Rådet for
Den Europæiske Union

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

7474/22
ADD 1

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.:	COM(2022) 122 final - Annexes.
Vedr.:	BILAG 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 COM(2022) 122 final - Annexes..

Bilag: COM(2022) 122 final - Annexes.

EUROPA-
KOMMISSIONEN

Bruxelles, den 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

BILAG

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

BILAG I

Følgende områder skal være omfattet af referencescenariet for cybersikkerhed:

(1) cybersikkerhedspolitikken, herunder mål og prioriteter for sikkerheden i net- og informationssystemer, navnlig hvad angår brugen af cloud computing-tjenester (jf. artikel 4, stk. 19, i direktiv [proposal NIS 2]) og tekniske foranstaltninger med henblik på at muliggøre telearbejde

(2) organisering af cybersikkerheden, herunder fastlæggelse af roller og ansvarsområder

(3) forvaltning af aktiver, herunder en liste over IT-aktiver og en kortlægning af IT-netværket

(4) adgangskontrol

(5) driftssikkerhed

(6) kommunikationssikkerhed

(7) erhvervelse, udvikling og vedligeholdelse af systemer

(8) forholdet til leverandører

(9) styring af hændelser, herunder tilgange til forbedring af beredskab, reaktion og genopretning i forbindelse med hændelser, og samarbejde med CERT-EU såsom vedligeholdelse af sikkerhedsmonitorering og logning

(10) styring af driftskontinuitet og krisestyring og

(11) uddannelse i cybersikkerhed, bevidstgørelse og kurser.

BILAG II

EU's institutioner, organer og agenturer skal som minimum arbejde med følgende specifikke cybersikkerhedsforanstaltninger i forbindelse med gennemførelsen af referencescenariet for cybersikkerhed og i deres cybersikkerhedsplaner i overensstemmelse med vejledende dokumenter og henstillinger udstedt af IICB:

(1) konkrete skridt hen imod en nultillidsarkitektur (dvs. en sikkerhedsmodel, et sæt systemkonstruktionsprincipper og en koordineret cybersikkerheds- og systemforvaltningsstrategi baseret på en anerkendelse af, at trusler findes både inden for og uden for traditionelle netværksgrænser)

(2) indførelsen af multifaktorautentificering som standard for alle net- og informationssystemer

(3) etableringen af forsyningssikkerhed for så vidt angår software ved hjælp af kriterier for sikker udvikling og evaluering af software

(4) forbedring af indkøbsprocedurerne med henblik på at fremme et højt fælles cybersikkerhedsniveau ved hjælp af:

   (a) fjernelsen af kontraktmæssige hindringer, der begrænser IT-tjenesteleverandørernes deling af oplysninger om cybertrusler, sårbarheder og hændelser med CERT-EU

   (b) indførelsen af en kontraktmæssig forpligtelse til at indberette cybertrusler, sårbarheder og hændelser samt til at have passende beredskab og overvågning i forbindelse med hændelser.