Rada
Európskej únie

V Bruseli 20. apríla 2023
(OR. en)

8512/23
ADD 1

Medziinštitucionálny spis:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	19. apríla 2023
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	COM(2023) 209 final - Annex
Predmet:	PRÍLOHY k NARIADENIU EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

Delegáciám v prílohe zasielame dokument COM(2023) 209 final - Annex.

Príloha: COM(2023) 209 final - Annex

EURÓPSKA
KOMISIA

V Štrasburgu 18. 4. 2023
COM(2023) 209 final

ANNEX

PRÍLOHY

k

NARIADENIU EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

PRÍLOHA

Nariadenie (EÚ) 2021/694 sa mení takto:

1. V prílohe I sa oddiel/kapitola „Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera“ nahrádza takto:

„Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera

Programom sa stimuluje posilnenie, budovanie a nadobúdanie kapacít nevyhnutných na zabezpečenie digitálneho hospodárstva, spoločnosti a demokracie v Únii posilnením priemyselného potenciálu a konkurencieschopnosti Únie v oblasti kybernetickej bezpečnosti, ako aj zlepšením možností verejného a súkromného sektora chrániť občanov a podniky pred kybernetickými hrozbami, a to aj podporou vykonávania smernice (EÚ) 2016/1148.

Počiatočné a v prípade potreby následné akcie v rámci tohto cieľa zahŕňajú:

1. Spoločné investovanie s členskými štátmi do vyspelého vybavenia, infraštruktúry a know-how v oblasti kybernetickej bezpečnosti, ktoré sú nevyhnutné na ochranu kritických infraštruktúr a Jednotného digitálneho trhu ako celku. Takéto spoločné investovanie by mohlo zahŕňať investície do kvantových zariadení a dátových zdrojov kybernetickej bezpečnosti, situačného povedomia v kybernetickom priestore ***vrátane vnútroštátnych centier bezpečnostných operácií a cezhraničných centier bezpečnostných operácií, ktoré tvoria európsky kybernetický štít***, ako aj do ďalších nástrojov, ktoré sa sprístupnia verejnému a súkromnému sektoru v celej Európe.

2. Rozšírenie existujúcich technologických kapacít a prepojenie kompetenčných centier v členských štátoch a zabezpečenie toho, aby tieto kapacity zodpovedali potrebám verejného sektora a priemyslu, a to aj prostredníctvom produktov a služieb, ktorými sa zvyšuje kybernetická bezpečnosť a dôvera na Jednotnom digitálnom trhu.

3. Zabezpečenie rozsiahleho zavádzania účinných a najmodernejších riešení v oblasti kybernetickej bezpečnosti a dôvery v členských štátoch. Takéto zavádzanie zahŕňa posilnenie ochrany a bezpečnosti produktov od ich návrhu až po ich komerčné využitie.

4. Podpora odstraňovania nedostatku zručností v oblasti kybernetickej bezpečnosti, napríklad zosúladením programov v uvedenej oblasti, ich prispôsobením konkrétnym potrebám daného odvetvia a uľahčením prístupu k cielenej špecializovanej odbornej príprave.

5. ***Podpora solidarity medzi členskými štátmi pri príprave na významné kybernetické incidenty a reakcii na ne prostredníctvom cezhraničného nasadenia služieb kybernetickej bezpečnosti vrátane podpory vzájomnej pomoci medzi orgánmi verejnej správy a vytvorenia rezervy dôveryhodných poskytovateľov v oblasti kybernetickej bezpečnosti na úrovni Únie.“***

2. V prílohe II sa oddiel/kapitola „Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera“ nahrádza takto:

„Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera

3.1. Počet infraštruktúr alebo nástrojov kybernetickej bezpečnosti alebo oboje, získaných prostredníctvom spoločného verejného obstarávania[1].

3.2. Počet používateľov a používateľských komunít s prístupom k európskym zariadeniam kybernetickej bezpečnosti.

3.3. Počet akcií, ktorými sa podporuje pripravenosť na kybernetické incidenty a reakcia na ne v rámci mechanizmu na riešenie kybernetických núdzových situácií.“

PRÍLOHA […]