Svar från CERT-EU, CERT-EU:s styrelseordförande och Enisa på Europeiska revisionsrättens särskilda rapport om cybersäkerheten vid EU:s institutioner, organ och byråer

1. Sammanfattning

Mot bakgrund av den ständigt föränderliga it-hotbilden har cybersäkerhet blivit en ytterst viktig och kritisk faktor för EU:s institutioner, organ och byråer, vilka har blivit föremål för allt fler mycket sofistikerade cyberattacker under de senaste åren. Inom ramen för sina mandat kan både Enisa och CERT-EU förse EU:s institutioner, organ och byråer med värdefullt stöd när det gäller cybersäkerhet på olika nivåer. Europeiska kommissionens förslag till förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid EU:s institutioner, organ och byråer är ett viktigt instrument i detta sammanhang – ett instrument som Enisa, CERT-EU och CERT-EU:s styrelseordförande uttrycker sitt starka stöd till.

I detta syfte välkomnar Enisa, CERT-EU och CERT-EU:s styrelseordförande den särskilda rapporten om cybersäkerheten vid EU:s institutioner, organ och byråer, som Europeiska revisionsrätten ger ut vid ett mycket lägligt tillfälle för att ta itu med beredskapen hos EU:s institutioner, organ och byråer som helhet. I rapporten framhålls tydligt de centrala roller som Enisa och CERT-EU kan ha i detta sammanhang. Behovet av ytterligare resurser och konkreta riktade åtgärder för att förbättra cybersäkerhetsläget för EU:s institutioner, organ och byråer beskrivs också i rapporten.

Mot denna bakgrund stöder Enisa, CERT-EU och CERT-EU:s styrelseordförande de huvudsakliga iakttagelserna och rekommendationerna i rapporten, som också tar hänsyn till kommissionens lagstiftningsförslag på områdena cybersäkerhet och informationssäkerhet för EU:s institutioner, organ och byråer.

Kommentarerna i nästa avsnitt syftar till att kasta ytterligare ljus över vissa områden i rapporten, särskilt när det gäller relevant arbete som redan utförts av Enisa och/eller CERT-EU, samt de åtgärder som Enisa och/eller CERT-EU har planerat, i synnerhet på området kapacitetsuppbyggnad för EU:s institutioner, organ och byråer. När det gäller rekommendationerna godtar Enisa och CERT-EU rekommendation 3 (om att öka CERT-EU:s och Enisas fokus på de EU-institutioner, EU-organ och EU-byråer som har en lägre

mognadsgrad), som riktar sig särskilt till dem.

2. De viktigaste iakttagelserna

Enisa och CERT-EU ställer sig bakom revisionsrättens viktigaste iakttagelser. Vi gör dock några förtydliganden nedan, som framför allt rör de befintliga åtgärder som vidtagits av Enisa och/eller CERT-EU och de planer som redan har slagits fast för kommande verksamhet.

Punkt 49

När det gäller ICTAC:s formella begäran till CERT-EU:s styrelseordförande angående rösträtt i styrelsen vill vi klargöra följande:

Med tanke på de betydande omkostnader som översynen av det nuvarande interinstitutionella avtalet skulle medföra, och eftersom de decentraliserade byråernas representation redan beaktas i det pågående arbetet med förordningen om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer, enades man om att låta förordningen bli den formella, långsiktiga lösningen. Såsom ordföranden bekräftar kommer nuvarande praxis att fortsätta gälla fram till dess, och ICTAC:s företrädare är även fortsättningsvis välkomna att framföra sina synpunkter, som kommer att beaktas i största möjliga utsträckning och på ett rättvist sätt.

Punkt 66

I slutet av 2021 upprättade Enisa en handlingsplan för cybersäkerhetsövningar som särskilt omfattar EU:s institutioner, organ och byråer. En relevant handlingsplan för utbildning till EU:s institutioner, organ och byråer kommer att tillhandahållas under första kvartalet 2022.

Ruta 3

Även om det inte uttryckligen nämns som operativa insatser har Enisa på begäran gett operativt stöd till och samarbetat med olika EU-institutioner, EU-organ och EU-byråer. Detta skedde exempelvis under mål 2.2 år 2018. Stöd till genomförandet av Europeiska unionens politik:

- Europeiska centralbanken begärde stöd för att utveckla Eurosystemets testram för röda lag (red teams).

- Europeiska unionens byrå för luftfartssäkerhet begärde stöd för att utveckla målen för europeiska centrumet för it-säkerhet inom luftfart och höja medvetenheten om cybersäkerhetsamt för det sektorsvisa genomförandet av NIS-direktivet.
- Europeiska unionens järnvägsbyrå begärde stöd i samband med genomförandet av NIS-direktivet inom järnvägssektorn. Stödet gällde särskilt utvecklingen av en sektorsspecifik informations- och analyscentral för infrastrukturförvaltare och järnvägsföretag samt kapacitetsuppbyggnad (anordnande av kurser och medvetandehöjande utbildningspass).
- Enisa stödde Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa) i arbetet med att förstärka byråns cybersäkerhet och driftskontinuitet. Enisa tillhandahöll i synnerhet sin sakkunskap när det gäller organisation av övningar/utarbetande av scenarier och ställde Enisas fullt utvecklade plattform för cyberövningar till eu-Lisas förfogande i samband med en beredskapsövning för ett av Europeiska unionens kritiska it-system.

Sedan 2019 har Enisa dessutom samarbetat med ett flertal EU-institutioner, EU-organ och EU-byråer (t.ex. ERA, Emsa, Easa och Acer) i samband med genomförandet av NIS-direktivet samt för att bygga upp sektorsspecifik kunskap, anordna medvetandehöjande cybersäkerhetsaktiviteter och hjälpa till med relaterade sektorsvisa initiativ på området cybersäkerhetsstrategier.

Punkt 71

Under 2021 tog Enisa fram en utbildning som riktar sig särskilt till EU:s institutioner, organ och byråer och som visar hur man skapar ett program för ökad medvetenhet och använder skrivbordsövningar i detta sammanhang. Denna utbildning kommer att rullas ut under 2022. Inom ramen för sitt strukturerade samarbete kommer Enisa och CERT-EU också att tillhandahålla gemensamma utbildningar till EU:s institutioner, organ och byråer under 2022.

Punkt 72

Det bör noteras att Enisas cybersäkerhetsövningar har ett brett tillämpningsområde och en omfattande målgrupp där EU:s institutioner, organ och byråer ingår. Denna strategi söker även tillgodose behoven hos EU:s institutioner, organ och byråer, eftersom de kan dra stor

nytta av denna typ av övningar tillsammans med företrädare för medlemsstaterna. Värt att nämna är också att Enisa sedan 2016 involverar teknisk personal från EU:s institutioner, organ och byråer i CyberEurope-övningarna, som anordnas under vägledning av CERT-EU, som också står för planeringen av detta initiativ. Som en fortsättning på dessa insatser planerar Enisa som en del av byråns övningsstrategi för 2022 att inom ramen för sin kapacitetsuppbyggande verksamhet ta fram en ny övningsprodukt som kommer att tillhandahållas med stöd från CERT-EU och ge EU:s institutioner, organ och byråer möjlighet att få utbildning i självutvärderingsövningar.

3. Slutsatser och rekommendationer

Enisa och CERT-EU godtar rekommendation 3 (om att öka CERT-EU:s och Enisas fokus på de EU-institutioner, EU-organ och EU-byråer som har en lägre mognadsgrad), som riktar sig särskilt till dem.