

Podwyższony poziom alarmowy – skuteczna ochrona

90 incydentów i wszystkie skutecznie odparte. Od 11 do 15 lutego, kiedy ze względu na konferencję bliskowschodnią w Warszawie obowiązywał drugi stopień alarmowy w obszarze cyberbezpieczeństwa, odnotowano 90 incydentów cyberbezpieczeństwa. Wszystkie ataki zostały odparte.

CERT Polska (NASK) podsumował okres, w którym obowiązywał podniesiony stopień alarmowy w sieci. Odnotowano 196 zgłoszeń. 90 z nich związanych było z incydentami naruszenia bezpieczeństwa. Dzięki podjętym działaniom wszystkie udało się zneutralizować.

- Obowiązujące od zeszłego roku unormowania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa działają właściwie – podkreśla Marek Zagórski, Minister Cyfryzacji.

Podniesiony poziom bezpieczeństwa (BRAVO-CRP) stanowił okazję do przetestowania współpracy i koordynacji działań zespołów reagowania z różnych obszarów państwa w ramach Krajowego Systemu Cyberbezpieczeństwa. W ocenie podmiotów zaangażowanych w działania w tym obszarze, współpraca przebiegała efektywnie przez cały czas trwania alarmu.

Stan podwyższonego pogotowia oznaczał zwiększoną czujność i więcej pracy dla specjalistów w dziedzinie bezpieczeństwa sieci. W naszej ocenie wdrażany od sierpnia 2018 roku Krajowy System Cyberbezpieczeństwa dobrze spełnił swoją rolę, a kluczowa w tych zadaniach komunikacja między zaangażowanymi podmiotami przebiegała właściwie – podkreśla Krzysztof Silicki, zastępca dyrektora NASK ds. cyberbezpieczeństwa i innowacji.

W praktyce skuteczne działania związane były przede wszystkim z koniecznością

koordynacji działań trzech zespołów CSIRT (ang. Computer Security Incident Response Team) najwyższego, krajowego poziomu. Są to: zespół CSIRT GOV – odpowiedzialny za bezpieczeństwo w sieciach instytucji państwowych i infrastruktury krytycznej, CSIRT MON – sieci resortu obrony narodowej i związane z wojskiem podmioty oraz CSIRT NASK – cywilne firmy, które nie są zaliczane do infrastruktury krytycznej, jednostki samorządu terytorialnego, infrastruktura i usługi cyfrowe.