

ROSYJSKA INFRASTRUKTURA KRYTYCZNA CELEM AMERYKANÓW. RZECZNIK KREMLA MÓWI O „CYBERWOJNIE”

The New York Times informuje, że Amerykanie włamali się do rosyjskich systemów teleinformatycznych w sektorze energetycznym. Miało to być ostrzeżenie dla prezydenta Putina oraz demonstracja jak w praktyce może wyglądać użycie ofensywnych operacji w cyberprzestrzeni, które na mocy ostatnich ataków prawnych stały się łatwiejsze do przeprowadzania. Działania Amerykanów miały również na celu odstraszenie Putina od kolejnych agresywnych kroków.

Informacje, które ujawnił amerykański dziennik The New York Times pochodzą od urzędników obecnej i poprzedniej administracji. Amerykanie mieli umieścić złośliwe oprogramowanie w sieciach energetycznych oraz innych kluczowych obiektach. Miało być ono uruchomione w przypadku sytuacji kryzysowej.

Autorzy artykułu przypominają, że Departament Bezpieczeństwa Wewnętrznego i FBI od dawna informowały, że Rosja umieściła złośliwe oprogramowanie w elektrowniach, systemach sterujących gazociągami i ropociągami oraz systemach zarządzania zasobami wodnymi w Stanach Zjednoczonych. Zdaniem amerykańskich ekspertów mogłyby one zostać użyte przez Rosjan w przypadku konfliktu ze Stanami Zjednoczonymi do paraliżu amerykańskiej infrastruktury. Z tego powodu, wielu ekspertów i polityków apelowało o zajęcie bardziej asertywnego stanowiska przez Stany Zjednoczone.

Czytaj też: [Stany Zjednoczone nie są gotowe do obrony. Eksperci nie mają wątpliwości](#)

W 2012 roku, rosyjskie sieci energetyczne stały się celem Amerykanów, ale badano je pod kątem możliwości znalezienia podatności. Administracja prezydenta Baracka Obamy sprzeciwiała się jednak bardziej asertywnemu podejściu, argumentując, że Stany Zjednoczone są bardziej narażone na cyberataki i w przypadku „cyberkonfliktu” z Rosją stracą o wiele więcej. Obecne działania są o wiele agresywniejsze i obejmują umieszczenie złośliwego oprogramowania w rosyjskich systemach.

Czytaj też: [Stany Zjednoczone najbardziej podatne na cyberataki na świecie](#)

W zeszłym roku uchwalono National Security Presidential Memoranda 13, które dawało o wiele większą swobodę w prowadzeniu operacji ofensywnych w cyberprzestrzeni US CYBERCOM. Administracja prezydenta Trumpa odmawia jednak podania szczegółowych informacji o operacjach, które zostały podjęte na mocy nowych wytycznych. Niedawno doradca ds. bezpieczeństwa

narodowego John Bolton powiedział, że Stany Zjednoczone mogą odpowiedzieć w cyberprzestrzeni na przypadki szpiegostwa. W ostatniej strategii cyberbezpieczeństwa Departamentu Obrony wprowadzono również koncepcję Defence Forward, która zakłada prowadzenie działań obronnych w sieciach państw neutralnych i wrogich. Wielkim zwolennikiem tego podejścia jest generał Paul M. Nakasone, głównodowodzący USCYBERCOM i NSA.

Czytaj też: [USA poszerzają doktrynę ofensywną w cyberprzestrzeni](#)

Według The New York Times operacja wymierzona w rosyjską infrastrukturę energetyczną miała zostać zaakceptowana przez Sekretarza Obrony, który nie potrzebował do tego zgody prezydenta. Co więcej, prezydent Trump miał nie wiedzieć o tej operacji. Wojskowi oraz oficerowie wywiadu nie chcieli informować prezydenta, obawiając się jego reakcji. Nie było to nielegalne, ponieważ operacje w cyberprzestrzeni odbywają się na takiej samej zasadzie jak każda inna aktywność sił zbrojnych.

Profesor prawa Robert M. Chesney z Uniwersytetu w Teksasie nazwał takie działania cyfrowym odpowiednikiem dyplomacji kanonierek. W rozmowie z The New York Times mówi, że kiedyś amerykańskie okręty pojawiały się przy brzegu państwa, z którym był problem, dzisiaj wygląda to w taki sposób, że Amerykanie włamują się do kluczowych systemów energetycznych. W ten sposób wywołują presję dyplomatyczną.

Donald Trump w reakcji na doniesienia gazety, zarzucił The New York Times cyfrową zdradę. Na doniesienia prasowe zareagował również rzecznik Kremla Dmitrij Pieskow, który mówił o hipotetycznej możliwości „cyberwojny” przeciwko Rosji.

Źródło: The New York Times