Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Wielka Brytania**
Information Commissioner (ICO)

Data wydania decyzji — **13.11.2020 r.**

Podmiot kontrolowany — **Ticketmaster UK ltd**

Wysokość kary — **1 405 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 5 (1) f), Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Brytyjski organ nadzorczy w związku z atakiem hakerskim dokonał w czerwcu 2018 r. czynności kontrolnych w Ticketmaster UK Limited.

Opis wydarzeń:

1) W kwietniu 2018 r. do Ticketmaster zaczęły wpływać informacje od Barclaycard, MasterCard, American Express, Bank Barclays, Monzo Bank oraz Commonwealth Bank of Australia o przypuszczalnym naruszeniu bezpieczeństwa danych osobowych.

2) Bank Barclays poinformował, że ujawniono około 60 000 danych dotyczących poszczególnych kart. Natomiast Monzo Bank poinformował, że około 50 jego klientów zgłosiło podejrzane transakcje na swoich kontach, w wyniku których ich karty płatnicze zostały wymienione. Z kolei Commonwealth Bank of Australia przekazał informację, że 1756 użytkowników kart MasterCard padło ofiarą oszustwa.

3) W maju 2018 r. Ticketmaster zaangażował cztery zewnętrzne firmy w celu zbadania podejrzenia naruszenia bezpieczeństwa danych osobowych. Ustalono, że wszelkie naruszenia systemów Ticketmaster najprawdopodobniej pochodziły z australijskiej witryny internetowej Ticketmaster, która w dużej mierze znajdowała się w sieciach i centrach danych w Ameryce Północnej.

4) Od maja do czerwca 2018 r. do Ticketmaster wpływały kolejne sygnały zarówno od osób prywatnych jak i podmiotów o złośliwym kodzie umieszczonym na stronie internetowej.

5) Pomimo analiz wykonanych zarówno przez zespół reagowania na incydenty oraz firmę Inbenta zajmująca się czatem pomocy – nie znaleziono żadnych oznak obecności złośliwego oprogramowania.

6) Pod koniec czerwca 2018 r. Barclaycard ponownie powiadomił Ticketmaster o 37 tys. przypadków zidentyfikowanych oszustw.

7) W tym samym dniu Ticketmaster złożył do brytyjskiego organu nadzorczego zawiadomienie o naruszeniu bezpieczeństwa danych osobowych.

8) Kolejnego dnia zidentyfikowano złośliwy kod w witrynie Ticketmaster, który był umieszczony w bocie czatu znajdującego się na wielu stronach w tym na stronie płatności.

9) W wyniku ataku przechwycono następujące dane: imiona i nazwiska, adresy, adresy e-mail, numery kart płatniczych, daty ich wygaśnięcia, numery CVV a także nazwy użytkownika i hasła do kont.

10) Formalnie naruszenie ochrony danych osobowych miało miejsce od 25 maja 2018 r. do 23 czerwca 2018 r. natomiast całkowity czas trwania naruszenia trwał od 10 lutego 2018 r. do 23 czerwca 2018 r.

11) Ticketmaster nie był w stanie przedstawić zestawienia osób, których dotknęło naruszenie danych osobowych. Dlatego przyjmuje się, że naruszeniem zostało dotkniętych 9,4 miliona osób z Europejskiego Obszaru Gospodarczego, z czego 1,5 miliona osób pochodziło z Wielkiej Brytanii.

Przyczyna naruszenia:

Brak wdrożenia odpowiednich środków w celu wyeliminowania ryzyka związanego z niebezpieczeństwem skryptów stron trzecich infekujących chat bot na stronie płatności w witrynie Ticketmaster.

Decyzja Data Protection Authority of Sweden (Datainspektionen):

1) Kara pieniężna w wysokości 1 250 000 £ (1 405 000 EUR).

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) Opracuj i wdróż procedurę zgłaszania naruszeń bezpieczeństwa danych osobowych, które będą uwzględniały kwestie związane ze sprawnym i szybkim stwierdzeniem naruszenia ochrony danych.

7) Nie ignoruj informacji o potencjalnym naruszeniu ochrony danych osobowych otrzymanych od osoby fizycznej lub z innego źródła. Każdy sygnał o ewentualnych nieprawidłowościach powinien być przedmiotem wnikliwej analizy.

8) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak