

Zabezpieczenie systemu informatycznego do przetwarzania danych osobowych. Co na to prawo i GODO?

[Marcin Maj](#), 9.03.2016

Prawo zobowiązuje administratorów danych osobowych do stosowania środków technicznych odpowiednio chroniących dane. W tej sytuacji niejedna firma lub instytucja może się zastanawiać, czy komputer podłączony do internetu jest odpowiednio zabezpieczony. Pewna dyrektor Poradni Psychologiczno-Pedagogicznej postanowiła spytać GODO o tę sprawę i uzyskała odpowiedź.

GODO odpowiedział dyrektorze PPP, że wskazówek dotyczących poziomu zabezpieczeń należy szukać w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w *sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. z 2004 r. Nr 100, poz. 1024).

To rozporządzenie mówi, że system informatyczny służący do przetwarzania danych powinien być zabezpieczony przed zagrożeniami z sieci publicznej - fizycznie lub logicznie. Zabezpieczenia logiczne obejmują kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną, a także kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

GODO wyjaśnia co to oznacza w praktyce.

- Kontrola ta może być oparta na instalacji specjalistycznego oprogramowania, które analizuje i rejestruje przepływ informacji na styku lokalnej sieci administratora danych z siecią publiczną oraz podejmuje zaprogramowane decyzje np. w zakresie czy daną informację przekazać do sieci lokalnej czy też zablokować z uwagi na związane z nią zagrożenie. Oprogramowanie, o którym wspomniano wyżej, wykorzystywane do analizy tego ruchu to systemy antywirusowe, antyspamowe, firewalle, IDS-y, IPS-y i inne, które należy wdrożyć w odpowiednich miejscach w strukturze lokalnej sieci administratora danych. Systemy te mogą być instalowane jako oddzielne, niezależne programy lub jako elementy określonych pakietów sprzętowo-programowych stanowiących wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia UTM (ang. Unified Threat Management) - czytamy w odpowiedzi GODO.

Wspomniane urządzenia mogą oferować funkcję antywirusowe, funkcje sondy wykrywającej i blokującej próby włamań, filtra treści stron internetowych, routera, VPN, translatora adresów (NAT) i inne. Wśród tych innych funkcji systemu UTM mogą być np. kontrola

aplikacji, kontrola sieci bezprzewodowej WiFi), czy ochrona przed wyciekiem danych (funkcja DLP).

Wymienione rozwiązania, jeśli zostaną właściwie wdrożone i będą monitorowane, są w stanie wypełnić zobowiązanie administratora danych w zakresie zabezpieczenia systemu w sposób określony w punkcie XII.2 załącznika do wymienionego rozporządzenia.

Poniżej, dla zainteresowanych, odpowiedź GIODO w całości.

[035 2919 15 Zabezpieczenia Internetowe 20160218 FIN Po Anonimizacji](#)