KARY ZAGRANICZNYCH URZĘDÓW OCHRONY DANYCH OSOBOWYCH:

WĘGRY

Organ: Węgierski Krajowy Urząd Ochrony Danych i Wolności Informacji (Nemzeti Adatvédelmi és Információszabadság Hatóság)

Podmiot ukarany: Digi Távközlési Szolgáltató Kft. Ltd. ("Digi") - jeden z największych dostawców usług łączności elektronicznej

Wysokość kary pieniężnej: 100 mln HUF (ok. 285 000 EUR)

Data wydania decyzji: 18 maja 2020

CO SIĘ WYDARZYŁO?

Etyczny haker odkrył słabość strony internetowej Digi - można było uzyskać dostęp do "testowej bazy danych" zawierającej znaczną ilość danych osobowych abonentów Digi (m.in. nazwisko, dane i miejsce urodzenia, adres e-mail i hasło, numer konta bankowego, numer dowodu osobistego, niekiedy krajowy numer identyfikacyjny).

Testowa baza danych została utworzona w celu tymczasowego wyeliminowania błędu, który polegał na tym, że serwery internetowe nie mogły uzyskać dostępu do serwerów baz danych. Przeniesienie danych miało na celu zapewnienie dostępności danych subskrybentów na czas eliminacji błędu. Dane nie zostały zaszyfrowane. Firma uznała, że wystarczające było ograniczenie dostępu i przydzielanie odpowiednich praw. Ponadto zdaniem Digi stosowanie takiego szyfrowania mogło powodować problemy w stosowaniu i działaniu baz danych. Okazało się jednak, że etyczny haker był w stanie uzyskać dostęp do bazy danych. Spółka nie była świadoma tej podatności do czasu uzyskania dostępu do bazy przez hakera.

Organ nadzorczy stwierdził następujące naruszenia:

- **naruszenie zasady "ograniczenia celu"** - po naprawie błędu Digi nie usunęła danych osobowych z "bazy testowej"; spółka przechowywała tam więc dane osobowe bezcelowo od momentu usunięcia usterki do momentu wystąpienia zdarzenia;
- **naruszenie zasady "ograniczenia przechowywania"** - po rozwiązaniu problemu Digi przechowywała dane w bazie testowej w niezmienionej formie, tj. nadal można było zidentyfikować konkretne osoby fizyczne na podstawie informacji tam zawartych;
- **brak odpowiedniego zabezpieczenia danych** - dane osobowe nie były zaszyfrowane, nie przeprowadzono oceny ryzyka; spółka nie przeprowadzała testów podatności strony internetowej; brak śledzenia i monitorowania nawet nieoficjalnych poprawek do systemu; luka w systemie była powszechnie znana od 9 lat - mimo to ukarany podmiot nie podjął żadnych działań w celu jej usunięcia

WNIOSKI DLA ADMINISTRATORÓW DANYCH OSOBOWYCH:

- dane osobowe **należy usunąć lub zanonimizować niezwłocznie po ustaniu celu**, dla którego dane zostały zebrane - **nie mogą być przechowywane dłużej niż to konieczne**;
- należy **dokonać analizy ryzyka** związanej z danym procesem przetwarzania danych osobowych, aby stwierdzić, czy brak stosowania określonych środków, np. szyfrowania danych osobowych, nie spowoduje zwiększenia ryzyka dla ochrony danych;
- należy **przeprowadzać testy podatności systemów, a także stron internetowych i śledzić informacje na temat stwierdzonych podatności oprogramowania i sposobów na ich usunięcie**

Opracowała: Agnieszka Rapcewicz

iSecure