Michał Kleiber

PAŃSTWO JAKO LIDER DZIAŁAŃ W ZAKRESIE CYBERBEZPIECZEŃSTWA

Mimo wielu bardzo znamiennych w tej sprawie wydarzeń nie wszyscy jeszcze uświadamiają sobie fakt, iż charakter znacznej części dzisiejszych zagrożeń dla obywateli, firm czy wręcz całych państw jest zasadniczo różny od sytuacji sprzed kilkunastu lat. Powodem są oczywiście często dramatyczne w skutkach problemy zwane w skrócie naruszeniem cyberbezpieczeństwa. Zagrożenia prywatności obywateli, możliwość zakłócania funkcjonowania instytucji państwowych i przedsiębiorstw, niebezpieczeństwo pozbawienia całych regionów dostępu do energii elektrycznej z wręcz niewyobrażalnymi konsekwencjami dla wszystkich, wreszcie międzypaństwowe konflikty o tzw. hybrydowym charakterze, to tylko przykłady problemów charakterystycznych dla dzisiejszego świata. Powszechny dostęp do internetu i złożoność funkcjonowania całego systemu komunikacji sieciowej tworzą wręcz nieograniczone możliwości podejmowania przestępczych działań. Najkrótszy nawet opis różnego rodzaju cyberprzestępstw popełnionych tylko w ostatnim roku zająłby wiele stron tekstu. Aby zilustrować choćby skalę zagrożeń przytoczmy za zeszłorocznym Internet Security Threat Raport przykładowo następujące dane – w roku 2016 wykryto prawie 150 mln rodzajów złośliwego oprogramowania, zidentyfikowano ponad miliard kradzieży tożsamości użytkowników z baz danych, a w przedsiębiorstwach średnio co pół godziny ktoś nieświadomie przesyłał do sieci ważne dla firmy poufne dane. Wobec oczywiście niekwestionowanego przez nikogo faktu niezbędności dalszego istnienia elektronicznej komunikacji i leżącej u jej podstaw idei w dużej mierze niekontrolowanego działania wszystkich jej użytkowników, problem jest oczywisty – inaczej niż w przeszłości, w sieciowym świecie każdy może zaatakować innych mając szanse na skuteczność swych działań. A ów każdy to dzisiaj często profesjonalna grupa stosująca wysoce wyspecjalizowane i trudne do rozszyfrowania metody ataku. Jeszcze groźniejszą czyni tę sytuację fakt, iż za grupami tymi stoją często służby specjalne obcych państw, wyspecjalizowane w zdobywaniu tajnych informacji czy wręcz w destabilizowaniu politycznym i gospodarczym swych sąsiadów bądź globalnych konkurentów.

Konsekwencje nieuprawnionych działań w sieci mogą być olbrzymie, bowiem we współczesnym świecie funkcjonowanie państwa, poszczególnych instytucji i pojedynczych obywateli bazuje w istotnej mierze na niezakłóconym działaniu istniejących systemów teleinformatycznych. Naruszenie, czy często jeszcze gorzej – zafałszowanie ich funkcjonalności, staje się szczególnie groźne w przypadku infrastruktury krytycznej, czyli problemów dotyczących najważniejszych obiektów, urządzeń, instalacji i kluczowych usług państwa. Systemy energetyczne, bankowe, ochrony zdrowia,

transport na czele z ruchem lotniczym, wiele innych instytucji o ważnym znaczeniu dla funkcjonowania państwa nie może dzisiaj obejść się bez sprawnej komunikacji sieciowej. Cyberatak na nie może prowadzić do wielkich szkód i zniszczeń, zagrażających także często życiu ludzkiemu i środowisku naturalnemu. Liczbę urządzeń podłączonych na świecie do internetu szacuje się obecnie na 30 mld, a tempo przyrostu tej liczby związane z rozwojem tzw. internetu rzeczy przekracza możliwości wiarygodnych oszacowań. W podobnie zawrotnym tempie rosną więc zapewne także możliwości popełniania sieciowych przestępstw. Stoimy wobec problemu, o którym trzeba dobitnie mówić i domagać się podejmowania odpowiednich działań przez właściwych decydentów. Kluczową rolę ma tu do odegrania państwo – konsekwentna polityka wyprzedzająca przestępcze zdarzenia w sferze bezpieczeństwa jest w nowoczesnym państwie koniecznością. Państwo powinno oczywiście w pierwszej kolejności podejmować działania skierowane na przeciwdziałanie potencjalnym problemom, a nie tylko koncentrować się na ich późniejszym usuwaniu. Polityka taka to z jednej strony odpowiednie regulacje na rynku telekomunikacyjnym i nadzór nad jego funkcjonowaniem, a z drugiej przemyślany system zachęt dla operatorów telekomunikacyjnych i innowacyjnych firm do podejmowania inicjatyw zwiększających cyberodporność na sieciowe przestępstwa. Istotne jest także znaczenie powszechnej edukacji na rzecz cyberodporności – dosłownie wszyscy musimy się uczyć i poznawać możliwości obrony przed sieciowymi przestępstwami.

