WARSZAWSKI INSTYTUT
INICJATYW STRATEGICZNYCH

CYBERBEZPIECZEŃSTWO W ERZE DONALDA TRUMPA

CYBERBEZPIECZEŃSTWO stało się jednym z głównych tematów prezydenckiego wyścigu do Białego Domu w 2016 roku. Nie było to jednak spowodowane ambitnymi i rewolucyjnymi propozycjami kandydatów, ale ingerencją rosyjskich hakerów w proces wyborczy w Stanach Zjednoczonych. Jakie działania ma zamiar podjąć prezydent Donald Trump, żeby podobna sytuacja nie miała już miejsca? Czego można spodziewać się po polityku, uchodzącym za nieprzewidywalnego, także w obszarze bezpieczeństwa teleinformatycznego?

WZMOCNIENIE OBRONY

Stany Zjednoczone są jednym z najczęściej atakowanych cybernetycznie krajów na świecie. Podczas kadencji prezydenta Obamy, doszło do wielu spektakularnych włamań i operacji wrogich hakerów. Wymienić należy choćby kradzieże materiałów o amerykańskich systemach bojowych, dane pracowników federalnych czy ostatnio informacje z Komitetu Partii Demokratycznej.

Po raz pierwszy swoje pomysły na wzmocnienie obrony sieci Donald Trump zaprezentował na konwencji Partii Republikańskiej w lipcu 2016 roku. Zwrócono uwagę na przestarzałe i źle zabezpieczone systemy komputerowe sieci energetycznych, które należy poddać gruntowanej modernizacji. Postulat ten w żaden sposób nie jest oryginalny, ponieważ prawie w każdym raporcie poświęconym cyberbezpieczeństwu, poruszano kwestię wzmocnienia infrastruktury krytycznej. Przy czym problem leży nie tylko w przestarzałych sieciach komputerowych, ale również we wdrażaniu obecnie coraz bardziej skomputeryzowanych procesów i narzędzi w sektorze energetycznym bez odpowiednich środków bezpieczeństwa. Zwielokrotnia to liczbę potencjalnych celów dla strony chcącej przeprowadzić taki atak. Ważnym i często pomijanym aspektem jest bezpieczeństwo łańcucha dostaw i sprzętu komputerowego, które zostało uwzględnione w agendzie Partii Republikańskiej. Nie przytoczono jednak żadnych szczegółów.

WZROST LICZBY MIEJSC PRACY

Na konwencji Partii Republikańskiej w lipcu 2016 roku stwierdzono też, że od zapewnienia cyberbezpieczeństwa zależy wzrost gospodarczy i liczba miejsc pracy. Tutaj propozycje Trumpa mogą stanowić zagrożenie. Jego administracja planowała zmniejszenie liczbę wiz typu H1B, które są wydawane osobom wykonującym specjalistyczne prace okresowe na terenie Stanów Zjednoczonych. Zdaniem niektórych ekspertów może to doprowadzić do zmniejszenia liczby ekspertów od cyberbezpieczeństwa w Stanach Zjednoczonych. Biorąc pod uwagę, że w tej branży popyt zdecydowanie przerasta podaż, może to być dodatkowym problemem. W końcu od dawna administracja federalna próbuje znaleźć sposób na zachęcenie ludzi do studiowania problematyki cyberbezpieczeństwa.

AGRESYWNA POLITYKA KLUCZEM DO SUKCESU?

Donald Trump jawi się jako polityk, który nie zawaha się użyć wszystkich środków, które posiadają Stany Zjednoczone do obrony amerykańskiego interesu. Pogląd ten znajduje również odzwierciedlenie w cyberprzestrzeni. Już w lipcu 2016 na Konwencji Partii Republikańskiej w przyjętej agendzie stwierdzono, że użytkownicy mają prawo do samoobrony w cyberprzestrzeni, w każdy sposób, który uznają za efektywny w danej sytuacji. Nie wykluczono tutaj tzw. kontr-hakowania polegającego na namierzeniu atakującego i włamaniu się do jego komputera. Wielu ekspertów krytykuje to rozwiązanie wskazując na to, że

doprowadzi ono do niekontrolowanej wymiany ciosów w cyberprzestrzeni. W tym samym dokumencie, Republikanie wyrazili poparcie dla sankcji dyplomatycznych, finansowych i prawnych przeciwko państwom dokonującym cyberataków. Wymieniono nawet możliwość odrzucania wniosków wizowych czy zamrażania środków finansowych. Przejście do działań ofensywnych ma być konieczne, żeby uniknąć cyfrowego Pearl Harbour. Prezydent Trump wyraźnie podkreślał, że zamierza zwiększyć rolę US CyberCommand odpowiedzialnego za operacje wojsk amerykańskich w cyberprzestrzeni.

Partia Republikańska podkreśliła również konieczność osłabiania kontroli internetu przez reżimy stosujące cenzurę oraz promowanie wolnej i otwartej cyberprzestrzeni. Jest to interesujący postulat, biorąc pod uwagę, że prezydent Trump wielokrotnie pozytywnie wypowiadał się na temat liderów państw autorytarnych.

