EUROPA-KOMMISSIONENS SVAR

PÅ DEN EUROPÆISKE REVISIONSRETS SÆRBERETNING

Cybersikkerhed i EU's institutioner, organer og agenturer: Beredskabsniveauet står ikke mål med truslerne

Indholdsfortegnelse

Dette dokument indeholder Europa-Kommissionens svar på Revisionsrettens bemærkninger som medtaget i en særberetning, jf. artikel 259 i finansforordningen, og offentliggøres sammen med den pågældende særberetning.

I. RESUMÉ AF KOMMISSIONENS SVAR

a) Generel indledning

Cybersikkerhed er blevet en politisk og operationel topprioritet for Europa-Kommissionen. Covid-19-krisen har fremskyndet vores afhængighed af digitale tjenester (cloud computing, bærbare enheder, kunstig intelligens osv.). De sidste to år har vi set et massivt skifte til hjemmearbejde. Dette betyder, at både cyberkriminalitet og cyberspionage, som udgør de to største trusler for EU's institutioner, organer og agenturer, også er gået massivt online. Kommissionen anerkender denne tendens og har udvist konsekvent og beslutsomt lederskab i forbindelse med cybersikkerhed. Forordningen om cybersikkerhed trådte i kraft i 2019 og udvidede bl.a. ENISA's mandat og gav det en mere varig karakter. Ved forordningen blev der også oprettet et formelt samarbejde mellem ENISA og CERT-EU (IT-Beredskabsenheden for EU's Institutioner, Organer og Agenturer). I 2020 foreslog Kommissionen en styrkelse af direktivet om net- og informationssystemer, som lovgiverne er tæt på at nå til enighed om.

EU's strategi for cybersikkerhed fra 2020 omfattede desuden tre tiltag vedrørende cybersikkerheden i EU's institutioner, organer og agenturer, nærmere betegnet: en forordning om informationssikkerhed i EU's institutioner og organer, en forordning om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer og et nyt retsgrundlag for CERT-EU med henblik på at styrke enhedens mandat og finansieringen af den og dermed sikre dens ressourcer i forbindelse med stigningen i trusler, risici og hændelser.

Arbejdet med disse forslag er fremskredent. Selv om de endnu ikke er vedtaget af kollegiet, forventes de vedtaget i første kvartal af 2022. Blandt de vigtige spørgsmål, som institutionerne har drøftet i denne forberedende fase, er retsgrundlaget for forslagene og EU-institutionernes, -organernes og -agenturernes budgetkapacitet med tanke på finansieringen af deres egne cybersikkerhedsbehov samt de nødvendige ressourcer til understøttelse af CERT-EU's budget, navnlig stillinger.

Cybersikkerhedsmodenheden varierer fra den ene EU-institution, -organ og -agentur til den anden. Flere EU-institutioner, -organer og -agenturer præsterer højt for så vidt angår cyberberedskab og bør fortsat tjene som frontløbere og stimulere og inspirere til fremskridt og yderligere forbedringer på tværs af hele cybersikkerhedslandskabet. Med henblik på at opnå målbare fremskridt er det vigtigt at anerkende de varierende modenhedsniveauer i EU's institutioner, organer og agenturer og fastsætte prioriteter ved i første omgang at rette forbedringstiltag mod de institutioner, organer og agenturer, hvor de konstaterede mangler fører til størst risikoeksponering.

b) Kommissionens holdning til Revisionsrettens vigtigste bemærkninger og anbefalinger

Kommissionen hilser Revisionsrettens særberetning om cybersikkerhed i EU's institutioner, organer og agenturer velkommen. Den noterer sig, at særberetningen understreger vigtigheden af fælles retlige rammer for alle EU's institutioner, organer og agenturer for så vidt angår informationssikkerhed og cybersikkerhed med henblik på at øge den samlede cybersikkerhed over hele linjen. Kommissionen noterer sig, at Revisionsrettens vigtigste bemærkninger og anbefalinger ikke som sådan er rettet mod Kommissionens egen operationelle cybersikkerhed, men snarere mod

Kommissionens politiske rolle for så vidt angår fremsættelsen af lovgivningsforslag til forbedring af cybermodenheden i EU's institutioner, organer og agenturer.

