ENISA i nowy unijny akt w sprawie cyberbezpieczeństwa

Komisja Europejska zaproponowała wniosek, którego celem jest zwiększenie odporności UE i usprawnienie reakcji na cyberataki przez przyznanie stałego mandatu i zwiększenie roli Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) będącej unijną agencją odpowiedzialną za kwestie cyberbezpieczeństwa. We wniosku przewidziano stworzenie pierwszych unijnych ram certyfikacji cyberbezpieczeństwa produktów i usług ICT, w czym ENISA będzie także odgrywać ważną rolę. W dniu 10 lipca 2018 r. Komisja Przemysłu, Badań Naukowych i Energii (ITRE) Parlamentu Europejskiego przyjęła swoje sprawozdanie, a także mandat upoważniający do podjęcia negocjacji międzyinstytucjonalnych. Rada przyjęła swój mandat w dniu 8 czerwca 2018 r. Podczas piątej tury rozmów trójstronnych w dniu 10 grudnia 2018 r. osiągnięto porozumienie. Parlament ma głosować nad nim na posiedzeniu plenarnym w marcu.

Kontekst

Liczba i różnorodność zagrożeń dla cyberbezpieczeństwa szybko wzrasta i prawdopodobnie nadal będzie rosnąć, biorąc pod uwagę rozwój urządzeń podłączonych do sieci. Oczekuje się, że w następstwie przyjęcia dyrektywy w sprawie bezpieczeństwa sieci i informacji w 2016 r., która jest pierwszym unijnym prawodawstwem w dziedzinie cyberbezpieczeństwa, ENISA będzie odgrywać większą rolę w obszarze cyberbezpieczeństwa UE, ale jej działalność jest ograniczona w związku z końcem jej mandatu w czerwcu 2020 r. i ograniczonymi zasobami.

Wniosek Komisji Europejskiej

We wniosku ustawodawczym Komisji przewiduje się zwiększenie budżetu oraz liczby pracowników i ustanowienie stałego mandatu ENISA, a także zwiększenie roli polegającej nie tylko na doradztwie fachowym, ale także na realizacji zadań operacyjnych i koordynacyjnych. Wniosek obejmuje również propozycję stworzenia pierwszych dobrowolnych unijnych ram certyfikacji cyberbezpieczeństwa produktów ICT. Certyfikacja bezpieczeństwa ICT jest ważna dla zwiększania zaufania konsumentów i przedsiębiorstw oraz stworzenia prawdziwie jednolitego rynku cyfrowego. Obecnie w UE istnieje jedynie ograniczona liczba systemów certyfikacji bezpieczeństwa, a niektóre z nich obowiązują wyłącznie na terytorium poszczególnych państw, co prowadzi do fragmentacji i wzrostu kosztów dla przedsiębiorstw.

Stanowisko Parlamentu Europejskiego

Komisja ITRE głosowała nad sprawozdaniem w dniu 10 lipca 2018 r., a jej mandat do negocjacji trójstronnych został zatwierdzony przez Parlament podczas sesji plenarnej we wrześniu 2018 r. Komisja poparła proponowany obszerniej zdefiniowany stały mandat ENISA oraz stworzenie dobrowolnych unijnych ram cyberbezpieczeństwa produktów, usług i procesów ICT, wskazując, że mogłyby one w przyszłości stać się obowiązkowe w niektórych obszarach. Rada przyjęła swoje stanowisko 8 czerwca 2018 r. Podczas piątej tury rozmów trójstronnych w dniu 10 grudnia 2018 r. osiągnięto porozumienie w sprawie tekstu. Przewiduje się w nim przydzielenie ENISA nowych zadań i dodatkowych zasobów, a tym samym rozszerzenie jej roli w celu poprawy koordynacji i wymiany najlepszych praktyk między państwami członkowskimi w dziedzinie edukacji dotyczącej cyberbezpieczeństwa, a także zwiększania świadomości obywateli i przedsiębiorstw w zakresie higieny cyberbezpieczeństwa. ENISA ma również organizować dwa razy w roku ćwiczenia symulacyjne w dziedzinie cyberbezpieczeństwa, aby zwiększyć odporność Unii i jej skoordynowaną reakcję na ataki, a także przedstawiać sprawozdanie na temat stanu cyberbezpieczeństwa. W odniesieniu do aktu w sprawie cyberbezpieczeństwa w porozumieniu podkreśla się, że ENISA we współpracy z państwami członkowskimi i odpowiednimi zainteresowanymi stronami musi odgrywać większą rolę w ustanawianiu europejskich systemów cyberbezpieczeństwa. W tekście wzmocniono wagę konsultacji z zainteresowanymi stronami oraz rolę branży. Przewidziano w nim również utworzenie

Autor: Mar Negreiro, Dyrekcja ds. Analiz dla Posłów
PE 625.160 – marzec 2019 r.

Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa złożonej z przedstawicieli krajowych organów ds. certyfikacji cyberbezpieczeństwa w celu kontrolowania jej wdrażania. Państwa członkowskie nie powinny utrzymywać w mocy lub wprowadzać nowych krajowych systemów certyfikacji cyberbezpieczeństwa, z wyjątkiem względów bezpieczeństwa narodowego.

Sprawozdanie w pierwszym czytaniu: 2017/0225(COD); Komisja przedmiotowo właściwa: ITRE; Sprawozdawczyni: Angelika Niebler (PPE, Niemcy). Więcej informacji można znaleźć w nocie informacyjnej z serii „EU Legislation in Progress" [Opracowywanie prawa UE].