Wojny szyfrów

Działka w podwarszawskim Legionowie, na której terenie funkcjonuje Narodowe Centrum Kryptologii, ma 27 ha. Do tej pory gospodarzem obiektu, liczącego 16 budynków, była 1. Warszawska Dywizja Zmechanizowana. W ub.r. Ministerstwo Obrony Narodowej postanowiło zamienić koszary na nowoczesny kompleks laboratoryjno-obliczeniowy, który docelowo ma dysponować największą mocą obliczeniową spośród wszystkich jednostek polskich sił zbrojnych. Wprowadzili się do niego matematycy i kryptolodzy pracujący nad prototypami nowych urządzeń i algorytmów szyfrujących. Powierzono im ochronę rządowych tajemnic. Tym samym, po latach przerwy, Polska wraca do rywalizacji na arenie międzynarodowej kryptologii. Pół wieku temu to nasi rodacy pierwsi złamali słynny szyfr Enigmy. Zdaniem specjalistów potencjału nie brak nam i dziś.

Polska twierdza szyfrów

Choć Narodowe Centrum Kryptologii (NCK) formalnie utworzono już w kwietniu 2013 r., dopiero w tym roku pracownicy wprowadzili się do nowej siedziby. Powołanie tak wyspecjalizowanej instytucji to także powrót do przedwojennej tradycji – słynnego Biura Szyfrów. NCK podlega bezpośrednio ministrowi obrony narodowej i jest jedną z najbardziej strategicznych gałęzi naszego systemu obronnego. – Głównym zadaniem Narodowego Centrum Kryptologii jest konsolidacja kompetencji i zasobów resortu obrony narodowej w dziedzinie kryptologii. Centrum ma zapewnić rozwój polskiej kryptologii, m.in. tworząc normy i standardy kryptograficzne, stymulując działania polskich instytucji i przemysłu w zakresie kryptologii, jak również uczestnicząc w wytwarzaniu i użytkowaniu odpowiednich narodowych urządzeń i technologii – wylicza płk Jacek Sońta, rzecznik MON. Na realizację tych zamierzeń kryptolodzy otrzymali od Narodowego Centrum Badań i Rozwoju 120 mln złotych.

Centrum skupia się przede wszystkim na działalności badawczej i funkcjonuje na zasadzie partnerstwa publiczno-prywatnego. Zatrudnieni w nim matematycy i urzędnicy współpracują więc z uczelniami i firmami prywatnymi z sektora obronnego. Tym samym nie jest to kolejna służba specjalna, jak chcieliby niektórzy, porównując Narodowe Centrum Kryptologii do amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA). Przynajmniej na razie. Dalsze losy i rozwój jednostki objęte są bowiem tajemnicą państwową i MON niechętnie wypowiada się na ten temat.

Faktem jest, że wojskową i cywilną kryptologię musimy tworzyć dziś właściwie od zera, bo do tej pory byliśmy uzależnieni od naszych zachodnich sojuszników, począwszy od algorytmów, na maszynach szyfrujących kończąc. Wiele rodzimych urzędów korzysta z zagranicznych urządzeń szyfrujących, częstokroć nie mając do nich kodów źródłowych. Kolejnym krokiem po utworzeniu Narodowego Centrum Kryptologii powinno być więc wykształcenie specjalistów na potrzeby rodzimego rynku. W tym celu w zeszłym roku NCK zamówiło w Wojskowej Akademii Technicznej studia z zakresu bezpieczeństwa systemów teleinformatycznych oraz przeciwdziałania zagrożeniom

w cyberprzestrzeni. Podobne umowy o stworzeniu studiów kryptograficznych podpisały też inne uczelnie, w tym Politechnika Warszawska i Politechnika Wrocławska.

– Państwo musi mieć własne rozwiązania kryptologiczne, musi też mieć pewność, że bezpieczne są technologie stosowane w urządzeniach do przesyłania ważnych danych – mówił w lutym płk Jacek Rychlica, kiedy obejmował funkcję dyrektora Narodowego Centrum Kryptologii. Zapewniał przy tym, że wszystkie nasze wojskowe systemy teleinformatyczne, którymi są przesyłane informacje niejawne, oddzielone są od wszelkich innych systemów, w tym od internetu.

