Rada
Evropské unie

Brusel 20. března 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	

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	19. března 2019
Příjemce:	Delegace
Č. předchozího dokumentu:	6866/19
Předmět:	Závěry Rady o budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU

Delegace naleznou v příloze závěry Rady o budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU, které přijala Rada pro obecné záležitosti na zasedání konaném dne 19. března 2019.

PŘÍLOHA

Závěry Rady o budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU

Rada Evropské unie,

1. PŘIPOMÍNAJÍC své závěry ke sdělení „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“[1];

2. PŘIPOMÍNAJÍC závěry o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[2];

3. PŘIPOMÍNAJÍC své závěry o budování vnějších kybernetických kapacit[3];

4. ZNOVU PŘIPOMÍNAJÍC, že vysokou míru bezpečnosti sítí a informačních systémů je možno zajistit zvýšením kapacit a schopností členských států a orgánů, agentur a subjektů EU v oblasti kybernetické bezpečnosti a následným posílením jejich kybernetické odolnosti;

5. VÍTAJÍC pokrok dosažený členskými státy při posilování bezpečnostních týmů typu CSIRT (týmy CSIRT);

6. OCEŇUJÍC vytvoření sítě týmů CSIRT členskými státy za aktivní podpory Komise a Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), jakož i posílenou spolupráci na strategické úrovni prostřednictvím skupiny pro spolupráci v oblasti bezpečnosti sítí složené z členských států, Komise a agentury ENISA;

---

1 Dokument 14435/17 (závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, 20. listopadu 2017).

2 Dokument 10086/18 (závěry o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize, 26. června 2018).

3 Dokument 10496/18 (závěry Rady o pokynech EU pro budování vnějších kybernetických kapacit, 26. června 2018).

7. ZDŮRAZŇUJÍC klíčovou úlohu skupiny pro spolupráci v oblasti bezpečnosti sítí při poskytování nezbytného vedení s cílem co nejvíce harmonizovat přístup při provádění směrnice o bezpečnosti sítí a informací[4] napříč EU, jakož i při řešení příslušných problémů v oblasti kybernetické bezpečnosti;

8. UZNÁVAJÍC stávající podporu poskytovanou Komisí prostřednictvím Nástroje pro propojení Evropy členským státům při budování kapacity týmů CSIRT;

9. UZNÁVAJÍC podporu poskytovanou donucovacím orgánům při budování kapacit pro boj proti kyberkriminalitě prostřednictvím Fondu pro vnitřní bezpečnost a Agentury Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL);

10. VÍTAJÍC aktualizaci politického rámce EU pro kybernetickou obranu s cílem dále podpořit rozvoj schopností v oblasti kybernetické obrany členských států;

11. OCEŇUJÍC pokrok dosažený při provádění směrnice o bezpečnosti sítí a informací členskými státy;

12. KONSTATUJÍC, že kybernetická bezpečnost je komplexní oblastí vyznačující se vzájemnou závislostí jednotlivých částí, jež se neustále proměňuje a vyžaduje přizpůsobování politického a právního rámce novým směrům technologického vývoje a nově vznikajícím technologiím, jako je umělá inteligence, technologie blockchain a kvantová výpočetní technika;

---

[4] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016).

13. ZDŮRAZŇUJÍC, že programy odborné přípravy a vzdělávání týkající se kybernetické bezpečnosti, jakož i informace a zvyšování povědomí o bezpečnostních hrozbách pro koncové uživatele jsou pro snížení rizik spojených s kybernetickou bezpečností klíčové;

14. VYZDVIHUJÍC, že účinnými nástroji pro posouzení a další zlepšení úrovně připravenosti EU a jejích členských států na řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí jsou kybernetická cvičení;

15. ZNOVU PŘIPOMÍNAJÍC, že kybernetický prostor nemá hranic, což znamená, že přeshraniční a meziodvětvová perspektiva a spolupráce představují pevné zásady činností a iniciativ budování kybernetické kapacity;

16. ZDŮRAZŇUJÍC význam spolupráce mezi veřejným sektorem, soukromým sektorem a akademickou obcí, zejména prostřednictvím projektů spolupráce;

17. ZDŮRAZŇUJÍC význam civilně-vojenské spolupráce zaměřené na společné cíle v oblasti kybernetiky, má-li být zajištěna soudržná a účinná reakce na kybernetické hrozby;

18. BERE NA VĚDOMÍ pokrok dosažený skupinou členských států při rozvoji týmů rychlé kybernetické reakce s cílem prohloubit dobrovolnou spolupráci v oblasti kybernetiky prostřednictvím vzájemné pomoci;

19. VÍTÁ probíhající diskusi v Radě o návrhu Komise, jehož předmětem je nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center;

20. VYBÍZÍ k aktivní účasti na probíhající činnosti skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, zejména pokud jde o budování kybernetických kapacit;

21. PODPORUJE probíhající činnost skupiny pro spolupráci v oblasti bezpečnosti sítí a informací věnovanou koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize;

22. VYZÝVÁ členské státy, aby v činnosti vycházely ze svých vnitrostátních strategií v oblasti kybernetické bezpečnosti a aby problematiku kybernetické bezpečnosti náležitě zohledňovaly se zřetelem ke konkrétním požadavkům jednotlivých odvětví;

23. VYZÝVÁ členské státy, aby prováděly průběžné sledování, hodnocení či posuzování dopadu opatření přijatých k posílení kybernetické odolnosti a aby posilovaly kybernetické schopnosti a kapacity na vnitrostátní úrovni;

24. VYZÝVÁ členské státy, aby začlenily kybernetickou bezpečnost a počítačovou gramotnost do vzdělávacích programů na všech úrovních vzdělávání (základní, střední, vysokoškolské, celoživotní učení), a to v relevantních případech na základě existujících i budoucích profesních profilů;

25. VYZÝVÁ členské státy, aby prováděly osvětové iniciativy v oblasti kybernetických hrozeb a kybernetické hygieny pro veřejnost i koncové uživatele, a to se zaměřením na zaměstnance ve veřejném odvětví;

26. VYBÍZÍ členské státy, aby prováděly cvičení v oblasti kybernetické bezpečnosti na vnitrostátní úrovni a na úrovni EU nebo aby se na takových cvičeních na úrovni EU podílely, s cílem testovat strategické a technologické aspekty a formou výcviku se na ně připravit, jakož i účinně a na praktické úrovni rozvinout nezbytné dovednosti;

27. VYZÝVÁ členské státy, aby dále rozvíjely technické a operační schopnosti svých týmů CSIRT v oblasti kybernetické bezpečnosti, pokud jde o předcházení incidentům, jejich zmírňování a reakci na incidenty;

28. VYZÝVÁ Komisi a agenturu ENISA, aby pokračovaly v podpoře členských států při rozvíjení kapacity a schopností sítě týmů CSIRT s cílem lépe spolupracovat, sdílet informace o incidentech a účinně reagovat na rozsáhlé přeshraniční incidenty;

29. VYZÝVÁ členské státy, aby byly nadále nápomocny donucovacím orgánům při rozvíjení zvláštních pravomocí v koordinaci s příslušnými evropskými orgány, s cílem účinně bojovat proti kyberkriminalitě na úrovni EU;

30. VYZÝVÁ členské státy, aby zvýšily své investice do budování kybernetických kapacit;

31. VYZÝVÁ Komisi a agenturu ENISA, aby prováděly osvětové programy a programy odborné přípravy v oblasti kybernetické bezpečnosti se zaměřením na zaměstnance orgánů, agentur a subjektů EU;

32. VYZÝVÁ EU a její členské státy, aby dobrovolně sdílely informace a osvědčené postupy s cílem přispět ke zjišťování a řešení hlavních potřeb v oblasti budování kybernetických kapacit na vnitrostátní úrovni i na úrovni EU;

33. VYZÝVÁ EU a její členské státy, aby podpořily výzkum v oblasti kybernetické bezpečnosti, prosazovaly kybernetickou bezpečnost jako téma v dalších oborech, spojily různé oblasti výzkumu a vývoje týkající se kybernetické bezpečnosti do jednoho souvislého celku a podporovaly ve výzkumu kybernetické bezpečnosti excelenci;

34. VYZÝVÁ EU a její členské státy, aby rozvíjely výzkum v oblasti kybernetické bezpečnosti zohledňující potřeby společnosti a začleňující výsledky výzkumu do trhu;

35. VYZÝVÁ EU a její členské státy, aby na otázky kybernetické bezpečnosti braly v relevantních případech zřetel při zadávání zakázek v oblasti IKT.