Tristan Szaniawski

Zagrożenia prywatnosci

Bezpieczeństwo osobiste i bezpieczeństwo danych wymuszają na ludziach stosowanie coraz to nowszych zabezpieczeń. Histeria jaka zapanowala po zaatakowaniu wujka Sama przez wujka Osame sprzyja takim dzialaniom. Ludzie bez wiekszego zastanowienia poddaja sie nowym technikom zabezpieczen, nie zastanawiajac sie nad zagrozeniami na jakie sie wystawiaja. Za przyklad niech posluzy nowa weryfikacja tozsamosci wprowadzonych na lotniskach w Stanach (jeszcze) Zjednoczonych. Osoba chcaca dostac zgode na wjazd do Imperium musi wpierw poddac sie skanowaniu teczowki oka. Skan ten jest zapamietywany w bazie danych , a nastepnie porownywany ze skanem teczowki oka osoby pragnacej przekroczyc granice USA. I gdzie tu zagrozenie? Zagrozenie kryje sie w samym systemie. Przyszlosc weryfikacji tozsamosci to wlasnie skany teczowki. Platnosci w sklepie, dostep do tajnych informacji, zatwierdzanie transakcji bedzie sie odbywac w ten sposob. Rzad USA dostal za darmo baze danych teczowek oka milionow ludzi. Sa w srod nich bizmesmeni, szefowie duzych korporacji, naukowcy, politycy, zolnierze. Wsrod rzeszy ludzi przekraczajacych granie Stanow sa tez ludzie ktorzy narazie sa nikim(taka przenosnia), ale w przyszlosci byc moze beda mieli do czynienia z jakimis tajemnicami. Rzad USA schcac uzyskac dostep do tych tajnych informacji bedzie musial praktycznie zrobic jedna rzecz. Wykonac kopie oka przy pomocy skanu ktory juz ma. A potem juz tylko przystawic kopie do urzadzenia weryfikujacego tozsamosc i tajemnice stoja otworem. Wszelkie proby wytlumaczenia ofiary takiej kradziezy, nie beda brane pod uwage. System sie nie myli i wskaze kto mial dostep do informacji w czasie kradziezy. "Winny" zawsze sie znajdzie. Tylko ze bedzie nie winny. USA dostalo do reki narzedzie do zbrodni doskonalej. Nalezy przepuszczac ze rzady innych krajow pojda w slady Stanow Zjednoczonych. Bedziemy mieli do czynienia ze szpiegostwem przemyslowym na ogromna skale. Nie nalezy wierzyc w zapewnienia "ekspertow" od zabezpieczen ze wykonanie wiernej kopii oka jest poza mozliwosciami obecnej czy najblizszej technologii. "Cel uswieca srodki" jak mowi przyslowie. Na kradziez informacji zawsze sa przeznaczane duze srodki. Z pewnoscia wieksze niz przecietny czlowiek jest w stanie sobie wyobrazic.A pozatym ,czy mozna wierzyc komus kto moze miec interes w zdobyciu naszych tajemnic?

Pozostawmy świat korporacji, rzadów i duzych pieniedzy. Zobaczmy jakie zagrozenia czyhaja na "nikogo waznego". Ludzie sa leniwi, lubią wygodę. W dzisiejszym, cywilizowanym, swiecie nie do pomyslenia jest zeby podejsc do telewizora i zmienic kanal. Kazdy kto nie jest dzikusem posluguje sie pilotem. Ale i on odejdzie w zapomnienie. W modzie bedzie zaopatrywanie sie w implanty wszczepiane do mozgu, umozliwajace poprzez specjalny interfejs, komunikacje ze sprzetem elektronicznym. Za pomocą mysli, bez ruszania się ze swojego ulubionego miejsca, zmienimy kanal w telewizorze (ktory zostanie zastąpiony przez nowsza wersje implantu umozliwiajaca przesylanie informacji [np. wizji] bezposrednio do mózgu [cóż za oszczedność wzroku]), napiszemy maila, badz przeslemy pin do karty kredytowej. Pierwsze potwierdzenia tej teorii już są. Bezprzewodowe zestawy Bluetooth pozwalaja na rozmowe telefoniczna, odsluchiwanie muzyki bez uzycia kabli czy trzymania urzadzenia w reku. Bluetooth zostal rowniez wykorzystany do komunikacji GamePadow w nowym XBox`ie. Implanty identyfikacjyjne juz istnieja, i sa wszczepiane psom, jak i ludziom którzy sobie tego zażyczą. Powstal juz implant przyjemnosci - ORGAZMOTRON (ma umozliwiac orgazm osobom ktore maja z nim klopoty). Połączenie wszystkich elementów w jedną całość pozostaje kwestia czasu. O podsluchanie informacji przesylanych drogą bezprzewodową nie trudno. Szyfrowanie nie na wiele sie zda. Rosnąca moc obliczeniowa komputerów jak i malejaca ich cena, spowoduja że zlamanie nawet wyszukanych metod

kryptograficznych nie nastręczy zadnych problemów. Pól biedy jezeli bedziemy tylko wysylac informacje, zawsze mozemy przestac myslec, przerywajac w ten sposow przesyl danych. Powazne kłopoty, przez duze 't':), zaczna sie gdy powstana implanty pozwalajace na odbior danych i pozwalajacych na buszowanie w mózgu nosiciela. Nowe pokolenie hakerow bedzie mialo pole do popisu. Nie beda jedynymi ktorzy zapragną poznać cudze myśli. Producenci implantów z pewnością wykorzystają nadarzającą się okazję. W końcu to oni decyduja jak zachowują się implanty. Jestem przekonany ze implanty beda zawierać tylne furtki, tak na wszelki wypadek. Poprostu taka okazja nie może przejść nie wykorzystana. Wyobraźmy sobie że takie implanty znajdą się u niektórych żołnierzy. W przypadku wojny, producent implantów zbije fortune oferując stronom kod uruchamiający autodestrukcję, male spięcie niszczące uklad i przy okazji paraliżujące spory obszar mózgu. Morze wojowników którzy się zawiesili. Tu juz nie pomoże RESET. Ludzkość pozostaje nieświadoma zagrożeń jakie niesie ze sobą postęp technologiczny, a szczególnie miniaturyzacja. Nawet się nie zorientujemy gdy nasza prywatność zostanie naruszona przez "inteligenty kurz". Calkiem realne jest zbudowanie mikrorobotów wielkości ziarenka piasku, a nawet mniejszych. Robot nawet nie musialby być jednostką autonomiczną, sterowany sztuczną inteligencją. Wystarczy żeby mial możliwość poruszania się. Zamontowanie malego mikrofonu (np. na bazie kondensatora z ruchomą okladką) i nanokamery umozliwi inwigilacje na nie znanym dotąd poziomie. Nigdzie już nie bedziemy bezpieczni, gdyz tak male urzadzenie pozostanie dla nas nie zauwazone, a w sytuacji zagrozenia może się schować w byle szparę. Nasza prywatność zostanie naruszona nie tylko w odniesieniu do otoczenia ale i wnętrza, ciala. W czasie snu, robocik może dostać się do naszego ciala przez jeden z wielu otworów w ktore jestesmy zaopatrzeni. I pozostanie tam tak dlugo jak operator robota zadecyduje.

Tak pokrótce przedstawiają się sposoby zagrożenia prywatności czlowieka 21 wieku.