Rada
Európskej únie

V Bruseli 20. marca 2019
(OR. en)

7737/19

CYBER 101	RELEX 287
COPEN 118	TELECOM 141
COPS 92	DAPIX 109
COSI 52	CATS 43
DATAPROTECT 98	CSC 111
IND 102	CSCI 47
JAI 313	IA 106
JAIEX 44	EJUSTICE 44
POLMIL 31	

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	19. marca 2019
Komu:	Delegácie
Č. predch. dok.:	6866/19
Predmet:	Závery Rady o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ

Delegáciám v prílohe zasielame závery Rady o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ, ktoré 19. marca 2019 prijala Rada pre všeobecné záležitosti.

PRÍLOHA

Závery Rady o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ

Rada Európskej únie,

1. PRIPOMÍNAJÚC svoje závery s názvom Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ[1];

2. PRIPOMÍNAJÚC svoje závery o koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu[2];

3. PRIPOMÍNAJÚC svoje závery o budovaní vonkajších kybernetických kapacít[3];

4. ZDÔRAZŇUJÚC, že vysoká úroveň bezpečnosti sietí a informačných systémov sa môže zabezpečiť posilnením kapacít a spôsobilostí členských štátov a inštitúcií, agentúr a orgánov EÚ v oblasti kybernetickej bezpečnosti, ako aj následným posilnením ich kybernetickej odolnosti;

5. VÍTAJÚC pokrok, ktorý dosiahli členské štáty pri posilňovaní jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT);

6. OCEŇUJÚC vytvorenie siete jednotiek CSIRT zo strany členských štátov s aktívnou podporou Komisie a agentúry ENISA, ako aj posilnenú spoluprácu na strategickej úrovni prostredníctvom skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti (NIS), ktorá sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA;

---

1 14435/17 (závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ z 20. novembra 2017)

2 10086/18 (závery o koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu z 26. júna 2018)

3 10496/18 (závery Rady o usmerneniach EÚ týkajúcich sa budovania vonkajších kybernetických kapacít z 26. júna 2018)

7. ZDÔRAZŇUJÚC kľúčovú úlohu, ktorú skupina pre spoluprácu v oblasti NIS zohráva pri poskytovaní usmernení potrebných na to, aby sa čo najviac zosúladil prístup, pokiaľ ide o transpozíciu smernice NIS[4] v celej EÚ, ako aj o riešenie dôležitých otázok kybernetickej bezpečnosti;

8. UZNÁVAJÚC existujúcu podporu, ktorú Komisia poskytuje členským štátom na účely budovania kapacít jednotiek CSIRT prostredníctvom Nástroja na prepájanie Európy;

9. UZNÁVAJÚC podporu poskytovanú orgánom presadzovania práva na účely budovania kapacít v oblasti boja proti počítačovej kriminalite prostredníctvom Fondu pre vnútornú bezpečnosť a agentúry CEPOL;

10. VÍTAJÚC aktualizáciu politického rámca EÚ pre kybernetickú obranu s cieľom viac podporiť rozvoj spôsobilostí členských štátov v oblasti kybernetickej obrany;

11. OCEŇUJÚC pokrok, ktorý členské štáty dosiahli vo vykonávaní smernice NIS;

12. POZNAMENÁVAJÚC, že kybernetická bezpečnosť je zložitou, vzájomne závislou a neustále sa meniacou oblasťou, ktorá si vyžaduje prispôsobenie politického a právneho rámca novým technologickým trendom a novým technológiám, ako sú napríklad umelá inteligencia, blockchain a kvantová výpočtová technika;

---

[4] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016).

13. ZDÔRAZŇUJÚC, že programy odbornej prípravy a vzdelávania súvisiace s kybernetickou bezpečnosťou, ako aj zvyšovanie informovanosti a povedomia o bezpečnostných hrozbách pre koncových používateľov majú kľúčový význam, pokiaľ ide o zníženie rizík v oblasti kybernetickej bezpečnosti;

14. ZDÔRAZŇUJÚC, že kybernetické cvičenia sú účinnými nástrojmi na hodnotenie a ďalšie zlepšovanie úrovne pripravenosti EÚ a jej členských štátov na boj proti kybernetickým incidentom a krízam veľkého rozsahu;

15. PRIPOMÍNAJÚC, že kybernetický priestor je bez hraníc, čo znamená, že cezhraničné a medziodvetvové perspektívy a spolupráca sú neochvejnou zásadou činností a iniciatív budovania kybernetických kapacít;

16. ZDÔRAZŇUJÚC význam spolupráce medzi verejným sektorom, súkromným sektorom a akademickou obcou, a to najmä prostredníctvom projektov spolupráce;

17. ZDÔRAZŇUJÚC význam civilno-vojenskej spolupráce, práce na dosiahnutí spoločných cieľov v kybernetickej oblasti s cieľom zabezpečiť koherentnú a účinnú reakciu na kybernetické hrozby;

18. BERIE NA VEDOMIE pokrok, ktorý dosiahla skupina členských štátov pri vytváraní tímov rýchlej kybernetickej reakcie na účely prehĺbenia dobrovoľnej spolupráce v kybernetickej oblasti prostredníctvom vzájomnej pomoci;

19. VÍTA rokovania, ktoré sa v Rade vedú o návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier, ktorý predložila Komisia;

20. NABÁDA k aktívnej účasti na prebiehajúcej práci skupiny pre spoluprácu v oblasti NIS, najmä pokiaľ ide o budovanie kybernetických kapacít;

21. PODPORUJE prebiehajúcu prácu skupiny pre spoluprácu v oblasti NIS na koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu;

22. VYZÝVA členské štáty, aby vytvárali svoje vnútroštátne stratégie v oblasti kybernetickej bezpečnosti a uplatňovali hľadisko kybernetickej bezpečnosti a zohľadňovali pri tom požiadavky špecifické pre konkrétne sektory;

23. VYZÝVA členské štáty, aby nepretržite monitorovali, hodnotili/posudzovali vplyv opatrení prijatých na posilnenie kybernetickej odolnosti a zlepšenie kybernetických spôsobilostí a kapacít na vnútroštátnej úrovni;

24. VYZÝVA členské štáty, aby začlenili otázku kybernetickej bezpečnosti a digitálnu gramotnosť do učebných plánov na všetkých úrovniach vzdelávania (základné, sekundárne, terciárne, celoživotné vzdelávanie) v prípade potreby na základe súčasných a budúcich pracovných profilov;

25. VYZÝVA členské štáty, aby pre verejnosť a koncových používateľov uskutočňovali iniciatívy na účely informovanosti o kybernetickej bezpečnosti a kybernetickej hygieny zamerané na zamestnancov verejného sektora;

26. NABÁDA členské štáty na uskutočňovanie cvičení v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni, ako aj na ich uskutočňovanie a/alebo účasť na nich na úrovni EÚ na účely testovania a školení v súvislosti so strategickými a technologickými aspektmi, ako aj na účinné rozvíjanie nevyhnutných zručností v praxi;

27. VYZÝVA členské štáty, aby ďalej rozvíjali technické a prevádzkové spôsobilosti svojich jednotiek CSIRT v oblasti kybernetickej bezpečnosti, pokiaľ ide o predchádzanie incidentom, ich zmierňovanie a reakciu na ne;

28. VYZÝVA Komisiu a agentúru ENISA, aby naďalej podporovali členské štáty pri rozvíjaní kapacít a spôsobilostí siete jednotiek CSIRT na účely lepšej spolupráce, výmeny informácií o incidentoch a účinnej reakcie na cezhraničné incidenty veľkého rozsahu;

29. VYZÝVA členské štáty, aby naďalej pomáhali orgánom presadzovania práva rozvíjať špecifické kompetencie v oblasti koordinácie s príslušnými európskymi orgánmi s cieľom účinne bojovať proti počítačovej kriminalite na úrovni EÚ;

30. VYZÝVA členské štáty, aby zvýšili investície do budovania kybernetických kapacít;

31. VYZÝVA Komisiu a agentúru ENISA, aby realizovali programy a odbornú prípravu na zvyšovanie informovanosti o kybernetickej bezpečnosti so zameraním na zamestnancov inštitúcií, agentúr a orgánov EÚ;

32. VYZÝVA EÚ a jej členské štáty, aby si na dobrovoľnom základe vymieňali informácie a najlepšie postupy s cieľom prispieť k identifikácii a riešeniu hlavných potrieb budovania kybernetických kapacít na vnútroštátnej úrovni a na úrovni EÚ;

33. VYZÝVA EÚ a jej členské štáty, aby podporovali výskum v oblasti kybernetickej bezpečnosti a propagovali otázku kybernetickej bezpečnosti v ďalších oblastiach štúdia, a dosiahli tak spojenie rôznych odvetví výskumu a rozvoja súvisiaceho s kybernetickou bezpečnosťou do uceleného celku, a aby v rámci výskumu v oblasti kybernetickej bezpečnosti podporovali excelentnosť;

34. VYZÝVA EÚ a jej členské štáty, aby zabezpečili výskum v oblasti kybernetickej bezpečnosti, a to pri zohľadňovaní potrieb spoločnosti a zavádzaní výsledkov výskumu na trh;

35. VYZÝVA EÚ a jej členské štáty, aby v rámci výziev na verejné obstarávanie v oblasti IKT podľa potreby zohľadňovali otázku kybernetickej bezpečnosti.