Przeciwdziałanie sieciowym atakom utrudnia fakt niezwykłej różnorodności motywacji cyberprzestępców. W szerokim kontekście obywatelskim podejmowane działania mogą służyć np. wywołaniu szerokich protestów społecznych bądź wręcz nawoływaniu do aktywnej walki z władzą, w kontekście gospodarczym kradzieży technologii, zakłóceniom zautomatyzowanych procesów wytwórczych bądź deprecjonowaniu rynkowych konkurentów (w krajach rozwiniętych już ponad 50 proc. firm doświadczyło takich działań), w kontekście politycznym nieuprawnionym formom (np. podszywającym się pod stanowisko renomowanych instytucji) promocji poglądów politycznych i oczerniania zwolenników innych ideologii, w kontekście militarnym prowadzeniu wojen hybrydowych, w których propaganda sieciowa stała się nieodłącznym elementem osłabiania przeciwnika. Nie można także pominąć problemu cyberprzestępczości w kontekście pojedynczych obywateli – prowadzone niekiedy z jawną premedytacją niszczenie wizerunku osób publicznych stało się zmorą współczesnej przestrzeni publicznej.

Różnorodne są także narzędzia używane przez cyberprzestępców. Należą do nich m.in. tzw. *spyware*, czyli programy szpiegujące użytkowników sieci bez ich wiedzy, *phishing*, czyli podstępne zdobywanie loginów i haseł, konie trojańskie, czyli programy podszywające się pod interesujące aplikacje, a mające w sobie dodatkową, niepożądaną funkcjonalność, bomby logiczne, czyli złośliwe oprogramowanie aktywizujące się po spełnieniu przez użytkownika określonych warunków, np. wybranej godziny bądź dnia, wreszcie tzw. *hoax'y*, czyli programy wyświetlające nieprawdziwą informację o istnieniu w urządzeniu wirusa. Połączenie powyższych metod z przemyślanymi działaniami socjotechnicznymi prowadzić może do tzw. APT (ang. Advanced

Persistent Threat), polegającego na ustaleniu zaplanowanych do ataku instytucji i osób, infiltracji ich urządzeń i podjęciu często długotrwałych działań o charakterze przestępczym. Już niebawem szczególną rolę w sprawach cyberprzestępczości odgrywać będzie z pewnością oprogramowanie wyposażone w tzw. sztuczną inteligencję (AI). Świadome tego potencjału światowe mocarstwa przeznaczają obecnie olbrzymie sumy na rozwój AI i jej zastosowań. Nawet jeśli głównym celem tego wsparcia są aplikacje cywilne mające prowadzić do korzyści ekonomicznych, świadomość tzw. *dual use*, czyli możliwości wykorzystywania osiągnięć badawczych sektora cywilnego do wzmacniania swej potęgi militarnej, każe oceniać inwestycje w AI także w kategoriach bezpieczeństwa.

Faktem jest, iż rozwój technologii wyprzedza dzisiaj znacznie pełne rozpoznanie ich innowacyjnych zastosowań i uniemożliwia szybkie wypracowanie procedur regulacyjnych. A to, wobec i tak z reguły opóźnionego procesu legislacyjnego, czyni sytuację niezwykle groźną. Cóż więc robić? Do działań niezbędnych do prowadzenia na poziomie państwa w celu zapewnienia właściwego poziomu bezpieczeństwa cyberprzestrzeni zaliczyć należy m.in.:

- jasne określenie odpowiedzialności za koordynację polityki bezpieczeństwa państwa i obywateli – kluczowa jest tu ponadresortowa rola kierownictwa rządu koordynującego działania podległych mu jednostek administracji państwa,
- ustalenie i konsekwentna realizacja państwowego programu ochrony cyberprzestrzeni, ze szczególnym naciskiem na bezpieczeństwo infrastruktury krytycznej,
- ustalenie regulacji prawnych dotyczących wymiany informacji oraz współpracy między instytucjami państwowymi a podmiotami prywatnymi, w szczególności operatorami telekomunikacyjnymi i wiodącymi dostawcami usług informatycznych i sprzętu,
- stworzenie systemu wymiany informacji operacyjnych pomiędzy podmiotami państwowymi i prywatnymi zaangażowanymi w ochronę cyberprzestrzeni,
- sukcesywne, zależne od powstających potrzeb wprowadzanie regulacji prawnych, precyzyjnie ustalających sposoby prowadzenia aktywnej ochrony cyberprzestrzeni i umożliwiających podejmowanie działań wyprzedzających,
- skrupulatne zbieranie szczegółowych informacji o zrealizowanych atakach w cyberprzestrzeni w kraju i na świecie oraz cykliczne prowadzenie pogłębionych analiz istniejącego ryzyka kolejnych takich ataków,
- precyzyjne powiązanie systemu ochrony cyberprzestrzeni w kraju z działaniami podejmowanymi w ramach Unii Europejskiej i NATO, a także z inicjatywami globalnymi, dotyczącymi np. problemu zarządzania internetem,
- wspieranie krajowych ośrodków naukowo-technicznych, prowadzących badania i prace wdrożeniowe w zakresie bezpieczeństwa cyberprzestrzeni, z wykorzystaniem możliwości współpracy międzynarodowej z instytucjami państw NATO,
- wykorzystywanie krajowych innowacyjnych firm działających w tym obszarze,

- uruchamianie programów edukacyjnych, skierowanych do urzędników i funkcjonariuszy państwowych, a także do wszystkich obywateli w celu systematycznego zwiększania ich świadomości co do zagrożeń wynikających z użytkowania sieci komputerowych i internetu,
- uruchamianie podobnych programów edukacyjnych w szkołach wszystkich typów.

Zapewnienie wysokiego poziomu bezpieczeństwa za absolutny priorytet uznaje od dawna Unia Europejska. Kolejno przyjmowane w Brukseli analityczne dokumenty takie jak „Strategia bezpieczeństwa cybernetycznego UE" z roku 2013, „Strategia jednolitego rynku cyfrowego" z 2015 r. czy podstawowa regulacja pt. „Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE" z 2016 r. są jednoznacznym dowodem dostrzeżenia powagi problemu. W dokumentach tych cyberbezpieczeństwo definiuje się jako „odporność sieci i systemów informatycznych na wszelkie działania naruszające dostępność, autentyczność, integralność bądź poufność przechowywanych, przekazywanych i przetwarzanych danych lub związanych z nimi usług dostępnych przez te sieci i systemy". Odpowiedzialnością za cyberbezpieczeństwo obciążono nie tylko sektor publiczny w państwach członkowskich, ale także sektor prywatny.

Aby zapewnić prawidłową realizację dyrektywy każde z państw członkowskich powinno m.in. wyznaczyć krajowe organy właściwe do spraw bezpieczeństwa sieci i systemów informatycznych, ustalić tzw. punkt kontaktowy, pełniący funkcję łącznikową, zapewniający współpracę na poziomie całej Unii oraz wyznaczyć zespoły szybkiego reagowania na wszelkie incydenty dotyczące cyberbezpieczeństwa. Zalecenia dyrektywy obowiązują kraje członkowskie Unii od maja bieżącego roku. Pytaniem oczywiście jest czy wszystkie państwa są przygotowane do właściwej realizacji zaleceń dyrektywy.

Wiele z powyższych postulatów ujętych jest w nowej polskiej ustawie o cyberbezpieczeństwie, obowiązującej od końca sierpnia 2018. Ustawa wyznacza Ministerstwo Obrony Narodowej, Agencję Bezpieczeństwa Wewnętrznego i Naukowo-Akademicką Sieć Komputerową jako instytucje odpowiedzialne za całość tej problematyki w państwie. Instytucje te mają przyjmować od użytkowników zgłoszenia wszystkich naruszeń bezpieczeństwa i podejmować odpowiednie działania zaradcze.

W podsumowaniu powiedzmy dobitnie, że definiowanie wyzwań i określenie właściwych działań dotyczących cyberbezpieczeństwa bez wątpienia będzie stawało się w przyszłości coraz trudniejsze. Przesądza o tym szybki rozwój technologii i jej wpływ na wszystkie w istocie sektory życia publicznego. Pewien ważny artykuł opublikowany ostatnio w amerykańskiej prasie nosił tytuł *Our future is hackable* (w wolnym tłumaczeniu – nasza przyszłość jest podatna na sieciowe ataki) – wobec ogromu potencjalnych strat państwo już dziś musi myśleć i działać, nadając cyberbezpieczeństwu wysoki priorytet, uprzedzając możliwe zdarzenia. Ze względu na wagę i zakres tej problematyki to właśnie szeroko rozumiana administracja państwa musi być liderem działań chroniących społeczeństwo przed sieciowymi przestępstwami.