Rosnące zagrożenie cyberatakami na infrastrukturę krytyczną

Kategoria: Aktualności
Opublikowano: wtorek, 14, styczeń 2025 09:46
Tomasz Smaś
Odsłony: 1081

W ostatnich latach infrastruktura krytyczna na całym świecie stała się celem intensywnych cyberataków. Według danych Europejskiego Repozytorium Cyberincydentów (EuRepoC) tylko w latach 2023–2024 doszło do około 1400 takich incydentów, z czego ponad połowa dotyczyła kluczowych sektorów, takich jak energetyka, transport czy opieka zdrowotna. Ochrona infrastruktury krytycznej nabiera więc szczególnego znaczenia, zwłaszcza w kontekście współczesnych konfliktów geopolitycznych.

Eksperci zwracają uwagę, że celem cyberataków staje się niemal wszystko, co jest sterowane online. Przykłady obejmują systemy wodociągowe, smart cities, oczyszczalnie ścieków czy rurociągi. Agresorzy, często powiązani z wrogimi państwami, wykorzystują zaawansowane technologie do zakłócania funkcjonowania tych systemów. W 2024 roku odnotowano około 500 incydentów w Europie, z których wiele przypisuje się rosyjskim działaniom hybrydowym.

W Stanach Zjednoczonych podobne zagrożenia uwidoczniły się w atakach na systemy wodociągowe oraz największego operatora rurociągów paliwowych, co paraliżowało kluczowe sektory gospodarki.

Eksperci podkreślają, że ochrona infrastruktury krytycznej wymaga nie tylko zaawansowanych technologii, takich jak sztuczna inteligencja, ale również budowania odporności społecznej. Jest to zdolność społeczności do zapobiegania, reagowania na zagrożenia oraz szybkiego powrotu do normalnego funkcjonowania po ataku.

Sztuczna inteligencja odgrywa kluczową rolę w analizowaniu zagrożeń, usprawnianiu komunikacji i przewidywaniu scenariuszy ataków. Jednocześnie wiąże się z ryzykiem, takim jak wykorzystywanie jej do szerzenia dezinformacji. Zdaniem ekspertów konieczne jest nauczenie się skutecznego przeciwdziałania tym zagrożeniom.

Raport Agencji UE ds. Cyberbezpieczeństwa (ENISA) wskazuje na rosnącą świadomość zagrożeń, ale także na wyzwania związane z niedoborem wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa. W odpowiedzi na te potrzeby rośnie liczba kierunków studiów związanych z tą tematyką, a uczelnie dostosowują swoje programy do wymogów rynku pracy.

Według „Barometru cyberbezpieczeństwa" KPMG, trudności z rekrutacją odpowiednich kadr to obecnie największa przeszkoda w osiągnięciu wysokiego poziomu zabezpieczeń. Ponad połowa respondentów badania wskazała ten problem jako kluczowy.

Zdaniem ekspertów ochrona infrastruktury krytycznej wymaga zintegrowanego podejścia, które łączy nowoczesne technologie z edukacją i wzmacnianiem kompetencji społeczeństwa. Współpraca międzynarodowa, rozwój kadr oraz zwiększanie świadomości zagrożeń są niezbędne, by sprostać wyzwaniom związanym z rosnącą liczbą cyberataków.

Działania na rzecz wzmocnienia odporności społecznej i technologicznej stanowią fundament ochrony infrastruktury krytycznej w obliczu nowych zagrożeń. Konieczne jest zrozumienie, że cyberbezpieczeństwo to nie tylko kwestia technologii, ale również odpowiedzialności społecznej i gotowości na zmieniające się wyzwania.

Źródło: Newseria

Phoca PDF