REAGOWANIE NA INCYDENTY · IR / DFIR

Raport z reakcji na incydent — fałszywa faktura (BEC)

Podmiot: **„Nordwind Logistyka" Sp. z o.o.** (fikcyjny) Klasa: **BEC / invoice fraud**

Czas reakcji: **< 1 h od zgłoszenia** Autor: **Bartek Binder — FatDot**

STRESZCZENIE DLA ZARZĄDU

Do księgowości wpłynął e-mail podszywający się pod stałego dostawcę, z prośbą o zmianę numeru rachunku przed płatnością faktury. Wątpliwość pracownika i zgłoszenie na retainer pozwoliły **wstrzymać przelew przed realizacją** – **brak strat finansowych**. W toku analizy wykryto podszywającą domenę (typosquat) oraz **jedno podejrzane logowanie** do skrzynki księgowości z utworzoną regułą przekierowania (usunięta). Ekspozycja ograniczona do treści korespondencji; **brak dowodów wycieku danych klientów**. Zamknięcie: reset i MFA, blokada domeny, powiadomienie prawdziwego dostawcy, wdrożenie procedury weryfikacji zmian rachunku.

Straty: **0 zł** | Kompromitacja: **1 skrzynka (ograniczona)** | Wyciek danych: **brak dowodów** | Status: **zamknięty**

1 · PRZEBIEG (TIMELINE)

Dz. 0 · 09:14
E-mail „zmiana rachunku" od rzekomego dostawcy. Domena podszywająca (litera zamieniona w nazwie).

Dz. 0 · 11:40
Księgowość przygotowuje przelew; pracownik zgłasza wątpliwość co do nowego numeru konta.

Dz. 0 · 12:05
Zgłoszenie na retainer. **Płatność wstrzymana.** Rozpoczęcie analizy.

Dz. 0 · 13:00
Analiza nagłówków: podszycie + domena look-alike. Wykryto podejrzane logowanie do skrzynki księgowości z nietypowego IP oraz regułę auto-forward.

Dz. 0 · 14:30
Wymuszony reset haseł, wylogowanie sesji, włączenie MFA, usunięcie reguły przekierowania.

Dz. 1
Potwierdzenie: brak wykonanego przelewu, brak dowodów eksfiltracji danych. Domknięcie i rekomendacje.

2 · USTALENIA

WEKTOR	BEC / oszustwo „na fakturę". Domena podszywająca (typosquat) + wcześniejsze rozpoznanie struktury firmy (dane publiczne).

POCZTA	Jedno podejrzane logowanie do skrzynki księgowości; utworzona reguła auto-forward (usunięta). Ograniczona kompromitacja jednej skrzynki.
STRATY	Brak – płatność wstrzymana przed realizacją.
DANE	Możliwa ekspozycja treści wątku e-mail; brak dowodów wycieku danych osobowych klientów.

3 · ZGŁASZANIE INCYDENTU – OBOWIĄZEK, SLA I DECYZJA

Ocena wykonana zgodnie z wdrożoną procedurą zgłaszania incydentów (terminy i kanał poniżej).

≤ 24 H	Wczesne ostrzeżenie do CSIRT – od wykrycia poważnego incydentu.
≤ 72 H	Zgłoszenie incydentu – ocena wstępna (dotkliwość, wpływ, wskaźniki kompromitacji).
≤ 1 MIES.	Raport końcowy; raporty pośrednie co 30 dni dla incydentów trwających.
KANAŁ	CSIRT NASK – `incydent.cert.pl` lub S46. Plus: informowanie odbiorców usług, których incydent może dotyczyć.

> Zgodnie z procedurą incydent oceniono pod kątem definicji „poważnego" (NIS2/KSC): brak istotnego zakłócenia usługi i brak strat – **poniżej progu zgłoszenia obowiązkowego**. Decyzję i jej podstawę zapisano w rejestrze incydentów (wymóg dowodowy). RODO: brak potwierdzonego naruszenia danych osobowych – udokumentowano analizę. Gdyby incydent przekroczył próg, procedura uruchamia wczesne ostrzeżenie w 24 h przez CSIRT NASK. **Dokumentacja gotowa do przedstawienia organowi na żądanie.**

4 · DZIAŁANIA NATYCHMIASTOWE (24-72 H)

- Reset haseł i wymuszenie MFA na skrzynce księgowości (oraz przegląd pozostałych).
- Usunięcie reguły auto-forward; przegląd reguł we wszystkich skrzynkach.
- Blokada domeny podszywającej; powiadomienie prawdziwego dostawcy.
- Komunikat do zespołu księgowości + wstrzymanie płatności do weryfikacji.

5 · REKOMENDACJE TRWAŁE

- Poczta: SPF / DKIM / DMARC (polityka `reject`) – utrudnia podszycie.
- MFA na wszystkich skrzynkach; alerty logowań z nietypowych lokalizacji.
- Procedura weryfikacji zmiany numeru rachunku (potwierdzenie drugim kanałem – telefon do znanego kontaktu).
- Szkolenie anty-BEC dla księgowości; monitoring tworzenia reguł auto-forward.

NASTĘPNY KROK

Gotowość na kolejny raz

Retainer gotowości: wdrożenie rekomendacji, hardening poczty i stały numer alarmowy — reakcja w godzinach, nie dniach, gdy przyjdzie następny incydent. Zakres i cena ustalone przed startem.

Dokument poglądowy. Podmiot, dane i przebieg zdarzeń są fikcyjne i służą wyłącznie prezentacji formatu i zakresu opracowania. Rzeczywisty raport jest zawsze indywidualny.