Ocena wagi naruszenia

naruszenie stwierdzone w dniu… o godz. …  
administrator danych: …

Przyjęta metodyka wg. ENISA (<https://www.enisa.europa.eu/publications/dbn-severity>)

WN – waga naruszenia

KPD – kontekst przetwarzania danych

PI – prawdopodobieństwo identyfikacji

ON – okoliczności naruszenia

CD – czynnik dodatkowy

## **Kontekst przetwarzania danych (KPD)**

Jest to suma czynników A i B, gdzie A określa rodzaj i kategorię danych, natomiast B określa czynniki kontekstu podwyższające bądź obniżające ocenę.

W naszym przypadku A = 3 z uwagi wystąpienie w zestawie danych również informacji z katalogu szczególnych danych osobowych, a charakter danych prowadzi do informacji finansowych.

Nadmienić należy, że niezwłocznie po wykryciu błędu zapobieżono możliwości dalszego trwania naruszenia. Skuteczność tych działań potwierdził podmiot przetwarzający będący autorem systemu, w którym stwierdzono lukę.

B z kolei możemy określić na poziomie 2 z uwagi relatywnie szeroki zakres danych o osobie, ale niewielkie prawdopodobieństwo negatywnych skutków dla podmiotu danych z uwagi na brak informacji o wykorzystaniu luki w oprogramowaniu.

Zatem:

## **Prawdopodobieństwo identyfikacji (PI)**

Należ je określić na poziomie 1 (pełna identyfikacja)

Zatem:

## **Okoliczności naruszenia (ON)**

Jest to suma atrybutów bezpieczeństwa (poufność, integralność, dostępność oraz działanie intencjonalne). W naszym przypadku mamy do czynienia wyłącznie z dostępem jednej (dotychczas zidentyfikowanej) osoby nieuprawnionej oraz działaniem nieintencjonalnym. Czynnikiem ryzyka jest tu jednak nieznana dotychczas skala wykorzystania luki w systemie.

Zatem:

## **Podsumowanie**

Skala wg, ENISA:

|  |  |  |  |
| --- | --- | --- | --- |
| Wynik | Waga naruszenia | Opis | Działanie |
| < 2 | niska | osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności | odnotowanie w rejestrze naruszeń |
| 2 <= 3 | średnia | osoby mogą napotkać niedogodności, które są możliwe do pokonania | odnotowanie w rejestrze naruszeń oraz notyfikacja UODO |
| 3 <= 4 | wysoka | konsekwencje z poważnym skutkiem, ale możliwe do pokonania | odnotowanie w rejestrze naruszeń oraz notyfikacja UODO |
| 4 <= | bardzo wysoka | znaczące, być może nieodwracalne skutki | odnotowanie w rejestrze naruszeń oraz notyfikacja UODO jak również powiadomienie podmiotów danych |

Zgodnie z klasyfikacją ENISA, określona powyżej waga naruszenia skutkuje koniecznością ujęcia naruszenia w rejestrze incydentów bez notyfikacji Urzędu Ochrony Danych Osobowych oraz obowiązku powiadomienia podmiotu danych.

Warszawa, …

Krzysztof Jankowski