Komputery i internet – zagrożenia nowej epoki

16 sierpnia 2014
Data publikacji: 28.06.2007

O pożytkach korzystania z komputerów przekonywać nikogo nie trzeba. Warto jednak mieć świadomość zagrożeń, jakie niesie za sobą powszechna komputeryzacja oraz posługiwanie się komunikacją internetową w epoce globalizacji i monopolizacji narzucanej przez wielkie koncerny. Wprawdzie na co dzień stykamy się często z informacjami związanymi z tematem, a jednak ocena wiarygodności i znaczenia wielu z nich jest niezwykle trudna dla niespecjalisty komputerowego, ba, ocena taka bywa trudna nawet dla wyarafinowanych, doświadczonych programistów i inżynierów. Dobrym przykładem podobnej sytuacji jest historia "klucza" NSA odnalezionego w kodzie Windows w 1999 roku przez Andrew Fernandesa: do dziś nie doczekaliśmy się w pełni jednoznacznego i wiarygodnego jej wyjaśnienia.

NSA (National Security Agency, http://www.nsa.gov) jest jedną z najważniejszych instytucji w USA zajmujących się wywiadem, współpracującą ściśle z organizacjami wojskowymi, z FBI, CIA. Budżet ani liczba pracowników NSA nie są publicznie znane, można jednak szacować na podstawie pewnych informacji, że sięga on co najmniej kilku miliardów dolarów rocznie.

W dużej mierze niezależna od innych organizacji rządowych i od władz w kraju, podlega głównie decyzjom Prezydenta. Teoretycznie powołana do ochrony krajowych zasobów informacyjnych i do zdobywania informacji za granicą metodami szpiegowskimi, informacji zarówno o znaczeniu militarnym, jak i przede wszystkim tej o znaczeniu gospodarczym i politycznym, albowiem tego właśnie rodzaju informacje mają w dzisiejszym świecie większą wagę. Ze względu na brak kontroli jej działalności przez szersze ciała demokratyczne podejrzewana

jednak bywa również o inwigilację własnych obywateli. Wprawdzie tego rodzaju inwigilacja byłaby sprzeczna z konstytucja, ale przypuszcza się, ze tę prawną przeszkodę można obejść korzystając ze współpracy z zagranicznymi agencjami o podobnym charakterze: my będziemy śledzić waszych obywateli w waszym kraju, a wy naszych w naszym, potem zaś wymienimy się informacjami… Czyż należy się dziwić istnieniu tego rodzaju podejrzeń w przypadku instytucji, nad której działalnością kontrolę sprawują jedynie inne instytucje rządowe? Wątpliwości nasuwają się same. Oto na przykład NSA powołuje się na dyrektywę (Executive Order 12333) zabraniającą zabójstw politycznych: "Żadna osoba zatrudniona przez rząd Stanów Zjednoczonych lub działająca w jego imieniu nie będzie angażować się lub spiskować w celu dokonania zabójstwa". Czymże jednak innym jak nie zabójstwem był zamach na życie (ponoć) jednego z liderów al-Qaiedy na początku listopada 2002 w Jemenie, przy pomocy zdalnie sterowanego bezzałogowego samolotu? Czymże innym jak nie próbą politycznego zabójstwa było wysłanie w 1986 roku amerykańskich samolotów w celu zbombardowania prywatnej rezydencji Kadafiego w Libii, położonej na obrzeżach stolicy kraju Tripoli, z dala od ważnych celów gospodarczych czy wojskowych? Przykładów sytuacji ilustrujących rozdźwięk miedzy prawem a rzeczywistymi działaniami amerykańskich instytucji istnieje więcej. Dlatego też będziemy traktować podejrzliwie informacje, jakie NSA przedstawia sama o sobie. Warto też pamiętać, iż wprowadzony niedawno Akt Patriotyczny znacznie zwiększył uprawnienia agencji wywiadowczych (patrz InfoNurt, numer 4 z ubiegłego roku).

Specyfika pracy NSA polega na tym, iż agencja ta zajmuje się zbieraniem i przetwarzaniem informacji w postaci elektronicznej.

Pierwsze głośniejsze problemy związane z jej działalnością pojawiły się kilka lat temu. Zaczęto szeroko spekulować w prasie i w internecie o tym, że NSA zajmuje się koordynacja i

nadzorem nad funkcjonowaniem wielkiej sieci wywiadu elektronicznego o nazwie Echelon, wywiadu prowadzonego w istocie na całym świecie, poprzez sieć wyspecjalizowanych baz przechwytujących wszelkie radiowe transmisje, rozmowy telefoniczne, korespondencję faksem oraz wymianę informacji w internecie. Do systemu tego należy pięć państw: Wielka Brytania, USA, Kanada, Australia i Nowa Zelandia, ale zasięg inwigilacji prowadzonej przez nie daleko przekracza granice tych państw. Wystarczy sobie choćby przypomnieć, że wiele łączy telekomunikacyjnych miedzy kontynentem amerykańskim a Europa przebiega przez teren Wielkiej Brytanii (do celu szpiegowskiego służy baza Menwith Hill w Yorkshire).

Do udziału w systemie Echelon pierwsza przyznała się Australia, w roku 1999, publikując przy okazji uspokajające swoja opinie publiczną informacje na temat ograniczeń, jakie obowiązują ich instytucje, jeśli idzie o sprawę inwigilacji własnych obywateli. Australijska agencja DSD (Defence Signals Directorate) zajmuje się również nasłuchem satelitów przy pomocy stacji szpiegowskiej ulokowanej głęboko na centralnej pustyni, w pobliżu Alice Springs.

Informacje o istnieniu systemu globalnej inwigilacji pośrednio potwierdził raport przygotowany w roku 2000 dla Parlamentu Europejskiego (http://www.iyp.org/3crypt/stoa/), gdzie kilka z państw zaniepokojone możliwością prowadzenia wywiadu ekonomicznego na tak szeroka skale postanowiło zaalarmować opinie publiczna i sprawę poruszyć na szerszym forum.

W jaki sposób odbywa się analiza przechwytywanych danych? Wszystko robią potężne komputery (NSA korzysta z najbardziej zaawansowanych na świecie systemów komputerowych). Na przykład miliony listów e-mail na godzinę są analizowane pod katem występowania w nich odpowiednich słów i wyrażeń, by po tej wstępnej selekcji listów zawierających podejrzane treści przepuścić je potem przez bardziej zaawansowane programy komputerowe, a w końcu te już nieliczne są analizowane przez ludzi. NSA nieprzerwanie poszukuje lingwistów do pracy,

szczególnie tych posługujących się mniej znanymi językami. Niewykluczone, że cały ten olbrzymi strumień informacji jest przechowywany – jest to już prawdopodobnie technicznie możliwe.

Istnienie Echelonu wzbudziło największy niepokój w Niemczech i Francji, państwach aspirujących do wiodącej roli w Europie, uczulonych na dbanie o swe żywotne interesy narodowe, a wykluczonych z udziału w programie globalnego podsłuchu Echelon (państwa te jednakowoż posiadają własne stacje przechwytu informacji, jest to jednak działalność prowadzona na znacznie mniejsza skalę). Jak się okazało wkrótce, niepokój ich nie był bezzasadny. W 2000 roku kilka dużych firm francuskich uznało, że mają dostatecznie wiele dowodów prowadzenia szpiegowskiej działalności ekonomicznej przez NSA, godzącej w ich ekonomiczne interesy i sprawa trafiła do sądu. Były dyrektor CIA, James Woolsey, potwierdzając istnienie faktu szpiegowania arogancko tłumaczy proceder istnieniem w Europie "narodowej kultury" przyjmowania łapówek…

Istnieje dość prosty sposób zabezpieczenia się przed przechwytywaniem ważnych informacji przez niepowołane osoby. Jest nim stosowanie kryptografii w odpowiednich urządzeniach czy oprogramowaniu służącemu komunikacji. Pierwszy przykład z brzegu to korzystanie z tak zwanych "bezpiecznych" stron www, czyli takich, których adres URL rozpoczyna się nie od "http", lecz od "https". Cały proces enkrypcji danych odbywa się wtedy bez szczególnej świadomości użytkowników internetu, a dokonywany jest po stronie serwera i po stronie użytkownika w jego internetowej przeglądarce. Jeśli o internet idzie, to oprogramowania, w zasadzie dostępnego powszechnie, a umożliwiającego "bezpieczne" przesyłanie informacji jest wiele (np. istnieją odpowiednie programy e-mail, istnieje tak zwana metoda klucza PGP (Pretty Good Privacy). Istnieje nawet oprogramowanie pozwalające na kodowanie i dekodowanie rozmowy telefonicznej czy przekazu faksem.

