Europeiska unionens råd

Bryssel den 22 mars 2022
(OR. en)

7474/22

Interinstitutionellt ärende:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	22 mars 2022
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2022) 122 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

För delegationerna bifogas dokument – COM(2022) 122 final.

Bilaga: COM(2022) 122 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Genom detta förslag inrättas en ram för att säkerställa gemensamma regler och åtgärder för cybersäkerhet hos unionens institutioner, organ och byråer. Det syftar till att ytterligare förbättra alla entiteters resiliens och incidenthanteringskapacitet. Det ligger i linje med kommissionens prioriteringar att göra Europa rustat för den digitala tidsåldern och att bygga en framtidssäkrad ekonomi som fungerar för människorna. Att säkerställa en säker och resilient offentlig administration är dessutom en hörnsten i digitaliseringen av samhället som helhet.

Detta förslag bygger på strategin för EU:s säkerhetsunion (COM(2020) 605 final) och EU:s strategi för cybersäkerhet för ett digitalt decennium (JOIN(2020) 18 final).

Förslaget moderniserar den befintliga rättsliga ramen för CERT-EU och tar hänsyn till den förändrade och ökade digitaliseringen av institutionerna, organen och byråerna under de senaste åren samt den föränderliga cyberhotbilden. Det har skett ytterligare utveckling på båda dessa områden sedan covid-19-krisen bröt ut, då antalet incidenter fortsätter att öka, med allt mer sofistikerade attacker från många olika källor.

Genom förslaget ändras CERT-EU:s namn från ”incidenthanteringsorganisationen” till ”cybersäkerhetscentrumet” för unionens institutioner, organ och byråer, i enlighet med utvecklingen i medlemsstaterna och globalt, där många CERT:ar nu i stället kallas cybersäkerhetscentrum, men kortnamnet ”CERT-EU” behålls eftersom det är inarbetat.

• Förenlighet med befintliga bestämmelser inom området

Detta förslag syftar till att öka unionens institutioners, organs och byråers cybersäkerhetsresiliens mot cyberhot, samtidigt som anpassningar görs till följande befintlig lagstiftning:

- Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Anpassningar görs också till förslaget till direktiv (EU) XXXX/XXXX om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 [förslaget till NIS 2].

- Förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

- Förslag till förordning (EU) XXXX/XXXX om informationssäkerhet inom unionens institutioner, organ och byråer.

- Kommissionens rekommendation av den 23 juni 2021 om att bygga en gemensam cyberenhet.

- Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.

Bilagan till kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser innehåller en plan för samordnade insatser vid stora gränsöverskridande cyberincidenter och cyberkriser.

I sin resolution av den 9 mars 2021 betonade Europeiska unionens råd att cybersäkerhet är avgörande för den offentliga förvaltningens funktion på både nationell nivå och EU-nivå samt för samhället och ekonomin som helhet och underströk vikten av en robust och konsekvent säkerhetsram för att skydda EU:s alla anställda, data, kommunikationsnät, informationssystem och beslutsprocesser. Detta ska särskilt uppnås genom ökad resiliens och förbättrad säkerhetskultur vid unionens institutioner, organ och byråer. Tillräckliga resurser och tillräcklig kapacitet bör frigöras, även vid förstärkningen av mandatet för CERT-EU.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den rättsliga grunden för denna förordning är artikel 298 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*), där det föreskrivs att unionens institutioner, organ och byråer när de fullgör sina uppgifter ska stödja sig på en öppen, effektiv och oberoende europeisk administration. Med beaktande av de tjänsteföreskrifter och anställningsvillkor som har antagits på grundval av artikel 336 ska Europaparlamentet och rådet genom förordningar i enlighet med det ordinarie lagstiftningsförfarandet fastställa bestämmelser för detta ändamål.

Informationsteknik har skapat nya sätt för unionens institutioner, organ och byråer att arbeta, samverka med medborgarna och förbättra den övergripande verksamheten. Vartefter som tekniken fortsätter att utvecklas, utvecklas även cyberhotbilden. Unionens institutioner, organ och byråer har blivit mycket attraktiva mål för sofistikerade cyberattacker. Inrättandet av system och krav för att säkerställa cybersäkerhet verkar bidra till den europeiska administrationens effektivitet och oberoende, så att unionens institutioner, organ och byråer kan fungera effektivare i en digital värld när de fullgör sina uppgifter.

Som förklaras i avsnitt 3 är dessutom de befintliga skillnaderna mellan unionens institutioners, organs och byråers säkerhetsstatus och förhållningssätt till cybersäkerhet ytterligare hinder för en öppen, effektiv och oberoende europeisk administration. Utan ett gemensamt förhållningssätt skulle säkerhetsstatusen hos unionens institutioner, organ och byråer fortsätta att utvecklas i olika riktningar. Denna rättsliga grund är därför lämplig med tanke på att förordningen syftar till att skapa en gemensam rättslig ram för cybersäkerhet inom unionens institutioner, organ och byråer.

• Subsidiaritetsprincipen

Förordningen om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer omfattas av unionens exklusiva befogenhet.

- **Proportionalitetsprincipen**

De regler som föreslås i denna förordning går inte utöver vad som är nödvändigt för att uppnå de specifika målen på ett tillfredsställande sätt. De planerade åtgärderna kommer att bidra till att en hög gemensam cybersäkerhetsnivå uppnås utan att överskrida vad som är nödvändigt för att uppnå målet mot bakgrund av de allt större riskerna.

- **Val av instrument**

En förordning, som är direkt tillämplig, anses vara det lämpliga rättsliga instrumentet för att fastställa och förenhetliga de skyldigheter som åläggs unionens institutioner, organ och byråer. För att möjliggöra riktade förbättringar är en förordning det lämpligaste rättsliga instrumentet.

3. RESULTAT AV FÖRHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Förhandsutvärderingar**

CERT-EU har gjort en bedömning av de främsta cyberhot som unionens institutioner, organ och byråer för närvarande är utsatta för eller sannolikt kommer att utsättas för inom överskådlig framtid.

Tre kategorier av iakttagelser användes i analysen:

- Försök att göra intrång i unionens institutioners, organs och byråers it-infrastruktur (när de lyckas behandlas de som incidenter; annars registreras de ändå som upptäckta försök).
- Hot som upptäcks i närheten av unionens institutioner, organ och byråer (t.ex. i relaterade sektorer, deras intressentgrupper eller i Europa).
- Betydande hottrender som observerats globalt.

Vid analysen övervägdes dessutom hur stora pågående förändringar påverkar unionsinstitutionernas sätt att förvalta och använda sin it-infrastruktur och sina it-tjänster. Det rör sig om förändringar såsom

- ökat distansarbete,
- migrering av system till molnet,
- ökad utkontraktering av it-tjänster.

Mellan 2019 och 2021 har antalet betydande incidenter[1] som påverkat unionens institutioner, organ och byråer och som skapats av APT-aktörer (*Advanced Persistent Threat*, dvs. avancerat långvarigt hot) ökat dramatiskt. Under första halvåret 2021 tillstötte lika många betydande incidenter som under hela 2020. Detta återspeglas också i att CERT-EU

[1] Med ”betydande incident” avses varje incident, såvida den inte har begränsad inverkan och sannolikt redan är välbekant i fråga om metod eller teknik.

analyserade tre gånger så många kriminaltekniska bilder (ögonblicksbilder av innehållet i berörda system eller enheter) 2020 jämfört med 2019, medan antalet betydande incidenter har ökat mer än tiofalt sedan 2018.

År 2020 fastställde CERT-EU:s styrelse ett nytt strategiskt mål för CERT-EU, nämligen att garantera en heltäckande nivå av cyberförsvar för alla institutioner, organ och byråer med lagom bredd och djup och kontinuerlig anpassning till befintliga eller nära förestående hot, inbegripet angrepp mot mobila enheter, molnmiljöer och enheter inom sakernas internet.

Som ett komplement till CERT-EU:s hotbildsanalys har kommissionen gjort en utvärdering av hur cybersäkerheten fungerar vid 20 av unionens institutioner, organ och byråer. Detta gav en inblick i etablerad cybersäkerhetspraxis och kapacitet för hantering av cybersäkerhet med extern riktmärkning av vissa tekniska säkerhetskontroller.

Utvärderingen baserades på frågeformulär som besvarades av dessa institutioner, organ och byråer, offentligt tillgängliga data samt data som unionens institutioner, organ och byråer själva tillhandahållit direkt. Den ger tillräckliga insikter i den nuvarande situationen för att man ska kunna dra följande slutsatser:

- Det finns avsevärda skillnader i cybersäkerhetsmognad, it-infrastrukturstorlek och kapacitetsnivåer mellan de institutioner, organ och byråer som utvärderades.

- Många av unionens institutioner, organ och byråer har visserligen en mogen detektions- och insatskapacitet i allmänhet, men med varierande nivåer av integrerad riskhantering i kapaciteten för cybersäkerhetsstyrning.

- I allmänhet är de utvärderade unionsinstitutionernas, unionsorganens och unionsbyråernas cybersäkerhetsramar (strategi, policy och en regelbas) väl etablerade på de centrala cybersäkerhetsområden som förtecknas i bilaga I till förordningen, men vissa av unionens institutioner, organ och byråer saknar mogen hantering av driftskontinuitet, kontroll av efterlevnad, revision och kontinuerlig förbättring.

- Tekniska åtgärder som anses vara bästa praxis visade sig tillämpas på ett ojämnt sätt av unionens institutioner, organ och byråer.

Sammanfattningsvis visar analysen av 20 av unionens institutioner, organ och byråer att deras styrning, cyberhygien, övergripande kapacitet och mognad varierar kraftigt. Det är därför nödvändigt att kräva att alla unionens institutioner, organ och byråer inför en baslinje för cybersäkerhetsåtgärder för att komma till rätta med denna skillnad i mognadsgrad och för att alla unionens institutioner, organ och byråer ska uppnå en hög gemensam cybersäkerhetsnivå.

Ingen unionslagstiftning har hittills varit inriktad på cybersäkerheten vid unionens institutioner, organ och byråer eller på ett heltäckande sätt tagit upp hotbilden på cybersäkerhetsområdet och de framväxande it-risker som digitaliseringen för med sig.

- **Samråd med berörda parter**

Kommissionen har samrått med berörda parter inom unionens institutioner, organ och byråer samt med företrädare för medlemsstaterna i rådet och berörda parter i Europaparlamentet. Den 25 juni 2021 deltog företrädare för medlemsstaterna och berörda parter från unionens institutioner, organ och byråer i en workshop som kommissionen anordnade för att diskutera innehållet i det framtida förslaget till förordning.

- **Konsekvensbedömning**

Detta förslag kommer endast att få konsekvenser för unionens institutioner, organ och byråer. En särskild konsekvensbedömning är därmed inte nödvändig eftersom medlemsstaterna inte berörs.

- **Grundläggande rättigheter**

Europeiska unionen är fast besluten att säkerställa en hög standard på skyddet av de grundläggande rättigheterna. Allt eventuellt informationsutbyte på grundval av denna förordning kommer att genomföras i betrodda miljöer med full respekt för rätten till skydd av personuppgifter enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna och relevant dataskyddslagstiftning, framför allt Europaparlamentets och rådets förordning (EU) 2018/1725.

4. BUDGETKONSEKVENSER

Marknadsriktmärken och studier[2] visar att de direkta cybersäkerhetsutgifterna tenderar att utgöra mellan 4 och 7 % av organisationers sammanlagda it-utgifter. Den hotanalys som CERT-EU har gjort till stöd för detta lagstiftningsförslag visar dock att internationella organ och politiska organisationer löper större risk och att ett lämpligare mål vore att satsa 10 % av it-utgifterna på cybersäkerhet. De exakta kostnaderna för sådana insatser kan inte fastställas på grund av bristen på detaljerad information om it-utgifter vid unionens institutioner, organ och byråer och cybersäkerhetsutgifternas andel av dessa.

Även om det därför är sannolikt att många av unionens institutioner, organ och byråer spenderar mindre på cybersäkerhet än de borde kommer denna förordning inte i sig att leda till att de löpande utgifterna ökar. Även utan förordningen skulle varje entitet behöva säkerställa en adekvat cybersäkerhetsnivå. Förordningen bibehåller det tidigare samarbetet i CERT-EU:s styrelse och formaliserar ett lager av informationsutbyte som redan delvis finns i dag. Som anges i finansieringsöversikten för rättsakten kommer CERT-EU att behöva ytterligare resurser för att kunna fullgöra sin utvidgade roll, och dessa resurser bör omfördelas från de av unionens institutioner, organ och byråer som drar nytta av CERT-EU:s tjänster.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Den interinstitutionella cybersäkerhetsstyrelsen (IICB) bör med hjälp av CERT-EU se över hur denna förordning fungerar, göra utvärderingar och lägga fram en rapport med sina resultat för kommissionen. Kommissionen bör säkerställa regelbunden rapportering till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén.

---

[2] Källa: Gartner, *Identifying the Real Information Security Budget* (2016). Detta är utöver indirekta utgifter för it-säkerhet bland annat för nätsäkerhet, såsom brandväggar och antivirusprogram, och systemägares ansvar, såsom riskbedömning och genomförande av säkerhetskontroller. I ett dokument från 2020 uppskattas cybersäkerhetsutgifterna utgöra 10–11 % av it-utgifterna för finansinstitut, källa: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

CERT-EU kan utarbeta ett förslag till en vägledning eller rekommendation som IICB kan välja att anta. En vägledning är ett rådgivande dokument som riktar sig till alla eller en undergrupp av unionens institutioner, organ och byråer, medan en rekommendation riktar sig till enskilda institutioner, organ och byråer. En uppmaning till åtgärder är ett rådgivande dokument från CERT-EU som beskriver brådskande säkerhetsåtgärder som unionens institutioner, organ och byråer uppmanas att vidta inom en fastställd tidsram.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Allmänna bestämmelser

I förordningen fastställs åtgärder i syfte att säkerställa en hög gemensam cybersäkerhetsnivå och den är tillämplig på unionens institutioner, organ och byråer så att de ska kunna utföra sina respektive uppdrag på ett öppet, effektivt och oberoende sätt. (Artiklarna 1–3, 23–25)

Åtgärder för en hög gemensam cybersäkerhetsnivå

Unionens institutioner, organ och byråer är skyldiga att inrätta en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker som säkerställer en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker. Institutionerna, organen och byråerna ska dessutom anta en baslinje för cybersäkerhet för att hantera de risker som identifierats inom ramen, göra regelbundna mognadsbedömningar av cybersäkerheten och anta en cybersäkerhetsplan. (Artiklarna 4–8)

Interinstitutionell cybersäkerhetsstyrelse

Den interinstitutionella cybersäkerhetsstyrelsen inrättas och får i uppgift att övervaka unionens institutioners, organs och byråers genomförande av denna förordning samt att bevaka CERT-EU:s genomförande av de allmänna prioriteringarna och målen och ge CERT-EU strategisk ledning. (Artiklarna 9–11)

CERT-EU

CERT-EU ska bidra till it-miljöns säkerhet hos alla unionens institutioner, organ och byråer genom att ge dem råd, hjälpa till att förebygga, upptäcka, begränsa och hantera incidenter och genom att fungera som deras nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering. (Artiklarna 12–17)

Samarbets- och rapporteringskrav

Förordningen säkerställer samarbete och informationsutbyte mellan CERT-EU och unionens institutioner, organ och byråer för att skapa förtroende och tillit. För detta ändamål får CERT-EU begära att unionens institutioner, organ och byråer tillhandahåller relevant information och CERT-EU får utbyta incidentspecifik information med unionens institutioner, organ och byråer för att underlätta upptäckt av liknande cyberhot eller incidenter utan den berörda avtalspartens samtycke. CERT-EU får utbyta incidentspecifik information som avslöjar identiteten på målet för cybersäkerhetsincidenten endast med den berörda avtalspartens samtycke.

Alla unionens institutioner, organ och byråer blir skyldiga att underrätta CERT-EU om betydande cyberhot, betydande sårbarheter och betydande incidenter utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter det att de fått kännedom om dem. (Artiklarna 18–22)

2022/0085 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

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, och

av följande skäl:

(1) I den digitala tidsåldern är informations- och kommunikationsteknik en hörnsten i en öppen, effektiv och oberoende unionsadministration. Ny teknik och de digitala systemens ökade komplexitet och sammankopplingar förstärker cybersäkerhetsriskerna och gör unionsadministrationen mer sårbar för cyberhot och incidenter, vilket i slutändan utgör ett hot mot administrationens driftskontinuitet och kapacitet att säkra sina data. Ökad användning av molntjänster, allmänt utbredd användning av it, omfattande digitalisering, distansarbete och framväxande teknik och konnektivitet är i dag centrala inslag i all verksamhet inom unionens administrativa entiteter, men den digitala resiliensen är ännu inte tillräckligt inbyggd.

(2) Unionens institutioner, organ och byråer konfronteras med ett cyberhotlandskap 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. De 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 institutioner, organ och byråer har sammankopplade it-miljöer och integrerade dataflöden, och deras användare har ett nära samarbete. Denna sammankoppling innebär att alla störningar, även om de inledningsvis endast berör enstaka institutioner, organ och byråer, kan få större kaskadeffekter med långtgående och långvariga negativa konsekvenser för de andra. Dessutom är vissa institutioners,

organs och byråers it-miljöer sammankopplade med medlemsstaternas it-miljöer, så att en incident hos en unionsentitet kan utgöra en risk för cybersäkerheten i medlemsstaternas it-miljöer och vice versa.

(4) Unionens institutioner, organ och byråer 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 den europeiska administrationen ska fungera är det därför nödvändigt att unionens institutioner, organ och byråer uppnår en hög gemensam cybersäkerhetsnivå genom en baslinje för cybersäkerhet (en uppsättning minimiregler för cybersäkerhet som nätverks- och informationssystem och deras operatörer och användare måste följa för att minimera cybersäkerhetsriskerna), informationsutbyte och samarbete.

(5) Direktivet [förslag till NIS 2] om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen syftar till att ytterligare förbättra cybersäkerhetsresiliensen och incidenthanteringskapaciteten hos offentliga och privata entiteter, nationella behöriga myndigheter och organ samt unionen som helhet. Det är därför nödvändigt att unionens institutioner, organ och byråer följer detta genom att säkerställa regler som är förenliga med direktivet [förslag till NIS 2] och som återspeglar dess ambitionsnivå.

(6) För att uppnå en hög gemensam cybersäkerhetsnivå är det nödvändigt att varje institution, organ och byrå inrättar en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker vilken säkerställer en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker och tar hänsyn till driftskontinuitet och krishantering.

(7) Skillnaderna mellan unionens institutioner, organ och byråer kräver flexibilitet i genomförandet eftersom samma lösning inte passar alla. Åtgärderna för en hög gemensam cybersäkerhetsnivå bör inte omfatta några skyldigheter som direkt inkräktar på unionens institutioners, organs och byråers utövande av sitt uppdrag eller deras institutionella autonomi. Dessa institutioner, organ och byråer bör därför fastställa sina egna ramar för hantering, styrning och kontroll av cybersäkerhetsrisker och anta sina egna baslinjer och cybersäkerhetsplaner.

(8) För att inte ålägga unionens institutioner, organ och byråer oproportionella finansiella och administrativa bördor bör riskhanteringskraven för cybersäkerhet stå i proportion till den risk som det berörda nätverks- och informationssystemet utgör, med beaktande av den senaste utvecklingen i fråga om sådana åtgärder. Alla unionens institutioner, organ och byråer bör sträva efter att anslå en tillräcklig procentandel av sin it-budget för att förbättra sin cybersäkerhetsnivå; på längre sikt bör man eftersträva ett mål i storleksordningen 10 %.

(9) En hög gemensam cybersäkerhetsnivå kräver att cybersäkerhet övervakas av den högsta ledningsnivån för varje unionsinstitution, unionsorgan och unionsbyrå, som bör godkänna en baslinje för cybersäkerhet som bör ta upp de risker som identifierats inom den ram som ska fastställas av varje institution, organ och byrå. Att etablera en cybersäkerhetskultur, dvs. dagliga cybersäkerhetsrutiner, är en viktig del av en baslinje för cybersäkerhet vid alla unionens institutioner, organ och byråer.

(10) Unionens institutioner, organ och byråer bör bedöma risker som rör förbindelser med leverantörer och tjänsteleverantörer, inbegripet leverantörer av datalagrings- och

databehandlingstjänster eller förvaltade säkerhetstjänster, och vidta lämpliga åtgärder för att hantera dem. Dessa åtgärder bör utgöra en del av baslinjen för cybersäkerhet och specificeras ytterligare i vägledningar eller rekommendationer som utfärdas av CERT-EU. Vid fastställandet av åtgärder och riktlinjer bör vederbörlig hänsyn tas till relevant EU-lagstiftning och EU-politik, inbegripet riskbedömningar och rekommendationer som utfärdats av samarbetsgruppen för nät- och informationssäkerhet, såsom EU:s samordnade riskbedömning och EU:s verktygslåda för 5G-cybersäkerhet. Dessutom kan certifiering av relevanta IKT-produkter, IKT-tjänster och IKT-processer krävas enligt särskilda EU-ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881.

(11) I maj 2011 beslutade generalsekreterarna för unionens institutioner och organ att inrätta en förkonfigurationsgrupp för en incidenthanteringsorganisation för unionens institutioner, organ och byråer (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 arbetsgrupp inom Europeiska kommissionen med ett interinstitutionellt mandat. I december 2017 ingick unionens institutioner och organ ett interinstitutionellt avtal om organisationen och driften av CERT-EU[3]. Detta arrangemang bör fortsätta att utvecklas för att stödja genomförandet av denna förordning.

(12) CERT-EU:s namn bör ändras från ”incidenthanteringsorganisationen” till ”cybersäkerhetscentrumet” för unionens institutioner, organ och byråer, i enlighet med utvecklingen i medlemsstaterna och globalt, där många CERT:ar nu i stället kallas cybersäkerhetscentrum, men kortnamnet ”CERT-EU” bör behållas eftersom det är inarbetat.

(13) Många cyberangrepp är en del av bredare kampanjer som inriktas på grupper av unionens institutioner, organ och byråer eller intressegrupper som inbegriper unionens institutioner, organ och byråer. För att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder bör unionens institutioner, organ och byråer underrätta CERT-EU om betydande cyberhot, betydande sårbarheter och betydande incidenter och dela med sig av lämpliga tekniska detaljer som gör det möjligt att upptäcka eller begränsa samt vidta åtgärder mot liknande cyberhot, sårbarheter och incidenter i andra av unionens institutioner, organ och byråer. Enligt samma tillvägagångssätt som i direktiv [förslag till NIS 2] bör entiteter som blir medvetna om en betydande incident vara skyldiga att lämna en första underrättelse till CERT-EU inom 24 timmar. Sådant informationsutbyte bör göra det möjligt för CERT-EU att sprida informationen till unionens andra institutioner, organ och byråer samt till lämpliga motparter, för att bidra till att skydda unionens it-miljöer och unionens motparters it-miljöer mot liknande incidenter, hot och sårbarheter.

(14) Utöver att ge CERT-EU fler uppgifter och en utökad roll bör det inrättas en interinstitutionell cybersäkerhetsstyrelse (IICB) som främjar en hög gemensam

[3] EUT C 12, 13.1.2018, s. 1.

cybersäkerhetsnivå vid unionens institutioner, organ och byråer genom att övervaka institutionernas, organens och byråernas genomförande av denna förordning, övervaka CERT-EU:s genomförande av allmänna prioriteringar och mål samt tillhandahålla strategisk ledning för CERT-EU. IICB bör säkerställa att institutionerna företräds och inkludera företrädare för byråer och organ genom unionsbyråernas nätverk.

(15) CERT-EU bör stödja genomförandet av åtgärder för en hög gemensam cybersäkerhetsnivå genom 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 institutioner, organ och byråer uppmanas att vidta inom en fastställd tidsram.

(16) IICB bör övervaka efterlevnaden av denna förordning samt uppföljningen av vägledningar, rekommendationer och uppmaningar till åtgärder från CERT-EU. IICB bör i tekniska frågor stödjas av tekniska rådgivande grupper i en sammansättning som IICB anser lämplig vilka bör arbeta i nära samarbete med CERT-EU, unionens institutioner, organ och byråer och andra intressenter i enlighet med vad som är nödvändigt. Vid behov bör IICB utfärda icke-bindande varningar och rekommendera revisioner.

(17) CERT-EU bör ha i uppdrag att bidra till säkerheten i it-miljön för alla unionens institutioner, organ och byråer. CERT-EU bör fungera som motsvarighet till den utsedda samordnaren för unionens institutioner, organ och byråer när det gäller samordnad information om sårbarheter till det europeiska sårbarhetsregister som avses i artikel 6 i direktiv [förslag NIS 2].

(18) År 2020 fastställde CERT-EU:s styrelse ett nytt strategiskt mål för CERT-EU, nämligen att garantera en heltäckande nivå av cyberförsvar för alla unionens institutioner, organ och byråer med lagom bredd och djup och kontinuerlig anpassning till befintliga eller nära förestående hot, inbegripet angrepp mot mobila enheter, molnmiljöer och enheter inom sakernas internet. Det strategiska målet inbegriper också omfattande säkerhetscentrum (SOC) som övervakar nätverk och dygnet-runt-bevakning för allvarliga hot. När det gäller unionens större institutioner, organ och byråer bör CERT-EU stödja deras it-säkerhetsgrupper, även med dygnet-runt-bevakning i första ledet. För små och vissa medelstora institutioner, organ och byråer bör CERT-EU tillhandahålla alla tjänster.

(19) CERT-EU bör också fullgöra den roll som föreskrivs i direktiv [förslag NIS 2] när det gäller samarbete och informationsutbyte med nätverket av enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*). I enlighet med kommissionens rekommendation (EU) 2017/1584[4] bör CERT-EU dessutom samarbeta och samordna insatserna med berörda parter. För att bidra till en hög cybersäkerhetsnivå i hela unionen bör CERT-EU utbyta incidentspecifik information med nationella motparter. CERT-EU bör också samarbeta med andra offentliga och privata motparter, även vid Nato, efter förhandsgodkännande från IICB.

[4] 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).

(20) För att stödja operativ cybersäkerhet bör CERT-EU utnyttja tillgänglig expertis hos Europeiska unionens cybersäkerhetsbyrå genom strukturerat samarbete i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881[5]. 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 Europeiska unionens cybersäkerhetsbyrå om hotbildsanalys och regelbundet dela med sig av sin hotbildsrapport till byrån.

(21) Till stöd för den gemensamma cyberenhet som byggts i enlighet med kommissionens rekommendation av den 23 juni 2021[6] bör CERT-EU samarbeta och utbyta information med berörda parter för att främja operativt samarbete och göra det möjligt för de befintliga nätverken att förverkliga sin fulla potential att skydda unionen.

(22) Alla personuppgifter som behandlas enligt denna förordning bör behandlas i enlighet med dataskyddslagstiftningen, inklusive Europaparlamentets och rådets förordning (EU) 2018/1725[7].

(23) CERT-EU:s och unionens institutioners, organs och byråers hantering av information bör stämma överens med reglerna i förordning [förslag till förordning om informationssäkerhet]. För att säkerställa samordning i säkerhetsfrågor bör kommissionens säkerhetsdirektorat och IICB:s ordförande utan onödigt dröjsmål informeras om alla kontakter som nationella säkerhets- och underrättelsetjänster initierar eller söker med CERT-EU.

(24) Eftersom CERT-EU:s tjänster och uppgifter ligger i alla unionens institutioners, organs och byråers intresse bör varje institution, organ och byrå med it-utgifter bidra med en skälig andel till dessa tjänster och uppgifter. Dessa bidrag påverkar inte budgetautonomin för unionens institutioner, organ och byråer.

(25) 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.

---

5 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).

6 Kommissionens rekommendation C(2021) 4520 av den 23 juni 2021 om att bygga en gemensam cyberenhet.

7 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).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Kapitel I
ALLMÄNNA BESTÄMMELSER

Artikel 1
Innehåll

I denna förordning fastställs

(a) skyldigheter för unionens institutioner, organ och byråer att inrätta en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker,

(b) riskhanterings- och rapporteringsskyldigheter på cybersäkerhetsområdet för unionens institutioner, organ och byråer,

(c) regler om organisationen och driften av Cybersäkerhetscentrumet för unionens institutioner, organ och byråer (CERT-EU) och om organisationen och driften av den interinstitutionella cybersäkerhetsstyrelsen (IICB).

