Denna förordning återspeglar det faktum att unionens entiteter skiljer sig åt i fråga om storlek och kapacitet, bland annat när det gäller ekonomiska resurser och personalresurser.

(50) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 17 maj 2022[1].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

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

Kapitel I
Allmänna bestämmelser

Artikel 1
Innehåll

I denna förordning fastställs åtgärder som syftar till att uppnå en hög gemensam cybersäkerhetsnivå inom unionsentiteterna med avseende på

a) varje unionsentitets inrättande av en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker enligt artikel 6,

b) riskhantering, rapportering och informationsutbyte på cybersäkerhetsområdet,

c) organisationen av, funktionssättet hos och driften av den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10 samt organisationen av, funktionssättet hos och driften av cybersäkerhetstjänsten för unionens institutioner, organ och byråer (CERT-EU),

d) övervakningen av genomförandet av denna förordning.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på unionens entiteter, på den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10 och på CERT-EU.

2. Denna förordning ska tillämpas utan att det påverkar den institutionella autonomin enligt fördragen.

3. Med undantag för artikel 13.8 är denna förordning inte tillämplig på nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter (EUCI).

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *unionens entiteter*: de unionsinstitutioner, unionsorgan och unionsbyråer som inrättats genom, eller enligt fördraget om Europeiska unionen, fördraget om Europeiska unionens funktionssätt (EUF-fördraget) eller fördraget om upprättandet av Europeiska atomenergigemenskapen.

2. *nätverks- och informationssystem*: ett nätverks- och informationssystem enligt definitionen i artikel 6.1 i direktiv (EU) 2022/2555.

3. *säkerhet i nätverks- och informationssystem*: säkerhet i nätverks- och informationssystem enligt definitionen i artikel 6.2 i direktiv (EU) 2022/2555.

4. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

5. *högsta ledningsnivå*: en chef, ett ledningsorgan eller ett samordnings- och tillsynsorgan med ansvar för en unionsentitets funktionssätt, på den högsta administrativa nivån, med mandat att fatta eller godkänna beslut i linje med styrningsarrangemangen på hög nivå inom den unionsentiteten, utan att det påverkar andra ledningsnivåers formella ansvar för efterlevnad och hantering av cybersäkerhetsrisker inom respektive ansvarsområde.

6. *tillbud*: ett tillbud enligt definitionen i artikel 6.5 i direktiv (EU) 2022/2555.

7. *incident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.

8. *större incident*: en incident som orsakar störningar som är så omfattande att en unionsentitet och CERT-EU inte kan hantera dem eller som har en betydande påverkan på åtminstone två unionsentiteter.

9. *storskalig cybersäkerhetsincident*: en storskalig cybersäkerhetsincident enligt definitionen i artikel 6.7 i direktiv (EU) 2022/2555.

10. *incidenthantering*: incidenthantering enligt definitionen i artikel 6.8 i direktiv (EU) 2022/2555.

11. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

12. *betydande cyberhot*: ett betydande cyberhot enligt definitionen i artikel 6.11 i direktiv (EU) 2022/2555.

13. *sårbarhet*: en sårbarhet enligt definitionen i artikel 6.15 i direktiv (EU) 2022/2555.

14. *cybersäkerhetsrisk*: en risk enligt definitionen i artikel 6.9 i direktiv (EU) 2022/2555.

15. *molntjänst*: en molntjänst enligt definitionen i artikel 6.30 i direktiv (EU) 2022/2555.

Artikel 4

Behandling av personuppgifter

1. Behandlingen av personuppgifter enligt denna förordning som utförs av CERT-EU, den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10 och unionens entiteter ska utföras i enlighet med förordning (EU) 2018/1725.

2. När de utför arbetsuppgifter eller fullgör skyldigheter enligt denna förordning ska CERT-EU, den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10 och unionens entiteter behandla och utbyta personuppgifter endast i den utsträckning som är nödvändig och uteslutande i syfte att utföra dessa arbetsuppgifter eller fullgöra dessa skyldigheter.

3. Den behandling av särskilda kategorier av personuppgifter som avses i artikel 10.1 i förordning (EU) 2018/1725 ska anses vara nödvändig av hänsyn till ett viktigt allmänt intresse enligt artikel 10.2 g i den förordningen. Sådana uppgifter får behandlas endast i den utsträckning som krävs för genomförandet av de riskhanteringsåtgärder för cybersäkerhet som avses i artiklarna 6 och 8, för CERT-EU:s tillhandahållande av tjänster i enlighet med artikel 13, för utbyte av incidentspecifik information enligt artiklarna 17.3 och 18.3, för informationsutbyte enligt artikel 20, för rapporteringsskyldigheter enligt artikel 21, för samordning och samarbete vid incidenthantering enligt artikel 22 och för hantering av större incidenter enligt artikel 23 i denna förordning. Unionens entiteter och CERT-EU ska, när de agerar som personuppgiftsansvariga, tillämpa tekniska åtgärder för att förhindra behandling av särskilda kategorier av personuppgifter för andra ändamål och ska föreskriva lämpliga och specifika åtgärder för att skydda de registrerades grundläggande rättigheter och intressen.

Kapitel II

Åtgärder för en hög gemensam cybersäkerhetsnivå

Artikel 5

Genomförande av åtgärder

1. Senast den … [åtta månader från dagen för denna förordnings ikraftträdande] ska den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10, efter samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa) och efter att ha fått vägledning av CERT-EU, utfärda riktlinjer för unionens entiteter i syfte att genomföra en första översyn av cybersäkerheten och inrätta en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker enligt artikel 6, utföra mognadsbedömningar av cybersäkerheten enligt artikel 7, vidta riskhanteringsåtgärder för cybersäkerhet enligt artikel 8 och anta cybersäkerhetsplanen enligt artikel 9.

2. Vid genomförandet av artiklarna 6–9 ska unionens entiteter beakta de riktlinjer som avses i punkt 1 i den här artikeln samt relevanta riktlinjer och rekommendationer som antagits enligt artiklarna 11 och 14.

Artikel 6

Ram för hantering, styrning och kontroll av cybersäkerhetsrisker

1. Senast den … [15 månader från dagen för denna förordnings ikraftträdande] ska varje unionsentitet, efter att ha genomfört en första översyn av cybersäkerheten, såsom en revision, inrätta en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker (*ramen*). Inrättandet av ramen ska övervakas av och ske under ansvar av unionsentitetens högsta ledningsnivå.

2. Ramen ska omfatta hela den icke-säkerhetsskyddsklassificerade IKT-miljön för unionsentiteten i fråga, inbegripet alla IKT-miljöer på plats, nätverk för operativ teknik, utkontrakterade tillgångar och tjänster i molnbaserade miljöer eller som förvaltas av tredje part, mobila enheter, interna nätverk, företagsnätverk som inte är anslutna till internet och alla enheter som är anslutna till dessa miljöer (IKT-miljön). Ramen ska bygga på en allriskstrategi.

3. Ramen ska säkerställa en hög cybersäkerhetsnivå. Ramen ska fastställa interna strategier för cybersäkerhet, inbegripet mål och prioriteringar, för säkerheten i nätverks- och informationssystem samt roller och ansvarsområden för unionsentitetens personal som har till uppgift att säkerställa ett effektivt genomförande av denna förordning. Ramen ska också innehålla mekanismer för att mäta hur effektivt genomförandet är.

4. Ramen ska ses över regelbundet mot bakgrund av de föränderliga cybersäkerhetsriskerna, och åtminstone vart fjärde år. När så är lämpligt och på begäran från den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10, får ramen för en unionsentitet uppdateras på grundval av vägledning från CERT-EU avseende identifierade incidenter eller eventuella konstaterade brister i genomförandet av denna förordning.

