Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Holandia

Dutch Supervisory Authority for Data Protection (AP)

Data wydania decyzji

12 listopad 2021 r.

Podmiot kontrolowany

Transavia Airlines CV

Wysokość kary

400 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 32 (1), (2) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Transavia Airlines CV (Transavia) dokonała zgłoszenia do holenderskiego organu nadzorczego naruszenia ochrony danych osobowych, które polegało na nieautoryzowanym dostępie do systemów informatycznych.

Opis wydarzeń:

1) W związku z otrzymanym zgłoszeniem holenderski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Transavia.

2) W trakcie czynności kontrolnych holenderski organ nadzorczy ustalił, iż:

a) cyberprzestępca uzyskał dostęp do systemów informatycznych Transavia za pośrednictwem adresów mailowych użytkowników korzystając z metody „rozpylania hasła" (password spraying) lub „upychania poświadczeń",

b) w związku z powyższymi działaniami skopiowane zostały m.in. dokumenty sieciowe, dokumenty biznesowe oraz dane z 6 skrzynek mailowych,

c) analiza śledcza wykazała, że w skrzynkach mailowych znajdowało się 49 plików z danymi osobowymi 81 000 osób w tym dane o:

- klientach w zakresie: imię i nazwisko, data urodzenia, informacja o locie, kod SSR (dane dotyczące korzystania z wózka inwalidzkiego, głuchoty i ślepoty),
- pracownikach w zakresie: imię i nazwisko, służbowy adres e-mail, adres, numer telefonu,
- dostawcach w zakresie: imię i nazwisko, służbowy adres e-mail, adres, numer telefonu,

d) atakujący mógł mieć dostęp do 25 milionów osób.

3) Na podstawie zebranego materiału dowodowego norweski organ nadzorczy dopatrzył się następujących uchybień:

a) brak stosowania wieloskładnikowego uwierzytelniania,

b) zainstalowanie w niektórych systemach przestarzałych systemów operacyjnych,

c) nienadzorowany dostęp do Internetu dla niektórych systemów,

d) stosowanie prostych i powszechnie używanych haseł, które były łatwe do odgadnięcia.

Przyczyna naruszenia:

Transavia nie wdrożyła odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.

Decyzja:

Kara pieniężna w wysokości 400 000 EUR.

Źródło:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf

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) Wykonuj testy podatności systemów informatycznych i aplikacji.

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

6) Stosuj wieloskładnikowe uwierzytelnianie.

7) Wprowadź politykę regularnej zmiany haseł dostępu.

8) Twórz skomplikowane i silne hasła dostępu.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak