

Cyberincydent w administracji szkoły

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

Granice narzędzia: materiał informacyjno-organizacyjny oparty na publicznych źródłach. Nie zastępuje zatwierdzonych planów danej placówki, opinii specjalistów ani poleceń służb. W bezpośrednim zagrożeniu życia lub zdrowia zadzwoń pod 112. Nie umieszczaj w publicznej aplikacji danych osobowych dzieci, opisów poufnych incydentów, planów zabezpieczeń ani haseł.

SYGNAŁ URUCHAMIAJĄCY

Kiedy użyć tej karty?

Nieoczekiwane blokady plików, fałszywe logowanie do konta, podejrzany załącznik, utrata dostępu do dziennika.

Warunek pilności: bezpośrednie zagrożenie życia lub zdrowia wymaga niezwłocznego wezwania właściwych służb. Nie odwołaj go do końca oceny formularza.

FAZA I

Pierwsze działania: ochrona życia i decyzje

- 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.

- Zidentyfikuj usługi krytyczne: kontakt z rodzicami, organizacja opieki, obsługa dokumentacji i ciągłość dydaktyki.

FAZA II

Pierwsza godzina: koordynacja i informacja

- Ustal, jakie usługi są dotknięte, które procesy trzeba uruchomić alternatywnie i kto odpowiada za komunikat.
- Rozważ wraz z administratorem danych i IOD, czy powstają obowiązki dotyczące naruszeń ochrony danych; ich ocena wymaga odrębnej analizy.
- Ustal kanały zgłoszenia incydentu do właściwych zespołów, np. CERT Polska, zgodnie z charakterem zdarzenia.

FAZA III

Po zdarzeniu: wsparcie, weryfikacja i poprawa

- Sprawdź, czy wykorzystano właściwe kopie i czy przywrócone usługi są rzeczywiście bezpieczne; nie zakładaj tego na podstawie samego uruchomienia systemu.
- Zidentyfikuj potrzebne szkolenia personelu z phishingu i haseł.
- Nie udostępniaj w publicznym raporcie szczegółów konfiguracji sieci ani danych podmiotów.

PRAKTYKA / PUŁAPKI

Co robić, a czego bezwzględnie unikać

Sprawdzone działania

- 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 dyrektora: pięć warunków

Odznacz jedynie po faktycznym sprawdzeniu w placówce. Zapis nie jest audytem, certyfikacją ani potwierdzeniem gotowości.

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

0 z 5 warunków przygotowania sprawdzonych lokalnie. To nie jest potwierdzenie bezpieczeństwa.

Zadanie dla zespołu kierownictwa

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

Minimalny rezultat: Lista krytycznych procesów cyfrowych, macierz kontaktów IT, procedura pierwszego zgłoszenia.

Ocena jakości: ustalono fakty, decyzję ochronną, odpowiedzialną rolę, granicę eskalacji, sposób weryfikacji i plan korekty. Nie zaliczaj tylko na podstawie testu.

Praktyczne wzory do adaptacji

Karta decyzji kierownictwa

Cel: udokumentować, czy występuje bezpośrednie zagrożenie, kto podejmuje decyzję i na jakiej podstawie.

Pola / elementy: Data i czas (do wpisania poza aplikacją), kategoria zdarzenia, potwierdzone fakty, brakujące dane, pilność, odpowiedzialna rola, decyzja ochronna, źródło decyzji, termin przeglądu i sposób weryfikacji wykonania.

Matryca ról i zastępstw

Cel: zapobiec sytuacji, w której nieobecność jednej osoby blokuje reagowanie.

Pola / elementy: Dla funkcji alarmowanie, kontakt ze służbami, opieka nad grupą, komunikat, dokumentacja i wsparcie psychologiczne wpisz rolę wiodącą, zastępcę, bezpieczny kanał alternatywny i sposób potwierdzenia.

Komunikat do rodziców

Cel: krótka, sprawdzalna informacja bez danych osobowych uczniów.

Pola / elementy: „Potwierdziliśmy [wyłącznie fakt]. Placówka [działanie zgodne z instrukcjami]. Prosimy o [jedno zalecenie]. Następny komunikat [kanał i termin].” Nie wypełniaj danymi dzieci w aplikacji.

Rejestr działań naprawczych

Cel: rozróżnić oznaczenie zadania jako „wykonane” od faktycznej skuteczności.

Pola / elementy: Anonimowy numer kryterium, luka, rezultat oczekiwany, rola odpowiedzialna, termin uzasadniony pilnością, dowód wdrożenia w systemie placówki, weryfikator, data kontroli i status ponowny.

Wzory to opisy elementów dokumentacji roboczej. Podpisane dokumenty, dane incydentu i wszystkie informacje poufne należy przechowywać wyłącznie w zatwierdzonych systemach placówki.

Oficjalne źródła i metodyka

- Ministerstwo Cyfryzacji / NASK — zgłaszaj dowody cyberprzemocy ↗
- UK DfE — Emergency Planning and Response for Education Settings ↗
- US Department of Education — Guide for Developing High-Quality School EOPs ↗

Aktualizacja redakcyjna: 12.10.2026. Źródła amerykańskie i brytyjskie mają charakter porównawczy; nie stanowią polskiego prawa. Nie przeprowadzono w ramach tej wersji niezależnego audytu przez służby ani szkolenia kontrterrorystycznego.