BYŁA DORADCZYNI BARACKA OBAMY: USA NIE TRAKTUJĄ POWAŻNIE CYBERBEZPIECZEŃSTWA [WYWIAD]

O amerykańskim systemie cyberbezpieczeństwa, wyzwaniach dla przyszłej administracji, postaci Edwarda Snowdena i nadchodzącej rewolucji związanej z internetem rzeczy mówi w wywiadzie dla Cyberdefence24.pl Melissa Hathaway – była doradczyni Baracka Obamy ds. cyberbezpieczeństwa oraz prezydent Hathaway Global Strategies.

Andrzej Kozłowski: Była Pani autorką Przeglądu Polityki Cyberbezpieczeństwa (*Cybersecurity Policy Review*) dla administracji Baracka Obamy w 2009 roku, w którym wystosowano szereg rekomendacji. Które z nich zostały wdrożone w życie?

Melissa Hathaway: Prezydent Obama skupił się na stworzeniu efektywnego mechanizmu i procesu wymiany informacji oraz współpracy z sektorem prywatnym. W 2015 roku przyjęto też Cybersecurity Act, umożliwiający rządowi i przemysłowi łatwiejsze dzielenie się informacjami, ponieważ nie łamały one antytrustowego prawa przeciwdziałającego zmowie rynkowej oraz nie obniżały wiarygodności przedsiębiorstw pracujących z naszym rządem.

A.K.: Współpraca prywatno-publiczna jest jednym z głównych problemów w budowie skutecznego systemu cyberbezpieczeństwa w każdym z państw na kuli ziemskiej? Czy Barackowi Obamie udało się osiągnąć sukces w tym obszarze?

M.H.: Partnerstwo publiczno-prywatne jest w bardzo wczesnej fazie rozwoju i nie jest operacyjne. Trzeba zbudować zaufanie pomiędzy podmiotami i obecna administracja stara się to zrobić poprzez dzielenie się precyzyjnymi informacjami o zagrożeniach, które mogą zostać wykorzystane przez sektor prywatny do dzielenia się podobnymi, przydatnymi informacjami z rządem, co prowadzi do wykreowania się lepszego obrazu sytuacji. Wciąż jednak pozostaje wiele rzeczy do zrobienia.

A.K.: Wiele dyskusji toczy się na temat partnerstwa publiczno-prywatnego, ale co z partnerstwem pomiędzy podmiotami prywatnymi? Jak to wygląda w Stanach Zjednoczonych?

M.H.: Mamy w Stanach Zjednoczonych bardzo specyficzne prawo, które prawie zakazuje wymiany informacji między podmiotami prywatnymi. Były wprawdzie próby stworzenia pewnych inicjatyw politycznych przez Departament Sprawiedliwości. W oficjalnym oświadczeniu wyrażono zgodę na dzielenie się informacjami o zagrożeniach między podmiotami prywatnymi. Najbardziej zaawansowany program partnerstwa pomiędzy instytucjami prywatnymi występuje w sektorze finansowym i nosi nazwę Wymiany Informacji i Analizy o Usługach Finansowych (Information Sharing and Financial Services Analysis). Mamy również listę ośmiu największych banków, które utworzyły sieci wymiany informacji i dzięki temu więcej informacji w czasie rzeczywistym może przepływać w

zdecydowanie bardziej uporządkowany sposób. Powołano również do życia nowy Zespół Zadaniowy (Task Force) jako odpowiedź na ostatni atak cybernetyczny na system SWIFT. Inne sektory także starają się wprowadzić efektywny mechanizm współpracy między podmiotami prywatnymi, ale dzieje się to raczej poza obszarem centrum wymiany informacji, który jest wspierany przez Departament Bezpieczeństwa Wewnętrznego. Są to nieformalne sieci, czego przykładem jest współpraca oparta na członkostwie, które wpierw należy opłacić i w ten sposób można stać się uczestnikiem mechanizmu wymiany informacji.

A.K.: Jednym z najbardziej kontrowersyjnym tematów ostatnich lat w obszarze cyberbezpieczeństwa jest Edward Snowden. Jaka jest Pani opinia na jego temat i czynów, które popełnił?

M.H.: Po pierwsze, należy zauważyć, że Edward Snowden złamał amerykańskie prawo i powinien zostać postawiony przed sądem jako zwykły przestępca. Jego działania można też oceniać pozytywnie. Dzięki ujawnieniu przez niego informacji mamy obecnie o wiele większą transparentność w dialogu z rządem na temat jego aktywności w cyberprzestrzeni. Zintensyfikował się również dialog na temat prywatności i bezpieczeństwa w skali globalnej, które moim zdaniem jest czymś dobrym i pożądanym. Myślę jednak, że Edward Snowden przede wszystkim spowodował poważne skutki dla bezpieczeństwa naszego kraju i jeszcze raz podkreślam, że złamał prawo.

A.K.: W ostatnim raporcie Izby Reprezentantów o działalności Edwarda Snowdena zaznaczono, że większość udostępnionych przez niego informacji dotyczyła tajemnic wojskowych i działalności amerykańskiego wywiadu oraz to, że przekazał je stronie rosyjskiej, co miał potwierdzić jeden z posłów rosyjskiej Dumy. Czy w takim razie możemy go nazwać szpiegiem?

M.H.: Nie podlega wątpliwości, że Edward Snowden był szpiegiem. Jeśli tylko bierzesz informacje od naszej społeczności wywiadu i dostarczasz je rządowi innego państwa, to jest to akt szpiegostwa. Inne czynniki nie odgrywają tu roli, więc nie ma znaczenia, czy obcy rząd kazał mu zrobić, czy nie. On po prostu ukradł te informacje i je opublikował.

A.K.: Mamy ostatnio do czynienia ze zwiększającą się liczbą ataków cyfrowych na infrastrukturę krytyczną. Część z nich, jak ten wymierzony w elektrownię na Ukrainie, doprowadziła do czasowego odcięcia od energii elektrycznej dużego obszaru kraju. Jak ochrona infrastruktury krytycznej wygląda w Stanach Zjednoczonych, czy jest ona bardziej podatna na cyberataki niż na Ukrainie?

M.H.: Moim zdaniem sieć energetyczna w Stanach Zjednoczonych jest prawdopodobnie bardziej podatna na cyberataki niż na Ukrainie, ponieważ jesteśmy bardziej usieciowieni. To właśnie tam zostały zaatakowane trzy podstacje. Atak nastąpił poprzez system nadzorujący przebieg procesu produkcyjnego i złośliwe oprogramowanie dostało się głęboko do systemów SCADA. Ukraina wciąż jednak miała zdolność do ręcznego resetu. W Stanach Zjednoczonych nie bylibyśmy w stanie tego zrobić, ponieważ procesowi cyfryzacji podlega prawie wszystko. W wielu przypadkach nasze systemy są bardziej podatne na ataki niż ukraińskie.

A.K.: Czy po incydencie na Ukrainie doszło w Stanach Zjednoczonych do intensyfikacji działań w tym obszarze zabezpieczenia infrastruktury krytycznej?

M.H: Doszło do intensyfikacji wymiany informacji z naszym sektorem energetycznym na temat tego, co wydarzyło się na Ukrainie. Powstało wiele raportów z tym związanych. Nasze organy nadzoru nie wymagają jednak od firm podjęcia żadnych dodatkowych działań bezpieczeństwa ani środków zabezpieczających.

A.K.: Czy w Stanach Zjednoczonych istnieje prawo zmuszające przedsiębiorstwa odpowiedzialne za ochronę infrastruktury krytycznej, w szczególności z sektora energetyki, do wprowadzenia minimalnych standardów bezpieczeństwa?

M.H.: W Stanach Zjednoczonych funkcjonuje North American Electric Reliability Corporation, które ustala standardy i sposób ich egzekwowania. Wymuszają one od sektora energetycznego implementację wyższych standardów bezpieczeństwa. Należy jednak zauważyć, że mają wiele lat na implementację i występuje duża liczba norm, których nie trzeba spełniać. Przykładowo nie ma w nich informacji, że przedsiębiorstwo pomaga usunąć złośliwe oprogramowanie, które występuje w ich systemach infrastruktury krytycznej.

Czytaj też: USA: Sankcje odpowiedzią na ataki rosyjskich hakerów?

A.K:. W ostatnim miesiącu media wielokrotnie informowały o atakach na systemy Partii Demokratycznej, których autorem była Rosja. Reakcja administracji Baracka Obamy jest dość bierna. Czy nie uważa Pani, że świadczy to o słabości Stanów Zjednoczonych i tylko zachęca Rosję do dalszej agresji?

M.H.: Myślę, że ataki na Komitet Partii Demokratycznej oraz innych baz danych pokazuje, że Ameryka nie traktuje poważnie inwestycji w bezpieczeństwo systemów i sieci oraz w ochronę danych i jest to problem wewnętrzny Stanów Zjednoczonych, a nie kwestia międzynarodowa. Jeżeli jednak jest to operacja przeprowadzana przez inne państwo w celu destabilizacji życia politycznego czy podważenia zaufania do naszych demokratycznych procesów i wartości, to jest to temat, który powinien zostać przedyskutowany. Należy wziąć pod uwagę różne punkty widzenia i narracje, określić, co jest ważne w naszym systemie politycznym i dlaczego określone działania są nie do zaakceptowania oraz w jaki sposób wzmocnić systemy chroniące nasze dane.

A.K.: Mija rok od historycznego porozumienia pomiędzy Stanami Zjednoczonymi a Chinami o ograniczeniu liczby ataków w cyberprzestrzeni wymierzonych w siebie. Jak Pani ocenia efektywność tej umowy?

M.H.: Moim zdaniem, kiedy dwóch przywódców państw zgadza się na ograniczenie nielegalnej kradzieży własności intelektualnej, to jest to ważna rzecz. Zobowiązanie dokonuje się na oczach całego świata i jest to pierwsza dźwignia nacisku w przypadku kiedy dany przywódca nie stosuje się do swojego poręczenia. Uważam, że chińscy hakerzy zmienią taktykę i procedury oraz będą doskonalili ciche działanie, ale nie przestaną pobierać ogromnych ilości danych.

A.K.: Jak Pani ocenia szanse, że rosyjscy hakerzy mogą zaatakować systemy wyborcze i wpłynąć na wynik wyborów? Nie mówimy tu o zmasowanych atakach, tylko kierunkowanych, wymierzonych w stany swingowe, w których rozstrzygnie się, kto zostanie następnym prezydentem. Bierzemy pod uwagę sytuację podobną do tej z 2000 roku, gdzie różnica pomiędzy George'em W. Bushem i Alem Gore'em była minimalna.

M.H.: Moim zdaniem wciąż jest bardzo trudno taki atak przeprowadzić. Nasz system wyborczy jest lokalny i zdywersyfikowany technicznie. Właśnie z powodu tych czynników trudno jest ingerować w nasz proces wyborczy. Głównym zmartwieniem pozostają tutaj wspomniane stany swingowe w Stanach Zjednoczonych. Władze lokalne i regionalne pracują jednak z ekspertami bezpieczeństwa, żeby podjąć dodatkowe środki w celu zabezpieczenia systemów i sieci. Jednak atak na dużą skalę jest bardzo trudny do wykonania, właśnie z powodu wyżej wymienionych czynników.

A.K: Jeżeli następny amerykański prezydent wyznaczyłby Panią do przeprowadzenia kolejnego Przeglądu Cyberbezpieczeństwa, jakie byłyby Pani rekomendacje?

M.H.: Pierwszym krokiem byłoby przeprowadzanie narodowego czyszczenia – kampanii na rzecz wyeliminowania złośliwego oprogramowania z naszej infrastruktury krytycznej oraz usunięcia botnetów, które są punktami infekcyjnymi występującymi w jądrze naszej infrastruktury krytycznej oraz unieszkodliwienie serwerów Command and Control, odpowiedzialnych za koordynację botnetów.

Kolejnym problemem jest eliminacja ransomware. W tych obszarach Stany Zjednoczone są najbardziej zainfekowanym państwem na kuli ziemskiej i dlatego myślę, że należy wyeliminować ten problem. Musimy być liderem technologicznym na świecie, a w tym celu trzeba zacząć od wyczyszczenia naszego własnego podwórka.

Drugim krokiem, który powinien podjąć następny prezydent jest skupienie się na trzech obszarach infrastruktury krytycznej. Pierwszym z nich jest sektor energetyczny zarówno nuklearny, jak i elektryczny. W nim powinno się pozbyć złośliwego oprogramowania. Jest to najważniejszy sektor, ponieważ wszystkie inne usługi bazują na nim. Drugi obszar to sektor telekomunikacyjny, który musi dostarczać nam nieprzerwanie usług na wysokim poziomie. Od tego zależy sukces naszej gospodarki oraz swobodny przepływ towarów i usług. Będzie to możliwe tylko, jeżeli wyeliminujemy złośliwe oprogramowanie, które znajduje się w systemach krytycznych, oraz unieszkodliwimy botnety. Wreszcie powiedziałabym prezydentowi, aby zapewnić integralność systemu finansowego. Stany Zjednoczone jako światowy lider, członek grupy G-8 i G-20 oraz uczestnik tego systemu muszą zapewnić, że można na nich polegać i na nie liczyć, a ryzyko oszustwa jest minimalne. Musimy pokazać, że możemy ufać Wirtualnym Sieciom Prywatnym, na których operują nasze systemy bankowe i które pozwalają nam na swobodny przepływ kapitału na całym świecie. Powiedziałabym też prezydentowi, że musi zacząć się również przygotowywać na nadejście internetu rzeczy, który stworzy o wiele więcej podatności i luk. Musi on przyjąć plan działania, jak sobie z tym problemem radzić. Jeżeli nic nie zrobimy z wiedzą, że nasz kraj jest obecnie zainfekowany przez botnety, to w przyszłości problem ten tylko się zwiększy i dlatego musimy zacząć spoglądać na dobrze zaprojektowane produkty jako na część systemu naszego państwa i biznesu.

A.K.: Z tego, co Pani powiedziała, wynika, że Stany Zjednoczone nie są najlepiej zabezpieczonym państwem na świecie w cyberprzestrzeni. Może to dziwić, ponieważ Stany Zjednoczone są pierwszym krajem, który rozpoczął proces tworzenia polityki bezpieczeństwa w świecie wirtualnym oraz pierwszym, który potraktował cyberzagrożenia jako ryzyko dla bezpieczeństwa narodowego?

M.H:. Problem leży w tym, że nie uznaliśmy cyberbezpieczeństa jako podstawowego narzędzia umożliwiającego wzrost gospodarczy i dlatego brak zabezpieczenia cyberprzestrzeni powoduje, że rozwój gospodarki jest kosztowny. Ponadto jesteśmy przekonani, że rynek naprawi się sam. Moim zdaniem musimy napędzać innowacje, żeby osiągnąć bardziej odporną na cyberataki infrastrukturę.