Rada
Unii Europejskiej

Bruksela, 31 października 2022 r.
(OR. en)

14128/22

Międzyinstytucjonalny numer referencyjny:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTA DO PUNKTU I/A

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli (część II)/Rada
Nr poprz. dok.:	10097/5/22 REV 5
Nr dok. Kom.:	7474/22 + ADD 1
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii – Podejście ogólne

WPROWADZENIE

1. W dniu 22 marca 2022 r. Komisja przyjęła wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii Wniosek był jednym ze środków przewidzianych w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[1], która ma na celu wzmocnienie zbiorowej odporności Unii na cyberzagrożenia.

   W konkluzjach z dnia 22 marca 2021 r. w sprawie tej strategii[2] Rada podkreśliła, że cyberbezpieczeństwo odgrywa podstawową rolę w funkcjonowaniu administracji publicznej

[1] Dok. 14133/20.
[2] Dok. 6722/21.

i instytucji publicznych zarówno na poziomie krajowym, jak i UE oraz, ogólnie, naszego społeczeństwa i naszej gospodarki.

2. Wniosek Komisji, oparty na art. 298 Traktatu o funkcjonowaniu Unii Europejskiej, ma na celu poprawę poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii poprzez ustanowienie wspólnych ram, z należytym uwzględnieniem autonomii każdego podmiotu Unii. W szczególności cele wniosku są następujące:

   – wzmocnienie mandatu i finansowania CERT-UE (autonomicznego międzyinstytucjonalnego zespołu reagowania na incydenty komputerowe w podmiotach Unii);

   – utworzenie międzyinstytucjonalnej struktury (Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa – IICB) skupiającej przedstawicieli wszystkich podmiotów Unii w celu zapewnienia właściwego wdrożenia rozporządzenia;

   – nałożenie na podmioty Unii obowiązku udostępniania CERT-UE (jawnych) informacji dotyczących incydentów oraz zgłaszania istotnych zagrożeń, podatności i incydentów; oraz

   – propagowanie koordynacji i współpracy w reakcji na znaczące incydenty.

3. W Parlamencie Europejskim na sprawozdawczynię została wyznaczona Henna Virkkunen (PPE) z przedmiotowo właściwej komisji ITRE. Projekt sprawozdania został opublikowany w dniu 7 października 2022 r.

4. W dniu 17 maja 2022 r. opinię wydał Europejski Inspektor Ochrony Danych[3].

[3] Dok. 9252/22.

5. W Radzie analiza wniosku na forum Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni (HWPCI) rozpoczęła się podczas prezydencji francuskiej w dniu 29 marca 2022 r. Prezydencja francuska przygotowała pierwszy tekst kompromisowy, który omówiono na forum HWPCI w czerwcu 2022 r., i przedłożyła Radzie sprawozdanie z postępu prac[4] w dniu 21 czerwca 2022 r.

6. Podczas prezydencji czeskiej HWPCI poświęciła osiem posiedzeń[5] dyskusjom na temat wniosku i kilku kolejnych tekstów kompromisowych.

7. W dniu 23 maja 2022 r. prezydencja zwróciła się do Komitetu ds. Bezpieczeństwa Rady o opinię na temat aspektów wniosku związanych z bezpieczeństwem informacji, a w szczególności z informacjami niejawnymi. Komitet wydał swoją opinię 19 września 2022 r.[6] Zgodnie z sugestią Komitetu informacje niejawne UE zostały wyraźnie wyłączone z zakresu stosowania rozporządzenia. Przepisy dotyczące zwolnień z obowiązków w zakresie udostępniania i zgłaszania w odniesieniu do informacji otrzymanych od podmiotów niebędących podmiotami Unii zostały odpowiednio zmienione.

8. W dniu 28 października 2022 r. HWPCI osiągnęła porozumienie w sprawie kompromisowego tekstu prezydencji w brzmieniu zawartym w załączniku.

---

4 Dok. 9719/22.
5 6 i 20 lipca, 13, 21 i 28 września oraz 5, 19 i 28 października 2022 r.
6 Dok. 12603/22 + COR 1.

GŁÓWNE KWESTIE

9. Państwa członkowskie z zadowoleniem przyjęły wniosek jako przedstawiony na czas i uzupełniający przyszłą dyrektywę w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii („dyrektywa NIS 2") i poparły jego ogólne cele. Państwa członkowskie wezwały jednak do dalszego dostosowania do dyrektywy NIS 2, większej wzajemności w wymianie informacji między podmiotami Unii a państwami członkowskimi oraz zwróciły uwagę na zbyt dobrowolny charakter niektórych proponowanych środków. Państwa członkowskie opowiedziały się również za skreśleniem odniesień do wspólnej jednostki ds. cyberprzestrzeni (której mandat i skład nie zostały jeszcze określone).

10. Na podstawie dyskusji na szczeblu Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni za główne kwestie polityczne uznano następujące zagadnienia:

a) Dostosowanie do przyszłej dyrektywy NIS 2

Zgodnie z wnioskiem państw członkowskich dokonano dalszego uzgodnienia z przyszłą dyrektywą NIS 2, m.in.:

- szereg definicji (art. 3) dostosowano do definicji zawartych w NIS 2;
- dodano nowy art. 7a dotyczący dobrowolnych wzajemnych ocen, zgodnie z NIS 2, dostosowany do potrzeb podmiotów Unii;
- obowiązki w zakresie zgłaszania określone w art. 20 zostały dostosowane do obowiązków w ramach NIS 2.

b) Skład Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa (IICB) (art. 9)

W wyniku dyskusji na temat odpowiedniego zaangażowania przedstawicieli państw członkowskich w prace IICB osiągnięto kompromis w formie oświadczenia Rady do protokołu.

c) Autonomia instytucjonalna

Znaleziono wyważone podejście między wolą państw członkowskich w zakresie wzmocnienia mechanizmów zapewniania zgodności a potrzebą poszanowania zasady autonomii instytucjonalnej, w szczególności w odniesieniu do audytów i środków dyscyplinarnych (art. 11).

Ponadto w motywie 8 usunięto odniesienie do przeznaczenia na cyberbezpieczeństwo określonego odsetka budżetu przewidzianego na technologie informatyczne.

PODSUMOWANIE

11. Komitet Stałych Przedstawicieli jest proszony o:

(a) zatwierdzenie tekstu kompromisowego w wersji zamieszczonej w załączniku, która następnie będzie stanowiła mandat do negocjacji z Parlamentem Europejskim;

(b) zwrócenie się do Rady, by na posiedzeniu 18 listopada 2022 r. zatwierdziła tekst kompromisowy w wersji zamieszczonej w załączniku i by dołączyła do protokołu oświadczenie Rady zamieszczone w addendum do niniejszego dokumentu.

ZAŁĄCZNIK

2022/0085 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 298,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej, w szczególności jego art. 106a,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W epoce cyfrowej technologie informacyjno-komunikacyjne stanowią podstawę otwartej, efektywnej i niezależnej administracji unijnej. Rozwój technologii, ich coraz większa złożoność i wzajemne powiązania systemów cyfrowych zwiększają ryzyko w cyberprzestrzeni, co sprawia, że administracja unijna jest bardziej podatna na cyberzagrożenia i incydenty, a to z kolei stanowi zagrożenie dla ciągłości działania administracji i jej zdolności do zabezpieczenia swoich danych. Mimo że coraz częstsze korzystanie z usług w chmurze, wszechobecne wykorzystanie technologii informacyjnych, wysoki poziom cyfryzacji, praca zdalna i rozwój technologii oraz możliwości połączenia z siecią stanowią obecnie trzon wszystkich działań podmiotów administracji Unii, to ich odporność cyfrowa nie rozwinęła się jeszcze w wystarczającym stopniu.

(2) Krajobraz cyberzagrożeń, z jakimi mierzą się **podmioty** [...] Unii, podlega ciągłym zmianom. Stosowane przez agresorów taktyki, techniki i sposoby działania ciągle ewoluują, natomiast główne motywy takich ataków zmieniają się w niewielkim stopniu – ich celem jest kradzież cennych, nieujawnionych informacji, osiągnięcie korzyści finansowych, manipulowanie opinią publiczną czy też osłabienie infrastruktury cyfrowej. Tempo przeprowadzania przez nich cyberataków stale rośnie, podczas gdy ich działania są coraz bardziej wyrafinowane i w coraz większym stopniu zautomatyzowane, ukierunkowane na eksponowane powierzchnie ataków, które stale powiększają się, i mają na celu szybkie wykorzystanie podatności na zagrożenia.

(3) Środowiska informatyczne **podmiotów** [...] Unii są współzależne, występują w nich zintegrowane przepływy danych, a ich użytkownicy ściśle ze sobą współpracują. Te powiązania oznaczają, że wszelkie zakłócenia, nawet początkowo ograniczone do jednego **podmiotu** [...] Unii, mogą mieć szerszy efekt kaskadowy, potencjalnie powodując dalekosiężne i długotrwałe negatywne skutki dla pozostałych podmiotów. Ponadto środowiska informatyczne niektórych [...] **podmiotów Unii** są połączone ze środowiskami informatycznymi państw członkowskich, co powoduje, że incydent w jednym podmiocie unijnym może stanowić zagrożenie dla cyberbezpieczeństwa środowisk informatycznych państw członkowskich i odwrotnie. **Ponadto podmioty Unii przetwarzają często duże ilości informacji szczególnie chronionych z państw członkowskich, a zatem incydenty mogą mieć negatywny skutek również dla państw członkowskich. Z tego powodu cyberbezpieczeństwo podmiotów Unii ma duże znaczenie także dla państw członkowskich. Informacje dotyczące konkretnych incydentów mogą również ułatwiać wykrywanie podobnych cyberzagrożeń lub incydentów uderzających w państwa członkowskie.**

(4) **Podmioty** [...] Unii stanowią atrakcyjne cele i muszą stawiać czoła dysponującym wysokimi umiejętnościami i znaczącymi zasobami agresorom, a także innym zagrożeniom. Jednocześnie poziom i dojrzałość w zakresie cyberodporności oraz zdolność do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie znacznie się w tych podmiotach różnią. Dla funkcjonowania administracji unijnej konieczne jest zatem, aby **podmioty** [...] Unii osiągnęły wysoki wspólny poziom cyberbezpieczeństwa dzięki **wdrażaniu środków w zakresie cyberbezpieczeństwa**, [...] wymianie informacji i współpracy.

(5) Dyrektywa [wniosek dotyczący dyrektywy NIS 2] w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii ma na celu dalszą poprawę odporności podmiotów publicznych i prywatnych, właściwych organów i instytucji krajowych, jak również całej Unii pod względem cyberbezpieczeństwa oraz dalsze zwiększenie ich zdolności reagowania na incydenty w zakresie cyberbezpieczeństwa. Konieczne jest zatem, by podobnymi środkami objęto [...] **podmioty** Unii, poprzez ustanowienie przepisów, które są zgodne z dyrektywą [wniosek dotyczący dyrektywy NIS 2] i odzwierciedlają przewidziany w niej poziom ambicji.

(6) Aby osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, każdy [...] **podmiot** Unii musi ustanowić wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli, które to ramy umożliwią skuteczne i ostrożne zarządzanie wszelkiego rodzaju ryzykiem w cyberprzestrzeni [...]. **Ramy te powinny określać polityki cyberbezpieczeństwa, w tym procedury oceny skuteczności wdrożonych środków w zakresie cyberbezpieczeństwa. Ramy te powinny być oparte na podejściu uwzględniającym wszystkie zagrożenia, które ma na celu ochronę sieci i systemów informatycznych oraz fizycznego środowiska tych systemów przed takimi zdarzeniami jak kradzież, pożar, zalanie, awaria łączności lub zasilania, lub też nieupoważniony dostęp fizyczny do tych systemów i ich uszkodzenie, a także ingerencja w należące do podmiotu Unii informacje i infrastrukturę przetwarzania informacji, które to zdarzenia mogłyby zagrozić dostępności, autentyczności, integralności lub poufności danych przechowywanych, przesyłanych, przetwarzanych lub dostępnych za pośrednictwem sieci i systemów informatycznych. Ramy powinny odzwierciedlać ustalenia analizy ryzyka, z uwzględnieniem wszystkich istotnych zagrożeń technicznych, operacyjnych i organizacyjnych, na które jest narażony dany podmiot Unii.**

(6a) Do celów zarządzania ryzykiem stwierdzonym dzięki tym ramom, każdy podmiot Unii powinien zapewniać, by zostały podjęte odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne. Powinny one dotyczyć poszczególnych dziedzin, w tym środków w zakresie cyberbezpieczeństwa określonych w niniejszym rozporządzeniu, aby wzmacniać cyberbezpieczeństwo każdego podmiotu Unii.

(6b) **Zidentyfikowane w tych ramach zasoby i ryzyko, a także wnioski wyciągnięte z regularnych ocen dojrzałości powinny zostać odzwierciedlone w planie dotyczącym cyberbezpieczeństwa ustalonym dla każdego podmiotu Unii. Plan dotyczący cyberbezpieczeństwa powinien obejmować środki w zakresie cyberbezpieczeństwa przyjęte w celu zwiększenia ogólnego cyberbezpieczeństwa danego podmiotu Unii.**

(6c) **Z racji tego, że zapewnianie cyberbezpieczeństwa jest procesem ciągłym, adekwatność i skuteczność wszystkich środków powinna być regularnie oceniana w świetle zmieniających się zagrożeń, aktywów i dojrzałości podmiotów Unii. Ramy powinny być poddawane regularnemu przeglądowi, przynajmniej co trzy lata, natomiast plan dotyczący cyberbezpieczeństwa powinien być poddawany przeglądowi przynajmniej co dwa lata lub po każdej ocenie dojrzałości lub po każdym przeglądzie ram.**

(6d) **Podmioty Unii powinny regularnie wymieniać istotne informacje, w tym dotyczące odpowiednich incydentów i cyberzagrożeń, zapewniając jednocześnie poufność i odpowiednią ochronę informacji dostarczanych przez dokonujący zgłoszenia podmiot Unii.**

(6e) **Należy wdrożyć mechanizm zapewniający skuteczną wymianę informacji, koordynację i współpracę podmiotów Unii w przypadku poważnych incydentów, obejmujący wyraźną identyfikację ról i odpowiedzialności zaangażowanych podmiotów Unii. Informacje objęte wymianą powinny być uwzględniane przez wyznaczony punkt kontaktowy dla EU-CyCLONe, przy dzieleniu się odpowiednimi informacjami z EU-CyCLONe w ramach wkładu we wspólną orientację sytuacyjną.**

(7) Zróżnicowanie [...] **podmiotów** Unii sprawia, że wymagana jest elastyczność w procesie wdrożenia, ponieważ w omawianym obszarze nie można zastosować uniwersalnego rozwiązania. Środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa nie powinny obejmować żadnych obowiązków bezpośrednio kolidujących z wykonywaniem przez [...] **podmioty** Unii ich misji lub naruszających ich autonomię instytucjonalną. **Podmioty Unii** [...] powinny zatem ustanowić własne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli, a także własne **plany dotyczące cyberbezpieczeństwa**, oraz przyjmować [...] **środki** w zakresie [...] cyberbezpieczeństwa. **Przy wdrażaniu takich środków należy odpowiednio uwzględnić synergie istniejące między podmiotami Unii, mając na celu odpowiednie zarządzanie zasobami oraz optymalizację kosztów. Należy również zwrócić szczególną uwagę, by środki te nie oddziaływały negatywnie na sprawność wymiany informacji oraz operacje prowadzone przez podmioty Unii z innymi podmiotami Unii i właściwymi organami krajowymi.**

(8) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na [...] **podmioty** Unii, wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni powinny być proporcjonalne do ryzyka związanego z daną siecią oraz danym systemem informatycznym, przy uwzględnieniu stanu techniki w kontekście takich środków. Wszystkie [...] **podmioty** Unii powinny dążyć do przeznaczenia odpowiedniego odsetka swojego budżetu przewidzianego na technologie informatyczne na poprawę swojego poziomu cyberbezpieczeństwa [...]. W **ocenie dojrzałości należy również przeanalizować, czy wydatki danego podmiotu Unii na cyberbezpieczeństwo są proporcjonalne do ryzyka, z jakim ten podmiot się mierzy.**

(9) W celu osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa konieczne jest, by cyberbezpieczeństwo było objęte nadzorem kierownictwa najwyższego szczebla każdego **podmiotu** [...] Unii. [...] **Kierownictwo najwyższego szczebla powinno nadzorować wdrażanie niniejszego rozporządzenia, w tym ustanowienie ram zarządzania ryzykiem, jego nadzorowania i kontroli oraz planów dotyczących cyberbezpieczeństwa obejmujących środki w zakresie cyberbezpieczeństwa.** Uwzględnienie kultury cyberbezpieczeństwa, tj. codziennej praktyki w dziedzinie cyberbezpieczeństwa, jest nieodłączną częścią **ram** dotyczących cyberbezpieczeństwa w każdym[...] **podmiocie** Unii [...].

(10) [...] [...] Środki w zakresie **cyberbezpieczeństwa** powinny stanowić część [...] **planu** dotyczącego cyberbezpieczeństwa i być szczegółowo określane w wytycznych lub zaleceniach wydawanych przez CERT-UE. Przy określaniu środków i wytycznych należy należycie uwzględniać **stan techniki oraz, w stosownych przypadkach, odpowiednie normy europejskie i międzynarodowe, a także** odpowiednie przepisy i polityki UE, w tym oceny ryzyka i zalecenia wydane przez grupę współpracy ds. bezpieczeństwa sieci i informacji, takie jak unijna skoordynowana ocena ryzyka i unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Ponadto można wprowadzić wymóg certyfikacji odpowiednich produktów, usług i procesów ICT zgodnie ze specjalnymi unijnymi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia (UE) 2019/881. W **stosownych przypadkach CERT-UE powinien współpracować z ENISA.**

(11) W maju 2011 r. sekretarze generalni instytucji i organów Unii postanowili utworzyć zespół ds. wstępnej konfiguracji zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-UE), pod nadzorem międzyinstytucjonalnej rady sterującej. W lipcu 2012 r. sekretarze generalni potwierdzili ustalenia praktyczne i zgodzili się co do utrzymania CERT-UE jako stałego podmiotu, tak aby dalej wspomagać poprawę ogólnego poziomu bezpieczeństwa technologii informacyjnej w instytucjach, organach i agencjach Unii jako przykład dostrzegalnej współpracy międzyinstytucjonalnej w dziedzinie cyberbezpieczeństwa. We wrześniu 2012 r. powołano CERT-UE jako grupę zadaniową Komisji Europejskiej z mandatem międzyinstytucjonalnym. W grudniu 2017 r. instytucje i organy Unii zawarły porozumienie międzyinstytucjonalne w sprawie organizacji i funkcjonowania CERT-UE[7]. [...] Niniejsze **rozporządzenie** powinno [...] **zapewniać kompleksowy zestaw przepisów dotyczących organizacji, funkcjonowania i działania CERT-UE. Przepisy niniejszego rozporządzenia mają pierwszeństwo przed postanowieniami porozumienia międzyinstytucjonalnego w sprawie organizacji i funkcjonowania CERT-UE, które zostało zawarte w grudniu 2017 r.**

[...]

[7] Dz.U. C 12 z 13.1.2018, s. 1–11.

(13) Wiele cyberataków jest częścią szerszych kampanii, których celem są grupy [...] **podmiotów** Unii lub wspólnoty interesów, do których należą [...] **podmioty** Unii. Aby umożliwić aktywne wykrywanie incydentów, reagowanie na nie lub wprowadzanie środków ograniczających ryzyko,[...] **podmioty** Unii powinny powiadamiać CERT-UE o [...] cyberzagrożeniach, [...] podatnościach, **zdarzeniach potencjalnie wypadkowych oraz** [...] o incydentach oraz przekazywać odpowiednie szczegółowe informacje techniczne, które umożliwiają wykrywanie lub ograniczenie ryzyka wystąpienia podobnych cyberzagrożeń, **podatności, zdarzeń potencjalnie wypadkowych i** incydentów w innych [...] **podmiotach** Unii, a także reagowanie na nie. Kierując się podejściem przewidzianym w dyrektywie [wniosek dotyczący dyrektywy NIS 2], należy zobowiązać podmioty **Unii**, które powzięły wiedzę o znaczącym incydencie, do przekazania w ciągu 24 godzin [...] **wczesnego ostrzeżenia** do CERT-UE. Taka wymiana informacji powinna umożliwić CERT-UE rozpowszechnienie tej informacji wśród innych [...] **podmiotów** Unii, jak również wśród ich właściwych odpowiedników, aby pomóc w ochronie środowisk informatycznych Unii i jej partnerów przed podobnymi incydentami [...].

(13a) W niniejszym rozporządzeniu ustanawia się wieloetapowe podejście do zgłaszania znaczących incydentów w celu zapewnienia odpowiedniej równowagi między – z jednej strony – szybkim zgłaszaniem pomagającym zahamować potencjalne rozprzestrzenianie się znaczących incydentów i umożliwiającym podmiotom Unii zwracanie się o wsparcie, a – z drugiej strony – szczegółowym zgłaszaniem umożliwiającym wyciąganie cennych wniosków z poszczególnych incydentów a z czasem przyczyniającym się do zwiększenia cyberodporności podmiotów Unii. W tym względzie niniejsze rozporządzenie powinno obejmować zgłaszanie incydentów, które – na podstawie wstępnej oceny przeprowadzonej przez dany podmiot Unii – mogłyby spowodować poważne zakłócenia operacyjne dla funkcjonowania podmiotu Unii lub straty finansowe dla tego podmiotu Unii lub też wpłynąć na inne osoby fizyczne lub prawne poprzez spowodowanie znacznych szkód materialnych lub niematerialnych. Taka wstępna ocena powinna uwzględniać między innymi sieci i systemy informatyczne, które zostały dotknięte incydentem, w szczególności ich znaczenie dla funkcjonowania danego podmiotu Unii, dotkliwość i właściwości techniczne danego cyberzagrożenia oraz wszelkie wykorzystane podatności, a także doświadczenie danego podmiotu Unii w zakresie podobnych incydentów. Wskaźniki, takie jak zakres, w jakim zakłócone jest funkcjonowanie podmiotu Unii, czas trwania incydentu lub liczba dotkniętych danym incydentem osób fizycznych lub prawnych, mogą odegrać ważną rolę w ustaleniu, czy zakłócenie operacyjne jest poważne.

(13b) Ponieważ infrastruktura i sieci odpowiedniego podmiotu Unii i państwa członkowskiego, w którym znajduje się ten podmiot, są powiązane, kluczowe znaczenie ma, by to państwo członkowskie zostało bez zbędnej zwłoki poinformowane o wystąpieniu znaczącego incydentu w tym podmiocie Unii. W tym celu dotknięty incydentem podmiot Unii powinien powiadomić krajowy odpowiednik CERT-UE, wyznaczony przez państwo członkowskie zgodnie z dyrektywą [wniosek NIS 2], w tym samym terminie, w jakim powinien zgłosić CERT-UE znaczący incydent. CERT-UE powinien również powiadomić tego krajowego odpowiednika, kiedy otrzyma informację o znaczącym incydencie w państwie członkowskim, chyba że został on już zgłoszony przez dotknięty incydentem podmiot Unii.

