Przemówienie ambasadora Stephena D. Mulla
na konferencji „Zagrożenia w cyberprzestrzeni – bezpieczeństwo ponad granicami”
28 października 2013 r.

Bardzo dziękuję Panu Orlińskiemu za miłe słowa wprowadzenia. Dziękuję też Boeingowi i Zarządowi Targów Warszawskich za zaproszenie. Cieszę się, że jest z nami tylu przedstawicieli firm zajmujących się infrastrukturą krytyczną, a także przedstawicieli rządu wysokiego szczebla.

Zapewnienie integralności sieci infrastruktury krytycznej pozostaje jedną z ważniejszych kwestii dla firm i rządów na całym świecie. Mimo że na bezpieczeństwo w cyberprzestrzeni zwraca się ostatnio coraz większą uwagę, na pewno wiele jeszcze można zrobić, by chronić najważniejsze sieci komputerowe, zarówno w Stanach Zjednoczonych, jak i w Polsce.

Chciałbym poświęcić kilka minut na omówienie paru głośnych cyberataków wymierzonych w firmy zarządzające infrastrukturą krytyczną w sektorze finansowym, a także energetycznym i opisać kilka spośród mechanizmów stosowanych w Stanach Zjednoczonych do zapobiegania i zwalczania takich ataków. Mechanizmy te wymagają aktywnej współpracy i wymiany informacji między partnerami z sektora prywatnego i publicznego. Okazuje się, ze praca

zespołowa – taka, która łączy nawet firmy konkurujące ze sobą na rynku – jest wysoce skuteczną metodą na nasze słabe strony związane z zagrożeniami w cyberprzestrzeni.

Przykłady cyberataków

Pierwszy przykład, jaki chciałbym Państwu podać, dotyczy sektora finansowego. Instytucje finansowe we wszystkich krajach ciągle stykają się z zagrożeniami w cyberprzestrzeni. W ciągu ostatnich kilku miesięcy trzy duże amerykańskie banki doświadczyły jednych z najbardziej zaawansowanych i uporczywych cyberataków, jakie miały kiedykolwiek miejsce. Straciły przez to miliony dolarów. Banki w Stanach Zjednoczonych i w Polsce są częstym celem ataków polegających na zmasowanym wysyłaniu zapytań, które mają na celu przeciążenie aplikacji internetowych i zablokowanie usług. Jednak w przypadku ostatnich ataków blokujących usługi chodziło tak naprawdę o odwrócenie uwagi po to, by oszuści mogli wykorzystać słabe punkty w sieciach banków i uzyskać dostęp do aplikacji realizujących przelewy. W wyniku tych działań hakerzy przesłali miliony dolarów przez sfałszowane przelewy zagraniczne, podczas gdy pracownicy odpowiedzialni za bezpieczeństwo sieci byli zajęci rozwiązywaniem problemu zablokowania usług. Ten przykład pokazuje, że charakter zagrożeń w cyberprzestrzeni cały czas się

zmienia, w związku z czym my też musimy przystosowywać się do zmieniającej się taktyki cyberprzestępców.

Teraz podam Państwu drugi przykład. Trochę ponad rok temu, w Arabii Saudyjskiej, potentat naftowy Saudi Aramco padł ofiarą jednego z najgorszych cyberataków, jakie kiedykolwiek widział świat biznesu. Hakerzy twierdzący, że Arabia Saudyjska jest odpowiedzialna za „zbrodnie i okrucieństwa" w krajach takich jak Syria i Bahrajn, przedostali się do wewnętrznej sieci Aramco. Wykorzystali sytuację, by zniszczyć ponad 30 tysięcy komputerów firmy. Aramco podało do wiadomości publicznej, że w wyniku ataku ucierpiało 85% komputerów. Chociaż atak nie spowodował zatrzymania wydobycia ropy czy gazu w Arabii Saudyjskiej, niesamowicie nadszarpnął wiarygodność firmy i utrudnił jej działanie. Proszę tylko wyobrazić sobie konsekwencje biznesowe takiego zdarzenia w Państwa firmach – gdyby zawartość 85% komputerów została kompletnie wyczyszczona.

Chyba najbardziej niepokojący atak ostatnich lat miał miejsce w Estonii w 2007 roku. Zorganizowana grupa dokonała zmasowanego ataku w celu zablokowania stron internetowych estońskiego rządu, mediów, firm telekomunikacyjnych i

banków. Hakerom udało się przejąć ponad milion komputerów w 175 różnych krajach. Wykorzystali je do zakłócenia usług internetowych w Estonii na dwa tygodnie. W czasie tych dwóch tygodni Estończycy nie mogli przeprowadzić podstawowych codziennych czynności, nad dostępnością których w XXI wieku w ogóle się nie zastanawiamy – były problemy z tym, żeby zadzwonić, dostać się do własnego rachunku bankowego, zapłacić za zakupy kartą debetową. Atak w Estonii w 2007 roku był sygnałem alarmowym ukazującym ryzyko związane z potencjalnymi przestępstwami cybernetycznymi i ich wpływ na krytyczną infrastrukturę komunikacyjną całego kraju.

Te trzy przykłady są bardzo odmienne: atakujący mieli różne motywacje i wykorzystali różne metody. Jednak efekt był taki sam: miliony dolarów strat i utrata wiarygodności instytucji dotkniętych atakiem, a nawet poważne zagrożenie bezpieczeństwa narodowego jednego z członków NATO. Co więcej, gdyby udało się te ataki w pełni zrealizować, mogłoby to doprowadzić do zakłócenia całego systemu finansowego i dostaw energii na świecie. Mając na uwadze te przykłady, chciałbym przejść do omówienia możliwych sposobów ograniczenia zagrożeń w cyberprzestrzeni, z jakich korzystamy w Stanach Zjednoczonych i sposobów radzenie sobie z podobnymi incydentami.

Uprawnienia do podjęcia decyzji

Potrzeba szybkiego reagowania to jeden z podstawowych wniosków wyciągniętych z omówionych przeze mnie ataków. Administratorzy infrastruktury krytycznej mają bardzo mało czasu na rozpoznanie ataku i podjęcie działań ograniczających wyrządzone szkody. Jedna z metod umożliwiających błyskawiczne działanie agencjom rządowym i prywatnym firmom to określenie *najniższego* szczebla, na którym może zostać podjęta decyzja blokująca rozprzestrzenianie się ataku. W przypadku zdarzenia w Estonii odpowiedzialność wziął na siebie 39-letni szef Estońskiego Zespołu do spraw Przeciwdziałania Awariom Komputerowym – to on podjął decyzję o zablokowaniu wszystkiego, co przychodziło z zagranicy do sieci w Estonii, kupując w ten sposób czas dla swoich kolegów na zneutralizowanie zainfekowanych komputerów.

Dzielenie się informacjami

Ataki w cyberprzestrzeni, które wcześniej opisałem, pokazują potrzebę dzielenia się informacjami pomiędzy administratorami infrastruktury krytycznej w sektorze publicznym i prywatnym. Niestety niełatwo jest osiągnąć przejrzystość

komunikacji w kwestiach dotyczących przestępstw w cyberprzestrzeni. Na przykład na początku reagowanie na atak cybernetyczny w Estonii było wstrzymywane ze względu na rządowy zakaz dotyczący przekazywania informacji zastrzeżonych. Jest to ciągły problem we wszystkich krajach. Tak samo prywatne firmy, jak na przykład ostatnio zaatakowane amerykańskie banki, obawiają się utraty pozycji rynkowej, jeśli publicznie przyznałyby, że padły ofiarą cyberprzestępstwa. Nawet dzielenie się informacjami o sukcesach w tej branży jest problematyczne, bo takie informacje mogłyby zostać wykorzystane przez cyberprzestępców do sforsowania naszych zabezpieczeń.

