AKTUALIZACJA

Kary organów nadzorczych w Unii Europejskiej

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Kraj oraz organ nadzorczy

Wielka Brytania

Information Commissioner (ICO)

Data wydania decyzji

30.10.2020 r.

Podmiot kontrolowany

Marriott International Inc.

Wysokość kary

18 400 000 funtów*

*ICO podkreśliło, że ustalając wysokość grzywny wzięło również pod uwagę gospodarczy wpływ pandemii COVID-19 („koronawirusa”).

Rodzaj naruszenia

Naruszenie Art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W listopadzie 2018 roku Marriott zgłosiło do Information Commissioner (ICO) naruszenie dotyczące incydentu cybernetycznego polegającego na ujawnieniu danych osobowych zawartych w około 339 milionach rekordów gości na całym świecie, z czego około 30 milionów dotyczyło mieszkańców 31 krajów Europejskiego Obszaru Gospodarczego (EOG) a 7 milionów związanych było z mieszkańcami Wielkiej Brytanii. Podatność danych rozpoczęła się najprawdopodobniej w 2014 r., kiedy to doszło do naruszenia systemu informatycznego grupy hoteli Starwood. W 2016 r. Marriott nabył Starwood, ale ujawnienie danych o klientach zostało odkryte dopiero w 2018 r.

Kompas FORSAFE

ZALECAMY ZWRÓCENIE UWAGI NA:

1. Stosowanie wieloskładnikowego uwierzytelniania dla kont w systemach, programach, aplikacjach uprawniających do dostępu do danych osobowych.

2. Wdrożenie odpowiedniego bieżącego monitorowania ruchu sieciowego i aktywności użytkowników, w szczególności aktywności na kontach uprzywilejowanych.

3. Weryfikację jakie systemy, usługi i informacje są wykorzystywane przez użytkowników.

4. Monitorowanie baz danych.

5. Kontrolę systemów krytycznych.

6. Wdrożenie systemu zarządzania zdarzeniami i incydentami bezpieczeństwa.

7. Przeanalizowanie systemu zarządzania zdarzeniami i incydentami bezpieczeństwa w aspekcie generowanych alertów.

8. Wdrożenie „białej listy”, tj. oprogramowania, które pozwala tylko niektórym użytkownikom lub adresom IP na dostęp do określonych systemów lub oprogramowania, w zależności od ich określonej roli.

Zaleca się wykorzystywanie „białej listy” na:

a) urządzeniach, do których można uzyskać zdalny dostęp;

b) urządzeniach, które przechowują duże ilości lub wrażliwe kategorie danych osobowych;

c) wszelkich innych systemach, które uważane są za „krytyczne” dla operacji sieciowych;

d) terminalach POS oraz wszelkich innych urządzeniach, które przetwarzają transakcje kartami płatniczymi.

9. Regularne testowanie i ocenianie skuteczności zastosowanych środków bezpieczeństwa.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak