Materiał Kancelarii Prawnej Skarbiec. Redakcja „Gazety Wyborczej" nie odpowiada za treść materiału.

SKARBIEC KANCELARIA PRAWNA

Nie martw się. To dla twojego dobra

MEC. **ROBERT NOGACKI**

Właściciel Kancelarii Prawnej Skarbiec

● Amnesty International udostępniła nieodpłatny program komputerowy, który wykrywa narzędzia szpiegostwa elektronicznego używane przez agencje rządowe do monitorowania swoich obywateli. Program, noszący nazwę Detekt, można pobrać ze strony internetowej resistsurveillance.org. Oprogramowanie powstało dzięki współpracy Amnesty International, Digitale Gesellschaft, Electronic Frontier Foundation oraz Privacy International.

Jak twierdzi Marek Marczyński z Amnesty International, rządy w coraz większym stopniu wykorzystują niebezpieczne i zaawansowane technologie, które umożliwiają im wgląd w e-maile dziennikarzy i aktywistów albo pozwalają zdalnie zamieniać mikrofony i kamery wbudowane w komputerach w wyrafinowane narzędzia inwigilacji. Dziś większą aktualność niż kiedykolwiek zachowuje rada Winstona z „Roku 1984": *„Jeśli chce się zachować tajemnicę, należy ukryć ją nawet przed sobą. Trzeba pamiętać o niej bez przerwy, lecz dopóki nie nadejdzie właściwa chwila, nie należy ani ubierać jej w słowa, ani pozwolić, aby przeniknęła do świadomości"*. Być może nie musimy jeszcze ukrywać tajemnic przed samymi sobą, ale zdecydowanie nie powinniśmy przesyłać ich e-mailem ani omawiać telefonicznie.

Organizacja Coalition Against Unlawful Surveillance Exports szacuje, że rynek oprogramowania szpiegowskiego wart jest już 5 mld dolarów rocznie, co wskazuje, jak ogromne pieniądze są przeznaczane przez rządy i międzynarodowe korporacje na inwigilację swoich obywateli i pracowników. Cenzura Internetu i inwigilacja obywateli to dziś ogromny przemysł, w którym o lukratywne kontrakty zabiegają największe korporacje.

Wśród wyróżnionych przez Reporterów bez Granic przeciwników Internetu znalazła się włoska firma Hacking Team, której oprogramowanie do infiltrowania komunikacji elektronicznej używają przypuszczalnie rządy Maroka i Zjednoczonych Emiratów Arabskich. Rząd Bahrajnu infiltrował komunikację opozycji za pomocą programu FinFisher Suite, którego dystrybucją zajmują się niemieckie i angielskie firmy o nazwie Gamma International. Muammar Kaddafi szpiegował Internet za pomocą programu EAGLE, który sprzedała mu francuska firma komputerowa Amesys. Rozwiązania oferowane przez amerykańską firmę Blue Coat wdrożyły rządy Syrii i Birmy, a związany z Uniwersytetem Toronto ośrodek badawczy Citizen Lab znalazł ślady tego oprogramowania również m.in. w Bahrajnie, Chinach, Indiach, Indonezji, Iraku, Kenii, Kuwejcie, Libanie, Malezji, Nigerii, Katarze, Rosji, Arabii Saudyjskiej, Korei Południowej, Singapurze, Tajlandii, Turcji i Wenezueli.

W rzeczywistości jednak metody działań zmierzających do inwigilacji obywateli są w najlepszym wypadku wątpliwe prawnie, a nierzadko są to działania wymykające się jakiemukolwiek nadzorowi i autoryzacji ze strony demokratycznie wybranych rządów. Produktem tego rodzaju praktyk są choćby wirusy komputerowe, w tym okrzyknięty najbardziej niebezpiecznym robakiem w historii Reign, który jest o tyle interesujący, że najwięcej jego ofiar znajduje się w Rosji (28%) oraz w Arabii Saudyjskiej (24%). Stopień jego kompleksowości wskazuje na to, że pochodzi on raczej z laboratoriów rządowych i jeśli wyeliminować z listy potencjalnych twórców Rosję i Chiny, to oczywistymi podejrzanymi stają się Stany Zjednoczone i Wielka Brytania. Lista ofiar dowodzi, że wirus nigdy nie był przeznaczony do masowej infekcji Internetu, ale do zarażania pojedynczych, indywidualnie wybranych komputerów. Dotychczas potwierdzono zaledwie setkę infekcji. Inne znane wirusy, które powszechnie podejrzewa się o pochodzenie z tajnych pracowni komputerowych w Europie bądź Ameryce Północnej, to Stuxnet oraz Flame.

Prawne uzasadnienia takich działań są w największym stopniu wątpliwe, a czasami wręcz humorystyczne. Przykładowo FBI usiłuje wymusić na Google i Apple deszyfrowanie smartfonów w oparciu o przepisy z 1789 roku – All Writs Act. Przy użyciu podobnych kruczków administracja federalna w Stanach Zjednoczonych rozprawia się z informatorami, którzy mogli inspirować wycieki niejawnych informacji do mediów. Do czasów prezydenta Obamy archaiczna i drakońska ustawa o szpiegostwie, która została uchwalona jeszcze podczas I wojny światowej, została użyta jedynie trzykrotnie. Tymczasem od początku rządów Baracka Obamy ustawa ta została wykorzystana już w ośmiu przypadkach oskarżenia skierowanego przeciwko amerykańskim urzędnikom państwowym.

Choć ideologie uzasadniające działania rządów bywają rozmaite, to chęć kontroli nad komunikacją elektroniczną połączyła niezwykłą koalicję obejmującą rządy totalitarne, islamistów i służby specjalne zachodnich demokracji. Opublikowana przez Reporterów bez Granic lista Wrogów Internetu 2014 obejmuje nie tylko takich weteranów inwigilacji jak Kuba, Białoruś, Sudan czy Korea Północna, ale również instytucje rządowe z kilku krajów uchodzących za demokratyczne: National Security Agency ze Stanów Zjednoczonych, Government Communications Headquarters z Wielkiej Brytanii oraz Centre for Development of Telematics z Indii. Choć trudno mówić tu o koordynacji ich działań, to dyskretnie wymieniają się one nowinkami technicznymi, choćby przy okazji takich targów międzynarodowych jak ISS World, Technology Against Crime czy Milipol, które Reporterzy bez Granic również umieścili na liście Wrogów Internetu. Wszystko to oczywiście dzieje się w celu ochrony nas, obywateli, przed przestępczością.

Buddyjski autor John Twelve Hawks trafnie napisał, że gdyby prywatność miała nagrobek, to napis na nim mógłby brzmieć: „Nie martw się. To było dla twojego dobra". Jak tymczasem słusznie twierdził Benjamin Franklin, jeden z ojców założycieli Stanów Zjednoczonych, gdy dla tymczasowego bezpieczeństwa zrezygnujemy z podstawowych wolności, nie będziemy mieli ani jednego, ani drugiego.

Kancelaria Prawna Skarbiec jest wiodącym podmiotem w zakresie przeciwdziałania bezprawiu urzędniczemu i kontroli podatkowych.