5. Varje unionsentitets högsta ledningsnivå ska ansvara för genomförandet av denna förordning och ska övervaka att dess organisation fullgör sina skyldigheter i fråga om ramen.

6. När så är lämpligt och utan att det påverkar dess ansvar för genomförandet av denna förordning får varje unionsentitets högsta ledningsnivå delegera vissa skyldigheter enligt denna förordning till högre tjänstemän i den mening som avses i artikel 29.2 i tjänsteföreskrifterna eller andra tjänstemän på motsvarande nivå inom den berörda unionsentiteten. Även om dessa skyldigheter delegeras kan den högsta ledningsnivån hållas ansvarig för den berörda unionsentitetens överträdelser av denna förordning.

7. Varje unionsentitet ska ha effektiva mekanismer för att säkerställa att en lämplig andel av IKT-budgeten spenderas på cybersäkerhet. Vid fastställandet av denna andel ska vederbörlig hänsyn tas till ramen.

8. Varje unionsentitet ska utse en lokal cybersäkerhetsansvarig eller motsvarande funktion som ska fungera som dess gemensamma kontaktpunkt för alla aspekter av cybersäkerhet. Den lokala cybersäkerhetsansvariga ska underlätta genomförandet av denna förordning och regelbundet rapportera om genomförandet direkt till den högsta ledningsnivån. Utan att det påverkar den lokala cybersäkerhetsansvarigas funktion som den gemensamma kontaktpunkten i varje unionsentitet får en unionsentitet delegera vissa av den lokala cybersäkerhetsansvarigas arbetsuppgifter när det gäller genomförandet av denna förordning till CERT-EU på grundval av ett servicenivåavtal mellan den unionsentiteten och CERT-EU, eller så får arbetsuppgifterna delas mellan flera unionsentiteter. När dessa arbetsuppgifter delegeras till CERT-EU ska den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10 besluta om huruvida tillhandahållandet av denna tjänst ska ingå i CERT-EU:s baslinjetjänster, med beaktande av den berörda unionsentitetens personalresurser och ekonomiska resurser. Varje unionsentitet ska utan onödigt dröjsmål meddela CERT-EU om utsedda lokala cybersäkerhetsansvariga och alla senare ändringar därav.

CERT-EU ska upprätta och föra en uppdaterad förteckning över utsedda lokala cybersäkerhetsansvariga.

9. Högre tjänstemän i den mening som avses i artikel 29.2 i tjänsteföreskrifterna eller andra tjänstemän på motsvarande nivå i varje unionsentitet samt all relevant personal som har till uppgift att genomföra de riskhanteringsåtgärder och att uppfylla de skyldigheter avseende cybersäkerhet som fastställs i denna förordning, ska regelbundet genomgå särskild utbildning för att få tillräckliga kunskaper och färdigheter så att de kan förstå och bedöma cybersäkerhetsrisker och rutiner för hantering av cybersäkerhet och deras inverkan på unionsentitetens verksamhet.

Artikel 7

Mognadsbedömningar av cybersäkerheten

1. Senast den … [18 månader från dagen för denna förordnings ikraftträdande] och minst vartannat år därefter ska varje unionsentitet utföra en mognadsbedömning av cybersäkerheten omfattande alla delar av dess IKT-miljö.

2. Mognadsbedömningarna av cybersäkerheten ska, när så är lämpligt, utföras med hjälp av en specialiserad tredje part.

3. Unionsentiteter med liknande strukturer får samarbeta vid utförandet av mognadsbedömningar av cybersäkerhet som avser deras respektive entiteter.

4. På grundval av en begäran från den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10, och med uttryckligt samtycke från den berörda unionsentiteten, får resultaten av en mognadsbedömning av cybersäkerheten diskuteras inom styrelsen eller den informella gruppen av lokala cybersäkerhetsansvariga i syfte att dra lärdom av tidigare erfarenheter och utbyta bästa praxis.

Artikel 8

Riskhanteringsåtgärder för cybersäkerhet

1. Utan onödigt dröjsmål och under alla omständigheter senast den … [20 månader från dagen för denna förordnings ikraftträdande] ska varje unionsentitet, under överinseende av den högsta ledningsnivån, vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera de cybersäkerhetsrisker som identifierats inom ramen, och för att förebygga eller minimera effekterna av incidenterna. Med beaktande av den senaste utvecklingen och, i tillämpliga fall, relevanta europeiska och internationella standarder, ska dessa åtgärder säkerställa en säkerhetsnivå för nätverks- och informationssystemen i hela IKT-miljön som står i proportion till cybersäkerhetsriskerna. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till unionsentitetens grad av exponering för cybersäkerhetsrisker, dess storlek samt sannolikheten för att incidenter ska inträffa och deras allvarlighetsgrad, inbegripet deras samhälleliga, ekonomiska och interinstitutionella konsekvenser.

2. Unionens entiteter ska vid genomförandet av riskhanteringsåtgärder för cybersäkerhet behandla åtminstone följande specifika områden:

a) Cybersäkerhetspolicy, inbegripet åtgärder som behövs för att nå målen och prioriteringarna enligt artikel 6 samt punkt 3 i den här artikeln.

b) Strategier för analys av cybersäkerhetsrisker och informationssystemens säkerhet.

c) Policymål för användningen av molntjänster.

d) Cybersäkerhetsrevision, när så är lämpligt, vilket kan inbegripa en bedömning av cybersäkerhetsrisker, sårbarhet och cyberhot, och penetrationstester som regelbundet utförs av en betrodd privat leverantör.

e) Genomförande av rekommendationer från de cybersäkerhetsrevisioner som avses i led d genom cybersäkerhetsuppdateringar och policyuppdateringar.

f) Organisation av cybersäkerhet, inbegripet fastställande av roller och ansvarsområden.

g) Förvaltning av tillgångar, inbegripet inventering av IKT-tillgångar och IKT-nätverkskartografi.

h) Säkerhets- och åtkomstkontroll för personal.

i) Driftssäkerhet.

j) Kommunikationssäkerhet.

k) Förvärv, utveckling och underhåll av system, inbegripet strategier för hantering och redovisning av sårbarheter.

l) Strategier, om möjligt, för insyn i källkoden.

m) Säkerhet i leveranskedjan, inbegripet säkerhetsrelaterade aspekter som rör förbindelserna mellan unionsentiteten och dess direkta leverantörer eller tjänsteleverantörer.

n) Incidenthantering och samarbete med CERT-EU, såsom underhåll av säkerhetsövervakning och loggning.

o) Hantering av driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering samt krishantering.

p) Främjande och utveckling av program för utbildning, kompetens, ökad medvetenhet, övning och fortbildning inom cybersäkerhet.

Vid tillämpningen av första stycket led m ska unionsentiteter ta hänsyn till de sårbarheter som är specifika för varje direkt leverantör och tjänsteleverantör och den övergripande kvaliteten på produkterna och deras leverantörers och tjänsteleverantörers cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling.

3. Unionens entiteter ska vidta åtminstone följande riskhanteringsåtgärder för cybersäkerhet:

a) Tekniska arrangemang för att möjliggöra och upprätthålla distansarbete.

b) Konkreta åtgärder för att närma sig nolltillitsprinciperna.

c) Användning av flerfaktorsautentisering som standard i nätverks- och informationssystem.

d) Användning av kryptografi och kryptering, särskilt totalsträckskryptering samt säkra digitala underskrifter.

e) Om möjligt, säker röst-, video- och textkommunikation samt säkra nödkommunikationssystem inom unionsentiteten.

f) Proaktiva åtgärder för att upptäcka och avlägsna sabotageprogram och spionprogram.

g) Inrättande av säkerhet i leveranskedjan för programvara genom kriterier för utveckling och utvärdering av säker programvara.

h) Upprättande och antagande av utbildningsprogram för cybersäkerhet som motsvarar de föreskrivna arbetsuppgifterna och den förväntade kapaciteten hos den högsta ledningen och personalen inom unionsentiteten med uppdrag att säkerställa ett effektivt genomförande av denna förordning.

i) Regelbunden utbildning i cybersäkerhet för personalen.

j) Om relevant, deltagande i riskanalyser av sammankopplingar mellan unionens entiteter.

k) Förbättrade upphandlingsregler för att underlätta en hög gemensam cybersäkerhetsnivå genom

   i) att undanröja avtalsmässiga hinder som begränsar informationsutbytet från leverantörer av IKT-tjänster om incidenter, sårbarheter och cyberhot med CERT-EU,

   ii) att införa avtalsenliga skyldigheter att rapportera incidenter, sårbarheter och cyberhot samt att ha lämpliga mekanismer för hantering och övervakning av incidenter.

Artikel 9

Cybersäkerhetsplaner

1. Som en uppföljning av slutsatsen från den mognadsbedömning av cybersäkerheten som utförts enligt artikel 7 och med beaktande av de tillgångar och cybersäkerhetsrisker som identifierats i ramen samt de riskhanteringsåtgärder för cybersäkerhet som vidtagits enligt artikel 8, ska varje unionsentitets högsta ledningsnivå godkänna en cybersäkerhetsplan utan onödigt dröjsmål, och under alla omständigheter senaste den … [24 månader från dagen för denna förordnings ikraftträdande]. Cybersäkerhetsplanen ska syfta till att öka unionsentitetens övergripande cybersäkerhet och ska därigenom bidra till att förbättra en hög gemensam cybersäkerhetsnivå inom unionsentiteterna. Cybersäkerhetsplanen ska omfatta åtminstone de riskhanteringsåtgärder för cybersäkerhet som vidtagits enligt artikel 8. Cybersäkerhetsplanen ska ses över vartannat år, eller mer frekvent vid behov, efter de mognadsbedömningar av cybersäkerheten som gjorts enligt artikel 7 eller en annan betydande översyn av ramen.

2. Cybersäkerhetsplanen ska omfatta unionsentitetens cyberkrishanteringsplan för större incidenter.

3. Unionsentiteten ska överlämna sin färdiga cybersäkerhetsplan till den interinstitutionella cybersäkerhetsstyrelse som inrättas enligt artikel 10.

Kapitel III

Interinstitutionell cybersäkerhetsstyrelse

Artikel 10

Interinstitutionell cybersäkerhetsstyrelse

1. Härigenom inrättas en interinstitutionell cybersäkerhetsstyrelse (IICB).

2. IICB ska ansvara för att

   a) övervaka och stödja unionsentiteternas genomförande av denna förordning,

   b) övervaka CERT-EU:s genomförande av de allmänna prioriteringarna och målen och ge CERT-EU strategisk ledning.

3. IICB ska bestå av följande:

   a) En företrädare som utses av var och en av följande:

      i) Europaparlamentet.

      ii) Europeiska rådet.

iii) Europeiska unionens råd.

iv) Kommissionen.

v) Europeiska unionens domstol.

vi) Europeiska centralbanken.

vii) Revisionsrätten.

viii) Europeiska utrikestjänsten.

ix) Europeiska ekonomiska och sociala kommittén.

x) Europeiska regionkommittén.

xi) Europeiska investeringsbanken.

xii) Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning.

xiii) Enisa.

xiv) Europeiska datatillsynsmannen (EDPS).

xv) Europeiska unionens rymdprogrambyrå.

b) Tre andra företrädare än de som avses i led a, som utses av EU-byråernas nätverk (EUAN) på grundval av ett förslag från dess rådgivande IKT-kommitté, att företräda intressena för unionens organ och byråer som driver sin egen IKT-miljö.

De unionsentiteter som är företrädda i IICB ska sträva efter att uppnå en jämn könsfördelning bland de utsedda företrädarna.

4. Ledamöterna i IICB får bistås av en suppleant. Ordföranden får bjuda in andra företrädare för de unionsentiteter som avses i punkt 3 eller för andra unionsentiteter att delta i IICB:s möten utan rösträtt.

5. CERT-EU:s chef och ordförandena för samarbetsgruppen, CSIRT-nätverket och EU-CyCLONe, som inrättats enligt artikel 14, 15 respektive 16 i direktiv (EU) 2022/2555, eller deras suppleanter, får delta som observatörer i IICB:s möten. I undantagsfall får IICB, i enlighet med sin interna arbetsordning, fatta ett annat beslut.

6. IICB ska själv anta sin interna arbetsordning.

7. IICB ska utse en ordförande bland sina ledamöter, i enlighet med sin arbetsordning, för en period på tre år. Ordförandens suppleant ska bli ordinarie ledamot av IICB för samma period.

8. IICB ska sammanträda minst tre gånger om året på ordförandens initiativ, på begäran av CERT-EU eller på begäran av någon av dess ledamöter.

9. Varje ledamot av IICB ska ha en röst. IICB:s beslut ska fattas med enkel majoritet om inte annat föreskrivs i denna förordning. IICB:s ordförande ska inte ha rösträtt utom vid lika röstetal, då ordföranden får avge en utslagsröst.

10. IICB får agera genom ett förenklat skriftligt förfarande som inleds i enlighet med dess interna arbetsordning. Enligt det förfarandet ska det relevanta beslutet anses vara godkänt inom den tidsram som fastställts av ordföranden, utom i de fall då en ledamot har invändningar.

11. IICB:s sekretariat ska tillhandahållas av kommissionen och ska vara ansvarigt inför IICB:s ordförande.

12. De företrädare som utsetts av EUAN ska vidarebefordra IICB:s beslut till EUAN:s medlemmar. Alla EUAN:s medlemmar ska ha rätt att med dessa företrädare eller IICB:s ordförande ta upp alla frågor som de anser att IICB bör uppmärksammas på.

13. IICB får inrätta en verkställande kommitté som ska bistå den i dess arbete och får delegera vissa av sina arbetsuppgifter och befogenheter till den. IICB ska fastställa den verkställande kommitténs arbetsordning, inbegripet dess arbetsuppgifter och befogenheter och dess ledamöters mandatperioder.

14. Senast den … [12 månader från dagen för denna förordnings ikraftträdande] och därefter årligen ska IICB lämna en rapport till Europaparlamentet och rådet med närmare uppgifter om hur genomförandet av denna förordning fortskrider och särskilt om omfattningen av CERT-EU:s samarbete med motparterna i var och en av medlemsstaterna. Rapporten ska utgöra underlag till den tvåårsrapport om cybersäkerhetssituationen i unionen som antas enligt artikel 18 i direktiv (EU) 2022/2555.