Artikel 2
Tillämpningsområde

Denna förordning är tillämplig på alla unionens institutioners, organs och byråers hantering, styrning och kontroll av cybersäkerhetsrisker och på organisationen och driften av CERT-EU och den interinstitutionella cybersäkerhetsstyrelsen.

Artikel 3
Definitioner

I denna förordning gäller följande definitioner:

(1) *unionens institutioner, organ och byråer*: de unionsinstitutioner, unionsorgan och unionsbyråer som inrättats genom, eller på grundval av, fördraget om Europeiska unionen, fördraget om Europeiska unionens funktionssätt eller fördraget om upprättandet av Europeiska atomenergigemenskapen.

(2) *nätverks- och informationssystem*: nätverks- och informationssystem i den mening som avses i artikel 4.1 i direktiv [förslag till NIS 2].

(3) *säkerhet i nätverks- och informationssystem*: säkerhet i nätverks- och informationssystem i den mening som avses i artikel 4.2 i direktiv [förslag till NIS 2].

(4) *cybersäkerhet*: cybersäkerhet i den mening som avses i artikel 4.3 i direktiv [förslag till NIS 2].

(5) *högsta ledningsnivå*: en chef eller ett lednings- eller samordnings- och tillsynsorgan på den högsta administrativa nivån, med beaktande av styrningsarrangemangen på hög nivå inom varje unionsinstitution, unionsorgan eller unionsbyrå.

(6) *incident*: incident i den mening som avses i artikel 4.5 i direktiv [förslag till NIS 2].

(7) *betydande incident*: varje incident, såvida den inte har begränsad inverkan och sannolikt redan är välbekant i fråga om metod eller teknik.

(8) *större angrepp*: varje incident som kräver mer resurser än vad som finns att tillgå vid unionens institutioner, organ eller byråer som berörs och vid CERT-EU.

(9) *incidenthantering*: incidenthantering i den mening som avses i artikel 4.6 i direktiv [förslag till NIS 2].

(10) *cyberhot*: cyberhot i den mening som avses i artikel 2.8 i förordning (EU) 2019/881.

(11) *betydande cyberhot*: ett cyberhot med avsikt, tillfälle och förmåga att orsaka en betydande incident.

(12) *sårbarhet*: sårbarhet i den mening som avses i artikel 4.8 i direktiv [förslag till NIS 2].

(13) *betydande sårbarhet*: en sårbarhet som sannolikt kommer att leda till en betydande incident om den utnyttjas.

(14) *cybersäkerhetsrisk*: en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverks- och informationssystem.

(15) *gemensam cyberenhet*: en virtuell och fysisk plattform för samarbete för de olika cybersäkerhetsgrupperna i unionen, med fokus på operativ och teknisk samordning gentemot större gränsöverskridande cyberhot och incidenter i den mening som avses i kommissionens rekommendation av den 23 juni 2021.

(16) *baslinje för cybersäkerhet*: en uppsättning minimiregler för cybersäkerhet vilka nätverks- och informationssystem och deras operatörer och användare måste följa för att minimera cybersäkerhetsriskerna.

Kapitel II
ÅTGÄRDER FÖR EN HÖG GEMENSAM CYBERSÄKERHETSNIVÅ

Artikel 4
Riskhantering, styrning och kontroll

1. Varje unionsinstitution, unionsorgan och unionsbyrå ska inrätta en egen intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker (*ramen*) till stöd för entitetens uppdrag och utövande av sin institutionella autonomi. Arbetet ska övervakas av entitetens högsta ledningsnivå för att säkerställa en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker. Ramen ska ha införts senast den ... [15 månader efter denna förordnings ikraftträdande].

2. Ramen ska omfatta hela it-miljön för institutionen, organet eller byrån i fråga, inbegripet alla it-miljöer på plats, 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 it-miljön. Ramen ska ta hänsyn till driftskontinuitet och krishantering och ska beakta säkerheten i leveranskedjan samt hanteringen av mänskliga risker som skulle kunna påverka cybersäkerheten i unionsinstitutionen, unionsorganet eller unionsbyrån i fråga.

3. Varje unionsinstitutions, unionsorgans och unionsbyrås högsta ledningsnivå ska övervaka att deras organisation fullgör sina skyldigheter i fråga om hantering, styrning och kontroll av cybersäkerhetsrisker, utan att det påverkar det formella ansvaret för efterlevnad och riskhantering på andra ledningsnivåer inom respektive ansvarsområden.

4. Varje unionsinstitution, unionsorgan och unionsbyrå ska ha effektiva mekanismer för att säkerställa att en lämplig andel av it-budgeten spenderas på cybersäkerhet.

5. Varje unionsinstitution, unionsorgan och unionsbyrå ska utse en lokal cybersäkerhetsansvarig eller motsvarande funktion som ska fungera som dess gemensamma kontaktpunkt för alla aspekter av cybersäkerhet.

Artikel 5
Baslinje för cybersäkerhet

1. Varje unionsinstitutions, unionsorgans och unionsbyrås högsta ledningsnivå ska godkänna entitetens egna baslinje för cybersäkerhet för att hantera de risker som identifierats inom den ram som avses i artikel 4.1. Den ska göra detta för att stödja entitetens uppdrag och utövande av sin institutionella autonomi. Baslinjen för cybersäkerhet ska ha införts senast den [18 månader efter denna förordnings ikraftträdande] och ska omfatta de områden som förtecknas i bilaga I och de åtgärder som förtecknas i bilaga II.

2. Varje unionsinstitutions, unionsorgans och unionsbyrås högre ledning ska regelbundet genomgå särskild utbildning för att skaffa sig tillräckliga kunskaper och färdigheter för att kunna förstå och bedöma cybersäkerhetsrisker och rutiner för hantering av cybersäkerhet och deras inverkan på organisationens verksamhet.

Artikel 6
Mognadsbedömningar

Varje unionsinstitution, unionsorgan och unionsbyrå ska genomföra en mognadsbedömning av cybersäkerheten minst vart tredje år, omfattande alla delar av deras it-miljö enligt beskrivningen i artikel 4, med beaktande av relevanta vägledningar och rekommendationer som antagits i enlighet med artikel 13.

Artikel 7
Cybersäkerhetsplaner

1. Som en uppföljning av slutsatserna från mognadsbedömningen och med beaktande av de tillgångar och risker som identifierats i enlighet med artikel 4 ska varje unionsinstitutions, unionsorgans och unionsbyrås högsta ledningsnivå godkänna en cybersäkerhetsplan utan onödigt dröjsmål efter inrättandet av ramen för riskhantering, styrning och kontroll och baslinjen för cybersäkerhet. Planen ska syfta till att öka den berörda entitetens övergripande cybersäkerhet och ska därigenom bidra till att uppnå eller förbättra en hög gemensam cybersäkerhetsnivå vid alla unionens institutioner, organ och byråer. För att stödja entitetens uppdrag på grundval av dess institutionella autonomi ska planen åtminstone omfatta de områden som förtecknas i bilaga I, de åtgärder som förtecknas i bilaga II samt åtgärder som rör incidentberedskap, incidenthantering och återställning, såsom säkerhetsövervakning och loggning. Planen ska ses över minst vart tredje år efter de mognadsbedömningar som gjorts i enlighet med artikel 6.

2. Cybersäkerhetsplanen ska omfatta personalens roller och ansvar för dess genomförande.

3. Cybersäkerhetsplanen ska beakta alla tillämpliga vägledningar och rekommendationer som utfärdats av CERT-EU.

Artikel 8
Genomförande

1. När mognadsbedömningarna har slutförts ska unionens institutioner, organ och byråer överlämna dem till den interinstitutionella cybersäkerhetsstyrelsen. När säkerhetsplanerna har slutförts ska unionens institutioner, organ och byråer underrätta den interinstitutionella cybersäkerhetsstyrelsen om slutförandet. På styrelsens begäran ska de rapportera om särskilda aspekter av detta kapitel.

2. Vägledningar och rekommendationer som utfärdas i enlighet med artikel 13 ska stödja genomförandet av bestämmelserna i detta kapitel.

Kapitel III
INTERINSTITUTIONELL CYBERSÄKERHETSSTYRELSE

Artikel 9
Interinstitutionell cybersäkerhetsstyrelse

1. Härigenom inrättas en interinstitutionell cybersäkerhetsstyrelse (IICB).

2. IICB ska ansvara för att

   (a) övervaka unionens institutioners, organs och byråers 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 tre företrädare som av unionsbyråernas nätverk (EUAN) på förslag av dess rådgivande IKT-kommitté utses att företräda intressena för de byråer och organ som driver sin egen it-miljö samt en företrädare som utses av var och en av följande:

(a) Europaparlamentet.

(b) Europeiska unionens råd.

(c) Europeiska kommissionen.

(d) Europeiska unionens domstol.

(e) Europeiska centralbanken.

(f) Europeiska revisionsrätten.

(g) Europeiska utrikestjänsten.

(h) Europeiska ekonomiska och sociala kommittén.

(i) Europeiska regionkommittén.

(j) Europeiska investeringsbanken.

(k) Europeiska unionens cybersäkerhetsbyrå.

Ledamöterna får bistås av en suppleant. Ordföranden får bjuda in andra företrädare för de organisationer som förtecknas ovan eller för unionens andra institutioner, organ och byråer att delta i IICB:s möten utan rösträtt.

