

kancelarie rp

Niezbędny Prawny Porady

WIĘCEJ PORAD NA  KANCELARIE.RP.PL

PRZEDSIĘBIORCY

Krajowy System Cyberbezpieczeństwa oznacza nowe obowiązki

Podniesienie poziomu cyberbezpieczeństwa w podmiotach stanowiących podmioty kluczowe lub ważne z punktu widzenia funkcjonowania państwa powinno stanowić dziś najwyższy priorytet.



TOMASZ KAMIŃSKI

adwokat, wspólnik w Kancelarii
Krzysztof Rożko i Wspólnicy



DANIEL NIWIŃSKI

prawnik, ekspert ds.
cyberbezpieczeństwa w Kancelarii
Krzysztof Rożko i Wspólnicy

pieniężnych – w zakresie części nowych obowiązków. W praktyce oznacza to, że podmioty objęte regulacją będą miały relatywnie krótki czas na przeprowadzenie analizy luki, wdrożenie systemowych zmian organizacyjnych i technicznych oraz przygotowanie dokumentacji zgodnej z nowymi wymogami.

Podmioty kluczowe

Nowelizacja UKSC wprowadza nową, dwupoziomą klasyfikację podmiotów: podmioty kluczowe oraz podmioty ważne. Klasyfikacja zależy przede wszystkim od sektora działalności (m.in. sektor finansowy, infrastruktura cyfrowa, energia, transport, ochrona zdrowia, administracja publiczna) i wielkości przedsiębiorstwa (kryteria zatrudnienia i obrotu). Załącznik nr 1 do nowelizowanej UKSC określa sektory kluczowe, natomiast załącznik nr 2 wskazuje katalog sektorów ważnych.

Co istotne – system opiera się w dużej mierze na mechanizmie samooceny. To dany podmiot ma obowiązek przeanalizować, czy spełnia kryteria uznania za podmiot kluczowy lub ważny. W terminie sześciu miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny dany podmiot powinien przeprowadzić formalną samoocenę, udokumentować jej wynik i złożyć wniosek o wpis do wykazu podmiotów kluczowych lub ważnych. Brak przeprowadzenia samooceny lub błędna klasyfikacja mogą prowadzić do naruszenia obowiązków ustawowych.

Najważniejsze obowiązki

Zakres obowiązków podmiotów kluczowych lub ważnych jest szeroki i obejmuje zarówno kwestie organizacyjne, jak i techniczne.

Podmioty będą zobowiązane do wdrożenia systemowego podejścia do zarządzania ryzykiem w zakresie bezpieczeństwa systemów informacyjnych. Obejmuje to m.in.: zarządzanie ryzykiem, opracowanie i wdrożenie polityk i procedur bezpieczeństwa, wdrożenie odpowiednich środków technicznych i organizacyjnych adekwatnych do poziomu ryzyka, zarządzanie ciągłością działania, zarządzanie bezpieczeństwem łańcucha dostaw.

Wiele z powyższych obowiązków jest już znanych instytucjom objętym reżimem RODO czy DORA, jednak dla większości podmiotów spoza sektora regulowanego będzie to pierwsze tak kompleksowe podejście do cyberbezpieczeństwa.

Nowelizacja UKSC przewiduje również obowiązek zarządzania incydentami, w tym zgłaszania ich do właściwego CSIRT w ściśle określonych terminach. System raportowania ma być wieloetapowy (wcześnie ostrzeżenie o incydencie, zgłoszenie incydentu, sprawozdanie okresowe z obsługi incydentu).

Spójny proces reagowania

Dla podmiotów objętych różnymi wymaganiami w zakresie zarządzania incydentami na gruncie RODO i UKSC, a nawet specyficznych ustaleń umownych z kontrahentami, szczególnie istotne będzie opracowanie spójnych procesów wewnętrznych reagowania oraz obsługi incydentów i naruszeń, zarówno z punktu widzenia tzw. twardego security, czyli technicznej odpowiedzi na incydent, jak również z punktu widzenia compliance, pozyskania odpowiednich dowodów na realizację wymagań, spełnienia obowiązków raportowych, obowiązków informacyjnych oraz odpowiedniej

komunikacji. Dodatkowo istotnym elementem będzie wykorzystanie w praktyce wniosków po zakończonej obsłudze incydentu (tzw. lessons learned) i przeprowadzenie szeregu działań naprawczych mających na celu wyeliminowanie występowania tego typu incydentów w przyszłości.