Artikel 11

IICB:s arbetsuppgifter

I IICB:s befogenheter ingår följande arbetsuppgifter, särskilt att

a) ge CERT-EU:s chef vägledning,

b) effektivt övervaka och utöva tillsyn över genomförandet av denna förordning och hjälpa unionens entiteter att stärka sin cybersäkerhet, inbegripet, när så är lämpligt, begära ad hoc-rapporter från unionens entiteter och CERT-EU,

c) efter en strategisk diskussion anta en flerårig strategi för att höja cybersäkerhetsnivån i unionens entiteter, utvärdera denna strategi regelbundet och under alla omständigheter vart femte år, och vid behov ändra strategin,

d) fastställa metoder och organisatoriska aspekter för hur unionsentiteternas frivilliga inbördes utvärderingar ska gå till, i syfte att dra nytta av gemensamma erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt förbättra unionsentiteternas cybersäkerhetskapacitet, och säkerställa att sådana inbördes utvärderingar utförs av cybersäkerhetsexperter som utsetts av en annan unionsentitet än den unionsentitet som utvärderas och att metoden grundar sig på artikel 19 i direktiv (EU) 2022/2555 och, i förekommande fall, är anpassad till unionsentiteterna,

e) på grundval av ett förslag från CERT-EU:s chef godkänna CERT-EU:s årliga arbetsprogram och övervaka dess genomförande,

f) på grundval av ett förslag från CERT-EU:s chef godkänna CERT-EU:s tjänstekatalog och eventuella uppdateringar av den,

g) på grundval av ett förslag från CERT-EU:s chef godkänna den årliga ekonomiska planeringen av inkomster och utgifter, inbegripet för personal, för CERT-EU:s verksamhet,

h) på grundval av ett förslag från CERT-EU:s chef godkänna arrangemangen för servicenivåavtal,

i) granska och godkänna den årsrapport som utarbetats av CERT-EU:s chef och som omfattar CERT-EU:s verksamhet och förvaltning av medel,

j) godkänna och övervaka de nyckelprestandaindikatorer som har fastställts för CERT-EU på grundval av ett förslag från CERT-EU:s chef,

k) godkänna samarbetsavtal, servicenivåavtal eller avtal mellan CERT-EU och andra entiteter i enlighet med artikel 18,

l) på grundval av ett förslag från CERT-EU anta vägledningar och rekommendationer i enlighet artikel 14 och ge CERT-EU i uppdrag att utfärda, dra tillbaka eller ändra ett förslag till vägledningar eller rekommendationer, eller en uppmaning till åtgärder,

m) inrätta tekniska rådgivande grupper med särskilda arbetsuppgifter för att bistå IICB i dess arbete, godkänna deras mandat och utse deras respektive ordförande,

n) ta emot och bedöma dokument och rapporter som lämnats in av unionens entiteter enligt denna förordning, såsom mognadsbedömningar av cybersäkerheten,

o) underlätta inrättandet av en informell grupp av lokala cybersäkerhetsansvariga från unionens entiteter, med stöd av Enisa, i syfte att utbyta bästa praxis och information i samband med genomförandet av denna förordning,

p) beakta den information om identifierade cybersäkerhetsrisker och tidigare erfarenheter som tillhandahålls av CERT-EU, övervaka lämpligheten i arrangemangen för sammankoppling mellan unionsentiteternas IKT-miljöer och ge råd om möjliga förbättringar,

q) upprätta en cyberkrishanteringsplan i syfte att på operativ nivå stödja en samordnad hantering av större incidenter som berör unionens entiteter och bidra till ett regelbundet utbyte av relevant information, särskilt när det gäller konsekvenserna av och allvarlighetsgraden hos, och möjliga sätt att begränsa effekterna av, större incidenter,

r) samordna antagandet av enskilda unionsentiteters cyberkrishanteringsplaner enligt artikel 9.2,

s) anta rekommendationer om den säkerhet i leveranskedjan som avses i artikel 8.2, första stycket led m, med beaktande av resultaten av samordnade säkerhetsriskbedömningar på unionsnivå av de kritiska leveranskedjor som avses i artikel 22 i direktiv (EU) 2022/2555 för att stödja unionens entiteter vid antagandet av effektiva och proportionella riskhanteringsåtgärder för cybersäkerhet.

Artikel 12

Kontroll av efterlevnad

1. IICB ska i enligt artikel 10.2 och artikel 11 effektivt övervaka hur unionens entiteter genomför denna förordning och antagna vägledningar, rekommendationer och uppmaningar till åtgärder. IICB får begära den information eller dokumentation som är nödvändig för detta ändamål från unionens entiteter. Vid antagande av efterlevnadsåtgärder enligt denna artikel, om den berörda unionsentiteten är direkt företrädd i IICB, ska denna unionsentitet inte ha rösträtt.

2. Om IICB konstaterar att en unionsentitet inte har genomfört denna förordning på effektivt sätt eller de vägledningar, rekommendationer eller uppmaningar till åtgärder i enlighet därmed får den, utan att det påverkar den berörda unionsentitetens interna förfaranden och efter att den berörda unionsentiteten har fått möjlighet att framföra sina synpunkter:

   a) lämna ett motiverat yttrande till den berörda unionsentiteten med konstaterade brister i genomförandet av denna förordning,

   b) efter samråd med CERT-EU ge vägledningar till den berörda unionsentiteten för att säkerställa att dess ram, riskhanteringsåtgärder för cybersäkerhet, cybersäkerhetsplan och rapportering är i överensstämmelse med denna förordning inom en angiven period,

c) utfärda en varning för att åtgärda konstaterade brister inom en angiven period, inbegripet rekommendationer om ändring av de åtgärder som antagits av den berörda unionsentiteten i enlighet med denna förordning,

d) utfärda ett motiverat meddelande till den berörda unionsentiteten, i händelse av att brister som konstaterats i en varning som utfärdats enligt led c inte åtgärdats i tillräcklig utsträckning inom den angivna perioden,

e) utfärda

i) en rekommendation om att en revision ska utföras, eller

ii) en begäran om att en revision ska utföras av en tredje parts revisionstjänst,

f) informera, i tillämpliga fall och inom ramen för sitt mandat, revisionsrätten om den påstådda bristande efterlevnaden,

g) utfärda en rekommendation om att alla medlemsstater och unionsentiteter inför ett tillfälligt stopp för dataflöden till den berörda unionsentiteten.

Vid tillämpning av första stycket c ska varningens målgrupp begränsas på lämpligt sätt, när så är nödvändigt med tanke på cybersäkerhetsrisken.

Varningar och rekommendationer som utfärdas enligt första stycket ska riktas till den berörda unionsentitetens högsta ledningsnivå.

3. Om IICB har antagit åtgärder enligt punkt 2, första stycket a–g ska den berörda unionsentiteten lämna uppgifter om de åtgärder som vidtagits och insatser som gjorts för att åtgärda de påstådda brister som IICB konstaterat. Unionsentiteten ska lämna in dessa uppgifter inom en rimlig tidsperiod som ska fastställas i överenskommelse med IICB.

4. Om IICB anser att en unionsentitet på ett ihållande sätt överträder denna förordning till direkt följd av handlingar eller försummelser från en tjänsteman eller annan anställd i unionen, inbegripet på högsta ledningsnivå, ska IICB begära att den berörda unionsentiteten vidtar lämpliga åtgärder, bland annat begära att den överväger disciplinära åtgärder i enlighet med de regler och förfaranden som fastställs i tjänsteföreskrifterna och andra tillämpliga regler och förfaranden. För detta ändamål ska IICB överföra nödvändig information till den berörda unionsentiteten.

5. Om unionsentiteter meddelar att de inte kan hålla de tidsfrister som anges i artiklarna 6.1 och 8.1 får IICB i vederbörligen motiverade fall, med beaktande av unionsentitetens storlek, godkänna en förlängning av dessa tidsfrister.

Kapitel IV
CERT-EU

Artikel 13

CERT-EU:s uppdrag och arbetsuppgifter

1. CERT-EU:s uppdrag ska vara att bidra till säkerheten i unionsentiteters icke-säkerhetsskyddsklassificerade IKT-miljö genom att ge dem råd om cybersäkerhet, hjälpa dem att förebygga, upptäcka, hantera, begränsa, bemöta och återställa efter incidenter och genom att fungera som deras nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering.

2. CERT-EU ska samla in, hantera, analysera och dela information med unionens entiteter om cyberhot, sårbarheter och incidenter som rör icke-säkerhetsskyddsklassificerad IKT-infrastruktur. CERT-EU ska samordna hanteringen av incidenter på interinstitutionell nivå och på unionsentitetsnivå, bland annat genom att ombesörja eller samordna tillhandahållandet av specialiserat operativt stöd.

3. CERT-EU ska utföra följande arbetsuppgifter för unionens entiteter:

   a) Stödja dem vid genomförandet av denna förordning och bidra till samordningen av genomförandet av denna förordning genom de åtgärder som förtecknas i artikel 14.1 eller genom ad hoc-rapporter som IICB begär.

b) Erbjuda standardiserade CSIRT-tjänster till unionens entiteter med hjälp av ett paket av cybersäkerhetstjänster som beskrivs i dess tjänstekatalog (baslinjetjänster).

c) Upprätthålla ett nätverk av kollegor och partner för att stödja de tjänster som beskrivs i artiklarna 17 och 18.

d) Uppmärksamma IICB på alla problem som rör genomförandet av denna förordning och genomförandet av vägledningarna, rekommendationerna och uppmaningarna till åtgärder.

e) På grundval av den information som avses i punkt 2 och i nära samarbete med Enisa bidra till unionens cybersituationsmedvetenhet.

f) Samordna hanteringen av större incidenter.

g) Agera för unionsentiteternas räkning som motsvarighet till den samordnare som utsetts för samordnad information om sårbarheter enligt artikel 12.1 i direktiv (EU) 2022/2555.

h) På begäran av en unionsentitet, tillhandahålla proaktiv, icke-inkräktande skanning av den unionsentitetens allmänt tillgängliga nätverks- och informationssystem.

Den information som avses i första stycket e ska delas med IICB, CSIRT-nätverket och Europeiska unionens underrättelse- och lägescentral (EU-Intcen), när så är tillämpligt och lämpligt, och omfattas av lämpliga överenskommelser om konfidentialitet.

4. CERT-EU får i enlighet med artikel 17 eller 18, beroende på vad som är lämpligt, samarbeta med relevanta cybersäkerhetsgrupper inom unionen och dess medlemsstater, bland annat på följande områden:

   a) Beredskap, incidentsamordning, informationsutbyte och krishantering på teknisk nivå i ärenden som rör unionens entiteter.

   b) Operativt samarbete med CSIRT-nätverket, inbegripet om ömsesidigt bistånd.

   c) Underrättelser om cyberhot, inbegripet situationsmedvetenhet.

   d) Vilket ämne som helst som kräver CERT-EU:s tekniska cybersäkerhetsexpertis.

5. Inom sitt befogenhetsområde ska CERT-EU inleda ett strukturerat samarbete med Enisa om kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot i enlighet med förordning (EU) 2019/881. CERT-EU får samarbeta och utbyta information med Europols europeiska it-brottscentrum.

6. CERT-EU får tillhandahålla följande tjänster som inte beskrivs i dess tjänstekatalog (avgiftsbelagda tjänster):

a) Andra tjänster som stöder cybersäkerheten i unionsentiteternas IKT-miljö än dem som avses i punkt 3, på grundval av servicenivåavtal och förutsatt att det finns tillgängliga resurser, särskilt omfattande övervakning av nätverk, även med dygnet-runt-bevakning i första ledet för mycket allvarliga cyberhot.

b) Andra tjänster som stöder unionsentiteternas cybersäkerhetsinsatser eller cybersäkerhetsprojekt än de som skyddar deras IKT-miljö, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

c) Proaktiv skanning, på begäran, av den berörda unionsentitetens nätverks- och informationssystem för att upptäcka sårbarheter med en potentiellt betydande inverkan.

d) Tjänster som stöder säkerheten i IKT-miljön hos andra organisationer än unionens entiteter vilka har ett nära samarbete med unionens entiteter, till exempel genom att få arbetsuppgifter och ansvar tilldelade enligt unionsrätten, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

Med avseende på första stycket d, får CERT-EU undantagsvis, med IICB:s förhandsgodkännande, ingå servicenivåavtal med andra entiteter än unionens entiteter.

7. CERT-EU ska anordna och får delta i cybersäkerhetsövningar eller rekommendera deltagande i befintliga övningar, i tillämpliga fall i nära samarbete med Enisa, för att testa unionsentiteternas cybersäkerhetsnivå.

8. CERT-EU får stödja unionens entiteter när det gäller incidenter i nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter om de berörda unionsentiteterna uttryckligen begär detta i enlighet med deras respektive förfaranden. Tillhandahållandet av stöd från CERT-EU enligt denna punkt ska inte påverka tillämpliga bestämmelser om skyddet av säkerhetsskyddsklassificerade uppgifter.

9. CERT-EU ska informera unionens entiteter om sina förfaranden och processer för incidenthantering.

10. CERT-EU ska, med en hög grad av konfidentialitet och tillförlitlighet, via lämpliga samarbetsmekanismer och rapporteringsvägar, bidra till relevant och anonymiserad information om större incidenter och det sätt på vilket de hanterades. Denna information ska ingå i den rapport som avses i artikel 10.14.

11. CERT-EU ska i samarbete med EDPS stödja berörda unionsentiteter när de hanterar incidenter som medför personuppgiftsincidenter, utan att det påverkar EDPS befogenheter och arbetsuppgifter som tillsynsmyndighet enligt förordning (EU) 2018/1725.

12. CERT-EU får, om unionsentiteternas politiska avdelningar uttryckligen så begär, tillhandahålla teknisk rådgivning eller tekniska synpunkter i relevanta politiska frågor.

Artikel 14

Vägledningar, rekommendationer och uppmaningar till åtgärder

1. CERT-EU ska stödja genomförandet av denna förordning genom att utfärda

a) uppmaningar till åtgärder som beskriver brådskande säkerhetsåtgärder som unionens entiteter uppmanas att vidta inom en fastställd tidsram,

b) förslag till IICB om vägledningar som riktar sig till alla eller en del av unionens entiteter,

c) förslag till IICB om rekommendationer som riktar sig till enskilda unionsentiteter.

Med avseende på första stycket a ska den berörda unionsentiteten, utan onödigt dröjsmål efter att ha mottagit uppmaningen till åtgärder, informera CERT-EU om hur de brådskande säkerhetsåtgärderna tillämpades.

2. Vägledningar och rekommendationer kan omfatta

a) gemensamma metoder och en modell för att bedöma unionsentiteternas nivå av cybersäkerhetmognad, inbegripet motsvarande skalor eller nyckelprestandaindikatorer, som används som referens till stöd för en kontinuerlig förbättring av cybersäkerheten i unionens entiteter, och som underlättar prioriteringen av cybersäkerhetsområden och cybersäkerhetsåtgärder med beaktande av entiteternas cybersäkerhetsstatus,

b) arrangemang för eller förbättringar av riskhanteringen för cybersäkerhet och riskhanteringsåtgärderna för cybersäkerhet,

c) arrangemang för mognadsbedömningar av cybersäkerhet och cybersäkerhetsplaner,

d) när så är lämpligt, användning av gemensam teknik, arkitektur, öppen källkod och tillhörande bästa praxis i syfte att uppnå interoperabilitet och gemensamma standarder, inbegripet en samordnad strategi för säkerhet i leveranskedjan,

e) när så är lämpligt, information för att underlätta användningen av instrument för gemensam upphandling i fråga om inköp av relevanta cybersäkerhetstjänster och cybersäkerhetsprodukter från tredjepartsleverantörer,

f) arrangemang för informationsutbyte enligt artikel 20.

Artikel 15

CERT-EU:s chef

1. Kommissionen ska, efter godkännande med två tredjedelars majoritet av IICB:s ledamöter, utnämna CERT-EU:s chef. IICB ska rådfrågas i alla skeden av utnämningsförfarandet, särskilt när det gäller att utarbeta meddelanden om den lediga tjänsten, granska ansökningar och utse uttagningskommittéer med avseende på tjänsten. Urvalsförfarandet, inbegripet slutlistan över de bästa kandidaterna från vilken CERT-EU:s chef ska utses, ska säkerställa en jämn könsfördelning, med beaktande av de ansökningar som kommer in.