4. IICB ska själv anta sin arbetsordning.

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

6. IICB ska sammanträda på ordförandens initiativ, på begäran av CERT-EU eller på begäran av någon av dess ledamöter.

7. Varje ledamot av IICB ska ha en röst. IICB:s beslut ska fattas med enkel majoritet om inte annat föreskrivs i denna förordning. Ordföranden får inte rösta utom vid lika röstetal, då han eller hon får avge en utslagsröst.

8. IICB får agera genom ett förenklat skriftligt förfarande som inleds i enlighet med IICB:s 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.

9. CERT-EU:s chef, eller dennas suppleant, ska delta i IICB:s möten om inte IICB beslutar något annat.

10. IICB:s sekretariat ska tillhandahållas av kommissionen.

11. De företrädare som utsetts av EUAN på förslag av den rådgivande IKT-kommittén ska vidarebefordra IICB:s beslut till unionens byråer och gemensamma företag. Alla unionens byråer och organ ska ha rätt att med företrädarna eller IICB:s ordförande ta upp alla frågor som de anser att IICB bör uppmärksammas på.

12. IICB får agera genom ett förenklat skriftligt förfarande som inleds av ordföranden och som innebär att det relevanta beslutet ska anses vara godkänt inom den tidsfrist som fastställts av ordföranden, utom i de fall då en ledamot har invändningar.

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

Artikel 10
IICB:s uppgifter

Vid utövandet av sina uppgifter ska IICB särskilt

(a) granska alla rapporter som begärs från CERT-EU om hur unionens institutioner, organ och byråer genomför denna förordning,

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

(c) på grundval av ett förslag från CERT-EU:s chef godkänna CERT-EU:s tjänstekatalog,

(d) 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,

(e) på grundval av ett förslag från CERT-EU:s chef godkänna formerna för servicenivåavtal,

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

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

(h) godkänna samarbetsavtal, servicenivåavtal eller avtal mellan CERT-EU och andra entiteter i enlighet med artikel 17,

(i) inrätta så många tekniska rådgivande grupper som behövs för att bistå IICB i dess arbete, godkänna deras mandat och utse deras respektive ordförande.

Artikel 11
Kontroll av efterlevnad

IICB ska övervaka hur unionens institutioner, organ och byråer genomför denna förordning och antagna vägledningar, rekommendationer och uppmaningar till åtgärder. Om IICB konstaterar att unionens institutioner, organ eller byråer inte effektivt har tillämpat eller genomfört denna förordning eller vägledningar, rekommendationer och uppmaningar till åtgärder som utfärdats enligt denna förordning, får den, utan att det påverkar de interna förfarandena för unionsinstitutionen, unionsorganet och unionsbyrån i fråga,

(a) utfärda en varning; när det är nödvändigt med tanke på en tvingande cybersäkerhetsrisk ska varningens målgrupp begränsas på lämpligt sätt,

(b) rekommendera en relevant revisionstjänst att utföra en revision.

Kapitel IV
CERT-EU

Artikel 12
CERT-EU:s uppdrag och uppgifter

1. CERT-EU, det autonoma interinstitutionella cybersäkerhetscentrumet för alla unionens institutioner, organ och byråer, ska ha i uppdrag att bidra till säkerheten i alla unionens institutioners, organs och byråers icke-säkerhetsskyddsklassificerade it-miljö genom att ge dem råd om cybersäkerhet, hjälpa dem att förebygga, upptäcka, begränsa och hantera incidenter och genom att fungera som deras nav för utbyte om cybersäkerhetsinformation och samordning av incidenthantering.

2. CERT-EU ska utföra följande uppgifter för unionens institutioner, organ och byråer:

   (a) Stödja dem vid genomförandet av denna förordning och bidra till samordningen av tillämpningen av denna förordning genom de åtgärder som förtecknas i artikel 13.1 eller genom ad hoc-rapporter som IICB begär.

   (b) Stödja dem med 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 16 och 17.

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

   (e) Rapportera om de cyberhot som unionens institutioner, organ och byråer utsätts för och bidra till EU:s cybersituationsmedvetenhet.

3. CERT-EU ska bidra till den gemensamma cyberenheten som byggts i enlighet med kommissionens rekommendation av den 23 juni 2021, bland annat på följande områden:

(a) Beredskap, incidentsamordning, informationsutbyte och krishantering på teknisk nivå i ärenden som rör unionens institutioner, organ och byråer.

(b) Operativt samarbete med nätverket av enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*), inbegripet om ömsesidigt bistånd, och det bredare cybersäkerhetssamfundet.

(c) Underrättelser om cyberhot, inbegripet situationsmedvetenhet.

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

4. CERT-EU ska inleda ett strukturerat samarbete med Europeiska unionens cybersäkerhetsbyrå om kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881.

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

(a) Andra tjänster som stöder cybersäkerheten i unionens institutioners, organs och byråers it-miljö än de som avses i punkt 2, på grundval av servicenivåavtal och förutsatt att det finns tillgängliga resurser.

(b) Andra tjänster som stöder unionens institutioners, organs och byråers cybersäkerhetsinsatser eller cybersäkerhetsprojekt än de som skyddar deras it-miljö, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

(c) Tjänster som stöder säkerheten i it-miljön hos andra organisationer än unionens institutioner, organ och byråer vilka har ett nära samarbete med unionens institutioner, organ och byråer, till exempel genom att ha tilldelats uppgifter och ansvar enligt unionsrätten, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

6. CERT-EU får anordna cybersäkerhetsövningar eller rekommendera deltagande i befintliga övningar, i tillämpliga fall i nära samarbete med Europeiska unionens cybersäkerhetsbyrå, för att testa cybersäkerhetsnivån hos unionens institutioner, organ och byråer.

7. CERT-EU får stödja unionens institutioner, organ och byråer när det gäller incidenter i säkerhetsskyddsklassificerade it-miljöer om den berörda avtalsparten uttryckligen begär detta.

Artikel 13

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 institutioner, organ och byråer uppmanas att vidta inom en fastställd tidsram,

(b) förslag till IICB till vägledningar som riktar sig till alla eller en del av unionens institutioner, organ och byråer,

(c) förslag till IICB till rekommendationer som riktar sig till enskilda unionsinstitutioner, unionsorgan och unionsbyråer.

2. Vägledningar och rekommendationer kan omfatta

(a) former för eller förbättringar av riskhanteringen för cybersäkerhet och baslinjen för cybersäkerhet,

(b) former för mognadsbedömningar och cybersäkerhetsplaner, och

(c) när så är lämpligt, användning av gemensam teknik, arkitektur och tillhörande bästa praxis i syfte att uppnå interoperabilitet och gemensamma standarder i den mening som avses i artikel 4.10 i direktiv [förslag till NIS 2].

3. IICB får anta vägledningar eller rekommendationer på CERT-EU:s förslag.

4. IICB får ge CERT-EU i uppdrag att utfärda, dra tillbaka eller ändra ett förslag till vägledningar eller rekommendationer, eller en uppmaning till åtgärder.

Artikel 14
CERT-EU:s chef

CERT-EU:s chef ska regelbundet lämna rapporter till IICB och IICB:s ordförande om CERT-EU:s resultat, finansiell planering, inkomster, genomförande av budgeten, servicenivåavtal och skriftliga avtal som ingåtts, samarbete med motparter och partner samt personalens uppdrag, inbegripet de rapporter som avses i artikel 10.1.

Artikel 15
Ekonomiska frågor och personalfrågor

1. Kommissionen ska, efter att ha fått IICB:s enhälliga godkännande, utnämna CERT-EU:s chef. IICB ska rådfrågas i alla skeden av förfarandet före utnämningen av CERT-EU:s chef, särskilt när det gäller att utarbeta meddelanden om den lediga tjänsten, granska ansökningar och utse uttagningskommittéer med avseende på tjänsten.

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

3. CERT-EU:s uppgifter och verksamhet, inbegripet tjänster som tillhandahålls av CERT-EU i enlighet med artiklarna 12.2, 12.3, 12.4, 12.6 och 13.1 till unionens institutioner, organ och byråer som finansieras genom den rubrik i den fleråriga budgetramen som är avsedd för europeisk offentlig administration, ska finansieras genom en särskild budgetpost i kommissionens budget. De tjänster som öronmärkts för CERT-EU ska anges i en fotnot till kommissionens tjänsteförteckning.

4. Unionens institutioner, organ och byråer, andra än de som avses i punkt 3, ska lämna ett årligt ekonomiskt bidrag till CERT-EU för att täcka de tjänster som CERT-EU

tillhandahåller i enlighet med punkt 3. Respektive bidrag ska baseras på riktlinjer som ges av IICB och som varje entitet 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 som inkomster avsatta för särskilda ändamål i enlighet med artikel 21.3 c i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046[8].

5. Kostnaderna för de uppgifter som anges i artikel 12.5 ska återkrävas från unionens institutioner, organ och byråer som tar emot CERT-EU-tjänsterna. Inkomsterna ska avsättas för de budgetposter som stöder kostnaderna.

Artikel 16

CERT-EU:s samarbete med motparter i medlemsstaterna

1. CERT-EU ska samarbeta och utbyta information med nationella motparter i medlemsstaterna, bland annat CERT:ar, nationella cybersäkerhetscentrum, CSIRT-enheter och de gemensamma kontaktpunkter som avses i artikel 8 i direktiv [förslag till NIS 2], om cyberhot, sårbarheter och incidenter, om möjliga motåtgärder och om alla frågor som är relevanta för att förbättra skyddet av it-miljön vid unionens institutioner, organ och byråer, inbegripet genom det CSIRT-nätverk som avses i artikel 13 i direktiv [förslag till NIS 2].

