ITSAILOR, RUNBOOK

Pierwsza godzina incydentu w Microsoft 365

Pierwsza godzina incydentu w Microsoft 365: kto co powstrzymuje, co zabezpieczyć, jakie zegary biegną

Wersja 2026-11 · 26.10.2026 · Stan prawny: ustawa o KSC, Dz. U. 2026 poz. 20 ze zm. (poz. 252, 815, 1003, 1206), odczyt 25.10.2026

ITSailor · Michal Jatczak, przedsiębiorca zarejestrowany na Malcie, działający pod nazwą handlową ITSailor

---

Wersja: 2026-11 (szablon i dokument publiczny) Stan prawny: ustawa o KSC, Dz. U. 2026 poz. 20 ze zm. (poz. 252, 815, 1003, 1206), odczyt 25.10.2026 Autor: Michal Jatczak, przedsiębiorca zarejestrowany na Malcie, działający pod nazwą handlową ITSailor

Do czego służy ten runbook

Do pierwszych sześćdziesięciu minut po tym, jak ktoś zauważy przejętą skrzynkę, podejrzane logowanie administratora albo masową wysyłkę z Państwa domeny. Mówi, kto co powstrzymuje w Entra ID i Exchange Online, jakie zapisy zabezpieczyć, zanim znikną, i jakie zegary zaczynają biec. Nie zastępuje Państwa procedury zarządzania incydentami (art. 8 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa), tylko wypełnia jej techniczną część w Microsoft 365. Decyzję, czy zdarzenie jest incydentem poważnym, i samo zgłoszenie podejmuje Państwa organizacja. Nie pełnię dyżuru i nie prowadzę SOC.

Wypełnić przed pierwszym użyciem:

Rola	Kto (imię, nazwisko, telefon)	Zastępca
Osoba decydująca o kwalifikacji i zgłoszeniu	[…]	[…]
Administrator z rolą Security Administrator i Exchange Administrator	[…]	[…]
Osoba odpowiedzialna za ochronę danych (IOD)	[…]	[…]
Osoba kontaktowa z art. 9 ustawy	[…]	[…]

Minuta 0 do 10: potwierdzić i ogłosić

1. Zapisać czas wykrycia (data, godzina, strefa czasowa) i źródło: alert Defender, zgłoszenie użytkownika, informacja z zewnątrz. Od tej chwili liczy się 24 godziny na wczesne ostrzeżenie (art. 11 ust. 1 pkt 4).
2. Powiadomić osobę decydującą i administratora. Jedna osoba prowadzi incydent i prowadzi notatkę z czasami; druga wykonuje działania techniczne.

3. Określić zasięg wstępny: jedno konto, kilka kont, konto administratora, urządzenie. Konto administratora albo masowa wysyłka to od razu wariant z izolacją.

Minuta 10 do 30: powstrzymać

W Entra ID, dla każdego podejrzanego konta:

1. Zablokować logowanie (nie usuwać konta: usunięcie niszczy dowody).
2. Unieważnić sesje i tokeny odświeżania, żeby wydane już tokeny przestały działać.
3. Zresetować hasło i wymusić ponowną rejestrację metod MFA; usunąć metody, których nikt nie rozpoznaje (napastnik mógł dopisać własny numer albo aplikację).
4. Sprawdzić i cofnąć zgody na aplikacje udzielone przez to konto w ostatnich dniach.

W Exchange Online:

1. Usunąć reguły skrzynki odbiorczej, które przekazują, usuwają albo ukrywają pocztę, i wyłączyć przekazywanie na zewnątrz.
2. Jeśli konto wysyłało phishing dalej: odszukać wiadomości w Threat Explorer (Defender for Office 365 P2) albo w śledzeniu wiadomości, usunąć je ze skrzynek odbiorców (ZAP), zablokować nadawcę i adres URL.

Na urządzeniu:

1. Jeśli zdarzenie dotyczy urządzenia: izolować je w Microsoft Defender (Defender for Business albo Defender for Endpoint), nie wyłączać zasilania.

Jeśli zablokowano dostęp administracyjny albo polityka Conditional Access zamknęła wszystkich: użyć konta awaryjnego według RUNBOOK-02 i zapisać to jako osobne zdarzenie.

Minuta 30 do 60: zabezpieczyć zapisy

Zapisy z art. 10 ust. 4 ustawy (automatycznie generowane zapisy w dziennikach) znikają po okresie retencji; Audit Standard przechowuje 180 dni, Audit Premium rok. Zabezpieczyć teraz:

1. Eksport ujednoliconego dziennika audytu z Microsoft Purview dla kont objętych incydentem, za ostatnie 30 dni (operacje na skrzynce, plikach, zgodach, rolach).
2. Eksport dziennika logowań Entra ID dla tych kont (adresy IP, lokalizacje, metody, aplikacje).
3. Zrzut incydentu z Microsoft Defender XDR, jeśli istnieje, i listę urządzeń.
4. Kopię usuniętych reguł skrzynki i wiadomości (metadane: nadawca, temat, odbiorcy, czas).
5. Notatkę z czasami wszystkich działań z minut 0 do 60.

Eksporty trafiają do `[LOKALIZACJA DOWODÓW]` z kontrolą dostępu; nie wysyła się ich pocztą i nie wkleja do czatu.

Zegary, które biegną

Co	Termin	Podstawa	Kto
wczesne ostrzeżenie o incydencie poważnym do właściwego CSIRT	do 24 godzin od wykrycia	art. 11 ust. 1 pkt 4 ustawy o KSC	osoba decydująca
zgłoszenie incydentu poważnego	do 72 godzin od wykrycia	art. 11 ust. 1 pkt 4a	osoba decydująca
raport końcowy	do miesiąca od zgłoszenia	art. 11 ust. 1 pkt 4c	osoba decydująca
zgłoszenie naruszenia ochrony danych osobowych do Prezesa UODO, jeśli naruszenie dotyczy danych osobowych i rodzi ryzyko dla osób	do 72 godzin od stwierdzenia naruszenia	art. 33 RODO	IOD i administrator danych
zawiadomienie osób, których dane dotyczą, przy wysokim ryzyku	bez zbędnej zwłoki	art. 34 RODO	IOD i administrator danych

Zgłoszenia z ustawy o KSC składa się przez system S46 do CSIRT sektorowego; do czasu ogłoszenia jego gotowości operacyjnej do CSIRT NASK, CSIRT GOV albo CSIRT MON (art. 44 ustawy zmieniającej). Progi incydentu poważnego określa rozporządzenie; dotychczasowe rozporządzenie wygasa najpóźniej 3.04.2027 (art. 32 ustawy zmieniającej), więc proszę sprawdzić w `[PROCEDURA KLIENTA]`, które progi obowiązują w dniu incydentu. Zgłoszenia innych zdarzeń przyjmuje incydent.cert.pl.

Czego nie robić

- Nie usuwać kont, skrzynek ani wiadomości bez kopii: to dowody.
- Nie informować napastnika (odpowiedź na jego wiadomość, pytanie w skrzynce, którą kontroluje).
- Nie rozsyłać do całej firmy wiadomości z treścią phishingu; wystarczy krótka informacja, że trwa obsługa zdarzenia i jak zgłaszać podobne wiadomości.
- Nie wklejać eksportów ani zrzutów do narzędzi AI ani do publicznych komunikatorów.

Po pierwszej godzinie

- Przejęte konto: RUNBOOK-01 (badanie i odzyskanie).
- Phishing: RUNBOOK-07 (czyszczenie i zaostrzenie polityk).
- Użyte konto awaryjne: RUNBOOK-02 (rotacja).
- Po zamknięciu: wpis do dziennika zmian i weryfikacji, aktualizacja wyjątków i zaległości, przegląd, czy incydent wskazuje na lukę w Conditional Access albo w retencji dzienników.

Zapis dowodu

Notatka z czasami, eksporty z punktu „Zabezpieczyć zapisy", lista działań i osób. Zapis wspiera dokumentację z art. 10 ust. 4 i, jeśli doszło do naruszenia ochrony danych, rejestr naruszeń z art. 33 ust. 5 RODO.

Ćwiczenie tego runbooka na własnych ustawieniach tenanta, z jednym scenariuszem i zapisem wyniku, to zakres „Gotowość na incydent" na itsailor.io/pl. Oferta wyłącznie dla firm. Usług opisanych na tej stronie nie świadczę konsumentom.