aut. Andrzej Kozłowski 02.10.2020

CZY USCYBERCOM JEST W STANIE PORADZIĆ SOBIE Z KAŻDYM WYZWANIEM? AMERYKAŃSKIE PRZYGOTOWANIA PRZED WYBORAMI

Wyciągnęliśmy wnioski z wyborów z 2016 roku. Jesteśmy lepiej przygotowani na potencjalne wrogie działania mówi Mellisa Hathway, doradczyni ds. cyberbezpieczeństwa administracji George W. Busha i Baracka Obamy. Ekspertka komentuje również ostatnie zawirowania wokół TikToka oraz wskazuje na największe wyzwania stojące w obszarze cyberbezpieczeństwa przez następną ekipą prezydencką.

Jak Stany Zjednoczone przygotowują się na potencjalną ingerencję w nadchodzące wybory prezydenckie?

Stany Zjednoczone podjęły liczne środki zaradcze, które mają zagwarantować, że nie dojdzie do naruszenia integralności wyborów, a sam proces liczenia głosów nie zostanie zakłócony. Mamy jednak do czynienia ze znaczącą liczbą kampanii dezinformacyjnych oraz zalewem informacji wprowadzających w błąd. Podważają one np. wiarygodność głosowania korespondencyjnego. Dlatego tak ważne jest przygotowanie jasnych i przejrzystych procedur dla obywateli oraz odpowiedniej dokumentacji dotyczącej tego rodzaju głosowania.

Jakie są szanse na powtórzenie scenariusza z 2016 roku, kiedy to wybory stały się celem zmasowanych operacji informacyjno-psychologicznych?

W 2016 roku wyniki głosowania nie zostały zmanipulowane, to ludzie padli ofiarą dezinformacji i propagandy. Moim zdaniem obecnie tyle mówimy o zagrożeniach informacyjnych, że ludzie stają się coraz bardziej świadomi i lepiej rozumieją ten problem. Ponadto platformy mediów społecznościowych podjęły liczne środki, aby zredukować ryzyko oszustów i manipulacji. Można powiedzieć, że jesteśmy lepiej przygotowani niż w 2016 roku.

Administracja Donalda Trumpa wprowadziła wiele nowych rozwiązań i inicjatyw w polityce cyberbezpieczeństwa. Jak Pani zdaniem można ocenić dokonania tego prezydenta w obszarze polityki cyberbezpieczeństwa?

Pierwszym krokiem administracji Trumpa było wydanie rozporządzenia wykonawczego, którego zadaniem była identyfikacja rzeczy, które muszą być zrobione. Następne akty prawne wydawane przez prezydenta wzmocniły nasze siły zbrojne i umożliwiły im podejmowanie działań umożliwiających lepszą ochronę Stanów Zjednoczonych. Wreszcie administracja wydała także rozporządzenie wykonawcze dotyczące zabezpieczenia łańcucha dostaw czy integralności infrastruktury energetycznej, która nabrała priorytetowego znaczenia. Wciąż jednak pozostaje dużo do zrobienia, w szczególności w odniesieniu do obszaru cyberbezpieczeństwa i innych kluczowych sektorów.

Wielu osób wskazuje, że wybory do Kongresu w 2018 roku były bezpieczne dzięki wzmocnieniu mandatu USCYBERCOM. Jak Pani ocenia rosnące znaczenie tej jednostki dla bezpieczeństwa narodowego USA?

Nowa strategia USCYBERCOM, która pozwala na podejmowanie agresywniejszych działań z pewnością okazała się pomocna w przeciwdziałaniu ingerencji w infrastrukturę wyborczą podczas wyborów w 2018 roku. Nie jestem jednak pewna, czy USCYBERCOM jest w stanie poradzić sobie z każdym wyzwaniem, które napotkają Stany Zjednoczone. Codziennie musimy mierzyć się z wrogą aktywnością w naszych sieciach. Są one atakowane przez Iran, Chiny, Rosję czy Koreę Północną i nie jestem pewna czy jedno dowództwo wojskowe jest w stanie sobie z tym poradzić.

Jednym z punktów zapalnych w relacjach amerykańsko-chińskich jest kwestia zablokowania udziału Huawei na amerykańskim rynku oraz próby ograniczenia działalności TikToka i WeChata. Czy faktycznie mówimy tutaj o zagrożeniu dla obywateli USA i bezpieczeństwa narodowego czy może jest to element wojny handlowej z Chinami?

W maju 2019 roku prezydent Trump wydał rozporządzenie wykonawcze na temat bezpieczeństwa łańcucha dostaw, które umożliwia mu zablokowanie wybranych podmiotów stanowiących zagrożenie dla bezpieczeństwa narodowego. Stworzono listę firm, które takie zagrożenie mogą stanowić i znalazł się tam m.in. Huawei. Chińska Partia Komunistyczna może nakazać chińskim firmom kradzież danych czy zablokowanie przesyłania informacji i komunikacji. Administracja Trumpa stwierdziła, że WeChat i TikTok zbierają informacje i profilują Amerykanów a dane przesyłają do Chin. W przypadku WeChata jest to prawda, ale informacje zbierane przez TikToka są przechowywane w Stanach Zjednoczonych i Singapurze. Moim zdaniem, popularna pośród młodzieży chińska aplikacja nie stanowi zagrożenia dla bezpieczeństwa narodowego i działania wymierzone przeciwko tej platformie to czysta polityka warunkowana osobistą niechęcią prezydenta Trumpa, który nie zdobył na niej odpowiedniej popularności .

Jakie zagrożenie w takim razie stanowi Huawei?

Huawei jest jednym z 5 największych dostawców sprzętu telekomunikacyjnego, który w przeszłości otrzymał wiele wsparcia od chińskiego rządu m.in. w dostępie do rynku czy subsydiowania cen. Australijczycy przeprowadzili badania pokazujące, że Huawei może na polecenie rządu zdobyć informacje przesyłane za pomocą jego infrastruktury lub zapewnić dostęp chińskiemu rządowi do swoich platform. Dlatego też, firma ta stanowi zagrożenie dla bezpieczeństwa narodowego i nie tylko dla naszej zdolności do komunikowania się, ale również dla cyfrowej gospodarki.

Jakie powinny być priorytety następnej administracji, która zasiądzie w Białym Domu w obszarze cyberbezpieczeństwa?

Obecnie głównym problemem jest wzrastająca liczba oprogramowania ransomware i problemy z infrastrukturą komunikacyjną, dlatego następna administracja powinna zainwestować znaczne środki w infrastrukturę komunikacyjną. Praca oraz nauka zdalna uświadomiła nam, że nie mamy stabilnej infrastruktury i co chwile zdarzają się przerwy w dostawach. Ostatnio Google i IBM miały poważne problemy z zapewnieniem ciągłości dostaw. Wiele z naszych przedsiębiorstw zostało również w ostatnim czasie zaatakowanych złośliwym oprogramowaniem ransowmare pochodzącymi z Rosji i Korei Północnej. Widzimy niepokojący trend wzrastającej liczby ataków z wykorzystaniem tej metody, co stanowi ryzyko dla stabilności gospodarczej kraju. Uważam, że te dwa problemy powinny być priorytetami dla nowej administracji.