C/2024/1049

9.2.2024

Opinia Europejskiego Komitetu Regionów – Akt UE w sprawie cybersolidarności i odporność cyfrowa

(C/2024/1049)

Sprawozdawca: Pehr GRANFALK (SE/EPL), członek rady gminy Solna

Dokument źródłowy: Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty

COM(2023) 209 final

I. ZALECANE POPRAWKI

COM(2023) 209

Poprawka 1

Motyw 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu we wszystkich sektorach działalności gospodarczej, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.	Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu***, ale także ujawniły słabe punkty*** we wszystkich sektorach działalności gospodarczej, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.

Uzasadnienie

Nie wymaga uzasadnienia.

Poprawka 2

Motyw 3

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy, konieczne jest zwiększenie odporności obywateli, przedsiębiorstw ***i*** podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. […]	Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy, konieczne jest zwiększenie odporności obywateli, przedsiębiorstw***, administracji publicznej szczebla krajowego, regionalnego i lokalnego oraz*** podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. […]

Uzasadnienie

Administracja lokalna i regionalna świadczy usługi zarówno bliskie obywatelom, jak i kluczowe dla społeczeństwa, a także jest jednym z najważniejszych elementów dynamicznego rynku europejskiego.

Poprawka 3

Motyw 29

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe"). Skoordynowane testowanie […]	Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory***, podobnie jak organy administracji publicznej na szczeblu regionalnym i lokalnym, niezależnie od tego, czy w prawie krajowym uznaje się je za wysoce krytyczne,*** należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe"). Skoordynowane testowanie […]

Uzasadnienie

Ponieważ państwa członkowskie mają możliwość wyłączenia władz lokalnych i regionalnych przy wdrażaniu dyrektywy NIS 2 ([1]), należy zapewnić ich uwzględnienie w akcie o cybersolidarności.

Poprawka 4

Motyw 30

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Ponadto w ramach mechanizmu cyberkryzysowego należy oferować wsparcie innych działań w zakresie gotowości i wsparcie gotowości w innych sektorach, nieobjętych skoordynowanym testowaniem podmiotów działających w sektorach ***wysoce*** krytycznych. Działania te mogą obejmować różnego rodzaju krajowe działania związane z gotowością.	Ponadto w ramach mechanizmu cyberkryzysowego należy oferować wsparcie innych działań w zakresie gotowości i wsparcie gotowości w innych sektorach, nieobjętych skoordynowanym testowaniem podmiotów działających w sektorach krytycznych. ***To samo powinno dotyczyć administracji publicznej, niezależnie od tego, czy w prawie krajowym uznaje się ją za kluczową***. Działania te mogą obejmować różnego rodzaju krajowe działania związane z gotowością.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

Uzasadnienie

Władze lokalne i regionalne powinny mieć możliwość korzystania ze wsparcia w ramach mechanizmu cyberkryzysowego.

Poprawka 5

Motyw 33

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i natychmiastowe usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę. Unijna rezerwa cyberbezpieczeństwa powinna zapewniać dostępność i gotowość usług. Usługi z unijnej rezerwy cyberbezpieczeństwa powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom ***działającym w sektorach krytycznych lub wysoce krytycznych*** jako uzupełnienie działań tych organów na szczeblu krajowym. Wnioskując o wsparcie z unijnej rezerwy cyberbezpieczeństwa, państwa członkowskie powinny wskazać wsparcie udzielone na szczeblu krajowym podmiotowi dotkniętemu incydentem, które należy uwzględnić przy ocenie wniosku państwa członkowskiego. Usługi z unijnej rezerwy cyberbezpieczeństwa mogą również służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii na podobnych warunkach.	Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i natychmiastowe usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę. Unijna rezerwa cyberbezpieczeństwa powinna zapewniać dostępność i gotowość usług. Usługi z unijnej rezerwy cyberbezpieczeństwa powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom jako uzupełnienie działań tych organów na szczeblu krajowym. Wnioskując o wsparcie z unijnej rezerwy cyberbezpieczeństwa, państwa członkowskie powinny wskazać wsparcie udzielone na szczeblu krajowym podmiotowi dotkniętemu incydentem, które należy uwzględnić przy ocenie wniosku państwa członkowskiego. Usługi z unijnej rezerwy cyberbezpieczeństwa mogą również służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii na podobnych warunkach.

