Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **11.01.2021 r.**

Podmiot kontrolowany **U.S.A.**

Wysokość kary **UPOMNIENIE**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5 ust. 1 lit. f), art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i ust. 2 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W maju 2020 r. U S.A. (Spółka) dokonała zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszenia ochrony danych osobowych, które polegało na przełamaniu zabezpieczeń systemu informatycznego Spółki, a następnie zaszyfrowaniu przetwarzanych w nim danych.

Opis wydarzeń:

1) W kwietniu 2020 r. złośliwe oprogramowanie szyfrujące „Devos" dezaktywowało ochronę antywirusową zastosowaną w Spółce, co skutkowało uniemożliwieniem zadziałania mechanizmów bezpieczeństwa systemów operacyjnych. Infekcja miała miejsce w godzinach nocnych, a nieprawidłowości stwierdzono dopiero w godzinach porannych.

2) Zaszyfrowane bazy danych obejmowały około 80 000 rekordów danych pracowników, klientów oraz pacjentów w zakresie imię i nazwisko, imiona rodziców, data urodzenia, numer rachunku bankowego, adres zamieszkania, numer ewidencyjny PESEL, adres e-mail, seria i numer dowodu osobistego, numer telefonu oraz dane dotyczące zdrowia.

Przyczyna naruszenia:

Brak aktualizacji oprogramowania oraz technicznego wsparcia producenta.

Decyzja PUODO:

Upomnienie.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2) Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

3) Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

4) Dokonaj wdrożenia procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowania ruchu sieciowego.

5) Przeprowadzaj testy nastawione na weryfikację zabezpieczeń programów i aplikacji.

6) Wykonuj kopie zapasowe na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych.

7) Do przetwarzania danych osobowych wykorzystuj oprogramowanie posiadające aktualne wsparcie techniczne producenta.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak