Komentarz KBN

Nr 17 (72) / 2020 28 grudnia 2020 r.

ACDC i hakowanie zwrotne: „Stairway to Heaven" czy jednak „Highway to Hell"?

Dominika Dziwisz

W państwach anglosaskich istnieje wielowiekowa tradycja delegowania uprawnień do egzekwowania prawa na osoby lub podmioty prywatne. W wielu stanach USA dostęp do broni jest łatwiejszy niż do alkoholu, ponieważ państwo ufa obywatelom, że broń palną wykorzystają odpowiedzialnie i zgodnie z prawem. Innym z przejawów tego zaufania jest istnienie profesji „łowców głów" (*bounty hunters*). Już w trzynastowiecznej Anglii ścigali oni oskarżonych, którzy chcieli ukryć się przed wymiarem sprawiedliwości. Pod koniec XIX w. Sąd Najwyższy Stanów Zjednoczonych zatwierdził ich działanie wyrokiem w sprawie Taylor przeciw Taintor. Obecnie łowcy głów odnajdują 90 proc. oskarżonych, którzy zbiegli.

Dlatego nie powinno zaskakiwać, że to właśnie w USA od wielu lat toczy się debata o aktywnej cyberobronie (ang. *active cyber defense*) i cyberataku zwrotnym (ang. *hack back*). Sednem dyskusji jest to, czy ofiary cyberprzestępstwa z sektora prywatnego powinny mieć w pewnych przypadkach możliwość przeprowadzenia odpowiedzi na atak poza własnymi sieciami. Do tej pory takie działania zarezerwowane były wyłącznie dla organów ściągania, w tym przede wszystkim FBI. Rozważana w Kongresie Ustawa o aktywnej cyberobronie (*Active Cyber Defense Certainty Act*, ACDC) zniosłaby to ograniczenie, umożliwiając firmom prywatnym stosowanie agresywnych środków cyberobrony tak, aby poza własnymi sieciami mogły nie tylko identyfikować napastników, ale nawet niszczyć informacje pierwotnie skradzione.

Od początku istnienia Internetu firmy zapewniają ochronę swoich sieci głównie poprzez działania pasywne, czyli zapory sieciowe (*firewalls*), systemy wykrywania i zapobiegania włamaniom (IDS/IPS), stosowanie technologii ochrony przed wyciekami informacji (DLP), systemy zabezpieczające przed złośliwym oprogramowaniem oraz regularne łatanie błędów w oprogramowaniu. Kiedy haker złamie te zabezpieczenia, firmie pozostaje niewiele opcji. Rzadko bowiem można odzyskać utracone dane zanim zostaną one sprzedane lub wykorzystane. Ponieważ ryzyko cyberataków na firmy amerykańskie nieustannie rośnie, przyznanie firmom dodatkowych uprawnień w zakresie cyberbezpieczeństwa jest w dłuższej perspektywie czasowej bardzo prawdopodobne.

Propozycje zmian w amerykańskim prawie złożył kongresman republikanów Tom Graves w marcu 2017 r., ale projekt nigdy nie wyszedł poza prace komisji. W 2019 r. znowelizowana ACDC ponownie trafiła do Kongresu i aktualnie jest na pierwszym etapie procesu legislacyjnego. Propozycja może wydawać się prostym przeniesieniem zasad obrony koniecznej ze świata fizycznego do cyberprzestrzeni, ale na tym analogie się kończą, a kontrowersje narastają. O ile ustawa ma zapewnić gwarancję, że pod określonymi warunkami można prowadzić działania odwetowe, co zmniejszy szkody dla ofiar i odstraszy niektóre włamania do sieci, to jednocześnie może wywołać wiele niezamierzonych efektów ubocznych zarówno dla napastnika i ofiary, jak i niezaangażowanych, niewinnych podmiotów. Ponadto działania odwetowe bez zaangażowania służb śledczych mogą nasuwać inne, mało pozytywne skojarzenie z samosądami, kiedy kara jest wymierzana przez osoby czy instytucje do tego niepowołane. W państwach demokratycznych samosądy są oczywiście nielegalne, a ściganiem przestępstw zajmują się powołane do tego wyspecjalizowane organy państwowe, co ma zapewnić bezstronność i odcięcie się od emocjonalnych pobudek.

Dlatego, bez względu na potencjalnie pozytywne efekty ACDC, nie można bagatelizować zagrożeń, jakie niesie ze sobą jej wprowadzenie. Czy warto zatem ponosić ryzyko dla konkretnych korzyści? Jaką cenę mogą ponieść USA w zamian za zwiększenie cybermożliwości? Czy przeniesienie na firmy części uprawnień tradycyjnie przynależnych organom państwowym może pomniejszyć katalog kompetencji tradycyjnie przypisanych organom ścigania? Dylematów i pytań, na które nie zawsze można znaleźć proste odpowiedzi, jest wiele. Poniżej przedstawiono tylko niektóre najważniejsze problemy i wyzwania, które wiążą się z rozszerzeniem uprawnień firm prywatnych na nowe formy aktywnej cyberobrony.

Problem atrybucji

Przeprowadzenie działań odwetowych w ramach aktywnej cyberobrony w praktyce może okazać się dyskusyjne ze względu na problem z ustaleniem źródła ataku i osób za niego odpowiedzialnych. Atrybucja cyberataku jest prawie niemożliwa, bo do jego przeprowadzenia wykorzystuje się wiele urządzeń, serwery proxy i łańcuchy zainfekowanych komputerów należących do niewinnych osób trzecich. Bardzo trudno też mieć pewność, że komputer, który wydaje się być przyczyną ataku, sam nie został zhakowany. W praktyce nawet ustalenie prawdopodobieństwa pochodzenia ataków wymaga także specjalistycznych zasobów, czyli wykwalifikowanego zespołu oraz odpowiednich środków. Konsekwencją błędnego przypisania źródła pochodzenia

ataku może być zaatakowanie niewłaściwych systemów albo wyrządzenie szkody niezaangażowanym podmiotom. W związku z tym spełnienie warunku zastosowania właściwych ACDM (*Active Cyber Defense Measures*), którym jest właśnie uzyskanie wysokiego stopnia pewności co do źródła pochodzenia ataku, w praktyce jest mało realne. Aby zmniejszyć problemy związane z przypisaniem cyberincydentu jego sprawcom, ACDC zalegalizowałoby użycie technologii *beacon*, czyli programów, kodów lub poleceń osadzonych w plikach, które sygnalizują systemom obrońcy, gdy plik oznaczony *beaconem* jest modyfikowany lub odczytywany poza systemem danej firmy. To pozwoli wyśledzić ścieżkę i lokalizację skradzionego pliku, zapewniając potencjalnie silniejszy, ale nadal niepewny dowód atrybucji.

Nieprecyzyjne pojęcia

Projekt zawiera dużą ilość niejasności językowych, które ostatecznie mogą zniweczyć wprowadzenie ustawy. Przykładowo, w błąd może prowadzić nieprecyzyjne określenie „trwałego nieuprawnionego wtargnięcia" (*persistent unauthorized intrusion*)". Prawdopodobnie ten termin został wprowadzony, aby zapobiec powołaniu się na ACDC przez firmy, która doświadczają tylko uciążliwości w swojej sieci komputerowej. Odnosi się on do czasu trwania konkretnego włamania lub do serii włamań, ale ostatecznie nie wiadomo, ile czasu wystarczy, aby uznać je za trwałe. Ponieważ termin pozostawia pole do interpretacji, to pojawia się pytanie, czy ofiara rzeczywiście może skorzystać z postanowień ustawy. Warto także zauważyć, że również krótkotrwałe włamania mogą wywoływać poważne konsekwencje, czego ustawodawca nie wziął pod uwagę.

Ustawa definiuje „atakującego" (*attacker*) jako „osobę lub jednostkę będącą źródłem trwałego nieuprawnionego wtargnięcia do komputera ofiary". Brakuje jednak doprecyzowania, czym jest „komputer atakującego". Jak wcześniej wspomniano, atak może przechodzić przez łańcuch zainfekowanych komputerów, a zatem włamanie może obejmować nie jeden, lecz wiele komputerów i trudno będzie określić rzeczywiste źródło ataku. Nowa, zaktualizowana wersja ustawy próbuje rozwiązać te niejasności poprzez wprowadzenie definicji „komputera pośredniczącego", czyli „komputera osoby lub podmiotu, który nie jest własnością ani nie jest pod główną kontrolą osoby atakującej, ale który został użyty do rozpoczęcia lub ukrycia źródła trwałego cyberataku". Nadal, w sytuacji, kiedy komputery pośredniczące będą pod kontrolą strony atakującej, przypisanie źródła pochodzenia ataku będzie utrudnione. Ostatecznie firmy, które będą chciały skierować atak na komputery pośredniczące, mogą mieć problem z rozstrzygnięciem, czy poprzez takie działania nie złamią prawa. Ustawa przewiduje bowiem wyjątki, które pozwalają pociągnąć do odpowiedzialności podmioty wykonujące czynności wymienione jako niemieszczące się w granicach ACDM. Są to działania, które celowo przekraczają poziom aktywności wymagany do przeprowadzenia rozpoznania na komputerze pośredniczącym, aby umożliwić przypisanie źródła trwałego cyberataku, lub celowo powodujące włamanie albo zdalny dostęp do komputera pośredniczącego. O ile taki zapis znajduje oczywiste uzasadnienie, to jednocześnie pozostawia pole do interpretacji, bo ostatecznie nie wiadomo, czy uzyskanie dostępu do komputera pośredniczącego tylko w celu rozpoznania sytuacji i przypisania źródła ataku, nie zostanie ocenione jako celowe uzyskanie zdalnego dostępu do takiego komputera.

Wśród innych niedoprecyzowanych sytuacji, w których firma ma ponosić odpowiedzialność za atak zwrotny są też te, kiedy m.in. atakowana firma „stwarza zagrożenie dla zdrowia lub bezpieczeństwa publicznego" lub gdy jej działanie „celowo powoduje trwałe zakłócenie łączności internetowej osoby lub podmiotów". Projekt ustawy nie precyzuje, co stanowi zagrożenie dla zdrowia lub bezpieczeństwa publicznego, ani czym jest trwałe zakłócenie.

Nadzór nad wykorzystaniem ACDM *(Active Cyber Defense Measures)*

Dopiero po uzyskaniu wysokiego stopnia pewności na temat źródła pochodzenia ataku należy powiadomić Cyber Investigative Joint Task Force FBI o zamiarze przeprowadzenia cyberataku i otrzymać potwierdzenie powiadomienia. Powiadomienie musi zawierać „rodzaj naruszenia cyberprzestrzeni, którego ofiarą padła osoba lub podmiot, zamierzony cel środka aktywnej cyberobrony, kroki, jakie obrońca planuje podjąć, aby zachować dowody cyberprzestępczości atakującego, a także kroki, jakie planują podjąć aby zapobiec uszkodzeniu komputerów pośredniczących, które nie są własnością atakującego i innych informacji wymaganych przez FBI w celu pomocy w nadzorze".

O ile informowanie FBI o wykorzystaniu technik ACDM jest obowiązkowe, o tyle już informacja o tym, jakie dokładnie techniki zostaną wykorzystane jest dobrowolna. Można założyć, że ofiara ataku nie będzie czekać na formalne przyzwolenie FBI, a w skrajnych przypadkach może nawet wykroczyć poza zadeklarowane wcześniej działania. Biorąc to wszystko pod uwagę można założyć, że gwarancje odpowiedzialności nie będą miały zastosowania w sposób, w jaki zostały zamierzone.

Oprócz dobrowolnego przeglądu działań przez FBI, projekt ACDC niewiele mówi o środkach nadzoru. National Cyber Investigative Joint Task Force będzie musiała opracować własne wewnętrzne procedury nadzoru i udzielania wskazówek dla firm. Jeszcze nie wiadomo, jak szczegółowo FBI będzie nadzorować programy aktywnej cyberobrony wprowadzane w firmach. Możliwe, że firmy nie zawsze uzyskają wystarczające wskazówki, aby działać w granicach prawa. Jakość realizacji ACDC zależy zatem nie tylko od samych zainteresowanych firm, ale także od wewnętrznych procedur i regulaminów FBI.

Konsekwencje prawnomiędzynarodowe

W myśl aktualnie obowiązujących przepisów, FBI potrzebowałoby nakazu, aby wejść do systemów domniemanego napastnika. Ustawa ACDC stwarza możliwość obejścia procedur prawnych, co może być niebezpieczne zarówno dla FBI, jak i dla samej ofiary. Można bowiem zastanawiać się, jakie będą konsekwencje odwetu, kiedy napastnik działa na zlecenie państwa. Przykładowo, jeśli Korea Północna włamie się do systemów teleinformatycznych amerykańskiego giganta IT, to negatywne konsekwencje międzynarodowe mogą przewyższać ewentualne korzyści wynikające z przeprowadzenia ataku. Ponadto, jak zauważają niektórzy eksperci, jeśli ustawa ACDC zostanie uchwalona, może to również stanowić precedens, który zachęci inne państwa do poluzowania własnych przepisów antyhakerskich.

Warto także dodać, że w związku z przerzucaniem części uprawnień państwa na firmy prywatne, może pojawić się niepokój związany z publicznym odbiorem takich działań, rozumianych jako

słabość państwa do wykonywania monopolu na użycie siły. Istnieje także ryzyko, że państwa będą stopniowo zmniejszać nadzór na działaniami firm w cyberprzestrzeni nawet jeśli te będą przekraczać granicę prawa. Konsekwencją takiego rozwoju sytuacji może być wymknięcie się aktywnej cyberobrony spod kontroli państwowej.

Niewystarczające przygotowanie firm

Niedofinansowane firmy zazwyczaj nie mają dobrze zdefiniowanych strategii ani metod działania w cyberprzestrzeni. Projekt ustawy ACDC nie określa, co dokładnie uprawnia firmę do podjęcia działań odwetowych. Zatem można uznać, że mogą być podejmowane zarówno przez doświadczonych gigantów sektora IT, jak i małe i nieprzygotowane do tego firmy. Skoro większość firm ma problemy z przestrzeganiem podstawowych zasad cyberhigieny, jak m.in. prowadzenie szkoleń uświadamiających w zakresie bezpieczeństwa wśród pracowników, regularnie wykonywanie kopii zapasowych danych, czy regularne łatanie luk w zabezpieczeniach, trudno oczekiwać od nich posiadania umiejętności i narzędzi do przeprowadzenia precyzyjnego i kontrolowalnego cyberataku zwrotnego. W rezultacie, nie sposób przewidzieć jego ostateczne konsekwencje.

Wnioski

Projekt ustawy ACDC wpisuje się w amerykański sposób myślenia o zapewnianiu bezpieczeństwa obywatelom. Tam, gdzie państwo nie jest w stanie zagwarantować bezpieczeństwa, należy przyznać uprawnienia obywatelom lub jednostkom prywatnym. Jednakże legalizacja cyberataku zwrotnego rodzi uzasadnione obawy związane przede wszystkim z nieprecyzyjnymi zapisami, możliwymi efektami ubocznymi, a także ewentualnymi niezamierzonymi konsekwencjami międzynarodowymi. Ryzyko eskalacji poprzez błędne przypisanie źródła pochodzenia ataku może okazać się zbyt dużą przeszkodą, aby przyjąć wniosek legislacyjny w obecnym kształcie. Pomimo oczywistej konieczności przyznania firmom prywatnym dodatkowych uprawnień w zakresie ochrony własnych sieci, najważniejsze pytanie dotyczy ceny jaką trzeba będzie zapłacić za te dodatkowe zdolności. Szef amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA), admirał Michael Rogers, na pytanie, czy aktywna obrona powinna być legalna odpowiedział, że państwa często korzystały z pomocy sektora prywatnego, gdy brakowało im odpowiednich zdolności, ale jednak „byłby nieufny wobec wypuszczania większej liczby rewolwerowców na ulice dzikiego zachodu”. Faktycznie, czasem bywa tak, że kiedy politycy próbują rozwiązać problem, proponowane lekarstwo tylko pogarsza sytuację. Politycy opowiadający się za wprowadzeniem ACDC nie rozumieją, że firmy-rewolwerowcy mogą nie mieć odpowiednich zasobów i umiejętności, a nawet mogą nie wiedzieć, w co wycelować. W świetle tych wszystkich wątpliwości nie dziwi fakt, że ACDC ma dzisiaj zaledwie 2 proc. szans na wprowadzenie w życie.