2. CERT-EU får utbyta incidentspecifik information med nationella motparter i medlemsstaterna för att underlätta upptäckt av liknande cyberhot eller incidenter utan den berörda avtalspartens samtycke. CERT-EU får utbyta incidentspecifik information som avslöjar identiteten på målet för cybersäkerhetsincidenten endast med den berörda avtalspartens samtycke.

Artikel 17

CERT-EU:s samarbete med motparter utanför medlemsstaterna

1. CERT-EU får samarbeta med motparter utanför medlemsstaterna, 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, inbegripet inom ramar där motparter utanför EU samarbetar med nationella motparter i medlemsstaterna, ska CERT-EU inhämta förhandsgodkännande från IICB.

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

---

[8] 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).

3. CERT-EU får, med samtycke från den avtalspart som berörs av en incident, lämna information om incidenten till partner som kan bidra till dess analys.

Kapitel V
SAMARBETS- OCH RAPPORTERINGSKRAV

Artikel 18
Informationshantering

1. CERT-EU och unionens institutioner, organ och byråer ska respektera tystnadsplikt i enlighet med artikel 339 i fördraget om Europeiska unionens funktionssätt eller likvärdiga tillämpliga ramar.

2. Bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 1049/2001[9] ska tillämpas på allmänhetens begäranden om tillgång till handlingar som innehas av CERT-EU, inbegripet skyldigheten enligt den förordningen att samråda med unionens övriga institutioner, organ och byråer när en begäran rör deras handlingar.

3. Behandling av personuppgifter enligt denna förordning ska omfattas av Europaparlamentets och rådets förordning (EU) 2018/1725.

4. CERT-EU:s och unionens institutioners, organs och byråers hantering av information ska stämma överens med reglerna i [förslag till förordning om informationssäkerhet].

5. Kommissionens säkerhetsdirektorat och IICB:s ordförande ska utan onödigt dröjsmål informeras om alla kontakter som nationella säkerhets- och underrättelsetjänster initierar eller söker med CERT-EU.

Artikel 19
Delningsskyldigheter

1. För att CERT-EU ska kunna samordna sårbarhetshantering och incidenthantering får centrumet begära att unionens institutioner, organ och byråer lämnar information från sina respektive it-systeminventarier som är relevant för CERT-EU:s stöd. Den institution eller byrå eller det organ som mottar begäran ska utan onödigt dröjsmål översända den begärda informationen och eventuella senare uppdateringar.

2. Unionens institutioner, organ och byråer ska, på CERT-EU:s begäran och utan onödigt dröjsmål, förse centrumet med digital information som skapats genom användning av elektroniska enheter som är inblandade i respektive incident. CERT-EU kan ytterligare klargöra vilka typer av sådan digital information som behövs för situationsmedvetenhet och incidenthantering.

3. CERT-EU får utbyta incidentspecifik information som avslöjar identiteten på den unionsinstitution, det unionsorgan eller den unionsbyrå som berörs av incidenten

[9] 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).

endast med den entitetens samtycke. CERT-EU får utbyta incidentspecifik information som avslöjar identiteten på målet för cybersäkerhetsincidenten endast med samtycke från den entitet som berörs av incidenten.

4. Delningsskyldigheterna ska inte omfatta säkerhetsskyddsklassificerade EU-uppgifter och uppgifter som unionens institutioner, organ eller byråer har mottagit från en medlemsstats säkerhets- eller underrättelsetjänst eller brottsbekämpande organ på det uttryckliga villkoret att de inte kommer att delas med CERT-EU.

Artikel 20
Underrättelseskyldigheter

1. Alla unionens institutioner, organ och byråer ska lämna en första underrättelse till CERT-EU om betydande cyberhot, betydande sårbarheter och betydande incidenter utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter det att de fått kännedom om dem.

   I vederbörligen motiverade fall och i samförstånd med CERT-EU får unionsinstitutionen, unionsorganet eller unionsbyrån i fråga avvika från den tidsfrist som anges i föregående punkt.

2. Unionens institutioner, organ och byråer ska utan onödigt dröjsmål underrätta CERT-EU om lämpliga tekniska detaljer om cyberhot, sårbarheter och incidenter som möjliggör upptäckt, incidenthantering eller riskreducerande åtgärder. Underrättelsen ska i förekommande fall innehålla

   (a) relevanta indikatorer på kompromettering,

   (b) relevanta mekanismer för upptäckt,

   (c) potentiella effekter,

   (d) relevanta riskreducerande åtgärder.

3. CERT-EU ska varje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade data om betydande cyberhot, betydande sårbarheter och betydande incidenter om vilka underrättelse lämnats i enlighet med punkt 1.

4. IICB får utfärda vägledningar eller rekommendationer om formerna för och innehållet i underrättelsen. CERT-EU ska sprida lämpliga tekniska detaljer för att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder hos unionens institutioner, organ och byråer.

5. Underrättelseskyldigheterna ska inte omfatta säkerhetsskyddsklassificerade EU-uppgifter och uppgifter som unionens institutioner, organ eller byråer har mottagit från en medlemsstats säkerhets- eller underrättelsetjänst eller brottsbekämpande organ på det uttryckliga villkoret att de inte kommer att delas med CERT-EU.

Artikel 21

Samordning av incidenthantering och samarbete vid betydande incidenter

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

   (a) unionens institutioner, organ och byråer,

   (b) de motparter som avses i artiklarna 16 och 17.

2. CERT-EU ska främja unionens institutioners, organs och byråers samordning av incidenthantering, genom bland annat

   (a) bidrag till konsekvent extern kommunikation,

   (b) ömsesidigt bistånd,

   (c) optimal användning av operativa resurser,

   (d) samordning med andra krishanteringsmekanismer på unionsnivå.

3. CERT-EU ska stödja unionens institutioner, organ och byråer när det gäller situationsmedvetenhet om cyberhot, sårbarheter och incidenter.

4. IICB ska utfärda riktlinjer 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.

Artikel 22

Större angrepp

1. CERT-EU ska samordna unionens institutioners, organs och byråers hantering av större angrepp. Centrumet ska föra en förteckning över den tekniska expertis som skulle behövas för incidenthantering i händelse av sådana angrepp.

2. Unionens institutioner, organ och byråer 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.

3. Med de berörda unionsinstitutionernas, unionsorganens och unionsbyråernas godkännande får CERT-EU också anlita experter från den förteckning som avses i punkt 2 för att bidra till hanteringen av ett större angrepp i en medlemsstat, i enlighet med den gemensamma cyberenhetens operativa förfaranden.

Kapitel VI
SLUTBESTÄMMELSER

Artikel 23
Inledande omfördelning av budgeten

Kommissionen ska föreslå en omfördelning av personal och ekonomiska resurser från unionens berörda institutioner, organ och byråer till kommissionens budget. Omfördelningen ska få verkan samtidigt som den första budget som antas efter det att denna förordning träder i kraft.

Artikel 24
Översyn

1. IICB ska med bistånd av CERT-EU regelbundet rapportera till kommissionen om genomförandet av denna förordning. IICB får också rekommendera kommissionen att föreslå ändringar av denna förordning.

2. Kommissionen ska rapportera om genomförandet av denna förordning till Europaparlamentet och rådet senast 48 månader efter denna förordnings ikraftträdande och därefter vart tredje år.

3. Kommissionen ska utvärdera hur denna förordning fungerar och rapportera till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén tidigast fem år efter dagen för ikraftträdandet.

Artikel 25
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 Bryssel den

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

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

1.2. Berörda politikområden

1.3. Förslaget eller initiativet avser

1.4. Mål

1.4.1. Allmänt/allmänna mål:

1.4.2. Specifikt/specifika mål:

1.4.3. Verkan eller resultat som förväntas

1.4.4. Prestationsindikatorer

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

1.5.3. Erfarenheter från tidigare liknande åtgärder

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

3.2.2. Beräknad output som finansieras med driftsanslag

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

Förslag till Europaparlamentets och rådets förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

1.2. Berörda politikområden

Europeisk offentlig förvaltning

Förslaget gäller åtgärder som säkerställer en hög gemensam cybersäkerhetsnivå inom unionens institutioner, organ och byråer

1.3. Förslaget eller initiativet avser

☑en ny åtgärd

☐ en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[10]

☐ en förlängning av en befintlig åtgärd

☑ en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd

1.4. Mål

1.4.1. Allmänt/allmänna mål:

– Att inrätta en ram för att säkerställa en hög gemensam cybersäkerhetsnivå inom unionens institutioner, organ och byråer

– Att tillhandahålla en ny rättslig grund för CERT-EU för att stärka dess mandat och finansiering

1.4.2. Specifikt/specifika mål:

(1) Att fastställa skyldigheter för unionens institutioner, organ och byråer att inrätta en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker

(2) Att fastställa skyldigheter för unionens institutioner, organ och byråer att rapportera om sin ram för hantering, styrning och kontroll av cybersäkerhetsrisker samt om cybersäkerhetsincidenter

[10] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

(3) Att fastställa regler om organisationen och driften av Cybersäkerhetscentrumet för unionens institutioner, organ och byråer (CERT-EU) och om organisationen och driften av den interinstitutionella cybersäkerhetsstyrelsen (IICB)

(4) Att bidra till den gemensamma cyberenheten

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

– Interna ramar för hantering, styrning och kontroll av cybersäkerhetsrisker, baslinjer för cybersäkerhet, regelbundna mognadsbedömningar och cybersäkerhetsplaner vid unionens institutioner, organ och byråer – Förbättrad cybersäkerhetsresiliens och incidenthanteringskapacitet vid unionens institutioner, organ och byråer – Modernisering av CERT-EU – Bidrag till den gemensamma cyberenheten

1.4.4. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

– Ramar och baslinjer, regelbundna mognadsbedömningar och cybersäkerhetsplaner som genomförs inom unionens institutioner, organ och byråer – Förbättrad hantering av incidenter – Ökad medvetenhet om cybersäkerhetsrisker på högsta ledningsnivå vid unionens institutioner, organ och byråer – Fastställda IKT-säkerhetsutgifter som en procentandel av de totala IKT-utgifterna – Starkt ledarskap för IICB och CERT-EU – Ökat informationsutbyte mellan unionens institutioner, organ och byråer och med relevanta organ och intressenter i EU – Ökat cybersäkerhetssamarbete med berörda organ och intressenter i EU, via CERT-EU och Enisa

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet.