Uzasadnienie

Wsparcie z unijnej rezerwy cyberbezpieczeństwa powinny otrzymywać dotknięte incydentami podmioty, jednak nie tylko te z sektorów krytycznych lub wysoce krytycznych.

Poprawka 6

Artykuł 1 ust. 2 lit. b)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;	zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych ***oraz administracji publicznej szczebla krajowego i niższego niż krajowy*** w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;

Uzasadnienie

Władze szczebla niższego niż krajowy powinny również wchodzić w zakres tego rozporządzenia.

Poprawka 7

Artykuł 4 ust. 1 akapit drugi

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. […]	Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym ***i niższym niż krajowy*** w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. […]

Uzasadnienie

Krajowe centra monitorowania bezpieczeństwa (SOC) powinny również gromadzić i analizować informacje od władz regionalnych i lokalnych.

Poprawka 8

Artykuł 5 ust. 2

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa konsorcjum przyjmujące. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.	W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa konsorcjum przyjmujące **z *innych środków niż środki przewidziane w rozporządzeniu (UE) 2021/1060 (rozporządzenie w sprawie wspólnych przepisów)***. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.

Uzasadnienie

Działania na podstawie aktu o cybersolidarności nie powinny być finansowane z programów polityki spójności.

Poprawka 9

Artykuł 9 ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na ***poważne*** zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm").	Ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm").

Uzasadnienie

Mechanizm cyberkryzysowy ma służyć gotowości na krótkoterminowe skutki wszystkich rodzajów cyberincydentów i te skutki łagodzić.

Poprawka 10

Artykuł 10 ust. 2 (nowy)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	2. Komisja sporządza roczne sprawozdanie, w którym ocenia funkcjonowanie mechanizmu oraz ewentualne zapotrzebowanie na dodatkowe wymogi w zakresie współpracy lub szkoleń.

Uzasadnienie

Komisja powinna składać regularne sprawozdania, ponieważ cyberbezpieczeństwo stale się zmienia i wymogi trzeba na bieżąco dostosowywać do rzeczywistości.

Poprawka 11

Artykuł 11 ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 10 ust. 1 lit. a), Komisja, po konsultacji z grupą współpracy NIS i ENISA, określa odnośne sektory lub podsektory spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, z których podmioty mogą podlegać skoordynowanemu testowaniu gotowości, z uwzględnieniem istniejących i planowanych skoordynowanych ocen ryzyka i testów odporności na szczeblu Unii	Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 10 ust. 1 lit. a), Komisja, po konsultacji z grupą współpracy NIS i ENISA, określa odnośne sektory lub podsektory spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, ***w tym organy administracji publicznej szczebla lokalnego,*** z których podmioty mogą podlegać skoordynowanemu testowaniu gotowości, z uwzględnieniem istniejących i planowanych skoordynowanych ocen ryzyka i testów odporności na szczeblu Unii.

Uzasadnienie

Władze lokalne i regionalne powinny mieć możliwość skorzystania z mechanizmu cyberkryzysowego. Celem poprawki jest umieszczenie w treści artykułu postulatu sprawozdawcy z poprawki 3 (do motywu 30).

Poprawka 12

Artykuł 14 ust. 2 lit. b)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
rodzaj podmiotu, na który incydent ma wpływ, przy czym jako ważniejsze traktuje się incydenty mające wpływ na podmioty kluczowe zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2022/2555;	rodzaj podmiotu, ***w tym podmiotu administracji publicznej na szczeblu regionalnym i lokalnym,*** na który incydent ma wpływ, przy czym jako ważniejsze traktuje się incydenty mające wpływ na podmioty kluczowe zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2022/2555;

Uzasadnienie

Wyjaśnienie zakresu obowiązywania oraz uwzględnienie podmiotów szczebla niższego niż krajowy.

Poprawka 13

Artykuł 18 ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA dokonuje przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA przekazuje sieci CSIRT, EU-CyCLONe i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań, w szczególności w świetle zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. W stosownych przypadkach Komisja udostępnia sprawozdanie to wysokiemu przedstawicielowi.	Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA dokonuje przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA przekazuje sieci CSIRT, EU-CyCLONe i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań, w szczególności w świetle zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. ***W miarę możliwości sieć CSIRT udostępnia sprawozdanie administracjom publicznym na szczeblu niższym niż krajowy.*** W stosownych przypadkach Komisja udostępnia sprawozdanie to wysokiemu przedstawicielowi.

