Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Hiszpania**
Spanish Data Protection Authority (AEPD)

Data wydania decyzji — **15 marca 2021 r.**

Podmiot kontrolowany — Air Europa Lineas Aereas, SA.

Wysokość kary — **600 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 32 (1), art. 33 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Air Europa Lineas Aereas, SA. (Air Europa) dokonał zgłoszenia do hiszpańskiego organu nadzorczego naruszenia ochrony danych osobowych. Polegało ono na nieautoryzowanym dostępie do danych kontaktowych i kart bankowych klientów.

Opis wydarzeń:

1) Air Europa otrzymał powiadomienie od VISA (Banco Popular) dotyczące potencjalnego incydentu bezpieczeństwa.

2) Ponadto firmy obsługujące karty kredytowe poinformowały, że około 4 000 kart kredytowych zostało wykorzystanych do popełnienia przestępstwa.

3) W związku z powyższym odkryto, że doszło do ataku na serwer Air Europa oraz pozyskania 1 500 000 rekordów danych oraz 489 000 danych klientów.

4) Prawdopodobną przyczyną naruszenia było włamanie na niezabezpieczone systemy dostępne w Internecie oraz wykorzystanie przez atakującego hasła, które nie spełniało wymagań dotyczących złożoności oraz długości.

5) Hiszpański organ nadzorczy na podstawie zgromadzonego materiału dowodowego uznał, że Air Europa nie zapewnił odpowiedniego poziomu bezpieczeństwa.

Przyczyna naruszenia:

Air Europa nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa.

Decyzja Spanish Data Protection Authority (AEPD):

1) Kara pieniężna w wysokości 600 000 EUR, w tym:

a) 500 000 EUR za brak wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa,

b) 100 000 EUR za poinformowanie o naruszeniu ochrony danych osobowych z opóźnieniem.

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) Wykonaj wdrożenie procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego.

3) Wykonuj regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

4) Wykonuj testy podatności systemów informatycznych i aplikacji.

5) Wprowadź politykę regularnej zmiany haseł dostępu.

6) Twórz skomplikowane i silne hasła dostępu.

7) Stosuj wieloskładnikowe uwierzytelnianie.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak