

# Rzeczpospolita podsłuchiwana

Jeśli wierzyć statystykom, zaglądnienie sąsiadom w okna to nasza narodowa pasja. Jako świadomi obywatele oburzamy się jednak, gdy mamy do czynienia z przejawami kontroli i inwigilacji – czy to policyjnej, czy dziennikarskiej. A mimo to w domowym zaciszu z wypiekami na twarzy śledzimy poczynania gwiazd czy znajomych, klikając w ekrany smartfonów.

**Mec. Robert Nogacki, ZAŁOŻYCIEL KANCELARII PRAWNEJ SKARBIEC**

**P**olacy wiodą prym w Europie pod względem niezdrowej ciekawości. W ostatnich dwóch latach kupiliśmy na rynku cywilnym ponad 10 tys. zminiaturyzowanych urządzeń podsłuchowych oraz kamer (źródło: „Gazeta Wrocławska”). Jeśli chodzi o oprogramowanie szpiegowskie, liczby są zapewne jeszcze bardziej porażające. Kogo zatem za pomocą tego sprzętu śledzi, podgląda, czy szpieguje przeciętny Kowalski? Głównie mniej lub bardziej niewiernych małżonków, dzieci, nianie, podwładnych, kontrahentów, a nawet sąsiadów.

## PO PIERWSZE OSTROŻNOŚĆ

Nie u wszystkich pasja podglądania kończy się na niezdrowej ciekawości. Coraz większy odsetek spraw związanych z wszelkiego rodzaju naruszeniami prywatności wynika z działań popełnianych z premedytacją i zmierzających do kradzieży danych, hasła, zdjęć czy nagrań. I nie łudźmy się, że tak długo, jak długo nie jesteśmy gwiazdami telewizji, sportu, czy estrady, nikt nie zainteresuje się zawartością naszych komputerów, telefonów, czy też wprost nie będzie próbował zajrzeć do naszego życia z mikrofonem i kamerą. Każdy ma jakieś tajemnice, które chciałby zachować dla siebie. Im bardziej zależy nam na ich ukryciu, tym większą wartość mają one dla potencjalnych łowców sensacji – bez względu na motywy, jakie nimi kierują. Co może więc zrobić przeciętny obywatel, biorąc pod uwagę, że nie wie, jak unikać zagrożeń w sieci, a na profesjonalny audyt bezpieczeństwa informacyjnego po prostu nie ma środków?

Warto zacząć od prostych metod i zwykłej życiowej ostrożności. Nikt z nas nie ma w zwyczaju opowiadać poznanym przypadkowo osobom o prywatnych szczegółach swojego życia. Tę zasadę warto przenieść

również na grunt wirtualny. Wszystko, co robimy w sieci, może stać się przedmiotem zainteresowania osób trzecich, których intencje są trudne do odgadnięcia. Pamiętając o tym, wybierajmy programy, które dają nam większe bezpieczeństwo. W zależności od naszych potrzeb mogą to być rozwiązania przeznaczone specjalnie do tego lub ogólnie dostępne. Wysyłając wiadomości, których nie chcemy nawet przypadkowo ujawnić, używajmy programów szyfrujących czy chociaż komunikatorów z opcją szyfrowania w czasie rzeczywistym.

Aby ograniczyć możliwość monitorowania naszej internetowej aktywności, wykorzystujmy sieci prywatne (VPN). Wówczas do oferujących takie rozwiązania usługodawców będą musieli zwracać się wszyscy, których interesuje, co robimy w internecie. A to oznacza dla nich wydłużenie drogi i dodatkowe komplikacje, działające na naszą korzyść.

Podobne możliwości, ograniczające jednak jeszcze bardziej ingerencję w nasze prywatne sprawy (również agend rządowych), daje przeglądarka TOR. Działa podobnie jak sieć wirtualna, ale – opierając się na sieci anonimowych routerów oraz szyfrowaniu i anonimizacji transferów – wyklucza udział podatnych na naciski usługodawców. TOR w znacznej mierze uniemożliwia analizę zawartości transmisji, nie ukrywa jednak faktu zaistnienia komunikacji. To w zdecydowanej większości przypadków wystarczy, by zniechęcić ewentualnych „zainteresowanych”.

## BEZPIECZNA KOMÓRKA

Internet i poczta elektroniczna to jednak nie wszystko. Podobnie jest z podsłuchiwaniami telefonów komórkowych. Współcześnie nikt nie instaluje już typowych, znanych z filmów, zminiaturyzowanych urządzeń podsłuchowych. Komórki podsłuchiwane są

zazwyczaj na odległość (przy użyciu specjalistycznego sprzętu nazywanego IMSI Catcher) lub przez operatora – na zlecenie odpowiednich organów państwowych.

Również w tym przypadku na rynku można znaleźć sporo rozwiązań oferujących różny poziom zabezpieczenia od kosztownych rozwiązań sprzętowych, jak telefony z opcją szyfrowania połączeń, aż po darmowe oprogramowanie, które można samodzielnie pobrać na telefon komórkowy. Znaczna część z nich, mimo że bezpłatna, charakteryzuje się wysoką skutecznością, uniemożliwiającą bądź znacznie utrudniającą przechwycenie rozmów przez osoby trzecie.

## JAK UCHYLONE OKNO

Nie wolno również zapominać o programach antywirusowych i antymalewarowych, obsługujących platformy mobilne. Włamanie do telefonu komórkowego jest równie proste, jak włamanie do niezabezpieczonego komputera. A ryzyko znacznie się zwiększa, kiedy korzystamy z publicznych, nie do końca sprawdzonych sieci. Warto więc uważać, z czym łączy się nasza komórka, a gdy w danej chwili nie korzystamy z dobrodziejstw transmisji danych, wyłączajmy tę usługę, analogicznie postępując z Wi-Fi oraz Bluetooth. Dla hakera są one jak uchylone okno, które wystarczy pchnąć, by wejść do domu.

Przeciętny użytkownik internetu oraz telefonu komórkowego ma więc do dyspozycji szeroki wybór środków ochrony prywatności. Biorąc pod uwagę, że koszt ich zastosowania jest naprawdę niewielki, warto wziąć sprawy we własne ręce i nie dać pożywki żadnym sensacji ludziom, których nasze życie osobiste nie powinno interesować. <