Rådet for
Den Europæiske Union

Bruxelles, den 22. marts 2022
(OR. en)

7474/22
ADD 3

Interinstitutionel sag:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	22. marts 2022
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	SWD(2022) 68 final
Vedr.:	ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE RESUMÉ AF KONSEKVENSANALYSEN Ledsagedokument til Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer

Hermed følger til delegationerne dokument SWD(2022) 68 final.

Bilag: SWD(2022) 68 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 22.3.2022
SWD(2022) 68 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Indledning

I 2020 steg antallet af væsentlige hændelser orkestreret af avancerede og vedholdende trusselsaktører i EU's institutioner, organer og agenturer voldsomt. Dette afspejles i det antal af kriminaltekniske kopier, som CERT-EU analyserede i 2020, idet tallet er tredoblet sammenlignet med 2019 og tidoblet siden 2018.

Forskellene i cybersikkerhedskapaciteten og udgifterne til IT-sikkerhed i EU's institutioner, organer og agenturer er imidlertid slående og resulterer i et bredt spektrum af cybersikkerhedsmodenhed på tværs af EU's institutioner, organer og agenturer. Derudover viser en analyse af trusselsbilledet og statistikkerne over IT-sikkerhedshændelser, at EU-institutionernes, -organernes og -agenturernes cybereksponering kun bliver større fremover.

2. Målsætninger

De mangler, der er konstateret, har i sidste ende resulteret i et utilstrækkeligt niveau af cybermodstandsdygtighed i EU's institutioner, organer og agenturer, fragmenteret finansiering af IT-sikkerhed og en skæv holdning til IT-sikkerhed.

Formålet med en lovgivningsmæssig retsakt er at indføre foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer. Dette vil fremme og garantere, at cybersikkerhedsmodenheden holder trit med den fremskyndte digitalisering af EU's institutioner, organer og agenturer.

3. Et interinstitutionelt råd og en ramme for cybersikkerhed

Forslaget om et interinstitutionelt råd for cybersikkerhed samt en ramme for cybersikkerhed har til formål at indføre foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU's institutioner, organer og agenturer, der gør det muligt at strømline efter en ramme, der tager højde for cybersikkerhedstrusler i alle EU's institutioner, organer og agenturer, og etablere overvågning og rapportering til et interinstitutionelt råd for cybersikkerhed.

Forslaget ajourfører CERT-EU's mission og opgaver i lyset af den ændrede og øgede digitalisering af EU's institutioner, organer og agenturer de senere år samt trusselsbilledet for cybersikkerheden, der løbende udvikler sig.

Der er ingen direkte virkninger eller budgetmæssige konsekvenser for medlemsstaterne eller borgerne i EU.

Retsgrundlaget for denne forordning er artikel 298 i traktaten om Den Europæiske Unions funktionsmåde, hvori det fastsættes, at Unionens institutioner, organer, kontorer og agenturer under udførelsen af deres opgaver støtter sig til en åben, effektiv og uafhængig europæisk forvaltning.

Dette forslag bygger på strategien for EU's sikkerhedsunion (COM(2020) 605 final) og EU's strategi for cybersikkerhed for det digitale årti (JOIN(2020) 18 final).

4. Konklusion

Et interinstitutionelt råd for cybersikkerhed og en ramme for cybersikkerhed bidrager til opnåelsen af de fleste af de påtænkte mål på relativt effektiv og lønsom vis og på en måde, der hænger sammen med EU's politik på andre områder med bredest mulig støtte fra interessenterne. Den valgte løsning er den bedst gennemførlige i lyset af de gældende retlige begrænsninger, som vi arbejder under, og samme model for alle ville ikke afspejle den

heterogene modenhed i EU's institutioner, organer og agenturer, der eksisterer i dag, eller de forskelle, der hersker for så vidt angår teknologiske risici og kompleksitet.