Warszawa, 03.03.2026 r.

Czy moja firma ma obowiązek wdrożyć wymogi NIS2?

18 stycznia 2026 r. prezydent podpisał nowelizację ustawy o krajowym systemie cyberbezpieczeństwa[1] („UKSC"), która implementuje do polskiego porządku prawnego unijną dyrektywę NIS2[2]. Lista podmiotów nią objętych jest długa i to same firmy mają obowiązek określić, czy podlegają pod nowe przepisy. Sektory gospodarki objęte regulacją wydają się jasne (dla podmiotów kluczowych: energia, transport, bankowość, ochrona zdrowia, woda pitna, ścieki, infrastruktura cyfrowa, kosmos i podmioty publiczne). Czy to oznacza, że firmy niedziałające w tych branżach nie zostaną podmiotem kluczowym? Niekoniecznie. Ustawa przewiduje bowiem jeszcze jeden istotny sposób uzyskania statusu (i licznych obowiązków) podmiotu kluczowego, który może niespodziewanie objąć bardzo wiele podmiotów. Jest nim „dostawca usług zarządczych". Kwestia ta dotyczy w szczególności spółek, które świadczą na rzecz innych podmiotów w grupie kapitałowej usługi IT.

Kto to jest dostawca usług zarządzanych?

Zgodnie z nowym brzmieniem art. 2 ust. 4j UKSC, przez dostawcę usług zarządzanych należy rozumieć podmiot, który „*świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych przez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy na miejscu lub zdalnie*". Mówiąc językiem mniej prawniczym: w tym zakresie całkowicie mieszczą się typowe usługi IT świadczone przez centra usług wspólnych (przygotowywanie komputerów dla pracowników, konfiguracja poczty e-mail, zarządzanie pakietem Microsoft Office 365, utrzymanie systemów ERP, CRM itp., pomoc przy wstawieniu tabelki do Worda i tysiąc innych czynności helpdesku). Zgodnie z nowym brzmieniem art. 5 UKSC (oraz Załącznika nr 1), podmiotem kluczowym jest również duże przedsiębiorstwo świadczące usługi zarządzane.

Co to oznacza w praktyce? Każda spółka w grupie kapitałowej mającej status dużego przedsiębiorstwa[3], która świadczy usługi IT dla pozostałych spółek w grupie jest podmiotem kluczowym zgodnie z UKSC. Całkowicie nieistotny jest tutaj główny profil działalności całej grupy kapitałowej czy poszczególnych spółek, jak również to, czy usługi są świadczone dla jednej, pięciu, czy pięćdziesięciu spółek w obrębie grupy.

Jakie obowiązki ma podmiot kluczowy?

W pewnym (sporym) uproszczeniu można podzielić obowiązki podmiotu kluczowego na trzy zasadnicze kategorie:

[1] Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (w dacie sporządzenia tekstu ustawa nie została jeszcze opublikowana w Dzienniku Ustaw) – dalej jako UKSC.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80 z późn. zm.).

[3] A więc która łącznie zatrudnia ponad 250 osób i ma obrót roczny powyżej 50 mln Euro zgodnie z Załącznikiem I do Rozporządzenia 651/2014 uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz.U.UE.L.2014.187.1 z późn. zm.). Podkreślić należy, że tego obliczenia należy dokonać dla całej grupy kapitałowej (wszystkich spółek powiązanych kapitałowo) łącznie, a zatem grupa może je spełniać nawet jeśli żadna ze spółek w jej skład wchodząca indywidualnie ich nie osiąga.

- obowiązki organizacyjne, polegające na wdrożeniu systemu zarządzania bezpieczeństwem informacji opartego na normie PN-EN ISO/IEC 27001 lub równoważnej oraz systemu zarządzania ciągłością działania opartego na PN-EN ISO/IEC 22301 lub równoważnej, a nadto prowadzeniu stosownych analiz ryzyka i stosowaniu zabezpieczeń adekwatnych do stwierdzonych ryzyk;
- obowiązki techniczne, polegające na objęciu systemów IT monitorowaniem w trybie 24/7;
- obowiązki związane z obsługą i raportowaniem incydentów, a nadto przechodzeniem cyklicznych audytów zewnętrznych.

Podkreślić należy, iż wdrożenie systemów, o których mowa powyżej to projekt, który w sprzyjających okolicznościach zajmie co najmniej 6 miesięcy (o ile chcemy zrobić to porządnie, a nie wydrukować kilka papierów i wrzucić na dno szuflady na wypadek kontroli).

Nowelizacja ustawy o KSC wchodzi w życie w miesiąc od publikacji w Dzienniku Ustaw. Podmioty, które dotychczas nie były objęte ustawą, będą miały 6 miesięcy od tej daty na określenie swojego statusu i ewentualne dokonanie zgłoszenia oraz 12 miesięcy na pełne wdrożenie wymagań wynikających z nowego brzmienia ustawy.

Jakie są konsekwencje braku zgodności?

Znowelizowana UKSC przewiduje dwa tryby odpowiedzialności za nieprzestrzeganie jej przepisów.

Pierwszym jest znana z NIS[4] i dotychczasowego brzmienia UKSC odpowiedzialność administracyjna firmy. Za naruszenia ustawy może zostać nałożona administracyjna kara pieniężna w wysokości do równowartości 10.000.000 euro lub 2% przychodów osiągniętych przez podmiot z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary (zastosowanie ma kwota wyższa[5]). Organ administracji może też – do czasu usunięcia niezgodności – zawiesić pozwolenia i koncesje wydane firmie, a w niektórych przypadkach nawet nakazać jej zawieszenie części lub całej prowadzonej działalności.

Nowym dodatkiem do ustawy jest osobista odpowiedzialność członków zarządu. W razie braku realizacji wymogów ustawy wszyscy członkowie zarządu mogą być osobiście zobowiązani do zapłacenia kary w kwocie do 300% otrzymywanego wynagrodzenia. Możliwe jest również zakazanie im w drodze decyzji administracyjnej pełnienia funkcji zarządczych. Podkreślić należy, że zarząd nie może w żaden sposób przenieść tej odpowiedzialności na inne osoby i za zgodność z UKSC zawsze odpowiadają osobiście wszyscy członkowie zarządu – bez względu na wewnętrzny podział obowiązków.

Podsumowując

Truizmem będzie powiedzieć, że na dostawcę usług kluczowych spadają liczne obowiązki – zarówno organizacyjne jak i techniczne. Warto jednak spojrzeć na te nieuniknione wydatki jak na inwestycję w zabezpieczenia takie jak piorunochrony czy systemy przeciwpożarowe. Ale ta analogia nie jest w 100% trafna. Pożar może zniszczyć jeden budynek, w skrajnych przypadkach kilka położonych obok siebie. Tymczasem atak hakerski może wyłączyć wszystkie obiekty firmy na całym świecie. Przekonał się o tym niedawno brytyjski gigant motoryzacyjny Jaguar – Landrover. Firma

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE. L. z 2016 r. Nr 194, str. 1).

[5] Dodatkowo, jeżeli zaniedbania skutkowały bezpośrednim i poważnym cyberzagrożeniem dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, albo zagrażały wywołaniem poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług – może być nałożona kara w wysokości do 100 000 000 zł.

produkcyjna zatrudniająca prawie ćwierć miliona ludzi musiała wstrzymać produkcję na całym świecie na blisko półtora miesiąca w wyniku ataku hakerskiego. Straty po tym incydencie szacowane są nawet na 2 miliardy funtów[6].

Daniel Taberski - radca prawny, audytor wiodący PN-EN ISO/IEC 27001 w iSecure Sp. z o.o.

[6] https://www.bbc.com/news/articles/cy9pdld4y81o [dostęp 25.02.2026 r.]