(14) Oprócz powierzenia CERT-UE większej liczby zadań i rozszerzonej roli należy ustanowić Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB), która – w **celu ułatwienia osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa między podmiotami Unii** – powinna **posiadać wyłączny mandat do** [...] monitorowania wdrażania niniejszego rozporządzenia przez [...[...] **podmioty** Unii oraz [...] **do** sprawowania nadzoru nad realizacją ogólnych priorytetów i celów przez CERT-UE i zapewnianiu CERT-UE strategicznego kierunku działania. IICB powinna **zatem** zapewnić, aby instytucje były należycie reprezentowane, a w jej skład powinni wchodzić przedstawiciele agencji i organów za pośrednictwem sieci agencji Unii Europejskiej. **Organizacja i funkcjonowanie IICB powinny być dodatkowo uregulowane w jej regulaminie wewnętrznym, który może obejmować dalsze doprecyzowanie dotyczące regularnych posiedzeń IICB, w tym corocznych zgromadzeń na szczeblu politycznym, podczas których dzięki obecności przedstawicieli kierownictwa najwyższego szczebla każdego z członków IICB można prowadzić dyskusje strategiczne i formułować wytyczne strategiczne IICB. IICB może ponadto ustanowić komitet wykonawczy, który będzie wspierał ją w jej pracach, oraz przekazać mu niektóre z jej zadań i uprawnień, zwłaszcza w przypadku zadań wymagających [...] szczególnej wiedzy fachowej jej członków, na przykład zatwierdzanie katalogu usług i jego późniejszych aktualizacji, warunków umów o gwarantowanym poziomie usług, ocen dokumentów i sprawozdań przedkładanych IICB przez podmioty Unii zgodnie z niniejszym rozporządzeniem lub zadania związane z przygotowaniem wydawanych przez IICB decyzji dotyczących środków zapewniania zgodności oraz z monitorowaniem ich wdrażania. IICB ustanawia regulamin wewnętrzny komitetu wykonawczego, w tym jego zadania i uprawnienia.**

(15) CERT-UE powinien wspierać realizację działań na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa, przedstawiając IICB propozycje wytycznych i zaleceń lub wydając wezwania do działania. Wspomniane wytyczne i zalecenia powinny być zatwierdzane przez IICB. W razie potrzeby CERT-UE powinien wydawać wezwania do działania opisujące pilne środki w zakresie bezpieczeństwa, o których wprowadzenie w określonym terminie apeluje się do [...] **podmiotów** Unii. **IICB może polecić CERT-UE wydanie, wycofanie lub zmianę propozycji wytycznych lub zaleceń, lub wezwań do działania.**

(16) IICB powinna monitorować przestrzeganie niniejszego rozporządzenia, jak również działania następcze związane z wytycznymi i zaleceniami oraz wezwaniami do działania [...]. W kwestiach technicznych IICB powinny wspierać techniczne grupy doradcze działające w składzie, który IICB uzna za stosowny, i ściśle współpracujące z CERT-UE, [...] **podmiotami** Unii oraz innymi zainteresowanymi stronami, jeżeli zajdzie taka potrzeba. [...] W **przypadku gdy IICB stwierdzi, że podmioty Unii nie stosują lub nie wdrażają niniejszego rozporządzenia, w tym wytycznych, zaleceń lub wezwań do działania wydanych na podstawie niniejszego rozporządzenia, może – bez uszczerbku dla wewnętrznych procedur odpowiedniego podmiotu Unii – zastosować środki zapewniania zgodności. System środków zgodności powinien być stosowany z progresywnym stopniem dotkliwości, co oznacza, że kiedy IICB przyjmuje środki zapewniania zgodności, powinna rozpocząć od ostrzeżenia jako najmniej dotkliwego środka, a następnie, w razie konieczności, przechodzić kolejno aż do najbardziej rygorystycznego środka, jakim jest wydanie zalecenia dotyczącego tymczasowego zawieszenia przepływu danych do danego podmiotu Unii, który to środek byłby stosowany w wyjątkowych przypadkach długotrwałego, rozmyślnego lub poważnego niewypełniania przez dany podmiot obowiązków wynikających z niniejszego rozporządzenia.**

(16a) Ostrzeżenie stanowi najmniej dotkliwy środek zapewniania zgodności służący wyeliminowaniu stwierdzonych niedociągnięć podmiotu Unii i obejmuje zalecenia dotyczące zmiany, w określonych ramach czasowych, jego dokumentów dotyczących cyberbezpieczeństwa. Ostrzeżenie powinno być podane do wiadomości wszystkich podmiotów Unii, chyba że jego jawność zostanie odpowiednio ograniczona zgodnie z niniejszym rozporządzeniem.

(16b) IICB może następnie zalecić przeprowadzenie audytu podmiotu Unii. Podmiot Unii może wykorzystać do tego celu własną jednostkę audytu wewnętrznego. IICB może również zażądać, by audyt został przeprowadzony przez zewnętrzną służbę audytu, w tym wspólnie uzgodnionego dostawcę usług z sektora prywatnego.

(16c) Na podstawie wyników audytu przeprowadzonego w następstwie zalecenia IICB lub przeprowadzonego na jej żądanie, IICB może następnie zwrócić się do podmiotu Unii, by dostosował zarządzanie ryzykiem w cyberprzestrzeni, jego nadzorowanie i kontrolowanie do przepisów niniejszego rozporządzenia.

(16d) Z racji tego, że państwa członkowskie wymieniają z odpowiednimi podmiotami Unii informacje, które mogą mieć charakter wrażliwy, cyberbezpieczeństwo adresata takich informacji ma kluczowe znaczenie dla państw członkowskich. W związku z tym w wyjątkowych przypadkach długoterminowego, rozmyślnego, uporczywego lub poważnego niewypełniania odnośnego obowiązku przez podmiot Unii, IICB może jako ostateczny środek wydać zalecenie dla wszystkich państw członkowskich i podmiotów Unii dotyczące tymczasowego zawieszenia przepływów danych do tego podmiotu Unii, które powinno obowiązywać do czasu poprawy stanu cyberbezpieczeństwa tego podmiotu. Zalecenie to powinno zostać przekazane wszystkim państwom członkowskim i podmiotom Unii za pośrednictwem odpowiednich bezpiecznych kanałów komunikacji.

(16e) **Aby zapewnić prawidłowe wdrażanie niniejszego rozporządzenia, IICB – jeżeli uzna, że naruszanie niniejszego rozporządzenia przez podmiot Unii ma charakter trwały i jest spowodowane bezpośrednio działaniem lub zaniechaniem jednego z członków personelu tego podmiotu, w tym przez kierownictwo najwyższego szczebla – może zwrócić się do danego podmiotu Unii, aby podjął odpowiednie działania wobec tego członka personelu zgodnie z regulaminem pracowniczym, a także innymi równoważnymi przepisami mającymi zastosowanie w określonych podmiotach Unii. Działania te mogą obejmować na przykład postępowanie dyscyplinarne oraz, w stosownych przypadkach, w konkretnym przypadku agencji Unii, wniosek do właściwego organu o podjęcie niezbędnych kroków dotyczących ewentualnego usunięcia ze stanowiska osoby, która może być odpowiedzialna za trwałe naruszanie przepisów niniejszego rozporządzenia.**

(17) CERT-UE należy powierzyć misję przyczyniania się do bezpieczeństwa środowiska informatycznego wszystkich [...] **podmiotów** Unii. **Rozważając, czy na wniosek podmiotu Unii zapewnić doradztwo techniczne lub wkład w odpowiednie kwestie dotyczące polityki, CERT-UE powinien zapewniać, by nie utrudniało to realizacji innych jego zadań ustanowionych w niniejszym rozporządzeniu.**

(17a) CERT-UE powinien działać w charakterze odpowiednika wyznaczonego koordynatora dla [...] **podmiotów** Unii, którego zadaniem jest koordynacja ujawniania podatności do celów europejskiego rejestru podatności, o którym mowa w art. 6 dyrektywy [wniosek NIS 2] **oraz powinien opracować politykę w zakresie zarządzania podatnościami, obejmującą propagowanie i ułatwianie dobrowolnego skoordynowanego ujawniania podatności.**

[...]

(19) CERT-UE powinien również wypełniać przewidzianą dla niego w dyrektywie [wniosek NIS 2] rolę dotyczącą współpracy i wymiany informacji z siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Ponadto, zgodnie z zaleceniem Komisji (UE) 2017/1584[8], CERT-UE powinien współpracować z odpowiednimi zainteresowanymi stronami przy prowadzeniu działań podejmowanych w reakcji na incydenty oraz koordynować te działania. Aby przyczyniać się do wysokiego poziomu cyberbezpieczeństwa w całej Unii, CERT-UE powinien prowadzić wymianę informacji dotyczących konkretnych incydentów ze swoimi odpowiednikami krajowymi. CERT-UE powinien również współpracować z innymi partnerami publicznymi i prywatnymi, w tym NATO, pod warunkiem uzyskania uprzedniej zgody IICB.

[8] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

(20) Wspierając cyberbezpieczeństwo na poziomie operacyjnym, CERT-UE powinien korzystać z dostępnej wiedzy fachowej Agencji Unii Europejskiej ds. Cyberbezpieczeństwa **(ENISA)** w ramach współpracy strukturalnej przewidzianej w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881[9]. W stosownych przypadkach należy poczynić specjalne ustalenia pomiędzy oboma podmiotami, aby określić sposób praktycznej realizacji takiej współpracy i uniknąć powielania działań. CERT-UE powinien współpracować z [...] **ENISA** w obszarze analizy zagrożeń i regularnie udostępniać Agencji swoje sprawozdanie dotyczące krajobrazu zagrożeń.

[...]

(22) **Działania CERT-UE i postępowanie przezeń z informacjami na podstawie niniejszego rozporządzenia mogą obejmować przetwarzanie danych osobowych.** Wszelkie dane osobowe przetwarzane na podstawie niniejszego rozporządzenia należy przetwarzać zgodnie z przepisami o ochronie danych, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[10]. W **przypadku gdy zgodnie z niniejszym rozporządzeniem dane osobowe są przekazywane mającym siedzibę w Unii odbiorcom niebędącym podmiotami Unii, powinno się to odbywać zgodnie z art. 9 rozporządzenia (UE) 2018/1725.**

---

9 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)

10 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(23) Postępowanie z informacjami przez CERT-UE oraz **podmioty** [...] Unii powinno być zgodne z **mającymi zastosowanie** przepisami [...] dotyczącymi bezpieczeństwa informacji [...]. [...]

(23a) Do celów udostępniania informacji stosuje się widoczne oznaczenia wskazujące, że odbiorcy tych informacji mają stosować granice udostępniania w oparciu, w szczególności, o umowy o poufności lub nieformalne ustalenia dotyczące poufności, takie jak kod poufności TLP lub inne wyraźne oznaczenia ustalone przez źródło danych. Kod poufności TLP należy rozumieć jako środek informowania o wszelkich ograniczeniach dotyczących dalszego rozpowszechniania informacji. Jest on stosowany niemal we wszystkich zespołach reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz w niektórych ośrodkach analizy i wymiany informacji.

(24) **Niniejsze rozporządzenie oraz nowe zadania przydzielone CERT-UE nie będą miały wpływu na całkowite wydatki w ramach wieloletnich ram finansowych.** Ponieważ usługi i zadania CERT-UE leżą w interesie wszystkich [...] **podmiotów** Unii, wszystkie [...] **podmioty** Unii, które ponoszą wydatki na technologię informatyczną, powinny wnosić odpowiedni wkład na poczet kosztów tych usług i zadań. Wkład ten pozostaje bez uszczerbku dla autonomii budżetowej [...] **podmiotów** Unii. **Wszystkie podmioty Unii i ich organy administracyjne powinny zapewniać optymalizację swoich zasobów przy utrzymaniu ich bieżącego poziomu i zwiększać przyrost wydajności, również poprzez pogłębianie współpracy międzyinstytucjonalnej w dziedzinie cyberbezpieczeństwa. W związku z tym wspólne podejście do łączenia wydatków administracyjnych powinno mieć pierwszeństwo przed zindywidualizowanymi wydatkami podmiotów Unii.**

(25) IICB, z pomocą CERT-UE, powinna dokonywać przeglądu i oceny wykonania niniejszego rozporządzenia oraz przedkładać Komisji sprawozdania zawierające jej ustalenia. Na tej podstawie Komisja powinna przedkładać regularne sprawozdania Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów, **Ponadto zachęca się Europejski Trybunał Obrachunkowy do przeprowadzania regularnych ocen funkcjonowania CERT-UE.**

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Rozdział I
PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. Niniejszym rozporządzeniem ustanawia się **środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w ramach podmiotów Unii** [...]

2. W tym celu niniejsze rozporządzenie ustanawia:

(c) spoczywający na **każdym** [...] **podmiocie** Unii obowiązek ustanowienia [...] ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli;

(d) spoczywające na **podmiotach** [...] Unii obowiązki w zakresie zarządzania ryzykiem w cyberprzestrzeni, zgłaszania incydentów i **wymiany informacji**;

(e) przepisy dotyczące organizacji, **funkcjonowania** i działania **autonomicznego międzyinstytucjonalnego zespołu reagowania na incydenty komputerowe** dla **podmiotów** [...] Unii (CERT-UE) oraz organizacji, **funkcjonowania** i działania Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa **(IICB)**;.

(f) przepisy dotyczące monitorowania wdrażania niniejszego rozporządzenia.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do [...] wszystkich [...] **podmiotów** Unii oraz do [...] [...] CERT-UE i **IICB** [...].

2. Niniejsze rozporządzenie stosuje się bez uszczerbku dla autonomii instytucjonalnej wynikającej z Traktatów.

3. Z wyjątkiem art. 12 ust. 7 niniejsze rozporządzenie nie ma zastosowania do sieci i systemów informatycznych przetwarzających informacje niejawne UE (EUCI).

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „**podmioty** [...] Unii" oznaczają instytucje, organy, **urzędy** i agencje Unii ustanowione Traktatem o Unii Europejskiej, Traktatem o funkcjonowaniu Unii Europejskiej lub Traktatem ustanawiającym Europejską Wspólnotę Energii Atomowej lub na podstawie wspomnianych traktatów;

2) „sieci i systemy informatyczne" oznaczają sieci i systemy informatyczne zgodnie z definicją w art. 4 pkt 1 dyrektywy [wniosek NIS 2];

3) „bezpieczeństwo sieci i systemów informatycznych" oznacza bezpieczeństwo sieci i systemów informatycznych zgodnie z definicją w art. 4 pkt 2 dyrektywy [wniosek NIS 2];

4) „cyberbezpieczeństwo" oznacza cyberbezpieczeństwo [...] **zgodnie z definicją w art. 2 pkt 1 rozporządzenia (UE) nr 2019/881**;

5) „kierownictwo najwyższego szczebla” oznacza kierownika, organ zarządzający lub organ ds. koordynacji i nadzoru na najwyższym szczeblu administracyjnym z **uprawnieniami decyzyjnymi**, z uwzględnieniem ustaleń dotyczących zarządzania na wysokim szczeblu w każdym **podmiocie** [...] Unii;

5a) „zdarzenie potencjalnie wypadkowe” oznacza zdarzenie potencjalnie wypadkowe zgodnie z definicją w art. 4 pkt 4a dyrektywy [wniosek NIS2];

6) „incydent” oznacza incydent [...] **zgodnie z definicją w** art. 4 pkt 5 dyrektywy [wniosek NIS2];

[...]

8) „poważny **incydent** [...]” oznacza każdy incydent **powodujący zakłócenie o takim stopniu, który wykracza poza zdolność podmiotu Unii i CERT-UE do reakcji w odpowiedzi na ten incydent lub który ma znaczący wpływ na co najmniej dwa podmioty Unii;** [...]

9) „postępowanie w przypadku incydentu” oznacza postępowanie w przypadku incydentu [...] **zgodnie z definicją w** art. 4 pkt 6 dyrektywy [wniosek NIS 2];

10) „cyberzagrożenie” oznacza cyberzagrożenie [...] **zgodnie z definicją w** art. 2 pkt 8 rozporządzenia (UE) 2019/881;

[...]

12) „podatność” oznacza podatność zgodnie z definicją w art. 4 pkt 8 dyrektywy [wniosek NIS 2];

[...]

14) „[...] ryzyko” oznacza **ryzyko zgodnie z definicją w art. 4 pkt 7b dyrektywy [wniosek NIS 2];**

[...]

[...]

Artykuł 3a

Przetwarzanie danych osobowych

1) Przetwarzanie danych osobowych na podstawie niniejszego rozporządzenia prowadzone przez CERT-UE, IICB lub podmioty Unii odbywa się zgodnie z rozporządzeniem (UE) 2018/1725.

2) CERT-UE, IICB i podmioty Unii przetwarzają dane osobowe i dokonują ich wymiany w niezbędnym zakresie i w wyłącznym celu wypełniania ich odpowiednich obowiązków wynikających z niniejszego rozporządzenia.

Rozdział II
ŚRODKI NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU CYBERBEZPIECZEŃSTWA

Artykuł 4

Ramy zarządzania ryzykiem, jego nadzorowania i kontroli

1. Każdy [...] **podmiot** Unii ustanawia swoje własne [...] ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli („ramy"), które mają wspierać misję danego podmiotu[...]. [...]Nadzór nad tymi **ramami** sprawuje kierownictwo najwyższego szczebla danego podmiotu, aby zapewnić skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka w cyberprzestrzeni. Ramy te wdraża się najpóźniej do dnia … [15 miesięcy po wejściu w życie niniejszego rozporządzenia] r.

2. Ramy obejmują swym zakresem całość jawnego środowiska informatycznego danego [...] **podmiotu Unii**, w tym każde środowisko informatyczne znajdujące się w jego siedzibie, **sieć technologii operacyjnej**, wszelkie aktywa i usługi, które przekazano w ramach outsourcingu do środowisk przetwarzania w chmurze lub których hosting prowadzą strony trzecie, a także urządzenia mobilne, sieci korporacyjne, sieci biznesowe niepodłączone do internetu oraz wszelkie urządzenia podłączone do środowiska informatycznego. Ramy są **oparte na podejściu uwzględniającym wszystkie zagrożenia oraz na ocenie dojrzałości zgodnie z art. 6 obejmującej każde istotne ryzyko techniczne, operacyjne i organizacyjne, które mogłoby wpłynąć na cyberbezpieczeństwo danego podmiotu Unii** [...].

2a. **Ramy te ustanawiają polityki w zakresie cyberbezpieczeństwa, w tym cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych oraz polityki i procedury w zakresie oceny skuteczności wdrożonych środków zarządzania ryzykiem w cyberprzestrzeni, a także określają role i odpowiedzialność personelu.**

2b. Ramy są poddawane regularnemu przeglądowi, a co najmniej raz na trzy lata, w świetle zmieniających się ryzyk, aktywów i dojrzałości danego podmiotu Unii.

3. Kierownictwo najwyższego szczebla każdego [...] **podmiotu** Unii zapewnia **nadzór** [...] nad wypełnianiem przez [...] **swoją** organizację obowiązków związanych z zarządzaniem ryzykiem w cyberprzestrzeni, jego nadzorowaniem i kontrolą, bez uszczerbku dla formalnej odpowiedzialności innych szczebli zarządzania za zgodność z przepisami i zarządzanie ryzykiem w ich odpowiednich obszarach odpowiedzialności.

3a. **W stosownych przypadkach i bez uszczerbku dla jego odpowiedzialności za wdrożenie niniejszego rozporządzenia kierownictwo najwyższego szczebla każdego podmiotu Unii może zlecić wypełnienie określonego obowiązku wynikającego z niniejszego rozporządzenia innym członkom kadry kierowniczej wyższego szczebla danego podmiotu. Niezależnie od ewentualnego zlecenia dotyczącego wypełnienia jego obowiązku kierownictwo najwyższego szczebla może zostać pociągnięte do odpowiedzialności za nieprzestrzeganie przez podmiot obowiązków wynikających z niniejszego rozporządzenia.**

3b. Kierownictwo najwyższego szczebla każdego podmiotu Unii zapewnia, by podmiot Unii zatwierdził plan dotyczący cyberbezpieczeństwa obejmujący środki zarządzania ryzykiem zgodnie z ich analizą ryzyka, tak by ramy zostały wdrożone zgodnie z niniejszym rozporządzeniem.

[...]

5. Każdy **podmiot** [...] Unii wyznacza lokalnego urzędnika ds. cyberbezpieczeństwa lub osobę pełniącą równoważną funkcję, która działa jako pojedynczy punkt kontaktowy w odniesieniu do wszystkich kwestii związanych z cyberbezpieczeństwem.

   Lokalny urzędnik ds. cyberbezpieczeństwa ułatwia wdrażanie niniejszego rozporządzenia i regularnie składa bezpośrednio kierownictwu najwyższego szczebla sprawozdania na temat stanu wdrożenia.

   Bez uszczerbku dla pełnionej przez lokalnego urzędnika ds. cyberbezpieczeństwa funkcji pojedynczego punktu kontaktowego w każdym podmiocie Unii, podmiot Unii może – na podstawie umowy o gwarantowanym poziomie usług zawartej między tym podmiotem Unii a CERT-UE – przekazać CERT-UE niektóre zadania lokalnego urzędnika ds. cyberbezpieczeństwa związane z wdrażaniem niniejszego rozporządzenia. IICB zdecyduje, czy świadczenie tej usługi będzie częścią podstawowych usług CERT-UE, uwzględniając zasoby ludzkie i finansowe danego podmiotu Unii. O wyznaczeniu lokalnych urzędników ds. cyberbezpieczeństwa oraz wszelkich zmianach w tym zakresie każdy podmiot Unii bez zbędnej zwłoki powiadamia CERT-UE. CERT-UE prowadzi regularnie aktualizowaną listę wyznaczonych lokalnych urzędników ds. cyberbezpieczeństwa.

6. Kadra kierownicza wyższego szczebla w rozumieniu art. 29 ust. 2 Regulaminu pracowniczego[11] lub inni urzędnicy równoważnego szczebla każdego podmiotu Unii regularnie uczestniczą w specjalnych szkoleniach, aby zdobyć wystarczającą wiedzę i wystarczające umiejętności umożliwiające zrozumienie i ocenę ryzyka w cyberprzestrzeni i praktyk zarządzania nim oraz ich wpływu na działalność organizacji.

---

11 **Rozporządzenie nr 259/68 Rady z dnia 29 lutego 1968 r. ustanawiające Regulamin pracowniczy urzędników Unii Europejskiej i warunki zatrudnienia innych pracowników Unii Europejskiej, Dz.U. L 56 z 4 marca 1968 r.**

7. Każdy podmiot Unii posiada skuteczne mechanizmy gwarantujące, że odpowiedni odsetek budżetu przewidzianego na technologie informatyczne jest przeznaczany na cyberbezpieczeństwo. Przy ustalaniu tego odsetka należy odpowiednio uwzględnić przedmiotowe ramy.

Artykuł 5

***Środki zarządzania ryzykiem w cyberprzestrzeni** [...]*

1. [...] **Każdy podmiot Unii pod nadzorem swojego** kierownictwa najwyższego szczebla [...] [...] **zapewnia, by zostały podjęte odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne do celów zarządzania ryzykami zidentyfikowanymi na podstawie ram, o których mowa w art. 4 ust. 1, oraz do celów zapobiegania incydentom lub minimalizacji ich skutków. Środki te zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do stwierdzonych rodzajów ryzyka, przy uwzględnieniu stanu techniki oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia. Przy ocenie proporcjonalności tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyka, jego rozmiar, prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym skutki społeczne i gospodarcze.**

[...]

3. Zgodnie z wytycznymi i zaleceniami IICB podmioty Unii w swoich planach dotyczących cyberbezpieczeństwa przy wdrażaniu środków zarządzania ryzykiem w cyberprzestrzeni uwzględniają co najmniej następujące konkretne dziedziny:

a) polityka w zakresie cyberbezpieczeństwa, w kontekście specyfikacji narzędzi i środków niezbędnych do osiągnięcia celów i priorytetów, o których mowa w art. 4 i w art. 5 ust. 4;

b) analiza ryzyka i polityka w zakresie bezpieczeństwa systemów informatycznych;

c) organizacja cyberbezpieczeństwa, w tym określenie ról i obowiązków;

d) zarządzanie aktywami, w tym baza zasobów informatycznych i mapy sieci informatycznych;

e) bezpieczeństwo zasobów ludzkich i kontrola dostępu;

f) bezpieczeństwo operacji;

g) bezpieczeństwo łączności;

h) nabywanie, rozwój i utrzymanie systemów, w tym postępowanie w przypadku podatności i ich ujawnianie;

i) bezpieczeństwo łańcucha dostaw, w tym aspekty bezpieczeństwa dotyczące stosunków między każdym podmiotem Unii a jego bezpośrednimi dostawcami lub usługodawcami. Podmioty Unii uwzględniają podatności właściwe dla każdego bezpośredniego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa stosowanych przez ich dostawców i usługodawców, w tym ich procedury bezpiecznego rozwoju;

j) postępowanie w przypadku incydentu oraz współpraca z CERT-UE, np. utrzymanie monitorowania bezpieczeństwa i rejestrowania danych dotyczących bezpieczeństwa;

k) zarządzanie ciągłością działania, np. zarządzanie procedurami awaryjnymi oraz przywracanie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej i zarządzanie kryzysowe; oraz

l) promowanie i rozwój programów w zakresie edukacji, umiejętności, podnoszenia świadomości, ćwiczeń i szkoleń w dziedzinie cyberbezpieczeństwa.

