Rada
Unii Europejskiej

Bruksela, 20 marca 2019 r.
(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	

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	19 marca 2019 r.
Do:	Delegacje
Nr poprz. dok.:	6866/19
Dotyczy:	Konkluzje Rady w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa przyjęte przez Radę do Spraw Ogólnych 19 marca 2019 r.

ZAŁĄCZNIK

Konkluzje Rady w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa

Rada Unii Europejskiej,

1. PRZYWOŁUJĄC swoje konkluzje pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”[1];

2. PRZYWOŁUJĄC swoje konkluzje w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę[2];

3. PRZYWOŁUJĄC swoje konkluzje w sprawie budowania zewnętrznych zdolności cyfrowych[3];

4. PRZYPOMINAJĄC, że wysoki poziom bezpieczeństwa sieci i systemów informacyjnych może być zapewniony poprzez zwiększenie potencjału i zdolności w zakresie cyberbezpieczeństwa państw członkowskich oraz instytucji, agencji i organów UE, i tym samym poprzez zwiększenie ich cyberodporności;

5. Z ZADOWOLENIEM PRZYJMUJĄC postępy poczynione przez państwa członkowskie we wzmacnianiu zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);

6. WYRAŻAJĄC UZNANIE w związku z ustanowieniem sieci CSIRT przez państwa członkowskie przy aktywnym wsparciu Komisji i agencji ENISA, a także w związku ze wzmocnioną współpracą na szczeblu strategicznym w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji, w skład której wchodzą państwa członkowskie, Komisja i ENISA;

---

1 Dok. 14435/17 (konkluzje Rady z 20 listopada 2017 r. w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”.

2 10086/18 (konkluzje z 26 czerwca 2018 r. w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę).

3 Dok. 10496/18 (konkluzje Rady z 26 czerwca 2018 r. w sprawie wytycznych dotyczących budowania przez UE zewnętrznych zdolności cyfrowych).

7. PODKREŚLAJĄC kluczową rolę grupy współpracy ds. bezpieczeństwa sieci i informacji w zapewnianiu strategicznych wskazówek w celu maksymalnego zbliżenia stosowanego podejścia do transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji[4]w całej UE, a także w rozwiązywaniu istotnych kwestii związanych z cyberbezpieczeństwem;

8. DOSTRZEGAJĄC wsparcie, jakie Komisja zapewnia obecnie państwom członkowskim – za pośrednictwem instrumentu „Łącząc Europę" – na rzecz budowania potencjału zespołów CSIRT;

9. DOSTRZEGAJĄC wsparcie zapewniane organom ścigania – za pośrednictwem Funduszu Bezpieczeństwa Wewnętrznego i CEPOL-u – na rzecz budowania potencjału do walki z cyberprzestępczością;

10. Z ZADOWOLENIEM PRZYJMUJĄC aktualizację unijnych ram polityki w zakresie cyberobrony mającą na celu dalsze wspieranie rozwijania zdolności państw członkowskich w zakresie cyberobrony;

11. WYRAŻAJĄC UZNANIE dla poczynionych przez państwa członkowskie postępów we wdrażaniu dyrektywy w sprawie bezpieczeństwa sieci i informacji;

12. ZAUWAŻAJĄC, że cyberbezpieczeństwo jest złożoną, współzależną od innych i nieustannie zmieniającą się dziedziną, wymagającą dostosowania politycznych i prawnych ram do nowych tendencji technologicznych i nowych technologii, takich jak sztuczna inteligencja, technologia blockchain i informatyka kwantowa;

---

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016).

13. PODKREŚLAJĄC, że programy kształcenia i szkolenia związane z cyberbezpieczeństwem, a także informowanie użytkowników końcowych i zwiększanie ich wiedzy na temat zagrożeń bezpieczeństwa mają kluczowe znaczenie dla zmniejszenia zagrożeń dla cyberbezpieczeństwa;

14. PODKREŚLAJĄC, że ćwiczenia w dziedzinie cyberbezpieczeństwa to skuteczne narzędzia oceny i dalszego podnoszenia poziomu gotowości UE i jej państw członkowskich do reagowania na cyberincydenty i cyberkryzysy na dużą skalę;

15. PRZYPOMINAJĄC, że cyberprzestrzeń nie ma granic, co oznacza, że transgraniczne i międzysektorowe perspektywy i współpraca to konieczne elementy działań i inicjatyw na rzecz budowania cyberpotencjału;

16. PODKREŚLAJĄC znaczenie współpracy między sektorem publicznym, prywatnym i środowiskami akademickimi, w szczególności poprzez projekty oparte na współpracy;

17. PODKREŚLAJĄC znaczenie współpracy cywilno-wojskowej, w ramach której pracuje się na rzecz realizacji wspólnych celów związanych z cyberprzestrzenią, by zapewnić spójne i skuteczne reagowanie na zagrożenia dla cyberbezpieczeństwa;

18. ODNOTOWUJE postępy osiągnięte przez grupę państw członkowskich w tworzeniu zespołów szybkiego reagowania na cyberincydenty w celu pogłębiania dobrowolnej współpracy w cyberprzestrzeni prowadzonej na zasadzie pomocy wzajemnej;

19. Z ZADOWOLENIEM PRZYJMUJE toczące się dyskusje na forum Rady na temat wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji;

20. ZACHĘCA do aktywnego udziału w bieżących pracach grupy współpracy ds. bezpieczeństwa sieci i informacji, zwłaszcza w zakresie budowania cyberpotencjału;

21. ZACHĘCA do kontynuowania prac grupy współpracy ds. bezpieczeństwa sieci i informacji w zakresie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę;

22. ZWRACA SIĘ do państw członkowskich, aby rozwijały swoje krajowe strategie cyberbezpieczeństwa i uwzględniały kwestię cyberbezpieczeństwa w innych politykach, biorąc pod uwagę specyficzne wymogi sektorowe;

23. ZWRACA SIĘ do państw członkowskich, aby prowadziły ciągły monitoring i dokonywały oceny wyników środków podjętych w celu poprawy cyberodporności i zwiększenia potencjału i zdolności w cyberbeprzestrzeni na szczeblu krajowym;

24. APELUJE do państw członkowskich, by włączały aspekty cyberbezpieczeństwa i umiejętności cyfrowych w programy nauczania na wszystkich poziomach kształcenia (podstawowego, średniego, wyższego, uczenia się przez całe życie), w stosownych przypadkach w oparciu o istniejące i przyszłe profile zawodowe;

25. ZWRACA SIĘ do państw członkowskich, by przeprowadzały inicjatywy na rzecz zwiększania wiedzy na temat cyberbezpieczeństwa i na rzecz higieny cyberbezpieczeństwa skierowane do ogółu społeczeństwa i użytkowników końcowych i koncentrujące się na pracownikach sektora publicznego;

26. ZACHĘCA państwa członkowskie do przeprowadzania na szczeblu krajowym ćwiczeń w dziedzinie cyberbezpieczeństwa, a także do prowadzenia takich ćwiczeń na szczeblu UE lub uczestnictwa w nich, by sprawdzić i doskonalić swoje umiejętności pod kątem kwestii strategicznych i technologicznych, a także by skutecznie rozwijać niezbędne umiejętności od strony praktycznej;

27. APELUJE do państw członkowskich, by nadal rozwijały techniczne i operacyjne zdolności z zakresu cyberbezpieczeństwa swoich zespołów CSIRT, co się tyczy zapobiegania incydentom, ograniczania ich skutków i reagowania na nie;

28. WZYWA Komisję i agencję ENISA, by nadal udzielały swojego wsparcia przy rozwijaniu przez państwa członkowskie potencjału i zdolności sieci CSIRT, tak by zespoły te lepiej współpracowały, dzieliły się informacjami i skutecznie reagowały na transgraniczne incydenty na dużą skalę;

29. ZWRACA SIĘ do państw członkowskich, by nadal wspomagały organy ścigania w rozwijaniu szczególnych kompetencji w zakresie koordynacji działań z właściwymi organami europejskimi z myślą o skutecznym zwalczaniu cyberprzestępczości na szczeblu UE;

30. APELUJE do państw członkowskich, by zwiększały inwestycje w budowanie potencjału odnośnie do cyberprzestrzeni;

31. WZYWA Komisję i agencję ENISA, by przeprowadziły kampanie informacyjne zwiększające wiedzę o cyberbezpieczeństwie i szkolenia dla pracowników instytucji, agencji i organów UE;

32. WZYWA UE i jej państwa członkowskie do dzielenia się informacjami i najlepszymi praktykami na zasadzie dobrowolności, by przyczyniać się do identyfikowania i zaspokajania głównych potrzeb – na szczeblu krajowym i unijnym – w zakresie budowania potencjału odnośnie do cyberprzestrzeni;

33. ZACHĘCA UE i jej państwa członkowskie, by wspierały badania nad cyberbezpieczeństwem i by propagowały uwzględnianie cyberbezpieczeństwa w innych obszarach nauki, integrując w spójną całość różne obszary badawczo-rozwojowe związane z cyberbezpieczeństwem i by sprzyjały doskonałości w dziedzinie badań nad cyberbezpieczeństwem;

34. ZACHĘCA UE i jej państwa członkowskie do rozwijania badań nad cyberbezpieczeństwem odzwierciedlających potrzeby społeczne i mających na celu wykorzystanie wyników tych badań na rynku;

35. APELUJE do UE i jej państw członkowskich, by w stosownych przypadkach uwzględniały kwestię cyberbezpieczeństwa w procedurach udzielania zamówień publicznych dotyczących ICT.