Nasłuch elektroniczny sieci internetowej to zresztą kolejne zadanie centrum. W przypadku ataku hakerów na nasze systemy obronne NCK pełni funkcję Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej. Jest to o tyle ważne, że działania wojenne prowadzi się dziś równie skutecznie przed monitorem komputera co na polu walki. Wystarczy zaatakować elektrownię, wodociągi, system bankowy czy komunikację przeciwnika, by na jego terytorium zapanował chaos.

Kody użytku codziennego

Przeciętnemu człowiekowi kryptologia kojarzy się z wyjątkowo tajemniczą dziedziną nauki, zarezerwowaną dla nielicznych. Tymczasem wszyscy posługujemy się nią każdego dnia, w bardziej lub mniej świadomy sposób. Rozmaite kody i szyfry wykorzystujemy, surfując choćby po internecie; z kolei algorytmy autoryzacyjne towarzyszą nam, kiedy wprowadzamy hasła do kont bankowych, bankomatów, telefonów czy wklepujemy kod uaktywniający alarm w mieszkaniu. Kupując płytę DVD z dowolnym filmem lub grą spotykamy się z kodowaniem, które uniemożliwia kopiowanie jej zawartości. Podstawą zrozumienia tego typu kodów jest znajomość klucza, wedle którego należy je czytać.

Zanim z dobrodziejstw współczesnej kryptologii zaczęli korzystać przedstawiciele branż cywilnych, rozwój tej dyscypliny był ściśle związany z działaniami militarnymi. Najpierw w czasie II wojny światowej, kiedy pojawiły się pierwsze elektromechaniczne i elektroniczne maszyny szyfrujące, jak niemiecka Enigma, a następnie wraz z pojawieniem się pierwszych komputerów. W latach 60. zainteresowanie kryptologią, zwłaszcza kryptografią, wykazał sektor prywatnych przedsiębiorców, co było spowodowane upowszechnieniem się elektronicznych form przekazywania informacji.

W następnej dekadzie położono najważniejszy chyba w dziejach kryptografii kamień milowy – w 1976 r. Whitfield Diffie i Martin Hellman opublikowali pracę „New Directions in Cryptography", w której zaprezentowali koncepcję szyfrowania z kluczem publicznym. Za sprawą ich publikacji wyższa matematyka stała się przedmiotem ożywionej debaty publicznej, a niektórzy zaczęli dostrzegać w kryptologii jedną z najgroźniejszych broni znanych ludzkości. W świecie coraz bardziej uzależnionym od techniki dostęp do informacji staje się coraz ważniejszy.

Po II wojnie światowej wiele zachodnich państw ustanowiło rygorystyczne rozwiązania prawne związane z eksportem technologii kryptograficznych. W USA za sprzedaż technologii kryptograficznych za granicę przez dekady można było trafić do więzienia. Bez względu na to, komu i w jakim celu taki transfer miał służyć. To się zmieniło dopiero w 1996 r. Doszło wówczas do podpisania przez 39 państw (w tym Polskę) porozumienia Wassenaar, które zezwalało na eksport uzbrojenia i technologii podwójnego zastosowania, w tym kryptografii. W myśl traktatu technologie szyfrowania oparte na krótkich kluczach (56-bitowych dla szyfrów symetrycznych i 512-bitowych dla RSA) nie podlegają ograniczeniom eksportowym. Dziś Polska idzie o krok dalej. Nie chce tylko kupować dostępnych rozwiązań, ale ma ambicje tworzyć własne.

Konflikty w sieci

Największymi eksporterami technologii kryptograficznych są dziś USA. Oczywiście nasi sojusznicy nie chcą się dzielić wszystkimi tajemnicami; najbardziej zaawansowane szyfry zostawiają sobie. Amerykanie mają też swoją Agencję Bezpieczeństwa Narodowego (NSA), odpowiedzialną za wywiad elektroniczny. W jej głównej siedzibie w Fort Meade (Maryland) zatrudnionych jest ponad 40 tys. matematyków, którzy pracują nad udoskonalaniem algorytmów stosowanych przez amerykańskie służby specjalne, administrację rządową i wojsko. Analitycy mają do dyspozycji globalną sieć dozoru źródeł emisji fal elektromagnetycznych, posługują się własnymi samolotami, systemem stacji naziemnych oraz satelitami. W trosce o bezpieczeństwo produkują nawet własne mikroprocesory. Dziś podobną instytucją może się pochwalić większość wysokorozwiniętych państw. Wystarczy wspomnieć brytyjską Centralę Łączności Rządowej, kanadyjską Służbę Bezpieczeństwa Łączności czy australijski Zarząd Łączności Ministerstwa Obrony.