4. Zgodnie z wytycznymi i zaleceniami IICB podmioty Unii w swoich planach dotyczących cyberbezpieczeństwa przy wdrażaniu środków zarządzania ryzykiem w cyberprzestrzeni uwzględniają co najmniej następujące konkretne środki zarządzania ryzykiem w cyberprzestrzeni:

a) cele i priorytety w odniesieniu do korzystania z usług w chmurze w rozumieniu art. 4 pkt 19 dyrektywy [wniosek NIS 2] i rozwiązań technicznych umożliwiających telepracę;

b) konkretne kroki na rzecz przyszłego wykorzystania zasad zerowego zaufania, w tym model bezpieczeństwa oraz skoordynowaną strategię na rzecz cyberbezpieczeństwa i zarządzania systemem oparte na przekonaniu, że zagrożenia istnieją zarówno wewnątrz tradycyjnych granic sieci, jak i poza nimi;

c) przyjęcie uwierzytelniania wieloskładnikowego jako normy we wszystkich sieciach i systemach informatycznych;

d) ustanowienie bezpieczeństwa łańcucha dostaw oprogramowania poprzez kryteria regulujące opracowywanie i ocenę bezpiecznego oprogramowania;

e) wzmocnienie przepisów dotyczących zamówień publicznych w celu ułatwienia wysokiego wspólnego poziomu cyberbezpieczeństwa poprzez:

i) usunięcie barier umownych, które ograniczają wymianę z CERT-UE informacji pochodzących od dostawców usług informatycznych na temat incydentów, podatności i cyberzagrożeń;

ii) zobowiązanie umowne do zgłaszania incydentów, podatności i cyberzagrożeń, a także do zapewnienia odpowiedniego reagowania na incydenty i ich monitorowania.

f) stosowanie kryptografii i szyfrowania, w szczególności szyfrowania end-to-end;

g) systemy bezpiecznej łączności w ramach organizacji.

Artykuł 6

Oceny dojrzałości

1. Każdy [...] **podmiot** Unii **– w stosownych przypadkach z pomocą wyspecjalizowanej strony trzeciej –** co najmniej raz na trzy lata przeprowadza ocenę dojrzałości [...], obejmującą wszystkie elementy swojego środowiska informatycznego opisane w art. 4, z uwzględnieniem odpowiednich wytycznych i zaleceń przyjętych zgodnie z art. 13.

2. IICB na zalecenie CERT-UE i po konsultacji z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przyjmuje w ciągu 4 miesięcy od wejścia w życie niniejszego rozporządzenia wytyczne metodologiczne dotyczące przeprowadzania ocen dojrzałości.

3. Po przeprowadzeniu oceny dojrzałości [...] podmiot Unii przedkłada ją IICB. Pierwszą ocenę dojrzałości przeprowadza się najpóźniej [12 miesięcy po wejściu w życie niniejszego rozporządzenia].

Artykuł 7

Plany dotyczące cyberbezpieczeństwa

1. Zgodnie z wnioskami wynikającymi z oceny dojrzałości oraz z uwzględnieniem aktywów i ryzyk określonych zgodnie z art. 4 kierownictwo najwyższego szczebla każdego **podmiotu** [...] Unii zatwierdza – bez zbędnej zwłoki po ustanowieniu ram, **przyjęciu środków zarządzania ryzykiem w cyberprzestrzeni [...] oraz przeprowadzeniu oceny dojrzałości, nie później jednak niż 21 miesięcy po wejściu w życie niniejszego rozporządzenia – plan dotyczący cyberbezpieczeństwa**. Plan dotyczący **cyberbezpieczeństwa** ma na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa **danego** podmiotu **Unii**, a tym samym przyczynia się do [...] wzmocnienia wysokiego wspólnego poziomu cyberbezpieczeństwa wszystkich [...] **podmiotów** Unii. [...] Plan dotyczący **cyberbezpieczeństwa** obejmuje przynajmniej **środki zarządzania ryzykiem w cyberprzestrzeni zgodnie z art. 5** [...] Plan dotyczący cyberbezpieczeństwa jest poddawany przeglądowi przynajmniej co **dwa** [...] lata lub w następstwie [...] **każdej** oceny dojrzałości [...] przeprowadzanej zgodnie z art. 6 **lub każdego przeglądu ram zgodnie z art. 4.**

2. [...]

3. Plan dotyczący cyberbezpieczeństwa **uwzględnia** [...] wszelkie mające zastosowanie wytyczne i zalecenia wydane **zgodnie z art. 13** [...].

4. **Po sporządzeniu planu dotyczącego cyberbezpieczeństwa podmiot Unii przedkłada go IICB.**

Artyku 7a

Wzajemna ocena

1. IICB na zalecenie CERT-UE i po konsultacji z ENISA, ustanawia, najpóźniej do dnia... [24 miesiące od wejścia w życie niniejszego rozporządzenia], korzystając z metodyki wzajemnych ocen i metodyki samooceny zgodnie z art. 16 dyrektywy [wniosek NIS 2] – dostosowanych w razie konieczności do potrzeb podmiotów Unii, metodykę i aspekty organizacyjne wzajemnych ocen z myślą o wyciąganiu wniosków ze wspólnych doświadczeń, wzmocnieniu wzajemnego zaufania, osiągnięciu wspólnego wysokiego poziomu cyberbezpieczeństwa, a także poprawie zdolności i polityk w dziedzinie cyberbezpieczeństwa, którymi dysponują podmioty Unii i które są niezbędne do wdrożenia niniejszego rozporządzenia. Udział we wzajemnych ocenach jest dobrowolny. Przedstawiciele państw członkowskich mogą uczestniczyć we wzajemnej ocenie w charakterze obserwatorów. Wzajemne oceny są prowadzone przez ekspertów w dziedzinie cyberbezpieczeństwa wyznaczonych przez co najmniej dwa podmioty Unii, niebędące podmiotami Unii poddawanymi ocenie, i obejmują co najmniej jeden z następujących elementów:

(i) poziom wdrożenia środków zarządzania ryzykiem w cyberprzestrzeni oraz obowiązków w zakresie zgłaszania incydentów, o których to obowiązkach mowa w art. 5 i 20;

(ii) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie;

(iii) poziom realizacji ram wymiany informacji, o których mowa w art. 19;

(iv) szczególne kwestie o charakterze międzysektorowym.

2. Podmioty Unii mogą wskazać szczegółowe kwestie wymienione ust. 1 ppkt (iv), które powinny zostać poddane ocenie. Zakres oceny, w tym wskazane kwestie, podaje się do wiadomości uczestniczących podmiotów Unii przed rozpoczęciem wzajemnej oceny.

3. Przed rozpoczęciem wzajemnej oceny podmioty Unii mogą przeprowadzić samoocenę aspektów poddawanych przeglądowi i dostarczyć tę samoocenę wyznaczonym ekspertom.

4. Wzajemne oceny wiążą się z fizycznymi lub wirtualnymi kontrolami na miejscu i zdalną wymianą informacji. Z uwagi na zasadę dobrej współpracy podmioty Unii podlegające wzajemnej ocenie dostarczają wyznaczonym ekspertom informacje niezbędne do przeprowadzenia oceny, bez uszczerbku dla przepisów krajowych lub prawa Unii dotyczących ochrony informacji szczególnie chronionych lub informacji niejawnych. Wszelkie informacje uzyskane w trakcie przeprowadzania wzajemnej oceny wykorzystuje się wyłącznie do tego celu. Eksperci uczestniczący we wzajemnej ocenie nie ujawniają osobom trzecim żadnych informacji szczególnie chronionych ani niejawnych uzyskanych w trakcie tej oceny.

5. Po przeprowadzeniu wzajemnej oceny te aspekty, które zostały poddane przeglądowi w danym podmiocie Unii, nie mogą być przedmiotem kolejnych wzajemnych ocen w tym podmiocie Unii przez dwa lata od zakończenia przedmiotowej wzajemnej oceny, chyba że podmioty Unii wystąpią o taką ocenę lub zostanie ona uzgodniona na wniosek IICB.

6. Podmioty Unii zapewniają, by przed rozpoczęciem wzajemnej oceny pozostałe podmioty Unii i IICB zostały poinformowane o wszelkim ryzyku wystąpienia konfliktu interesów w odniesieniu do wyznaczonych ekspertów. Podmioty Unii poddawane wzajemnej ocenie mogą sprzeciwić się wyznaczeniu konkretnych ekspertów z należycie uzasadnionych powodów, o których informują wyznaczające podmioty Unii.

7. **Eksperci uczestniczący we wzajemnych ocenach sporządzają sprawozdania dotyczące ustaleń i wniosków z ocen. Podmioty Unii mogą zgłaszać uwagi do projektów dotyczących ich sprawozdań, które to uwagi są załączane do sprawozdania. Sprawozdania zawierają zalecenia dotyczące poprawy aspektów objętych wzajemną oceną. Sprawozdania składane są IICB i – w stosownych przypadkach – sieci CSIRT. Podmioty Unii poddane ocenie mogą zdecydować o podaniu swojego sprawozdania lub jego zredagowanej części do wiadomości publicznej.**

Artykuł 8

Wykonanie

1. [...]

2. Wykonanie przepisów ustanowionych w niniejszym rozdziale wspierają wytyczne i zalecenia wydawane zgodnie z art. 13.

3. **Na wniosek IICB podmioty Unii składają sprawozdanie na temat konkretnych aspektów niniejszego rozdziału.**

Rozdział III
MIĘDZYINSTYTUCJONALNA RADA DS. CYBERBEZPIECZEŃSTWA

Artykuł 9

Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa

1. Ustanawia się Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB).

2. IICB jest odpowiedzialna za:

   a) monitorowanie wdrażania niniejszego rozporządzenia przez [...] **podmioty Unii**.

   b) nadzór nad realizacją ogólnych priorytetów i celów przez CERT-UE oraz zapewnianie mu strategicznego kierunku działania.

3. W skład IICB wchodzi:

   a) po jednym przedstawicielu wyznaczonym przez:

      (i) Parlament Europejski;

      (ii) Radę Europejską

      (iii) Radę Unii Europejskiej;

      (iv) Komisję Europejską;

      (v) Trybunał Sprawiedliwości Unii Europejskiej;

      (vi) Europejski Bank Centralny;

(vii) Europejski Trybunał Obrachunkowy;

(viii) Europejską Służbę Działań Zewnętrznych;

(ix) Europejski Komitet Ekonomiczno-Społeczny,

(x) Europejski Komitet Regionów;

(xi) Europejski Bank Inwestycyjny;

(xii) Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz

(xiii) Agencję Unii Europejskiej ds. Cyberbezpieczeństwa;

b) trzech przedstawicieli [...] **wyznaczonych** przez sieć agencji Unii Europejskiej (EUAN) na wniosek jej komitetu doradczego ds. ICT w celu reprezentowania interesów agencji i organów, które posiadają własne środowisko informatyczne. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. Członkowie mogą być wspomagani przez zastępców. Przewodniczący może zaprosić innych przedstawicieli [...] **podmiotów** wymienionych powyżej lub innych [...] **podmiotów** Unii do udziału w posiedzeniach IICB bez prawa głosu.

4. IICB uchwala swój regulamin wewnętrzny.

5. IICB wyznacza spośród swoich członków przewodniczącego, zgodnie z regulaminem wewnętrznym, na okres [...] **dwóch** lat. Zastępca przewodniczącego staje się pełnoprawnym członkiem IICB na ten sam okres.

6. IICB **co najmniej trzy razy do roku** odbywa posiedzenia z inicjatywy swojego przewodniczącego **lub** na wniosek CERT-UE **lub** na wniosek któregokolwiek z członków IICB.

7. Każdy członek IICB dysponuje jednym głosem. Decyzje IICB zapadają zwykłą większością głosów, chyba że niniejsze rozporządzenie stanowi inaczej. Przewodniczący nie bierze udziału w głosowaniach, z wyjątkiem sytuacji gdy oddano taką samą liczbę głosów za i przeciw, w którym to przypadku przewodniczący może oddać decydujący głos.

8. IICB może podejmować działania w drodze uproszczonej procedury pisemnej zainicjowanej zgodnie z regulaminem wewnętrznym IICB. W ramach tej procedury daną decyzję uznaje się za zatwierdzoną w terminie wyznaczonym przez przewodniczącego, z wyjątkiem sytuacji, gdy członek zgłosi sprzeciw.

9. O ile IICB nie zdecyduje inaczej, w posiedzeniach IICB w **charakterze obserwatorów** [...] **mogą** uczestniczyć szef CERT-UE, **przewodniczący grupy współpracy NIS**, **przewodniczący EU-CyCLONe oraz przewodniczący sieci CSIRT** lub **ich** zastępcy.