Kolejnym istotnym elementem nowelizacji UKSC będzie wzmocnienie odpowiedzialności organów zarządzających. Kierownictwo podmiotu ma być bezpośrednio zaangażowane w nadzór nad systemem zarządzania cyberbezpieczeństwem wewnątrz organizacji.

” Kary za brak realizacji obowiązków wynikających z nowelizowanej UKSC, w zależności od wagi naruszenia, będą mogły sięgać wielomilionowych kwot

stwem, w tym zatwierdzanie polityk oraz monitorowanie ich realizacji. Oznacza to, że cyberbezpieczeństwo przestanie być wyłącznie odpowiedzialnością osób obsługujących IT – staje się zadaniem zarządczym i strategicznym.

Poważne sankcje

Choć przez pierwsze dwa lata przewidziano okres przejściowy, w którym za brak realizacji części obowiązków nie będzie można nakładać administracyjnych kar pieniężnych, docelowy model sankcyjny jest bardzo restrykcyjny – kary za brak realizacji obowiązków wynikających z nowelizowanej UKSC, w zależności od wagi naruszenia, będą mogły sięgać wielomilionowych kwot. Nowelizacja UKSC przewiduje również indywidualną odpowiedzialność osób zarządzających podmiotem, dzięki czemu przewiduje się większe zaangażowanie najwyższego kierownictwa w zarządzanie cyberbezpie-

czeństwem wewnątrz organizacji.

Okres przejściowy nie powinien być traktowany jako „czas beczynności”, lecz jako okazja do uporządkowania procesów i dokumentacji. Jak rozpocząć przygotowania? Przede wszystkim należy przeprowadzić analizę statusu podmiotu – czy podmiot może zostać uznany za kluczowy lub ważny – oraz złożyć wniosek o wpis do rejestru. Następnie wymagane będzie przeprowadzenie mapowania istniejących regulacji na wymagania nowelizowanej UKSC oraz identyfikacja powiązanych ze

sobą obowiązków wynikających m.in. z RODO, wytycznych sektorowych czy też ustaleń umownych. Konieczne będzie również przeprowadzenie analizy luk (gap analysis), czyli oceny zgodności aktualnych rozwiązań z projektowanymi wymogami, a także opracowanie i realizacja planu wdrożenia nowych wymagań.

Oczekiwanie na TK

Poza złożeniem podpisu pod ustawą, Prezydent RP podjął jednocześnie decyzję o skierowaniu ustawy do kontroli następnej przez Trybunał Konstytucyjny.

Decyzja Prezydenta RP o przekazaniu ustawy do kontroli pod względem konstytucyjności, jest wynikiem głosów środowisk pracodawców i przedsiębiorców, którzy apelowali o zbadanie proporcjonalności przyjętych rozwiązań.

Oczekując na ostateczne rozstrzygnięcie tej kwestii, zaznaczyć należy, iż wejście w

życie nowelizacji UKSC ma kluczowe znaczenie z punktu widzenia bezpieczeństwa państwa, a termin implementacji dyrektywy NIS 2 w polskim systemie prawnym upłynął już w październiku 2024 r.

Warto zaznaczyć, że podniesienie poziomu cyberbezpieczeństwa w podmiotach stanowiących podmioty kluczowe lub ważne z punktu widzenia funkcjonowania państwa stanowić musi dziś najwyższy priorytet. Miesięczne raporty opracowywane przez CERT Polska we współpracy z CSIRT NASK

wskazują na wzrost liczby raportowanych incydentów o 10 proc. w skali roku – w całym 2025 r. liczba zgłoszeń zarejestrowanych przez zespół CERT Polska wyniosła 658,3 tys. (601 tys. w roku 2024). Liczba incydentów cyberbezpieczeństwa w 2025 r. wyniosła 260,8 tys., co stanowi wzrost o 152 proc. w stosunku do roku poprzedniego (103,4 tys.). W samym grudniu 2025 r. odnotowano o 331 proc. więcej incydentów cyberbezpieczeństwa niż w grudniu 2024 r.

Nowelizacja UKSC to jedna z najważniejszych zmian w krajowym systemie regulacyjnym w obszarze cyberbezpieczeństwa ostatnich lat.

Choć ustawodawca przewidział okres dostosowawczy i przejściowy model sankcyjny, realny czas na wdrożenie kompleksowych rozwiązań jest ograniczony. Dla podmiotów, które już dziś podchodzą do cyberbezpieczeństwa w sposób systemowy, nowelizacja będzie ewolucją. Dla pozostałych – może oznaczać konieczność głębokiej transformacji organizacyjnej. /eoe