Uzasadnienie

Wyjaśnienie zakresu obowiązywania oraz uwzględnienie podmiotów szczebla niższego niż krajowy.

II. **ZALECENIA POLITYCZNE**

STANOWISKO EUROPEJSKIEGO KOMITETU REGIONÓW

Europejski Komitet Regionów (KR) z zadowoleniem przyjmuje wniosek Komisji dotyczący rozporządzenia w sprawie wzmocnienia europejskiej współpracy w dziedzinie cyberbezpieczeństwa. Państwa członkowskie UE są obecnie ściśle ze sobą połączone – także cyfrowo – i w nadchodzących latach trend ten będzie jeszcze silniejszy. Dlatego Komitet z zadowoleniem przyjmuje inicjatywę Komisji dotyczącą wspólnego przeciwdziałania zagrożeniom cybernetycznym, które idą w parze ze zwiększoną cyfryzacją. We wniosku zwraca się uwagę na rosnącą liczbę cyberincydentów, które mają miejsce również w obszarach, za które odpowiadają gminy i regiony. Podkreślono potrzebę przygotowania się na incydenty w krytycznych obszarach społeczeństwa, reagowania na nie i wyciągania z nich wniosków. KR uważa, że propozycje Komisji mogą przyczynić się do zwiększenia odporności cyfrowej w Unii.

1. Politycy oraz obywatelki i obywatele muszą zrozumieć, że dla osiągnięcia celu cyfrowej odporności Europy trzeba połączyć siły w dziedzinie cyberbezpieczeństwa. KR wzywa więc państwa członkowskie, Komisję i wszystkie władze lokalne, by wspólnie podnosiły świadomość na temat potrzeby podjęcia działań, w tym zwiększenia inwestycji w odporność cyfrową – zwłaszcza na szczeblu lokalnym i regionalnym. Ponadto zwraca się do nich, by rozważyły opracowanie instrumentów politycznych w celu ochrony przed atakami typu ransomware w sektorze finansowym. Wymaga to odpowiednich środków finansowych, technicznych i szkoleniowych.

2. Komitet zauważa, że pod wieloma względami wniosek odnosi się do dyrektywy NIS 2 i do niej nawiązuje. Przy transpozycji dyrektywy NIS 2 na szczeblu krajowym każde państwo członkowskie ustala, czy jego władze lokalne mają być objęte zakresem jej obowiązywania ([2]). Skoro każde państwo członkowskie z osobna może zdecydować, czy przy wdrażaniu dyrektywy NIS 2 uznaje swoje gminy za podmioty istotne lub ważne, wszelkie różnice między państwami będą miały wpływ na ich podejście do aktu o cybersolidarności w obecnej formie. Aby nie wyłączać władz lokalnych odpowiedzialnych za kluczowe zadania w niektórych państwach członkowskich z zakresu stosowania aktu o cybersolidarności, w tekście prawnym należy wyjaśnić, że organy te uznaje się za objęte jego zakresem stosowania, niezależnie od tego, czy są one objęte dyrektywą NIS 2.

3. Ponieważ cyberbezpieczeństwo jest podstawą interoperacyjności cyfrowej, wysiłki na rzecz zwiększenia interoperacyjności między regionami muszą być wspierane solidnymi środkami w zakresie cyberbezpieczeństwa. Ma to zapewnić, że cyberzagrożenia nie będą utrudniać interoperacyjności regionów w całej Europie.

4. Gminy i regiony muszą otrzymywać konkretne wsparcie ze strony struktur, które mają zostać utworzone, a nie tylko być zobowiązane do składania im sprawozdań. Dlatego Komitet apeluje o większą jasność co do sposobu wspierania regionów, w szczególności w celu zwiększenia poziomu cyberbezpieczeństwa w małych społecznościach.

Stanowisko na temat obszarów działania, o których mowa we wniosku

Europejska tarcza cyberbezpieczeństwa

Budowa ogólnoeuropejskiej infrastruktury centrów monitorowania bezpieczeństwa w celu rozwijania i poprawy wspólnych zdolności w zakresie wykrywania, analizowania i przetwarzania danych dotyczących cyberzagrożeń i cyberincydentów.

5. Aby uzyskać kompleksowy obraz obecnego stanu cyberbezpieczeństwa w UE, konieczne jest gromadzenie informacji, scenariuszy ryzyka, zagrożeń i incydentów również od lokalnych i krajowych operatorów systemów. Zdaniem KR-u problemem jest brak jasnych zachęt i procedur dotyczących tego, w jaki sposób gminy i regiony mogą aktywnie uczestniczyć we wzmacnianiu odporności cyfrowej. Zaangażowanie szczebla lokalnego i regionalnego jest niezwykle ważne, ponieważ ten poziom dysponuje rozwiązaniami cyfrowymi, które są narażone na ataki. Trzeba zatem zapewnić otoczenie, w którym gminy i regiony będą mogły – i powinny – zaangażować się jako partnerzy w wysiłki na rzecz zwiększenia cyberbezpieczeństwa w UE.

6. Na podstawie swego rozeznania Komitet stwierdza, że pomiędzy poszczególnymi krajami istnieją znaczne różnice, jeśli chodzi o zaawansowanie podejmowanych środków ochrony i bezpieczeństwa. Nawet w obrębie państw występują spore różnice, np. między organami krajowymi a mniejszymi władzami lokalnymi, zarówno pod względem zdolności, jak i celów w zakresie cyberbezpieczeństwa. Dlatego Komitet uważa, że rozporządzenie powinno przyczynić się do zmniejszenia tych różnic i zapewnić wszystkim zainteresowanym stronom w miarę zbliżone możliwości i cele.

7. Zwraca przy tym uwagę na ryzyko pokrywania się zadań nowej sieci krajowych i transgranicznych centrów monitorowania bezpieczeństwa (SOC) z zadaniami sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) ([3]). W przypadku gdy obok CSIRT tworzone są krajowe SOC, trzeba jasno określić zasady ich współpracy i obowiązków każdego z nich w przypadku incydentu.

([2]) Artykuł 2 ust. 5 dyrektywy NIS 2: „Państwa członkowskie mogą postanowić, że niniejsza dyrektywa ma zastosowanie do: (a) podmiotów administracji publicznej na poziomie lokalnym;".

([3]) Zgodnie z art. 11 ust. 3 dyrektywy NIS 2 CSIRT mają następujące zadania:
a) monitorowanie i analizowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym oraz, na wniosek, udzielanie pomocy danym podmiotom kluczowym i ważnym w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego;
b) wczesne ostrzeganie i alarmowanie danych podmiotów kluczowych i ważnych oraz właściwych organów i innych zainteresowanych stron o cyberzagrożeniach, podatnościach i incydentach, a także kierowanie do nich ogłoszeń oraz przekazywanie im informacji dotyczących cyberzagrożeń, podatności i incydentów, w miarę możliwości w czasie zbliżonym do rzeczywistego;
c) reagowanie na incydenty i w stosownych przypadkach udzielanie pomocy danym podmiotom kluczowym i ważnym;
d) gromadzenie i analizowanie danych kryminalistycznych i zapewnianie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej w zakresie cyberbezpieczeństwa;
e) przeprowadzanie, na wniosek podmiotu kluczowego lub ważnego, aktywnego skanowania sieci i systemów informatycznych danego podmiotu w celu wykrycia podatności o potencjalnym znaczącym wpływie;
f) uczestnictwo w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci CSIRT na ich wniosek, w miarę własnych zdolności i kompetencji;
g) w stosownych przypadkach działanie w charakterze koordynatora w celu skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1;
h) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z art. 10 ust. 3.

8. Komitet przyjmuje z zadowoleniem konkretne cele wniosku dotyczącego rozporządzenia i proponowane w nim środki. Jednocześnie ubolewa, że pomimo coraz częstszych cyberataków władze lokalne i regionalne nie zostały we wniosku wystarczająco uwzględnione, i proponuje szereg zmian legislacyjnych, aby zaradzić tym niedociągnięciom.

9. Obecnie brakuje danych i jasnych pomiarów dotyczących incydentów, zagrożeń i ryzyka dla gmin i regionów. W ramach europejskiej tarczy cyberbezpieczeństwa należy więc opracować wskaźniki, które pozwolą ocenić, na ile wdrażanie rozporządzenia przyczynia się do przyspieszenia rozwoju i stopnia zaawansowania. Na dłuższą metę takie wskaźniki mogą przyczynić się do opracowania opartej na danych mapy ryzyka i wskazać obszary, w których podjęcie działań jest najbardziej potrzebne.

Mechanizm cyberkryzysowy

Jego celem jest zwiększenie gotowości, testowanie gotowości w sektorach uznanych za krytyczne, wzmocnienie zdolności w zakresie przywracania normalnego działania po incydentach oraz ustanowienie unijnej rezerwy cyberbezpieczeństwa.

10. Incydenty w cyberbezpieczeństwie na dużą skalę mogą być spowodowane wydarzeniami lokalnymi. Dlatego we wniosku należy wskazać, jak SOC i rezerwa cyberbezpieczeństwa mają wychwytywać także poważne lokalne zakłócenia, a nie tylko poważne i już zaistniałe incydenty na dużą skalę. Wymiana informacji nie powinna ograniczać się do incydentów na dużą skalę, lecz powinna również obejmować potencjalne zagrożenia.

11. Informacje związane z cyberincydentami są często wysoce wrażliwe i mogą zawierać szczegóły techniczne lub nawet dane osobowe, które nie mogą jeszcze być udostępniane bez umów i porozumień między stronami. Wymiana informacji na szczeblu krajowym przebiega obecnie mozolnie. Tym bardziej złożona jest kwestia wymiany informacji na poziomie transgranicznym. Aby mechanizm cyberkryzysowy mógł funkcjonować, Komisja musi zapewnić wszystkim zainteresowanym stronom – podmiotom publicznym i prywatnym objętym unijną rezerwą cyberbezpieczeństwa – warunki prawne i techniczne umożliwiające wymianę i otrzymywanie informacji. Zdaniem Komitetu rozpowszechnianie informacji dotyczy przede wszystkim usuwania skutków incydentów, czyli tego, jak zaatakowane podmioty mogą najlepiej radzić sobie z poważnym incydentem.

12. Komitet Regionów z zadowoleniem przyjmuje wysoki poziom wymogów nałożonych na tych dostawców usług z sektora prywatnego, którzy będą uczestniczyć w proponowanej rezerwie cyberbezpieczeństwa. Opracowanie tych wymogów nie może jednak prowadzić do wykluczenia pewnych umiejętności lub wiedzy systemowej, ponieważ tylko nieliczne, bardzo duże podmioty mogłyby spełnić wymogi nałożone na dostawców usług w zakresie bezpieczeństwa. Działania UE w zakresie bezpieczeństwa muszą mieć szeroki zasięg, aby zapewnić jak największą odporność.

13. Wniosek przewiduje, że rezerwa cyberbezpieczeństwa będzie polegała na usługach świadczonych przez zaufanych dostawców, którzy byliby certyfikowani zgodnie z aktem o cyberbezpieczeństwie ([4]). Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) byłaby odpowiedzialna za zapewnienie, że oferowane produkty i usługi odpowiadałyby określonym wymogom cyberbezpieczeństwa. Komitet Regionów podkreśla, że ENISA powinna jak najszybciej opracować systemy certyfikacji, aby za pomocą nowoczesnych technologii umożliwić dostawcom zdobycie certyfikatów ([5]).

14. Przy tworzeniu rezerwy cyberbezpieczeństwa należy też dopilnować, by nie utrudniała ona konkurencji lub nie wykluczała podmiotów działających tylko w niektórych częściach UE. Ustanowienie rezerwy cyberbezpieczeństwa i certyfikacji wymaga szybkich i przejrzystych procedur mających na celu identyfikację najbardziej kompetentnych i kluczowych podmiotów w tej dziedzinie.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

([5]) W ENISA trwają obecnie prace (jeszcze nieukończone) nad trzema certyfikatami. Dotyczą one, odpowiednio: technologii informacyjno-komunikacyjnych, 5G i usług w chmurze. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq.

15. KR uważa, że należy zidentyfikować krajowych dostawców technologii i usług dla systemów krytycznych, a następnie rejestrować te informacje w odpowiedniej bazie danych. Takie dane mogą być bardzo cenne w sytuacji, gdy trzeba podjąć działania z udziałem podmiotów lokalnych. Można je również wykorzystać w pracach Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa.

16. W przypadku wystąpienia incydentu skuteczność środków zaradczych zależy od szybkości reakcji. Dlatego złożone informacje na temat incydentów i zagrożeń muszą niezwłocznie dotrzeć do odpowiednich grup docelowych. Wniosek zakłada utworzenie nowej organizacji i struktury, które mają odpowiadać właśnie za wymianę informacji. KR podkreśla jednak, że przy tworzeniu krajowych i transgranicznych SOC trzeba wykorzystywać i rozwijać istniejące kanały informacyjne, np. CyCLONe ([6]) i CSIRT.

Mechanizm przeglądu incydentów w cyberbezpieczeństwie

Mechanizm ma za zadanie przeprowadzanie przeglądu incydentów w cyberbezpieczeństwie, w szczególności incydentów o znacznych skutkach.

17. Zapotrzebowanie na umiejętności w zakresie cyberbezpieczeństwa i na ich finansowanie idzie w parze z szybkim rozwojem cyfryzacji. KR z zadowoleniem przyjmuje utworzenie przez Komisję Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa i wzywa do opracowania jasnej strategii, by ułatwić mniejszym i mniej zamożnym gminom i regionom zaradzenie niedoborowi wykwalifikowanej siły roboczej w UE.

18. Stwierdza, że osiągnięcie silnej odporności cyfrowej wymaga współpracy różnych podmiotów i udziału podmiotów publicznych i prywatnych dysponujących wiedzą fachową, doświadczeniem i kadrami. Podkreśla rolę władz lokalnych i regionalnych w budowaniu odporności cyfrowej, ponieważ mogą one wzajemnie się wspierać poprzez kampanie informacyjne, wymianę najlepszych praktyk i specjalistycznej wiedzy. Zauważa, że im więcej przedsiębiorstw inwestuje w swoją odporność cyfrową, tym wyższe są koszty ataków dla sprawców. To również może służyć jako działanie odstraszające.

19. Obecnie to europejskie gminy i regiony ponoszą koszty utrzymania wysokiego poziomu cyberbezpieczeństwa, a także koszty wynikające ze skutków tych incydentów. KR ostrzega, że rozporządzenie może wywierać dodatkową presję na i tak już ograniczone zasoby. Nie może ono zatem generować obciążeń, lecz powinno przyczyniać się do wzmocnienia zdolności wszystkich podmiotów za pomocą konkretnych narzędzi, procedur i wsparcia.

20. Komitet Regionów rozważa, czy w ramach sieci krajowych i transgranicznych SOC nie można by dzielić się sprawozdaniami z przeglądów. Wniosek przyznaje krajowym SOC jedynie prawo dostępu do informacji publicznych. Tymczasem niezwykle ważne jest uczenie się na dotychczasowych incydentach, aby można było stale poprawiać i rozwijać cyberbezpieczeństwo. Dlatego wszystkie uczestniczki i wszyscy uczestnicy sieci powinni mieć dostęp do wszystkich szczegółowych informacji.

21. We wniosku zbyt ogólnie potraktowano finansowanie. KR pragnąłby bardziej precyzyjnego określenia, w jaki sposób środki będą wykorzystywane i jaka ich część będzie bezpośrednio przydzielana regionom i gminom.

([6]) Art. 16 ust. 1 i 3 dyrektywy NIS 2.
Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe)
1. Ustanawia się EU CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii.
3. EU-CyCLONe ma następujące zadania:
   a) podnoszenie poziomu gotowości do zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;
   b) rozwijanie wspólnej świadomości sytuacyjnej pod kątem incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę;
   c) ocenę konsekwencji i wpływu istotnych incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę oraz proponowanie możliwych środków ograniczających ryzyko;
   d) koordynowanie zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do takich incydentów i sytuacji kryzysowych;
   e) na wniosek zainteresowanego państwa członkowskiego – omawianie krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, o których mowa w art. 9 ust. 4.

22. Komitet podkreśla na koniec, że wniosek jest zgodny z zasadami pomocniczości i proporcjonalności.

Bruksela, dnia 30 listopada 2023 r.

Vasco ALVES CORDEIRO

Przewodniczący
Europejskiego Komitetu Regionów