O rozbudowie środków ofensywnych, Trump informował na swojej stronie internetowej, na której przedstawiał planowaną politykę. Zapowiedział rozbudowę USCYBERCOM oraz dalszy ciąg rozwoju zdolności ofensywnych w celu walki zarówno z aktorami państwowymi, jak i niepaństwowymi. W szczególności podkreślił konieczność efektywniejszej walki z organizacjami terrorystycznymi. Jego zdaniem broń cyfrowa powinna stanowić główny oręż w walce z terrorystami paraliżując ich działania propagandowe oraz rekrutacyjne.

Rozbudowane zdolności cyberofensywne mają pozwolić na wyprowadzenia niszczących kontrataków, które będą używane jako narzędzie odstraszania. Ten pogląd jest dość osobliwy, ponieważ Stany Zjednoczone już posiadają najbardziej zaawansowany arsenał broni cyfrowej. Problemem w zastosowaniu koncepcji odstraszania jest przede wszystkim zlokalizowanie atakującego.

OSOBY

Nawet najlepsze pomysły nie zostaną zrealizowane, jeżeli osoby odpowiedzialne za cyberbezpieczeństwo nie rozumieją tego tematu i nie dostrzegają znaczenia problemu. Donald Trump jako prezydent będzie w tym obszarze podejmował najważniejsze decyzje. Jego początkowe wypowiedzi wskazywały na jego niewielką wiedzę w tym zakresie. Wydaje się jednak, że wraz z trwaniem kampanii wyborczej zgłębiał tę tematykę. Słusznie zauważył, że obrona przed cyberatakami jest bardzo trudna do zrealizowania. Zapowiedział również, że jego administracja będzie pracowała nad ulepszeniem narodowego systemu cyberbezpieczeństwa i ma to być jeden z priorytetów jego prezydentury. Trump oskarżył też Chiny, Rosję, Koreę Północną oraz organizacje terrorystyczne i przestępcze jako głównych sprawców cyberataków. Wiedza i umiejętności prezydenta są niezwykle istotne w kwestiach związanych z cyberbezpieczeństwem. Bill Clinton i George W. Bush nie byli specjalnie zainteresowani tą tematyką, dlatego też nie odgrywała ona istotnej roli za czasów ich urzędowania. Dopiero Barack Obama, który zdecydowanie lepiej rozumiał omawianą problematyką uczynił z cyberbezpieczeństwa jeden z priorytetów w obszarze bezpieczeństwa.

W prowadzeniu skutecznej polityki nieodłączną rolę odgrywają doradcy i to od nich zależy często kształt podejmowanych działań. Wśród najbliższych osób doradzających Trumpowi w kwestiach cyberbezpieczeństwa jest Karen Evans, która ostatnio stała na czele organizacji U.S. Cyber Challenge. Rolę tzw. cybercara powierzono byłemu burmistrzowi Nowego Yorku Rudiemu Giullianiemu, który ma na tym polu bardzo małe doświadczenie. Z drugiej jednak strony nominacja Giullianiego, który uchodzi za ważną postać w amerykańskiej polityce, może świadczyć o poważnym traktowaniu problemu. Nie można też zapominać o Tomie Bossercie, doradcy prezydenta George'a W. Busha ds. cyberbezpieczeństwa. Sprawował on również funkcję w Atlantic Council, zajmując się tematyką cyberbezpieczeństwa oraz prowadził własną firmę doradczą z zakresu szeroko pojętego bezpieczeństwa. Jak widać doradcy Trumpa, to osoby z dużym doświadczeniem w sprawach związanych z cyberbezpieczeństwem albo jak w przypadku Giullianiego doświadczone w pracy w administracji państwowej.

Niestety ani przyszły szef CIA ani sekretarz obrony James Mattis nie wykazują wystarczającego zainteresowania cyberbezpieczeństwem. Podczas ich przesłuchania w Kongresie, temat ten został zmarginalizowany i potraktowany bardzo ogólnie.

DECYZJE

Trump zapowiedział, że powoła zespół przeglądowy ds. cyberbezpiezczeństwa. Na podobny ruch zdecydował się wcześniej jego poprzednik. Wtedy też zespół pod przewodnictwem Melissy Hathaway sporządził szereg rekomendacji, które były realizowane przez Obamę. Trump oznajmił, że jego zespół składać się ma z cywilów, wojskowych oraz przedstawicieli sektora prywatnego. Głównym zadaniem ma być znalezienie podatności w systemach rządowych, w szczególności skupiając się na priorytetowych obszarach. Trump zapowiedział również cykliczne przeglądy bezpieczeństwa oraz stworzenie rekomendacji dostosowanych do potrzeb każdej agencji oraz urzędów federalnych i zagrożeń, z którymi się mierzą. Dodatkowo mają zostać wdrożone protokoły bezpieczeństwa oraz obowiązkowe szkolenia zwiększające świadomość w cyberprzestrzeni wśród administracji federalnej. Zespół ma zakończyć pracę w ciągu 90 dni.