2. CERT-EU:s chef ska ansvara för att CERT-EU fungerar väl och ska agera inom det behörighetsområde som han eller hon tilldelats och under ledning av IICB. CERT-EU:s chef ska regelbundet rapportera till IICB:s ordförande och ska på dess begäran lämna in ad hoc-rapporter till IICB.

3. CERT-EU:s chef ska stödja den behöriga delegerade utanordnaren i utarbetandet av den årliga verksamhetsrapport med finansiella och administrativa uppgifter, inbegripet resultaten av kontroller, som upprättas i enlighet med artikel 74.9 i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046[1], och ska regelbundet rapportera till den delegerade utanordnaren om genomförandet av åtgärder för vilka befogenheter har vidaredelegerats till CERT-EU:s chef.

4. CERT-EU:s chef ska en gång om året utarbeta en finansiell plan för administrativa inkomster och utgifter för dess verksamhet, ett förslag till årligt arbetsprogram, ett förslag till en tjänstekatalog för CERT-EU, förslag till översyner av tjänstekatalogen, förslag till arrangemang för servicenivåavtal och förslag till nyckelprestandaindikatorer för CERT-EU vilka ska godkännas av IICB i enlighet med artikel 11. Vid översynen av förteckningen över tjänster i CERT-EU:s tjänstekatalog ska CERT-EU:s chef beakta de resurser som tilldelats CERT-EU.

---

[1] Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (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 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012 (EUT L 193, 30.7.2018, s. 1).

5. CERT-EU:s chef ska minst en gång om året lämna rapporter till IICB och IICB:s ordförande om CERT-EU:s verksamhet och resultat under referensperioden, inbegripet om genomförandet av budgeten, servicenivåavtal och skriftliga avtal som ingåtts, samarbete med motparter och partner samt personalens tjänsteresor, inbegripet de rapporter som avses i artikel 11. Dessa rapporter ska omfatta ett arbetsprogram för kommande period, den finansiella planeringen av inkomster och utgifter, inklusive personal, planerade uppdateringar av CERT-EU:s tjänstekatalog och en bedömning av de förväntade effekterna av sådana uppdateringar i fråga om ekonomiska resurser och personalresurser.

Artikel 16

Ekonomiska frågor och personalfrågor

1. CERT-EU ska integreras i den administrativa strukturen vid ett av kommissionens generaldirektorat för att kunna dra nytta av kommissionens stödstrukturer för administration, ekonomisk förvaltning och redovisning, samtidigt som CERT-EU behåller sin status som autonom interinstitutionell tjänsteleverantör för alla unionsentiteter. Kommissionen ska informera IICB om CERT-EU:s administrativa lokalisering och eventuella ändringar därav. Kommissionen ska regelbundet, och under alla omständigheter före inrättandet av en flerårig budgetram i enlighet med artikel 312 i EUF-fördraget, se över de administrativa arrangemang som rör CERT-EU, för att göra det möjligt att vidta lämpliga åtgärder. Översynen ska inbegripa möjligheten att inrätta CERT-EU som unionsbyrå.

2. När det gäller tillämpningen av de administrativa och finansiella förfarandena ska CERT-EU:s chef handla under kommissionens överinseende och under IICB:s tillsyn.

3. CERT-EU:s arbetsuppgifter och verksamhet, inbegripet tjänster som tillhandahålls av CERT-EU i enlighet med artiklarna 13.3, 13.4, 13.5, 13.7 och 14.1 till unionens entiteter som finansieras genom den rubrik i den fleråriga budgetramen som är avsedd för europeisk offentlig administration, ska finansieras med hjälp av en särskild budgetpost i kommissionens budget. De tjänster som öronmärkts för CERT-EU ska anges i en fotnot till kommissionens tjänsteförteckning.

4. Andra unionsentiteter än dem som avses i punkt 3 i denna artikel, ska lämna ett årligt ekonomiskt bidrag till CERT-EU för att täcka de tjänster som CERT-EU tillhandahåller i enlighet med denna punkt. Bidragen ska baseras på riktlinjer som ges av IICB och som varje unionsentitet och CERT-EU kommer överens om sinsemellan i servicenivåavtal. Bidragen ska utgöra en rättvis och proportionell andel av de totala kostnaderna för de tjänster som tillhandahålls. De ska tas emot under den särskilda budgetpost som avses i punkt 3 i denna artikel som interna inkomster avsatta för särskilda ändamål i enlighet med artikel 21.3 c i förordning (EU, Euratom) 2018/1046.

5. Kostnaderna för de tjänster som anges i artikel 13.6 ska återkrävas från de unionsentiteter som tar emot CERT-EU-tjänster. Inkomsterna ska avsättas för de budgetposter som stöder kostnaderna.

Artikel 17

CERT-EU:s samarbete med motparter i medlemsstaterna

1. CERT-EU ska, utan onödigt dröjsmål, samarbeta och utbyta information med motparter i medlemsstaterna, särskilt CSIRT-enheter som utsetts eller inrättats enligt artikel 10 i direktiv (EU) 2022/2555, eller i tillämpliga fall de behöriga myndigheter och gemensamma kontaktpunkter som utsetts eller inrättats enligt artikel 8 i det direktivet, om incidenter, cyberhot, sårbarheter, tillbud, möjliga motåtgärder såväl som bästa praxis och om alla frågor som är relevanta för att förbättra skyddet av IKT-miljön vid unionens entiteter, inbegripet genom det CSIRT-nätverk som inrättats enligt artikel 15 i direktiv (EU) 2022/2555. CERT-EU ska stödja kommissionen i den EU-CyCLONe som inrättats enligt artikel 16 i direktiv (EU) 2022/2555 om den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser.

2. När CERT-EU får kännedom om en betydande incident som inträffar inom en medlemsstats territorium ska den utan dröjsmål underrätta alla relevanta motparter i den medlemsstaten, i enlighet med punkt 1.

3. Förutsatt att personuppgifter skyddas i enlighet med unionens tillämpliga dataskyddslagstiftning, ska CERT-EU, utan onödigt dröjsmål, utbyta relevant incidentspecifik information med motparter i medlemsstaterna för att underlätta upptäckt av liknande cyberhot eller incidenter, eller för att bidra till analysen av en incident, utan tillstånd från den berörda unionsentiteten. CERT-EU får utbyta incidentspecifik information som avslöjar identiteten på målet för cybersäkerhetsincidenten endast i något av följande fall:

a) Den berörda unionsentiteten ger sitt samtycke.

b) Den berörda unionsentiteten ger inte sitt samtycke i enlighet med led a, men offentliggörandet av den berörda unionsentitetens identitet skulle öka sannolikheten för att incidenter på annat håll skulle undvikas eller begränsas.

c) Den berörda unionsentiteten har redan offentliggjort att den berörts.

Beslut om utbyte av incidentspecifik information som avslöjar identiteten på målet för incidenten i enlighet med första stycket b ska godkännas av CERT-EU:s chef. Innan CERT-EU utfärdar ett sådant beslut ska CERT-EU skriftligen kontakta den berörda unionsentiteten och tydligt förklara hur avslöjandet av dess identitet skulle bidra till att undvika eller begränsa incidenter på annat håll. CERT-EU:s chef ska tillhandahålla en förklaring och uttryckligen begära att unionsentiteten anger om den samtycker inom en fastställd tidsram. CERT-EU:s chef ska också informera unionsentiteten om att han eller hon, mot bakgrund av den förklaring som lämnats, förbehåller sig rätten att offentliggöra informationen även utan samtycke. Den berörda unionsentiteten ska informeras innan informationen offentliggörs.

