SPRAWA NIEWIECHOWICZA OBNAŻA LUKI POLSKIEGO SYSTEMU BEZPIECZEŃSTWA INFORMACYJNEGO

Prowokacja dziennikarska Jakuba Wiecha i Piotra Maciążka polegająca na stworzeniu fikcyjnego eksperta obnaża słabość bezpieczeństwa informacyjnego Polski oraz pokazuje brak świadomości zagrożeń informacyjnych wśród polityków, dziennikarzy oraz członków administracji publicznej. Jeżeli profesjonalne podmioty zdecydowałby się na zaawansowaną operację, wykraczającą poza tak ograniczone działania, jakie były wykorzystane przez dziennikarzy Energetyka24.com, to jej skutki mogłyby być opłakane.

Dziennikarze

W obecnych czasach, praktycznie każdy może w krótkim czasie zostać dziennikarzem, dzięki łatwemu dostępowi do informacji oraz środków dystrybucji. Dlatego profesjonaliści w branży powinni odgrywać szczególną rolę. Coraz częstsze występowanie fałszywych informacji, czyli tzw. fake newsów powoduje, że istotniejsze staje się weryfikowanie treści oraz źródeł. Wykorzystanie przez uznane portale tekstów od nieznanych bliżej osób, gdzie kontakt ogranicza się tylko do komunikacji online jest tylko jednym z przykładów negatywnych tendencji. Konto na Twitterze, Facebooku czy LinkedIn jest banalnie łatwe do stworzenia, ale co więcej, należy także pamiętać, że nawet te autentyczne mogą zostać przejęte przez hakerów praktycznie w dowolnym momencie. W przeszłości udało się im włamać chociażby na konto Twitter U.S. Central Command czy amerykańskiej agencji prasowej Assiociated Press.

Dodatkowo brak sprawdzenia materiału pod kątem merytorycznym przed jego publikacją w popularnym miejscu powoduje, że dane medium może stać się nieświadomie tzw. pudłem rezonansowym, biorąc czynny udział w operacji informacyjnej lub psychologicznej i może przyczynić się świadomie lub nie do kryzysu, nawet na szczeblu państwa lub w taki czy inny sposób pomóc infoagresorowi w realizacji jego celów wobec danego audytorium. Szczególną atencją powinny w związku z tym zostać otoczone strategiczne oraz wrażliwe sektory, od których zależy bezpieczeństwo państwa, takie jak np. sektor energetyczny, przemysł obronny, ale i inne podmioty, w tym i same media lub instytucje państwowe.

Działania propagandowe lub dezinformacyjne w cyberprzestrzeni doprowadzały już do wybuchu zamieszek w Stanach Zjednoczonych, wpływały na wynik wyborów jak w Stanach Zjednoczonych w 2016 roku czy powodowały kryzysy dyplomatyczne jak to miało miejsce w Katarze. Dlatego społeczna odpowiedzialność dziennikarzy za publikowanie informacji oraz ich rozpowszechnianie w dobie trwającej wojny informacyjnej jest niezwykle ważna.

Czytaj też: Śmierć papieża na Twitterze: Nie fake newsy są problemem, a brak higieny w pracy z

informacją [KOMENTARZ]

Fałszywa informacja o sprzedaży Mistrali za jednego dolara Rosji przez Egipt, rozpowszechniony Tweet o śmierci Benedykta XVI to tylko wybrane przykłady potwierdzające brak świadomości zagrożeń wśród dziennikarzy. Należy jednak pamiętać, że prawdziwym zagrożeniem dla polskiej przestrzeni informacyjnej nie są fake newsy, z którymi stanowiąca największe zagrożenie propaganda Kremla pracuje stosunkowo rzadko. Znacznie bardziej niebezpieczne jest instalowanie narracji, które jest tym łatwiejsze, im wyższy jest w danym kraju poziom polaryzacji społecznej czy brak zaufania do klasycznych mediów. Odbywa się to na różne sposoby, najczęściej jednak poprzez tzw. autorytety moralne lub liderów opinii w określonych środowiskach, tzw. influencerów. Mogą to być podmioty krajowe lub zagraniczne. Niestety sprawa Niewiechowicza pokazuje, jak potencjalnie łatwo stworzyć jest eksperta w danej strategicznej branży, który potencjalnie może zostać w dłuższej perspektywie jeżeli nie liderem opinii, to wpływowym uczestnikiem debaty wewnętrznej. Przykłady z USA pokazują, że możliwe jest dla fikcyjnego użytkownika osiągnięcie poziomu międzynarodowego.

