**Będą kary za brak zabezpieczeń. Jedynie 44% firm traktuje poważnie szyfrowanie danych**

**Dzisiejsze regulacje już w momencie ich wdrażania nie przystawały w pełni do zmieniającej się rzeczywistości technologicznej. W rozporządzeniu o zabezpieczeniu danych wskazano jedynie ogólną normę, mówiącą, że środki bezpieczeństwa danych powinny być adekwatne do zagrożeń. Eksperci alarmują, że firmy bezzwłocznie powinny zmienić podejście do zabezpieczania swoich danych!**

Jak wskazuje Generalny Inspektor Ochrony Danych Osobowych (GIODO) powinno się szyfrować wszelkie dane przesyłane do sieci publicznej, pomimo, że obecnie tego typu obowiązek nie jest literalnie wskazany w dzisiejszych regulacjach prawnych. Wydaje się, że stanowisko GIODO jest w pełni uzasadnione na gruncie koncepcji adekwatnego zabezpieczenia danych osobowych, a także przygotowuje częściowo do implementacji prawnej Unijnego rozporządzenia o ochronie danych osobowych.

 Już za półtora roku – pod koniec maja 2018 – na terenie całej Unii Europejskiej wejdzie w życie RODO, które przewidywać będzie poważne sankcje w przypadku nieodpowiedniego przetwarzania lub zabezpieczenia danych. Firma będąca administratorem danych może ponieść odpowiedzialność administracyjną, uregulowaną na poziomie państwowym, a także w części przypadków otrzymać sankcję finansową – zależną od rocznych obrotów firmy, sięgającą nawet 20 mln Euro!

- *W firmach i administracji często brakuje odpowiedniej polityki bezpieczeństwa, nie stosuje się także szyfrowania urządzeń.Tymczasem na rynku są dostępne, m.in. polskie rozwiązania szyfrowania urządzeń z wykorzystaniem mechanizmu HVKM (Hybrid Virtual Key Management), które wykluczają przechowywanie danych na serwerach zewnętrznych firm w sposób jawny. Dodatkowo firmy - usługodawcy nie posiadają pary kluczy deszyfrujących, tym samym uniemożliwiając odtworzenie przechowywanej treści bez wiedzy klienta* – podkreśla Kamil Kaczyński z Instytutu Matematyki i Kryptologii, Wydział Cybernetyki Wojskowej Akademii Technicznej (WAT).

 Tymczasem wg rapotu firmy Sophos wynika, że jedynie 44% przebadanych firm "w znacznym stopniu" wykorzystuje możliwość zabezpieczenia danych poprzez szyfrowanie. Większość z nich – 61% - decyduje się na szyfrowanie w celu ochrony własnych danych, a ponad połowa z uwagi na ochronę danych osobowych pracowników. 18% uważa, że szyfrowanie może pomóc w uniknięciu kosztów finansowych towarzyszących naruszeniu danych wrażliwych.

 Jak twierdzą eksperci bezpieczeństwa IT, cyberprzestępstwa niosą ze sobą koszty wyższe niż wartość skradzionych informacji. Efekty fali są często bardziej szkodliwe niż sama kradzież. Utrata zaufania – zarówno ze strony firmy, jak i klientów – skłania do nadmiernych wydatków na środki zaradcze, wywołuje poczucie zobowiązania do zapłaty dla poszkodowanych dostawców i partnerów oraz, przynajmniej przez pewien czas, skutkuje odpływem klientów. Wg danych zawartych w Check Point Security Report 2016 w 2014 roku głównym celem hakerów były dane kart kredytowych o stosunkowo krótkim czasie przydatności – wystawcy kart kredytowych szybko anulują rachunki i wydają nowe karty.

W 2015 roku autorzy ataków zmienili cel na dane o dłuższym okresie przydatności – dane osobowe i kradzież tożsamości. Dodatkowo w 2014 roku byli ukierunkowani głównie na cele w handlu detalicznym i branży finansowej, a w 2015 roku przenieśli obszar swoich zainteresowań na cele rządowe i służbę zdrowia.

Im dłuższy jest okres przydatności rekordu, tym bardziej kosztowne jest sprzątanie. Polskie komputery coraz częściej znajdują się na celowniku hakerów czego przykładem mogą być cyberataki podczas Światowych Dni Młodzieży czy szczytu NATO. W Polsce co godzinę firmy ściągają ponad 100 plików zagrożonych wirusem, z kolei na świecie nawet 88% organizacji doświadczyło utraty danych…

*- Biorąc pod uwagę zeszłoroczne statystyki Rządowego Zespołu Reagowania na Incydenty Komputerowe działającego w ramach ABW, mówiące o blisko 9 tys. zidentyfikowanych ataków na firmy strategiczne w Polsce, ryzyko jest bardzo duże –* przestrzegają przedstawiciele polskiej firmy CryptoMind, tworzącej programy kryptograficzne.