UODO: Kara pieniężna dla burmistrza za dobór nieskutecznych zabezpieczeń

Kategoria: Aktualności
Opublikowano: czwartek, 06, lipiec 2023 17:38
Alicja Cisowska

Prezes UODO nałożył administracyjną karę pieniężną w wysokości 30 tys. zł na jednego z burmistrzów za dobór nieskutecznych zabezpieczeń dla wykorzystywanego systemu informatycznego oraz za ich nieprzetestowanie.

Do organu nadzorczego wpłynęło zgłoszenie naruszenia ochrony danych osobowych spowodowane atakiem ransomware na skutek wykorzystania podatności istniejącej w systemie teleinformatycznym.

Podczas postępowania i po dokonaniu analizy materiału dowodowego UODO uznał, że faktyczną przyczyną wystąpienia ataku ransomware była niezaktualizowana baza wirusów. Co więcej, administrator przeprowadził w sposób nierzetelny analizę ryzyka (szczególnie w zakresie wykonywania kopii zapasowych), a także wdrożył niepełne środki techniczne i organizacyjne, które miały gwarantować bezpieczeństwo w procesie przetwarzania danych osobowych.

Efektem tego było przełamanie zabezpieczeń wykorzystywanego przez administratora systemu informatycznego, a następnie zaszyfrowanie przetwarzanych w nim danych z użyciem złośliwego oprogramowania.

Odpowiednie zabezpieczenia techniczne

Jednym z istotnych elementów, które mają wpływ na bezpieczeństwo danych osobowych jest zapewnienie, aby wykorzystywane do przetwarzania danych oprogramowanie posiadało najnowszą wersję udostępnioną przez jego producenta. Takie oprogramowanie posiadają wszystkie wydane przez producenta aktualizacje, w tym te dotyczące zabezpieczeń i poprawek działania oprogramowania.

W trakcie postępowania ustalono, że system operacyjny, zainstalowany przez administratora na serwerze, w czasie wystąpienia naruszenia ochrony danych osobowych, nie miał wsparcia producenta.

W ocenie UODO, korzystanie z systemów informatycznych służących do przetwarzania danych osobowych po zakończeniu wsparcia technicznego przez ich producenta, w sposób istotny obniża ich poziom bezpieczeństwa.

Administrator przed wystąpieniem naruszenia ochrony danych osobowych zidentyfikował ryzyko związane z wykorzystywaniem przestarzałego oprogramowania, jednak go nie aktualizował, a więc sam nie zastosował się do procedur, których był autorem.

Kopie zapasowe

Prowadzone postępowanie wskazało, że dane osobowe przetwarzane przez administratora zostały zaszyfrowane, w wyniku czego nastąpiła utrata dostępności do baz danych administratora.

Obowiązujące u administratora zasady tworzenia kopii zapasowych oraz praktyka wykonywania tej kopii nie zapewniały jednak dostępności systemów i usług przetwarzania oraz do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w przypadku zaistniałego naruszenia. Jak ustalono, serwer, na którym miała być wykonana dodatkowa kopia danych uległ awarii, co uniemożliwiło szybkie odtworzenie znajdujących się na nim danych. Administrator odzyskał dane dopiero po prawie trzech miesiącach.

Kategoria: Aktualności
Opublikowano: czwartek, 06, lipiec 2023 17:38
Alicja Cisowska
Odsłony: 1143

Regularne testowanie

Przyjęte przez administratora środki techniczne mające służyć właściwej ochronie danych osobowych w żaden sposób nie były przez burmistrza testowane, mierzone i oceniane celem weryfikacji ich skuteczności. W trakcie prowadzonego postępowania administrator nie był w stanie wykazać, że zastosowane rozwiązania są wystarczające dla zapewnienia bezpieczeństwa przetwarzanych danych. Ponadto administrator nie przedstawił dowodu, że po wystąpieniu naruszenia ochrony danych osobowych dokonuje regularnego testowania.

Po raz kolejny należy przypomnieć, że testowanie, mierzenie i ocenianie zastosowanych zabezpieczeń, musi być dokonywane w sposób regularny, nie może mieć charakteru jednorazowego.

Pełna treść decyzji: www.uodo.gov.pl

Źródło: UODO