Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Wielka Brytania

Information Commissioner (ICO)

Data wydania decyzji

19 październik 2022 r.

Podmiot kontrolowany

Interserve Group Limited

Wysokość kary

5 033 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

Interserve Construction Limited (Interserve) dokonał zgłoszenia do brytyjskiego organu nadzorczego naruszenia ochrony danych osobowych, które polegało na nieautoryzowanym dostępie do systemów informatycznych.

Opis wydarzeń:

1) W związku z otrzymanym zgłoszeniem brytyjski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Interserve.

2) W trakcie czynności kontrolnych brytyjski organ nadzorczy ustalił, iż:

a) naruszenie trwało od 30 marca do 2 maja 2020 r.,

b) naruszenie było wynikiem cyberataku, który polegał na wysłaniu wiadomości e-mail zawierającej phishing, a w rezultacie po rozpakowaniu przez pracownika pliku znajdującego się w wiadomości – instalację szkodliwego oprogramowania na jego stacji roboczej, umożliwiającego dostęp do danych na komputerze,

c) atakujący korzystając z dostępu do komputera pracownika włamał się na serwer, a następnie zhakował 283 systemy i 16 kont (w tym 12 kont uprzywilejowanych) w czterech domenach,

d) ponadto cyberprzestępca odinstalował oprogramowanie antywirusowe, a następnie włamał się do czterech baz danych zawierających dane kadrowe,

e) w wyniku powyższej czynności, uzyskał dostęp do danych osobowych ok. 113 000 byłych i obecnych pracowników oraz zaszyfrował systemy przez co stały się one niedostępne dla Interserve.

3) Na podstawie zebranego materiału dowodowego brytyjski organ nadzorczy dopatrzył się następujących uchybień:

a) wykorzystywanie systemów operacyjnych, które przestały być wspierane przez producenta, a tym samym nie były już aktualizowane pod kątem zabezpieczeń mających na celu naprawienie znanych luk w systemie, które mogą być wykorzystane przez cyberprzestępców,

b) niewłaściwa ochrona punktu końcowego:

• brak najnowszej ochrony antywirusowej,

• wyłączona zapora sieciowa,

• brak wdrożonej listy „zezwól lub odrzuć”,

c) brak cyklicznego wykonywania testów podatności,

d) brak realizacji szkoleń w zakresie ochrony danych osobowych i bezpieczeństwa informacji,

e) stosowanie nieaktualnego protokołu SMB,

f) zespół ds. bezpieczeństwa informacji Interserve nie zbadał wykrytego incydentu uznając, że oprogramowanie antywirusowe usunęło złośliwy skrypt,

g) szerokie uprawnienia dla 280 użytkowników w grupie administratorów domeny.

Przyczyna naruszenia:

Interserve nie dopełnił obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu ochrony odpowiedniego do ryzyka oraz szybkiego przywrócenia dostępności do danych osobowych w przypadku incydentu.

Decyzja:

Kara pieniężna w wysokości 4 400 000 GBP (5 033 000 EUR).

Źródło:

https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2) Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

3) Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak