Europeiska unionens råd

Bryssel den 10 juni 2022
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

I/A-PUNKTSNOT

från:	Rådets generalsekretariat
till:	Ständiga representanternas kommitté (Coreper)/rådet
Föreg. dok. nr:	9317/2/22 REV 2
Ärende:	Utkast till rådets slutsatser om Europeiska revisionsrättens särskilda rapport 05/2022, ”Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapen står inte alltid i proportion till hoten” – Godkännande

1. Den 30 mars 2022 offentliggjorde Europeiska revisionsrätten sin särskilda rapport 05/22 Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapen står inte alltid i proportion till hoten[1].

2. Vid sitt möte den 13 april 2022 överlämnade Coreper den särskilda rapporten till den övergripande arbetsgruppen för cyberfrågor[2].

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

3. Den 3 maj 2022 presenterade revisionsrättens företrädare den särskilda rapporten för den övergripande arbetsgruppen för cyberfrågor. Efter diskussionerna om rapporten vid samma möte i arbetsgruppen utarbetade ordförandeskapet ett utkast till rådets slutsatser, som diskuterades av arbetsgruppen vid dess möte den 24 maj 2022.

4. Den 10 juni 2022 nådde den övergripande arbetsgruppen för cyberfrågor en överenskommelse om texten i bilagan.

5. Coreper uppmanas att godkänna detta utkast till slutsatser och föreslå att rådet antar det vid ett kommande möte.

BILAGA

UTKAST TILL RÅDETS SLUTSATSER

om Europeiska revisionsrättens särskilda rapport 05/2022

Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapen står inte alltid i proportion till hoten

EUROPEISKA UNIONENS RÅD,

SOM ERINRAR OM sina slutsatser om förbättring av granskningen av de särskilda rapporter som upprättas av revisionsrätten i syfte att bevilja ansvarsfrihet[3],

1. NOTERAR Europeiska revisionsrättens särskilda rapport 05/2022 *Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapen står inte alltid i proportion till hoten*[4]*,*

2. UNDERSTRYKER hur viktigt och brådskande det är att stärka cybersäkerhetsnivån inom EU:s institutioner, organ och byråer, med tanke på den senaste tidens intensifiering av den digitala omställningen inom institutionerna, den känsliga information som de behandlar, det ständigt ökande antalet angrepp mot EU:s institutioner, organ och byråer och deras allvarlighetsgrad samt den hotnivå som påverkar dem,

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

3. ERINRAR OM Europeiska rådets slutsatser av den 20 juni 2019[5], där Europeiska rådet uppmanade EU:s institutioner att, tillsammans med medlemsstaterna, arbeta med åtgärder för att stärka EU:s resiliens och säkerhetskultur med avseende på cyberhot och hybridhot från länder utanför EU och bättre skydda EU:s informations- och kommunikationsnätverk och dess beslutsprocesser mot alla former av skadlig verksamhet,

4. ERINRAR OM sina slutsatser av den 10 december 2019 om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot[6], där rådet uppmanade EU:s institutioner, organ och byråer att med stöd av medlemsstaterna säkerställa unionens förmåga att skydda den egna integriteten och öka säkerheten i EU:s informations- och kommunikationsnätverk och beslutsprocesser mot skadlig verksamhet av alla slag, på grundval av en övergripande bedömning av hotbilden; i detta syfte, anfördes i slutsatserna, bör institutioner, organ och byråer, med stöd av medlemsstaterna, utarbeta och genomföra en omfattande uppsättning åtgärder för att garantera sin säkerhet, i enlighet med Europeiska rådets mandat från juni 2019[7],

5. ERINRAR OM sina slutsatser av den 22 mars 2021 om EU:s strategi för cybersäkerhet för ett digitalt decennium[8], där det betonades att cybersäkerhet är avgörande för den offentliga förvaltningens och institutionernas funktion på både nationell nivå och EU-nivå och för vårt samhälle och ekonomin som helhet,

---

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

6. ERINRAR OM sina slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet[9], där EU:s institutioner, organ och byråer uppmanades att delta i en kartläggning av de befintliga verktygen för säker kommunikation på cyberområdet, för diskussion i relevanta rådsorgan och med relevanta samarbetsgrupper, t.ex. CSIRT-nätverket och EU CyCLONe,

7. UNDERSTRYKER behovet av att ta itu med den systemrisk som finns i sammanlänkningen mellan EU:s institutioner, organ och byråer samt mellan dem och medlemsstaternas institutioner, trots deras institutionella oberoende och administrativa självständighet,

8. NOTERAR iakttagelserna i den särskilda rapporten, nämligen att EU:s institutioner, organ och byråer inte har uppnått en cyberberedskap som står i proportion till hoten och att de har olika nivåer av cybersäkerhetsmognad, INSER att nivån på EU:s institutioners, organs och byråers cybersäkerhetsberedskap, liksom synergierna mellan dem, bör förbättras,

9. UPPMANAR därför med eftertryck EU:s institutioner, organ och byråer att fortsätta genomförandet av riskhanteringsåtgärder för cybersäkerhet som säkerställer en proportionerlig cybersäkerhetsnivå, i enlighet med förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och om upphävande av direktiv (EU) 2016/1148, i syfte att förbättra sin beredskap,

10. UPPMANAR EU:s institutioner, organ och byråer att intensifiera både sina insatser för att skydda sig mot cyberhot och sitt samarbete för att fastställa konsekventa standarder och specifikationer, särskilt för offentlig upphandling, projekt och tjänster med anknytning till cybersäkerhet, och att förbättra interoperabiliteten mellan sina it-system, bland annat i syfte att säkerställa säkert utbyte av icke-säkerhetsskyddsklassificerad information,

[9] Dok. 9364/22.

11. UPPMANAR Europeiska unionens cybersäkerhetsbyrå (Enisa) och incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU) att inom ramen för sina befogenheter intensifiera sitt samarbete för att stödja EU:s institutioner, organ och byråer i deras insatser för cybersäkerhet, särskilt när det gäller kapacitetsuppbyggnad för de av EU:s institutioner, organ och byråer som har en lägre nivå av cybersäkerhetmognad,

12. NOTERAR slutsatserna och rekommendationerna i den särskilda rapporten och ÄR MEDVETET OM att nivån på EU:s institutioners, organs och byråers cybersäkerhetsberedskap liksom synergierna mellan dem bör förbättras avsevärt; EU:s institutioner, organ och byråer bör ha en omfattande ram för hantering av cybersäkerhetsrisker, genomföra regelbundna riskbedömningar och revisioner, på grundval av en gemensam eller välkänd metod och internationella standarder, och systematiskt anordna program för cybermedvetenhet och utbildningsprogram för personal,

13. BETONAR även att EU:s institutioner, organ och byråer bör anslå tillräckliga budgetmedel för att säkerställa genomförandet av skyddsåtgärder mot cyberhot samtidigt som den fleråriga budgetramen respekteras, och NOTERAR rekommendationen i den särskilda rapporten att en enhet som företräder alla EU:s institutioner, organ och byråer bör utses och ges de befogenheter och medel som krävs för att övervaka efterlevnad med de gemensamma cybersäkerhetsreglerna,

14. ÄR MEDVETET OM att CERT-EU utan dröjsmål bör informeras om betydande cybersäkerhetsincidenter inom EU:s institutioner, organ och byråer och därför bör tilldelas tillräckliga resurser som är förutsägbara och anpassade till den nuvarande hotnivån och till behoven hos EU:s institutioner, organ och byråer, särskilt när det gäller personal, teknisk utrustning och infrastruktur,

15. NOTERAR att samarbetet och informationsutbytet om cybersäkerhet, samt interoperabiliteten hos säkra kommunikationskanaler mellan EU:s institutioner, organ och byråer bör stärkas och systematiseras, FÖRESPRÅKAR att ett sådant samarbete och informationsutbyte även bör omfatta offentliga myndigheter med ansvar för cybersäkerhet i medlemsstaterna,

16. NOTERAR de svar från kommissionen, CERT-EU och Enisa som åtföljer den särskilda rapporten,

17. UPPMANAR kommissionen att beakta rekommendationerna i den särskilda rapporten och att vara ambitiös vid utformningen av EU:s institutioners, organs och byråers politik för cybersäkerhet och att förespråka fler synergier mellan dem.