10. Sekretariat IICB jest zapewniany przez **ENISA** [...] i **jest odpowiedzialny przed przewodniczącym IICB**.

11. Przedstawiciele wyznaczeni przez EUAN na wniosek komitetu doradczego ds. ICT przekazują decyzje IICB **członkom EUAN** [...]. Każda agencja lub organ Unii ma prawo zwracać się do przedstawicieli lub przewodniczącego IICB z każdą sprawą, o której zdaniem tej agencji lub organu należy poinformować IICB.

12. [...]

13. IICB może **ustanowić** [...] komitet wykonawczy, który będzie pomagał w jej pracach, i przekazać mu niektóre swoje zadania i uprawnienia, w **szczególności te, które określono w art. 10 lit. c) i e)**. IICB ustanawia regulamin wewnętrzny komitetu wykonawczego, w tym jego zadania i uprawnienia, oraz określa kadencje jego członków.

14. IICB co 12 miesięcy składa Radzie sprawozdanie, w którym szczegółowo przedstawia postępy we wdrażaniu niniejszego rozporządzenia, a w szczególności opisuje zakres współpracy CERT-UE z jego odpowiednikami krajowymi w każdym z państw członkowskich. Sprawozdanie to stanowi wkład do przedstawianego co dwa lata sprawozdania na temat stanu cyberbezpieczeństwa w Unii w tym samym okresie zgodnie z art. 15 dyrektywy [wniosek NIS 2].

Artykuł 10

Zadania IICB

Wykonując swoje obowiązki, IICB w szczególności:

(a) [...] **skutecznie monitoruje i nadzoruje stosowanie** niniejszego rozporządzenia [...] **oraz wspiera** [...] **podmioty** [...] Unii **we wzmacnianiu ich cyberbezpieczeństwa;** w **tym celu IICB może zwracać się do CERT-UE i podmiotów unijnych o sprawozdania *ad hoc*;**

aa) w następstwie dyskusji strategicznej przyjmuje wieloletnią strategię na rzecz podnoszenia poziomu cyberbezpieczeństwa w podmiotach Unii i regularnie – przynajmniej raz na pięć lat – ją ocenia i w razie potrzeby ją zmienia;

b) zatwierdza, na podstawie propozycji **przedłożonej przez** [...] szefa CERT-UE, roczny program prac CERT-UE i monitoruje jego wykonanie;

c) zatwierdza, na podstawie propozycji szefa CERT-UE, katalog usług CERT-UE **oraz jego wszelkie kolejne aktualizacje;**

d) zatwierdza, na podstawie propozycji szefa CERT-UE, roczne planowanie finansowe w zakresie przychodów i wydatków, w tym dotyczące personelu, na potrzeby działalności CERT-UE;

e) zatwierdza, na podstawie propopozycji szefa CERT-UE, ustalenia dotyczące umów o gwarantowanym poziomie usług;

f) analizuje i zatwierdza sprawozdanie roczne sporządzone przez szefa CERT-UE dotyczące działalności CERT-UE i zarządzania środkami finansowymi przez CERT-UE;

g) zatwierdza i monitoruje kluczowe wskaźniki skuteczności w odniesieniu do CERT-UE, określone w oparciu o wniosek szefa CERT-UE;

h) zatwierdza porozumienia o współpracy, **umowy** [...] o gwarantowanym poziomie usług lub umowy między CERT-UE a innymi podmiotami zawarte na podstawie art. 17;

i) ustanawia [...] techniczne grupy doradcze, [...] aby wspierały prace IICB, zatwierdza zakres ich uprawnień i zadań i wyznacza ich przewodniczących.

j) **przyjmuje wytyczne i zalecenia na podstawie propozycji CERT-UE zgodnie z art. 13 i zleca CERT-UE wydanie, wycofanie lub zmianę propozycji wytycznych lub zaleceń lub wezwania do działania;**

k) otrzymuje i ocenia dokumenty i sprawozdania składane przez podmioty Unii na podstawie niniejszego rozporządzenia;

l) wspiera utworzenie nieformalnej grupy skupiającej lokalnych urzędników ds. cyberbezpieczeństwa ze wszystkich podmiotów i tym samym ułatwia wymianę najlepszych praktyk i informacji dotyczących wdrażania niniejszego rozporządzenia;

m) opracowuje plan zarządzania kryzysami w cyberprzestrzeni, by wspierać skoordynowane zarządzanie, na poziomie operacyjnym, poważnymi incydentami, z jakimi mierzą się podmioty Unii oraz by przyczyniać się do regularnej wymiany istotnych informacji, zwłaszcza na tema skutków i dotkliwości poważnych incydentów oraz możliwych sposobów łagodzenia ich skutków.

Artykuł 11

Zapewnianie zgodności

1. IICB **zgodnie z art. 9 ust. 2 i art. 10 skutecznie** monitoruje wdrażanie przez [...] **podmioty** Unii niniejszego rozporządzenia oraz przyjętych wytycznych, zaleceń i wezwań do działania. W **tym celu IICB może zwrócić się o informacje lub dokumentację niezbędne do oceny właściwego stosowania przepisów niniejszego rozporządzenia przez podmioty Unii. Do celów przyjmowania środków zapewniania zgodności na podstawie niniejszego artykułu dany podmiot Unii nie ma prawa głosu.**

2. W przypadku gdy IICB stwierdzi, że **podmioty** [...] Unii nie stosują lub nie wdrażają skutecznie niniejszego rozporządzenia lub wytycznych, zaleceń i wezwań do działania wydanych na podstawie niniejszego rozporządzenia – bez uszczerbku dla wewnętrznych procedur odpowiedniego **podmiotu** Unii i **po daniu temu podmiotowi lub danej osobie możliwości przedstawienia swojego stanowiska – może:**

a) wydaje ostrzeżenie w **celu usunięcia stwierdzonych niedociągnięć w określonym terminie, zawierające zalecenia dotyczące zmiany przyjętych przez podmioty Unii na podstawie niniejszego rozporządzenia dokumentów dotyczących cyberbezpieczeństwa;** w stosownych przypadkach ze względu na istotne ryzyko w cyberprzestrzeni grono odbiorców ostrzeżenia ulega odpowiedniemu ograniczeniu;

aa) wydaje uzasadnione powiadomienie skierowane do podmiotu Unii, w przypadku gdy niedociągnięcia stwierdzone w wydanym uprzednio ostrzeżeniu nie zostały usunięte w wystarczającym stopniu i w określonym terminie oraz formalnie przekazuje tę opinię Radzie, Parlamentowi Europejskiemu i Komisji;

b) **wydaje w szczególności:** [...]

(i) zalecenie dotyczące przeprowadzenia audytu podmiotu Unii;

(ii) żądanie przeprowadzenia audytu przez zewnętrzną służbę audytu.

c) zwraca się do podmiotu Unii o zapewnienie zgodności zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontrolowania z przepisami niniejszego rozporządzenia, w stosownych przypadkach w określony sposób i w określonym terminie.

d) wydaje skierowaną do wszystkich państw członkowskich i podmiotów Unii opinię zalecającą tymczasowe zawieszenie przepływów danych do danego podmiotu Unii.

3. W przypadku gdy IICB przyjęła środki na podstawie ust. 2 lit. a)–d), dany podmiot Unii przedstawia szczegółowy opis środków i działań podjętych w celu usunięcia zarzucanych mu niedociągnięć stwierdzonych przez IICB. Podmiot Unii przedkłada ten opis w rozsądnym terminie uzgodnionym z IICB.

4. **W przypadku gdy IICB uzna, że naruszenie przepisów niniejszego rozporządzenia przez dany podmiot Unii ma charakter trwały i wynikający bezpośrednio z działań lub zaniechań ze strony urzędnika lub innego pracownika Unii, w tym kierownictwa najwyższego szczebla, IICB zwraca się do danego podmiotu o podjęcie odpowiednich działań, w tym o charakterze dyscyplinarnym, zgodnie – w szczególności – z przepisami ustanowionymi w regulaminie pracowniczym i warunkach zatrudnienia innych pracowników Unii Europejskiej. W tym celu IICB przekazuje danemu podmiotowi niezbędne informacje.**

Rozdział IV
CERT-UE

Artykuł 12

Misja i zadania CERT-UE

1. [...] [...] **Misją CERT-UE** jest przyczynianie się do bezpieczeństwa jawnego środowiska informatycznego wszystkich **podmiotów** [...] Unii poprzez doradzanie im w zakresie cyberbezpieczeństwa, pomaganie im w zapobieganiu incydentom, wykrywaniu ich, łagodzeniu ich skutków i reagowaniu na nie oraz poprzez występowanie dla tych podmiotów w roli punktu wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty.

1a. CERT-UE gromadzi, analizuje i udostępnia podmiotom Unii informacje na temat zagrożeń, podatności i incydentów dotyczących jawnej infrastruktury ICT oraz zarządza tymi informacjami. Koordynuje reagowanie na incydenty na poziomie międzyinstytucjonalnym i na poziomie podmiotów Unii, również poprzez świadczenie lub koordynowanie specjalistycznej pomocy operacyjnej.

2. CERT-UE wykonuje następujące zadania dla **podmiotów** [...] Unii:

a) wspiera je we wdrażaniu niniejszego rozporządzenia oraz przyczynia się do koordynacji stosowania niniejszego rozporządzenia za pomocą **przepisów** [...] wymienionych w art. 13 ust. 1 lub poprzez sporządzanie doraźnych sprawozdań, o które wystąpiła IICB;

b) [...] **świadczy standardowe usługi CSIRT wszystkim podmiotom Unii za pośrednictwem** pakietu usług z zakresu cyberbezpieczeństwa opisanych w katalogu usług („usługi podstawowe”);

c) utrzymuje sieć równorzędnych podmiotów i partnerów w celu wspierania usług określonych w art. 16 i 17;

d) zwraca uwagę IICB na wszelkie problemy związane z wdrażaniem niniejszego rozporządzenia oraz wdrażaniem wytycznych, zaleceń i wezwań do działania;

e) **na podstawie informacji, o których mowa w ust. 1a,** [...] przyczynia się do zapewnienia w **ścisłej współpracy z ENISA** orientacji sytuacyjnej w zakresie cyberbezpieczeństwa UE. **Takie informacje udostępnia się IICB oraz sieci CSIRT i EU-INTCEN;**

f) występuje w charakterze odpowiednika wyznaczonego koordynatora dla podmiotów Unii, jak określono w art. 6 dyrektywy [wniosek NIS 2].

[...]

[...]

[...]

[...]

[...]

4. **W granicach swoich kompetencji** CERT-UE prowadzi ustrukturyzowaną współpracę z [...] **ENISA** w zakresie budowania zdolności, współpracy operacyjnej i długoterminowych analiz strategicznych cyberzagrożeń zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881.

5. CERT-UE może świadczyć następujące usługi nieopisane w jego katalogu usług („usługi płatne”):

   a) usługi wspierające cyberbezpieczeństwo środowisk informatycznych **podmiotów** [...] Unii inne niż usługi określone w ust. 2, na podstawie umów o gwarantowanym poziomie usług i z zastrzeżeniem dostępnych zasobów;

   b) usługi wspierające operacje lub projekty w zakresie cyberbezpieczeństwa **podmiotów** [...] Unii inne niż usługi zapewniające ochronę ich środowiska informatycznego, na podstawie pisemnych umów i po uprzednim zatwierdzeniu przez IICB;

   c) usługi świadczone na rzecz organizacji niebędących **podmiotami** [...] Unii i ściśle współpracujących z **podmiotami** [...] Unii, na przykład ze względu na przydzielone im zadania lub obowiązki na mocy prawa Unii, które to usługi wspierają bezpieczeństwo środowiska informatycznego tych organizacji, na podstawie pisemnych umów i po uprzednim zatwierdzeniu przez IICB.

6. CERT-UE może organizować ćwiczenia w zakresie cyberbezpieczeństwa **lub w nich uczestniczyć** lub zalecać uczestnictwo w istniejących ćwiczeniach, w stosownych przypadkach w ścisłej współpracy z [...] **ENISA**, w celu testowania poziomu cyberbezpieczeństwa **podmiotów** [...] Unii.

7. CERT-UE może udzielać pomocy **podmiotom** [...] Unii w zakresie incydentów w niejawnym środowisku informatycznym, o ile zainteresowane **podmioty** [...] **Unii** wyraźnie się o to zwrócą **zgodnie ze swoimi odpowiednimi procedurami**. **W takim przypadku przepisy określone w art. 19–21 niniejszego rozporządzenia nie mają zastosowania. Udzielanie pomocy przez CERT-UE na podstawie niniejszego ustępu pozostaje bez uszczerbku dla mających zastosowanie przepisów państw członkowskich lub przepisów Unii dotyczących ochrony informacji szczególnie chronionych lub informacji niejawnych.**

8. CERT-UE informuje podmioty Unii o swoich procedurach i procesach postępowania w razie incydentów.

9. CERT-UE może, za zgodą danego podmiotu Unii, monitorować ruch w jego sieci.

10. CERT-UE może, na wyraźny wniosek jednostek politycznych podmiotów Unii, zapewnić doradztwo techniczne lub wkład techniczny w zakresie odpowiednich spraw z dziedziny polityki.

11. CERT-UE, we współpracy z Europejskim Inspektorem Ochrony Danych, wspiera zainteresowane podmioty Unii w reagowaniu na incydenty, których skutkiem są naruszenia ochrony danych osobowych.

Artykuł 13

Wytyczne, zalecenia i wezwania do działania

1. CERT-UE wspiera wdrażanie niniejszego rozporządzenia poprzez:

   a) wydawanie wezwań do działania opisujących pilne środki w zakresie bezpieczeństwa, o których zastosowanie w określonym terminie apeluje się do podmiotów [...] Unii; Bez zbędnej zwłoki po otrzymaniu wezwania do działania odnośny podmiot Unii informuje CERT-UE o sposobie zastosowania tych środków;

   b) przedstawianie IICB propozycji wytycznych skierowanych do wszystkich [...] **podmiotów** Unii lub części z nich;

   c) przedstawianie IICB propozycji zaleceń skierowanych do poszczególnych **podmiotów** [...] Unii.

2. Wytyczne i zalecenia mogą obejmować:

   a) sposoby zarządzania ryzykiem w cyberprzestrzeni i formułowania **środków z tego zakresu** [...] lub usprawnienia tych procesów;

   b) sposoby przeprowadzania ocen dojrzałości i opracowywania planów dotyczących cyberbezpieczeństwa; oraz

   c) w stosownych przypadkach, wykorzystanie wspólnej technologii, architektury i powiązanych najlepszych praktyk w celu osiągnięcia interoperacyjności i wspólnych norm, w **tym skoordynowanego podejścia do bezpieczeństwa łańcucha dostaw** [...].

[...]

[...]

Artykuł 14

Szef CERT-UE

1. Szefa CERT-UE mianuje Komisja, po uzyskaniu zgody dwóch trzecich członków IICB. Na wszystkich etapach procedury poprzedzającej mianowanie szefa CERT-UE, w szczególności podczas przygotowywania ogłoszeń o naborze, rozpatrywania zgłoszeń oraz powoływania komisji selekcyjnych w odniesieniu do tego stanowiska, zasięga się opinii IICB.

2. Szef CERT-UE jest odpowiedzialny za odpowiednie funkcjonowanie tego zespołu, działając w ramach swoich kompetencji pod kierunkiem IICB. Jest on odpowiedzialny za wprowadzanie w życie strategicznego kierunku, wytycznych, celów i priorytetów określonych przez IICB i za zarządzanie CERT-UE, w tym jego zasobami finansowymi i ludzkimi. Regularnie składa sprawozdania przewodniczącemu IICB.

3. Szef CERT-UE wspomaga odpowiedzialnego delegowanego urzędnika zatwierdzającego w sporządzaniu rocznego sprawozdania z działalności zawierającego informacje dotyczące finansów i zarządzania, w tym wyniki kontroli, przygotowywanego zgodnie z art. 66 ust. 9 rozporządzenia finansowego i regularnie składa temu urzędnikowi sprawozdania z realizacji działań, co do których szefowi CERT-UE przekazano uprawnienia na zasadzie subdelegacji.

4. Szef CERT-UE opracowuje co roku w odniesieniu do swoich działań plan finansowy dochodów i wydatków administracyjnych, propozycję rocznego programu prac, katalogu usług CERT-UE i jego aktualizacji, propozycję warunków umów o gwarantowanym poziomie usług oraz propozycję kluczowych wskaźników skuteczności działania CERT-UE, które mają zostać zatwierdzone przez IICB zgodnie z art. 10.

Dokonując przeglądu wykazu usług w katalogu usług CERT-UE, szef CERT-UE uwzględnia zasoby przydzielone CERT-UE.

5. Szef CERT-UE [...] przedkłada IICB [...] **roczne** sprawozdania dotyczące realizacji zadań CERT-UE, planowania finansowego, przychodów, wykonania budżetu, zawartych umów o gwarantowanym poziomie usług i pisemnych umów, współpracy z jego odpowiednikami i partnerami, a także podróży służbowych realizowanych przez jego pracowników, w tym sprawozdania, o których mowa w art. 10 [...] lit. a).

Artykuł 15

Sprawy finansowe i kadrowe

[...]

1a. Wprawdzie CERT-UE jest ustanowiony jako autonomiczny, międzyinstytucjonalny dostawca usług dla wszystkich podmiotów Unii, jest jednak zintegrowany ze strukturą administracyjną jednej z dyrekcji generalnych Komisji, aby mógł korzystać z komisyjnych struktur wsparcia administracyjnego, finansowego, zarządczego i rachunkowego. Komisja informuje IICB o umiejscowieniu CERT-UE w strukturze administracyjnej oraz o wszelkich zmianach w tym zakresie. Podejście to będzie regularnie oceniane, najpóźniej przed końcem każdych wieloletnich ram finansowych ustanowionych zgodnie z art. 312 TFUE, aby umożliwić podjęcie odpowiednich działań.

2. W zakresie stosowania procedur administracyjnych i finansowych szef CERT-UE działa z upoważnienia Komisji.

3. Zadania i działania CERT-UE, w tym usługi świadczone przez CERT-UE zgodnie z art. 12 ust. 2, [...] 4 i 6 oraz art. 13 ust. 1 na rzecz [...] **podmiotów** Unii finansowanych w ramach działu wieloletnich ram finansowych dotyczącego europejskiej administracji publicznej, są finansowane z odrębnej linii budżetowej budżetu Komisji. Stanowiska przeznaczone dla CERT-UE wyszczególnia się w przypisie do planu zatrudnienia Komisji.

4. **Podmioty** [...] Unii inne niż te wymienione w ust. 3 wnoszą roczny wkład finansowy na rzecz CERT-UE w celu pokrycia kosztów usług świadczonych przez CERT-UE na podstawie ust. 3. Odpowiednie wkłady opierają się na wskazówkach wydanych przez IICB i są przedmiotem uzgodnień zawartych między każdym podmiotem a CERT-UE w umowach o gwarantowanym poziomie usług. Wkłady odzwierciedlają sprawiedliwy i proporcjonalny udział w całkowitych kosztach świadczonych usług. Ujmuje się je w odrębnej linii budżetowej, o której mowa w ust. 3, jako dochody przeznaczone na określony cel, jak przewidziano w art. 21 ust. 3 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046[12].

5. Koszty realizacji zadań określonych w art. 12 ust. 5 odzyskuje się od [...] **podmiotów** Unii korzystających z usług CERT-UE. Dochody przypisuje się do linii budżetowych przeznaczonych na pokrycie kosztów.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

Artykuł 16

Współpraca CERT-UE z jego odpowiednikami w państwach członkowskich

1. CERT-UE podejmuje **bez zbędnej zwłoki** współpracę i prowadzi wymianę informacji z odpowiednikami krajowymi w państwach członkowskich, **zwłaszcza** [...] [...] [...] z zespołami CSIRT, o **których mowa w art. 9 dyrektywy [wniosek NIS 2], lub, w stosownych przypadkach, właściwymi organami krajowymi** oraz pojedynczymi punktami kontaktowymi, o których mowa w art. 8 dyrektywy [wniosek NIS 2], w zakresie cyberzagrożeń, podatności i incydentów, możliwych środków przeciwdziałania oraz wszystkich kwestii istotnych dla poprawy ochrony środowiska informatycznego [...] **podmiotów** Unii, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 13 dyrektywy [wniosek NIS 2].

1a. CERT-UE niezwłocznie powiadamia wszystkich właściwych krajowych odpowiedników, o których mowa w ust. 1, w danym państwie członkowskim, gdy dowie się o znaczących incydentach występujących na terytorium tego państwa członkowskiego, chyba że CERT-UE posiada informacje, że dotknięty incydentem podmiot Unii zgłosił już ten incydent zgodnie z art. 20 ust. 2a.

2. CERT-UE **bez zbędnej zwłoki** [...] prowadzi wymianę informacji dotyczących konkretnych incydentów ze swoimi odpowiednikami krajowymi w państwach członkowskich, aby ułatwić wykrywanie podobnych cyberzagrożeń lub incydentów **lub wnieść wkład w analizę incydentu** bez **konieczności** uzyskania zgody **podmiotu Unii** dotkniętego incydentem. CERT-UE **nie prowadzi** [...] wymiany informacji dotyczących konkretnych incydentów, która umożliwiłaby identyfikację celu, w który wymierzony był cyberincydent, **chyba że** [...]

   a) odbywa się to za zgodą podmiotu Unii dotkniętego incydentem;

   b) podmiot Unii dotknięty incydentem podał już do wiadomości fakt, że był celem cyberincydentu;

c) podmiot Unii dotknięty incydentem nie wyraził zgody, ale podanie do wiadomości tożsamości podmiotu Unii dotkniętego incydentem może zwiększyć prawdopodobieństwo uniknięcia lub złagodzenia innych incydentów w innych podmiotach. Takie decyzje wymagają zatwierdzenia przez szefa CERT-UE. Odnośny podmiot Unii dotknięty incydentem, jest informowany przed takim upublicznieniem.

Artykuł 17

Współpraca CERT-UE z [...] <u>innymi</u> odpowiednikami

1. CERT-UE może współpracować ze swoimi odpowiednikami w **Unii Europejskiej innymi niż wymienieni w art. 16**, w tym z odpowiednikami działającymi w konkretnych sektorach, w zakresie narzędzi i metod, takich jak techniki, taktyka, procedury i najlepsze praktyki, a także w zakresie cyberzagrożeń i podatności. CERT-UE zwraca się do IICB o uprzednią – **analizowaną indywidualnie dla każdego przypadku** – zgodę na podjęcie wszelkiej współpracy z takimi [...] odpowiednikami. **CERT-UE informuje wszystkich właściwych krajowych odpowiedników, o których mowa w art. 16 ust. 1, w państwie członkowskim, w którym dany odpowiednik ma siedzibę, w przypadku gdy CERT-UE nawiązuje współpracę z takimi odpowiednikami.**

2. CERT-UE może współpracować z innymi partnerami, takimi jak podmioty handlowe, organizacje międzynarodowe, podmioty krajowe spoza Unii Europejskiej lub indywidualni eksperci, w celu gromadzenia informacji na temat ogólnych i szczególnych cyberzagrożeń, podatności i możliwych środków przeciwdziałania. CERT-UE zwraca się do IICB o uprzednią – **analizowaną indywidualnie dla każdego przypadku** – zgodę na podjęcie szerszej współpracy z takimi partnerami.

3. CERT-UE może, **pod warunkiem zawarcia z danym partnerem uzgodnień lub umowy o poufności** – za zgodą danego **podmiotu Unii** [...] dotkniętego incydentem, przekazać partnerom, o **których mowa w ust. 1 i 2**, informacje dotyczące konkretnego incydentu **wyłącznie do celów uzyskania ich wkładu** [...] w jego analizę. **Takie porozumienia lub umowy o poufności podlegają weryfikacji prawnej zgodnie z odpowiednimi procedurami wewnętrznymi Komisji. Porozumienia czy umowy o poufności nie wymagają uprzedniej zgody IICB, ale o ich zawarciu informuje się przewodniczącego IICB.**

4. **Za uprzednią zgodą IICB CERT-UE może w drodze wyjątku zawierać umowy o gwarantowanym poziomie usług z podmiotami innymi niż podmioty Unii.**

Rozdział V
OBOWIĄZKI W ZAKRESIE WSPÓŁPRACY I ZGŁASZANIA

Artykuł 18

Postępowanie z informacjami

1. CERT-UE oraz [...] **podmioty** Unii przestrzegają obowiązku zachowania tajemnicy zawodowej zgodnie z art. 339 Traktatu o funkcjonowaniu Unii Europejskiej lub równoważnymi mającymi zastosowanie ramami.

