Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

8 lutego 2024 r.

Podmiot kontrolowany

UniCredit S.p.a.

Wysokość kary

2 800 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) f), art. 32 (1), (2) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W październiku 2018 r. do włoskiego organu nadzorczego wpłynęło zgłoszenie naruszenia ochrony danych osobowych od UniCredit S.p.a. (UniCredit) polegające na ataku cybernetycznym na system bankowości internetowej dla kanału mobilnego.

Opis wydarzeń:

1. W piśmie wskazano, iż naruszenie polegało na masowym użyciu kodów sekwencyjnych w celu identyfikacji istniejących kodów dostępu do systemu bankowości internetowej.

2. W wyniku incydentu uzyskano dane osobowe klientów, takie jak imiona i nazwiska, kody podatkowe oraz wewnętrzne kody identyfikacyjne banku.

3. Naruszenie dotknęło 777 765 obecnych i byłych klientów.

4. Bank odpowiedział na incydent, publikując komunikat prasowy i informując 6859 klientów o zablokowaniu ich haseł po ich identyfikacji przez atakujących.

5. Włoski organ nadzorczy uznał te działania za niewystarczające i zażądał poinformowania wszystkich dotkniętych osób.

6. Po analizie materiału dowodowego stwierdzono, że procedury uwierzytelniania nie były zgodne z przepisami o ochronie danych osobowych, między innymi przez uniemożliwienie stosowania prostych haseł przez użytkowników.

7. UniCredit nie zgodził się z tą oceną, twierdząc, że stosowane środki bezpieczeństwa były standardem w sektorze bankowym i że atak mógłby zostać uniknięty, gdyby audytorzy poinformowali o wykrytej luce pięć dni przed atakiem.

Przyczyna naruszenia:

Atak hackerski doprowadził do pozyskania danych osobowych obecnych i byłych klientów UniCredit.

Decyzja:

1. Kara pieniężna w wysokości 2 800 000 EUR.

Źródło:

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9991020

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

Jak uniknąć ataku typu 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 Kawczyńska