Czy Twoja firma jest gotowa? Odpowiedzialność zarządu w świetle NIS 2

Damaris Jeż

W dobie postępującej cyfryzacji przemysł – niezależnie od sektora – staje przed nowymi wyzwaniami związanymi z cyberbezpieczeństwem. Choć Dyrektywa NIS 2 (*Network and Information Security*) została przyjęta przez Unię Europejską i wymaga implementacji na poziomie krajowym, ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC), która ma ją wdrożyć, nadal nie została uchwalona. W środowisku ekspertów nie brakuje głosów, że uchwalenie ustawy w 2025 roku może się nie wydarzyć.

Dla wielu przedsiębiorstw jest to dobra wiadomość. Otrzymują dodatkowy czas na dostosowanie się do nowych regulacji, w tym na: ocenę ryzyka, wzmocnienie bezpieczeństwa systemów informatycznych, a także uporządkowanie ról i odpowiedzialności w organizacji.

Znaczenie cyberbezpieczeństwa w przemyśle

W ostatnich latach obserwujemy wzrost liczby ataków ukierunkowanych na systemy przemysłowe. Jak donosił Reuters[1] w październiku 2024 roku celem działań o charakterze zarówno cybernetycznym, jak i fizycznym stała się fińska spółka energetyczna Fortum. Wśród zidentyfikowanych incydentów znalazły się próby ataków na infrastrukturę IT i OT oraz działania rozpoznawcze prowadzone przez drony. Ataki miały miejsce w kontekście napięć geopolitycznych i były szeroko komentowane przez media jako przykład zagrożenia dla infrastruktury krytycznej.

Zagrożenia dotyczą również sektora spożywczego, który często nie dysponuje równie rozbudowanymi strukturami ochrony jak energetyka. Wraz ze wzrostem automatyzacji produkcji i procesów okołoprodukcyjnych podatność środowiska przemysłowego na ataki cybernetyczne rośnie.

Dyrektywa NIS 2 i jej wpływ na sektor przemysłowy

NIS 2 zakłada istotne rozszerzenie katalogu podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa. Katalog podmiotów, o których mówi Dyrektywa obejmuje 18 sektorów. Uwagę na liście zwracają przede wszystkie sektory takie jak np. produkcja żywności, gospodarowanie odpadami, które do tej pory nie były uznawane za kluczowe gałęzie gospodarki jeśli chodzi o cyberbezpieczeństwo. Przedsiębiorstwa przemysłowe mogą zostać sklasyfikowane jako podmioty kluczowe lub ważne – w zależności od wielkości, sektora i znaczenia dla łańcuchów dostaw.

Obowiązek samoidentyfikacji i rejestracji

Zgodnie z projektem nowelizacji KSC, implementującym Dyrektywę NIS 2, **podmioty kluczowe i ważne** będą zobowiązane do samodzielnego zgłoszenia się do wykazu prowadzonego przez ministra właściwego ds. informatyzacji poprzez rejestrację w systemie S46. System ten pełni rolę centralnej platformy do zgłaszania incydentów oraz wymiany informacji o zagrożeniach cybernetycznych. Termin wejścia w życie obowiązku rejestracji zostanie określony w nowelizacji

NIS 2 zakłada istotne rozszerzenie katalogu podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa. Katalog podmiotów, o których mówi dyrektywa obejmuje 18 sektorów. Uwagę na liście zwracają przede wszystkie sektory takie jak np. produkcja żywności, gospodarowanie odpadami, które do tej pory nie były uznawane za kluczowe gałęzie gospodarki jeśli chodzi o cyberbezpieczeństwo.

ustawy o KSC. Po uchwaleniu ustawy, podmioty spełniające kryteria będą miały dwa miesiące na dokonanie rejestracji.

Warto śledzić komunikaty Ministerstwa Cyfryzacji oraz odpowiednich organów, aby być na bieżąco z terminami i szczegółowymi wytycznymi dotyczącymi procesu rejestracji.

Kogo dotyczyć będą przepisy?

W stosunku do obecnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa, katalog sektorów objętych przepisami rozszerzył się. Wynika to bezpośrednio z dyrektywy NIS 2, w której obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę, infrastruktury cyfrowej, znalazły się także sektory: ścieków, zarządzania ICT, przestrzeni kosmicznej, poczty, produkcji, produkcji i dystrybucji chemikaliów, produkcji i dystrybucji żywności.

Sektory[2] zostały podzielone na dwie kategorie:

- Sektory kluczowe: energia, transport, bankowość, infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną, gospodarka ściekowa, infrastruktura cyfrowa, administracja publiczna, przestrzeń kosmiczna.
- Sektory ważne: usługi pocztowe i kurierskie, gospodarka odpadami, produkcja, produkcja i dystrybucja chemikaliów, produkcja i dystrybucja żywności, badania naukowe, dostawcy usług ICT.

Podstawą klasyfikacji będą m.in. liczba pracowników, roczny obrót oraz znaczenie dla funkcjonowania państwa lub stabilności gospodarki.

Czego mogą się spodziewać przedsiębiorstwa?

Obowiązki nałożone na podmioty kluczowe i ważne zgodnie z Dyrektywą NIS 2 obejmują:

1. Zarządzanie ryzykiem – wdrażanie środków technicznych, operacyjnych i organizacyjnych w celu ograniczenia ryzyka związanego z cyberzagrożeniami.
2. Zgłaszanie incydentów – obowiązek zgłaszania poważnych incydentów do CSIRT[3] lub właściwego organu nadzorczego w trzech etapach: zgłoszenie wstępne (do 24 h), szczegółowe (do 72 h) i końcowe (do 1 miesiąca).
3. Utrzymywanie ciągłości działania – przygotowanie i wdrożenie procedur zapewniających ciągłość usług i minimalizację skutków incydentów.
4. Weryfikacja dostawców – obowiązek oceny ryzyka wynikającego z łańcucha dostaw i wdrażania zabezpieczeń przy nabywaniu usług i technologii.
5. Szkolenie i świadomość personelu – obowiązek edukacji i podnoszenia świadomości zagrożeń wśród pracowników.
6. Zarządzanie podatnościami – aktywne monitorowanie podatności (luk w systemach) i reagowanie na ich ujawnienie.
7. Bezpieczeństwo w projektowaniu i nabywaniu systemów (security by design) – uwzględnianie cyberbezpieczeństwa na etapie projektowania oraz przy zakupie systemów i komponentów.
8. Publiczne informowanie o incydentach – w przypadkach, gdy incydent może mieć istotny wpływ na interes publiczny lub usługobiorców.
9. Dokumentacja i raportowanie – prowadzenie i przechowywanie dokumentacji działań z zakresu bezpieczeństwa oraz udostępnianie jej organom nadzorczym.
10. Współpraca z organami nadzoru – przekazywanie informacji i współdziałanie podczas kontroli i audytów.

Odpowiedzialność i sankcje

Projekt przewiduje kary administracyjne:

- do 10 mln EUR lub 2% globalnego obrotu – dla podmiotów kluczowych,
- do 7 mln EUR lub 1,4% globalnego obrotu – dla podmiotów ważnych.

Dodatkowo, członkowie kierownictwa mogą zostać ukarani kwotą sięgającą 600% miesięcznego wynagrodzenia. Osobista odpowiedzialność obejmuje m.in. nadzór nad wdrożeniem obowiązków ustawowych i podejmowanie decyzji mających wpływ na poziom bezpieczeństwa organizacji. To wzmocnienie sankcji o osobistą odpowiedzialność członków zarządu zapewne skłoni wszystkich do potraktowania tej regulacji z dużą uważnością.

Współpraca i wymiana informacji jako fundament odporności

Zbliżające się zmiany prawne wymagają od przemysłu większego zaangażowania sił i środków w obszar cyberbezpieczeństwa. Opóźnienie ustawodawcze to szansa, by nie działać reaktywnie, lecz planowo i świadomie. Warto już teraz nawiązywać relacje z CSIRT, organizacjami branżowymi i innymi uczestnikami rynku. Wymiana informacji o zagrożeniach i dobrych praktykach pomaga wzmacniać gotowość przedsiębiorstwa na cyberataki. Przedsiębiorstwa, które zintensyfikują przygotowania, zyskają nie tylko zgodność z regulacjami, ale też realną odporność operacyjną.

Przypisy

1. https://www.reuters.com/business/energy/finnish-utility-fortums-power-assets-targeted-with-surveillance-cyber-attacks-2024-10-10/
2. https://cyberapolicy.nask.pl/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-zmiany-dla-podmiotow/
3. https://csirt.gov.pl/ □

Damaris Jeż – Audytor Wiodący ISO/IEC 27001