Nowe przepisy o cyberbezpieczeństwie coraz bliżej – dyrektywa NIS2 zmienia zasady gry

Kategoria: Aktualności
Opublikowano: środa, 14, maj 2025 13:00
Ewelina Kocemba

Według zapewnień rządu w tym kwartale zakończą się rządowe prace nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, która wdroży do polskiego prawa zapisy dyrektywy NIS2. Będzie to mieć istotne znaczenie dla kształtowania polityk cyberbezpieczeństwa przez duże i średnie podmioty zaliczane do kategorii kluczowych i ważnych. Choć pojawiają się głosy krytyczne, sugerujące, że regulacje są zbyt daleko idące, to eksperci od cyberbezpieczeństwa są przekonani, że akurat w tym obszarze mogą one przynieść szereg korzyści, zwłaszcza we współczesnych warunkach geopolitycznych.

„Barometr Cyberbezpieczeństwa 2025" KPMG wskazuje, że w 2024 roku 83 proc. firm w Polsce odnotowało przynajmniej jeden incydent związany z cyberbezpieczeństwem. To o 16 pp. więcej niż w poprzednim badaniu. Ponad połowa przedstawicieli badanych firm uważa, że technologia AI spowoduje wzrost zagrożeń w cyberprzestrzeni.

– Dyrektywa NIS jest jedną z kluczowych regulacji Unii Europejskiej, która ma za zadanie podnieść poziom cyberbezpieczeństwa na wielu poziomach. Ona będzie wpływała na funkcjonowanie konkretnych przedsiębiorstw, szczególnie z sektorów infrastruktury krytycznej, ale jest także dyrektywą, która niejako wprowadza konieczność wdrożenia systemowych rozwiązań na poziomie krajów członkowskich, jak również wprowadza pewne mechanizmy koordynacji i współpracy pomiędzy krajami Unii Europejskiej. Jest więc w opiniach wielu specjalistów jedną z fundamentalnych regulacji, która wpływa na podniesienie poziomu cyberbezpieczeństwa w Unii Europejskiej – mówi Joanna Świątkowska, zastępczyni sekretarza generalnego Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO).

Unijna dyrektywa weszła w życie w 2023 roku. Jesienią ubiegłego roku minął termin na wprowadzenie jej założeń do prawa krajowego w państwach członkowskich. W Polsce jednak trwają prace nad ustawą o krajowym systemie cyberbezpieczeństwa, która ma stanowić implementację dyrektywy. Ze względu na istotę przepisów i ich zakres projekt na etapie prac rządowych był już wielokrotnie modyfikowany. Według zapowiedzi resortu cyfryzacji, które padły podczas Europejskiego Kongresu Gospodarczego, rządowy etap prac nad nowym projektem ma się zakończyć jeszcze w II kwartale br. Nowe przepisy obejmą ok. 38 tys. podmiotów w Polsce.

W NIS2 nastąpiła zmiana dotychczasowego podziału na operatorów usług kluczowych, dostawców usług cyfrowych oraz podmioty publiczne. W miejsce tego pojawił się podział na podmioty ważne oraz podmioty kluczowe. Jako podmioty kluczowe wskazane zostały organizacje o krytycznym znaczeniu dla funkcjonowania gospodarki i społeczeństwa, czyli podmioty z najważniejszych sektorów gospodarki, takich jak m.in. sektor energetyczny, finansowy, ochrona zdrowia czy infrastruktura cyfrowa. Do podmiotów ważnych zaliczono m.in. dostawców usług telekomunikacyjnych, sektor pocztowy i kurierski czy podmioty przetwarzające odpady. Podmioty objęte dyrektywą mają wdrożyć odpowiednie środki mające zmniejszyć ryzyko dla bezpieczeństwa sieci i systemów informatycznych, uwzględniające wszelkie możliwe zagrożenia.

– Jednym z takich wymagań jest zwrócenie uwagi na ryzyka, które płyną z funkcjonowania łańcucha dostaw. Wyobraźmy sobie, że infrastruktura krytyczna w różnych sektorach, powiedzmy szpital czy elektrownia lub sektor telekomunikacyjny, w ramach realizowania swoich działań korzysta z wielu partnerów biznesowych, dostawców, ale i on sam dostarcza rozwiązania oczywiście dla swoich klientów. W ramach tego skomplikowanego łańcucha zależności mogą się pojawić pewne ryzyka wynikające ze współdziałania i współzależności, właśnie również na poziomie cyfrowym, które trzeba zaopiekować poprzez wprowadzenie całego systemu zarządzania tymi ryzykami. Dyrektywa NIS w sposób bardzo konkretny i po raz pierwszy zwraca uwagę i wymaga, że cyberbezpieczeństwo łańcucha dostaw powinno

się stać jednym z elementów, które poszczególne organizacje muszą wziąć pod uwagę i wdrożyć – wskazuje Joanna Świątkowska.

Jak wynika z raportu KPMG, badane firmy nie uważają ataków na łańcuch dostaw za pośrednictwem partnerów biznesowych za duże zagrożenie. Uznaje je za takie tylko 5 proc. przedsiębiorstw, ale to i tak pięciokrotny wzrost w porównaniu z poprzednim rokiem. Z kolei odsetek 20 proc. firm, które oceniły, że takie ryzyko nie istnieje, to spadek aż o 18 pp. w porównaniu z wcześniejszą edycją badania. Być może nowe regulacje (jak NIS2) kładące nacisk na ochronę przed tymi zagrożeniami podniosły poziom świadomości polskich przedsiębiorstw w tym zakresie.

Przepisami dyrektywy NIS2 objęte zostały duże i średnie firm. Jako podmioty kluczowe kwalifikują się takie, które zatrudniają co najmniej 250 pracowników, a ich roczny obrót przekracza 50 mln euro. Do podmiotów ważnych zalicza się średnie przedsiębiorstwa, czyli podmioty zatrudniające co najmniej 50 pracowników, o rocznym obrocie powyżej 10 mln euro. Podmioty objęte regulacjami mają szereg obowiązków, takich jak m.in. przeprowadzanie regularnych ocen ryzyka, wdrażanie zaawansowanych środków ochronnych czy zgłaszanie do CERT incydentów bezpieczeństwa. Do stosowania nowej dyrektywy będą zobowiązane również mikroprzedsiębiorstwa i małe przedsiębiorstwa, które spełnią kryteria wskazujące na ich kluczową rolę dla społeczeństwa, gospodarki, określonych sektorów lub typów usług. Będą to np. kwalifikowani dostawcy usług zaufania, dostawcy usług DNS czy rejestry nazw domen najwyższego poziomu.

– *Kluczem do sukcesu jest nie tylko wprowadzenie i zaprojektowanie właściwych rozwiązań, ale przede wszystkim ich skuteczna implementacja. Na poziomie Unii Europejskiej w tym momencie toczy się bardzo burzliwa dyskusja á propos potencjalnych deregulacji i potencjalnego zastanowienia się, czy faktycznie Unia Europejska nie idzie za daleko w wymaganiach, które wprowadza za pomocą różnych polityk* – zauważa ekspertka ECSO. – *Akurat sektor cyberbezpieczeństwa jest tym, gdzie regulacje wnoszą wiele dobrego, rzeczywiście przekładają się bardzo często na wzrost świadomości, większe inwestycje i większe zaangażowanie.*

Jak podkreśla, w kontekście uproszczeń można rozważać nie samą regulację, ale sposób jej wprowadzania.

– *Inna sprawa jest taka, czy faktycznie te regulacje nie mogłyby być wprowadzane w sposób nieco bardziej przyjazny dla użytkowników końcowych. I tutaj faktycznie ta debata w chwili obecnej się odbywa, między innymi za sprawą prezydencji Polski, która wprowadziła ją bardzo wysoko na agendę polityczną. W kontekście dyrektywy NIS w chwili obecnej toczy się dyskusja, jak wdrożyć ją na przestrzeni całej Unii Europejskiej w sposób zharmonizowany, w sposób skoordynowany, aby faktycznie nie piętrzyć trudności, ale wprowadzić ją w sposób efektywny* – dodaje Joanna Świątkowska.

Niewątpliwie dyrektywa jest odpowiedzią na zwiększone zagrożenie Europy na płaszczyźnie związanej z cyberbezpieczeństwem. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w raporcie opublikowanym w październiku 2024 roku wskazała, że w 2023 roku zanotowała ponad 11 tys. incydentów, z czego 322 były wymierzone w co najmniej dwa państwa unijne. Stwierdzono również prawie 20 tys. luk bezpieczeństwa, z czego ponad 9 proc. dotyczyło kategorii kluczowej, a prawie 22 proc. – ważnej.

Źródło: IP