Czytaj też: Amerykańska blogerka tworem farmy trolli z Petersburga

Konieczne jest szkolenie, uświadamianie i uczulanie konkretnych grup zawodowych na kwestie zagrożeń związanych z oddziaływaniami informacyjnymi i psychologicznymi. Szczególna rola dziennikarzy w społeczeństwie wymaga zmiany podejścia do wielu kwestii i adaptacji do zmieniającego świata informacyjnego. Potrzeba nie tylko nauczyć się efektywnego wykorzystywania mediów społecznościowych, a przede wszystkim dowiedzieć się o ograniczeniach i zagrożeniach związanych z tymi narzędziami. Pożądane jest również zatrudnianie w redakcjach osób, odpowiedzialnych tylko za kontrolę treści. Dziennikarze muszą być świadomi, że *de facto* są niezwykle istotnym elementem całego systemu, który składa się na bezpieczeństwo informacyjne kraju, a ich błędy lub brak profesjonalizmu mogą zostać wykorzystane przez wrogie podmioty, których celem może być np. destabilizacja sytuacji w kraju.

Czytaj też: Światowe media i propaganda Kremla: przypadek samobójstwa ukraińskiego pilota [ANALIZA]

Administracja państwa i politycy

Zaniedbania edukacyjne w obszarach bezpieczeństwa informacyjnego oraz cyberbezpieczeństwa w administracji publicznej i wśród polityków były widoczne już wielokrotnie. Warto wspomnieć przykłady polityków, którzy mieli przyczepioną do swojego laptopa karteczkę z loginem i hasłem czy też liczne, nieprofesjonalne wypowiedzi podczas protestów przeciwko ACTA. Sprawa Niewiechowicza dokłada do tego kolejną cegiełkę. Przekazywanie informacji o strategicznym projekcie przez urzędnika państwowego do konta na Twitterze można porównać do wysłania tych wiadomości na skrzynki pocztowe wywiadów obcych państw. Trzeba to jeszcze raz wyraźnie powtórzyć, że za takim profilem może stać każdy. W administracji państwowej poza obowiązkowymi szkoleniami na wysokim poziomie potrzebna jest również skuteczniejsza kontrola informacji oraz regulowanie dostępu do nich. Ponadto należy wdrożyć kodeks wykorzystania mediów społecznościowych i wyraźnie ostrzec o możliwych konsekwencjach i zagrożeniach płynących z ich użytkowania. To w końcu nie są prywatne konta nieznanych osób, ale konta urzędników państwowych lub polityków.

Sprawa Niewiechowicza ma szerszy kontekst, niż zachowania pojedynczych dziennikarzy czy pracowników administracji państwowej. Chodzi o bezpieczeństwo państwa, procedury, konkretne

rozwiązania instytucjonalne, ale przede wszystkim edukację i popularyzację zmiany nawyków i zachowania w sieci. Musimy zmienić sposób myślenia o bezpieczeństwie państwa, ale i o tym indywidualnym i zrozumieć, że każdy użytkownik sieci jest w większym lub mniejszym stopniu uczestnikiem informacyjnego pola bitwy. W świecie wirtualnym podział na walczących i cywilów praktycznie się zaciera. Przebywając w tzw. silosach informacyjnych, definiowanych przez język, światopoglądy czy ideologię, możemy nie dostrzegać szerszego obrazu i szeregu zagrożeń dla nas samych, które taka sytuacja powoduje.

