Naruszenia ochrony danych osobowych spowodowane atakiem Ransomware

Prezesa Urzędu ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych osobowych spowodowane atakiem ransomware na skutek wykorzystania podatności istniejącej w systemie teleinformatycznym.

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 w **drożył niepełne środki techniczne i organizacyjne,** które miały gwarantować bezpieczeństwo w procesie przetwarzania danych osobowych.
Podmiot 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.
Serwer, na którym miała być wykonana kopia danych uległ awarii, co uniemożliwiło szybkie odtworzenie znajdujących się na nim danych. Administrator odzyskał dane dopiero po prawie trzech miesiącach.
W trakcie prowadzonego postępowania podmiot nie był w stanie wykazać, że zastosowane rozwiązania są wystarczające dla zapewnienia bezpieczeństwa przetwarzanych danych. Ponadto nie przedstawił dowodu, że po wystąpieniu naruszenia ochrony danych osobowych dokonuje regularnego testowania.

Jakie wnioski zatem należy wyciągnąć, aby przeciwdziałać?

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 posiada wszystkie wydane przez producenta aktualizacje, w tym te dotyczące zabezpieczeń i poprawek działania oprogramowania m.in. systemy operacyjne.
Korzystanie z systemów informatycznych po zakończeniu wsparcia technicznego przez ich producenta, w sposób istotny obniża ich poziom bezpieczeństwa.

Kopie zapasowe
Obowiązujące u administratora zasady tworzenia kopii zapasowych oraz praktyka wykonywania tej kopii muszą zapewniać dostępności systemów i usług przetwarzania oraz szybkie przywrócenie dostępności danych osobowych i dostępu do nich w przypadku zaistniałego naruszenia.

Regularne testowanie
Przyjęte przez administratora środki techniczne mające służyć właściwej ochronie danych osobowych powinny być testowane, mierzone i oceniane celem weryfikacji ich skuteczności.

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:
https://www.uodo.gov.pl/decyzje/DKN.5131.56.2022