Ministerstwo
Obrony Narodowej

Tarcza WSCHÓD

Sekretarz Stanu
Paweł BEJDA

BMON-WP.053.267.2025/In-105-25/SW
Warszawa, 18.04.2025 r.

Pan Szymon HOŁOWNIA
Marszałek Sejmu Rzeczypospolitej Polskiej

Do wiadomości: Dyrektor Departamentu Spraw Parlamentarnych w KPRM.

ePuap

Dotyczy: interpelacji Pani Poseł Moniki Pawłowskiej nr 8832 w sprawie cyberataku na Szpital MSWiA w Krakowie

Szanowny Panie Marszałku,

odpowiadając, z upoważnienia Ministra Obrony Narodowej, na interpelację Pani Poseł Moniki Pawłowskiej nr 8832 w sprawie cyberataku na Szpital MSWiA w Krakowie, uprzejmie proszę o przyjęcie poniższych informacji.

Obsługą incydentu wskazanego w interpelacji zajmuje się Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego - CSIRT NASK.

W celu wzmocnienia ochrony przed cyberzagrożeniami w Polsce w Ministerstwie Obrony Narodowej, w oparciu o Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC), zbudowany został Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Ministerstwa Obrony Narodowej (CSIRT MON), który monitoruje zagrożenia w cyberprzestrzeni, analizuje i reaguje na incydenty (np. ataki hakerskie, wycieki danych, infekcje złośliwym oprogramowaniem), wspiera inne instytucje w usuwaniu skutków cyberataków, opracowuje zalecenia i procedury poprawiające bezpieczeństwo systemów IT, współpracuje z Ministerstwem Cyfryzacji, Ministerstwem Spraw Wewnętrznych i Administracji, Policją, Agencją Bezpieczeństwa Wewnętrznego i innymi zespołami CSIRT na poziomie krajowym (CSIRT NASK, CSIRT GOV). Zdobywa także doświadczenie na poziomie międzynarodowym dzięki udziałowi w ćwiczeniach NATO np. Locked Shields oraz prowadzeniu wymiany informacji z partnerami z NATO i UE o pozyskanych lukach w zabezpieczeniach czy narzędziach i sposobach ataku przez adwersarzy.

Oprócz opisanych wyżej zadań DKWOC prowadzi szereg działań prewencyjnych, takich jak ciągłe monitorowanie ruchu w wojskowych systemach teleinformatycznych, prowadzenie analizy danych w celu wykrywania anomalii, wczesne ostrzeganie o atakach typu ATP, ransomware czy DDoS. Stosowana jest także wielowarstwowa ochrona w sieci.

Istotne są także szkolenia i ćwiczenia dla żołnierzy i pracowników resortu obrony narodowej i rozwijanie kompetencji dot. ochrony informacji niejawnych poprzez rozwój własnych rozwiązań kryptograficznych. Dzięki między innymi takim działaniom budowany jest kompleksowy system odporności na cyberzagrożenia, który nie tylko chroni infrastrukturę w chwili obecnej, ale też przygotowuje się do jej ochrony w przyszłości.

Z wyrazami szacunku

Paweł BEJDA
/dokument podpisany kwalifikowanym podpisem elektronicznym/

tel.: +48 261 874 432
sekretariat.bmon@mon.gov.pl
www.gov.pl/web/obrona-narodowa

al. Niepodległości 218
00-911 Warszawa