Globalny wzrost liczby cyberataków

Kategoria: Styl życia
Opublikowano: czwartek, 28, listopad 2024 16:08
Tomasz Smaś
Odsłony: 2168

Liczba cyberataków o charakterze destrukcyjnym wzrośnie globalnie o 105 proc. w latach 2020-2024 – wynika z analiz przeprowadzonych przez firmę ubezpieczeniową QBE. Szacuje się, że w 2024 roku na świecie odnotowanych zostanie 211 takich incydentów, co odzwierciedla narastającą skalę zagrożeń w cyberprzestrzeni.

Destrukcyjne skutki cyberataków

Cyberataki o charakterze destrukcyjnym wyróżniają się nieodwracalnymi skutkami, które wykraczają poza zakłócenia w dostępie do danych czy systemów. Przykładem jest atak na zakłady petrochemiczne w Arabii Saudyjskiej, podczas którego złośliwe oprogramowanie Triton unieruchomiło systemy bezpieczeństwa. Skutki tego incydentu mogły doprowadzić do katastrofy przemysłowej o międzynarodowym zasięgu. Innym przykładem jest niedawny atak na brytyjski system opieki zdrowotnej NHS England, w wyniku którego przejęto dane ponad 2 milionów pacjentów, a setki operacji i wizyt zostały odwołane.

Motywy i koszty cyberataków

Według raportu QBE, głównym motywem cyberprzestępców jest wymuszanie okupu. Organizacje o rocznych przychodach przekraczających 5 miliardów USD są szczególnie podatne na ataki i częściej decydują się na wypłatę okupu – robi tak 61 proc. takich firm, w porównaniu do 25 proc. organizacji o przychodach poniżej 10 milionów USD. W 2023 roku średnia wartość okupu wyniosła 2 miliony USD, co oznacza pięciokrotny wzrost w porównaniu do roku poprzedniego.

Najbardziej zagrożone sektorami są przemysł, opieka zdrowotna, IT, edukacja oraz instytucje rządowe. Prognozy wskazują, że liczba ofiar ransomware zwiększy się o kolejne 11 proc. do 2025 roku.

Zapotrzebowanie na zaawansowane zabezpieczenia

Eksperci podkreślają konieczność wprowadzenia zaawansowanych systemów zabezpieczeń oraz procedur reagowania na incydenty. Podstawowe środki, takie jak silne hasła, dwuskładnikowe uwierzytelnianie czy ochrona antywirusowa, są ważne, ale niewystarczające wobec coraz bardziej złożonych zagrożeń.

Wyzwania regulacyjne i niedobór specjalistów

Rosnąca liczba ataków zmusza organizacje do dostosowania się do nowych wymagań prawnych, takich jak unijna dyrektywa NIS2. Przepisy nakładają obowiązek wprowadzenia zaawansowanych procedur i zasobów, co stwarza wyzwania w obliczu globalnego niedoboru specjalistów ds. cyberbezpieczeństwa.

Automatyzacja procesów ochrony oraz inwestycje w rozwój kompetencji stają się kluczowymi elementami strategii zarządzania ryzykiem. Organizacje posiadające wyspecjalizowane zespoły lub korzystające z usług zewnętrznych firm mogą skuteczniej chronić swoje dane i zasoby przed nieodwracalnymi skutkami cyberataków.

Cyberbezpieczeństwo jako priorytet

W dobie narastających zagrożeń cyfrowych cyberbezpieczeństwo stało się kluczowym elementem strategii ochrony organizacji. Bez odpowiednich procedur i struktur, takich jak SOC i IRT, organizacje

narażają się na poważne konsekwencje finansowe i wizerunkowe. Tymczasem odpowiednie inwestycje w technologie i ludzi mogą zminimalizować ryzyko oraz zapewnić ochronę przed rosnącą falą destrukcyjnych ataków.

Źródło: IP