Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Holandia**
Dutch Supervisory Authority for Data Protection (AP)

Data wydania decyzji — **10.12.2020 r.**

Podmiot kontrolowany — **Booking.com B.V.**

Wysokość kary — **475 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 33 RODO
Niewystarczające wypełnienie obowiązków powiadamiania o naruszeniu danych.

Przedmiot decyzji

Źródło postępowania:

W lutym 2019 r. Booking.com B.V. dokonał zgłoszenia do holenderskiego organu nadzorczego naruszenia ochrony danych osobowych, które polegało na uzyskaniu dostępu do systemu rezerwacji przez osobę do tego nieuprawnioną.

Opis wydarzeń:

1) 9 stycznia 2019 r. podmiot oferujący rezerwacje swoich obiektów zgłosił do Booking, że klient poinformował go o kontakcie, podczas którego osoba podszywająca się pod pracownika obiektu prosiła o podanie daty urodzenia lub numeru karty kredytowej celem opłacenia rezerwacji.

2) 13 stycznia 2019 r. ten sam podmiot zgłosił kolejną próbę wyłudzenia danych osobowych. Tym razem osoba dzwoniąca podawała się za pracownika Booking.

3) W kolejnych dniach do Booking wpłynęło więcej zgłoszeń opisujących podobny lub identyczny sposób działań socjotechnicznych.

4) Sprawa została zgłoszona do Zespołu ds. Bezpieczeństwa Booking, który przeprowadził stosowne sprawdzenie.

5) W wyniku kontroli ustalono, że nieznana osoba trzecia uzyskała dostęp do Extranetu rezerwacji Booking, najprawdopodobniej w wyniku podania przez pracownika obiektu turystycznego osobie podającej się za pracownika Booking danych uwierzytelniających (nazwa użytkownika, hasło, dwuskładnikowy kod uwierzytelniający) w Extranecie rezerwacji.

6) Dochodzenie ujawniło również, że 40 innych podmiotów w Zjednoczonych Emiratach Arabskich współpracujących z Booking padło ofiarą oszustw socjotechnicznych, w wyniku których skradziono prawdopodobnie dane osobowe 4 109 osób.

7) Atak dotknął osoby, które pochodziły z Europy (w tym z Wielkiej Brytanii, Francji, Irlandii, Szwajcarii, Belgii, Holandii) i innych części świata (w tym RPA, Ameryki, Kanady i Bahrajnu).

8) W jego wyniku ujawniono następujące dane: imiona, nazwiska, adresy, numery telefonu, daty zameldowania i wymeldowania, ceny całkowite, numery rezerwacji, ceny za noc, wszelką korespondencję między obiektami turystycznymi a gośćmi, dane kart kredytowych (283 osoby) oraz kody weryfikacyjne kart (97 osób).

Przyczyna naruszenia:

Zbyt późne zgłoszenie przez największy portal rezerwacyjny w Europie kradzieży danych osobowych kilku tysięcy jego klientów.

Decyzja Dutch Supervisory Authority for Data Protection (AP):

1) Kara pieniężna w wysokości 475 000 EUR.

Kompas FORSAFE

JAK UNIKAĆ PODOBNYCH NARUSZEŃ?

1) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę:

a) konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia,

b) czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone.
Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne,

c) liczbę osób fizycznych, na które naruszenie wywiera wpływ.

2) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować ryzyko dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.

3) Jeśli masz wątpliwości co do oceny ryzyka dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia bezpieczeństwa danych osobowych, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.

4) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, dokonaj zawiadomienia o zaistniałym naruszeniu osób fizycznych, których dane dotyczą. Zawiadomienia należy wykonać bez zbędnej zwłoki.

5) Realizuj szkolenia dla osób zaangażowanych w przetwarzanie danych osobowych z tematyki cyberbezpieczeństwa, w tym ataków socjotechnicznych oraz metod obrony przed nimi.

JAB BRONIĆ SIĘ PRZED ATAKAMI SOCJOTECHNICZNYMI?

1) Zawsze pytaj osobę, która się z Tobą kontaktuje, dlaczego musisz podać określone dane.

2) Zweryfikuj tożsamość osoby, która się z Tobą kontaktuje. Jeśli wzbudzi Twoją wątpliwość, rozłącz się i zadzwoń na ogólny telefon podany na autentyczniej stronie firmy Konsultanta.

3) Weryfikuj adres strony w przeglądarce oraz sprawdź, czy połączenie jest szyfrowane i strona posiada certyfikat bezpieczeństwa (adres rozpoczyna się od https:/ oraz pojawia się symbol zamkniętej kłódki.

4) W przypadku linków znajdujących się na stronach internetowych lub w przysłanych wiadomościach e-mail sprawdź jaki adres kryje się pod linkiem, ale także dokąd prowadzi (po najechaniu na dany link u dołu przeglądarki powinien wyświetlić się faktyczny adres, pod który kieruje odnośnik).

5) Aktualizuj oprogramowanie – zarówno system operacyjny, programy i aplikacje, z których korzystasz oraz oprogramowanie antywirusowe.

6) Nie stosuj jednego hasła do logowania w różnych miejscach. Tam, gdzie jest to możliwe wykorzystuj weryfikację wieloskładnikową.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak