Podsłuch przez gniazdko elektryczne

17 lipca 2009

Czy kiedykolwiek siedząc w swoim biurze przy komputerze pomyślałaś(eś) o tym, że to co piszesz może ujrzeć osoba niepowołana? Nie mów tylko, że masz zainstalowany i dobrze skonfigurowany program antywirusowy oraz firewall, tak że żaden haker się nie włamie.

Czy kiedykolwiek siedząc w swoim biurze i opracowując dokumenty pomyślałaś(eś) o tym, że to co piszesz może ujrzeć osoba postronna, czyli niepowołana? Nie mów tylko, że masz zainstalowany i dobrze skonfigurowany program antywirusowy oraz firewall, tak że żaden keylogger ani koń trojański nie pozwoli hakerowi wykraść Twoich poufnych danych. Zagrożenie wcale nie musi przyjść z Internetu. Złodziej danych (nawet off-line) może równie dobrze kryć się w sąsiednim pokoju bądź na korytarzu…

Jak podaje serwis informacyjny BBC, 2 pracownice firmy Inverse Path, zajmującej się sprawami bezpieczeństwa komputerów, przeprowadziły test, który wykazał, że do „podsłuchania" tego, co piszemy na klawiaturze wystarczy zwykłe gniazdko elektryczne oraz oczywiście sprzęt rejestrujący zmiany napięcia elektrycznego, w który musi być wyposażony cracker (złodziej naszych danych). Panie Andrea Barisani oraz Daniele Bianco udowodniły, że nawet z odległości 15 metrów od komputera ofiary możliwe jest zarejestrowanie naciskanych przez nią klawiszy. Nie znaczy to, że na większe dystanse odczyt jest całkowicie niemożliwy – po prostu pogarsza się tylko jego jakość.

Brzmi to wszystko niemal niewiarygodnie i przypomina scenę z filmów science-fiction. Gdzie leży przyczyna luki w zabezpieczeniach naszych komputerów? Otóż, winowajcą jest

standardowy kabel PS/2, przez który podłączonych jest na świecie wiele klawiatur komputerowych. Posiadacze klawiatur podłączonych przez USB oraz bezprzewodowych przynajmniej na razie mogą odetchnąć z ulgą (dopóki ktoś nie odnajdzie słabych stron tych przekaźników informacji). Konkretnie, problem leży w konstrukcji kabla. Składa się on z sześciu żył, które znajdują się bardzo blisko siebie i nie są ekranowane, co znaczy, że wskutek interferencji sygnału dane przesyłane z klawiatury do komputera mogą przenikać z „żył danych" do przewodu uziemieniowego. Ten właśnie przewód uziemieniowy jest połączony z przewodem uziemieniowym wtyczki zasilającej pecet. Wtyczka ta jest z kolei podłączona do gniazda elektrycznego. Jeżeli do tego samego gniazdka lub innego, wchodzącego w skład tego samego obwodu zostanie podłączone urządzenie rejestrujące zmiany napięcia elektrycznego, cracker może dowiedzieć się, co piszemy na naszej klawiaturze. Może wykraść nasze dokumenty, loginy i hasła do kont w portalach internetowych, a także w wirtualnych bankach!

Jak to możliwe, żeby napastnik odróżnił sygnały z naszej klawiatury od innych sygnałów, pochodzących z komputera oraz innych urządzeń? Otóż, przebiegły złodziej może zastosować filtr, który wytłumi inne sygnały. Rozpoznanie zmian napięcia pochodzących właśnie z klawiatury nie jest szczególnie trudnym zadaniem, gdyż:

1. Dane z klawiatury do komputera są przekazywane w relatywnie dużych odstępach czasu (znacznie większych niż w przypadku transferu informacji z innych urządzeń podłączonych do peceta).

2. Informacje są przesyłane bit po bicie, więc nie istnieje zagrożenie, że sygnały rejestrowane przez złodzieja na oscyloskopie nałożą się na siebie i w ten sposób staną się niewyraźne.

Widać więc, że nawet odłączeni od Internetu nie możemy być pewni, czy ktoś niepowołany nie uzyska dostępu do naszych

danych, posługując się urządzeniem do podsłuchu elektrycznego za pośrednictwem zwyczajnego gniazdka elektrycznego! Nie należy jednak wpadać w panikę. Żeby potencjalnemu złodziejowi zależało na naszych danych, muszą być one bardzo cenne, aby inwestycja w sprzęt rejestrujący zmiany napięcia opłacała mu się. Poza tym, możemy kupić klawiaturę podłączaną przez kabel USB.

Doświadczenie ze zdalnym przechwytywaniem transmisji między klawiaturą a komputerem ma zostać zaprezentowane podczas konferencji Black Hat w Las Vegas (USA), która odbędzie się w dniach 25-30 lipca.

Autor: Bartosz Krawczyk
Źródło: iThink