aut. Maksymilian Dura 20.03.2020

NARODOWA KRYPTOLOGIA KLUCZEM DO SUWERENNOŚCI TECHNOLOGICZNEJ

Chociaż od lat eksperci i urzędnicy mówią o konieczności rozwijania suwerenności technologicznej, w wielu obszarach państwa brakuje spójnych i długofalowych strategii, które wymuszałyby adekwatne działania. W newralgicznych obszarach bezpieczeństwa potrzebne są decyzje, które pozwolą wykorzystać krajowe zasoby zarówno intelektualne jak i produkcyjne do budowy systemu opartego na synergii potencjałów przy zachowaniu strategicznej kontroli państwa.

Szybki wzrost zagrożeń teleinformatycznych i kolejne informacje o incydentach i naruszeniach powodują, że kwestia szeroko rozumianej cybersuwerrenności nie schodzi z agendy publicznej. Jednym z głównych zagrożeń na jakie wskazują eksperci jest nadmierne uzależnienie od technologii i urządzeń produkowanych za granicą. Szczególnie dotyczy to systemów bezpieczeństwa narodowego i infrastruktury krytycznej.

- *Nowa strategia cyfrowa da Unii technosuwerenność* – mówi nowa szefowa KE Ursula von der Leyen, która za swój główny cel polityczny na najbliższe lata stawia uniezależnienie UE od amerykańskich i chińskich gigantów technologicznych. To warunek konieczny dalszego rozwoju gospodarczego, naukowego czy w obszarze innowacji. I chociaż cyfrowa strategia UE nie będzie obejmować kwestii systemów bezpieczeństwa, bo te są zarezerowane dla państwa narodowych, dla wszystkich członków wspólnoty powinien być to wyraźny sygnał ostrzegawczy.

Dlaczego budowa suwerenności technologicznych w strategicznych obszarach jest taka ważna? Z informacji opublikowanych niedawno przez „The Washington Post" wynika, że agencja CIA potajemnie wykupiła i kontrolowała szwajcarską firmę Crypto AG, produkującą zaawansowane rozwiązania kryptograficzne, które mogły służyć Amerykanom do działań wywiadowczych.

O współpracy amerykańskiej agencji wywiadowczej z Crypto AG wiadomo już było z przecieku opublikowanego w 1995 roku przez gazetę „The Baltimore Sun", ale z informacji ujawnionej ostatnio przez „The Washington Post" wynika, że agencja CIA miała pełną kontrolę nad szwajcarską firmą. Według dziennikarzy „The Washington Post" urządzenia te były tak zaprojektowane, by z zewnątrz, bez wiedzy użytkowników można było odszyfrowywać informacje przekazywane za ich pośrednictwem.

Jednocześnie, już od 1994 roku, Crypto AG jest właścicielem firmy InfoGuard AG dostarczającej rozwiązania szyfrujące dla banków. Jest więc bardzo prawdopodobne, że w najgorszym scenariuszu Amerykanie mogli mieć dostęp do najważniejszych informacji politycznych, oraz gospodarczych i bankowych tych krajów, które z rozwiązań Crypto AG korzystały.

W roku 1999, uchwalona została *Ustawa o ochronie informacji niejawnych* (znowelizowana dnia 5 sierpnia 2010 r.). Ustawa stwierdza min., że cyt. „urządzenia i narzędzia kryptograficzne

przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych: albo przez ABW (w obszarze cywilnym), albo SKW" - Służbę Kontrwywiadu Wojskowego (w obszarze wojskowym).

Oba te podmioty realizują swoje ustawowe zadania w oparciu o własne polityki:

- W sierpniu 2011 roku, ABW ogłosiła i wprowadziła w życie „Politykę Kryptograficzną Agencji Bezpieczeństwa Wewnętrznego". W dokumencie tym przedstawione zostały wytyczne i zasady obowiązujące producentów rozwiązań kryptograficznych w obszarze cywilnym. W dokumencie stwierdzono min., że cyt. „projektowanie, wytwarzanie lub modernizacja urządzeń narzędzi kryptograficznych służących do ochrony informacji niejawnych …. musi być od początku realizowane we współpracy oraz nadzorem i na zasadach określonych przez ABW".
- Dokument o podobnym charakterze w obszarze wojskowym, pn „Kierunki rozwoju systemu ochrony kryptograficznej w resorcie Obrony Narodowej" został wprowadzony dopiero 8 grudnia 2017 roku przez Narodowe Centrum Kryptologii (przemianowane 5 marca 2019 roku w Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni).

„Polityka Kryptograficzna Agencji Bezpieczeństwa Wewnętrznego" jest dostępna na stronie ABW, natomiast „Kierunków Rozwoju…" nie ma na stronie NCBC– chociaż nie są one niejawne. Pewne założenia można jednak znaleźć w opublikowanym na oficjalnych stronach rządowych zakresie zadań Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. Przegląd tych ustaleń wyraźnie wskazuje na konieczność rozwijania zaawansowanych technologii informatycznych i kryptograficznych oraz to, że służby odpowiedzialne za realizację ustawowych zadań w zakresie ochrony informacji niejawnych, preferują rozwiązania narodowe, polskie.

Ustawowe, pryncypialne podejście do kwestii bezpieczeństwa informacji, umożliwiło podjęcie prac nad narodowymi rozwiązaniami, w pełni weryfikowalnymi i nadzorowanymi przez służby i zachęciło polskie firmy do badań i produkcji polskich rozwiązań kryptograficznych. Od początku 2000 roku, polscy producenci oferują wysokiej jakości urządzenia kryptograficzne służące do ochrony informacji o klauzulach *Zastrzeżone* i *Poufne* (posiadające certyfikaty ABW lub SKW).

