Rada
Európskej únie

V Bruseli 22. marca 2022
(OR. en)

7474/22
ADD 1

Medziinštitucionálny 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

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	22. marca 2022
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2022) 122 final – Annexes
Predmet:	PRÍLOHY k Návrhu NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

Delegáciám v prílohe zasielame dokument COM(2022) 122 final – Annexes.

Príloha: COM(2022) 122 final – Annexes

EURÓPSKA
KOMISIA

V Bruseli 22. 3. 2022
COM(2022) 122 final

ANNEXES 1 to 2

PRÍLOHY

k

Návrhu NARIADENIA EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

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

PRÍLOHA I

Nasledujúce oblasti sa budú riešiť v základných kybernetickobezpečnostných pravidlách:

1. politika v oblasti kybernetickej bezpečnosti vrátane cieľov a priorít v rámci bezpečnosti sietí a informačných systémov, najmä v súvislosti s používaním služieb cloud computingu [v zmysle článku 4 ods. 19 smernice (návrh NIS 2)] a technických opatrení umožňujúcich teleprácu;
2. organizácia kybernetickej bezpečnosti vrátane vymedzenia úloh a povinností;
3. správa aktív vrátane inventára aktív IT a kartografie sietí IT;
4. kontrola prístupov;
5. bezpečnosť operácií;
6. komunikačná bezpečnosť;
7. nákup, vývoj a údržba systémov;
8. vzťahy s dodávateľmi;
9. riadenie incidentov vrátane prístupov v záujme zlepšenia pripravenosti a reakcie na incidenty a obnovy po incidentoch a spolupráce s CERT-EU, ako je udržiavanie monitorovania bezpečnosti a vedenia záznamov;
10. riadenie kontinuity činností a krízové riadenie a
11. vzdelávanie, zvyšovanie informovanosti a programy odbornej prípravy v oblasti kybernetickej bezpečnosti.

PRÍLOHA II

Inštitúcie, orgány a agentúry Únie riešia pri vykonávaní základných kybernetickobezpečnostných pravidiel a v rámci svojich plánov kybernetickej bezpečnosti v súlade s usmerňovacími dokumentmi a odporúčaniami IICB aspoň tieto špecifické opatrenia v oblasti kybernetickej bezpečnosti:

1. konkrétne kroky pre prechod k architektúre s nulovou dôverou (t. j. bezpečnostný model, súbor zásad navrhovania systémov a koordinovaná stratégia kybernetickej bezpečnosti a riadenia systému založená na uznaní toho, že hrozby existujú v rámci tradičných hraníc siete aj mimo nich);
2. prijatie dvojstupňovej autentifikácie ako normy v sieťach a informačných systémoch;
3. zavedenie bezpečnosti dodávateľského reťazca týkajúceho sa softvéru prostredníctvom kritérií bezpečného vývoja a hodnotenia softvéru;
4. posilnenie pravidiel obstarávania s cieľom uľahčiť dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti prostredníctvom:
    a) odstránenia zmluvných prekážok, ktoré obmedzujú poskytovanie informácií o incidentoch, zraniteľnostiach a kybernetických hrozbách od poskytovateľov služieb IT tímu CERT-EU;
    b) zmluvnej povinnosti oznamovať incidenty, zraniteľnosti a kybernetické hrozby, ako aj mať zavedenú primeranú reakciu na incidenty a monitorovanie incidentov.