45. prezydent Stanów Zjednoczonych zadeklarował również utworzenie wszechstronnego planu ochrony infrastruktury krytycznej. Nie podał jednak żadnych szczegółów działań, które ma zamiar podjąć. Podkreślił jedynie, że dużą rolę odgrywać ma Kolegium Połączonych Szefów Sztabów oraz wojsko. Pomysł ten wydaje się być nienajlepszym rozwiązaniem, ponieważ siły zbrojne ze względu na obowiązujące prawo mają ograniczone możliwości ochrony elementów infrastruktury krytycznej, które znajdują się na terytorium Stanów Zjednoczonych. Co więcej podjęte przez Baracka Obamę próby uczynienia z USCYBERCOM głównej jednostki odpowiedzialnej za monitorowanie sieci zakończyły się niepowodzeniem na skutek głośnych protestów ze strony przedstawicieli amerykańskiej Izby Handlowej (US Chamber of Commerce). Ponowienie tych starań czy też inna ingerencja wojska w ochronę cywilnych struktur przed cyberatakami skończy się z pewnością podobnym skutkiem.

Na stronie prezydenta możemy przeczytać również o planach stworzenia przez Departament Sprawiedliwości Połączonego Zespołu Zadaniowego (Joint Task Forces), który będzie koordynował działania federalnych, stanowych i lokalnych organów egzekwowania prawa. Trump argumentując konieczność utworzenia takiej struktury posłużył się przykładem walki z mafią. Wtedy to Departament Sprawiedliwości wraz z FBI, DAE oraz stanową i lokalną policją skutecznie poradziły sobie ze zorganizowaną przestępczością. Rozwiązanie to jest o tyle dobre, że pomoże w walce z cyberprzestępcami władzom lokalnym, które często nie mają odpowiednich środków ani zasobów ludzkich. Należy jednak również wziąć pod uwagę, że organizacje cyberprzestępców różnią się od tradycyjnych mafii, gdzie nie zawsze występuje układ hierarchiczny. Nie wiadomo również czy Zespół Zadaniowy będzie zajmował się przestępstwami popełnionymi za pomocą internetu czy przestępstwami skierowanymi przeciwko komputerom (DDoS czy hakowanie) czy też dwoma ich rodzajami.

WNIOSKI

W zapowiedziach przedwyborczych Donald Trump przeszedł od mówienia o cyberbezpieczeństwie jako o mało poważnym problemie do traktowania go priorytetowo, przedstawiając jednak niewiele konkretów. Wnioskując, po przedwyborczych zapowiedziach, administracja 45. prezydenta będzie kontynuowała działania swojego poprzednika, skupiając się na ochronie infrastruktury krytycznej. Różnica będzie prawdopodobnie leżała w podejściu do operacji ofensywnych. W tym obszarze nowa administracja będzie prowadziła zdecydowanie agresywniejszą politykę, co może doprowadzić do zaostrzenia się relacji z Rosją i Chinami. Rozluźnienie więzów NSA i innych agencji zajmujących się śledzeniem i zdobywaniem danych, z pewnością wywoła protesty obrońców praw człowieka.

Trump jednak nie wypowiedział się wciąż na wiele istotnych tematów takich jak szyfrowanie, dzielenie informacji pomiędzy sektorem prywatnym i rządowym czy w jaki sposób ma zamiar inicjować rozwój, nowego bezpiecznego oprogramowania. Nie poznaliśmy również jego poglądów na dyskutowany ostatnio problem rozdzielnia NSA i USCYBERCOM.

Co ciekawe, zapowiedzi Trumpa raczej wskazują na kontynuowanie przez niego inicjatyw zapoczątkowanych przez Obamę, który znacznie rozwinął zdolności ofensywne oraz promował doktrynę odstraszania w cyberprzestrzeni. Co więcej, to właśnie za jego rządów, USCYBERCOM

zrzucało – jak to określił sekretarz obrony Ash Carter – cyberbomby na ISIS.

Obecnie wydaje się, że niezależnie od osobistego zainteresowania prezydenta cyberbezpieczeństwem, temat ten musi zostać podjęty. W szczególności biorąc pod uwagę jak uzależnionym od internetu państwem są Stany Zjednoczone. Zaniedbanie ochrony sieci teleinformatycznych może tylko pogorszyć tę sprawę i narazić na ataki cyfrowe.

Największym wyzwaniem dla nowego prezydenta będzie z pewnością zbudowanie solidnego i wiarygodnego odstraszania w cyberprzestrzeni, które spowoduje, że podobny atak jak w wykonaniu rosyjskich hakerów podczas wyborów prezydenckich się nie powtórzy. Wydaje się, że odpowiedź Obamy była zbyt łagodna i nie podnosi kosztów podjęcia podobnego wysiłku na odpowiedni poziom, żeby odstraszyć potencjalnych naśladowców Rosjan.