Świadomi użytkownicy sieci czy odbiorcy informacji mogą najskuteczniej wzmocnić odporność kraju, jego cyberprzestrzeni i przestrzeni informacyjnej, redukując obszary podatności i neutralizując możliwość działań hybrydowych prowadzonych przez podmioty zewnętrzne, ale i potencjalnie wewnętrzne. Aby to się jednak stało musimy usprawnić i przyspieszyć adaptację do nowych wyzwań w obszarze bezpieczeństwa i cyberbezpieczeństwa. Warto czerpać wzorce z rozwiązań w innych państwach. Wydaje się, że rozwiązania przyjmowane przez państwa skandynawskie mogą tutaj być stawiane za pozytywny przykład do naśladowania. Edukacja i budowanie świadomości musi rozpocząć się na już na wczesnym etapie, np. szkoły podstawowej, a najlepiej jeszcze wcześniej. Czerpiąc z wzorców naszych sojuszników, warto rozważyć rozpoczęcie tych procesów od nauczania krytycznego myślenia i bezpieczeństwa w sieci poprzez bajki czy kreskówki dla dzieci. Konieczne jest jednak jej kontynuowanie i rozszerzanie również dla osób dorosłych, ponieważ niestety cały czas mamy do czynienia z sytuacją, że Twitter czy inne media społecznościowe traktowane są przez polityków, dziennikarzy czy ekspertów instrumentalnie i bez należytej rozwagi. Jak pokazały jednak liczne przykłady, a zwłaszcza wybory prezydenckie w USA, mogą się one stać groźną bronią.

Wnioski

Od lat coraz szerzej analizowane i komentowane są kwestie zagrożeń hybrydowych, cyberbezpieczeństwa, wojny informacyjnej czy oddziaływań psychologicznych, a państwa przywiązują coraz większą wagę do rozwiązań prawno-administracyjnych, aby im przeciwdziałać. Widać jednak, że to wciąż za mało. Najsłabszym ogniwem każdego systemu bezpieczeństwa pozostaje człowiek. Niski poziom świadomości zagrożeń oraz wysoki poziom polaryzacji w społeczeństwie znajdują swoje odzwierciedlenie w funkcjonowaniu państwa. Mamy tu do czynienia nie tylko z problemem nieprzestrzegania lub braku procedur bezpieczeństwa na poziomie administracyjnym kraju. Wyraźnie widać, że mamy jeszcze wiele do zrobienia w obszarze edukacji społecznej, popularyzacji bezpiecznych zachowań i nawyków w sieci, zwłaszcza krytycznego myślenia, ale i zacieśniania współpracy pomiędzy instytucjami państwowymi a społeczeństwem obywatelskim. Budowa odporności społecznej, czyli societal resilience jest odpowiedzią na tego typu wyzwania. Trzeba bowiem pamiętać, że kontekstem dla tej sytuacji będzie nie tylko rosyjskie zagrożenie pozamilitarne. Działania związane z oddziaływaniem psychologicznym czy informacyjnym mogą być przeprowadzone także przez inne podmioty, zarówno państwowe, niepaństwowe, jak i prywatne, w tym także zlokalizowane na własnym terytorium. Nasze bezpieczeństwo zależy w pierwszej kolejności od nas samych, a dbając o nie, zwiększamy też odporność państwa na zagrożenia wewnętrzne i zewnętrzne.

Sprawa dziennikarskiej prowokacji, która celowo nie była zbytnio zaawansowana technicznie, nie powinna zostać absolutnie zlekceważona. Zbliżają się wybory samorządowe, które mogą być celem skoordynowanych operacji psychologicznych i informacyjnych prowadzonych przez podmioty zewnętrzne, o wysokim poziomie finansowania i organizacji. Z takich sytuacji jak ta powinniśmy wyciągać wnioski, które nas wzmacniają, pamiętając o tym, co mówią eksperci NATO – „jesteśmy tak silni, jak nasze najsłabsze ogniwo”.

Opracowali: dr Andrzej Kozłowski i dr Adam Lelonek – prezes Centrum Analiz Propagandy i Dezinformacji