INCIDENT-PLAYBOOK PHI-04

CEO-Fraud oder Rechnungsbetrug

Phishing & Social Engineering

Eine Zahlung soll ausgelöst oder eine Bankverbindung geändert werden. Die Anweisung kommt scheinbar von der Geschäftsführung oder von einem bekannten Lieferanten, wirkt dringend und bittet um Vertraulichkeit oder darum, den üblichen Weg abzukürzen.

- Geschäftsführung bittet um eine eilige Überweisung
- Lieferant meldet eine neue Kontonummer
- Rechnung mit geänderter IBAN bei bekanntem Betrag
- Bitte um Gutscheinkauf oder Barauslage

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Zahlung anhalten. Nichts freigeben und nichts vorbereiten, solange die Anweisung nicht über einen zweiten Weg bestätigt ist.

02 Bei bekannter Rufnummer aus dem eigenen Verzeichnis rückfragen, nie über Kontaktdaten aus der Nachricht oder der Rechnung.

03 Ist die Überweisung schon draußen: sofort die Bank anrufen und den Rückruf der Zahlung verlangen. Das ist zeitkritisch.

04 Geschäftsführung und Buchhaltung unmittelbar informieren, auch wenn der Betrug nur vermutet wird.

05 Nachricht, Rechnung und Kontodaten unverändert sichern, inklusive vollständigem Absender.

Melden

SOFORT

WEN

Geschäftsführung und Buchhaltung sofort, parallel die IT-Verantwortlichen. Bei erfolgter Zahlung zusätzlich die Hausbank.

WIE

Telefonisch, nicht per Mail. Läuft der Betrug über ein übernommenes Postfach, lesen die Täter mit.

WAS BEREITHALTEN

- Betrag, Empfängerbank und IBAN der verlangten Zahlung
- Über welchen Kanal die Anweisung kam
- Ob die Zahlung bereits freigegeben oder ausgeführt wurde
- Wer im Haus sonst noch kontaktiert wurde
- Welche Frist oder Begründung genannt wurde

Nicht tun

HÄUFIGE FEHLER

- × Auf die Bitte um Vertraulichkeit eingehen. Sie dient allein dazu, die Vier-Augen-Kontrolle auszuhebeln.
- × Über den Kanal der Anweisung rückfragen, auch nicht auf eine mitgeschickte Telefonnummer.
- × Die geänderte Bankverbindung im Lieferantenstamm speichern, bevor sie telefonisch bestätigt ist.
- × Aus Zeitdruck teilweise zahlen oder eine Anzahlung leisten.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Geschäftsführung entscheidet über Anzeige bei der Polizei und die Einbindung der Versicherung. Beides ist zeitkritisch.
- → Die IT prüft, ob ein Postfach im Haus oder beim Lieferanten übernommen wurde und seit wann mitgelesen wird.
- → Der Freigabeprozess für Zahlungen und Stammdatenänderungen wird überprüft und wo nötig nachgeschärft.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Lieferant wurde gehackt (SUP-01) · Interne Kontakte siehe Incident-Kontaktblatt