Nowe przepisy mające na celu wzmocnienie cyberbezpieczeństwa i bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach UE

Bruksela, 22 marca 2022 r.

Komisja zaproponowała dziś nowe przepisy mające na celu ustanowienie wspólnych środków w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji we wszystkich instytucjach, organach, urzędach i agencjach UE. Propozycja ta ma na celu wzmocnienie ich odporności i zdolności reagowania na zagrożenia cyberbezpieczeństwa i cyberincydenty, a także zapewnienie odpornej i bezpiecznej administracji publicznej UE w kontekście nasilających się szkodliwych działań w cyberprzestrzeni na świecie.

Komisarz ds. budżetu i administracji Johannes **Hahn** powiedział: *W połączonym środowisku pojedynczy cyberincydent może mieć wpływ na całą organizację. Dlatego też kluczowe znaczenie ma stworzenie silnej ochrony przed zagrożeniami cyberbezpieczeństwa i cyberincydentami, które mogłyby zakłócić naszą zdolność do działania. Przestawione dziś rozporządzenia stanowią istotny etap w dziedzinie cyberbezpieczeństwa i bezpieczeństwa informacji w UE. Opierają się one na zacieśnionej współpracy i wzajemnym wsparciu między instytucjami, organami, urzędami i agencjami UE oraz na skoordynowanej gotowości i skoordynowanym reagowaniu. Jest to prawdziwe wspólne przedsięwzięcie UE.*

W kontekście pandemii COVID-19 i coraz poważniejszych wyzwań geopolitycznych wspólne podejście do cyberbezpieczeństwa i bezpieczeństwa informacji jest koniecznością. W związku z tym Komisja zaproponowała rozporządzenie w sprawie cyberbezpieczeństwa i rozporządzenie w sprawie bezpieczeństwa informacji. Dzięki ustanowieniu wspólnych priorytetów i ram, przepisy te przyczynią się do dodatkowego wzmocnienia współpracy międzyinstytucjonalnej, zminimalizowania narażenia na ryzyko i podniesienia poziomu kultury bezpieczeństwa UE.

Rozporządzenie w sprawie cyberbezpieczeństwa

Proponowane rozporządzenie w sprawie cyberbezpieczeństwa wprowadzi **ramy nadzoru, zarządzania ryzykiem i kontroli** w dziedzinie cyberbezpieczeństwa. Doprowadzi to do utworzenia nowej **Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa**, zwiększenia zdolności w zakresie cyberbezpieczeństwa oraz stymulowania regularnych ocen dojrzałości i lepszej higieny cyberbezpieczeństwa. Zostanie również rozszerzony mandat **zespołu reagowania na incydenty komputerowe** dla instytucji, organów, urzędów i agencji UE (CERT-UE) jako punktu analizy cyberzagrożeń, wymiany informacji i koordynacji reagowania na incydenty, centralnego organu doradczego i dostawcy usług.

Kluczowe elementy wniosku dotyczącego rozporządzenia w sprawie cyberbezpieczeństwa:

- wzmocnienie mandatu CERT-UE i zapewnienie potrzebnych zasobów do wykonywania jego mandatu;
- zobowiązanie wszystkich instytucji, organów, urzędów i agencji UE do:
  - posiadania ram nadzoru, zarządzania ryzykiem i kontroli w dziedzinie cyberbezpieczeństwa;
  - wdrożenia podstawowych środków w zakresie cyberbezpieczeństwa odnoszących się do zidentyfikowanych zagrożeń;
  - przeprowadzania regularnych ocen dojrzałości;
  - posiadania planu poprawy cyberbezpieczeństwa zatwierdzonego przez kierownictwo danego podmiotu;
  - wymiany informacji dotyczących incydentów z CERT-UE bez zbędnej zwłok;
- ustanowienie nowej Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa w celu stymulowania i monitorowania wykonania rozporządzenia oraz kierowania CERT-UE;
- zmiany nazwy CERT-UE z „zespołu reagowania na incydenty komputerowe” na „centrum ds.

cyberbezpieczeństwa", zgodnie z rozwojem sytuacji w państwach członkowskich i na całym świecie, przy zachowaniu skróconej nazwy „CERT-UE" na potrzeby jej rozpoznawalności.

Rozporządzenie w sprawie bezpieczeństwa informacji

Proponowane rozporządzenie w sprawie bezpieczeństwa informacji stworzy minimalny zestaw **zasad i norm bezpieczeństwa informacji** dla wszystkich instytucji, organów, urzędów i agencji UE, aby zapewnić lepszą i spójną ochronę przed stopniowo zmieniającymi się zagrożeniami dla ich informacji. Te nowe przepisy zapewnią stabilne podstawy **bezpiecznej wymiany informacji** w ramach instytucji, organów, urzędów i agencji UE oraz państw członkowskich w oparciu o znormalizowane praktyki i środki ochrony przepływu informacji.

Kluczowe elementy wniosku dotyczącego rozporządzenia w sprawie bezpieczeństwa informacji:

- wprowadzenie skutecznego monitorowania w celu wspierania współpracy między wszystkimi instytucjami, organami, urzędami i agencjami UE, a mianowicie międzyinstytucjonalnej grupy koordynacyjnej ds. bezpieczeństwa informacji;
- ustanowienie wspólnego podejścia do kategoryzacji informacji w oparciu o poziom poufności;
- modernizacja polityki bezpieczeństwa informacji, z pełnym uwzględnieniem transformacji cyfrowej i pracy zdalnej;
- usprawnienie obecnych praktyk i osiągnięcie większej kompatybilności między odpowiednimi systemami i urządzeniami.

Kontekst

W rezolucji z marca 2021 r. Rada Unii Europejskiej podkreśliła znaczenie solidnych i spójnych ram bezpieczeństwa dla ochrony całego personelu, danych, sieci komunikacyjnych, systemów informacyjnych i procesów decyzyjnych UE. Można to osiągnąć jedynie poprzez zwiększenie odporności i podniesienie poziomu kultury bezpieczeństwa instytucji, organów, urzędów i agencji UE.

W następstwie strategii UE w zakresie unii bezpieczeństwa oraz strategii UE w zakresie cyberbezpieczeństwa rozporządzenie w sprawie cyberbezpieczeństwa zapewni spójność z obecną polityką UE w dziedzinie cyberbezpieczeństwa przy pełnej zgodności z obowiązującym ustawodawstwem unijnym:

- dyrektywą w sprawie bezpieczeństwa sieci i informacji (NIS) oraz przyszłą dyrektywą w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (NIS 2), którą Komisja zaproponowała w grudniu 2020 r.;
- aktem o cyberbezpieczeństwie;
- zaleceniem Komisji w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni;
- zaleceniem Komisji w sprawie skoordynowanego reagowania na szczeblu unijnym na incydenty i kryzysy cybernetyczne na dużą skalę.

Biorąc pod uwagę stale rosnące ilości szczególnie chronionych informacji jawnych i informacji niejawnych UE przetwarzanych przez instytucje, organy, urzędy i agencje UE, proponowane rozporządzenie w sprawie bezpieczeństwa informacji ma na celu wzmocnienie ochrony informacji poprzez usprawnienie różnych ram prawnych instytucji, organów, urzędów i agencji Unii w tej dziedzinie. Wniosek jest zgodny:

- ze strategią UE w zakresie unii bezpieczeństwa, która obejmuje kompleksowe zobowiązanie UE do uzupełnienia wysiłków państw członkowskich we wszystkich obszarach bezpieczeństwa;
- z głównym elementem Programu strategicznego na lata 2019–2024, przyjętego przez Radę Europejską w czerwcu 2019 r., którym jest ochrona naszych społeczeństw przed stale zmieniającymi się zagrożeniami, na jakie narażone są informacje przetwarzane przez instytucje, organy i agencje;
- z konkluzjami Rady do Spraw Ogólnych z grudnia 2019 r., w których wezwano instytucje, organy, urzędy i agencje UE, przy wsparciu państw członkowskich, do opracowania i wdrożenia kompleksowego zestawu środków w celu zapewnienia ich bezpieczeństwa.

Dodatkowe informacje

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii

Kontakty z mediami:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

Zapytania od obywateli: Serwis Europe Direct – tel. [00 800 67 89 10 11] lub e-mail