ANTWOORDEN VAN DE EUROPESE COMMISSIE

OP HET SPECIAAL VERSLAG VAN DE EUROPESE REKENKAMER

Cyberbeveiliging van EU-instellingen, -organen en -agentschappen: paraatheidsniveau staat niet in verhouding tot dreigingen

Inhoudsopgave

Dit document bevat de antwoorden van de Europese Commissie op de opmerkingen naar aanleiding van een speciaal verslag van de Europese Rekenkamer, overeenkomstig artikel 259 van het financieel reglement, dat samen met het speciaal verslag zal worden bekendgemaakt.

I. BEKNOPT ANTWOORD VAN DE COMMISSIE

a) Algemene inleiding

Cyberbeveiliging is een politieke en operationele topprioriteit van de Europese Commissie geworden. De coronacrisis heeft onze afhankelijkheid van digitale diensten (cloud computing, mobiele apparaten, artificiële intelligentie) versneld. De afgelopen twee jaar is er een enorme verschuiving geweest naar thuiswerken. Dit betekent dat cybercriminaliteit en cyberspionage, de twee belangrijkste bedreigingen waarmee de instellingen, organen en agentschappen van de Europese Unie (EU-IOA's) worden geconfronteerd, ook op grote schaal online zijn gegaan. De Commissie erkent deze trend. Zij heeft blijk gegeven van consistent en doorslaggevend leiderschap op het gebied van cyberbeveiliging. In 2019 is de cyberbeveiligingsverordening in werking getreden, die onder meer het mandaat van Enisa uitbreidt en het agentschap een permanente basis geeft. Bij deze verordening is ook een formele samenwerking tot stand gebracht tussen Enisa en CERT-EU (het computercrisisteam dat alle EU-IOA's ondersteunt). In 2020 heeft de Commissie een aanscherping van de netwerk- en informatiebeveiligingsrichtlijn voorgesteld, waarover tijdens de legislatuur bijna overeenstemming is bereikt.

De cyberbeveiligingsstrategie van 2020 bevatte ook drie acties met betrekking tot de cyberbeveiliging van de EU-IOA's. Zij kondigde een verordening inzake informatiebeveiliging in de instellingen, organen en agentschappen van de EU en een verordening inzake gezamenlijke cyberbeveiligingsregels voor de instellingen, organen en agentschappen van de EU aan, alsmede haar voornemen om een nieuwe rechtsgrondslag te verschaffen voor CERT-EU om zijn mandaat en financiering te versterken zodat het over voldoende middelen beschikt om het hoofd te bieden aan toenemende dreigingen, risico's en incidenten.

Met de voorbereiding van deze voorstellen is vooruitgang geboekt. Hoewel zij nog niet door het college zijn goedgekeurd, zullen zij naar verwachting in het eerste kwartaal van 2022 worden aangenomen. Belangrijke kwesties die in deze voorbereidende fase tussen de instellingen worden besproken, betreffen de rechtsgrondslag van het voorstel en de begrotingscapaciteit van alle EU-IOA's om aan de vereisten te voldoen, zowel wat betreft de financiering van hun eigen behoeften op het gebied van cyberbeveiliging als wat betreft het vinden van de nodige middelen ter ondersteuning van CERT-EU, de begroting en met name de posten.

De mate van paraatheid van de instellingen, organen en agentschappen van de EU op het gebied van cyberbeveiliging is verschillend. Verschillende EU-IOA's presteren sterk op het gebied van cyberparaatheid en moeten als leiders blijven fungeren, waardoor vooruitgang en verdere verbeteringen in het hele cyberbeveiligingslandschap worden gestimuleerd en geïnspireerd. Om meetbare vooruitgang te boeken is het belangrijk rekening te houden met de uiteenlopende maturiteitsniveaus in de EU-IOA's en prioriteiten te stellen door de verbeteringsmaatregelen in de eerste plaats te richten op die EU-IOA's waar de vastgestelde lacunes tot de hoogste risicoblootstelling leiden.

b) Standpunt van de Commissie over de belangrijkste opmerkingen en aanbevelingen van de Rekenkamer

De Commissie is ingenomen met het verslag van de Rekenkamer over cyberbeveiliging van de instellingen, organen en agentschappen van de EU. Zij neemt er nota van dat in het verslag wordt

gewezen op het belang van gemeenschappelijke rechtskaders voor alle EU-IOA's inzake informatiebeveiliging en cyberbeveiliging om het algemene niveau van cyberbeveiliging over de hele lijn te verhogen. De Commissie merkt op dat de belangrijkste opmerkingen en aanbevelingen van de Rekenkamer niet specifiek gericht zijn op de eigen operationele cyberbeveiliging van de Commissie, maar op de beleidsrol van de Commissie bij het voorstellen van wetgeving om de cybermaturiteit van de EU-IOA's te vergroten.

In de toekomstige verordeningen inzake informatiebeveiliging in de instellingen, organen en agentschappen van de EU en inzake gezamenlijke cyberbeveiligingsregels voor de instellingen, organen en agentschappen van de EU zullen gemeenschappelijke regels worden vastgesteld voor het bereiken van een hoog niveau van informatiebeveiliging en cyberbeveiliging, maar de uitvoering ervan, binnen de organisatorische en operationele context van de afzonderlijke EU-IOA's (met name hun dreigings- en risicoprofielen), blijft onder de autonome verantwoordelijkheid van de EU-IOA's vallen. De voorgestelde verordening inzake cyberbeveiliging zal nalevingsmechanismen bevatten die passend zijn en in verhouding staan tot de doelstelling en het toepassingsgebied van de nieuwe regels, zonder afbreuk te doen aan de autonomie van instellingen, organen en agentschappen.

De Commissie zit momenteel de subgroep Cyberbeveiliging van het Interinstitutioneel Comité voor digitale transformatie (ICDT) voor, die een roulerende benoeming is (voor een periode van maximaal 2 jaar). Er zij op gewezen dat er geen specifieke middelen zijn uitgetrokken voor de werkzaamheden van de subgroep: alle acties zijn gebaseerd op inspanningen van de deelnemers op vrijwillige basis.

De Commissie is het eens met het algemene idee om de middelen en het mandaat van CERT-EU te versterken.

Met dit begrip steunt de Commissie de belangrijkste opmerkingen en aanbevelingen van het verslag. Ons gedetailleerde standpunt wordt toegelicht in de aanvullende opmerkingen in deel III. Wat de aanbevelingen betreft, aanvaardt de Commissie de aanbevelingen 1 a, b, c, d, e, f, g, en 2 a, b, c.

c) Relevante meest recente ontwikkelingen en volgende stappen

Een formele raadpleging op het niveau van directeuren-generaal van EU-IOA's over de geconsolideerde ontwerpen van de twee verordeningen (informatiebeveiliging, cyberbeveiliging) is afgerond en de beoordeling van de ontvangen feedback is aan de gang, vóór de voltooiing van het pakket en de goedkeuring door het college in het eerste kwartaal van 2022.

II. ANTWOORDEN VAN DE COMMISSIE OP DE BELANGRIJKSTE OPMERKINGEN VAN DE REKENKAMER

1. Maturiteitsniveaus op het gebied van cyberbeveiliging van EU-IOA's

De Commissie is het ermee eens dat bij het vaststellen van het uitgavenniveau van de EU-IOA's voor cyberbeveiliging rekening moet worden gehouden met dreigingen en risico's.

Ook wat het personeelsaspect betreft, wordt de stabiliteit van het personeel van de EU-IOA's beïnvloed door een aantal factoren. De markt voor de aanwerving van gespecialiseerde deskundigen op het gebied van cyberbeveiliging wordt steeds complexer. In veel gevallen zijn de personeelsregels niet aangepast aan gespecialiseerde profielen (aanwerving, loopbaanontwikkeling, opleiding). Bovendien betekent de algemene druk op de personeelsbezetting in de EU-IOA's door de begrotingsautoriteit dat opkomende gebieden met een hoge prioriteit, zoals cyberbeveiliging, nog steeds onvoldoende van posten zijn voorzien, met name in de interne operationele diensten.

Bij de verwijzing naar de vooruitgang op het gebied van governance en risicobeheer moet rekening worden gehouden met het feit dat het toezicht op de naleving nu verschuift van proefproject naar volledige uitrol. Het is dus normaal dat de dekking tot dusver vrij laag is. Dit nalevingsproject is de volgende fase van een proces ter verbetering van de cybermaturiteit op lange termijn, dat begon met de vaststelling van een gemeenschappelijke risicomethodologie, de ontwikkeling van gemeenschappelijke instrumenten, de uitrol van het beheer van kwetsbaarheden, en monitoring, toetsing en validering van de inventaris van hulpbronnen. Op deze lange weg is vooruitgang geboekt ondanks de complexiteit van de hulpbronnenbasis van de Commissie met meer dan 1 000 informatiesystemen die door meer dan 50 directoraten-generaal en uitvoerende agentschappen worden beheerd.

2. Samenwerkingsmechanismen van de EU-IOA's

CERT-EU is een fenomenaal succesverhaal bij het bevorderen van samenwerking, niet alleen tussen EU-IOA's, maar ook op Europees niveau, door zijn deelname als volwaardig lid van het CSIRT-netwerk dat in het kader van de NIS-richtlijn is opgezet. Op deze manier is CERT-EU een voorbeeld van hoe samenwerking en cyberbeveiligingsdiensten kunnen worden verbeterd. De opmerkingen van de Europese Rekenkamer over CERT-EU illustreren zeer duidelijk het uitstekende werk dat CERT-EU verricht in het licht van een steeds vijandiger cyberdreigingslandschap en met chronische onderfinanciering.

In het kader van de huidige interinstitutionele regeling (IR) worden gedecentraliseerde agentschappen en gemeenschappelijke ondernemingen van de EU officieel vertegenwoordigd in het stuurcomité van CERT-EU door Enisa. Daarnaast worden hun standpunten in de vergaderingen van het stuurcomité naar voren gebracht door een vertegenwoordiger van het ICT-adviescomité (ICTAC), die Enisa mag bijstaan in zijn rol als vertegenwoordiger van de agentschappen, maar geen formele zetel of stem heeft. Het punt van adequate vertegenwoordiging van agentschappen in het stuurcomité van CERT-EU zal in de voorgestelde verordening worden behandeld door de

samenstelling van het stuurcomité aan te vullen met maximaal drie vertegenwoordigers die worden aangewezen door het Netwerk van agentschappen van de Unie (EUAN), op voorstel van zijn ICT-adviescomité.

Deelname aan de subgroep Cyberbeveiliging van het ICDT geschiedt op basis van de beste inspanningen, op het door alle EU-IOA's vastgestelde niveau van betrokkenheid. Verbeteringen op het gebied van informatie-uitwisseling over aanbestedingen, een belangrijk onderwerp binnen het toepassingsgebied van taskforce 2 van de subgroep Cyberbeveiliging, worden behandeld bij de voorbereiding van de nieuwe raamovereenkomst inzake cyberbeveiliging.

Wat de gemeenschappelijke instrumenten voor diensten zoals versleuteld e-mailverkeer of videoconferencing betreft, bestaat er reeds de mogelijkheid om voor alle EU-IOA's gebruik te maken van het SECEM-2-systeem voor versleutelde e-mail, afhankelijk van het doeltreffende beheer van encryptiesleutels en -certificaten. Daar komt bij dat SECABC, een instrument om e-mailversleuteling tussen instellingen mogelijk te maken, in ontwikkeling is, met de bedoeling om vanaf 2022 toegang te verlenen aan alle geïnteresseerde EU-IOA's. Beveiligde videoconferencing voor diensten op het gebied van beveiligde netwerkcommunicatie zijn reeds tot stand gekomen en kunnen op ad-hocbasis tot andere EU-IOA's worden uitgebreid door de identiteit van de deelnemers aan de vergadering te beheren. Het delen van gevoelige informatie zal ook aan bod komen in de voorgestelde verordening inzake informatiebeveiliging (d.w.z. door middel van gemeenschappelijke etikettering en markeringen).

3. Informatie uitwisselen over significante incidenten of kwetsbaarheden

Het feit dat niet alle EU-IOA's CERT-EU in kennis stellen van significante incidenten of kwetsbaarheden wordt behandeld in de ontwerpverordening inzake cyberbeveiliging in overeenstemming met het voorstel van de Commissie in de NIS-2-richtlijn[1]. Het uitvoeringsniveau zal afhangen van de extra middelen die de autonome EU-IOA's hiervoor uittrekken. De mogelijkheden voor de handhaving van dergelijke kennisgevingen blijven beperkt, ook in het kader van de voorgestelde verordening zoals momenteel gepland, vanwege de institutionele autonomie van de EU-IOA's. De voorgestelde verordening inzake cyberbeveiliging zal nalevingsmechanismen bevatten die passend zijn en in verhouding staan tot de doelstelling en het toepassingsgebied van de nieuwe regels, zonder afbreuk te doen aan de autonomie van instellingen, organen en agentschappen.

[1] Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148, COM(2020) 823 final van 16 december 2020.

III. ANTWOORDEN VAN DE COMMISSIE OP DE CONCLUSIES EN AANBEVELINGEN VAN DE EUROPESE REKENKAMER

Aanbeveling 1 — Verbeter de cyberparaatheid van EU-IOA's door gemeenschappelijke bindende normen vast te stellen en versterk CERT-EU met meer middelen

De voorgestelde tekst van de verordening zal specifieke maatregelen bevatten om het gemeenschappelijke niveau van cyberbeveiliging verder te verhogen. Deze maatregelen zullen worden omgezet in plannen voor cyberbeveiliging, die op het niveau van de EU-IOA's worden vastgesteld en uitgevoerd in het kader van hun eigen governancekader voor cyberbeveiliging.

De Commissie aanvaardt deze aanbeveling. Met betrekking tot de specifieke subaanbevelingen merkt de Commissie het volgende op:

a) De Commissie aanvaardt aanbeveling 1a. De ontwerpverordening zal bepalingen bevatten over governance- en controlekaders, die op het hoogste niveau van uitvoerend beheer van alle EU-IOA's zijn opgezet om een doeltreffend en prudent beheer van alle cyberbeveiligingsrisico's te waarborgen.
b) De Commissie aanvaardt aanbeveling 1b. In de ontwerpverordening wordt de notie van de risicogebaseerde benadering van het beheer van cyberbeveiliging benadrukt door duidelijk te maken dat beoordelingen de grondslag moeten vormen voor acties, IT-beveiligingsplannen en de daadwerkelijke uitvoering van essentiële controles.
c) De Commissie aanvaardt aanbeveling 1c. In de ontwerpverordening zullen onderwijs-, bewustmakings- en opleidingsprogramma's op het gebied van cyberbeveiliging worden genoemd als onderdeel van de uitgangssituatie op het gebied van cyberbeveiliging.
d) De Commissie aanvaardt aanbeveling 1d. Naar onze ervaring zijn regelmatige controles en tests weliswaar van essentieel belang, maar volstaan zij niet om ervoor te zorgen dat er vooruitgang wordt geboekt. Daarom is regelmatige verslaglegging en transparantie noodzakelijk, als onderdeel van het kader voor cyberbeveiligingsgovernance onder punt a).
e) De Commissie aanvaardt aanbeveling 1e. De ontwerpverordening zal bepalingen bevatten met betrekking tot de kennisgeving door de EU-IOA's van significante cyberdreigingen, kwetsbaarheden en incidenten aan CERT-EU.
f) De Commissie aanvaardt aanbeveling 1f. De Commissie steunt de noodzaak om de middelen van CERT-EU te versterken. Bepalingen met betrekking tot personeel en financiële bijdragen uit de EU-IOA's zullen in de tekst van de ontwerpverordening worden opgenomen.
g) De Commissie aanvaardt aanbeveling 1g. De voorgestelde verordening zal voorzien in nalevingsmechanismen die in verhouding staan tot en afgestemd zijn op het doel en de reikwijdte van de bepalingen, met inachtneming van de institutionele autonomie van de EU-IOA's. De inhoud van de toekomstige verordening hangt af van het resultaat van de wetgevingsprocedure en is het resultaat van een besluit van de EU-wetgever over het voorstel van de Commissie.

Aanbeveling 2 — Streef naar verdere synergieën tussen EU-IOA's op specifieke gebieden

De Commissie, die momenteel voorzitter is van de subgroep Cyberbeveiliging van het Interinstitutioneel Comité voor digitale transformatie (ICDT), is het eens met de aanbevelingen om oplossingen te bevorderen voor een consistente en veilige uitwisseling van gevoelige informatie, de systematische uitwisseling van informatie over cyberbeveiligingsprojecten en gemeenschappelijke aanbestedingskaders en overeenkomsten voor cyberbeveiligingsdiensten.

De Commissie aanvaardt deze aanbeveling. Met betrekking tot de specifieke subaanbevelingen merkt de Commissie het volgende op:

a) De Commissie aanvaardt aanbeveling 2a. De Commissie stelt technische initiatieven en diensten ter beschikking van de subgroep Cyberbeveiliging van het ICDT om gemeenschappelijke instrumenten voor het delen van gevoelige informatie te bevorderen en te ondersteunen, waardoor diensten zoals videoconferencing mogelijk worden. Wij merken ook op dat gemeenschappelijke markeringen en gemeenschappelijke regels voor de behandeling van gevoelige niet-gerubriceerde informatie zullen worden behandeld in de voorgestelde verordening inzake informatiebeveiliging.
b) De Commissie aanvaardt aanbeveling 2b. De bestaande taskforces in het kader van de subgroep Cyberbeveiliging van het ICDT behandelen dit punt en het zal daar verder worden uitgewerkt. Verbeteringen op het gebied van informatie-uitwisseling over aanbestedingen worden aangepakt bij de voorbereiding van de nieuwe raamovereenkomst voor cyberbeveiliging.
c) De Commissie aanvaardt aanbeveling 2c. De EU-IOA's hebben reeds toegang tot interinstitutionele raamovereenkomsten op het gebied van ICT die door de Commissie worden beheerd. De voorbereiding van de nieuwe raamovereenkomst voor cyberbeveiliging zal worden gecoördineerd met de subgroep Cyberbeveiliging van het ICDT.

Aanbeveling 3 — Laat CERT-EU en Enisa meer aandacht besteden aan EU-IOA's met een minder hoog maturiteitsniveau

Deze aanbeveling is gericht tot CERT-EU en Enisa.