Artikel 18

CERT-EU:s samarbete med andra motparter

1. CERT-EU får samarbeta med andra motparter i unionen än dem som avses i artikel 17 vilka omfattas av unionens cybersäkerhetskrav, inbegripet branschspecifika motparter, om verktyg och metoder, såsom teknik, taktik, förfaranden och bästa praxis, och om cyberhot och sårbarheter. För allt samarbete med sådana motparter ska CERT-EU från fall till fall inhämta förhandsgodkännande från IICB. När CERT-EU upprättar samarbete med sådana motparter ska det informera alla de relevanta motparter i medlemsstaterna som avses i artikel 17.1, i den medlemsstat där motparten är belägen. När så är tillämpligt och lämpligt ska sådant samarbete och villkoren för detta, inbegripet när det gäller cybersäkerhet, dataskydd och informationshantering, fastställas i särskilda överenskommelser om konfidentialitet, såsom avtal eller administrativa arrangemang. Överenskommelser om konfidentialitet ska inte kräva något förhandsgodkännande från IICB, men IICB:s ordförande ska informeras. I händelse av ett brådskande och överhängande behov av att utbyta cybersäkerhetsinformation, i unionsentiteternas eller en annan parts intresse, får CERT-EU göra det med en entitet vars särskilda kompetens, kapacitet och expertis rimligen krävs för att tillgodose ett sådant brådskande och överhängande behov, även om CERT-EU inte har någon överenskommelse om konfidentialitet med den entiteten. I sådana fall ska CERT-EU omedelbart informera IICB:s ordförande och rapportera till IICB genom regelbundna rapporter eller möten.

2. CERT-EU får samarbeta med partner, såsom kommersiella entiteter, inbegripet branschspecifika entiteter, internationella organisationer, nationella entiteter eller enskilda experter utanför unionen, för att samla in information om allmänna och specifika cyberhot, tillbud, sårbarheter och möjliga motåtgärder. För ett bredare samarbete med sådana partner ska CERT-EU från fall till fall inhämta förhandsgodkännande från IICB.

3. CERT-EU får, med samtycke från den unionsentitet som berörs av en incident och förutsatt att det finns en överenskommelse eller ett avtal om konfidentialitet med den relevanta motparten eller partnern, lämna information om den specifika incidenten till de motparter eller partner som avses i punkterna 1 och 2 endast i syfte att bidra till dess analys.

Kapitel V
Samarbets- och rapporteringskrav

Artikel 19

Informationshantering

1. Unionens entiteter och CERT-EU ska respektera tystnadsplikt i enlighet med artikel 339 i EUF-fördraget eller likvärdiga tillämpliga ramar.

2. Europaparlamentets och rådets förordning (EG) nr 1049/2001[1] ska tillämpas på allmänhetens begäranden om tillgång till handlingar som innehas av CERT-EU, inbegripet skyldigheten enligt den förordningen att samråda med unionens övriga entiteter, och i förekommande fall medlemsstaterna, när en begäran rör deras handlingar.

3. Unionsentiteternas och CERT-EU:s hantering av information ska vara förenlig med tillämpliga regler om informationssäkerhet.

Artikel 20

Arrangemang för informationsutbyte om cybersäkerhet

1. Unionens entiteter får på frivillig basis meddela CERT-EU om och tillhandahålla information om incidenter, cyberhot, tillbud och sårbarheter som berör dem. CERT-EU ska säkerställa att effektiva medel för kommunikation, med en hög grad av spårbarhet, konfidentialitet och tillförlitlighet, finns tillgängliga i syfte att underlätta informationsutbytet med unionens entiteter. CERT-EU får vid behandlingen av underrättelser, ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser. Utan att det påverkar tillämpningen av artikel 12 får ett frivilligt inlämnande av underrättelser inte leda till att den rapporterande unionsentiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelsen.

---

[1] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

2. För att CERT-EU ska kunna utföra de uppdrag och arbetsuppgifter som den tilldelats i enlighet med artikel 13 får CERT-EU begära att unionens entiteter lämnar information från sina respektive IKT-systeminventarier, inbegripet information om cyberhot, tillbud, sårbarheter, angreppsindikatorer, cybersäkerhetsvarningar och rekommendationer avseende konfiguration av cybersäkerhetsverktyg för att upptäcka incidenter. Den unionsentitet som mottar begäran ska utan onödigt dröjsmål översända den begärda informationen och eventuella senare uppdateringar.

3. CERT-EU får med unionens entiteter utbyta incidentspecifik information som avslöjar identiteten på den unionsentitet som berörs av incidenten, under förutsättning att den unionsentitet som berörs samtycker. Om en unionsentitet inte ger sitt samtycke ska den tillhandahålla CERT-EU de skäl som ligger till grund för detta beslut.

4. Unionens entiteter ska på begäran utbyta information med Europaparlamentet och rådet om slutförandet av cybersäkerhetsplanerna.

5. IICB eller CERT-EU, beroende på vad som är tillämpligt, ska på begäran dela riktlinjer, rekommendationer och uppmaningar till åtgärder med Europaparlamentet och rådet.

6. Delningsskyldigheterna i denna artikel ska inte omfatta

   a) säkerhetsskyddsklassificerade EU-uppgifter,

b) uppgifter vars vidare spridning har uteslutits genom en synlig markering, såvida inte delning av denna information med CERT-EU uttryckligen har tillåtits.

Artikel 21

Rapporteringsskyldigheter

1. En incident ska anses vara betydande om

a) den har orsakat, eller kan orsaka, allvarliga driftstörningar i verksamheten eller ekonomiska förluster för den berörda unionsentiteten,

b) den har påverkat, eller kan påverka, andra fysiska eller juridiska personer genom att åsamka betydande materiell eller immateriell skada.

2. Unionens entiteter ska till CERT-EU lämna

a) en tidig varning – utan onödigt dröjsmål, och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten – som i tillämpliga fall ska ange att den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller skulle kunna ha entitetsövergripande eller gränsöverskridande konsekvenser,

b) en incidentanmälan – utan onödigt dröjsmål, och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten – som i tillämpliga fall ska uppdatera den information som avses i led a och ange en första bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer,

c) en delrapport – på begäran av CERT-EU – om relevanta statusuppdateringar,

d) en slutrapport – senast en månad efter inlämningen av den incidentanmälan som avses i led b – som ska innehålla

   i) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och dess konsekvenser,

   ii) den typ av hot eller grundorsak som sannolikt utlöst incidenten,

   iii) tillämpade och pågående begränsande åtgärder.

   iv) i tillämpliga fall, incidentens gränsöverskridande eller entitetsövergripande konsekvenser.

e) en lägesrapport – i händelse av en pågående incident vid tidpunkten för inlämningen av den slutrapport som avses i led d – vid den tidpunkten och en slutrapport inom en månad efter deras hantering av incidenten.

3. En unionsentitet ska, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om en betydande incident, informera alla relevanta motparter i medlemsstaterna som avses i artikel 17.1 i den medlemsstat där den är belägen om att en betydande incident har inträffat.

4. Unionens entiteter ska bland annat lämna all information som gör det möjligt för CERT-EU att fastställa eventuella entitetsövergripande konsekvenser, konsekvenser för värdmedlemsstaten eller gränsöverskridande konsekvenser efter en betydande incident. Utan att det påverkar artikel 12 ska själva anmälan inte medföra ökat ansvar för unionsentiteten.

