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 — **OTE Group**

Wysokość kary — **3 250 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 32 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, które znajdowały się w infrastrukturze informatycznej OTE Group (OTE).

Opis wydarzeń:

1) Administratorzy systemów wykonali analizę logów, która ujawniła włamanie na stronę internetową, która była hostowana na infrastrukturze OTE oraz instalację złośliwego oprogramowania na serwerze OTE (atak typu Brute Force).

2) 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.

3) Grecki organ nadzorczy na podstawie zgromadzonego materiału dowodowego uznał, że OTE nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa współmiernego do ryzyka dla osób, których dane dotyczą.

Przyczyna naruszenia:

OTE nie wdrożył adekwatnych środków technicznych i organizacyjnych.

Decyzja Hellenic Data Protection Authority (HDPA):

1) Kara pieniężna w wysokości 3 250 000 EUR.

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