W Stanach Zjednoczonych ustanowiliśmy struktury, które są tak zaplanowane, by pokonywać bariery komunikacyjne. Mamy między innymi ośrodki, które nazywamy „fusion centers", gdzie spotykają się prywatni operatorzy infrastruktury krytycznej i przedstawiciele organów ścigania. Dzięki temu władze mogą szybko dzielić się informacjami dotyczącymi zagrożeń z sektorem prywatnym – metodami, które były kiedyś hamowane przez procesy biurokratyczne. Informacje płyną też z powrotem do władz, jako że często sektor prywatny jest lepiej poinformowany niż rząd w obszarach, gdzie w grę wchodzą

nowe, dopiero pojawiające się zagrożenia. Ponadto w takich centrach zawierane są porozumienia prawne, umożliwiające konkurentom działającym na tym samym rynku wymianę informacji na temat powszechnych zagrożeń. To zaufanie nie bierze się znikąd – jest z biegiem czasu wypracowywane dzięki współpracy i dzieleniu się informacjami dotyczącymi powszechnych zagrożeń. Konkurenci korzystają z takiej wymiany, lepiej funkcjonują dzięki temu, że wspólnie rozwiązują problemy, zanim ich słabe punkty zostaną wykorzystane przez przestępców. Przekonaliśmy się, że te ośrodki to jedne z najbardziej efektywnych narzędzi promowania przejrzystej wymiany informacji dotyczących zagrożeń cybernetycznych.

Ramy bezpieczeństwa w cyberprzestrzeni

Atak na Saudi Aramco przypomniał nam, że firmy prywatne muszą być przygotowane – zarówno pod kątem personelu, jak i technologii — na szybkie rozpoznanie i zneutralizowanie cyberataku. A rządy mogą i powinny odgrywać rolę pomocnika, pomagającego firmom w ochronie infrastruktury krytycznej przed cyberatakami. W Stanach Zjednoczonych powstała inicjatywa, w ramach której władze federalne mają określić dobrowolne ramy cyberbezpieczeństwa dla

operatorów infrastruktury krytycznej. Chodzi o określenie standardów i najlepszych praktyk ochrony tych systemów komputerowych, które kontrolują infrastrukturę krytyczną, a także o wsparcie operatorów w zarządzaniu ryzykiem. Odbywa się to przy bliskiej współpracy z sektorem prywatnym – by standardy były odpowiednio zdefiniowane, stosowane i nie stanowiły zbytniego obciążenia dla danej branży. Oczekujemy, że projekt wspomnianych ram bezpieczeństwa będzie gotowy w przyszłym roku do końca lutego. Jednak nie możemy osiąść na laurach, będziemy cały czas zwalczać przestępców w cyberprzestrzeni z taką samą wytrwałością, z jaką oni działają.

Wnioski

Podsumowując, ochrona cyberprzestrzeni jest wspólnym obowiązkiem biznesu i rządów. Jest to problem ogólnoświatowy, więc też i nasza współpraca musi wykraczać poza granice państw. Zagrożenia, przed jakimi stoją sieci w Ameryce, zwłaszcza związane z cyberprzestępstwami, są w dużej mierze takie same jak te w Polsce. Dlatego musimy więcej ze sobą współpracować, zarówno na szczeblu międzyrządowym, jak i pomiędzy poszczególnymi firmami. Musimy zdefiniować standardowe praktyki, cały czas się rozwijać, stosując się jednocześnie do istniejących międzynarodowych konwencji. Ważny jest też swobodny i

odpowiednio szybki przepływ informacji. Trzeba tworzyć mechanizmy współpracy, takie jak partnerstwo publiczno-prywatne, a także ośrodki współpracy w poszczególnych sektorach, o których mówiłem wcześniej – aby wspomóc różne branże i rządy w odpowiednio szybkim i skutecznym reagowaniu na pojawiające się zagrożenia. Stany Zjednoczone są gotowe dzielić się wiedzą i doświadczeniem i współdziałać z Polską w zwalczaniu zagrożeń w cyberprzestrzeni. W miarę jak cyberataki przybierają coraz bardziej międzynarodowy charakter, taki rodzaj partnerstwa jest absolutnie kluczowy.

Bardzo dziękuję za uwagę.