Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Grecja

Hellenic Data Protection Authority (HDPA)

Data wydania decyzji

28 lutego 2024 r.

Podmiot kontrolowany

Hellenic Post Offices

Wysokość kary

2 995 140 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

Grecki organ nadzorczy otrzymał zgłoszenie naruszenia ochrony danych osobowych od Hellenic Post Offices polegające na ataku na systemy informatyczne.

Opis wydarzeń:

1. W wyniku włamania do systemu informatycznego, oprogramowanie Hellenic Post Offices zostało zaszyfrowane, a dane osobowe zostały skradzione i opublikowane w Dark Webie.

2. Naruszenie dotyczyło ok. 4-5 milionów osób, w tym pracowników Hellenic Post Offices.

3. Grecki organ nadzorczy uznał, żeHellenic Post Offices:

a) nie zastosował adekwatnych środków technicznych i organizacyjnych,

b) nie wdrożył odpowiednich polityk ochrony danych osobowych,

c) nie zapewnił poufności, dostępności i niezawodności systemów oraz procedur regularnego testowania i oceny skuteczności zastosowanych środków technicznych i organizacyjnych.

Przyczyna naruszenia:

Hellenic Post Offices padł ofiarą ataku cybernetycznego, ponieważ doszło do uzyskania dostępu do hasła do kont administracyjnych.

Decyzja:

1. Kara pieniężna w wysokości 2 995 140 EUR.

Źródło:

https://www.dpa.gr/sites/default/files/2024-04/10_2024%20anonym_0.pdf

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