Łaszczuk

NIS 2

Jak w 5 krokach przygotować organizację do nowego standardu cyberbezpieczeństwa

W obliczu coraz częstszych ataków na zasoby przedsiębiorców i użytkowników Internetu oraz coraz mocniej odczuwalnych skutków cyberwojny zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga konsolidacji sił zarówno organów państwa odpowiedzialnych za kwestie bezpieczeństwa i dysponentów infrastruktury krytycznej, ale także coraz szerszego grona przedsiębiorców.

Już dziś

warto przeanalizować, w jaki sposób projektowane właśnie – a mające wejść w życie najpóźniej 15 października 2024 r. – nowe polskie regulacje dotyczące cyberbezpieczeństwa wpłyną na funkcjonowanie przedsiębiorców i z jakimi nowymi obowiązkami trzeba się będzie zmierzyć.

NIS 2 – nowe ramy prawne cyberbezpieczeństwa

W styczniu 2023 r. uchwalona została dyrektywa unijna w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej (tzw. dyrektywa NIS 2). Ważną zmianą – w porównaniu do wcześniej wdrożonego standardu bezpieczeństwa (dyrektywa NIS) – jest rozszerzenie zakresu podmiotów objętych systemem budowania i nadzoru nad cyberbezpieczeństwem. Dotychczas obowiązki z tym związane odnosiły się przede wszystkim do podmiotów publicznych i przedsiębiorców budujących de facto infrastrukturę krytyczną państwa (np. operatorów sieci telekomunikacyjnych, usług bankowych czy producentów pasz i nawozów). Pod rządami nowych regulacji zakres podmiotów zostanie rozszerzony o wiele małych i średnich przedsiębiorstw, tworząc tzw. grupę podmiotów ważnych – przyjmując założenie, że pozornie drobny incydent np. **wyciek danych osobowych klientów sklepu internetowego może skutkować poważnymi zagrożeniami dla cyberbezpieczeństwa.**

Nowe regulacje kładą też większy nacisk na kwestie związane z zapewnieniem bezpieczeństwa łańcucha dostaw, raportowanie incydentów bezpieczeństwa i spełnienie obowiązków informacyjnych oraz wprowadzenie mechanizmów współpracy z krajowymi organami odpowiedzialnymi za cyberbezpieczeństwo. Obecnie w Polsce trwają prace nad przygotowaniem krajowych przepisów implementujących dyrektywę NIS 2 – nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa jest obecnie procedowana. Państwa członkowskie muszą bowiem wdrożyć nowe przepisy do 15 października 2024 r.

Kogo dotyczą nowe obowiązki?

Oprócz podmiotów dotychczas budujących infrastrukturę krytyczną państwa dyrektywa NIS 2 rozszerzyła z 7 do 18 liczbę branż, z których przedsiębiorcy zobowiązani są wdrożyć nowe proaktywne zasady zarządzania bezpieczeństwem cybernetycznym.

Operatorzy usług kluczowych

W tej grupie mogą znaleźć się przedsiębiorcy z następujących sektorów:

- Energetyka
- Transport (lotniczy, wodny, kolejowy i drogowy)
- Bankowość
- Infrastruktura rynków finansowych
- Opieka zdrowotna
- Dostawcy i dystrybutorzy wody pitnej
- Ścieki (w tym przedsiębiorcy zbierający, odprowadzający i uzdatniający ścieki)
- Infrastruktura cyfrowa
- Zarządzanie ICT między przedsiębiorcami
- Podmioty administracji publicznej
- Przestrzeń kosmiczna

Operatorzy usług ważnych

W tej grupie mogą znaleźć się przedsiębiorcy z poniższych sektorów:

- Usługi pocztowe i kurierskie
- Gospodarowanie odpadami
- Produkcja i wytwarzanie chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Dostawcy usług cyfrowych (w tym dostawcy internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych)
- Produkcja, w tym: produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, komputerów, wyrobów elektrycznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń gdzie indziej niesklasyfikowanych, pojazdów samochodowych, przyczep i naczep a także pozostałego sprzętu transportowego
- Podmioty prowadzące badania naukowe