Förslaget syftar till att öka cyberresiliensen hos unionens institutioner, organ och byråer, att minska skillnaderna i resiliens mellan dessa entiteter och att förbättra den

gemensamma situationsmedvetenheten och den kollektiva förmågan att förbereda sig och reagera.

Förslaget är helt konsekvent och förenligt med andra relaterade initiativ, framför allt förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 [förslag till NIS 2].

Förslaget är en viktig del av strategin för EU:s säkerhetsunion och EU:s strategi för cybersäkerhet för ett digitalt decennium.

Europeiska kommissionen planerar att lägga fram förslaget till förordningen i oktober 2021. Europaparlamentet och rådet förväntas anta förordningen 2022 och bestämmelserna kommer att börja tillämpas från och med förordningens ikraftträdande. De ekonomiska och personalrelaterade konsekvenser som beskrivs i denna finansieringsöversikt för rättsakt förväntas börja 2023. En förberedande period inleddes redan 2021, men de förberedande åtgärderna under 2021 och 2022 omfattas inte av förslagets finansiella konsekvenser.

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Skäl för åtgärder på europeisk nivå (ex ante)

Mellan 2019 och 2021 har antalet betydande incidenter som påverkat unionens institutioner, organ och byråer och som skapats av APT-aktörer ökat dramatiskt. Under första halvåret 2021 tillstötte lika många betydande incidenter som under hela 2020. Detta återspeglas också i att CERT-EU analyserade tre gånger så många kriminaltekniska bilder (ögonblicksbilder av innehållet i berörda system eller enheter) 2020 jämfört med 2019, medan antalet betydande incidenter har ökat mer än tiofalt sedan 2018.

Nivåerna av cybersäkerhetsmognad varierar avsevärt från en entitet till en annan[11]. Denna förordning säkerställer att alla unionens institutioner, organ och byråer kommer att införa en baslinje av säkerhetsåtgärder och samarbeta med varandra för att unionens administration ska fungera på ett öppet och effektivt sätt.

De system som ska bevaras omfattas av autonomin för unionens institutioner, organ och byråer och drivs av dem; de föreslagna åtgärderna skulle inte kunna vidtas av medlemsstaterna.

1.5.3. Erfarenheter från tidigare liknande åtgärder

NIS-direktivet var det första övergripande instrument för den inre marknaden som syftade till att förbättra resiliensen hos nätverk och system i unionen mot cybersäkerhetsrisker. Sedan det trädde i kraft 2016 har det i hög grad bidragit till att

[11] Referens: [*ECA Special Report on cybersecurity at the Union institutions, bodies and agencies*].

höja den gemensamma cybersäkerhetsnivån i medlemsstaterna. Förslaget till NIS2-direktivet syftar till att ytterligare förbättra dessa åtgärder.

Förordningen syftar till att föreskriva liknande åtgärder för unionens institutioner, organ och byråer.

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Förslaget är förenligt med den fleråriga budgetramen och är en viktig del av strategin för EU:s säkerhetsunion och EU:s strategi för cybersäkerhet för ett digitalt decennium.

Enligt förslaget ska åtgärder för en hög gemensam cybersäkerhetsnivå tillämpas på unionens institutioner, organ och byråer. Förslaget är förenligt med förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 [förslag till NIS 2].

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

CERT-EU:s förvaltning av uppgifterna kräver särskilda profiler och medför en ytterligare arbetsbörda som inte kan absorberas utan någon ökning av personalresurserna och de ekonomiska resurserna.

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

☐ **begränsad varaktighet**

– ☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ

– ☐ budgetkonsekvenser från och med YYYY till och med YYYY för åtagandebemyndiganden och från och med YYYY till och med YYYY för betalningsbemyndiganden.

☑ **obegränsad varaktighet**

– Budgetkonsekvenserna torde börja med den första budget som antas efter det att förordningen har trätt i kraft. En omfördelning av resurser från unionens institutioner och viktigaste organ till kommissionen skulle ske under det första året, som betraktas som ett övergångsår; denna och annan (om)fördelning av resurser kommer att ske inom ramen för de årliga budgetarna. Om förordningen antas 2022 kommer budgetåret 2023 att vara övergångsperioden, medan den genomförs fullt ut 2024.

1.7. Planerad metod för genomförandet[12]

☑ **Direkt förvaltning** som sköts av kommissionen och av varje unionsinstitution, unionsorgan och unionsbyrå

– ☑ av dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

– ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐ EIB och Europeiska investeringsfonden

– ☐ organ som avses i artiklarna 70 och 71 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de lämnar tillräckliga ekonomiska garantier

[12] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som lämnar tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

Anmärkningar

När det gäller tillämpningen av de administrativa och finansiella förfarandena handlar CERT-EU under kommissionens överinseende.

Ytterligare medel som härrör från utkastet till förordning:

Genomförandet av artiklarna 12 och 13 i utkastet till förordning leder till en utökad tjänstekatalog med ytterligare baslinjetjänster. Vid fullskalig verksamhet kommer följande ytterligare resurser att behövas (fram till slutet av den fleråriga budgetramen 2027): 21 heltidsekvivalenter och 14,05 miljoner EUR.

Fördelningen av de ytterligare budgetmedlen mellan de olika uppgifterna ser ut på följande sätt:

(a) För utförandet av de uppgifter för unionens institutioner, organ och byråer som anges i artikel 12.2 a, b, c och e: 13,75 heltidsekvivalenter och 11,275 miljoner EUR.

(b) För utförandet av de uppgifter som anges i artikel 12.3 (bidrag till den gemensamma cyberenheten): 2 heltidsekvivalenter och 381 000 EUR.

(c) För utförandet av de uppgifter som anges i artikel 12.4 (strukturerat samarbete med Enisa): 0,25 heltidsekvivalenter och 236 000 EUR.

(d) För utförandet av de uppgifter som anges i artikel 12.6 (cybersäkerhetsövningar): 0,25 heltidsekvivalenter och 79 000 EUR.

(e) För utförandet av de uppgifter som anges i artiklarna 12.2 d och 13 (analys och rapportering om genomförandet av förordningen, utarbetande av vägledningar, rekommendationer och uppmaningar till åtgärder): 3,75 heltidsekvivalenter och 2,079 miljoner EUR.

(f) För utförandet av uppgifter till stöd för den interinstitutionella cybersäkerhetsstyrelsens (IICB) sekretariat: 1 heltidsekvivalent.

Översikt över nuvarande resurser och övergång till full verksamhet:

I september 2021 hade CERT-EU följande resurser:

- Fasta tjänster och utstationeringar: 14 heltidsekvivalenter.

- Kontraktsanställda som finansieras genom servicenivåavtal: 24 heltidsekvivalenter.

- Totalt 38 heltidsekvivalenter.

CERT-EU:s budget för 2020 var följande: 250 000 EUR enligt kommissionens budget, 3,5 miljoner EUR genom inkomster avsatta för särskilda ändamål från servicenivåavtal. Totalt: 3,75 miljoner EUR. Detta utgjorde CERT-EU:s hela budget för utbildning, maskinvara, programvara, tjänsteresor, stöd, kontraktsanställda och konferenser.

När förordningen har trätt i kraft planeras CERT-EU:s framtida resurser vara följande:

- Fasta tjänster: 34 heltidsekvivalenter.

- Kontraktsanställda: 15 heltidsekvivalenter.

- Totalt 49 heltidsekvivalenter, alltså en nettoökning med 11 heltidsekvivalenter.

Förändringen i förhållandet mellan fasta tjänster och kontraktsanställda är en lösning på den ständiga svårigheten att anställa och behålla högre cybersäkerhetspersonal på grund av bristen på dem på arbetsmarknaden.

Dessutom kommer 1 kontraktsanställd (heltidsekvivalent) att krävas inom kommissionens generaldirektorat för informationsteknik för att stödja den interinstitutionella cybersäkerhetsstyrelsen (IICB).

Totalt kommer det alltså att krävas ytterligare 21 heltidsekvivalenter för att genomföra förordningen (20 heltidsekvivalenter för CERT-EU och 1 för kommissionens generaldirektorat för informationsteknik). Detta kommer att kompenseras genom en parallell minskning med 9 kontraktsanställda heltidsekvivalenter inom CERT-EU som tidigare finansierades genom inkomster avsatta för särskilda ändamål från servicenivåavtal.

CERT-EU:s icke-personalrelaterade budget kommer 2024 efter övergångsperioden att täcka de uppgifter som anges ovan under a–e och finansieringen planeras ske enligt följande:

- 8,921 miljoner EUR per år från unionsinstitutioner som finansieras under rubrik 7 i unionens budget.

- 2,459 miljoner EUR per år från unionens institutioner, organ och byråer som finansieras under rubrikerna 1–6 i unionens budget.

