

Cyberincydent w administracji szkoły

Zasada: Ogranicz skutki, powiadom uprawnione osoby i administratora IT, chroń dane oraz zachowaj możliwość odtworzenia działania.

Reakcja ochronna — pierwsze działania

- Niezwłocznie zgłoś incydent upoważnionemu administratorowi IT i osobie odpowiedzialnej za bezpieczeństwo danych.
- W razie podejrzenia ataku unikaj dalszego korzystania z podejrzanego konta / wiadomości; działania techniczne, w tym izolowanie urządzeń, wykonuje uprawniony specjalista zgodnie z procedurą.
- Nie usuwaj pochopnie komunikatów, logów ani wiadomości mogących pomóc ustalić zakres incydentu; postępuj według instrukcji administratora.

Dobre praktyki

- Stosuj uwierzytelnianie wieloskładnikowe i odrębne uprawnienia tam, gdzie to możliwe.
- Ustal odpowiedzialność za kopie i testy odtwarzania.
- Ćwicz na fikcyjnych wiadomościach phishingowych.

Czego nie robić

- Nie przekazuj podejrzanego załącznika całemu gronu pedagogicznemu „do ostrzeżenia”.
- Nie podejmuj ryzykownych zmian technicznych bez administratora.
- Nie wpisuj do DSS haseł, adresów kont i danych naruszenia.

Checklista gotowości przed zdarzeniem

1. ☐ Znany jest kontakt do administratora IT i jego zastępcy.
2. ☐ Stosowane są bezpieczne metody dostępu.
3. ☐ Sprawdzono dostępność kopii i proces odtwarzania.
4. ☐ Istnieją zasady zgłaszania naruszeń i komunikacji.
5. ☐ Przeprowadzono ćwiczenie phishingowe bez prawdziwych danych uczniów.

Ćwiczenie dla personelu

Przykład fikcyjnego e-maila o pilnym przelewie i błędnym linku: wskaż sygnały ostrzegawcze, komu zgłosić, które procesy kontynuować offline.

UWAGA: W bezpośrednim zagrożeniu życia lub zdrowia 112. Stosuj własne zatwierdzone procedury i polecenia służb. Nie zapisuj w DSS danych dzieci, poufnych incydentów ani wrażliwych informacji o ochronie placówki.