Europeiska unionens råd

Bryssel den 22 mars 2022
(OR. en)

7474/22
ADD 1

Interinstitutionellt ärende:
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

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	22 mars 2022
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2022) 122 final - Annexes
Ärende:	BILAGOR till förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

För delegationerna bifogas dokument – COM(2022) 122 final - Annexes.

Bilaga: COM(2022) 122 final - Annexes

EUROPEISKA
KOMMISSIONEN

Bryssel den 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

BILAGOR

till

förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

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

BILAGA I

Följande områden ingår i baslinjen för cybersäkerhet:

(1) Policy för cybersäkerhet, inbegripet mål och prioriteringar för säkerhet i nätverks- och informationssystem, särskilt när det gäller användningen av molntjänster (i den mening som avses i artikel 4.19 i direktiv [förslag till NIS 2]) och tekniska lösningar för att möjliggöra distansarbete.

(2) Organisation av cybersäkerhet, inbegripet fastställande av roller och ansvarsområden.

(3) Förvaltning av tillgångar, inbegripet inventering av digitala tillgångar och it-nätverkskartografi.

(4) Åtkomstkontroll.

(5) Driftssäkerhet.

(6) Kommunikationssäkerhet.

(7) Förvärv, utveckling och underhåll av system.

(8) Leverantörsförbindelser.

(9) Incidenthantering, inbegripet strategier för att förbättra beredskap inför, hantering av och återställning efter incidenter samt samarbete med CERT-EU, såsom underhåll av säkerhetsövervakning och loggning.

(10) Hantering av driftskontinuitet och krishantering.

(11) Utbildning, medvetandehöjande åtgärder och utbildningsprogram inom cybersäkerhet.

BILAGA II

Unionens institutioner, organ och byråer ska vidta åtminstone följande specifika cybersäkerhetsåtgärder vid genomförandet av baslinjen för cybersäkerhet och i sina cybersäkerhetsplaner, i linje med vägledningar och rekommendationer från IICB:

(1) Konkreta åtgärder för att uppnå nolltillitsarkitektur (dvs. en säkerhetsmodell, ett antal principer för systemets utformning och en samordnad strategi för cybersäkerhet och systemhantering baserade på det faktum att det finns en hotbild både inom och utanför traditionella nätverksgränser).

(2) Införande av flerfaktorsautentisering som standard i nätverks- och informationssystem.

(3) Inrättande av säkerhet i leveranskedjan för programvara genom kriterier för utveckling och utvärdering av säker programvara.

(4) Förbättrade upphandlingsregler för att underlätta en hög gemensam cybersäkerhetsnivå genom

(a) att undanröja avtalsmässiga hinder som begränsar informationsutbytet från leverantörer av it-tjänster om incidenter, sårbarheter och cyberhot med CERT-EU,

(b) att införa en avtalsenlig skyldighet att rapportera incidenter, sårbarheter och cyberhot samt att ha lämpliga åtgärder för hantering och övervakning av incidenter.