Checklista 72h — wyciek u vendora EDM / procesora

Dla administratora danych (placówka / praktyka). Wolno kopiować do memo; przy publikacji podaj źródło.

Rama: problem zaczyna się od zależności od vendora, nie od samego ataku.

Kanonicznie: https://bezpiecznyblog.pl/checklista-72h-vendor-edm/
Case: https://bezpiecznyblog.pl/odpowiedzialnosc-vendora-edm/

0–4 h

[ ] Potwierdź, czy korzystacie z danego dostawcy i w jakim module (EDM / terminarz / inne)

[ ] Wyznacz ownera incydentu (IOD + IT/security + zarządzanie)

[ ] Zamroź spekulacyjną komunikację zewnętrzną („nie wiemy jeszcze zakresu”)

4–24 h

[ ] Pismo / ticket do procesora: zakres tenantów, kategorie danych, timeline, IOCs, rekomendacje

[ ] Poproś o listę: czy Wasze ID klienta / baza jest w zakresie (tak / nie / nieustalone)

[ ] Zabezpiecz logi własne (dostępy, integracje, eksporty)

24–72 h

[ ] Udokumentuj ocenę ryzyka (dla Waszych osób / danych)

[ ] Decyzja: zgłoszenie do UODO — tak / nie / wstępne + uzasadnienie

[ ] Decyzja: zawiadomienie pacjentów — tak / nie / po doprecyzowaniu zakresu

[ ] Przygotuj komunikat antyphishing (recepty, wizyty, „dopłaty”, kody BLIK)

[ ] Sprawdź polisę cyber / obowiązki zgłoszenia do ubezpieczyciela

Równolegle (umowa i odporność)

[ ] Umowa powierzenia: prawo audytu, SLA powiadomień, podprocesorzy, exit/eksport

[ ] Lista innych vendorów z danymi wrażliwymi (top 10) — ten sam scenariusz „co jeśli jutro?”

5 pytań do vendora (wklej)

1. Jaki jest potwierdzony zakres per nasz tenant?
2. Jakie kategorie danych mogły zostać ujawnione?
3. Od kiedy wiecie / od kiedy informujecie administratorów?
4. Jakie działania containment już wykonano?
5. Kiedy dostaniemy materiał do oceny ryzyka i zawiadomień?

Stan PDF: 2026-08-21 · Bezpieczny Blog / hub odpowiedzialności · bez pitchu usług