PARLAMENT EUROPEJSKI PODPISAŁ DYREKTYWĘ NIS

Dyrektywa dotycząca bezpieczeństwa sieci i informacji (NIS) poprawi funkcjonowanie firm na rynkach europejskich. Będą one działały na takich samych zasadach w każdym państwie Unii Europejskiej. Nowe przepisy przewidują strategiczne "grupy współpracy" w celu wymiany informacji i wspierania państw członkowskich w budowaniu potencjału bezpieczeństwa sieci i systemów informatycznych. Państwa członkowskie będą miały 21 miesięcy na transpozycję dyrektywy do prawa krajowego od momentu wpisania jej do Dziennika Urzędowego UE.

Jak informuje UE, Parlament przyjął w środę dyrektywę, która nakłada na firmy świadczące podstawowe usługi internetowe nowe wymagania odnośnie wytrzymałości ich systemów na ataki hakerów. Chodzi o takie dziedziny jak energia, transport, bankowość i ochrona zdrowia oraz usługi cyfrowe (wyszukiwarki, przechowywanie danych w chmurze). Ustanowienie wspólnych standardów cyberbezpieczeństwa oraz poprawa współpracy między krajami Unii pomoże przedsiębiorstwom skuteczniej stawiać czoła hakerom, a także pomóc w zapobieganiu atakom na infrastrukturę cyfrową, której sieć pokrywa wiele krajów lub całą UE, uważają posłowie.

"Incydenty w zakresie bezpieczeństwa komputerowego bardzo często mają charakter transgraniczny, a zatem dotyczą więcej niż jednego państwa członkowskiego UE. Fragmentaryczna ochrona bezpieczeństwa wystawia nas na coraz większe zagrożenie, w całej Europie. Ta dyrektywa ustanawia wspólny poziom bezpieczeństwa sieci i informacji i wzmacnia współpracę między państwami członkowskimi UE, która pomoże zapobiegać w przyszłości cyberatakom na ważne, wzajemnie ze sobą powiązane europejskie systemy" - powiedział poseł sprawozdawca Andreas Schwab.

Unijna dyrektywa dotycząca bezpieczeństwa sieci i informacji (NIS) "jako jedna z pierwszych tworzy ramy prawne, które mają zastosowanie do platform usługowych. Zgodnie ze strategią jednolitego rynku cyfrowego, ustanawia zharmonizowane wymagania dotyczące platform i gwarantuje im, że wszędzie w UE mogą oczekiwać podobnych zasad, gdziekolwiek działają. To ogromny sukces i wielki pierwszy krok w stronę ustanowienia całościowych ram prawnych regulujących funkcjonowanie platform w UE " - dodał Schwab. Nowe unijne przepisy na "operatorów usług kluczowych" obowiązki w zakresie zapewnienia poziomu bezpieczeństwa i zgłaszania incydentów. Dotyczy to takich sektorów jak energetyka, transport, ochrona zdrowia, bankowość i zaopatrzenie w wodę pitną. Państwa członkowskie UE będą miały obowiązek zidentyfikować działające w tych dziedzinach podmioty kierując się określonymi w dyrektywie kryteriami. Na liście znajdą się na przykład podmioty świadczące usługi, która mają kluczowe znaczenie dla "utrzymania krytycznej działalności społecznej lub gospodarczej", a incydenty w dziedzinie bezpieczeństwo sieci miałby "istotny skutek zakłócający świadczenia tej usługi".

Niektórzy usługodawcy internetowi, choć nieuznani za "kluczowych" (operatorzy platform handlowych, wyszukiwarek i usług w chmurze) też będą zobowiązani, choć w mniejszym stopniu, do zapewnienia bezpieczeństwa swojej infrastruktury i zgłaszania poważnych incydentów organom krajowym. Firmy z

sektora MŚP będą zwolnione z tych wymogów. Nowe przepisy przewidują strategiczne "grupy współpracy" w celu wymiany informacji i wspierania państw członkowskich w budowaniu potencjału bezpieczeństwa sieci i systemów informatycznych. Każdy kraj UE będzie zobowiązany do przyjęcia krajowej strategii NIS.

Państwa członkowskie będą musiały utworzyć Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). W ramach Zespołów omawiane będą transgraniczne problemy bezpieczeństwa i sposoby skoordynowanej reakcji na nie. Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) będzie odgrywać kluczową rolę we wdrażaniu dyrektywy, w szczególności w zakresie koordynowania współpracy między państwami w ramach sieci CSIRT. Dyrektywa NIS wkrótce zostanie opublikowana w Dzienniku Urzędowym UE i wejdzie w życie dwudziestego dnia po opublikowaniu. Począwszy od tego momentu państwa członkowskie będą miały 21 miesięcy na transpozycję dyrektywy do prawa krajowego i dodatkowe sześć miesięcy na opracowanie spisu operatorów usług kluczowych.

Czytaj też: Otwarcie Narodowego Centrum Cyberbezpieczeństwa