



Minister – Członek Rady Ministrów Koordynator Służb Specjalnych

Tomasz Siemoniak

DBN.WAS.4511.1.2025

Warszawa, /data zgodna z podpisem elektronicznym/

Pan
Szymon Hołownia
Marszałek Sejmu Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na zapytanie nr 2110 Poseł na Sejm RP Bożeny Lisowskiej w sprawie *ataków hakerskich w cyberprzestrzeni* pragnę przekazać następujące informacje.

Działający w strukturze Agencji Bezpieczeństwa Wewnętrznego Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV (The Computer Security Incident Response Team) odpowiada na poziomie krajowym za koordynację procesu reagowania na incydenty komputerowe poprzez wspieranie centralnych podmiotów administracji publicznej oraz operatorów usług kluczowych i infrastruktury krytycznej w zakresie rozpoznawania i przeciwdziałania zagrożeniom cybernetycznym.

Zespół CSIRT GOV prowadzi bieżący monitoring cyberprzestrzeni RP za pomocą narodowego systemu wczesnego ostrzegania o zagrożeniach w sieci Internet oraz reaguje na wszelkie zdarzenia obejmujące m.in. ataki typu DDoS (powodujące niedostępność stron internetowych) czy phishingowe (służące uzyskaniu nieautoryzowanego dostępu do sieci i systemów w celu np. upośledzenia ich pracy lub zniszczenia danych).

Na dedykowanych platformach w sposób ciągły prowadzona jest wymiana informacji o zagrożeniach i incydentach w cyberprzestrzeni RP, m.in. pomiędzy CSIRT GOV a innymi CSIRT-ami szczebla krajowego (CSIRT MON, CSIRT NASK), CSIRT-ami sektorowymi oraz pozostałymi podmiotami krajowego systemu cyberbezpieczeństwa.

Wydawane przez CSIRT GOV komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa służą podwyższeniu świadomości innych użytkowników Internetu (w tym przedsiębiorców) oraz dostarczeniu wskazówek ułatwiających poprawę bezpieczeństwa ich systemów komputerowych.

Do zadań CSIRT GOV należy również przeprowadzanie oceny bezpieczeństwa systemów teleinformatycznych.

Niezależnie od powyższego podkreślić należy, że efektywność funkcjonowania krajowego systemu cyberbezpieczeństwa zależy również od działań przedsiębiorców, w szczególności operatorów usług kluczowych i infrastruktury krytycznej, na których spoczywa obowiązek dbałości o bezpieczeństwo wykorzystywanych przez nich systemów teleinformatycznych.

Z wyrazami szacunku

Tomasz Siemoniak

/-podpisano kwalifikowanym podpisem elektronicznym/