Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2025 roku

Zespół CSIRT GOV Agencji Bezpieczeństwa Wewnętrznego opublikował „Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2025 roku". Opracowanie przedstawia najważniejsze zagrożenia i ryzyka obserwowane w polskiej cyberprzestrzeni oraz podsumowuje działania związane z identyfikacją zagrożeń i reagowaniem na incydenty bezpieczeństwa komputerowego. Po raz pierwszy Raport został uzupełniony również o perspektywę zespołów CSIRT NASK i CSIRT KNF.

Z danych i analiz CSIRT GOV - ABW wynika, że poziom zagrożenia w cyberprzestrzeni RP pozostaje wysoki. W 2025 roku liczba zarejestrowanych incydentów wzrosła o ponad jedną czwartą w porównaniu z rokiem poprzednim. Szczególnie widoczny był wzrost zagrożeń związanych z podatnościami systemów oraz kampaniami socjotechnicznymi. Coraz większe znaczenie ma również wykorzystanie sztucznej inteligencji – m.in. do tworzenia wiarygodniejszych wiadomości phishingowych, automatyzacji rozpoznania podatności oraz przygotowywania materiałów dezinformacyjnych.

Raport wskazuje cztery dominujące zjawiska:

utrzymującą się wysoką aktywność grup powiązanych z Rosją i Białorusią,
rozwój zdolności prorosyjskich grup haktywistycznych,
nasilenie kampanii phishingowych i socjotechnicznych oraz
rosnące wykorzystanie AI przez atakujących.

Polska pozostaje celem operacji cyberszpiegowskich, działań wpływu informacyjnego oraz aktywności wymierzonych w administrację państwową i podmioty strategiczne.

Autorzy zwracają także uwagę na próby wykorzystania podatności, w tym luk typu zero-day, oraz na niezmiennie istotną rolę człowieka w systemie bezpieczeństwa. Problemem pozostaje m.in. korzystanie z oprogramowania, dla którego zakończono wsparcie producenta, niewdrażanie dostępnych aktualizacji oraz podatność użytkowników na socjotechnikę.

Szczególnym wydarzeniem końca 2025 roku był pierwszy w cyberprzestrzeni RP atak o potencjale destrukcyjnym, wymierzony w sektor energii. Nie doprowadził on do przerwania dostaw energii i ciepła, jednak – jak wskazują autorzy Raportu – tego rodzaju działania mogą być testem odporności i w przyszłości pojawiać się częściej.

CSIRT GOV (www.csirt.gov.pl) to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełniący rolę zespołu CSIRT poziomu krajowego. Odpowiada m.in. za koordynację przeciwdziałania na incydenty oraz rozpoznawanie, zapobieganie i wykrywanie zagrożeń dotyczących systemów teleinformatycznych administracji publicznej i infrastruktury krytycznej, istotnych dla ciągłości funkcjonowania państwa.

Zapraszamy do lektury!

Pliki do pobrania

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2025 roku (pdf, 50.5 MB, 02.09.2026)

Poprzedni Strona