Analizy OSW

OŚRODEK STUDIÓW WSCHODNICH 4.02.2026 www.osw.waw.pl

Niemcy: nowa ustawa o ochronie infrastruktury krytycznej

Kamil Frymark, Michał Kędzierski

29 stycznia – głosami koalicji CDU/CSU–SPD oraz opozycyjnej AfD – Bundestag uchwalił ustawę ramową o ochronie infrastruktury krytycznej (KRITIS-Dachgesetz), implementującą unijną dyrektywę CER o odporności podmiotów krytycznych. Nowe prawo wprowadza jednolite standardy dotyczące fizycznego bezpieczeństwa infrastruktury w kluczowych sektorach: energetyki, transportu i komunikacji, finansów i ubezpieczeń, ochrony zdrowia, zaopatrzenia w wodę pitną, gospodarki ściekowej i odpadami komunalnymi, technologii informacyjnych i telekomunikacji, zaopatrzenia w żywność, przestrzeni kosmicznej oraz administracji publicznej. Ustawa obejmuje tylko te podmioty (m.in. koleje, sektor bankowy, elektrownie etc.), które zaopatrują co najmniej 500 tys. osób. Operatorzy takich obiektów są m.in. zobowiązani do systematycznej analizy ryzyka (przynajmniej raz na cztery lata), wdrażania odpowiednich środków technicznych i organizacyjnych w celu jego minimalizowania oraz zgłaszania poważnych incydentów związanych z bezpieczeństwem. Kraje związkowe mają możliwość identyfikowania dodatkowych obiektów krytycznych w zakresie usług leżących wyłącznie w ich kompetencjach. W każdym landzie ma powstać podmiot odpowiedzialny za wprowadzanie nowych przepisów. Nadzór nad realizacją ustawy sprawować będzie Federalny Urząd Ochrony Ludności i Pomocy w Katastrofach (BBK), który w przypadku stwierdzenia naruszeń prawa będzie mógł nałożyć kary w wysokości od 100 tys. do 1 mln euro.

Wzmocnienie ochrony infrastruktury krytycznej wymuszają nie tylko regulacje UE, lecz także coraz liczniejsze ataki na nią. Dotychczas kwestie zabezpieczenia regulowano głównie w ustawach branżowych i przepisach dotyczących bezpieczeństwa IT. Nowa ustawa wdraża ponadsektorowe regulacje i wzmacnia fizyczną ochronę kluczowych obiektów.

Komentarz

- **Od 2022 r. w Niemczech obserwuje się stały wzrost liczby ataków na infrastrukturę krytyczną – zarówno fizycznych, jak i cybernetycznych.** Coraz częściej dochodzi m.in. do podejrzanych przelotów dronów nad obiektami wojskowymi, energetycznymi czy komunikacyjnymi. Według Federalnego Urzędu Kryminalnego (BKA) tylko w ub.r. odnotowano ponad 1000 takich przypadków. Ponadto w ocenie BKA i kontrwywiadu (BfV) rośnie także liczba aktów sabotażu, za którymi mogą stać obce państwa – w pierwszej połowie 2025 r. zaobserwowano 143 takie incydenty (m.in. podłożenie ognia w porcie w Rostocku, skąd eksportowane jest ukraińskie zboże). Coraz więcej notuje się również ataków cybernetycznych. Zgodnie z danymi Federalnego Urzędu ds. Bezpieczeństwa Techniki Informacyjnej (BSI) od połowy 2024 do połowy 2025 r. było ich ponad 720 (rok wcześniej – 490) – najczęściej dotykały one sektory zdrowotny,

energetyczny i transportowy. Jako sprawców identyfikuje się pospolitych przestępców, politycznych ekstremistów oraz aktorów państwowych, w tym przede wszystkim Rosję, Chiny, Iran i Koreę Północną.

- **Ustawa spotkała się z szeroką krytyką ze strony ekspertów, przedstawicieli zainteresowanych branż, samorządów i opozycji – jako niewystarczająca wobec zagrożeń.** Wskazuje się m.in., że rozporządzenia wykonawcze, określające konkretne minimalne wytyczne dla operatorów infrastruktury krytycznej, mają zostać przyjęte do 2030 r., co znacznie wydłuża pełne wdrożenie ustawy. Ponadto krytykuje się objęcie regulacjami wyłącznie największych podmiotów. W uchwalonym akcie prawnym nie uwzględniono też wniosków ze styczniowego ataku lewicowych ekstremistów na sieć energetyczną w Berlinie (zob. *Konsekwencje blackoutu w Berlinie*), w tym m.in. postulatu zakazu upubliczniania danych dotyczących szczegółów położenia sieci energetycznych i wodociągowych. Rząd zapowiedział dodatkową inicjatywę ustawodawczą w tym zakresie. Poza tym operatorzy infrastruktury podnoszą potrzebę uregulowania kwestii finansowania ochrony – obowiązek ten spoczywa obecnie na samych podmiotach. Przedsiębiorstwa domagają się wsparcia, np. z budżetu resortu obrony. Wyzwaniem pozostaje także rozproszenie kompetencji między szczeble federalny i landowy, co utrudnia skuteczną koordynację działań i efektywną ochronę infrastruktury.
- **Przyjęte regulacje wpisują się w szereg działań RFN zwiększających ochronę przed zagrożeniami hybrydowymi.** Jako szczególne zagrożenie identyfikuje się drony. W grudniu ub.r. powołano w tym celu specjalną jednostkę policji federalnej (Drohnenabwehreinheit der Bundespolizei) oraz uruchomiono Wspólne Centrum Obrony przed Dronami (Gemeinsames Drohnenabwehrzentrum), które ma koordynować działania policji federalnej, policji landowych i Bundeswehry. Procedowane są nowelizacje ustaw o policji federalnej oraz bezpieczeństwie w przestrzeni powietrznej, mające poszerzyć uprawnienia służb w zakresie zwalczania zagrożeń dronowych (zob. *Drony nad Niemcami – łatanie luk prawnych i sprzętowych*). Ponadto przy Urzędzie Kanclerskim tworzone jest Centrum Obrony przed Zagrożeniami Hybrydowymi.