5. I tillämpliga fall ska unionens entiteter utan onödigt dröjsmål informera användarna av de berörda nätverks- och informationssystemen, eller andra komponenter i IKT-miljön, som potentiellt berörs av en betydande incident eller ett betydande cyberhot och, när så är lämpligt, behöver vidta riskreducerande åtgärder, om de åtgärder eller avhjälpande arrangemang som de kan vidta för att hantera denna incident eller detta hot. När så är lämpligt ska unionens entiteter informera dessa användare om det betydande cyberhotet.

6. Om en betydande incident eller ett betydande cyberhot berör ett nätverks- och informationssystem, eller en komponent inom en unionsentitets IKT-miljö som har en avsiktlig sammankoppling med en annan unionsentitets IKT-miljö, ska CERT-EU utfärda en relevant cybersäkerhetsvarning.

7. Unionens entiteter ska, på CERT-EU:s begäran och utan onödigt dröjsmål, förse CERT-EU med digital information som skapats genom användning av elektroniska enheter som är inblandade i deras respektive incident. CERT-EU kan tillhandahålla ytterligare uppgifter om vilka typer av uppgifter som behövs för situationsmedvetenhet och incidenthantering.

8. CERT-EU ska var tredje månad lämna in en sammanfattande rapport till IICB, Enisa, EU Intcen och CSIRT-nätverket med anonymiserade och aggregerade data om betydande incidenter, incidenter, cyberhot, tillbud och sårbarheter enligt artikel 20 och betydande incidenter som anmälts enligt punkt 2 i den här artikeln. Den sammanfattande rapporten ska utgöra underlag till den tvåårsrapport om cybersäkerhetssituationen i unionen som antas enligt artikel 18 i direktiv (EU) 2022/2555.

9. Senast den … [sex månader från dagen för denna förordnings ikraftträdande] ska IICB utfärda vägledningar eller rekommendationer som ytterligare specificerar formerna och formatet för samt innehållet i rapporteringen enligt den här artikeln. Vid utarbetandet av sådana riktlinjer eller rekommendationer ska IICB beakta eventuella genomförandeakter som antagits enligt artikel 23.11 i direktiv (EU) 2022/2555 och som specificerar typen av information, formatet och förfarandet för underrättelsen. CERT-EU ska sprida lämpliga tekniska detaljer för att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder hos unionens entiteter.

10. Rapporteringsskyldigheterna i denna artikel ska inte omfatta

a) säkerhetsskyddsklassificerade EU-uppgifter,

b) uppgifter vars vidare spridning har uteslutits genom en synlig markering, såvida inte delning av denna information med CERT-EU uttryckligen har tillåtits.

Artikel 22

Samordning av incidenthantering och samarbete

1. I sin funktion som nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering ska CERT-EU främja informationsutbyte om incidenter, cyberhot, sårbarheter och tillbud mellan

a) unionens entiteter,

b) de motparter som avses i artiklarna 17 och 18.

2. CERT-EU ska, i tillämpliga fall i nära samarbete med Enisa, främja unionsentiteters samordning av incidenthantering, genom bland annat

a) bidrag till konsekvent extern kommunikation,

b) ömsesidigt stöd, såsom utbyte av information som är relevant för unionens entiteter eller tillhandahållande av bistånd, i förekommande fall direkt på plats,

c) optimal användning av operativa resurser,

d) samordning med andra krishanteringsmekanismer på unionsnivå.

3. CERT-EU ska, i nära samarbete med Enisa, stödja unionens entiteter när det gäller situationsmedvetenhet om incidenter, cyberhot, sårbarheter och tillbud samt dela med sig av relevant utveckling på cybersäkerhetsområdet.

4. Senast den … [12 månader från dagen för denna förordnings ikraftträdande] ska IICB på grundval av ett förslag från CERT-EU, anta riktlinjer eller rekommendationer för samordning av incidenthantering och samarbete vid betydande incidenter. När en incident misstänks vara brottslig ska CERT-EU ge råd om hur incidenten ska rapporteras till de brottsbekämpande myndigheterna utan onödigt dröjsmål.

5. Efter en särskild begäran från en medlemsstat och med de berörda unionsentiteternas godkännande får CERT-EU anlita experter från den förteckning som avses i artikel 23.4 för att bidra till hanteringen av en större incident som påverkar den medlemsstaten, eller en storskalig cybersäkerhetsincident i enlighet med artikel 15.3 g i direktiv (EU) 2022/2555. Särskilda regler om tillgång till och användning av tekniska experter från unionens entiteter ska godkännas av IICB på grundval av ett förslag från CERT-EU.

Artikel 23

Hantering av större incidenter

1. För att på operativ nivå stödja en samordnad hantering av större incidenter som berör unionens entiteter och bidra till ett regelbundet utbyte av relevant information mellan unionens entiteter och med medlemsstaterna ska IICB i enlighet med artikel 11 led q, i nära samarbete med CERT-EU och Enisa, upprätta en cyberkrishanteringsplan på grundval av den verksamhet som avses i artikel 22.2. Cyberkrishanteringsplanen ska innehålla åtminstone följande:

   a) Arrangemang för samordning och informationsflöde mellan unionens entiteter för hantering av större incidenter på operativ nivå.

   b) Gemensamma operationella standardförfaranden (SOP).

   c) En gemensam taxonomi för större incidenters allvarlighetsgrad och kriströskelpunkter.

   d) Regelbundna övningar.

   e) Uppgift om vilka säkra kommunikationskanaler som ska användas.

2. Kommissionens företrädare i IICB ska, med förbehåll för den cyberkrishanteringsplan som upprättats enligt punkt 1 i denna artikel och utan att det påverkar tillämpningen av artikel 16.2 första stycket i direktiv (EU) 2022/2555, vara kontaktpunkt för utbyte av relevant information om större incidenter med EU-CyCLONe.

3. CERT-EU ska samordna unionsentiteternas hantering av större incidenter. Det ska föra en förteckning över den tillgängliga tekniska expertis som skulle behövas för incidenthantering i händelse av större incidenter och bistå IICB med att samordna unionsentiteters cyberkrishanteringsplaner för sådana större incidenter som avses i artikel 9 2.

4. Unionens entiteter ska bidra till förteckningen över teknisk expertis genom att tillhandahålla en årligen uppdaterad förteckning över experter som finns tillgängliga inom respektive organisation med detaljerade uppgifter om deras specifika tekniska kompetens.

Kapitel VI
Slutbestämmelser

Artikel 24

Inledande omfördelning av budgeten

För att säkerställa att CERT-EU fungerar korrekt och stabilt får kommissionen föreslå en omfördelning av personal och ekonomiska resurser till kommissionens budget för användning i CERT-EU-insatser. Omfördelningen ska få verkan samtidigt som unionens första årliga budget som antas efter det att denna förordning träder i kraft.

Artikel 25

Översyn

1. IICB ska, senast den … [12 månader från den dag då denna förordning träder i kraft] och därefter årligen, med bistånd av CERT-EU rapportera till kommissionen om genomförandet av denna förordning. IICB får rekommendera kommissionen att se över denna förordning.

2. Kommissionen ska, senast den … [36 månader från den dag då denna förordning träder i kraft] och därefter vartannat år, bedöma och rapportera om genomförandet av denna förordning och om den erfarenhet som gjorts på strategisk och operativ nivå till Europaparlamentet och rådet.

Den rapport som avses i första stycket i denna punkt ska innehålla den översyn som avses i artikel 16.1 om möjligheten att inrätta CERT-EU som unionsbyrå.

3. Kommissionen ska, senast den … [fem år från den dag då denna förordning träder i kraft], utvärdera hur denna förordning fungerar och lämna en rapport till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén. Kommissionen ska också utvärdera lämpligheten i att inkludera nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter inom ramen för denna förordning, med beaktande av andra unionsrättsakter som är tillämpliga på dessa system. Rapporten ska vid behov åtföljas av ett lagstiftningsförslag.

Artikel 26

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*