Szyfruj z nami: bezpieczne dane

6 grudnia 2014

Przypadek 1. Piątkowy wieczór na mieście. Twój telefon leży na blacie stolika, przy którym siedzisz ze znajomymi. Co chwilę upewniasz się, czy jest na miejscu. W pewnym momencie wciąga Cię rozmowa i dopiero po jakimś czasie orientujesz się, że nie możesz znaleźć komórki. Po prostu rozpłynęła się w powietrzu.

Przypadek 2. Spieszysz się na pociąg do innego miasta. Nie możesz się spóźnić, bo czeka Cię ważne spotkanie. Ale wszystko idzie na opak: deszcz, korki, spóźniony autobus, tłok i zamieszanie. Udaje Ci się zdążyć na pociąg w ostatniej chwili. Dopiero w środku orientujesz się, że nie masz przy sobie torby z komputerem.

TO MOŻE SPOTKAĆ KAŻDEGO

Sytuacji, w których możemy stracić laptopa, tablet czy smartfon, jest znacznie więcej. Ryzyko to dotyczy każdego posiadacza tego rodzaju urządzeń i wiąże się nie tylko z utratą cennego sprzętu, ale również zapisanych na nim danych. Zdjęcia z wakacji, poufne dokumenty, dane klientów, zapisy prywatnych rozmów – w czyich są rękach i co się z nimi dzieje? Wyobraźnia podpowiada najgorsze scenariusze. Niestety niektóre z nich mogą się zrealizować. Dzisiaj, gdy tak wiele informacji gromadzimy na komputerach i telefonach, nie sposób uniknąć stresu związanego z ich utratą. Na taką sytuację można się jednak przygotować. Przede wszystkim warto zaszyfrować pamięć urządzeń, z których korzystamy. Odczytanie tak zabezpieczonych danych jest bardzo trudne, dlatego w razie utraty sprzętu będzie można spać trochę spokojniej.

Poziom zabezpieczeń warto dostosować do konkretnej sytuacji. Szyfrowanie danych powinno być standardem zwłaszcza wówczas, gdy zapisujemy na przenośnym sprzęcie poufne czy intymne

informacje. Szczególną uwagę powinno się zwracać na zabezpieczenie danych innych osób, na przykład klientów firmy czy podopiecznych organizacji pozarządowej.

Szyfrowanie danych – wbrew pozorom – nie jest szczególnie trudne i właściwie każdy może z niego korzystać. Zachęcamy, by spróbować i tłumaczymy co i jak warto zaszyfrować.

SZYFROWANIE DYSKU KOMPUTERA

Szyfrowanie dysku systemowego w komputerze (stacjonarnym lub laptopie) jest prostym i skutecznym sposobem ochrony zgromadzonych na nim danych. Oprócz zabezpieczenia dostępu do informacji, uniemożliwia wykorzystanie zapamiętanych na komputerze haseł (np. w przeglądarce internetowej). W przypadku systemów z rodziny Windows zaleca się użycie oprogramowania BitLocker firmy Microsoft (dostarczane z wersjami Ultimate i Enterprise systemu) lub TrueCrypt 7.1a (o wątpliwościach dotyczących wersji 7.2 przeczytasz TUTAJ). Dla komputerów firmy Apple z systemem Mac OS dostępne jest narzędzie FileVault wbudowane w system operacyjny. Dla systemów GNU/Linux stworzono LUKS, zwykle dostępny jako opcja do wyboru już na etapie instalacji systemu.

SZYFROWANIE PAMIĘCI TELEFONU

Zagrożenia w przypadku utraty smartfona są podobne jak w przypadku komputera osobistego. Tu jednak musimy się zdać na rozwiązania przygotowane dla systemu operacyjnego naszej komórki. W telefonach pod kontrolą Androida szyfrowanie całej pamięci dostępne jest od dla wersji 3.0 systemu i nowszych: wystarczy wybrać tę opcję w ustawieniach urządzenia (Bezpieczeństwo/Zabezpieczenia). W urządzeniach firmy Apple możemy zabezpieczyć dane od wersji iOS v4.0 poprzez wprowadzenie w ustawieniach kodu odblokowującego (Touch ID/Kod).

SZYFROWANIE DANYCH W CHMURZE

Dane coraz częściej zapisujemy nie tylko w pamięci urządzeń, ale również w chmurze. To wygodne rozwiązanie, które w przypadku utraty sprzętu chroni zapisane pliki przed utratą. Niestety nie jest optymalne z punktu widzenia bezpieczeństwa informacji. Osoba zapisująca pliki w chmurze może stracić nad nimi kontrolę, nawet jeśli nie będzie rozstawać się ze swoim sprzętem. Dlatego warto dwa razy się zastanowić, zanim pozwolimy zapisać jakiejś firmie zapisać nasze dane na swoich serwerach.

Jeśli zdecydujemy się na takie rozwiązanie, warto się zabezpieczyć – nawet jeśli mamy zaufanie do naszego usługodawcy, jego infrastruktura może być celem ataku włamywaczy. Coraz częściej usługodawcy zapewniają jako standard lokalne (czyli przeprowadzane na naszym sprzęcie przed przesłaniem plików przez Internet) szyfrowanie naszych plików (np. SpiderOak i Wuala). Jako alternatywę warto rozważyć również instalację wolnego oprogramowania Duplicati, które oprócz silnego szyfrowania naszych danych pozwala korzystać z wielu różnych usług dysków wirtualnych (takich jak Google Drive, Amazon S3 czy Windows Live SkyDrive) lub z własnego serwera (program obsługuje dostęp do plików po WebDAV, SSHi FTP).

SZYFROWANIE DYSKÓW ZEWNĘTRZNYCH

Najlepszym sposobem na tworzenie kopii zapasowych jest ich zapisywanie na dyskach zewnętrznych. Sprzęt wykorzystywany do robienia backupów również warto zabezpieczyć, podobnie jak pamięć przenośną (pendrive), która jest szczególnie narażona na utratę. Można je zaszyfrować w całości lub stworzyć na nich zaszyfrowane foldery (tzw. kontenery). Jeśli pracujemy na systemie Windows, możemy wykorzystać oprogramowanie TrueCrypt, a w przypadku systemów Mac OS oraz GNU/Linux – użyć wbudowanych funkcjonalności.

PODSUMOWANIE

Szyfrowanie danych jest bardzo użyteczne i stanowi podstawowe narzędzie ochrony w przypadku utraty sprzętu. Trzeba jednak pamiętać, że nie stanowi odpowiedzi na wszystkie zagrożenia. Dlatego warto korzystać z różnych zabezpieczeń, na przykład czyścić historię przeglądanych stron. A najbardziej poufnych informacji nie zapisywać w chmurze ani na urządzeniach, które możemy łatwo stracić.

Autorstwo: Michał „czesiek” Czyżewski, Małgorzata Szumańska
Współpraca: Kamil Śliwowski
Źródło: Fundacja Panoptykon