- 2,670 miljoner EUR från unionens självfinansierade institutioner, organ och byråer.

- CERT-EU:s totala budget: 14,05 miljoner EUR.

De uppgifter som anges i artikel 12.5 beskrivs inte i tjänstekatalogen, eftersom de är avgiftsbelagda tjänster. De är kompletterande, i huvudsak tillfälliga tjänster till relativt låga belopp och kostnaderna för dessa tjänster kommer att återkrävas från mottagarna av tjänsterna genom servicenivåavtal eller skriftliga avtal.

När det gäller bidrag till CERT-EU:s personal: unionens institutioner och huvudorgan ska bidra med en skälig andel som står i proportion till organisationens respektive andel av de fasta AD-tjänsterna. Det återstår att se om ECB och EIB också kan bidra med en skälig andel genom utstationering av fast anställda.

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Kommissionen kommer med hjälp av IICB och CERT-EU att regelbundet se över hur förordningen fungerar och rapportera till Europaparlamentet och rådet, första gången senast 48 månader efter det att denna förordning har trätt i kraft och därefter vart tredje år.

De datakällor som används för översynerna kommer främst från IICB och CERT-EU. Dessutom kan särskilda datainsamlingsverktyg användas vid behov, t.ex. enkäter från unionens institutioner, organ och byråer, Enisa eller CSIRT-nätverket.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Åtgärder som följer av förordningen kommer att förvaltas inom varje unionsinstitution, unionsorgan och unionsbyrå i enlighet med deras tillämpliga regler och förordningar.

Den administrativa och ekonomiska förvaltningen av CERT-EU:s verksamhet ingår i kommissionens administration och följer dess tillämpliga förvaltnings- och genomförandemekanismer, betalningsvillkor och kontroller.

Kommissionens internrevisor har samma befogenheter gentemot CERT-EU som gentemot kommissionens avdelningar.

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

Mycket låg risk, eftersom CERT-EU redan är administrativt knutet till generaldirektoratet för informationsteknik som en kommissionsarbetsgrupp, och IICB bygger på den nuvarande styrelsen för CERT-EU. Ekosystemet för ekonomisk förvaltning och intern kontroll finns alltså redan.

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Förfaranden för upphandling, ekonomisk förvaltning och kontroll finns redan och är väl testade. Kontrollernas kostnadseffektivitet och risknivåerna för fel motsvarar de som gäller för varje unionsinstitution, unionsorgan eller unionsbyrå och kommissionens sådana för CERT-EU:s verksamhet.

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

Kommissionens system för ekonomisk förvaltning och intern kontroll gäller för CERT-EU:s verksamhet.

För att bekämpa bedrägeri, korruption och andra rättsstridiga handlingar tillämpas bestämmelserna i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) oinskränkt.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgifter	Bidrag			
	Nummer	Diff./Icke-diff[13].	från Efta-länder[14]	från kandidatländer[15]	från tredjeländer	enligt artikel 21.2 b i budgetförordningen
1 till 6	Budgetposter som omfattar unionens bidrag till decentraliserade byråer och organ	Diff.	NEJ	NEJ	NEJ	NEJ
7	Budgetposter för personalens löner, it-utgifter och andra administrativa utgifter i de olika avsnitten i EU:s budget	Icke-diff.	NEJ	NEJ	NEJ	NEJ

- Nya budgetrubriker som föreslås

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	Nummer	Diff./Icke-diff.	från Efta-länder	från kandidat-länder	från tredjeländer	enligt artikel 21.2 b i budgetförordningen
	Inga		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

[13] Diff. = differentierade anslag / Icke-diff. = icke-differentierade anslag.
[14] Efta: Europeiska frihandelssammanslutningen.
[15] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☑ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	1 till 6	Rubriker som omfattar bidrag till decentraliserade byråer och organ

GD: flera			År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT**
○ Driftsanslag								
Budgetposter som omfattar unionens bidrag till decentraliserade byråer (xx 10 xx xx)[16]	Åtaganden	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program[17]								
Budgetrubrik		(3)						
TOTALA anslag För GD: flera	Åtaganden	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	=2a+2b	2,459	2,459	2,459	2,459	2,459	12,293

16 Enligt den officiella kontoplanen.

17 Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

		+3						

○ TOTALA driftsanslag	Åtaganden	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		(6)						
TOTALA anslag för RUBRIKERNA 1–6 i den fleråriga budgetramen	Åtaganden	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Upprepa avsnittet ovan om flera rubriker avseende driftsanslag i budgetramen påverkas av förslaget eller initiativet:

○ TOTALA driftsanslag (alla rubriker avseende driftsanslag)	Åtaganden	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program (alla driftsrelaterade rubriker)		(6)						
TOTALA anslag för RUBRIKERNA 1–6 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalningar	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Rubrik i den fleråriga budgetramen	7	”Administrativa utgifter”

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansieringsöversikt för rättsakt (bilaga V till de interna bestämmelserna), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		År **2023**	År **2024**	År **2025**	År **2026**	**År 2027**	**TOTALT**
GD: Informationsteknik (CERT-EU)							
○ Personalresurser		1,184	2,126	2,754	3,225	3,225	12,514
○ Övriga administrativa utgifter		7,938	8,921	8,921	8,921	8,921	43,622
TOTALT GD Informationsteknik (CERT-EU)	Anslag	9,122	11,047	11,675	12,146	12,146	56,136

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	9,122	11,047	11,675	12,146	12,146	**56,136**

Miljoner euro (avrundat till tre decimaler)

		År 2023	År 2024	År 2025	År 2026	År 2027	**TOTALT**
TOTALA anslag för RUBRIKERNA 1–7 i den fleråriga budgetramen (*)	Åtaganden	11,581	13,506	14,134	14,605	14,605	68,429
	Betalningar	11,581	13,506	14,134	14,605	14,605	68,429

(*) Bidragen från unionens självfinansierade institutioner, organ och byråer uppskattas till 2,670 miljoner EUR per år (13,350 miljoner EUR totalt för de fem åren). Bidragen kommer att utgöra inkomster avsatta för särskilda ändamål för CERT-EU. Tabellerna ovan innehåller endast den beräknade totala inverkan på unionens budget och inkluderar inte dessa bidrag.

3.2.2. Beräknad output som finansieras med driftsanslag

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Ange mål och output			År **n**		År **n+1**		År **n+2**		År **n+3**		För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**	
	OUTPUT																	
⇩	Typ[18]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[19]…																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Output																		
Delsumma för specifikt mål nr 2																		
TOTALT																		

[18] Output som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

[19] Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– ☑ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År 2023	År 2024	År 2025	År 2026	År 2027	**TOTALT**
RUBRIK 7 i den fleråriga budgetramen						
Personalresurser						
Fast anställd personal (lönegrad AD)	1,099	2,041	2,669	3,14	3,14	12,089
Kontraktsanställda	0,085	0,085	0,085	0,085	0,085	0,425
Övriga administrativa utgifter	7,938	8,921	8,921	8,921	8,921	43,622
Delsumma för RUBRIK 7 i den fleråriga budgetramen	9,122	11,047	11,675	12,146	12,146	56,136

Utanför RUBRIK 7[20] i den fleråriga budgetramen						
Personalresurser						
Övriga utgifter av administrativ natur						
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen						

TOTALT	9,122	11,047	11,675	12,146	12,146	56,136

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av anslag inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

[20] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.1. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☑ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

		År 2023	År 2024	År 2025	År 2026	År 2027		
O Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		7	13	17	20	20		
20 01 02 03 (vid delegationer)								
01 01 01 01 (indirekta forskningsåtgärder)								
01 01 01 11 (direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
O Extern personal (i heltidsekvivalenter)[21]								
20 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)		1	1	1	1	1		
20 02 03 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 xx **yy zz** [22]	- vid huvudkontoret							
	- vid delegationer							
01 01 01 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)								
01 01 01 12 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT		**8**	**14**	**18**	**21**	**21**		

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	Tjänstemän kommer att genomföra CERT-EU:s uppgifter och verksamhet i enlighet med förordningen, särskilt kapitlen IV och V.
Extern personal	Den kontraktsanställda kommer att bistå den interinstitutionella cybersäkerhetsstyrelsen med sekretariatsuppgifter.

[21] [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

[22] Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

3.2.4. Förenlighet med den gällande fleråriga budgetramen

Förslaget/initiativet

– ☑ kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen.

Förklara i förekommande fall vilka omfördelningar som krävs, och ange berörda budgetrubriker och motsvarande belopp. Bifoga en Excel-tabell om det gäller en större omfördelning.

– ☐ kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen.

Beskriv vad som krävs, ange berörda rubriker och budgetrubriker, motsvarande belopp och de instrument som är föreslagna för användning.

– ☐ kräver en översyn av den fleråriga budgetramen.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt de motsvarande beloppen.

3.2.5. Bidrag från tredje part

Förslaget/initiativet

– ☑ innehåller inga bestämmelser om samfinansiering från tredje parter[23]

– ☐ innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **n**[24]	År **n+1**	År **n+2**	År **n+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilket organ som deltar i samfinansieringen								
TOTALA anslag som tillförs genom samfinansiering								

[23] De inkomster avsatta för särskilda ändamål som härrör från sporadiskt tillhandahållande av tjänster till organisationer som inte är avtalsparter enligt artikel 12.5 c har inte uppskattats eftersom de torde vara marginella.

[24] Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

3.3. Beräknad inverkan på inkomsterna

– ☑ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på andra inkomster

– ange om inkomsterna har avsatts för utgiftsposter☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[25]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

[25] Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.