Ved de kommende forordninger om "informationssikkerhed i EU's institutioner og organer" og "foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer" fastsættes der fælles regler til opnåelse af et højt informations- og cybersikkerhedsniveau, men gennemførelsen af dem inden for hver enkelt EU-institutions, -organs eller agenturs organisatoriske og operationelle rammer (navnlig deres trussels- og risikoprofiler) er fortsat EU-institutionernes, -organernes og -agenturernes autonome ansvar. Den foreslåede forordning om cybersikkerhed vil omfatte håndhævelsesordninger, som er forholdsmæssige og står mål med målsætningen og anvendelsesområdet for de nye regler, uden at dette berører institutionernes, organernes og agenturernes autonomi.

Kommissionen er i øjeblikket formand for undergruppen vedrørende cybersikkerhed i det interinstitutionelle udvalg for digital omstilling (ICDT), som besættes i henhold til en rotationsordning (for en periode på op til to år). Det bemærkes, at undergruppens arbejde ikke har fået tildelt nogen ressourcer: alle tiltag er baseret på deltagernes bedst mulige frivillige bestræbelser.

Kommissionen tilslutter sig den overordnede idé om at øge CERT-EU's ressourcer og styrke dets mandat.

I overensstemmelse med denne forståelse støtter Kommissionen de vigtigste bemærkninger og anbefalinger i særberetningen. Vores holdning forklares nærmere i de supplerende bemærkninger i afsnit III. Hvad angår anbefalingerne accepterer Kommissionen anbefaling 1a, 1b, 1c, 1d, 1e, 1f, 1g samt 2a, 2b og 2c.

c) Seneste udvikling og næste skridt

En høring af EU's institutioner, organer og agenturer på generaldirektørniveau om de konsoliderede forslag til de to forordninger (om informations- og cybersikkerhed) er afsluttet, således at der for nuværende pågår en vurdering af den modtagne feedback, inden pakken forventes færdiggjort og vedtaget af kollegiet i første kvartal af 2022.

II. KOMMISSIONENS SVAR PÅ REVISIONSRETTENS VIGTIGSTE BEMÆRKNINGER

1. Cybersikkerhedsmodenheden i EU's institutioner, organer og agenturer

Kommissionen er enig i, at det er vigtigt at tage højde for trusler og risici i forbindelse med EU-institutionernes, -organernes og -agenturernes udgifter til cybersikkerhed.

Hvad angår de menneskelige ressourcer afhænger stillingstildelingen i EU's institutioner, organer og agenturer ligeledes af en række faktorer. Rekrutteringsmarkedet for specialiserede cybersikkerhedseksperter er i stigende grad komplekst. I mange tilfælde er reglerne om menneskelige ressourcer ikke tilpasset de specialiserede profiler (rekruttering, karriereudvikling og

uddannelse). Derudover betyder budgetmyndighedens generelle pres på personaleniveauet i EU's institutioner, organer og agenturer, at nye områder med høj prioritet såsom cybersikkerhed fortsat ikke får tildelt nok stillinger, navnlig hvad angår de interne operationelle tjenester.

I forbindelse med henvisningen til fremskridtene for så vidt angår forvaltning og risikostyring bør der tages højde for det faktum, at overvågningen af overholdelsen nu bevæger sig fra pilotfasen til fuld iværksættelse. Det er derfor normalt, at dækningen på nuværende tidspunkt er så lav. Overholdelsesprojektet udgør næste fase i den proces for forbedring af cybermodenheden på lang sigt, som begyndte med fastlæggelsen af en fælles risikometode, opbygningen af fælles værktøjer, iværksættelsen af sårbarhedsstyring samt overvågning af aktiver, afprøvning og validering. Der er gjort fremskridt på dette område til trods for, at Kommissionens aktivbase er meget kompleks, idet den indeholder over 1 000 informationssystemer, der drives af over 50 generaldirektorater og forvaltningsorganer.

2. EU-institutionernes, -organernes og -agenturernes mekanismer for samarbejde

CERT-EU er en fænomenal succeshistorie hvad angår øget samarbejde ikke blot mellem EU's institutioner, organer og agenturer, men også på europæisk plan, nærmere betegnet CERT-EU's deltagelse i CSIRT-netværket som fuldgyldigt medlem, jf. NIS-direktivet. Således er CERT-EU et forbilledligt eksempel på, hvordan samarbejdet og cybersikkerhedstjenesterne kan forbedres. Revisionsrettens bemærkninger om CERT-EU illustrerer meget tydeligt det glimrende stykke arbejde, som CERT-EU leverer i en situation, hvor trusselsbilledet for cybersikkerheden er mere og mere fjendtligt, og hvor manglen på ressourcer er kronisk.

I medfør af den gældende interinstitutionelle aftale repræsenteres EU's decentrale agenturer og fællesforetagender officielt af ENISA i CERT-EU's styringsråd. Derudover udtrykkes deres synspunkter på styringsrådets møder af en repræsentant for ICTAC, som har tilladelse til at deltage for at bistå ENISA i dets rolle som repræsentant for agenturerne, men som ikke har et formelt sæde eller ret til at stemme. Spørgsmålet om passende repræsentation af agenturerne i CERT-EU's styringsråd tages op i forslaget til forordning, idet sammensætningen af styringsrådet fuldendes med op til tre repræsentanter udpeget af EU-agenturernes netværk (EUAN) efter forslag fra netværkets rådgivende IKT-udvalg (ICTAC).

Deltagelse i ICDT's undergruppe vedrørende cybersikkerhed er baseret på deltagernes bedst mulige bestræbelser i henhold til, hvor meget hver EU-institution, -organ og- agentur har besluttet at engagere sig. Forbedringer for så vidt angår udveksling af oplysninger om offentlige indkøb er et vigtigt emne, der behandles af taskforce 2 i undergruppen vedrørende cybersikkerhed, og som vil blive taget op i forbindelse med udarbejdelsen af den nye rammekontrakt vedrørende cybersikkerhed.

Hvad angår fælles værktøjer til brug for tjenester såsom e-mail og videokonferencer er der allerede mulighed for at anvende SECEM-2-systemet, der er indført af Kommissionen for alle EU's institutioner, organer og agenturer, til krypterede e-mails afhængig af den effektive forvaltning af krypteringsnøgler og -certifikater. Desuden er SECABC, som er et værktøj til udveksling af krypterede e-mails mellem institutionerne, under udvikling, og det forventes, at alle interesserede EU-institutioner, -organer og -agenturer kan tilbydes adgang til dette system fra 2022. Sikre videokonferencer til SNC-tjenester er allerede på plads og kan udbredes til andre EU-institutioner, -organer og -agenturer på ad hoc-basis ved at forvalte identiteten på mødets deltagere. Udveksling

af følsomme oplysninger tages også op i den foreslåede forordning om informationssikkerhed (i form af fælles mærkning).

3. Udveksling af oplysninger om væsentlige hændelser og sårbarheder

Det faktum, at ikke alle EU-institutioner, -organer og -agenturer underretter CERT-EU om væsentlige hændelser og sårbarheder, tages op i den foreslåede forordning om cybersikkerhed i overensstemmelse med Kommissionens forslag om NIS 2-direktivet[1]. Gennemførelsesniveauet vil afhænge af de autonome EU-institutioners, -organers og -agenturers tildeling af ekstra ressourcer hertil. Muligheden for at gøre sådanne underretninger obligatoriske er fortsat begrænsede, også i henhold til den foreslåede forordning, som den foreligger, under henvisning til EU-institutionernes, -organernes og -agenturernes institutionelle autonomi. Den foreslåede forordning om cybersikkerhed vil omfatte håndhævelsesordninger, som er forholdsmæssige og står mål med målsætningen og anvendelsesområdet for de nye regler, uden at dette berører institutionernes, organernes og agenturernes autonomi.

III. KOMMISSIONENS SVAR PÅ REVISIONSRETTENS KONKLUSIONER OG ANBEFALINGER

Anbefaling 1 — Forbedre EU-institutionernes, -organernes og -agenturernes cybersikkerhedsberedskab gennem fælles standarder og øgede ressourcer til CERT-EU

Den foreslåede forordning omfatter specifikke foranstaltninger, der skal øge det fælles cybersikkerhedsniveau yderligere. Disse foranstaltninger vil blive omsat til cybersikkerhedsplaner, som udarbejdes og gennemføres lokalt i EU's institutioner, organer og agenturer inden for deres egne rammer for forvaltning af cybersikkerhed.

Kommissionen accepterer denne anbefaling. Hvad angår de specifikke underanbefalinger bemærker Kommissionen følgende:

a) Kommissionen accepterer anbefaling 1a. Den foreslåede forordning omfatter bestemmelser om rammer for forvaltning og kontrol af cybersikkerhedsrisici, der fastlægges på højeste ledelsesniveau i hver EU-institution, -organ og -agentur med henblik på at sikre effektiv og fornuftig styring af alle cybersikkerhedsrisici.
b) Kommissionen accepterer anbefaling 1b. Den foreslåede forordning styrker den risikobaserede tilgang til forvaltning af cybersikkerheden ved at gøre det tydeligt, at tiltag, IT-sikkerhedsplaner og faktisk gennemførelse af vigtige kontroller bør følge vurderingerne.

[1] Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (COM(2020) 823 final).

c) Kommissionen accepterer anbefaling 1c. Uddannelse i cybersikkerhed, bevidstgørelse og kurser anføres i den foreslåede forordning som en del af referencescenariet for cybersikkerhed.
d) Kommissionen accepterer anbefaling 1d. Det er vores erfaring, at regelmæssige revisioner og prøvning er meget vigtige, men at dette ikke er tilstrækkeligt til at sikre, at der gøres fremskridt. Regelmæssig rapportering og åbenhed er derfor nødvendig som en del af rammen for forvaltning af cybersikkerhed, jf. underpunkt a).
e) Kommissionen accepterer anbefaling 1e. Den foreslåede forordning omfatter bestemmelser om EU-institutionernes, -organernes og -agenturernes underretning om væsentlige cybertrusler, sårbarheder og hændelser til CERT-EU.
f) Kommissionen accepterer anbefaling 1f. Kommissionen støtter behovet for at øge CERT-EU's ressourcer. Den foreslåede forordning omfatter bestemmelser om personale og finansielle bidrag fra EU's institutioner, organer og agenturer.
g) Kommissionen accepterer anbefaling 1g. Den foreslåede forordning vil omfatte håndhævelsesordninger, som står mål med og i forhold til målsætningen og anvendelsesområdet for bestemmelserne og samtidig respekterer institutionernes, organernes og agenturernes autonomi. Indholdet af den kommende forordning afhænger af resultatet af lovgivningsproceduren og følger af den beslutning, som lovgiverne træffer om Kommissionens forslag.

Anbefaling 2 — Fremme yderligere synergier mellem EU's institutioner, organer og agenturer på udvalgte områder

Kommissionen, der i øjeblikket er formand for undergruppen vedrørende cybersikkerhed i det interinstitutionelle udvalg for digital omstilling (ICDT), er enig i anbefalingerne om at fremme løsninger til konsekvent og sikker udveksling af følsomme oplysninger, systematisk udveksling af oplysninger om cybersikkerhedsrelaterede projekter og fælles indkøb af og rammekontrakter for cybersikkerhedstjenester.

Kommissionen accepterer denne anbefaling. Hvad angår de specifikke underanbefalinger bemærker Kommissionen følgende:

a) Kommissionen accepterer anbefaling 2a. Kommissionen foreslår tekniske initiativer og tjenester for ICDT's undergruppe vedrørende cybersikkerhed med henblik på at fremme og støtte fælles værktøjer til udveksling af følsomme oplysninger og muliggøre tjenester såsom e-mail og videokonferencer. Vi bemærker også, at fælles mærkning og fælles regler for håndtering af følsomme ikkeklassificerede oplysninger tages op i den foreslåede forordning om informationssikkerhed.
b) Kommissionen accepterer anbefaling 2b. Den eksisterende taskforce under ICDT's undergruppe vedrørende cybersikkerhed behandler dette spørgsmål, og der vil blive arbejdet yderligere på det. Forbedringer for så vidt angår udveksling af oplysninger om offentlige indkøb tages op i forbindelse med udarbejdelsen af den nye rammekontrakt vedrørende cybersikkerhed.
c) Kommissionen accepterer anbefaling 2c. EU's institutioner, organer og agenturer har allerede adgang til interinstitutionelle rammekontrakter på området for IKT, der forvaltes af Kommissionen. Udarbejdelsen af den nye rammekontrakt vedrørende cybersikkerhed koordineres med ICDT's undergruppe vedrørende cybersikkerhed.

Anbefaling 3 — Øge CERT-EU's og ENISA's fokus på EU-institutioner, -organer og -agenturer med et lavere modenhedsniveau

Denne anbefaling er rettet til CERT-EU og ENISA.