Nowe obowiązki i nowe wyzwania

1. **Samoidentyfikacja** – Regulacje NIS 2 oraz projektowane obecnie przepisy krajowe bazują na odmiennej niż dotychczas zasadzie. Zarówno operatorzy usług kluczowych, jak i usług ważnych muszą dokonać samoidentyfikacji, czyli przeanalizować liczne warunki oraz wyłączenia dla poszczególnych sektorów gospodarki i określić, czy będą zaliczani do wskazanych grup
2. **Zgłoszenie do bazy podmiotów kluczowych i ważnych**
3. **Wyznaczenie osoby** odpowiedzialnej w organizacji za cyberbezpieczeństwo i współpracę z innymi podmiotami kluczowymi i ważnymi

3. **Pogłębiona i systematyczna analiza ryzyka** – podmioty kluczowe i ważne zostaną zobowiązane do wdrożenia odpowiednich polityk bezpieczeństwa oraz procedur wewnętrznych zarządzania cyberbezpieczeństwem
4. **Wdrożenie procedur współpracy** z właściwym krajowym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)
5. **Wprowadzenie cyklicznych szkoleń** z zakresu cyberbezpieczeństwa i cyberhigieny dla organów zarządzających i pracowników
6. **Wdrożenie procedur obsługi i raportowania incydentów** w zakresie cyberbezpieczeństwa

Nowe sankcje i zasady odpowiedzialności

Przepisy NIS 2 przewidują wprowadzenie dotkliwych kar dla podmiotów, które nie dostosują się do nowych standardów bezpieczeństwa.

- W przypadku operatorów usług kluczowych – co najmniej 10 mln euro lub co najmniej 2% rocznego obrotu
- W przypadku operatorów usług ważnych – co najmniej 7 mln euro lub 1,4% rocznego obrotu

Jak w 5 krokach przygotować się do wymogów NIS 2

Wprawdzie polskie przepisy wdrażające dyrektywę NIS 2 są jeszcze procedowane, jednak już teraz warto rozpocząć audyt i przygotowanie organizacji do nowych obowiązków, podejmując co najmniej 5 wskazanych przez nas kroków.

1.	**Potwierdzenie przynależności do grupy operatorów usług kluczowych i ważnych –** w pierwszym kroku należy dokonać analizy zakresu prowadzonej działalności gospodarczej z punktu widzenia wskazanych w przepisach branż (w tym sektorów, podsektorów, rodzajów podmiotów objętych nowymi obowiązkami w tym proponowanych wyłączeń)
2.	**Analiza procedur organizacyjnych** z punktu widzenia wdrożenia wymogów cyberbezpieczeństwa i określenie procedur kluczowych
3.	**Prawny audyt obowiązującej dokumentacji**, np. regulaminu pracy, polityki zarządzania systemami informatycznymi

4.	**Przygotowanie podręcznika informacyjnego** zawierającego nowe obowiązki z uwzględnieniem struktury organizacyjnej i bieżących procesów w firmie, w tym wytyczne dla podwykonawców i podmiotów wchodzących do Państwa łańcucha dostaw.
5.	**Przygotowanie wewnętrznych procedur pogłębionej i systematycznej analizy ryzyka** z uwzględnieniem struktury organizacyjnej i bieżących procesów biznesowych, w tym wytycznych dla podmiotów współpracujących i uczestniczących w Państwa łańcuchu dostaw.

Skontaktuj się z nami i sprawdź, jak możemy pomóc

Chętnie spotkamy się, by porozmawiać o Państwa potrzebach w zakresie dostosowania działalności Państwa firmy do nowych wymogów.

dr hab. Justyna Kurek-Sobieraj
Adwokat / Senior Associate
justyna.kurek@laszczuk.pl

Marek Korcz
Radca prawny / Partner zarządzający
marek.korcz@laszczuk.pl