2. Przepisy rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[13] mają zastosowanie w odniesieniu do wniosków o udzielenie publicznego dostępu do dokumentów przechowywanych przez CERT-UE, w tym wynikającego z tego rozporządzenia obowiązku konsultowania się z innymi [...] **podmiotami** Unii **oraz – w stosownych przypadkach – z państwami członkowskimi**, jeśli przedmiotem wniosku są ich dokumenty.

[...]

4. Postępowanie z informacjami przez CERT-UE oraz **podmioty** [...] Unii jest zgodne z **mającymi zastosowanie** przepisami [...] dotyczącymi bezpieczeństwa informacji [...].

[...]

Artykuł 19

[...] ***Wymiana informacji o cyberbezpieczeństwie***

-1. Podmioty Unii mogą dobrowolnie przekazywać CERT-UE informacje na temat zagrożeń cyberbezpieczeństwa, incydentów, zdarzeń potencjalnie wypadkowych i podatności, które ich dotyczą. CERT-UE zapewnia dostępność skutecznych środków komunikacji, aby ułatwić wymianę informacji z podmiotami Unii. CERT-UE może rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych.

[13] Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

1. W [...] celu **realizacji swojej misji i zadań określonych w art. 12** CERT-UE [...] może zwracać się do **podmiotów** [...] Unii o przekazanie mu informacji z ich odpowiednich rejestrów zasobów informatycznych, w **tym informacji dotyczących cyberzagrożeń, zdarzeń potencjalnie wypadkowych, podatności, oznak naruszenia integralności systemu, alarmów i zaleceń dotyczących konfiguracji narzędzi cyberbezpieczeństwa do celów wykrywania cyberincydentów** [...]. **Podmiot** [...] Unii, do którego się zwrócono, bez zbędnej zwłoki przekazuje przedmiotowe informacje oraz ich wszelkie późniejsze aktualizacje.

2. **Podmioty** [...] Unii, na wniosek CERT-UE i bez zbędnej zwłoki, przekazują mu informacje cyfrowe powstałe w wyniku korzystania z urządzeń elektronicznych uczestniczących w incydentach, które u nich wystąpiły. CERT-UE może dodatkowo sprecyzować, jakich rodzajów tych informacji cyfrowych potrzebuje do celów orientacji sytuacyjnej i reagowania na incydenty.

3. CERT-UE może prowadzić z **podmiotami Unii** wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację **podmiotu** [...] Unii dotkniętego incydentem, wyłącznie za zgodą tego podmiotu. W **przypadku odmowy udzielenia zgody dany podmiot przedstawia CERT-UE należycie uzasadnione powody.** [...]

4. Obowiązki w zakresie wymiany informacji nie obejmują informacji niejawnych UE (EUCI) ani informacji, w **przypadku których źródło informacji za pomocą widocznego oznaczenia wykluczyło możliwość ich dystrybucji poza podmiot Unii będący odbiorcą, chyba że źródło informacji [...] wyraźnie pozwoli na przekazanie tych informacji CERT-UE.** [...]

Artykuł 20

[...] ***Obowiązki w zakresie <u>zgłaszania</u>***

-1. Incydent uznaje się za znaczący, jeżeli:

a) spowodował lub ma potencjał spowodować poważne zakłócenia operacyjne w funkcjonowaniu podmiotu Unii lub straty finansowe danego podmiotu Unii;

b) wpłynął lub może wpłynąć na inne osoby fizyczne lub prawne poprzez spowodowanie znaczących szkód materialnych lub niematerialnych.

1. Wszystkie **podmioty** [...] Unii **przedkładają CERT-UE**: [...]

[...].

(a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od uzyskania wiedzy o znaczącym incydencie – wczesne ostrzeżenie, w którym w stosownych przypadkach wskazuje się, czy znaczący incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze i czy wywarł lub może wywrzeć wpływ transgraniczny;

(b) bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od uzyskania wiedzy o znaczącym incydencie – zgłoszenie incydentu, w stosownych przypadkach z aktualizacją informacji, o których mowa w lit. a), i ze wskazaniem wstępnej oceny znaczącego incydentu, jego dotkliwości i skutków, a w stosownych przypadkach także **oznak** naruszenia integralności systemu;

(c) na wniosek CERT-UE sprawozdanie okresowe na temat odpowiednich aktualizacji statusu;

(d) sprawozdanie końcowe nie później niż miesiąc po dokonaniu zgłoszenia znaczącego incydentu, o którym mowa w lit. b), zawierające co najmniej następujące elementy:

(i) szczegółowy opis znaczącego incydentu, jego dotkliwości i skutków;

(ii) rodzaj zagrożenia lub pierwotną przyczynę, które prawdopodobnie były źródłem znaczącego incydentu;

(iii) zastosowane i bieżące środki ograniczające ryzyko;

(iv) w stosownych przypadkach – transgraniczny wpływ znaczącego incydentu;

(e) w przypadku znaczących incydentów nadal trwających w momencie składania sprawozdania końcowego, o którym mowa w lit. d), sprawozdanie z postępu prac w danym momencie oraz sprawozdanie końcowe w terminie jednego miesiąca od rozwiązania incydentu.

[...]

(g) [...]

(h) [...]

(i) [...]

(j) [...]

2a. Wszystkie podmioty Unii udostępniają informacje zgłoszone zgodnie z ust. 1 w tym samym terminie wszelkim stosownym odpowiednikom krajowym, o których mowa w art. 16 ust. 1, właściwym z uwagi na siedzibę podmiotów Unii.

3. **Co trzy miesiące** CERT-UE przedkłada [...] **IICB, EU INTCEN oraz sieci CSIRT** [...] sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane na temat [...] cyberzagrożeń, [...] podatności **zgodnie z art. 19, odpowiedzi podmiotów Unii na wezwania do działania wydane zgodnie z art. 13 ust. 1 lit. a)** oraz znaczących incydentów zgłoszonych zgodnie z ust. 1. **Sprawozdanie to stanowi wkład do przedstawianego co dwa lata sprawozdania na temat stanu cyberbezpieczeństwa w Unii zgodnie z art. 15 dyrektywy [wniosek NIS 2].**

4. IICB [...] **do dnia [6 miesięcy od daty wejścia w życie niniejszego rozporządzenia]** wyda wytyczne lub zalecenia **doprecyzowujące** warunki, **format** i treść **zgłoszeń i sprawozdań** [...]. **Wytyczne lub zalecenia w należyty sposób uwzględniają przepisy wdrażane wszelkimi aktami wykonawczymi zgodnie z art. 20 ust. 11 dyrektywy [wniosek NIS 2];** CERT-UE rozpowszechnia odpowiednie szczegółowe informacje techniczne w celu umożliwienia proaktywnego wykrywania incydentów, reagowania na nie lub wprowadzania środków łagodzących ich skutki przez **podmioty** [...] Unii

5. Obowiązki w zakresie zgłaszania [...] nie obejmują EUCI ani informacji, w **przypadku których źródło informacji za pomocą widocznego oznaczenia wykluczyło możliwość ich dystrybucji poza podmiot Unii będący odbiorcą, chyba że źródło informacji [...] wyraźnie pozwoli na przekazanie tych informacji CERT-UE.** [...]

Artykuł 21

***Koordynacja i współpraca w zakresie reagowania na incydenty** [...]*

1. Działając jako punkt wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty, CERT-UE ułatwia wymianę informacji dotyczących cyberzagrożeń, podatności i incydentów między:

   a) **podmioty** [...] Unii;

   b) odpowiednikami, o których mowa w art. 16 i 17.

2. CERT-UE [...] **w stosownych przypadkach w ścisłej współpracy w ENISA zgodnie z art. 7 ust. 7 lit. d) aktu o cyberbezpieczeństwie**[14] ułatwia koordynację między **podmiotami** [...] Unii w zakresie reagowania na incydenty, co obejmuje:

   a) przyczynianie się do spójnej komunikacji zewnętrznej;

   [...]

   c) optymalne wykorzystanie zasobów operacyjnych;

   d) koordynację z innymi mechanizmami reagowania kryzysowego na szczeblu Unii.

3. CERT-UE, w **ścisłej współpracy z ENISA**, wspiera **podmioty** [...] Unii w zakresie orientacji sytuacyjnej w odniesieniu do cyberzagrożeń, podatności i incydentów.

---

14 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)

4. IICB, **do dnia [12 miesięcy od daty wejścia w życie niniejszego rozporządzenia], na podstawie propozycji CERT-UE, [...] przyjmie wytyczne lub zalecenia** dotyczące koordynacji reagowania na incydenty i współpracy w tym zakresie w odniesieniu do znaczących incydentów. W przypadku podejrzenia, że incydent nosi znamiona przestępstwa, CERT-UE doradza, jak zgłaszać incydent organom ścigania.

Artykuł 22

***Zarządzanie poważnymi incydentami** [...]*

-1. Aby wspierać skoordynowane zarządzanie poważnymi incydentami na poziomie operacyjnym mającymi wpływ na podmioty Unii oraz przyczyniać się do regularnej wymiany istotnych informacji między podmiotami Unii i z państwami członkowskimi, IICB opracowuje plan zarządzania kryzysami w cyberprzestrzeni oparty o działania wyszczególnione w art. 21 ust. 2, w ścisłej współpracy z CERT-UE i ENISA, i uwzględnia w nim co najmniej następujące elementy:

a) zasady koordynacji i przepływu informacji między podmiotami Unii na potrzeby zarządzania poważnymi incydentami na poziomie operacyjnym;

b) wspólne standardowe procedury operacyjne(SPD);

c) wspólną taksonomię dotkliwości poważnych incydentów i punktów wywołujących kryzys;

d) regularne ćwiczenia;

e) kanały bezpiecznej komunikacji, które mają być wykorzystywane;

f) punkt kontaktowy dla EU-CyCLONe, który dzieli się odpowiednimi informacjami z EU-CyCLONe w ramach wkładu we wspólną orientację sytuacyjną.

1. CERT-UE koordynuje między **podmiotami** [...] Unii reagowanie na poważne **incydenty**. Prowadzi wykaz fachowej wiedzy technicznej, która może być potrzebna, aby reagować na incydenty w przypadku **poważnych incydentów** [...].

2. **Podmioty** [...] Unii wnoszą wkład w tworzenie wykazu fachowej wiedzy technicznej, udostępniając aktualizowany co roku wykaz ekspertów dostępnych w ich odpowiednich organizacjach, z wyszczególnieniem ich konkretnych umiejętności technicznych.

3. W następstwie szczególnego wniosku państwa członkowskiego, w którym znajduje się dotknięty incydentem podmiot Unii, oraz za [...] zgodą **tego** [...] **podmiotu** [...] Unii CERT-UE może również zwrócić się do ekspertów wymienionych w wykazie, o którym mowa w ust. 2, o wniesienie wkładu w działania podejmowane w reakcji na poważny **incydent [...] w tym podmiocie Unii [...].**

Rozdział VI
PRZEPISY KOŃCOWE

Artykuł 23

Początkowa realokacja środków budżetowych

Komisja proponuje realokację zasobów ludzkich i finansowych z odpowiednich **podmiotów** [...] Unii do budżetu Komisji. Realokacja ta staje się skuteczna w tym samym czasie co pierwszy budżet przyjęty po wejściu w życie niniejszego rozporządzenia.

Artykuł 24

Przegląd

1. IICB, z pomocą CERT-UE, składa Komisji okresowe sprawozdania z wykonania niniejszego rozporządzenia. IICB może również kierować do Komisji zalecenia, aby Komisja przeprowadziła **przegląd** [...] niniejszego rozporządzenia.

2. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie z wykonania niniejszego rozporządzenia najpóźniej **36** [...] miesięcy po jego wejściu w życie, a następnie co trzy lata.

3. Komisja dokonuje oceny funkcjonowania niniejszego rozporządzenia i składa sprawozdanie Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów nie **później** [...] niż pięć lat od daty jego wejścia w życie. **Do sprawozdania dołącza się w razie potrzeby wniosek ustawodawczy.**

Artykuł 25

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący / Przewodnicząca	*Przewodniczący / Przewodnicząca*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ZAŁĄCZNIK II

[...]

[...]

[...]

[...]

[...]

[...]

[...]