Problem cyberzagrożeń i hakowania strategicznie wrażliwych danych dotyczy niemal wszystkich rządów. Nie jest to rzecz nowa, bo do systemów informatycznych włamywano się już za czasów wojny w Zatoce Perskiej. Naturalnie zmienia się jednak skala działań, bo internet z każdym rokiem staje się coraz bardziej integralną częścią naszego życia i bezpieczeństwa. O atakach na strategiczne obiekty państwowe z pewnością wiele mogliby powiedzieć Amerykanie. Co roku dochodzi tam do… 500 tys. hakerskich ataków, które mają na celu zdezorganizowanie pracy państwa i jego obywateli.

Głośnym echem odbiła się sprawa inwigilowania kanadyjskiego systemu teleinformatycznego Nortel. Hakerzy, działający przede wszystkim z terytorium Chin, przez 10 lat mieli pełny dostęp do wewnętrznej sieci komputerowej firmy: wiadomości pocztowych, sprawozdań finansowych, dokumentacji technicznej i wyników badań. Niedawno ofiarą hakerów padło również Sony, skąd wykradziono plany rozwoju firmy, prywatną korespondencję oraz wiele nieupublicznionych jeszcze materiałów filmowo-graficznych.

Do ataków dochodzi nie tylko na poziomie wielkiego biznesu. Zagrożone są również tajne dane państwowe, na które chrapkę mają najwięksi gracze na arenie międzynarodowej. Tajemnicą poliszynela jest, że USA, Rosja czy Chiny mają na swoich usługach cały sztab hakerów, którzy każdego dnia toczą ze sobą wirtualną wojnę na informacje i zabezpieczenia. Wygra ten, kto stworzy szyfr zdolny oprzeć się wszelkim próbom złamania.

O tym, że nie jest to łatwe, przekonały się władze Estonii w kwietniu 2007 r. Doszło wówczas do największego w dziejach ataku hakerskiego na państwo. Hakerom udało się na całe tygodnie zdezorganizować internetową strukturę kraju. Wszystko zaczęło się od decyzji władz Estonii, które zarządziły demontaż pomnika żołnierzy radzieckich w Tallinie. Doszło przy tej okazji do demonstracji i kryzysu dyplomatycznego na linii Estonia–Rosja. Największa walka rozegrała się jednak w sieci. Nieznani sprawcy sparaliżowali najważniejsze serwery w kraju. Fala spamu zablokowała m.in. serwer obsługujący pocztę elektroniczną estońskiego parlamentu, a kilkanaście dni później na godzinę zablokowano serwis największego banku Estonii, w wyniku czego straty wyliczono na miliony dolarów. Mimo że ślady prowadzą do Rosji, nigdy nie udało się znaleźć twardych dowodów na potwierdzenie tych zarzutów.

Ogółem roczne straty dla światowej gospodarki spowodowane cyberatakami mogą sięgać nawet 500 mld dolarów. Oczywiście nie da się stworzyć systemu idealnego. Przykład USA pokazuje, że nawet najbardziej wymyślne zabezpieczenia padają wobec akcji sabotażowych, jak w przypadku Edwarda Snowdena czy Juliana Assange’a. Wyścig kryptologiczny jednak trwa. I choć Polska dopiero buduje struktury, niewykluczone, że za kilka lat będziemy mogli się pochwalić osiągnięciem na miarę przedwojennych bohaterów.

Autor: **Kamil Nadolski**

Więcej w miesięczniku „Wiedza i Życie" nr 09/2015 »
https://laboratoria.net/felieton/24116.html
Informacje dnia: Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego

Partnerzy