ABW ZIDENTYFIKOWAŁA PONAD 6 TYS. INCYDENTÓW INFORMATYCZNYCH W 2018 ROKU

6 236 przypadków faktycznego naruszenia bezpieczeństwa teleinformatycznego w instytucjach państwowych odnotowano w 2018 r. - wynika z rocznego raportu działającego w ABW Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV.

Agencja Bezpieczeństwa Wewnętrznego ma w swoich kompetencjach zabezpieczenie informatycznego bezpieczeństwa na poziomie instytucji państwowych. Do zespołu CSIRT zgłaszane są przypadki podejrzenia naruszenia bezpieczeństwa sieci i zasobów informatycznych w instytucjach domeny państwowej.

Według raportu takich zgłoszeń było w 2018 r. prawie 31,8 tys. przy 28,3 tys. w 2017 r. CSIRT GOV w ABW weryfikuje te zgłoszenia i określa, ile z nich nastąpiło faktycznie, a ile to np. część tego samego ataku. W 2017 r. faktycznych incydentów było 5,8 tys. przy 6,2 tys. w ubiegłym roku - wynika z danych ABW.

Najwięcej zgłoszeń o potencjalnych incydentach - 70 proc. pochodzi z własnych systemów wykorzystywanych przez CSIRT GOV w ABW, 27 proc. to zgłoszenia zewnętrzne - od użytkowników sieci rządowej, a pozostałe 3 proc. wynika z własnych ustaleń Zespołu.

Z raportu wynika, że z każdym rokiem rośnie liczba wykrywanych ataków polegających na próbach zawirusowania stacji roboczych, serwerów lub urządzeń sieciowych, m.in. przez złośliwe załączniki w wiadomościach email. W 2018 r. zanotowano ponad 2,4 tys. przypadków, podczas gdy w 2017 r. prawie 1,9 tys., a w 2016 r. 540.

Spada natomiast liczba incydentów spowodowanych złą konfiguracją urządzeń - w 2018 r. było ich 1,1 tys., przy 1,8 tys. rok wcześniej i prawie 4,2 tys. w 2016 r. Złą konfiguracja może stanowić furtkę do przeprowadzenia skutecznego ataku.

W 2018 r. mniej było incydentów spowodowanych skanowaniem urządzeń sieciowych w poszukiwaniu otwartych portów i usług, przez które można złamać zabezpieczenia systemów teleinformatycznych - 636 przypadków. Takie zdarzenia były na poziomie 2016 r., gdy odnotowano ich 661, przy znaczącym wzroście w 2017 r. - ponad 1 tys. przypadków.

Z raportu wynika, że przez stosowany przez ABW automatyczny system wczesnego ostrzegania o zagrożeniach w sieci - ARAKIS 3.0 GOV w 2018 r. zanotowano 320 milionów przepływów danych. Z tej liczby system wyłapał przeszło 424 tys. alarmów, z czego 60 proc. z nich miało poziom informacyjny - niski.

62 tys. alarmów miało rangę pilnych - z wysokim ryzykiem przełamania zabezpieczeń rządowej sieci i urządzeń. Najwięcej razy ARAKIS alarmował o skanowaniu - 60 proc. przypadków, z czego ponad 57

proc. dotyczyło instytucji z kategorii "urzędy" prawie 18 proc. - "ministerstwa", blisko 13 proc. "infrastruktury krytycznej", a prawie 6 proc. "służb i wojska" - wynika z raportu.

W dokumencie wskazano, że z wszystkich zanotowanych przez system przepływów najwięcej należało do Chin (22 proc.) i Stanów Zjednoczonych (19 proc.), ale po raz pierwszy liczba polskich przepływów jest na czwartym miejscu (12 proc.) - przy nieznacznie większej 13 proc. aktywności z adresów rosyjskich w 2018 r.

Autorzy raportu zaznaczają jednak, że te dane należy traktować poglądowo, ponieważ specyfika Internetu pozwala na rozproszone ataki z miejsc w dowolnych państwach.

Raport podaje też, że zespół CSIRT GOV w 2018 r. w ramach zapobiegania terroryzmowi przeprowadził testy systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej. Podczas ocen bezpieczeństwa wykryto podatność na błędy krytyczne w 38 przypadkach, 130 w kategorii wysokiego zagrożenia, 1051 średniego a 166 niskiego - wynika z raportu.

Do sierpnia 2018 r. i wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa zadania ochrony rządowej cyberprzestrzeni należały do Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL przekształconego wówczas w CSIRT GOV. W kraju tę samą rangę co zespół w ABW mają CSIRT MON doglądający sieci wojskowej i CSIRT NASK zajmujący się pozostałym obszarem polskiego internetu.

AK/ABW