Dyrektywa, która ma poprawić cyberbezpieczeństwo w UE

Parlament Europejski przyjął w ubiegłym tygodniu dyrektywę NIS (Network and Information Security), która ma na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii Europejskiej. Ma ona skutkować wdrożeniem nie tylko wspólnych standardów ochrony świadczonych w Europie usług, ale także wypracowaaniem zasad wymiany informacji o zagrożeniach pomiędzy państwami. To oznacza też koszty dla sektora prywatnego.

W zamyśle ustanowienie wspólnych standardów cyberbezpieczeństwa oraz poprawa współpracy między krajami UE ma pomóc przedsiębiorstwom skuteczniej stawiać czoła hakerom, a także pomóc w zapobieganiu atakom na infrastrukturę cyfrową.

Prace na tym dokumentem trwały ponad trzy lata, tj. dłużej niż standardowo pracuje się w UE nad podobnymi dokumentami, gdzie trwa to zazwyczaj dwa lata. To pokazuje, że poruszane w dyrektywie kwestie nie są łatwe. Dyrektywę nakłada na firmy świadczące podstawowe usługi internetowe nowe wymagania odnośnie wytrzymałości ich systemów na ataki hakerów. Chodzi m.in. o takie dziedziny jak energia, transport, bankowość i ochrona zdrowia oraz usługi cyfrowe (wyszukiwarki, przechowywanie danych w chmurze).

Mirosław Maj, prezes Fundacji Bezpieczna Cyberprzestrzeń, kilka miesięcy temu podczas konferencji PLNOG mówił, że w Polsce szczególnie trudna implementacja dyrektywy może się okazać w sektorze medycznym. To jest bowiem dziś obszar bardzo zaniedbany pod względem cyberbezpieczeństwa.

Zgodnie z dyrektywą państwa członkowskie przygotują listy tzw. operatorów usług kluczowych, na których będą ciążyć obowiązki w zakresie zapewnienia poziomu bezpieczeństwa i zgłaszania cyberincydentów. Dotyczy to takich sektorów jak energetyka, transport, ochrona zdrowia, bankowość i zaopatrzenie w wodę pitną.

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. Mikro- i małe przedsiębiorstwa cyfrowe będą zwolnione z tych wymogów.

Nowe przepisy przewidują też powołanie tzw. strategicznych grup 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.

Przepisy przewidują również powołanie grupy współpracy (składającej się z przedstawicieli państw członkowskich) oraz sieci krajowych CSIRTów, tj. Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego, wspomaganej przez ENISA (Europejską Agencję Bezpieczeństwa Sieci i Informacji). W Polsce rolę CSIRT-u krajowego najprawdopodobniej będzie pełnić NASK.

Według Mirosława Maja najwięcej czasu we wdrażaniu dyrektywy NIS będzie wymagać nawiązanie efektywnej współpracy między CSIRT-em krajowym a sektorem prywatnym. Konieczne tu będzie m.in. wypracowanie procedur postępowania w przypadku cyberincydentów czy określenie formatów wymiany informacji.

Joanna Świątkowska, ekspert Instytutu Kościuszki zwraca natomiast uwagę, że dyrektywa jest dokumentem ogólnym i to od tego, jak rzetelnie będzie wdrażana na poziomie krajowym, zależeć będzie efekt końcowy. Podkreśla, że diabeł tkwi w szczegółach. Kluczowe będzie między innymi to, jak dobrze uda się zaprojektować

system wyznaczania operatorów, którzy poddani zostaną regulacjom. Istotne też będzie, jak wyglądać będą środki bezpieczeństwa, które będą musieli oni wdrażać, jaki będzie proces nadzoru i kontroli. A w końcu, jak określone zostaną szczegóły choćby tego, które incydenty powinno się raportować.

W tym kontekście trzeba też pamiętać, że w Ministerstwie Cyfryzacji trwają zaawansowane prace nad projektem strategii cyberbezpieczeństwa dla RP oraz nad ustawą o krajowym systemie cyberbezpieczeństwa. Zarówno strategia jak ustawa będą uwzględniać wymagania nałożone przez NIS.

Wdrażanie dyrektywy NIS oczywiście będzie kosztować. Na razie nie wiadomo jeszcze, jakie będą to kwoty, ale sektor prywatny będzie musiał ponieść pewne koszty. Według Mirosława Maja same zachęty, że warto stawiać na cyberbezpieczeństwo, mogą tu być niewystarczające - Dobrym pomysłem byłyby ulgi podatkowe - mówił prezes Fundacji Bezpieczna Cyberprzestrzeń podczas konferencji PLNOG.

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.

Marek Jaślan

Zdjęcie: Photogenica