Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Grecja
Hellenic Data Protection Authority (HDPA)

Data wydania decyzji
27 stycznia 2022 r.

Podmiot kontrolowany
Cosmote Mobile Telecommunications S.A.

Wysokość kary
5 850 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5 (1) a), art. 5 (2), art. 13, art. 14, art. 25 (1), art. 26, art. 28, art. 35 (7) RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Cosmote Mobile Telecommunications S.A. (Cosmote) dokonał zgłoszenia do greckiego organu nadzorczego naruszenia ochrony danych osobowych, które polegało na wycieku danych osobowych klientów.

Opis wydarzeń:

1) Administratorom systemu wyświetlił się komunikat o przekroczeniu limitu pojemności dysku do przechowywania danych na serwerze.

2) Po dokonaniu czynności sprawdzających odnaleziono plik o wielkości 30 GB, który zawierał dane dotyczące połączeń abonenckich z okresu od 1.09.2020 r. do 5.09.2020 r. oraz stwierdzono wystąpienie ruchu sieciowego 30 GB danych między serwerem Cosmote a zewnętrznym adresem IP, który należał do dostawcy usług hostingowych z Litwy.

3) Analiza logów ujawniła również włamanie na stronę internetową, która była hostowana na infrastrukturze OTE Group (OTE) oraz instalację złośliwego oprogramowania na serwerze OTE (atak typu Brute Force).

4) Hakerowi udało się uzyskać dostęp administracyjny za pomocą hasła administratora OTE, które było w posiadaniu hakera w przeszłości, po incydencie z wyciekiem haseł do aplikacji społecznościowej LinkedIn.

5) Wykradziony plik z danymi zawierał następujące informacje: numer telefonu osoby dzwoniącej, numer telefonu osoby odbierającej połączenie, współrzędne stacji bazowej, identyfikator IMEI, identyfikator IMSI, znacznik czasu, czas trwania połączenia, informacje o dostawcy, plan taryfowy, wiek, płeć, średni przychód na użytkownika.

6) Ilość osób dotkniętych naruszeniem: ok. 10 milionów.

7) Czas trwania naruszenia: 6 lat.

8) Biorąc pod uwagę powyższe grecki organ nadzorczy dokonał czynności kontrolnych i dopatrzył się następujących naruszeń:

a) naruszenie zasady legalności – Cosmote przetwarzał dane osobowe w tzw. „wzbogaconym" pliku w celu zarządzania usterkami i błędami bez podstawy prawnej,

b) naruszenie zasady minimalizacji – Cosmote przetwarzał zbyt szeroki zakres danych osobowych w celu zarządzania usterkami i błędami,

c) błędnie wykonana ocena skutków dla ochrony danych – Cosmote nie poparł wykonania oceny skutków dla ochrony danych dowodami i nie wykazał zastosowania wszelkich możliwych zagrożeń,

d) naruszenie zasady przejrzystości – Cosmote przekazał klientom informacje o celach i okresach przetwarzania danych osobowych w sposób niejasny, niedokładny i niekompletny,

e) naruszenie zasady przejrzystości – Cosmote nie przekazał klientom informacji o przetwarzaniu ich danych osobowych w tzw. „wzbogaconym" pliku, który był wykorzystywany do celów statystycznych i optymalizacji sieci,

f) naruszenie zasady rozliczalności – Cosmote i OTE nie określili jasnych i przejrzystych odpowiedzialności za kwestie bezpieczeństwa w systemach informatycznych,

g) brak zawartej umowy powierzenia przetwarzania danych osobowych między Cosmote a OTE.

Przyczyna naruszenia:

Cosmote nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu zapewnienia prawidłowego wykonania procesu anonimizacji danych.

Decyzja Hellenic Data Protection Authority (HDPA):

1) Kara pieniężna w wysokości 5 850 000 EUR, w tym:

a) 1 300 000 EUR za błędnie wykonaną ocenę skutków dla ochrony danych,

b) 650 000 EUR za naruszenie zasady przejrzystości opisanej w pkt 7 d) powyżej,

c) 1 300 000 EUR za naruszenie zasady przejrzystości opisanej w pkt 7 e) powyżej,

d) 1 300 000 EUR za brak uwzględnienia ochrony danych w fazie projektowania,

e) 1 300 000 EUR za naruszenie zasady rozliczalności.

Kompas FORSAFE

JAK UNIKNĄĆ ATAKU BRUTE FORCE?

1) Wprowadź politykę regularnej zmiany haseł dostępu.

2) Twórz skomplikowane i silne hasła dostępu.

3) Przechowuj hasła w menadżerze haseł.

4) Stosuj wieloskładnikowe uwierzytelnianie.

5) Twórz nowe i unikalne loginy.

6) Korzystaj z narzędzi szyfrujących i twórz silne klucze dostępu.

7) Ogranicz możliwość nieskończonych prób logowania.

8) Blokuj użytkowników lub konta, które przekroczą określoną przez administratora liczbę nieudanych prób logowania.

9) Kontroluj logi serwera w celu określenia aktywności pochodzącej spoza środowiska, w którym pracujesz.

10) Ogranicz możliwość dostępu do poszczególnych systemów dla określonych grup użytkowników.

11) Korzystaj ze wsparcia zewnętrznych aplikacji, np. narzędzia do ochrony przed malware, program antywirusowy, program do wykonywania kopii zapasowych.

12) Korzystaj ze wsparcia operatora zabezpieczeń witryn internetowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak