Rada
Unii Europejskiej

Bruksela, 17 października 2022 r.
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	17 października 2022 r.
Do:	Delegacje
Nr poprz. dok.:	12930/22
Dotyczy:	Konkluzje Rady w sprawie bezpieczeństwa łańcucha dostaw ICT – Konkluzje Rady zatwierdzone przez Radę na posiedzeniu 17 października 2022 r.

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie bezpieczeństwa łańcucha dostaw ICT w wersji zatwierdzonej przez Radę na posiedzeniu 17 października 2022 r.

ZAŁĄCZNIK

Konkluzje Rady w sprawie bezpieczeństwa łańcucha dostaw ICT

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC swoje konkluzje:

– z 20 listopada 2017 r. w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”,

– w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa,

– w sprawie znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczenia zagrożeń dla bezpieczeństwa związanych z 5G,

– w sprawie kształtowania cyfrowej przyszłości Europy,

– pt. „Odbudowa przyspieszająca przechodzenie na bardziej dynamiczny, odporny i konkurencyjny przemysł europejski”,

– w sprawie cyberbezpieczeństwa urządzeń podłączonych do internetu,

– w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę,

– w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni,

– w sprawie sprawozdania specjalnego Europejskiego Trybunału Obrachunkowego nr 3/2002 pt. „Wprowadzenie sieci 5G w UE: opóźnienia we wdrażaniu i nierozwiązane kwestie związane z bezpieczeństwem”,

PRZYWOŁUJĄC konkluzje Rady Europejskiej:

– z 1–2 października 2020 r. w sprawie COVID-19, jednolitego rynku, polityki przemysłowej, kwestii cyfrowych i stosunków zewnętrznych,

– z 24–25 marca 2022 r. w sprawie rosyjskiej agresji wojskowej na Ukrainę, bezpieczeństwa i obrony, energii, kwestii gospodarczych, COVID-19 i stosunków zewnętrznych,

– z 30–31 maja 2022 r. w sprawie Ukrainy, bezpieczeństwa żywnościowego, bezpieczeństwa i obrony oraz energii,

1. Biorąc pod uwagę rosnące znaczenie, jakie ma dla cyberbezpieczeństwa geopolityka, PODKREŚLA, że Unia Europejska i jej państwa członkowskie muszą zajmować się cyberbezpieczeństwem w sposób kompleksowy i strategiczny. Rosyjska agresja wojskowa na Ukrainę spowodowała poważną zmianę w strategicznej sytuacji Unii Europejskiej i w jej środowisku bezpieczeństwa i pokazała, że Unia Europejska musi być silniejsza i musi dysponować większymi zdolnościami w obszarach bezpieczeństwa i obrony. Uwypukliła, że niezwykle ważne jest odpowiednie uwzględnienie otoczenia geopolitycznego nie tylko przy reagowaniu na szkodliwe działania w cyberprzestrzeni, ale również przy budowaniu i utrzymywaniu odporności technologii informacyjno-komunikacyjnych (ICT). Ma to szczególne znaczenie dla łańcuchów dostaw produktów i usług ICT (łańcuchów dostaw ICT), które mogą zostać zakłócone w ramach rywalizacji geopolitycznej, co unaocznił atak SolarWinds, oraz dotknięte napięciami geopolitycznymi i niestabilnością, jak pokazuje zagrożenie związane z zależnością od rosyjskich dostawców ICT w trakcie trwania rosyjskiej agresji wojskowej na Ukrainę.

2. ZAUWAŻA, że charakter ryzyk związanych z łańcuchem dostaw ICT, który to łańcuch składa się z połączonego zestawu zasobów i procesów należących do różnych podmiotów gospodarczych (zgodnie z definicją w rozporządzeniu (UE) 2019/1020) i zaczyna się od pozyskiwania surowców, a rozciąga na produkcję, przetwarzanie, obsługę i dostarczanie produktów i usług ICT, w tym udzielanie wsparcia podczas cyklu życia produktów i usług ICT, powoduje wyjątkowe wyzwania i ma potencjalnie dalekosiężne konsekwencje. Oprócz ryzyka związanego z niedostępnością produktów ICT, na przykład z powodu niedoborów potrzebnych do ich produkcji surowców krytycznych i półprzewodników, łańcuchy dostaw produktów i usług ICT są narażone na inne zagrożenia. W szczególności mogą je obrać za cel lub niewłaściwie wykorzystywać podmioty działające w złej wierze w wyrafinowany, często ukryty sposób, który ma wpływ na poufność, integralność i dostępność przekazywanych i przechowywanych danych wrażliwych.

3. Dostrzegając, że potrzebne jest podejście uwzględniające wszystkie zagrożenia, aby zabezpieczyć aktywa ICT, UZNAJE znaczenie wniosku dotyczącego dyrektywy w sprawie odporności podmiotów krytycznych dla poprawy bezpieczeństwa fizycznego podmiotów krytycznych i PODKREŚLA, że oprócz zwiększenia odporności na ataki na łańcuchy dostaw przeprowadzane za pomocą cyberśrodków równie ważne jest wzmocnienie całościowo odporności i bezpieczeństwa łańcuchów dostaw ICT względem różnych czynników zagrożenia, takich jak zdarzenia naturalne, awarie systemu, zagrożenia wewnętrzne lub błędy ludzkie. W tym kontekście UZNAJE, że bezpieczeństwo łańcucha dostaw ICT obejmuje zapewnienie ochrony produktów i usług ICT wytwarzanych, dostarczanych, zamawianych i wykorzystywanych w łańcuchach dostaw ICT, w tym poprzez ochronę poszczególnych komponentów i przekazywanych danych.

4. Opierając się na wnioskach wyciągniętych w oparciu o skutki strategicznych zależności Unii Europejskiej od rosyjskich paliw kopalnych, a także skutki zakłóceń w łańcuchach dostaw podczas pandemii COVID-19, w szczególności w odniesieniu do produktów farmaceutycznych i półprzewodników, w przypadku których ujawniono strategiczne zależności UE, ZACHĘCA państwa członkowskie do działań na rzecz zapobieżenia podobnym niepożądanym zależnościom zewnętrznym w odniesieniu do produktów i usług ICT. Ze względu na postępującą cyfryzację społeczeństwa i coraz częstsze wykorzystywanie ICT w infrastrukturach krytycznych należy stale oceniać strategiczne zależności zewnętrzne związane z produktami i usługami ICT oraz ich łańcuchami dostaw, a w stosownych przypadkach zaradzać im.

5. PRZYPOMINA, że osiągnięcie strategicznej autonomii przy jednoczesnym zachowaniu otwartej gospodarki jest kluczowym celem Unii, który obejmuje zidentyfikowanie i ograniczenie strategicznych zależności oraz zwiększenie odporności w najbardziej wrażliwych ekosystemach przemysłowych i konkretnych obszarach, w tym w obszarze cyfrowym. Obejmuje to rozwijanie i rozmieszczanie strategicznych zdolności cyfrowych i infrastruktury cyfrowej, a także wzmacnianie zdolności do dokonywania autonomicznych wyborów technologicznych i, jako jeden z głównych filarów, zapewnianie odpornych i bezpiecznych infrastruktur, produktów i usług służących budowaniu zaufania na jednolitym rynku cyfrowym i w społeczeństwie europejskim, przy jednoczesnym utrzymaniu otwartości, globalnej współpracy z partnerami o podobnych poglądach i konkurencyjności, a także czerpaniu z nich potencjalnych korzyści. Podstawowe wartości Unii Europejskiej chronią w szczególności prywatność, bezpieczeństwo, równość, godność ludzką, praworządność i otwarty charakter internetu jako warunki niezbędne do osiągnięcia procyfrowych i ukierunkowanych na człowieka społeczeństwa, gospodarki i przemysłu.

6. ODNOTOWUJE, że ze względu na zmiany w krajobrazie cyberzagrożeń – takie jak obserwowana w ostatnich latach tendencja do wysoce skutecznych i wyrafinowanych ataków na łańcuchy dostaw (np. SolarWinds, Mimecast czy Kaseya) – zachodzące jednocześnie ze zjawiskiem outsourcingu podstawowych usług ICT i nasilone w wyniku ogólnego uzależnienia od produktów i usług ICT wytwarzanych, dostarczanych lub obsługiwanych przez osoby trzecie, wysoce prawdopodobne jest występowanie w przyszłości większej liczby ataków na łańcuchy dostaw, skutkujących znacznymi szkodami dla gospodarki i społeczeństw. W związku z tym PODKREŚLA, jak ważne dla funkcjonowania jednolitego rynku jest zwiększenie bezpieczeństwa i odporności łańcuchów dostaw ICT, a także zapewnienie dostępności, bezpieczeństwa i różnorodności produktów i usług ICT na jednolitym rynku. W związku z tym UZNAJE potrzebę maksymalizacji i usprawnienia wykorzystywania istniejących unijnych instrumentów i podejść na rzecz osiągnięcia tych celów, a także potrzebę ciągłego dostosowywania się do zmieniającego się krajobrazu cyberzagrożeń poprzez wprowadzanie dodatkowych odpowiednich środków i mechanizmów, w tym w odniesieniu do potencjalnych zagrożeń dla bezpieczeństwa związanych z nowymi i przełomowymi technologiami. ZACHĘCA państwa członkowskie, by w tym kontekście stosowały podejście oparte na ocenie ryzyka z myślą o radzeniu sobie w obliczu rozwoju nowych technologii.

7. UZNAJE, że zrozumienie stale zmieniającego się krajobrazu cyberzagrożeń i złożonego charakteru ataków na łańcuchy dostaw ma zasadnicze znaczenie dla skutecznego ograniczania zagrożeń związanych z łańcuchami dostaw ICT. W związku z tym PODKREŚLA konieczność dostosowania się do nowych zagrożeń poprzez aktywne stałe monitorowanie, analizowanie i ocenianie krajobrazu zagrożeń związanych z łańcuchem dostaw, podnoszenie świadomości i budowanie wiedzy na temat zagrożeń i słabych punktów oraz proaktywne ostrzeganie odpowiednich podmiotów w zindywidualizowany sposób. Z ZADOWOLENIEM PRZYJMUJE prace Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) związane z bezpieczeństwem łańcucha dostaw ICT, w szczególności jej sprawozdanie w sprawie krajobrazu zagrożeń związanych z atakami na łańcuch dostaw.

INSTRUMENTY I PODEJŚCIA MIĘDZYSEKTOROWE

8. POTWIERDZA, jak ważne jest, by państwa członkowskie wzięły pod uwagę potrzebę zdywersyfikowania dostawców krytycznych technologii informacyjno-komunikacyjnych w celu uniknięcia lub ograniczenia tworzenia istotnych zależności od pojedynczych dostawców, zwłaszcza dostawców wysokiego ryzyka, ponieważ zależności takie zwiększają narażenie na skutki wynikające z potencjalnych przerw w dostawach. UZNAJE unikanie uzależnienia od jednego dostawcy i dywersyfikację dostawców ICT za jeden z istotnych elementów w zapewnianiu stabilności i bezpieczeństwa rynku wewnętrznego. PODKREŚLA potrzebę promowania i wdrażania odpowiednich strategii ułatwiających dywersyfikację dostawców i konkurencyjność w sposób neutralny pod względem technologicznym. Ponadto ZACHĘCA do włączenia aspektów związanych z zapobieganiem uzależnieniu od jednego dostawcy do prawodawstwa UE. W tym kontekście WYRAŻA ZADOWOLENIE z proponowanego rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych), którego celem jest zwiększenie interoperacyjności usług przetwarzania danych i usunięcie przeszkód utrudniających zmianę dostawców usług przetwarzania danych.

9. DOSTRZEGA, że bezpieczeństwo łańcucha dostaw ICT ma przełożenie na zamówienia publiczne. PODKREŚLA, że w procedurach udzielania zamówień publicznych należy odpowiednio uwzględnić wagę bezpieczeństwa łańcucha dostaw ICT poprzez wprowadzenie, w stosownych przypadkach, obiektywnych i opartych na analizie ryzyka kryteriów wyboru dotyczących zdolności oferentów do zapewnienia wysokiego poziomu bezpieczeństwa świadczonych usług. APELUJE o znalezienie właściwej równowagi między interesem publicznym, jakim jest, z jednej strony, jak najefektywniejsze i najsprawiedliwsze wykorzystywanie środków publicznych, a z drugiej strony – zabezpieczenie systemów informacyjnych i zapewnienie sprawnego funkcjonowania jednolitego rynku. Aby ułatwić wdrażanie odnośnych przepisów dotyczących zamówień publicznych w świetle zwiększania cyberbezpieczeństwa, ZWRACA SIĘ do Komisji, by do trzeciego kwartału 2023 r. opracowała wytyczne metodologiczne, aby zachęcić instytucje zamawiające do położenia odpowiedniego nacisku na praktyki w zakresie cyberbezpieczeństwa stosowane przez oferentów i ich podwykonawców oraz by przeprowadziła ocenę i, w razie potrzeby, przedstawiła wnioski dotyczące zmiany lub uzupełnienia odpowiedniego prawodawstwa dotyczącego zamówień publicznych.

10. UZNAJE, że bezpośrednie inwestycje zagraniczne związane z produktami i usługami ICT, choć zapewniają korzyści gospodarcze i społeczne państwom członkowskim, przedsiębiorstwom i obywatelom, mogą pociągać za sobą ryzyka dla bezpieczeństwa i porządku publicznego, i ODNOTOWUJE, że unijny mechanizm monitorowania bezpośrednich inwestycji zagranicznych – wraz z odpowiednimi krajowymi systemami monitorowania, które zapewniają środki przeciwdziałania takim zagrożeniom – mógłby być również stosowany jako użyteczne narzędzie służące ochronie bezpieczeństwa i odporności łańcucha dostaw ICT, przyczyniając się do eliminowania inwestycji wysokiego ryzyka mogących wpływać na takie bezpieczeństwo i odporność. DOSTRZEGA, że informacje wymieniane i udostępniane za pośrednictwem tego mechanizmu mogą pomóc państwom członkowskim lepiej ocenić ewentualne zagrożenia dla bezpieczeństwa łańcuchów dostaw ICT i podjąć odpowiednie niezbędne kroki. APELUJE do właściwych podmiotów krajowych, by w stosownych przypadkach uwzględniły również ten aspekt mechanizmu monitorowania.

11. W odniesieniu do obronności POTWIERDZA swój apel do Komisji o dokonanie w 2023 r. wraz z państwami członkowskimi oceny zagrożeń dla łańcuchów dostaw infrastruktury krytycznej w różnych dziedzinach, w tym w dziedzinie cyfrowej, związanych z interesami UE w zakresie bezpieczeństwa i obrony, a także o zbadanie możliwości zwiększenia cyberbezpieczeństwa w całym łańcuchu dostaw unijnej bazy technologiczno-przemysłowej sektora obronnego. Ponadto ZWRACA SIĘ do państw członkowskich i Komisji o wzięcie pod uwagę bezpieczeństwa łańcucha dostaw ICT w kontekście realizacji zobowiązań i działań w ramach Strategicznego kompasu.

12. Mając na względzie znaczenie surowców krytycznych i wszelkiego rodzaju półprzewodników jako podstawowych elementów składowych produktów ICT, ZACHĘCA do konstruktywnych negocjacji nad wnioskiem w sprawie rozporządzenia ustanawiającego ramy dotyczące środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników (akt w sprawie czipów) oraz wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (UE) 2021/2085 ustanawiające wspólne przedsięwzięcia w ramach programu „Horyzont Europa” w odniesieniu do Wspólnego Przedsięwzięcia na rzecz Czipów.

INSTRUMENTY DOTYCZĄCE CYBERBEZPIECZEŃSTWA

13. W szczególności w odniesieniu do infrastruktury telekomunikacyjnej UZNAJE osiągnięcia na szczeblu Unii w zakresie poprawy bezpieczeństwa łańcucha dostaw sieci 5G, w szczególności w postaci unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (zestaw narzędzi UE na potrzeby sieci 5G). APELUJE do państw członkowskich o wymianę informacji na temat najlepszych praktyk i metod dotyczących wdrażania środków zalecanych w zestawie narzędzi UE na potrzeby sieci 5G, a w szczególności o stosowanie odpowiednich ograniczeń wobec dostawców wysokiego ryzyka w odniesieniu do kluczowych aktywów określonych w unijnej skoordynowanej ocenie ryzyka jako krytyczne i wrażliwe. PODKREŚLA, że zestaw narzędzi UE na potrzeby sieci 5G stanowi sprawny, oparty na analizie ryzyka instrument służący rozwiązywaniu zidentyfikowanych problemów w zakresie bezpieczeństwa, umożliwiający terminowe i skuteczne zajmowanie się aspektami cyberbezpieczeństwa sieci 5G, przy jednoczesnym poszanowaniu kompetencji państw członkowskich, i UZNAJE, że jest on cennym instrumentem dalszego wzmacniania – przy zachowaniu pełnej przejrzystości – bezpieczeństwa łańcucha dostaw sieci telekomunikacyjnych w skoordynowany sposób, na którym to instrumencie można wzorować narzędzia oceny i ograniczania ryzyka związane z innymi kluczowymi sektorami. PRZYPOMINA o wystosowanym do właściwych organów zaproszeniu do formułowania zaleceń, w oparciu o oceny ryzyka, dla państw członkowskich i Komisji dotyczących wzmocnienia odporności sieci i infrastruktur komunikacyjnych w Unii Europejskiej, w tym dalszego wdrażania zestawu narzędzi UE na potrzeby sieci 5G.

14. ZAUWAŻA, że istotne są podejścia interoperacyjne, które mogą zaradzić problemowi uzależnienia od jednego dostawcy i zmniejszyć ryzyko koncentracji, a jednocześnie poprawić bezpieczeństwo łańcucha dostaw całego spektrum infrastruktury i usług ICT. W szczególności w odniesieniu do sieci 5G UZNAJE w tym względzie potencjalne korzyści wynikające z koncepcji otwartej sieci dostępu radiowego, a jednocześnie PRZYPOMINA o sprawozdaniu na temat cyberbezpieczeństwa otwartej sieci dostępu radiowego opublikowanym przez grupę współpracy ds. bezpieczeństwa sieci i informacji wskazującym, że koncepcja ta jest nadal przedmiotem prac, a jej bezpieczeństwo, przejrzystość i normalizacja znajdują się na wczesnym etapie rozwoju, a także PODKREŚLA, jak ważna jest ocena ryzyka dokonywana każdorazowo przed przejściem na nowe normy lub nową architekturę.

15. PODKREŚLA znaczenie, jakie dla zwiększenia bezpieczeństwa łańcucha dostaw ICT, mają istniejące i przyszłe horyzontalne instrumenty ustawodawcze dotyczące cyberbezpieczeństwa, w szczególności rozporządzenie w sprawie agencji ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie), przyszła dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS 2), wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii, a także wniosek dotyczący rozporządzenia w sprawie horyzontalnych wymogów w zakresie cyberbezpieczeństwa dla produktów z elementami cyfrowymi (akt dotyczący cyberodporności). Ponadto ODNOTOWUJE istotne zmiany wprowadzone w sektorowych rozporządzeniach w sprawie cyberbezpieczeństwa, w szczególności w przyszłym rozporządzeniu w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) obejmującym ramy nadzoru nad zewnętrznymi dostawcami usług ICT, którzy mają kluczowe znaczenie dla podmiotów finansowych. Wspomniane rozporządzenia wprowadzają ogólne obowiązki związane z bezpieczeństwem łańcucha dostaw, a także szczegółowe, konkretne wymogi istotne dla danego sektora. PODKREŚLA przy tym, że dostawcy często dostarczają swoje produkty i usługi w różnych sektorach, a nie na rzecz wyłącznie jednej branży. W związku z tym niezwykle ważne jest zapewnienie, aby wymogi bezpieczeństwa dotyczące łańcucha dostaw były w miarę możliwości ujednolicone we wszystkich odpowiednich sektorach, zwłaszcza tych objętych przyszłą dyrektywą NIS 2 – w celu uniknięcia rozbieżności między obowiązkami nałożonymi na dostawców oraz w celu zmniejszenia obciążenia operatorów w sektorach krytycznych, które to obciążenie wiąże się z ocenianiem przestrzegania tych obowiązków przez dostawców – a jednocześnie aby wspomniane wymogi uwzględniały specyfikę danego sektora.

16. WYRAŻA ZADOWOLENIE z wniosku w sprawie aktu dotyczącego cyberodporności, gdyż jest to ważny instrument ustawodawczy służący przyspieszeniu bezpiecznego rozwoju produktów z elementami cyfrowymi oraz zapewnieniu uwzględniania cyberbezpieczeństwa w całym cyklu życia takich produktów. ZAUWAŻA, że wniosek w sprawie aktu dotyczącego cyberodporności może w znacznym stopniu przyczynić się do wzmocnienia bezpieczeństwa łańcucha dostaw ICT. ZACHĘCA do konstruktywnych negocjacji i terminowego przyjęcia tego aktu.

17. W tym kontekście DOCENIA prace prowadzone obecnie przez agencję ENISA wraz z państwami członkowskimi i innymi interesariuszami, by zapewnić w UE programy certyfikacji produktów, usług i procesów ICT, zgodnie z aktem o cyberbezpieczeństwie, co powinno przyczynić się do podniesienia ogólnego poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. ZACHĘCA wszystkich interesariuszy do udziału w pracach przygotowawczych nad poszczególnymi europejskimi programami certyfikacji w celu zbudowania zaufania do bezpiecznych produktów, procesów i usług ICT oraz wzmocnienia ich odporności i APELUJE do Komisji o szybkie sporządzenie aktów wykonawczych dotyczących europejskich programów certyfikacji po zakończeniu wspomnianych prac przygotowawczych, w szczególności odnośnie do wspólnego opartego na kryteriach europejskiego programu certyfikacji cyberbezpieczeństwa (EUCC). ZAUWAŻA, że europejskie programy certyfikacji powinny w razie potrzeby obejmować wymogi dotyczące bezpieczeństwa łańcucha dostaw, w tym relacji z dostawcami;

18. ZWRACA UWAGĘ na potrzebę dokładnego wdrożenia wszystkich przyszłych przepisów NIS 2 dotyczących bezpieczeństwa łańcucha dostaw ICT. W związku z tym PODKREŚLA znaczenie unijnych skoordynowanych ocen ryzyka krytycznych łańcuchów dostaw (skoordynowanych ocen ryzyka łańcuchów dostaw), krajowych polityk w zakresie bezpieczeństwa łańcucha dostaw i środków bezpieczeństwa związanych z łańcuchem dostaw. ODNOTOWUJE, że należy zwrócić uwagę nie tylko na głównych dostawców, ale również na odpowiednich podwykonawców – w kwestii ryzyka dla bezpieczeństwa głównego dostawcy lub odbiorcy końcowego. Aby ułatwić wdrażanie środków zarządzania ryzykiem w łańcuchu dostaw, ZACHĘCA agencję ENISA do przeprowadzenia, z pomocą grupy współpracy ds. bezpieczeństwa sieci i informacji, przeglądu najlepszych dostępnych praktyk w zakresie zarządzania ryzykiem w łańcuchu dostaw i do zestawienia ich w postaci wytycznych metodologicznych. ZACHĘCA też agencję ENISA do monitorowania inwestycji w bezpieczeństwo łańcucha dostaw ICT dokonywanych przez podmioty, które mają podlegać przyszłej dyrektywie NIS 2.

19. Ponadto ZWRACA UWAGĘ na pożytki, jak i ryzyka związane z korzystaniem z dostawców usług zarządzanych i dostawców usług zarządzanych w zakresie bezpieczeństwa w kontekście bezpieczeństwa łańcucha dostaw. Chociaż korzystanie z usług tych dostawców może znacznie poprawić bezpieczeństwo w ramach organizacji i prowadzić do wyższego poziomu cyberbezpieczeństwa, zdalne zarządzanie systemami i usługami ICT w połączeniu z uprzywilejowanym dostępem do środowiska ICT klientów, którego mogą potrzebować dostawcy usług zarządzanych i dostawcy usług zarządzanych w zakresie bezpieczeństwa, w przypadku udanego ataku na tych dostawców może mieć kaskadowe skutki dla dużej liczby klientów. Dlatego też niezwykle ważne jest, aby dostawcy usług zarządzanych i dostawcy usług zarządzanych w zakresie bezpieczeństwa utrzymywali wysoki poziom własnego bezpieczeństwa wewnętrznego i bezpieczeństwa świadczonych przez siebie usług oraz aby stosowali przejrzyste podejście względem swoich klientów w odniesieniu do bezpieczeństwa świadczonych przez siebie usług. W związku z tym Z ZADOWOLENIEM PRZYJMUJE przyszłe włączenie tych dostawców usług w zakres przygotowywanej dyrektywy NIS 2.

20. Jeżeli chodzi o wdrożenie mechanizmu skoordynowanych ocen ryzyka łańcuchów dostaw zgodnie z przyszłą dyrektywą NIS 2, ODNOTOWUJE znaczenie nietechnicznych czynników ryzyka w tym kontekście, takich jak nadmierny wpływ wywierany na dostawców i usługodawców przez państwa trzecie, i w tym względzie ZWRACA UWAGĘ na czynniki, które można wykorzystać do oceny profilu ryzyka, wymienione w unijnej skoordynowanej ocenie ryzyka dotyczącej cyberbezpieczeństwa sieci 5G. ZWRACA SIĘ do Komisji, by do drugiego kwartału 2023 r., po konsultacji z grupą współpracy ds. bezpieczeństwa sieci i informacji i agencją ENISA, określiła konkretne usługi, systemy lub produkty ICT, w odniesieniu do których można by w pierwszej kolejności przeprowadzić skoordynowane oceny ryzyka łańcucha dostaw.

21. ZAUWAŻA, że zależności od dostawców wysokiego ryzyka, jeśli chodzi o produkty i usługi ICT wykorzystywane do eksploatacji krytycznych sieci i systemów, stanowią strategiczne zagrożenie, które należy ograniczyć za pomocą odpowiednich strategii zarówno na szczeblu krajowym, jak i unijnym oraz w drodze współpracy między państwami członkowskimi i z partnerami międzynarodowymi o podobnych poglądach. Aby ułatwić ograniczanie tego strategicznego ryzyka i wesprzeć skoordynowane oceny ryzyka łańcucha dostaw, ZWRACA SIĘ do grupy współpracy ds. bezpieczeństwa sieci i informacji, by we współpracy z Komisją i agencją ENISA opracowała zestaw środków służących ograniczaniu krytycznych ryzyk w łańcuchach dostaw ICT (zestaw narzędzi na rzecz łańcucha dostaw ICT). Zestaw narzędzi na rzecz łańcucha dostaw ICT powinien opierać się na określonych dla łańcuchów dostaw ICT scenariuszach dotyczących strategicznych zagrożeń i zapewniać środki reagowania na te scenariusze, wykorzystując doświadczenia związane z zestawem narzędzi na potrzeby 5G i doświadczenia zdobyte na szczeblu krajowym. Powinien on w przejrzysty sposób uzupełniać skoordynowane oceny ryzyka łańcucha dostaw w odniesieniu do konkretnych usług, systemów lub produktów ICT dokonywane na mocy przyszłej dyrektywy NIS 2 poprzez oferowanie ogólnych środków ograniczania ryzyka, które można dostosować do konkretnych usług, systemów lub produktów ICT w sposób skalowalny, na podstawie ryzyka zidentyfikowanego w indywidualnych skoordynowanych ocenach ryzyka łańcucha dostaw.

22. PODKREŚLA ważną rolę badań naukowych, innowacji, inwestycji i przedsiębiorczości w obszarze cyfrowym i cyberbezpieczeństwa, a także ważną rolę finansowania takich działań, jeśli chodzi o zapobieganie ewentualnym przyszłym niepożądanym strategicznym zależnościom i wzmacnianie ogólnej odporności łańcuchów dostaw ICT. W tym kontekście PODKREŚLA rolę i znaczenie zarówno strategicznych, jak i wykonawczych zadań Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) oraz sieci krajowych ośrodków koordynacji w przyczynianiu się do maksymalizacji efektów inwestycji służących wzmocnieniu wiodącej roli Unii i jej otwartej strategicznej autonomii w dziedzinie cyberbezpieczeństwa, wsparciu unijnych zdolności i umiejętności technologicznych oraz zwiększeniu globalnej konkurencyjności Unii. W związku z tym APELUJE o szybkie uruchomienie ECCC. ZWRACA SIĘ do ECCC, by uwzględniało w swoim programie strategicznym aspekty bezpieczeństwa łańcucha dostaw ICT, w tym na przykład opracowywanie bezpiecznego oprogramowania, przy jednoczesnym zapewnianiu spójności i komplementarności oraz unikaniu powielania działań. POPIERA zwiększanie europejskiej konkurencyjności w dziedzinie cyberbezpieczeństwa poprzez programy finansowania, takie jak program „Horyzont Europa” w zakresie badań naukowych i innowacji, a także program „Cyfrowa Europa” w zakresie wzmacniania, budowania i nabywania podstawowych zdolności na rzecz gospodarki cyfrowej, społeczeństwa i demokracji w UE.

MECHANIZMY WSPARCIA

23. ZACHĘCA do zwiększania zachęt finansowych na rzecz wprowadzania środków służących wzmacnianiu bezpieczeństwa łańcucha dostaw ICT. APELUJE do ECCC, Komisji i odpowiednich interesariuszy, w trybie priorytetowym, również z myślą o zbliżającym się wdrożeniu dyrektywy NIS 2, o zbadanie możliwości uwzględnienia aspektów bezpieczeństwa łańcucha dostaw ICT w przyszłych zaproszeniach do składania wniosków w kontekście programów prac w dziedzinie cyberbezpieczeństwa w ramach programu „Cyfrowa Europa" i programu „Horyzont Europa" lub o rozważenie wykorzystania wszelkich innych odpowiednich możliwości finansowania. Te możliwości finansowania powinny między innymi pozwolić organizacjom wspierać utrzymywanie wysokiego poziomu cyberbezpieczeństwa w zakresie zamówień na produkty i usługi ICT w całym łańcuchu dostaw, w szczególności w kontekście zastępowania konkretnych krytycznych usług, systemów lub produktów ICT, które w wyniku przyszłych skoordynowanych ocen ryzyka łańcucha dostaw zostałyby uznane za obarczone wysokim ryzykiem.

24. UZNAJE, że ze względu na globalizację i specjalizację w dziedzinie usług ICT oraz zwiększone uzależnienie od produktów i usług stron trzecich konieczna jest ścisła współpraca w UE i na arenie międzynarodowej w zakresie dzielenia się wiedzą i know-how w gronie odpowiednich interesariuszy, których ZACHĘCA do wypracowania zdecydowanego i skoordynowanego stanowiska zapewniającego bezpieczeństwo łańcucha dostaw ICT w kompleksowy sposób. UZNAJE również potrzebę dalszego badania odpowiednich najnowocześniejszych podejść i technik, zarówno w kontekście właściwej podstawowej higieny cyberbezpieczeństwa, jak i długoterminowych rozwiązań służących osiągnięciu bezpiecznych i odpornych łańcuchów dostaw ICT, a także najodpowiedniejszych sposobów ich promowania i potencjalnego włączania do strategii lub innych inicjatyw. DOSTRZEGA w związku z tym, że należy zwrócić szczególną uwagę na zbadanie zalet i wad rozwiązań systemowych, takich jak zasady zerowego zaufania, zestawienie komponentów oprogramowania i podobne rozwiązania długoterminowe. ZALECA wykorzystanie w tym celu grupy współpracy ds. bezpieczeństwa sieci i informacji.

25. ZAUWAŻA korzyści, jakie płyną z monitorowania cyberincydentów i cyberazagrożeń i skutecznej wymiany informacji na ich temat dla zapobiegania atakom w łańcuchu dostaw, wykrywania ich i łagodzenia ich skutków. PODKREŚLA potrzebę dalszego budowania zaufania i pewności wśród państw członkowskich w celu skutecznej wymiany takich informacji. PRZYPOMINA w tym względzie o propozycji Komisji dotyczącej wsparcia państw członkowskich w tworzeniu i umacnianiu centrów monitorowania bezpieczeństwa (SOC), by stworzyć sieć SOC w całej UE, co pozwoli dokładniej monitorować sygnały świadczące o atakach na sieci i przewidywać takie ataki. PRZYPOMINA o potrzebie komplementarności i koordynacji w ramach istniejących sieci i mechanizmów – w szczególności PODKREŚLA rolę, jaką odgrywa w tym względzie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) – oraz o potrzebie dalszego badania potencjału odpowiednich sieci w celu promowania efektywnej, bezpiecznej i niezawodnej kultury wymiany informacji. PRZYPOMINA o wysiłkach podejmowanych przez państwa członkowskie wspierane przez UE, by utworzyć sektorowe, krajowe i regionalne zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz krajowe lub europejskie ośrodki wymiany i analizy informacji jako część skutecznej sieci partnerstw na rzecz cyberbezpieczeństwa w Unii.

26. Ze względu na wzajemne powiązania i globalny charakter zagrożeń związanych z łańcuchem dostaw ICT PODKREŚLA znaczenie zajęcia się bezpieczeństwem łańcucha dostaw ICT na szczeblu globalnym i wzmacnianiem go na tym szczeblu. W związku z tym ZALECA wykorzystywanie partnerstw cyfrowych, cyberdialogów i innych odpowiednich inicjatyw UE, w tym, w stosownych przypadkach, umów o wolnym handlu z myślą o promowaniu opartych na analizie ryzyka ocen dostawców produktów ICT i dostawców usług ICT i korzystania z wiarygodnych dostawców oraz z myślą o posługiwaniu się bezpiecznym i innowacyjnym ekosystemem cyfrowym opartym na otwartych, interoperacyjnych i przejrzystych normach. Ponadto PRZYPOMINA o założeniach partnerstw w ramach *Global Gateway* oraz Rady UE–USA ds. Handlu i Technologii i działań jej grup roboczych, z myślą o promowaniu korzystania z dostawców zaufanych / nieobarczonych wysokim ryzykiem oraz opracowaniu mechanizmu finansowania umożliwiającego realizację projektów zwiększających bezpieczeństwo, odporność infrastruktury i usług ICT w państwach trzecich i poziom zaufania do nich, w tym poprzez powstrzymanie się od finansowania zakupów od dostawców niezaufanych / wysokiego ryzyka w sposób, który nie będzie wpływał na technologię.

27. POTWIERDZA swoje zobowiązanie do wnoszenia wkładu w otwartą, wolną, globalną, stabilną i bezpieczną cyberprzestrzeń oraz do jej propagowania, a także do przestrzegania norm, przepisów i zasad odpowiedzialnego zachowania państw w cyberprzestrzeni uzgodnionych w ramach ONZ. W szczególności w odniesieniu do bezpieczeństwa łańcucha dostaw ICT – PRZYPOMINA o normie zatwierdzonej przez grupę ekspertów rządowych ONZ i otwartą grupę roboczą, zachęcającej państwa do podejmowania rozsądnych kroków w celu zapewnienia integralności łańcucha dostaw, w tym poprzez opracowanie obiektywnych środków opartych na współpracy, tak aby użytkownicy końcowi mogli mieć zaufanie do bezpieczeństwa produktów ICT, oraz w celu zapobiegania rozprzestrzenianiu się złośliwych narzędzi i technik ICT i wykorzystywaniu szkodliwych ukrytych funkcji, a także POPIERA szerokie wdrożenie tej normy.