Raad van de
Europese Unie

Brussel, 10 juni 2022
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

NOTA I/A-PUNT

van:	het secretariaat-generaal van de Raad
aan:	het Comité van permanente vertegenwoordigers/de Raad
nr. vorig doc.:	9317/2/22 REV 2
Betreft:	Ontwerpconclusies van de Raad over Speciaal verslag 05/2022 van de Europese Rekenkamer: "Cyberbeveiliging van EU-instellingen, -organen en -agentschappen: paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen" - Goedkeuring

1. De Europese Rekenkamer heeft op 30 maart 2022 Speciaal verslag 05/2022 "Cyberbeveiliging van EU-instellingen, -organen en -agentschappen: paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen" gepubliceerd.[1]

2. Tijdens zijn vergadering van 13 april 2022 heeft het Comité van permanente vertegenwoordigers besloten het speciaal verslag toe te wijzen aan de Horizontale Groep cybervraagstukken.[2]

[1] Doc. 8040/22.
[2] Doc. 8041/22.

3. De vertegenwoordigers van de Rekenkamer hebben het speciaal verslag op 3 mei 2022 toegelicht in de Horizontale Groep cybervraagstukken. Tijdens die vergadering werd het verslag ook besproken in de groep. Naar aanleiding daarvan stelde het voorzitterschap ontwerpconclusies van de Raad op, die tijdens de vergadering van de groep van 24 mei 2022 werden besproken.

4. Op 10 juni 2022 heeft de Horizontale Groep cybervraagstukken overeenstemming bereikt over de tekst in de bijlage.

5. Het Comité van permanente vertegenwoordigers wordt verzocht de ontwerpconclusies goed te keuren en de Raad voor te stellen deze ontwerpconclusies tijdens een volgende zitting aan te nemen.

BIJLAGE

ONTWERPCONCLUSIES VAN DE RAAD

over Speciaal verslag 05/2022 van de Europese Rekenkamer,
getiteld
"Cyberbeveiliging van EU-instellingen, -organen en -agentschappen: paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen"

DE RAAD VAN DE EUROPESE UNIE,

HERINNEREND AAN zijn conclusies over de verbetering van de behandeling van de speciale verslagen van de Rekenkamer in het kader van de kwijtingsprocedure[3];

1. NEEMT NOTA van Speciaal verslag 05/2022 van de Europese Rekenkamer, getiteld "Cyberbeveiliging van EU-instellingen, -organen en -agentschappen: paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen"[4].

2. BENADRUKT dat het cyberbeveiligingsniveau binnen de EU-instellingen, -organen en -agentschappen snel moet worden verhoogd, gelet op de recent versnelde digitalisering binnen de instellingen, de gevoelige informatie die zij verwerken, het toenemende aantal aanvallen op EU-instellingen, -organen en -agentschappen en de toenemende ernst ervan, en het dreigingsniveau dat voor hen geldt.

[3] Doc. 7515/00 + COR 1.
[4] Doc. 8040/22.

3. HERINNERT AAN de conclusies van de Europese Raad van 20 juni 2019[5], waarin de Europese Raad de EU-instellingen verzoekt om samen met de lidstaten aan maatregelen te werken om de weerbaarheid te vergroten en de veiligheidscultuur van de EU tegen cyber- en hybride dreigingen van buiten de EU te verbeteren, en om de informatie- en communicatienetwerken en de besluitvormingsprocessen van de EU beter te beschermen tegen alle soorten kwaadwillige activiteiten.

4. HERINNERT AAN zijn conclusies van 10 december 2019 over extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen[6], waarin hij de instellingen, organen en agentschappen van de EU oproept om, ondersteund door de lidstaten, te zorgen voor het vermogen van de Unie om haar integriteit te beschermen en de beveiliging te verbeteren van de EU-informatie- en communicatienetwerken en -besluitvormingsprocessen tegen alle soorten kwaadwillige activiteiten, op basis van een uitgebreide dreigingsanalyse. Voorts staat in deze conclusies dat de instellingen, organen en agentschappen, ondersteund door de lidstaten, daartoe een uitgebreide reeks maatregelen moeten uitwerken en toepassen om hun veiligheid te waarborgen, overeenkomstig het mandaat van de Europese Raad van juni 2019[7].

5. HERINNERT AAN zijn conclusies van 22 maart 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[8], waarin hij benadrukt dat cyberbeveiliging essentieel is voor de werking van openbare diensten en instellingen, zowel nationaal als op EU-niveau, en voor onze samenleving en de gehele economie.

---

5 Doc. EUCO 9/19.
6 Doc. 14972/19.
7 Doc. EUCO 9/19.
8 Doc. 6722/21.

6. HERINNERT AAN zijn conclusies van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie[9], waarin de EU-instellingen, -organen en -agentschappen worden verzocht de bestaande instrumenten voor beveiligde communicatie op cybergebied in kaart te brengen, zodat deze in de betrokken Raadsorganen en met de betrokken samenwerkingsgroepen, zoals het CSIRT-netwerk en EU CyCLONe, kunnen worden besproken.

7. BENADRUKT dat het systeemrisico dat de onderlinge verwevenheid van de EU-instellingen, -organen en -agentschappen en hun verwevenheid met de instanties van de lidstaten, ondanks hun institutionele en administratieve autonomie, met zich mee brengen, moet worden aangepakt.

8. NEEMT NOTA van de opmerkingen in het speciaal verslag, met name dat het door de EU-instellingen, -organen en -agentschappen bereikte niveau van cyberparaatheid niet in verhouding staat tot de dreigingen, en dat zij sterk uiteenlopende niveaus van cyberbeveiligingsmaturiteit hebben. ERKENT dat het paraatheidsniveau op het gebied van cyberbeveiliging van de EU-instellingen, -organen en -agentschappen, en de synergie tussen hen, moeten worden verbeterd.

9. MOEDIGT de EU-instellingen, -organen en -agentschappen daarom ten zeerste AAN risicobeheersmaatregelen op het gebied van cyberbeveiliging te blijven nemen om een passend cyberbeveiligingsniveau te waarborgen, zoals beoogd in de voorgestelde richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148, teneinde hun paraatheid te verbeteren.

10. VERZOEKT de EU-instellingen, -organen en -agentschappen zowel hun inspanningen om zichzelf te beschermen tegen cyberdreigingen als de samenwerking voor de vaststelling van consistente normen en specificaties op te voeren, met name als het gaat om overheidsopdrachten, -projecten en -diensten op het gebied van cyberbeveiliging, en de interoperabiliteit van hun IT-systemen te verbeteren, om er onder meer voor te zorgen dat niet-gerubriceerde informatie veilig kan worden uitgewisseld.

---

[9] Doc. 9364/22.

11. VERZOEKT het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie (CERT-EU) om, binnen hun bevoegdheden, meer samen te werken om de EU-instellingen, -organen en -agentschappen te ondersteunen bij hun cyberbeveiliging, met name bij de capaciteitsopbouw voor EU-instellingen, -organen en -agentschappen met een lager niveau van cyberbeveiligingsmaturiteit.

12. NEEMT NOTA van de conclusies en aanbevelingen in het speciaal verslag, en ERKENT dat de mate van paraatheid op het gebied van cyberbeveiliging van de EU-instellingen, -organen en -agentschappen, alsook de synergie tussen hen, aanzienlijk moet worden verbeterd. De EU-instellingen, -organen en -agentschappen moeten beschikken over een alomvattend kader voor risicobeheer op het gebied van cyberbeveiliging, regelmatig risicobeoordelingen en audits uitvoeren op basis van gemeenschappelijke of gevestigde methoden en internationale standaarden, en systematisch cyberbewustzijns- en opleidingsprogramma's organiseren voor hun personeel.

13. BENADRUKT daarnaast dat de EU-instellingen, -organen en -agentschappen voldoende middelen moeten uittrekken om de uitvoering van beschermingsmaatregelen tegen cyber-dreigingen te waarborgen, met inachtneming van het meerjarig financieel kader, en NEEMT NOTA van de aanbeveling in het speciaal verslag om een vertegenwoordiger aan te stellen voor alle EU-instellingen, -organen en -agentschappen, met een toereikend mandaat en voldoende middelen, om toe te zien op de naleving van de gemeenschappelijke regels voor cyberbeveiliging.

14. ERKENT dat significante cyberincidenten binnen de EU-instellingen, -organen en -agentschappen onmiddellijk moeten worden gemeld aan CERT-EU, dat daartoe moet beschikken over voldoende, voorspelbare middelen, rekening houdend met het huidige dreigingsniveau en de behoeften van de EU-instellingen, -organen en -agentschappen, met name op het gebied van personeel, technische uitrusting en infrastructuur.

15. MERKT OP dat de samenwerking en informatie-uitwisseling op het gebied van cyberbeveiliging tussen EU-instellingen, -organen en -agentschappen, alsook de interoperabiliteit van hun beveiligde communicatiekanalen, moeten worden opgevoerd en gesystematiseerd. PLEIT ervoor dat bij deze samenwerking en informatie-uitwisseling ook overheidsinstanties die verantwoordelijk zijn voor cyberbeveiliging in de lidstaten worden betrokken.

16. NEEMT NOTA van de reacties van de Commissie, CERT-EU en Enisa op het speciaal verslag.

17. VERZOEKT de Commissie rekening te houden met de aanbevelingen in het speciaal verslag, een ambitieus cyberbeveiligingsbeleid uit te tekenen voor de EU-instellingen, -organen en -agentschappen, en te pleiten voor meer synergie tussen deze instellingen, organen en agentschappen.