Rådet for
Den Europæiske Union

Bruxelles, den 21. juni 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	21. juni 2022
til:	delegationerne
Tidl. dok. nr.:	9716/22
Vedr.:	Rådets konklusioner om Den Europæiske Revisionsrets særberetning nr. 5/2022 med titlen "Cybersikkerhed i EU's institutioner, organer og agenturer: Beredskabsniveauet står samlet set ikke mål med truslerne" – Rådets konklusioner som godkendt af Rådet på samlingen den 21. juni 2022

Vedlagt følger til delegationerne ovennævnte rådskonklusioner som godkendt af Rådet på samlingen den 21. juni 2022.

BILAG

RÅDETS KONKLUSIONER

om Den Europæiske Revisionsrets særberetning nr. 5/2022 med titlen "Cybersikkerhed i EU's institutioner, organer og agenturer: Beredskabsniveauet står samlet set ikke mål med truslerne"

RÅDET FOR DEN EUROPÆISKE UNION,

SOM MINDER OM sine konklusioner om forbedring af gennemgangen af Revisionsrettens særberetninger i forbindelse med meddelelsen af decharge[1],

1. NOTERER SIG Den Europæiske Revisionsrets særberetning nr. 5/2022 med titlen "Cybersikkerhed i EU's institutioner, organer og agenturer: Beredskabsniveauet står samlet set ikke mål med truslerne"[2].

2. UNDERSTREGER, hvor vigtigt og presserende det er at styrke cybersikkerhedsniveauet i EU-institutionerne, -organerne og -agenturerne i betragtning af den nylige intensivering af den digitale omstilling i institutionerne, de følsomme oplysninger, som de behandler, det stadigt stigende antal og den stadigt stigende alvor af angreb på EU-institutioner, -organer og -agenturer og det trusselsniveau, der påvirker dem;

3. MINDER OM Det Europæiske Råds konklusioner af 20. juni 2019[3], hvori det opfordrer EU-institutionerne til sammen med medlemsstaterne at arbejde på foranstaltninger til at styrke EU's modstandsdygtighed og forbedre dets sikkerhedskultur over for cybertrusler og hybride trusler fra lande uden for EU og til bedre at beskytte EU's informations- og kommunikationsnetværk og dets beslutningsprocesser mod alle former for ondsindede handlinger;

---

1 7515/00 + COR 1.
2 8040/22.
3 EUCO 9/19.

4. MINDER OM sine konklusioner af 10. december 2019 om supplerende tiltag for at styrke modstandsdygtigheden og imødegå hybride trusler[4], hvori det opfordrer EU's institutioner, organer og agenturer til med støtte fra medlemsstaterne at sikre Unionens evne til at beskytte sin integritet og øge sikkerheden i EU's informations- og kommunikationsnetværk og beslutningsprocesser mod ondsindede aktiviteter af enhver art på grundlag af en omfattende trusselsvurdering; Med henblik herpå anførtes i konklusionerne, at institutioner, organer og agenturer med støtte fra medlemsstaterne bør udvikle og gennemføre et omfattende sæt foranstaltninger for at sikre deres sikkerhed i overensstemmelse med mandatet fra Det Europæiske Råd i juni 2019[5];

5. MINDER OM sine konklusioner af 22. marts 2021 om EU's strategi for cybersikkerhed for det digitale årti[6], hvori det understreger, at cybersikkerhed er afgørende for en velfungerende offentlig forvaltning og velfungerende offentlige institutioner på både nationalt plan og EU-plan og for vores samfund og økonomi som helhed;

6. MINDER OM sine konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition[7], hvori EU-institutioner, -organer og -agenturer tilskyndes til at deltage i kortlægningen af eksisterende redskaber til sikker kommunikation på cyberområdet, der skal drøftes i relevante rådsorganer og med relevante samarbejdsgrupper såsom CSIRT-netværket og EU-CyCLONe;

7. UNDERSTREGER behovet for at tage hånd om den systemiske risiko, der findes i forbindelsen mellem EU-institutionerne, -organerne og -agenturerne samt mellem disse og medlemsstaternes institutioner trods deres institutionelle og administrative uafhængighed;

---

4 14972/19.
5 EUCO 9/19.
6 6722/21.
7 9364/22.

8. NOTERER SIG særberetningens bemærkninger, nemlig at EU-institutionerne, -organerne og -agenturerne ikke har opnået et cyberberedskabsniveau, der står mål med truslerne, og har forskellige modenhedsniveauer, når det gælder cybersikkerhed; ANERKENDER, at cybersikkerhedsberedskabet i EU's institutioner, organer og agenturer samt synergierne mellem dem bør forbedres;

9. TILSKYNDER derfor kraftigt EU-institutionerne, -organerne og -agenturerne TIL at fortsætte gennemførelsen af cyberrisikostyringsforanstaltninger, der sikrer et rimeligt cybersikkerhedsniveau som planlagt i forslaget til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, der ophæver direktiv (EU) 2016/1148, for at forbedre deres beredskabsniveau;

10. OPFORDRER EU-institutionerne, -organerne og -agenturerne TIL både at intensivere deres bestræbelser på at beskytte sig mod cybertrusler og deres samarbejde om etablere konsekvente standarder og specifikationer, navnlig med henblik på offentlige udbud, projekter og tjenester vedrørende cybersikkerhed, og TIL at forbedre deres IT-systemers interoperabilitet, herunder med henblik på sikker kommunikation af uklassificeret indhold;

11. OPFORDRER Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og IT-Beredskabsenheden for EU's Institutioner, Organer og Agenturer (CERT-EU) TIL inden for rammerne af deres beføjelser at intensivere deres samarbejde om at støtte EU-institutionerne, -organerne og -agenturerne i deres cybersikkerhedsbestræbelser, navnlig med hensyn til kapacitetsopbygning for de EU-institutioner, -organer og -agenturer, der har et lavt modenhedsniveau, når det gælder cybersikkerhed;

12. NOTERER SIG særberetningens konklusioner og anbefalinger og ANERKENDER, at cybersikkerhedsberedskabet i EU's institutioner, organer og agenturer samt synergierne mellem dem bør forbedres betydeligt. EU-institutionerne, -organerne og -agenturerne bør have en omfattende ramme for cybersikkerhedsrisikostyring, foretage regelmæssige risikovurderinger og revisioner på grundlag af en fælles eller velkendt metode og internationale standarder og systematisere cybersikkerhedsbevidstgørelses- og uddannelsesprogrammer for personale;

13. FREMHÆVER også, at EU-institutionerne, -organerne og -agenturerne bør afsætte et tilstrækkeligt budget til at sikre gennemførelse af beskyttelsesforanstaltninger mod cybertrusler, samtidig med at den flerårige finansielle ramme respekteres, og NOTERER SIG særberetningens anbefaling om, at der bør udpeges et organ, der repræsenterer alle EU-institutionerne, -organerne og -agenturerne, og som gives behørigt mandat og passende midler til at overvåge overholdelse af de fælles cybersikkerhedsregler;

14. ANERKENDER, at CERT-EU straks bør underrettes om væsentlige cyberhændelser i EU-institutionerne, -organerne og -agenturerne og med henblik herpå udstyres med passende ressourcer, der er forudsigelige og tilpasset det nuværende trusselsniveau og EU-institutionernes, -organernes og -agenturernes behov, navnlig med hensyn til personale, teknisk udstyr og infrastruktur;

15. BEMÆRKER, at samarbejdet og informationsudvekslingen om cybersikkerhed samt interoperabiliteten mellem sikre kommunikationskanaler mellem EU-institutionerne, -organerne og -agenturerne bør styrkes og systematiseres; OPFORDRER TIL, at dette samarbejde og denne informationsudveksling også omfatter de offentlige myndigheder, der er ansvarlige for cybersikkerhed i medlemsstaterne;

16. NOTERER SIG Kommissionens, CERT-EU's og ENISA's svar, der følger med særberetningen;

17. OPFORDRER Kommissionen TIL at tage hensyn til særberetningens anbefalinger og at være ambitiøs ved udformningen af EU-institutionernes, -organernes og -agenturernes cybersikkerhedspolitikker og TIL at være fortaler for flere synergier mellem dem.