W przypadku Służb Kontrwywiadu Wojskowego aktualnych obecnie certyfikatów wydano osiem: w tym trzy dla Wojskowego Instytutu Łączności i pięć dla spółki Enigma Systemy Ochrony Informacji Sp. z o.o. W przypadku Agencji Bezpieczeństwa Wewnętrznego sprawdzonych i dopuszczonych urządzeń jest więcej – bo jedenaście. Sześć z nich otrzymała firma Krypton Polska Sp. z o.o, a pięć otrzymała firma Enigma SOI Sp. z o.o.

Jednakże, do ochrony informacji o klauzuli *Tajne,* dopuszczone zostało tylko jedno rozwiązanie (o wyjątkowo małej przepustowości, jak na dzisiejsze czasy), a kompletnych rozwiązań *Ściśle Tajne*, zgodnie z listami publicznie dostępnymi nie ma w ogóle. Dzieje się tak, pomimo że polskie instytuty badawcze i przemysłowe są w stanie opracować i produkować również nowoczesne rozwiązania także dla najwyższych klauzul ochrony.

Bez wsparcia Agencji Bezpieczeństwa Wewnętrznego i SKW (oraz NCBC) w zakresie pozyskania modeli stosownych algorytmów oraz jasnej polityki zamówieniowej, prywatne firmy nie będą ryzykować angażowania znacznych, własnych środków na produkcję urządzeń „na półkę". Firmy państwowe (lub spółki z udziałem skarbu Państwa), w ostatnich 10 latach nie certyfikowały żadnego rozwiązania kryptograficznego.

Siły Zbrojne RP, pozyskiwały krajowe urządzenia kryptograficzne jednostkowo i wykorzystywały je w systemach informatycznych o niższych klauzulach tajności. Sprzęt do wyższych klauzul oraz urządzenia zabezpieczające działania typowo wojskowe (np. pracujące w ramach systemów

współpracujących z systemami NATO) były (i być może są), kupowane za granicą.

Zmiany w tych praktykach zapowiedziały dopiero „Kierunki rozwoju systemu ochrony kryptograficznej w resorcie Obrony Narodowej", z których wynikała m.in. chęć tworzenia w kraju wszystkich elementów ochrony kryptograficznej. Ta chęć nie oznacza jednak zaangażowania w to polskiej nauki i przemysłu, ale przejęcie tych zdań przez szeroko pojęte „państwo". Kto jednak konkretnie w tym państwie miałby się zajmować produkcją szyfratorów jak na razie nie wiadomo. Polski przemysł, który ma kompetencje w tym zakresie i już wiele certyfikowanych wyrobów ochrony kryptograficznej z zaniepokojeniem obserwuje niektóre deklaracje wojskowych.

Łatwo jest zrozumieć, czemu ma służyć zasygnalizowane w „Kierunkach rozwoju SOK w MON" przejmowanie przez NCK (obecnie NCBC) wszelkich wyrobów (demonstratorów technologii, prototypów, oprogramowania, dokumentacji itp.) realizujących zadania szyfrujące, wraz z majątkowymi prawami autorskimi. Ponieważ jest to jednak wyraźny drenaż technologii z firm projektujących i de facto oznacza zastopowanie innych prac danej firmy w tym zakresie, bez wskazania, kto i jak miałby dalsze prace później kontynuować (np. produkować), polskie prywatne przedsiębiorstwa mają opory przed tak określoną współpracą. Tymczasem istnieją już dobrze sprawdzone procedury zapewnienia bezpieczeństwa, które wcale nie muszą być związane z gromadzeniem wszystkiego w magazynach NCBC.

Wydane certyfikaty oraz zrealizowane programy rozwojowe potwierdzają tezę, że Polska posiada bazę naukową i przemysłową do uzyskania samodzielności, jeżeli chodzi o zabezpieczenie kryptograficzne na wszystkich poziomach niejawności. Prawdą jest również, że istnieją dokumenty nakazujące korzystanie z tej bazy w celu uzyskania pełnej autonomii w działaniu. Do wykorzystania tych dwóch atutów potrzebna jest jednak wola i konkretne działania, których jak na razie nie widać: ani ze strony cywilnej (ABW), ani ze strony wojskowej (SKW, NCBC).

Jeżeli istnieją dwa niezależne ośrodki certyfikujące: ABW i SKW, to czy nie należałoby się zastanowić nad pełnym ujednoliceniem zasad certyfikacji, tak aby obie te służby mogły się wzajemnie wspierać, np. wspólnie realizując badania? Założenie Narodowego Centrum Kryptologii dawało nadzieję, że rzeczywiście może dojść do takiej koordynacji.

Warunkiem posiadania suwerenności technologicznej przez dowolne państwo jest posiadanie własnych, narodowych rozwiązań w zakresie ochrony swoich najważniejszych informacji (niejawnych i innych, stanowiących tajemnice). Urządzenia zapewniające ochronę informacji niejawnych i wrażliwych, powinny być produkowane przez polskie firmy. Kontrolowanie przez amerykańską agencję wywiadu CIA firmy Crypto AG dostarczającej urządzenia szyfrujące (lub jakiejkolwiek innej, obcej służby oczywiście), dobitnie o tym przekonuje.