DOCHODZENIE WS. CYBERATAKU NA DEMOKRATYCZNEGO KANDYDATA DO KONGRESU

FBI wszczęło dochodzenie ws. cyberataku na demokratycznego kandydata do Kongresu USA startującego w Kalifornii Davida Mina - poinformowała agencja Reutera powołując się na źródła zbliżone do sprawy. Hakerzy mieli zyskać dostęp do służbowego komputera polityka.

Kandydat przegrał w czerwcu w prawyborach. Informacje o incydencie nie były wcześniej podane do wiadomości publicznej, a cała sprawa została według Reutersa ujawniona dopiero wraz z ukazaniem się materiału w magazynie "Rolling Stone". Znalazły się w nim doniesienia o dochodzeniu w podobnej sprawie dotyczącej cyberataku na kalifornijskiego Demokratę Hansa Keirsteada, który również przegrał w czerwcu prawybory w swoim okręgu.

Reuters podkreśla, że obaj politycy to osoby uważane za kluczowe w wyścigu przed wyborami w listopadzie. Dzięki nim Partia Demokratyczna może przełamać dominację w Kongresie Republikanom - ocenia agencja.

Zdaniem Reutersa, nie jest też jasne, kto stoi za cyberatakami na obu polityków, ani jakie były motywacje hakerów, ostatecznie zaś nie wiadomo również, do jakich informacji udało im się dotrzeć. Szczegóły techniczne ataków podkreślają jednakże istotę obaw ekspertów ds. bezpieczeństwa narodowego. W ich opinii, amerykańskie wybory nie są obecnie zabezpieczone w dostateczny sposób przed ingerencją z zewnątrz, możliwą m.in. za sprawą cyberataków.

Niezależny ekspert ds. cyberbezpieczeństwa i prywatności dr Łukasz Olejnik zwraca uwagę, że w przypadku ataków na obu polityków oprogramowanie antywirusowe na ich komputerach nie wykryło złośliwego oprogramowania używanego przez cyberprzestępców. "Być może antywirus był przestarzały. Hipotetycznie jednak może to wskazywać na bardzo zaawansowany rodzaj ataku" - mówi.

W jego opinii "cyberataki na sztaby wyborcze to już standardowe ryzyko, na które musi być gotowe każde ugrupowanie, w każdej kampanii - choć tu specyfika jest bardzo różna pomiędzy różnymi krajami i rodzajami wyborów. Z innymi zagrożeniami mamy do czynienia w wyborach prezydenckich, parlamentarnych, a z innymi w przypadku samorządowych" - tłumaczy ekspert.

Olejnik ocenia, że zaprojektowanie strategii cyberbezpieczeństwa i bezpieczeństwa informacji dla sztabu wyborczego nie jest łatwym zadaniem. "Trudno zabezpieczyć model organizacji opartej na luźnej współpracy grup i osób wcześniej nie wchodzących ze sobą w interakcje, nie współpracujących" - wyjaśnia. "Jednorazowe szkolenia - nawet, jeśli podnoszą świadomość, nie są środkiem mogącym zapewnić w tym wypadku całkowite bezpieczeństwo" - dodaje.