

WIELKA BRYTANIA: NAJWIĘKSZE ZAGROŻENIE TO CYBERATAKI INSPIROWANE PRZEZ PAŃSTWA

Cyberataki prowadzone na zlecenie rządów państw - adwersarzy to największe zagrożenie dla bezpieczeństwa Wielkiej Brytanii - oceniło w dorocznym raporcie Narodowe Centrum Cyberbezpieczeństwa (NCSC) wchodzące w skład brytyjskiej agencji wywiadu elektronicznego (GCHQ).

Szef NCSC Ciaran Martin w przedmowie do raportu podkreślił, iż znacząca część wysiłków brytyjskiej agencji w ostatnim roku koncentrowała się na odpieraniu ataków ze strony wrogich aktorów sceny geopolitycznej. Jako państwa stanowiące zagrożenie wymieniono Rosję, Chiny, Iran i Koreę Północną.

Według raportu w ciągu ostatniego roku Wielka Brytania była celem ponad 658 cyberataków na 900 organizacji, w tym - szkoły, lotniska i służby kryzysowe. Pośród metod, które brytyjskie służby zastosowały do walki z cyberprzestępczością, wyróżniono m.in. program Haulstera, który automatycznie oflagowuje podejrzane czynności w bazie informacji o skradzionych kartach kredytowych, co zdaniem agencji przekłada się na wyższy poziom bezpieczeństwa dla setek tysięcy osób chronionych w ten sposób przed oszustwami finansowymi.

W raporcie NSCS czytamy, że cyberprzestępcy wciąż bardzo chętnie korzystają z podatności bezpieczeństwa otwartej platformy handlu elektronicznego Magento. Nadużycia najczęściej mają postać nieuprawnionego przechwytywania danych z kart płatniczych przez skrypty JavaScript, które potrafią pobierać wszystkie dane wpisywane w formularz internetowy osadzony na stronie i wykorzystywany do transakcji. Informacje te przesyłane są następnie na serwery hakerów.

Narodowe Centrum Cyberbezpieczeństwa Wielkiej Brytanii poinformowało, że unieszkodliwiło ponad 1,1 tys. ataków ukierunkowanych na zdobywanie danych z kart płatniczych, z czego 19 proc. zatrzymano w ciągu doby od wykrycia.

Kolejnym obszarem ryzyka zdiagnozowanym przez NCSC w raporcie, są ataki hakerskie na domeny internetowe sektora publicznego i powiązane z nimi adresy poczty elektronicznej. Podczas jednego z opisanych przez służbę incydentów, sprawcy próbowali w ramach oszustwa wysłać 200 tys. fałszywych e-maili podszywających się pod jedno z brytyjskich lotnisk z użyciem nieistniejącego adresu w rządowej domenie.

Atak ten nie powiódł się - podkreślono. Fałszywe e-maile nigdy nie dotarły do odbiorców ze względu na aktywne systemy cyberobrony, które automatycznie wykryły podejrzaną nazwę spreparowanej przez hakerów domeny i zablokowały możliwość dostarczenia przesyłek.

Narodowe Centrum Cyberbezpieczeństwa zostało powołane w 2016 roku w ramach sformowanej przez agencję wywiadu elektronicznego GCHQ strategii nadzoru nad cyberbezpieczeństwem, z budżetem na 1,9 mld funtów. NCSC zajmuje się również działalnością doradczą dla działających w

Wielkiej Brytanii firm i organizacji.