Rada
Unii Europejskiej

Bruksela, 12 grudnia 2017 r.
(OR. en)

15748/17

CYBER 215
TELECOM 362
ENFOPOL 618
JAI 1206
MI 959
COSI 333
JAIEX 117
RELEX 1122
IND 377
CSDP/PSDC 720
COPS 400
POLMIL 167

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	12 grudnia 2017 r.
Do:	Delegacje
Nr poprz. dok.:	14435/17 + COR 1
Dotyczy:	Plan działania w celu wdrożenia konkluzji Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE” - Plan działania (12 grudnia 2017)

Delegacje otrzymują w załączeniu plan działania w celu wdrożenia konkluzji Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE” przyjęty przez Radę do Spraw Ogólnych w dniu 12 grudnia 2017 r.

ZAŁĄCZNIK

Niniejszy plan działania w celu wdrożenia konkluzji Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE" to dokument strategiczny opracowany w odpowiedzi na postulat Rady Europejskiej z 19 października 2017 r. i Rady z 24 października 2017 r. Jak wskazano w tych konkluzjach Rady z dnia 20 listopada 2017 r., niniejszy plan działania jest dokumentem dynamicznym, który będzie regularnie poddawany przeglądowi i aktualizowany przez Radę. Ma on służyć jako instrument kontroli horyzontalnej i strategicznego monitorowania wdrażania konkluzji Rady oraz działań wyszczególnionych poniżej.

Działanie[1]	**Kierownictwo / główna odpowiedzialność**	**Zainteresowane podmioty lub inne zaangażowane strony**	**Termin**	**Postęp**	**Uwagi/komentarze**
Zapewnienie pełnej i skutecznej transpozycji i wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji					
Transpozycja i wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji	Państwa członkowskie; Komisja Europejska		maj 2018 r.	Postępy zostaną podsumowane przez Komisje i omówione w ramach grupy współpracy	
Zapewnienie skutecznej współpracy strategicznej między państwami członkowskimi w ramach grupy współpracy	Państwa członkowskie / prezydencja Rady	Komisja Europejska, ENISA		Postępy zostaną podsumowane w ramach regularnego sprawozdania grupy współpracy	Prace grupy współpracy opisano w sposób bardziej szczegółowy w stosownym dwuletnim programie jej prac

[1] W stosownych przypadkach działania są realizowane z uwzględnieniem zasobów przewidzianych w wieloletnich ramach finansowych.

Osiągnięcie pełnej operacyjności sieci CSIRT	Państwa członkowskie / prezydencja Rady	ENISA, Komisja Europejska		Poczynione postępy zostaną podsumowane w ramach regularnego sprawozdania sieci CSIRT dla grupy współpracy	
Wzmocnienie reakcji UE na cyberincydenty na dużą skalę poprzez prowadzenie ogólnoeuropejskich ćwiczeń w dziedzinie cyberbezpieczeństwa					
Prowadzenie ćwiczeń w dziedzinie dyplomacji cyfrowej dotyczących wykorzystania ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne	ESDZ	Państwa członkowskie, Komisja Europejska i ENISA		Kolejne prezydencje Rady, dyskusje na temat ćwiczeń dotyczących wykorzystania odnośnych ram rozpoczęto podczas prezydencji EE	
Prowadzenie regularnych ćwiczeń CYBER EUROPE	Prezydencja wraz z państwami członkowskimi	Państwa członkowskie, w tym sieć CSIRT, ENISA, ESDZ, Komisja Europejska			Częstotliwość określona w ramach mandatu ENISA i podczas dyskusji Zarządu ENISA

Prowadzenie regularnych ćwiczeń strategicznych w dziedzinie cyberbezpieczeństwa w różnych składach Rady	Prezydencja	wspierana przez ESDZ lub Komisję Europejską		W trakcie prezydencji EE przeprowadzono ćwiczenia EU CYBRID 2017 dla Rady do Spraw Zagranicznych (Obrona)	Częstotliwość ćwiczeń określona przez państwa członkowskie w ramach Rady
Przyjęcie przez współprawodawców ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ENISA, „Agencji UE ds. Cyberbezpieczeństwa", uchylenia rozporządzenia (UE) nr 526/2013, oraz w sprawie certyfikacji bezpieczeństwa cybernetycznego w zakresie technologii informacyjno-komunikacyjnych („akt w sprawie cyberbezpieczeństwa")[2]					
Szczegółowe omówienie wniosku ustawodawczego na forum horyzontalnej grupy roboczej w celu wypracowania podejścia ogólnego	Prezydencja BG		czerwiec 2018 r.	Analiza wniosku prowadzona przez prezydencję EE	
Sfinalizowanie negocjacji między współprawodawcami	Prezydencja AT		grudzień 2018 r.		Termin orientacyjny

[2] Realizacja odbywa się bez uszczerbku dla kompetencji Parlamentu Europejskiego.

Utworzenie sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa i europejskiego centrum badań naukowych i kompetencji w dziedzinie cyberbezpieczeństwa					
Przedstawienie oceny skutków i projektu budżetu oraz stosownych instrumentów prawnych w celu utworzenia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa i europejskiego centrum badań naukowych i kompetencji w dziedzinie cyberbezpieczeństwa	Komisja Europejska	Państwa członkowskie, ESDZ, EDA	czerwiec 2018 r.		Po przedstawieniu odnośnych instrumentów decyzje dotyczące dalszych działań zostaną podjęte przez państwa członkowskie w ramach Rady
Rozpoczęcie fazy pilotażowej w ramach programu „Horyzont 2020”	Komisja Europejska	Państwa członkowskie, grupy współpracy ds. bezpieczeństwa sieci i informacji	koniec 2018 r. / początek 2019 r.		

Wypracowanie zdolności Europy do oceny solidności mechanizmów kryptograficznych wykorzystywanych w produktach i usługach dostępnych dla obywateli, przedsiębiorstw i rządów w ramach jednolitego rynku cyfrowego	Państwa członkowskie		2019		
Zapewnienie wystarczającego finansowania, aby wesprzeć budowanie cyberodporności oraz działania na rzecz badań naukowych i rozwoju w zakresie cyberbezpieczeństwa w całej UE					
Zapewnienie wystarczającego finansowania na rzecz cyberbezpieczeństwa z uwzględnieniem dostępnych zasobów	Państwa członkowskie, Komisja Europejska		2020		

Zwiększenie udziału w budowaniu sektora publicznego na rzecz budowania cyberodporności oraz nasilenie działań na rzecz badań naukowych i rozwoju w zakresie cyberbezpieczeństwa	Państwa członkowskie		2020		
Zachęcanie sektora prywatnego do inwestycji na rzecz budowania cyberodporności i nasilenia działań na rzecz badań naukowych i rozwoju w zakresie cyberbezpieczeństwa	Komisja Europejska	wspierana przez ECSO	2018		
Zwiększenie inwestycji w zastosowania nowych technologii w cyberbezpieczeństwie	Komisja Europejska, państwa członkowskie	wspierane przez ECSO	2020		

Analiza możliwego wniosku w sprawie utworzenia funduszu pomocy w sytuacjach zagrażających cyberbezpieczeństwu	Rada[3]				Działanie to będzie rozpatrywane dopiero po przedstawieniu stosownego wniosku przez Komisję Europejską
Utrzymanie wystarczających środków finansowych na działania w zakresie cyberbezpieczeństwa w ramach istniejących instrumentów i uzgodnionych programów	Państwa członkowskie, Komisja Europejska	EBI	2020		

[3] Bez uszczerbku dla kompetencji Parlamentu Europejskiego, stosownie do przypadku.

Zapewnienie wiarygodnych, sprawdzonych i skoordynowanych sposobów świadczenia usług w zakresie cyberbezpieczeństwa i zarządzania tymi usługami w instytucjach UE					
Doprecyzowanie i ujednolicenie zarządzania w dziedzinie cyberbezpieczeństwa w instytucjach, organach i agencjach UE	Rada, Komisja Europejska i ESDZ	Instytucje, organy i agencje UE	2020	Sprawozdanie na temat zarządzania i postępów w tym zakresie należy przedstawić Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni	
Zapewnienie odpowiednich zasobów i wsparcia na rzecz rozwoju CERT-UE	Instytucje, organy i agencje UE		2020	CERT-UE regularnie składa Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni sprawozdania na temat zagrożeń dla cyberbezpieczeństwa w odniesieniu do podmiotów uczestniczących w CERT-UE. Przydział zasobów dla CERT-UE może być omawiany podczas stosownych dyskusji na forum Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni	
Położenie większego nacisku na świadomość zagrożeń dla cyberbezpieczeństwa, umiejętności cyfrowe oraz kształcenie i szkolenie w tym zakresie					
Nasilenie kampanii informacyjnych na temat zagrożeń dla cyberbezpieczeństwa w państwach członkowskich	Państwa członkowskie	ENISA	2020		

Uwzględnianie w większym stopniu tematyki cyberbezpieczeństwa w programach akademickich i edukacyjnych oraz w programach szkoleń zawodowych	Państwa członkowskie	Komisja Europejska, ECSO	2020	Monitorowanie postępów przez państwa członkowskie i Komisję Europejską	
Utworzenie sieci punktów kontaktowych w dziedzinie edukacji	Państwa członkowskie	ENISA	2020		
Włączanie w główny nurt i rozwijanie programów staży w dziedzinie cyberbezpieczeństwa	Państwa członkowskie	Komisja Europejska, ECSO	2020		
Prowadzenie działań informacyjnych na tematy związane z cyberbezpieczeństwem w organach administracji publicznej, które uczestniczą w kluczowej działalności społecznej lub gospodarczej	Państwa członkowskie		2020	Zobowiązanie na rzecz higieny cyberbezpieczeństwa podpisane przez sześć państw członkowskich, ESDZ i EDA w maju 2015 r.	

Zwiększenie zdolności UE do zapobiegania wrogim działaniom w cyberprzestrzeni, ich powstrzymywania i wykrywania oraz reagowania na nie					
Uwzględnienie kwestii cyberbezpieczeństwa w istniejących mechanizmach zarządzania kryzysowego na szczeblu UE	Komisja Europejska, Rada	ESDZ, agencje UE	2018		
Odpowiednie uwzględnienie kwestii reagowania na incydenty w zakresie cyberbezpieczeństwa w krajowych mechanizmach zarządzania kryzysowego oraz zapewnienie niezbędnych procedur współpracy na szczeblu UE	Państwa członkowskie		2018		
Aktualizacja ram polityki UE w zakresie cyberobrony	Państwa członkowskie, ESDZ, EDA, Komisja Europejska		2018		
Zachęcanie do współpracy między cywilnymi i wojskowymi służbami reagowania na incydenty	Państwa członkowskie				

Utworzenie platformy szkolenia i kształcenia w dziedzinie cyberobrony	Komisja Europejska	ESDZ, EDA, EKBiO	koniec 2018 r.		
Pełne wykorzystanie proponowanych inicjatyw w dziedzinie obronności, aby przyspieszyć rozwój zdolności w zakresie cyberobrony w UE	Państwa członkowskie	ESDZ, EDA, Komisja Europejska			Projekty w zakresie cyberobrony mogą być opracowywane w ramach PESCO, jeżeli państwa uczestniczące w PESCO uznają, że jest to konieczne EFR może finansować projekty w zakresie cyberobrony, jeżeli zostanie to przewidziane w programach prac

Nasilenie walki z cyberprzestępczością i usuwanie przeszkód utrudniających skuteczne wymierzanie sprawiedliwości w sprawach karnych dotyczących cyberprzestrzeni					
Opracowanie planu działania w celu zwalczania rosnącej przestępczości w darknecie	Europol	Państwa członkowskie	początek 2018 r.	COSI powinien zatwierdzić plan działania i monitorować jego wdrażanie	
Wdrożenie zaproponowanych przez Komisję praktycznych środków w celu rozwiązania problemu dotyczącego szyfrowania w kontekście postępowań karnych, przy jednoczesnym zapewnieniu poszanowania praw człowieka i podstawowych wolności	Komisja Europejska	państwa członkowskie, Europol	w toku	Postępy monitorowane przez CATS	

Zwiększenie zdolności organów ścigania i organów sądowych w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw	Państwa członkowskie	Komisja Europejska		Postępy monitorowane przez COSI; wraz z dostawcami usług dostępu do internetu należy zaproponować dobrowolne kodeksy postępowania, aby ograniczyć liczbę abonentów poszczególnych adresów IPv4 poprzez uruchomienie technologii będących alternatywą dla technologii translacji adresów sieciowych klasy operatorskiej (Carrier-Grade NAT) Na forum UE poświęconym internetowi Komisja Europejska ma poruszyć z dostawcami treści internetowych kwestię rejestrowania numerów portów źródłowych.	Uwzględnienie zaleceń sprawozdania końcowego grupy roboczej GENVAL z 7. rundy wzajemnej oceny dotyczącej zwalczania cyberprzestępczości

Zachęcanie sektora prywatnego do uruchomienia IPv6, np. poprzez ewentualne wprowadzenie stosownych wymogów w ramach zamówień publicznych	Państwa członkowskie	Komisja Europejska	w toku	Postępy będą monitorowane przez odpowiednie organy przygotowawcze Rady (Horyzontalna Grupa Robocza ds. Cyberprzestrzeni, COSI)	
Opracowanie i zatwierdzenie protokołu dotyczącego reagowania w sytuacjach nadzwyczajnych w celu zapewnienia skoordynowanych działań w zakresie egzekwowania prawa podejmowanych w reakcji na cyberincydenty na dużą skalę	Europol	Państwa członkowskie, Komisja Europejska, ESDZ, Rada	początek 2018 r.	COSI powinien zatwierdzić protokół i monitorować jego wdrażanie	
Przedstawienie wniosku ustawodawczego dotyczącego ułatwienia transgranicznego dostępu organów ścigania do dowodów elektronicznych	Komisja Europejska	Rada, Parlament Europejski	początek 2018 r.	Postępy monitorowane przez CATS	

Przedstawienie sprawozdanie z postępów we wdrażaniu konkretnych środków na rzecz usprawnienia transgranicznego dostępu do dowodów elektronicznych (w tym współpracy między organami ścigania a dostawcami usług z sektora prywatnego)	Komisja Europejska	Państwa członkowskie	koniec 2017 r.	Postępy monitorowane przez CATS	
Utworzenie w pełni operacyjnej platformy umożliwiającej państwom członkowskim bezpieczne udostępnianie i przekazywanie formularzy online europejskiego nakazu dochodzeniowego oraz dowodów elektronicznych	Komisja Europejska	Państwa członkowskie	połowa 2019 r.	Postępy monitorowane przez CATS	

Pogłębienie międzynarodowej współpracy na rzecz otwartej, wolnej, pokojowej i bezpiecznej globalnej cyberprzestrzeni					
Kontynuowanie dialogu z międzynarodowymi partnerami, aby zapewnić ogólnoświatowe wsparcie dla otwartej, wolnej, pokojowej i bezpiecznej globalnej cyberprzestrzeni	ESDZ, Rada, Komisja Europejska	Państwa członkowskie	połowa 2019 r.	Postępy monitorowane przez Horyzontalną Grupę Roboczą ds. Cyberprzestrzeni	
Ustanowienie unijnej sieci w zakresie budowania zdolności w dziedzinie cyberbezpieczeństwa i opracowanie unijnych wytycznych w zakresie budowania takich zdolności	ESDZ, Komisja Europejska, przy wsparciu państw członkowskich				Możliwa współpraca z Globalnym Forum Wiedzy Cyfrowej (GFCE)
Rozwijanie współpracy między UE a NATO w dziedzinie kształcenia i szkolenia	ESDZ, Rada, EDA	Państwa członkowskie			
Kontynuowanie współpracy między UE a NATO w zakresie ćwiczeń dotyczących cyberobrony oraz wymiany dobrych praktyk w zakresie zarządzania kryzysowego	ESDZ, Rada	Państwa członkowskie, EDA, Komisja Europejska			

Zajęcie się kwestią kluczowych zastosowań nowych technologii w cyberbezpieczeństwie w ramach odnośnych systemów kontroli eksportu	Państwa członkowskie, Komisja Europejska				
Opracowanie i zaprezentowanie jednolitego stanowiska UE w sprawie decyzji dotyczących zarządzania internetem na szczeblu globalnym	Rada, Komisja Europejska i ESDZ	Państwa członkowskie	2018 r i w toku	COSI powinien ułatwić przyjęcie wspólnego stanowiska UE w sprawie systemu WHOIS zgodnego z ogólnym rozporządzeniem o ochronie danych, dzięki czemu zapewniony zostanie terminowy i szybki dostęp do rzetelnych informacji na temat rejestrowania nazw domen i właścicieli adresów IP (danych WHOIS) w uzasadnionych przypadkach, m.in. do celów egzekwowania prawa, ochrony konsumenta, ochrony praw własności intelektualnej oraz działań w zakresie cyberbezpieczeństwa.	