Niestety, owe metody zabezpieczania się przed podsłuchem,

mimo, że dość łatwo dostępne, nie są powszechnie znane wśród szerokiego kręgu użytkowników internetu, a są też nieco niewygodne w korzystaniu. Z tych to powodów większość Państwa raczej nie spotkała się z nimi. Nie wszędzie też na świecie stosowanie enkrypcji przez osoby prywatne jest legalne. W Ameryce na szczęście jest i zapewne pozostanie takim, mimo pojawiających się od czasu do czasu sugestii ograniczenia tej formy "swobody wypowiedzi" (pod pretekstem rzecz jasna walki z przestępczością, a teraz z "terroryzmem"). W istocie, być może ważniejszym powodem niż potrzeba przestrzegania konstytucji stały się pieniądze: bez stosowania kryptografii i możliwości przeprowadzania bezpiecznych transakcji internetowych runęłaby wielka gałąź przemysłu przez który przepływają obecnie co najmniej dziesiątki miliardów dolarów rocznie.

Pojawia się naturalne pytanie: na ile kryptografia jest "bezpieczna"? Czy oby na pewno nie jest możliwe rozkodowanie przez osoby trzecie informacji ukrytej przy pomocy metod kryptograficznych? Odpowiedz na tak postawione pytanie jest nieco złożona, z kilku przyczyn. Otóż przede wszystkim, "bezpieczeństwo" metod kryptograficznych zależy od przestrzegania pewnych ścisłych reguł tyczących korzystania z tych metod. Na przykład jakiś drobny błąd w oprogramowaniu komputerowym może z powodzeniem umożliwić dostęp do tajnej informacji, niwecząc wszelkie próby jej ukrycia. Wydaje się, że to właśnie ta kategoria defektów spowodowanych albo błędem programisty albo tez błędem po stronie administratora serwera jest najczęstszą przyczyną umożliwiająca dostęp do informacji przez niepowołane osoby.

Istnieje też czysto techniczne ograniczenie "siły" kryptografii. Otóż mogą Państwo pamiętać, że pierwsze przeglądarki internetowe korzystały z tak zwanego 40-bitowego klucza kryptograficznego. Wtedy, kilka lat temu, był to względnie "bezpieczny" sposób enkrypcji. Ale postęp w dziedzinie rozwoju komputerów następuje szybko. Uważa się, że 40-bitowy klucz można obecnie "złamać" bez istotnego problemu.

Teraz już w powszechnym użyciu są klucze 128-bitowe. Do złamania takich potrzebne są już potężne komputery i długi czas ich pracy (a wiec zadanie bardzo drogie). No cóż… takimi komputerami dysponuje NSA i z całą pewnością korzysta z nich do podobnych celów w sytuacjach szczególnych. Zapamiętajmy: krotki klucz łatwo "złamać", zaś złamanie klucza długiego jest bardzo trudne, czasochłonne i kosztowne.

Możnaby zapytać: co NSA na to, iż klucze 128-bitowe staja się powszechne w użytku? Oczywiście, ta nowa technologia jest utrudnieniem wielkim w ich pracy. W USA (Kanada dostosowuje się do praw, jakie obowiązują w USA) kryptografia jest traktowana przez prawo tak samo jak broń lub amunicja i istnieją ścisłe ograniczenia dotyczące eksportu oprogramowania lub urządzeń z nią związanych. Czy wiecie na przykład, że popularne przeglądarki internetowe (Internet Explorer, czy Netscape) były produkowane w dwóch wersjach, jednej przeznaczonej na użytek "domowy", to jest w obrębie USA i Kanady oraz wersji "międzynarodowej", gdzie stosowano zaledwie 40-bitowy klucz kryptograficzny? Co więcej, wysyłanie kopii "domowej" wersji tych przeglądarek do niektórych krajów (np. Kuba, albo państwa byłej Jugosławii) było traktowane jako przestępstwo? Niedawno wprawdzie, ze względu na dość powszechne stosowanie "silnej" kryptografii na świecie, restrykcje zostały złagodzone, ale nie zniesione.

W celu ułatwienia sobie zadania, agencje zajmujące się wywiadem bezustannie usiłują wywierać naciski na ciała ustawodawcze w rożnych krajach celem "osłabienia" kryptografii dostępnej szerokiej publiczności. Jedną z metod technicznych służących temu celowi byłoby zainstalowanie dodatkowego klucza w urządzeniach i oprogramowaniu kryptograficznym. Klucz taki umożliwiałby łatwiejszy dostęp do zakodowanych informacji, tworząc jak gdyby boczne wejście do oprogramowania, dostępne wyłącznie instytucji czy osobie która klucz taki zainstalowała.

Wracamy powoli do wspomnianej na początku sprawy "klucza"

kryptograficznego znalezionego w systemie operacyjnym Windows przez Andrew Fernandesa. Poprzez analizę zawartości pewnych plików binarnych będących składowa częścią systemu znalazł on informacje o co najmniej dwóch dziwnych "kluczach" zakodowanych w Windows, przy czym jeden z nich miął nazwę "NSA key". Pierwsza hipoteza Fernandesa była następująca: przez pomyłkę programiści pracujący dla Microsoft zapomnieli wymazać te informacje, zaś sam klucz rzeczywiście został "podrzucony" do systemu (zapewne za wiedza Microsoft) przez NSA. W prasie podniosła się wrzawa. Microsoft oficjalnie oświadczył, że klucz znaleziony przez Fernandesa należy do nich zaś firma nigdy nie kontaktowała się z NSA ani też nie wywierano na nią żadnych nacisków. Ponadto, oryginał klucza prywatnego, odpowiadającego znalezionemu kluczowi publicznemu jest dobrze zabezpieczony w sejfach Microsoft. Niektórzy uwierzyli w te wersje, tym bardziej, ze Fernandes, aczkolwiek z pewnością doskonały programista, zrobił pewne błędy w sposobie, w jaki opublikował swoje oprogramowanie pozwalające na zastąpienia "klucza NSA" innym. Autora niniejszego artykułu niepokoi jednak nie tyle to, czy rzeczywiście znaleziony przez Fernandesa klucz należał do NSA, lecz to, że klucz taki wogóle istnieje. Nie jest istotnie ważne, kto ma dostęp do niego, NSA czy Microsoft. Jakakolwiek instytucja by to była – posiada przez sam fakt posiadania klucza niewyobrażalne wręcz możliwości penetracji systemów komputerowych na całym świecie. Nie bez przyczyny wiec Niemcy, kraj dbający o własne bezpieczeństwo narodowe, bronią się wszelkimi sposobami przed produktami Microsoft, zaś rozwój kryptografii, w tym tej dostępnej w ramach tak zwanego "wolnego" oprogramowania (open source) stoi w tym kraju na wysokim poziomie.

Wkrótce zaś, w ciągu co najwyżej kilku lat, enkrypcję danych będzie przeprowadzał procesor na poziomie "hardware", nie zaś jak teraz na poziomie "software". Wtedy wykrycie i identyfikacja zainstalowanego w nim potajemnie dodatkowego klucza kryptograficznego staną się prawie niemożliwe.

Autor: Zbigniew Kozioł
Źródło: “Infonurt” nr 10 (luty 2003)

MATERIAŁY ŹRÓDŁOWE

1. Duncan Campbell, Australia first to admit “we’re part of global surveillance system”, http://www.heise.de/tp/english/inhalt/te/2889/1.html
2. Steve Kettmann and James Glave, MS Denies Windows ‘Spy Key’, http://www.wired.com/news/technology/0,1282,21577,00.html
3. Duncan Campbell, How NSA access was built into Windows, http://www.heise.de/tp/english/inhalt/te/5263/1.html
4. Duncan Campbell, NSA Builds Security Access Into Windows, http://www.techweb.com/wire/story/TWB19990903S0014
5. Duncan Campbell, Interception Capabilities 2000 (raport przygotowany dla Parlamentu Europejskiego), http://www.iyp.org/3crypt/stoa/
6. National Security Agency, Frequently Asked Questions, http://www.nsa.gov/about_nsa/faqs_internet.html