Ostatni dzwonek na rejestrację w Wykazie KSC. Eksperci INEA: firmy wciąż nie wiedzą, że ich to dotyczy

Ponad 42 tysiące polskich firm ma czas tylko do 3 października 2026 roku, by zgłosić się do *Wykazu podmiotów kluczowych i ważnych* - nowego rejestru prowadzonego przez Ministerstwo Cyfryzacji w ramach systemu S46. To efekt wejścia w życie 3 kwietnia 2026 roku nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa, która wdraża do polskiego prawa unijną dyrektywę NIS2. Do tej pory przepisy o KSC obejmowały około 400 podmiotów - głównie operatorów infrastruktury krytycznej. Po nowelizacji krąg objętych obowiązkami firm wzrósł ponad stukrotnie, a wiele z nich wciąż nie wie, że nowe przepisy ich dotyczą.

Czym jest NIS2 i o czym mówi ustawa

Dyrektywa NIS2 (Network and Information Security 2) to unijna regulacja z 2022 roku, której celem jest podniesienie odporności kluczowych sektorów gospodarki na cyberzagrożenia. Polska wdrożyła ją nie nową ustawą, lecz nowelizacją obowiązującej od 2018 roku Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Nowe przepisy weszły w życie 3 kwietnia 2026 roku i objęły firmy działające w osiemnastu sektorach wymienionych w załącznikach do ustawy - m.in. energetyce, transporcie, ochronie zdrowia, gospodarce wodno-ściekowej oraz infrastrukturze cyfrowej i telekomunikacji.

Ustawa dzieli objęte nią podmioty na dwie kategorie: podmioty kluczowe i podmioty ważne. Przynależność do jednej z nich zależy nie tylko od sektora, w którym firma działa, ale też od jej wielkości - liczby zatrudnionych oraz rocznego obrotu lub sumy bilansowej. Co do zasady regulacja obejmuje średnie i duże przedsiębiorstwa, choć w niektórych przypadkach obowiązek dotyczy firmy niezależnie od jej rozmiaru - decyduje wtedy szczególna rola danego podmiotu dla gospodarki lub bezpieczeństwa państwa.

Firmy, które spełniają kryteria ustawy, mają dwa równolegle biegnące terminy. Pierwszy to sześć miesięcy od wejścia przepisów w życie na dokonanie samoidentyfikacji i złożenie wniosku o wpis do Wykazu KSC - to właśnie ten termin upływa 3 października 2026 roku. Drugi to dwanaście miesięcy na wdrożenie pełnego systemu zarządzania bezpieczeństwem informacji, zgodnego z wymogami ustawy.

Maciej Hojszyk: pomagamy firmom ocenić, gdzie właściwie stoją

- Największym problemem, z jakim spotykamy się dziś w rozmowach z klientami biznesowymi, nie jest brak woli działania, tylko brak punktu odniesienia. Firmy nie wiedzą, czy w ogóle podlegają ustawie, a jeśli tak - w jakim stopniu spełniają już stawiane przez nią wymogi - mówi Maciej Hojszyk, Commercial B2B Director w INEA. - Dlatego jako INEA nie zaczynamy od sprzedawania konkretnych rozwiązań, tylko od wspólnej z klientem oceny sytuacji wyjściowej. Sprawdzamy, w jakim sektorze działa firma, jaka jest jej realna skala - bo klasyfikacja pod NIS2 wymaga spojrzenia zarówno na branżę, jak i na zatrudnienie oraz obrót - a dopiero potem układamy z klientem plan dochodzenia do zgodności. To podejście, które oszczędza firmom czasu i pieniędzy, bo pozwala inwestować dokładnie tam, gdzie są realne luki, a nie tam, gdzie wydaje się, że mogą być.

Sylwester Białasiewicz: najczęściej brakuje MFA, monitoringu i planu na wypadek awarii

Z audytów dojrzałości cyberbezpieczeństwa, które INEA przeprowadza dla swoich klientów biznesowych, wyłania się powtarzalny obraz braków. - Widzimy to praktycznie w każdej ocenianej organizacji: dokumentacja systemu zarządzania bezpieczeństwem informacji istnieje częściowo i wymaga gruntownej przebudowy, zarządzanie tożsamością i uprawnieniami jest nieformalne, a wieloskładnikowe uwierzytelnianie w wielu miejscach po prostu nie funkcjonuje - wylicza Sylwester Białasiewicz, Pre-Sales Manager w INEA. - Bardzo często zabezpieczenia sieci, takie jak segmentacja czy VPN, są niewystarczające, a systemy i oprogramowanie działają bez wsparcia producenta, czyli w praktyce po zakończeniu ich cyklu życia. Kopie zapasowe najczęściej nie są sformalizowane w postaci procedury, a funkcja ciągłego monitorowania bezpieczeństwa - czyli SOC - w ogóle nie istnieje. Do tego dochodzi brak lub niepełne plany ciągłości działania i odtwarzania po awarii, nieformalne zarządzanie podatnościami, brak spójnego procesu weryfikacji dostawców i łańcucha dostaw ICT, a także brak zarządzania urządzeniami mobilnymi - w praktyce oznacza to pracę na prywatnym sprzęcie i kontach

niezwiązanych z firmową infrastrukturą. Zabezpieczenia fizyczne bywają wdrożone tylko częściowo, a dokumentacja w tym obszarze jest niepełna.

Ekspert zwraca uwagę, że żaden z tych braków osobno nie dyskwalifikuje firmy z rynku, ale ich suma pokazuje skalę pracy, jaka czeka wiele przedsiębiorstw w najbliższych miesiącach. - To nie jest lista rzeczy, które trzeba zrobić na wczoraj. To jest mapa, od której zaczynamy rozmowę o priorytetach – dodaje Biełasiewicz.

Stawka jest wysoka

Ustawa przewiduje realne konsekwencje finansowe za brak zgodności. Kary administracyjne mogą sięgnąć do 10 milionów euro lub 2 procent rocznego obrotu przedsiębiorstwa, w zależności od tego, która z tych wartości jest wyższa. Co istotne, odpowiedzialność nie ogranicza się do samej organizacji - ustawa wprowadza także osobistą odpowiedzialność finansową członków zarządu, sięgającą do 300 procent ich wynagrodzenia, a także obowiązek corocznych szkoleń kadry zarządzającej z zakresu cyberbezpieczeństwa.

- Dlatego zachęcamy firmy, żeby nie czekały do ostatnich tygodni przed terminem - podsumowuje Hojszyk. - Ocena sytuacji wyjściowej, którą oferujemy jako INEA, to pierwszy krok, który pozwala świadomie zaplanować kolejne miesiące, zamiast działać w pośpiechu pod presją zbliżającego się terminu.

Zegar tyka

Do upływu terminu na samoidentyfikację zostało niewiele ponad miesiąc, a jak pokazują doświadczenia z audytów prowadzonych przez INEA, sama ocena, czy firma podlega ustawie i w jakim stopniu spełnia jej wymogi, bywa czasochłonna nawet dla organizacji, które już wiedzą o zmianie przepisów. Skala braków ujawnianych podczas takich przeglądów – od niedziałającego uwierzytelniania wieloskładnikowego po brak planów ciągłości działania – często zaskakuje same zarządy.

Przy karach sięgających 10 milionów euro i osobistej odpowiedzialności finansowej członków zarządu, zwlekanie z decyzją o zgłoszeniu się do Wykazu KSC – lub jego zaniechanie – może się okazać kosztowne długo po tym, jak minie październikowy termin.