Każdy kabel to jest antena – wywiad z mjr. rez. Pawłem Tomczykiem

Kategoria: Wywiady
Opublikowano: piątek, 17, styczeń 2025 10:51
Anna Dąbrowska

Jeśli chodzi o urząd, należy ocenić czy inwestycja jest analogiczna do ryzyka. Zawsze trzeba zrobić bilans zysków i strat – mówi mjr rez. Paweł Tomczyk ze spółki Sekkura w rozmowie z redaktorką Dziennika Warto Wiedzieć, a dotyczącą tematyki bezpieczeństwa informacji.

Panie Majorze, zgodzi się Pan ze stwierdzeniem, że w dzisiejszych czasach informacja to najcenniejszy towar?

Nie tylko dzisiaj. Informacja zawsze była najcenniejszym towarem. Już kilka tysięcy lat temu niejaki Sun Tzu w książce „Sztuka wojny" podkreślał wagę zbierania informacji. Tak więc ludzie od dawna zdawali sobie sprawę ze znaczenia informacji i próbowali zdobywać ją w różny sposób – albo przez źródła osobowe albo poprzez rozwiązania techniczne. W Polsce takim ciekawym przykładem jest zamek Krzyżaków w Malborku, gdzie Wielki Mistrz, siedząc w sali kominkowej, słyszał wszystko o czym rozmawia się w pokojach gościnnych, bo tak był – oczywiście niezupełnie przypadkowo – skonstruowany system wentylacji. Także ta informacja, nie tylko dzisiaj, ale zawsze, była towarem trudnym do przecenienia.

Czy nie jest jednak tak, że dziś sami te informacje oddajemy? Korzystając chociażby z różnych aplikacji.

Dokładnie tak. Z jednej strony postęp technologiczny jest fajny, bo ułatwia życie. Z drugiej – umożliwia zbieranie informacji, o którym użytkownicy nawet nie zdają sobie sprawy. Takim przykładem z ostatnich dni jest afera związana z podsłuchiwaniem użytkowników iPhone'ów przez pracowników Apple. Jest tajemnicą poliszynela, że jeżeli rozmawia się o czymś przy iPhone'ie, to następnego dnia dostaje się reklamy związane z tematem rozmowy. Ale tego, powiedzmy sobie, jesteśmy świadomi. Problem polega na tym, że sprzęt zbiera dane także bez udziału naszej świadomości. Tak jak powiedziałem, iPhone'y zbierają dane, nagrywają to, o czym się w ich otoczeniu rozmawia. Nie tylko rozmowy na temat produktów, ale wszystkie – biznesowe, o polityce, damsko-męskie. To wszystko można sobie później odtworzyć…

…i wykorzystać. Pytanie: w jaki sposób?

W różny, np. do personalizowania reklam. Można dowiedzieć się, że użytkownik danego telefonu, załóżmy, o godzinie siódmej rano wyszedł z domu, zatrzymał się przed przedszkolem, następnie przed szkołą, później osiem godzin siedział w danym miejscu, potem odwiedził konkretny sklep, znowu pojechał do szkoły i do przedszkola i wrócił do domu. Program, analizując dane z tego telefonu, wie, że jego właściciel ma dzieci w wieku przedszkolnym i szkolnym, że pracuje w danej okolicy, więc będzie np. dostarczał mu reklamy ubranek dla dzieci, które można kupić w okolicy miejsca pracy. To, powiedzmy, jest jeszcze dość zanonimizowane. Gorzej, jeżeli system potrafi wyciągnąć o wiele bardziej konkretne informacje, bez wiedzy użytkownika. Mistrzem nie do pobicia jest w tym prawdopodobnie Windows, ponieważ nawet jeżeli w Windowsie wyłączy się wszystkie dostępne opcje dotyczące śledzenia użytkownika, to i tak będzie on wysyłał dziennie – o ile dobrze pamiętam – około 5000 pakietów dotyczących sposobu użytkowania komputera. Mało który użytkownik zdaje sobie sprawę z tego, że to de facto system jest jego właścicielem, a nie on właścicielem systemu.

Czy użytkownik może się przed tym ochronić?

Ludzie mają coraz większą świadomość tej inwigilacji. W Niemczech ok. roku temu administracja

jednego z landów, Schleswig-Holstein, podjęła decyzję o przejściu z Windowsa na Linuxa. Po pierwsze jest systemem darmowym i dużo bardziej stabilnym od Windowsa, po drugie – nie śledzi.

Jako współwłaściciel spółki Sekkura, zajmuje się Pan szeroko pojmowanym bezpieczeństwem w praktyce. Co robił Pan przed naszym dzisiejszym spotkaniem?

Omawiałem dwie roboty: w przyszłym tygodniu będziemy sprawdzali dwa obiekty w celu wykrycia ewentualnych podsłuchów.

Jaką formę mogą przybrać takie urządzenia?

Może to być np. rejestrator ukryty w doniczce z kwiatkiem, oczywiście odpowiednio zabezpieczony przed wodą, jeśli jest to żywa roślina. Kiedyś znaleźliśmy podsłuch ukryty w gniazdku, kilka w listwach zasilających, w samochodzie. Na szczęście u osób prywatnych. By zostawić podsłuch, najlepiej jest zdobyć zdjęcie danego pomieszczenia i następnie podmienić jeden element na drugi, tak by użytkownik się nie zorientował. To może być wszystko, np. długopis z rejestratorem. Pytanie, co chcę osiągnąć? Jeżeli interesuje mnie podsłuch w czasie rzeczywistym, to musi być to urządzenie nadawcze lub w częstotliwościach radiowych, powiedzmy, ok. 300 Mega Hz albo ukryty moduł GSM. Jest o tyle dobry, że umożliwia podsłuch danego pomieszczenia z każdego miejsca na świecie. Minusem jest to, że urządzenia nadawcze potrzebują więcej prądu niż rejestratory, więc najlepiej jak będą zasilane z sieci. Umożliwi to długotrwałe działanie.

Jeżeli mowa o instytucjach publicznych, mających duże znaczenie, to podsłuchujący może nie chcieć ryzykować wejścia do obiektu i będzie wolał zastosować podsłuch zewnętrzny, czyli albo mikrofon laserowy albo podsłuch komputerów.

Czy jest na to jakieś antidotum?

Jeżeli jest pocisk, to zawsze znajdzie się pancerz, który ten pocisk zatrzyma. Możemy zrobić zabezpieczenia. Np. zabezpieczenie przed podsłuchem laserowym robi się poprzez naklejenie na szyby tzw. „wibroczujek", które podłączone do generatora, powodują drgania szyb, co uniemożliwia laserowi odczytanie fal akustycznych.

Wiem, że często zwracają się do Pana osoby prywatne? A co z urzędnikami?

Urzędnicy coraz częściej zdają sobie sprawę z grożącego niebezpieczeństwa i zaczynają słuchać ekspertów. Ja cały czas im powtarzam: na spotkania nie wnosimy telefonów. Ja nigdy nie zostawiam swojego telefonu w obcym miejscu. Zostawiam go w samochodzie albo używam czegoś takiego jak depozytor aktywny. Może mieć postać pudełka z „szumatorem", w którym zamyka się telefon, lub rozwiązanie oparte o ultradźwięki. Można wówczas rozmawiać bez obaw, że rozmowa zostanie podsłuchana, a jednocześnie ma się telefon na oku. Samo wyłączenie telefonu nic nie daje. Kiedyś można było wyjąć baterię, dziś jest to niemożliwe.

W jednym z wywiadów Jarosław Kaczyński pokazał swój telefon – starego typu Nokię, sugerując, że taki telefon trudniej jest podsłuchać. Powinniśmy brać przykład?

To jest absolutna nieprawda. Stare telefony działają na starych systemach kodowania rozmów. Mając

telefon, powinniśmy ustawić najwyższy z możliwych standard kodowania np. 4G zamiast 2G. Jeżeli używamy na przykład „dwójki", to można podsłuchiwać nas praktycznie bez żadnych urządzeń. Także to jest taki mit, że stare Nokie są najbezpieczniejsze, bo na nich nie zainstaluje się oprogramowania szpiegowskiego. Nie trzeba go instalować. Już od momentu, w którym te telefony zaczęły wchodzić na rynek, można je było podsłuchiwać, bo algorytmy kodowanych danych zostały nie tylko złamane, ale też ujawnione. Tak więc, jeżeli ktoś ma wiedzę i trochę sprzętu, to może taką Nokię podsłuchać.

Wspominał Pan, że urzędnicy podchodzą do tematu nielegalnego pozyskiwania informacji z coraz większą świadomością. Czy urzędy powinny mieć szczególne zabezpieczenia? Co by im Pan rekomendował?

Jeżeli mówimy o rozmowach na bardzo istotne tematy, szczególnie finansowe, to uważam, że sala, w której mają się one odbywać, powinna być sprawdzona. Byłoby dobrze, gdyby w każdej instytucji było jakieś bezpieczne pomieszczenie. Oczywiście, nie dajmy się zwariować. Nie chodzi o to, żeby wszędzie wstawiać klatki Faradaya: finanse nie takie i skala informacji nie ta. Ale – chociaż przynajmniej w podstawowym stopniu – jakieś zabezpieczenie mogłoby funkcjonować, np. wspomniany depozytor w środku pomieszczenia bądź przed pomieszczeniem, żeby można było schować telefony czy żeby ludzie mieli nawyk niewchodzenia na spotkania z elektroniką. Dobrym pomysłem jest również pomieszczenie bez okien, ponieważ – jak wspominałem – podsłuchiwać można nie tylko z wewnątrz, ale i z zewnątrz. Pamiętajmy również o komputerach. Każdy kabel to jest antena. Jeżeli ktoś ma do obrobienia bardzo ważne informacje, to uważam, że powinien zainwestować w tak zwany komputer tempestowy, czyli taki, który jest dobrze ekranowany i którego podsłuch jest na tyle utrudniony, że przestaje się opłacać. Podkreślam jednak raz jeszcze: jeśli chodzi o urząd, należy ocenić czy inwestycja jest analogiczna do ryzyka, czy informacje są na tyle istotne, żeby opłacało się inwestować w ich ochronę. Zawsze trzeba zrobić bilans zysków i strat. Nie ma sensu inwestowanie miliona złotych, jeżeli rozmawiamy o przetargach na 10 tys zł. Pamiętam jednak sytuację związaną z organizacją przetargu, kiedy to wygrał człowiek, który dzięki podsłuchowi znał oferty wszystkich innych osób.

Jak dotąd nie znaleźliśmy podsłuchów w żadnej ze sprawdzanych przez nas spółek Skarbu Państwa. Zdarzało się w niektórych urzędach, że pracownicy przypadkowo znajdowali podsłuchy. Czasami przy wycieku informacji zawodzi jednak czynnik ludzki. Dyrektor ds. bezpieczeństwa jednej ze spółek Skarbu Państwa, po 4 latach współpracy, powiedział, że od kiedy zaczęliśmy regularnie sprawdzać ich pomieszczenia, skończyły się wszelkiego rodzaju wycieki do prasy, wycieki o przetargach na miliony euro. Tam nie było żadnych podsłuchów. To ludziom zdarzało się dzielić informacjami, które były poufne. Tak więc trzeba pamiętać też o tym, że najsłabszym ogniwem zawsze jest człowiek. Jeżeli ma świadomość, że jest tak zwana profilaktyka i dba się o bezpieczeństwo informacji; że obiekt jest sprawdzany i nie można zrzucić winy na podsłuchy, to 4 razy ugryzie się w język zanim w nieautoryzowanym środowisku przekaże jakieś informacje.

Jak bardzo kosztowna jest taka usługa?

Koszty mogą być zależne od różnych czynników. Przykładowo, są firmy, które liczą każdy sprawdzany punkt osobno: gniazdko, sufit podwieszany, wentylację itd. Niektóre firmy liczą metry sześcienne, inne kwadratowe. Na rynku warszawskim taka usługa wynosi średnio ok. 60 zł za metr kwadratowy.

Dziękuję za rozmowę.

Kategoria: Wywiady
Opublikowano: piątek, 17, styczeń 2025 10:51
Anna Dąbrowska

*Mjr rez. **Paweł Tomczyk** – absolwent Wojskowej Akademii Technicznej i Akademii Sztabu Generalnego, wyższy oficer Wojska Polskiego przeniesionym do rezerwy. Odbywał służbę czynną w jednostkach liniowych wojsk pancernych i zmechanizowanych, a następnie w IC MON. Brał udział w misji SFOR w Bośni i Hercegowinie. Specjalizuje się w zagadnieniach dotyczących ochrony informacji niejawnych. Posiada licencję detektywistyczną. Aktualnie jest członkiem zarządu i współwłaścicielem firmy Sekkura, w ramach której od ponad 10 lat doradza polskim i zagranicznym firmom w zakresie szeroko pojmowanego bezpieczeństwa — fizycznego, teleinformatycznego, zabezpieczenia transmisji danych, przeciwdziałania nieuprawnionemu podsłuchowi i obserwacji, bezpieczeństwa spotkań i negocjacji biznesowych oraz cyberbezpieczeństwa.*
Wraz ze współpracownikami zajmuje się zabezpieczeniem pomieszczeń i wykrywaniem podsłuchów; projektowaniem i realizowaniem lokalnych i kompleksowych audytów bezpieczeństwa firm, w tym bezpieczeństwa systemów operacyjnych, obejmujących m.in. analizy podatności na podsłuchy, ataki wewnętrzne i sabotaż, ocenę działań ochrony fizycznej i technicznej, analizy zagrożeń ze strony „firm trzecich", szpiegostwo gospodarcze; realizowaniem szkolenia on- i offline dla firm i osób indywidualnych, w zakresie m.in. infobrokeringu, bezpieczeństwa informacji, umiejętności interpersonalnych, zaawansowanych technik eksploracji Internetu; świadczeniem usług detektywistycznych; prowadzeniem badań termowizyjnych; projektowaniem i wykonywaniem instalacji zabezpieczających sale konferencyjne, gabinety kadry kierowniczej przed podsłuchem laserowym, GSM, radiowym, mikrofonami kontaktowymi; prowadzeniem szkoleń z samoobrony oraz pierwszej pomocy.