Akt o cybersolidarności

W kwietniu 2023 r. Komisja Europejska zaproponowała rozporządzenie mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty („akt w sprawie cybersolidarności"). Podczas drugiej kwietniowej sesji plenarnej Parlament ma głosować w sprawie porozumienia osiągniętego w wyniku negocjacji z Radą.

Kontekst

Wojna Rosji przeciwko Ukrainie ujawniła skalę naszej zależności od technologii cyfrowej i niestabilność przestrzeni cyfrowej. Wywołała ona gwałtowny wzrost cyberataków, które są szczególnie destrukcyjne, gdy są wymierzone w infrastrukturę krytyczną – taką jak energia, zdrowie lub finanse – w coraz większym stopniu uzależnioną od technologii, co sprawia, że jest ona bardziej wydajna, ale również bardziej podatna na zakłócenia cybernetyczne. W tym kontekście Komisja zaproponowała rozporządzenie dotyczące aktu w sprawie cybersolidarności, które ma być odpowiedzią na pilną potrzebę zwiększenia solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty. Dzięki zmianie rozporządzenia ustanawiającego program „Cyfrowa Europa" zapewniono by finansowanie utworzenia systemu ostrzeżeń dotyczących cyberbezpieczeństwa („tarcza cyberbezpieczeństwa") oraz mechanizmu cyberkryzysowego wspierającego działania w zakresie gotowości, w tym rezerwy cyberbezpieczeństwa.

Stanowisko Parlamentu Europejskiego

W grudniu 2023 r. Komisja Przemysłu, Badań Naukowych i Energii (ITRE) Parlamentu przyjęła swoje sprawozdanie, a także mandat upoważniający do podjęcia negocjacji międzyinstytucjonalnych. Również Rada uzgodniła swoje stanowisko w grudniu 2023 r. Współprawodawcy osiągnęli porozumienie polityczne w sprawie tekstu w marcu 2024 r. Uzgodniony tekst zachowuje elementy pierwotnego wniosku Komisji, jednocześnie wyjaśniając i rozszerzając niektóre definicje oraz dostosowując przepisy do obowiązującego prawodawstwa, a mianowicie do dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS2), aby uniknąć powielania działań. Rozporządzenie opierałoby się zatem na trzech filarach:

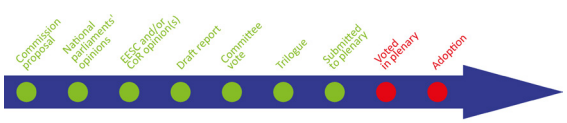
- ogólnoeuropejskim **systemie ostrzeżeń dotyczących cyberbezpieczeństwa**, składającym się z infrastruktury sieciowej „**centrów ds. cyberbezpieczeństwa**", zarówno **krajowych** (pojedynczych podmiotów ustanowionych przez państwo członkowskie i działających z jego upoważnienia, które mogą współpracować z podmiotami sektora prywatnego), jak i **transgranicznych** (konsorcjum przyjmujące składające się z co najmniej trzech uczestniczących państw członkowskich), które będą wymieniały się informacjami na temat cyberincydentów w celu wzmocnienia wspólnej odporności;
- **mechanizmie cyberkryzysowym**, obejmującym **rezerwę cyberbezpieczeństwa** – grupę przedsiębiorstw prywatnych (w tym podmiotów spoza UE) oferujących wsparcie państwom członkowskim (i niektórym państwom trzecim) na ich wniosek, aby wspomagać je w przypadku poważnego cyberincydentu lub cyberincydentu na dużą skalę;
- **mechanizmie przeglądu incydentów w cyberbezpieczeństwie**, za pomocą którego Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), na wniosek Komisji lub sieci organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU-CyCLONe), dokonuje przeglądu i ocenia zagrożenia, znane i możliwe do wykorzystania podatności oraz działania łagodzące związane z poważnymi incydentami lub incydentami na dużą skalę, przedstawiając sprawozdanie z przeglądu incydentów obejmujące zdobyte doświadczenia.

Parlament zapewnił dodanie do celów szczegółowych wniosku rozwój umiejętności, zdolności i kompetencji siły roboczej oraz zwiększenie roli i zasobów ENISA, w szczególności w odniesieniu do unijnej

Autorka: Polona Car, Dyrekcja ds. Analiz dla Posłów
PE 760.431 – kwiecień 2024 r.

rezerwy cyberbezpieczeństwa. Parlament zadbał również o to, by fundusze przeznaczone na rezerwę cyberbezpieczeństwa nie zagrażały innym celom programu „Cyfrowa Europa", takim jak umiejętności cyfrowe i sztuczna inteligencja.

Sprawozdanie w pierwszym czytaniu: 2023/0109(COD); komisja przedmiotowo właściwa: ITRE; sprawozdawczyni: Lina Gálvez Muñoz (S&D, Hiszpania). Więcej informacji w briefingu z serii „Opracowywanie prawa UE".



Wyniki końcowe Konferencji w sprawie przyszłości Europy: omawiany wniosek dotyczy środków 28(1), (2); 33(3).