Transport, dostawy energii i wody pitnej niewystarczająco zabezpieczone przed cyberatakami

27.8.2026 - | Najwyższa Izba Kontroli

W minionym roku średnio co dwie minuty w polskiej cyberprzestrzeni dochodziło do incydentu mogącego zagrażać bezpieczeństwu. Tymczasem środki cyberbezpieczeństwa stosowane w latach 2021-2025 przez ośmiu skontrolowanych przez NIK operatorów usług kluczowych, którzy dostarczali energię i wodę pitną oraz zapewniali transport kolejowy i wodny były niewystarczające i nieadekwatne do obecnego charakteru zagrożeń oraz ich skali.

Niewystarczający był też nadzór sprawowany nad cyberbezpieczeństwem w tych sektorach przez ministrów: energii i infrastruktury. Mimo że wiedzieli o niedostatecznym zabezpieczeniu przed cyberatakami podstawowych usług, nie podjęli odpowiednich działań nadzorczych i nie skontrolowali operatorów odpowiedzialnych za zapewnienie bezpieczeństwa usług. Oznaczało to, że mechanizmy Krajowego Systemu Cyberbezpieczeństwa (KSC) nie zapewniły skutecznego identyfikowania i egzekwowania od operatorów realizacji nałożonych na nich obowiązków. Jest to tym bardziej niepokojące, że od utworzenia KSC upłynęło już ponad siedem lat, a w 2025 r. Polska była jednym z najczęściej atakowanych przez cyberprzestępców państw na świecie.

Sieci i systemy informatyczne oraz łączności elektronicznej odgrywają kluczową rolę w społeczeństwie i stanowią dziś fundament wzrostu gospodarczego. Zakłócenie ich działania może prowadzić do przerw w dostawach energii i wody, ograniczenia funkcjonowania transportu, strat gospodarczych, a także zagrożenia bezpieczeństwa ludzi. Wyniki kontroli NIK wskazują na powtarzające się i istotne słabości zarządzania cyberbezpieczeństwem oraz nadzoru w zbadanych sektorach.

Żaden z ośmiu skontrolowanych operatorów nie zapewnił systemom służącym do świadczenia usługi kluczowej, odporności na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych. W dodatku większość operatorów (sześciu) systematycznie ignorowało krytyczne alerty generowane przez systemy monitorujące i zabezpieczające, a w skrajnych przypadkach w ogóle nie prowadziło takiego monitoringu, choć skala zagrożeń cybernetycznych systematycznie rosła. W konsekwencji mogli nawet nie wiedzieć, że doszło do ataku na ich systemy.

W 2025 r. Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) z poziomu krajowego obsłużyły niemal 273 tys. tzw. incydentów – o 144,4% więcej niż rok wcześniej, co oznacza, że do incydentu w polskiej cyberprzestrzeni dochodziło statystycznie średnio co dwie minuty. Zaliczamy do nich każde zdarzenie, które m.in. zakłóca działanie systemów informatycznych, zagraża poufności danych lub narusza zasady bezpieczeństwa technologii informacyjnych (Information Technology, IT).

Szczególne znaczenie mają incydenty dotyczące systemów wykorzystywanych do świadczenia usług kluczowych, ponieważ ich skutki mogą wykraczać poza sferę cyfrową. Atak hakerski na wodociągi umożliwia np. manipulowanie parametrami wody. Zwiększenie w niej ilości chloru może z kolei zagrażać zdrowiu, a nawet życiu jej odbiorców. Przejęcie kontroli przez

hakerów nad sieciami elektroenergetycznymi może prowadzić do rozległych i długotrwałych przerw w dostawach prądu. **Dodatkowo Polska, jako członek Unii Europejskiej i NATO, mierzy się z zagrożeniami ze strony cyberprzestępczych grup hakerskich, czy grup sponsorowanych przez obce państwa.**

W obliczu rosnącej powszechności technicznie zaawansowanych metod ataku, takich jak złośliwe oprogramowanie, czy z wykorzystaniem sztucznej inteligencji, utrzymywanie i ciągłe doskonalenie standardów bezpieczeństwa przestaje być jedynie kwestią techniczną. Staje się ono niezbędnym elementem zgodności z wymogami prawnymi oraz wyrazem odpowiedzialności za stabilność całego systemu, w którym działalność jednego podmiotu bezpośrednio wpływa na funkcjonowanie innych uczestników rynku i konsumentów. Zdaniem NIK w obliczu napięć geopolitycznych i ekonomicznych kluczowe staje się również identyfikowanie nawet marginalnych zagrożeń w zakresie cyberbezpieczeństwa.

NIK skontrolowała:

- Ministerstwo Cyfryzacji,
- Ministerstwo Energii,
- Ministerstwo Infrastruktury,
- ośmiu operatorów usług kluczowych (w sektorach: transport, dostawy energii oraz zaopatrzenie w wodę pitną i jej dystrybucja).

Okres objęty kontrolą: 1 stycznia 2021 r. – 16 lutego 2026 r.

https://www.nik.gov.pl/aktualnosci/transport-dostawy-energii-i-wody-pitnej-niewystarczajaco-zabezpieczone-przed-cyberatakami.html