SZYFRUJESZ CZY RYZYKUJESZ?

Ile laptopów ginie z polskich firm? Co nam grozi, jeżeli doprowadzimy do wycieku firmowych danych? Ile wynosi maksymalna kara za taki wyciek i czy może doprowadzić firmę do bankructwa?

„Przy dzisiejszych metodach kryptograficznych (...) osoba, która przejmie nad dyskiem kontrolę, bo na przykład ukradnie nam sprzęt, nie będzie w stanie dotrzeć do zapisanych tam danych. (...) szyfrowanie danych na twardych dyskach czy pendrivach jest absolutnie konieczne. W przeciwnym przypadku możemy być współodpowiedzialni za utratę danych osobowych."

dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych w latach 2010-2014[1]

OBOWIĄZKI PRZEDSIĘBIORCY

- Szyfrowanie każdego komputera zawierającego dane osobowe wynoszonego poza siedzibę firmy.

§ *Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.*

pkt. V Załącznika A (Środki bezpieczeństwa na poziomie podstawowym) do Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. (Dz.U.2004.100.1024).

- Dobre praktyki bezpieczeństwa przedstawicieli zawodów przetwarzających wrażliwe dane np. lekarzy, ubezpieczycieli i adwokatów.

§ *Adwokat posługujący się w pracy zawodowej komputerem lub innymi środkami elektronicznego utrwalania danych obowiązany jest stosować oprogramowanie i inne środki zabezpieczające dane przed ich niepowołanym ujawnieniem.*

§ 19 ust. 5 Kodeksu etyki adwokackiej

JAK TRACIMY DANE?

- Niemal co druga polska firma nie szyfruje danych na swoich laptopach[2]
- 3 na 10 polskich firm miało w 2013 do czynienia z utratą komputera przenośnego[3]
- Niemal 1/3 laptopów skradzionych w Polsce zabrano bezpośrednio z biura firmy [4]
- 96% informacji traconych przez firmy na skutek wycieków to dane osobowe [5]

KONSEKWENCJE WYCIEKU DANYCH OSOBOWYCH

- BANKRUCTWO
  Utrata dwóch niezaszyfrowanych laptopów z danymi 14 000 klientów zakończyła w 2012 roku działalność amerykańskiej firmy Impairment Resources LLC. Łączna szacowana wysokość kar tj. 2,5 miliona dolarów ponad 10-krotnie przekroczyła budżet firmy doprowadzając ją do bankructwa.[6]

- KARY FINANSOWE
  Grzywna w celu przymuszenia nakładana przez Generalnego Inspektora Ochrony Danych Osobowych (do 200 tys. zł) lub grzywna orzekana przez sąd w postępowaniu karnym (do 1 mln 80 tys. zł).

- STRATY FINANSOWE
  182 tys. zł to największa strata polskiej firmy związana z wyciekiem danych. Średnią wartość danych utraconych w wyniku jednorazowej utraty laptopa oszacowano na 32 tys. zł - ponad 6 x więcej, niż wartość samego utraconego sprzętu (średnio 5 tys. zł).[7]

- UTRATA ZAUFANIA
  Utrata zaufania klientów i partnerów handlowych może być znacznie dotkliwsza niż kary finansowe. Dotyczy to zwłaszcza firm i instytucji zaufania publicznego jak banki czy placówki opieki zdrowotnej.

- KONSEKWENCJE DLA OSOBY ODPOWIEDZIALNEJ ZA WYCIEK
  Grzywna, ograniczenie albo pozbawienie wolności.

§ *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Art. 51 ust. 1 ustawy z 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.2014.1182.j.t. ze zm.)

PRZYPADKI KRADZIEŻY DANYCH

- Kradzież laptopa Kamila Durczoka (listopad 2014)[8]
- Kradzież laptopa komisji śledczej z danymi nt. śmierci Krzysztofa Olewnika (sierpień 2009)[9]
- Kradzież laptopa posła Wiesława Kaczmarka z danymi PKN Orlen (październik 2004)[10]

DLACZEGO WARTO SZYFROWAĆ?

- Szyfrując firmowe dane spełniamy prawne wymogi dotyczące bezpieczeństwa przetwarzanych informacji.
- Dane zawarte na firmowych komputerach i osobistych urządzeniach mobilnych pracowników są chronione przed niepowołanym dostępem.
- W przypadku przesyłania szczególnie wrażliwych danych można utworzyć zaszyfrowaną wiadomość, którą odczyta jedynie jej odbiorca posiadający ustalony klucz.
- Współczesne rozwiązania szyfrujące są proste w obsłudze i zarządzaniu – pozwalają pracownikom m.in. szyfrować dane po prostu kopiując je do wyznaczonego przez administratora folderu.

Źródła:
1. „Lekarze powinni pamiętać o szyfrowaniu danych na laptopach" z 6.02.2013r., pobrano 17.03.2015r./ www.giodo.gov.pl
2, 3, 4, 7. „Intel: firmowe laptopy najczęściej giną w trakcie podróży" z 10.10.2013r., pobrano 17.03.2015r. / www.biznes.newseria.pl
5. „Global Data Leakage Report 2010", s.9, pobrano 17.03.2015r. / www.infowatch.com
6. „Privacy Law Alert: Data Breach Leads to Bankruptcy" z 19.08.2013r., pobrano 17.03.2015r. / www.smlrgroup.com
8. Wprost - „Kamil Durczok. Fakty po Faktach", s.11, nr 8/2015. / www.wprost.pl
9. „Sprawa Olewnika: skradziono laptopy obrońcy" z 25.07.2009r., pobrano 17.03.2015r. / www.interia.pl
10. „Napad na prok. Kapustę – zapiski dot. PKN Orlen skradzione" z 20.10.2004r., pobrano 17.03.2015r. / www.wp.pl

DAGMA Biuro Bezpieczeństwa IT
tel. 32 793 11 00 / 32 259 11 00 | handel@dagma.pl
www.dagma.com.pl