aut. Andrzej Kozłowski 31.07.2018

CYBERSZPIEGOSTWO - WIRTUALNA BROŃ W WALCE HANDLOWEJ [ANALIZA]

Najnowszy raport Narodowego Centrum Bezpieczeństwa i Kontrwywiadu (NCSC) opisuje działania podejmowane przez Chiny, Rosję i Iran, których celem jest kradzież amerykańskich tajemnic handlowych z wykorzystaniem środków w cyberprzestrzeni. Autorzy raportu szczególnie zwracają uwagę na dostawy zagranicznego oprogramowania. Jest ono często wykorzystywane w działalności szpiegowskiej w środowisku wirtualnym.

China, Rosja i Iran zostały określone jako państwa z największymi zdolnościami do prowadzenia operacji szpiegowskich w cyberprzestrzeni. Są one również najbardziej agresywnymi podmiotami w środowisku wirtualnym i kradną największą liczbę danych gospodarczych oraz informacji o najnowocześniejszych technologiach w Stanach Zjednoczonych. Raport podkreśla, że również inne państwa podejmowały próby wejścia w posiadanie amerykańskiej technologii. Nie wymienia ich jednak z nazwy. Zdaniem autorów publikacji cyberszpiegostwo oferuje możliwość zdobycia szerokiego spektrum własności intelektualnej przy niskich kosztach własnych. Sytuacja ta nie ulega zmianie i to pomimo znaczących inwestycji w cyberbezpieczeństwo.

Chiny poprzez operacje szpiegowskie w cyberprzestrzeni wspierają swój strategiczny rozwój dążąc do pozyskania zaawansowanej technologii oraz usprawnienia systemu edukacji, modernizacji wojska oraz realizacji celów polityki gospodarczej. Operacje w cyberprzestrzeni są częścią skomplikowanej, wielowektorowej strategii rozwoju, która używa legalnych i nielegalnych metod w celu realizacji swoich celów. Chińskie firmy najczęściej nabywają amerykańską technologię w celach komercyjnych i naukowych. Zdaniem autorów raportu zagrożenie to będzie się nasilało i jeżeli nie zostanie znaleziona na nie recepta to może ono zagrozić przewadze technologicznej Stanów Zjednoczonych.

Rosja ma w swoich działaniach skupiać się na kradzieży przede wszystkim technologii wojskowych, które maja umożliwić modernizację jej sił zbrojnych. Ponadto stara się uzyskać informacje, które pomogą jej przeprowadzić gruntowne reformy gospodarcze. Szczególnym zainteresowaniem cieszy się tutaj sektor energetyczny. Raport zauważa również, że Rosja w ostatnim czasie zdecydowanie częściej żąda kodów źródłowych dla zagranicznych rozwiązań technologicznych, które są sprzedawane w kraju.

Iran pomimo tego, że skupia się głównie na atakowaniu wrogów na Bliskim Wschodzie takich jak Arabia Saudyjska czy Izrael, dąży również do pozyskania amerykańskich danych. Celem jest tutaj pobudzenie wzrostu gospodarczego, modernizacja sił zbrojnych oraz zwiększenie sprzedaży międzynarodowej. Atakowane były amerykańskie jednostki badawcze, przedsiębiorstwa naftowe oraz firmy związane z przemysłem lotniczym i kosmicznym. Zarówno w przypadku Iranu i Rosji, autorzy raportu prognozują, że działalność szpiegowska w cyberprzestrzeni będzie kontynuowana. Działalność irańskich i rosyjskich hakerów nie stanowi zagrożenia dla strategicznych interesów Stanów Zjednoczonych.

W przeszłości władze Iranu, Rosji i Chin zaprzeczały, że wykorzystują cyberprzestrzeń do kradzieży własności intelektualnej. Stany Zjednoczone podkreślają, że nie przeprowadzają tego typu operacji.

Autorzy raportu piszą, że ostatni rok był przełomowy jeśli chodzi o incydenty w łańcuchu dostaw. Było ich aż 7, w porównaniu do 4 w latach 2014 – 2016. Wymienia się tutaj atak NotPetya oraz „tylną furtkę" w CClenarze, która zainfekowała ponad 2 milionów klientów i miała być wykorzystywana przez chińskich hakerów. Takie incydenty stanowią zagrożenie dla infrastruktury krytycznej państwa, ale również dla innych sektorów.

W dalszej części raportu autorzy prognozują jakie sektory gospodarki oraz technologie będą z dużą dozą prawdopodobieństwa celem ataku. W sektorze energetycznym będą to m.in. technologie pozyskiwania energii słonecznej i gazu łupkowego, turbiny wiatrowe, inteligentne sieci energetyczne, biopaliwa oraz elektrownie atomowe. Następnym sektorem wymienionym w publikacji jest biotechnologia. Tutaj hakerzy mają być szczególnie zainteresowani zaawansowanymi urządzeniami medycznymi, biomateriałami, nowymi szczepionkami i lekarstwami, genetycznie modyfikowanymi organizmami. W sektorze zbrojeniowym to głównie radary, optyka, systemy morskie oraz lotnicze i kosmiczne. Celem ma również być sektor ochrony środowiska i tutaj wymienia się auta hybrydowe i elektryczne, nowe rodzaje baterii, technologie utylizacji śmieci czy kontroli zanieczyszczenia powietrza i wody. Warto wskazać, że Chiny mają ogromny problem z ochroną środowiska. Przed długi okres kompletnie lekceważyły ten problem. Autorzy raportu wskazują również na zagrożenie dla sektora nowoczesnych technologii. Tutaj hakerów interesować będzie drukowanie 3D, zaawansowana robotyka, silniki samolotów, materiały kompozytowe, technologie kosmiczne, Big Data, Internet Rzeczy, komputery kwantowej i wiele inne.

Dokument zwraca również uwagę, na najnowsze rozwiązania technologiczne takie jak sztuczna inteligencja i Internet Rzeczy, których wprowadzenie spowoduje powstanie nowych podatności dla amerykańskich sieci komputerowych. Na to firmy w Stanach Zjednoczonych nie są gotowe. Autorzy raportu wskazują tutaj na zmiany, które zaszły wraz ze wprowadzeniem technologii chmurowych, zdecydowanie ułatwiając kradzież własności intelektualnej przez różnego rodzaju podmioty.

W wnioskach autorzy raportu stwierdzają, że konieczna jest międzynarodowa dyskusja nad bezpieczeństwem łańcucha dostaw, ponieważ problem jest zagrożeniem dla światowej gospodarki. Dokument ten jest rozszerzeniem raportu dla Kongresu z 2011 roku zatytułowanego „Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, w którym to zarysowano główne wyzwania w cyberprzestrzeni dla przemysłu i nauki.

Dyrektor NCSC William Evanina przyznał, że Stany Zjednoczone nie są gotowe do radzenia sobie z zagrożeniami dla łańcucha dostaw. Dodał, że Chiny łamią postanowienia umowy z 2015 roku pomiędzy prezydentem Barackiem Obamą a jego chińskim odpowiednikiem Xi Jinpingiem. Na jej mocy oba państwa miał powstrzymać się od szpiegostwa gospodarczego w cyberprzestrzeni, Dyrektor przypomniał o wielu aktach i oskarżeniach wystosowanych przez Departament Sprawiedliwości przeciwko chińskim hakerom.

Publikacja raportu zbiega się w czasie z pracami w Kongresie, których celem jest zmniejszenie ryzyka wynikającego ze stosowania zagranicznego oprogramowania komputerowego, w szczególności pochodzącego z państw określanych mianem wrogich. Amerykańskim ustawodawcą udało się wykluczyć z łańcucha dostaw, rosyjską firmę Kaspersky Lab oraz chińskie telekomy Huawei i ZTE. Departament Bezpieczeństwa Wewnętrznego wymusił usunięcie Kaspersky'ego z sieci i systemów wszystkich cywilnych agencji. Z tych trzech firm, raport NCSC wymienia z nazwy tylko rosyjską firmę. Autorzy zwracają jednak uwagę, że zagranicznej firmy komputerowe dostarczają usług wymagających szerokiego dostępu do komputerów i sieci na których są zainstalowane.

Kaspersky w celu uniknięcia dalszych oskarżeń o szpiegostwo, ogłosił w maju, że przenosi część swoich operacji do Szwajcarii. Evanina stwierdził, że ten ruch nie wpłynie w żaden sposób na decyzję amerykańskiego rządu. Niedawno poinformowano również o stworzeniu przez Pentagon tzw. czarnej listy oprogramowania czyli produktów IT, które nie powinne być używane przez Departament Obrony oraz firmy z nim współpracujące.

W tym kontekście warto zastanowić się jak Polska reaguje na ten problem. Huawei – wymieniony w raporcie i od dawna podejrzewany o szpiegostwo i bliską współprace z chińskim wywiadem bierze udział w budowie 5G w Polsce. Używane było również oprogramowanie Kaspersky czy komputery marki Lenovo. W polskich raport i strategii cyberbezpieczeństwa problem bezpieczeństwa łańcucha dostaw nie został poruszony. To nie jest tylko kwestia produktów z państw autorytarnych, ale również z demokratycznych krajów takich jak Stany Zjednoczone. Amerykańskie firmy blisko współpracują z wywiadem, co zostało potwierdzone przez wycieki danych. Dlatego Polska powinna rozwijać jak najwięcej rodzimych technologii w celu budowy własnej cybersuwerenności i kontroli przepływu informacji.