Cyberdefence 24

aut. Andrzej Kozłowski 25.06.2019

LITWA I POLSKA CELEM ATAKU INFORMACYJNEGO. W TLE ĆWICZENIA WOJSKOWE [KOMENTARZ]

W zeszłym tygodniu doszło w Polsce do publikacji nieprawdziwych informacji o ewakuacji mieszkańców przez wojsko amerykańskie i Żandarmerię Wojskową. Okazuje się, że w tym samym czasie do bardzo podobnego incydentu doszło na Litwie. Wydaje się, że działania te były ze sobą skoordynowane.

W zeszłym tygodniu na serwisach niezalezna.pl, epoznan.pl oraz kilku innych pojawiała się informacja o tym, że nastąpi ewakuacja miejscowej ludności ze względu na ćwiczenia Dragon 19. Informowano, że w przypadku odmowy wykonania polecenia MON, może dojść do siłowego wysiedlenia przez sił Military Police wojsk USA. Prawdopodobnie ktoś włamał się na strony serwisów informacyjnych i umieścił tam fałszywy komunikat.

Okazuje się, że w tym samym czasie doszło do podobnego incydentu na Litwie. Sposób działania był bardzo podobny. Włamano się tam na strony niedużych litewskich portali i umieszczono fałszywą informację o zanieczyszczeniu radioaktywnymi materiałami wód na Litwie przez wojska NATO uczestniczące w szkoleniu „Iron Wolf". Dokładnie rzecz biorąc pociski z zubożałym uranem miały wpaść do jednej z miejscowych rzek i skazić wody w rejonie Kowna.

Włamanie się na nieduże polskie i litewskie portale oraz umieszczenie fałszywych informacji to kolejna próba skompromitowania NATO. Termin operacji również nie jest przypadkowy, ponieważ zbiegł się w czasie z ćwiczeniami „Iron Wolf" na Litwie oraz ćwiczeniami Dragon-19 w Polsce. W przeszłości wielokrotnie żołnierze NATO, stacjonujący na wschodniej flance, byli ofiarą różnego rodzaju operacji dezinformacyjnych. Odpowiadać mieli za gwałty czy pobicia. Wcześniej w wyniku włamania na serwis epoznan.pl opublikowano fałszywą historię, że amerykański żołnierz jest poszukiwany za zabójstwo polskiego kolegi. Informacje powieliły również inne portale informacyjne.

Incydenty, które miały miejsce w Polsce i na Litwie stanowią połączenie cyberataków – włamanie się na stronę internetową, prawdopodobnie ze względu na jej błędną konfigurację oraz operacji informacyjnej – umieszczenie fałszywej wiadomości. Wydaje się, że operacje były ze sobą skoordynowane. Celem takich działań informacyjnych jest przedstawienie Sojuszu w jak najgorszym świetle, a jego żołnierzy jako barbarzyńców, aby obniżyć popularność i zaufanie do NATO w społeczeństwie.

Ze względu na naturę cyberprzestrzeni bardzo trudno jest wskazać potencjalnego napastnika. Biorąc jednak pod uwagę motyw i cel działań, pojawia się potencjalny podmiot, który mógł stać za taką operacją – Rosja. Państwo to określa NATO jako przeciwnika, a obecność wojsk Sojuszu na wschodniej flance traktuje jako zagrożenie. Ponadto analiza lingwistyczna wskazuje, że fałszywa wiadomość opublikowana na polskich portalach została stworzona przez osobę, której językiem ojczystym jest rosyjski. Zła odmiana wyrazów, stosowanie konstrukcji jak „epizod praktyczny" czy „łagr" zamiast obóz wskazują na język rosyjski. Nie oznacza to jednak, że operacja została przeprowadzona przez

rosyjskie służby. Mały profesjonalizm działań raczej to wyklucza. Mogła to być jednak grupa sympatyzująca z reżimem Putina pochodząca z Rosji, ale sympatyzująca z mniejszością rosyjską w państwach bałtyckich. Na szczęście tego typu incydenty, pomimo tego, że się pojawią dość często nie odnoszą praktycznie żadnego skutku i popularność NATO wcale nie spada. Według badań CBOSu z marca 2019 roku, 67 proc. społeczeństwa popiera stacjonowania wojsk NATO w Polsce. Społeczeństwa Litwy i Polski są świadome, kto stanowi prawdziwe zagrożenie i wiedzą również, że stacjonujący żołnierze Sojuszu są sojusznikami. Prawie 70 proc. osób wierzy, że NATO będzie bronić Polski - wynika z tych samych badań CBOSu. W walce z dezinformacją ważna jest rzetelna polityka informacyjna NATO, wyjaśniająca powody stacjonowania żołnierzy. Takie działania informacyjne powinny być kontynuowane, wzmacniając odporność społeczeństwo na działania dezinformacyjne.