Hakerzy zaatakowali kraj NATO i wykradli miliony danych

25 grudnia 2017

Uwaga – hakerzy wykradli miliony danych. Spora część z nich to loginy i hasła sił zbrojnych jednego z krajów NATO. Dla wszystkich, którzy w ostatnim czasie mówili, że koncepcję cyberwojny można włożyć między bajki, powinien to być kolejny dowód na realne skutki konfliktów w cyberprzestrzeni i ogromne zagrożenie z tym związane.

Bez większego echa w polskich mediach przechodzą informacje o zmasowanym ataku hakerów w Portugalii. Poza krótkimi wzmiankami, możemy znaleźć niewiele informacji na ten temat, a sprawa jest niezwykle poważna. Z pewnością dziennikarze nie wyczuli w tej historii „newsa", ponieważ ich czujność uśpiła informacja lizbońskiego tygodnika „Sabado". Gazeta podała bowiem, że choć same ataki prowadzone były w ciągu ubiegłego roku, portugalskie władze potwierdziły fakt masowej kradzieży danych i ataku na strategiczne struktury teleinformatyczne dopiero w maju tego roku.

Cyberbezpieczeństwo, pomimo licznych publikacji na ten temat cały czas nie jest jeszcze tematem medialnie „chwytliwym", a

szkoda, bo jest to jeden z kluczowych aspektów współczesnego bezpieczeństwa. Należy podkreślić, że ataku na taką skalę nie było już dawno. Cel ataku stanowiły strategiczne urzędy i instytucje takie jak banki, urzędy publiczne, sieci szpitali, poszczególne ministerstwa, policja, a nawet serwery sił zbrojnych.

Z informacji portugalskiej telewizji SIC wynika, że łupem hakerów padły m.in. dane umożliwiające logowanie do kont mailowych najważniejszych portugalskich urzędników, w tym pracowników ministerstw, parlamentu, sądów, prokuratury, policji, banków, szpitali oraz sił zbrojnych. Atak wymierzono również w przedstawicieli portugalskiego rządu oraz linie lotnicze TAP, największego w Portugalii operatora energetycznego – firmę EDP oraz część mediów.

Doprawdy zatrważająca zdaje się być skala samego ataku. Z pewnością nie był to zwykły atak hakerski, lecz raczej prawdziwa zmasowana operacja prowadzona w cyberprzestrzeni przeciwko strategicznym portugalskim urzędom i instytucjom. Co ciekawe okazuje się, że do swoich działań hakerzy wykorzystywali przede wszystkim media społecznościowe i informacje rozpowszechniane z fikcyjnych kont.

O zagrożeniach związanych z tego typu operacjami w cyberprzestrzeni pisałem już w październiku 2017 r. na łamach miesięcznika „Wpis”. Poniżej krótki fragment dotykający sedna problemu: „Już w 1993 roku amerykański socjolog i futurolog Alvin Toffler w swojej głośnej książce „Wojna i antywojna” bardzo obrazowo opisywał początek cyberwojny. Ostrzegał on, że zbagatelizowanie zagrożenia może doprowadzić do sytuacji, w której grupa sprawnych hakerów będzie w stanie doprowadzić cały kraj na skraj finansowego krachu i anarchii, która następnie rozprzestrzeni się na cały świat. Toffler był także przekonany, że wraz z rozwojem technologicznym terrorysta z dowolnego miejsca na świecie będzie mógł wyrządzić znacznie większe szkody posługując się klawiaturą komputera, niż bombą czy karabinem. Jako jeden z pierwszych naukowców, to właśnie

Alvin Toffler już na początku lat 1990. przewidział nadejście nowego gatunku wojny i pojawienie się nowego rodzaju wojowników. Na tym, globalnym polu walki główną rolę miała odgrywać informacja. W celu zrozumienia o jakim polu bitwy mówimy, należy wrócić uwagę na pojęcia takie jak cyberwojna i cyberterroryzm. Są to w zasadzie pojęcia tożsame, choć o cyberwojnie mówimy z reguły w sensie globalnym (w relacji państwo-państwo), a o cyberterroryzmie w sensie lokalnym (w relacji hacker/komórka terrorystyczna-państwo). W obu przypadkach mechanizm działania jest praktycznie taki sam: użycie przez agentów, hakerów lub grupy terrorystyczne informacji oraz systemów teleinformatycznych do ataku w celu przejęcia danych, przerwania lub zniszczenia systemów teleinformatycznych i sieci komputerowych przeciwnika. Cyberwojna odnosi się jednak do ataków (cracków) popełnianych przez państwa. Najbardziej aktualna wydaje się zatem definicja cyberwojny proponowana przez analityka australijskiego departamentu obrony Jerry'ego Everarda, który uważa, że cyberwojna to „skierowane przeciwko komputerowym sieciom dystrybucji operacje informacyjne, przeprowadzane środkami komputerowymi przez przeciwnika na poziomie narodowym". Z cyberterroryzmem mamy natomiast do czynienia, kiedy rodzaje technik hakerskich, stosowanych przez państwa w celu prowadzenia cyberwojny, są przejmowane przez grupy niepowiązane z żadnym rządem. Rozróżnienie obu tych pojęć jest w tym wypadku kluczowe i ma spore znaczenie w kontekście dyplomacji i geopolityki. Już na tym etapie wyłaniają się zatem dwie grupy potencjalnych agresorów: całe państwa oraz pojedyncze komórki hackerów/terrorystów. W celu zabezpieczenia się przed ich działaniami poszczególne kraje dokonały rewolucyjnych zmian w sztuce prowadzenia wojny. Coraz większe znaczenie zaczęła odgrywać możliwość pozyskania informacji niezbędnych do pokonania wroga w możliwie najkrótszym czasie przy minimalnych stratach własnych. Z tych właśnie względów na nowoczesnym polu bitwy pojawiły się szpiegowskie samoloty bezzałogowe, zdalnie sterowane pociski dalekiego zasięgu oraz systemy precyzyjnego celowania i lokalizacji. Można zatem

stwierdzić, że największą rolę we współczesnych działaniach wojennych odgrywa komunikacja komputerowa, której bezpośrednim celem jest całkowite usunięcie żołnierzy z nowoczesnego pola bitwy. Nie oznacza to jednak, że cyberwojna nie ma z klasycznym konfliktem zbrojnym nic wspólnego. W przypadku cyberwojny, tak jak w przypadku klasycznego starcia wojsk występują strony konfliktu i walczący ze sobą żołnierze. Obecnie możemy wyróżnić cztery kraje będące hegemonami na nowoczesnym polu bitwy, są to: USA, Chiny, Rosja oraz Izrael.”

Autorstwo: dr Piotr Łuczuk
Ilustracja: TheDigitalArtist (CC0)
Źródło: Swiato-Podglad.pl