Rada
Evropské unie

Brusel 22. března 2022
(OR. en)

**7474/22**
**ADD 1**

**Interinstitucionální spis:**
**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**

**NÁVRH**

| | |
|---|---|
| Odesílatel: | Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise |
| Datum přijetí: | 22. března 2022 |
| Příjemce: | Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie |
| Č. dok. Komise: | COM(2022) 122 final - Annexes |
| Předmět: | PŘÍLOHY návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie |

Delegace naleznou v příloze dokument COM(2022) 122 final - Annexes.

Příloha: COM(2022) 122 final - Annexes

EVROPSKÁ
KOMISE

V Bruselu dne 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

# PŘÍLOHY

**návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,**

**kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie**

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

## PŘÍLOHA I

V základním souboru opatření k zajištění kybernetické bezpečnosti je třeba řešit následující oblasti:

1) politika v oblasti kybernetické bezpečnosti, včetně cílů a priorit v oblasti bezpečnosti sítí a informačních systémů, zejména souvisejících s využíváním služeb cloud computingu (ve smyslu čl. 4 odst. 19 směrnice [návrh směrnice NIS 2]) a s technickými opatřeními k umožnění práce na dálku;

2) organizace kybernetické bezpečnosti, včetně vymezení úloh a odpovědnosti;

3) správa aktiv, včetně seznamu aktiv v oblasti informačních technologií a zmapování sítí informačních technologií;

4) kontrola přístupu;

5) bezpečnost operací;

6) bezpečnost komunikací;

7) akvizice, vývoj a údržba systémů;

8) dodavatelské vztahy;

9) řízení incidentů, včetně přístupů pro zlepšení připravenosti na incidenty, reakce na incidenty a zotavení z incidentů, a spolupráce s centrem CERT-EU, jako je zachování monitorování a vedení protokolů bezpečnosti;

10) řízení kontinuity provozu a krizové řízení a

11) vzdělávání v oblasti kybernetické bezpečnosti, zvyšování povědomí a programy odborné přípravy.

## PŘÍLOHA II

Orgány, instituce a jiné subjekty Unie při provádění základního souboru opatření k zajištění kybernetické bezpečnosti a v jejich plánu kybernetické bezpečnosti řeší alespoň tato specifická opatření v oblasti kybernetické bezpečnosti, a to v souladu s pokyny a doporučeními výboru IICB:

1) konkrétní kroky pro přechod k architektuře nulové důvěry (což znamená bezpečnostní model, soubor zásad pro navrhování systémů a koordinovaná strategie kybernetické bezpečnosti a řízení systémů založená na uznání toho, že hrozby existují uvnitř i vně tradičních hranic sítě);

2) přijetí multifaktoriálního ověřování jako normy u sítí a informačních systémů;

3) zabezpečení softwarového dodavatelského řetězce prostřednictvím kritérií pro bezpečný vývoj a hodnocení softwaru

4) posílení pravidel pro zadávání veřejných zakázek s cílem usnadnit dosažení vysoké společné úrovně kybernetické bezpečnosti prostřednictvím:

   a) odstranění smluvních překážek, které omezují sdílení informací ohledně incidentů, zranitelných míst a kybernetických hrozeb obdržených od poskytovatelů služeb informačních technologií s centrem CERT-EU,

   b) smluvní povinnosti hlásit incidenty, zranitelná místa a kybernetické hrozby a smluvní povinnosti mít zavedeny vhodné reakce na incidenty a monitorování incidentů.