CNEXT SECURITY SERVICES · SPURENBERICHT · EINMALIG

Spurenbericht Breach Inspection

KUNDE
Muster AG, Bern (erfunden)

FALL
BI-2026-017, Verdacht auf Kontoübernahme in der Buchhaltung

AUSLÖSER
Kundenmeldung vom Montag, 2. November 2026, 08:10

EINSTUFUNG
Kritisch, bestätigt durch CNEXT

11	4	2	30 d
Stellen geprüft	Funde mit Beweis	Konten betroffen	Protokolle zurück

Wann Sie dieses Dokument erhalten: Am Ende des ersten Prüftags, per Mail an die Personen im Alarmplan.

Zusammenfassung

Das Konto der Buchhaltung wurde am Freitag, 30. Oktober 2026, um 14:52 aus Lagos mit einem gültigen Token angemeldet, das am Vortag über eine gefälschte Anmeldeseite abgegriffen wurde. Der Angreifer legte eine Posteingangsregel an, registrierte eine Authenticator-App auf einem unbekannten Gerät und schickte am Freitagabend eine Zahlungsaufforderung an drei Kunden. Ein zweites Konto zeigt dieselbe Anmeldeseite, aber keine weitere Spur. Massendownloads oder Freigaben in SharePoint fanden wir nicht.

Funde

STELLE	FUND	BEWEIS	STUFE
Anmeldungen	Anmeldung aus Lagos mit gültigem Token, Gerät unbekannt, Mehrfaktor-Prüfung übersprungen (Token wiederverwendet)	Anmeldeprotokoll, Export 01	**Kritisch**
Postfach	Posteingangsregel «.», verschiebt Antworten mit «Rechnung» in RSS-Feeds und markiert sie gelesen	Regel-Export 02	**Kritisch**
Anmeldemethoden	Authenticator-App auf Android-Gerät registriert, Freitag 14:58	Überwachungsprotokoll, Export 03	**Hoch**
Versand	Zahlungsaufforderung mit neuer Bankverbindung an drei Kunden, Freitag 17:20	Versandprotokoll, Export 04	**Hoch**
Apps und Rollen	Keine neue Einwilligung, keine Rollenänderung, keine Änderung an bedingtem Zugriff	Exporte 05 bis 08	**Niedrig**
Dateien	Keine Massendownloads, keine neuen Freigabelinks in SharePoint und OneDrive	Export 09	**Niedrig**

Zeitlinie

- Do 29.10., 16:41: Mitarbeiterin öffnet den Link einer Mail «Rechnung freigeben» und meldet sich auf einer gefälschten Seite an; Token wird abgegriffen.
- Fr 30.10., 14:52: Anmeldung aus Lagos mit dem Token; 14:55 Posteingangsregel; 14:58 Authenticator-App; 17:20 Zahlungsaufforderung an drei Kunden.
- Mo 2.11., 08:10: Kunde meldet die Mail; 09:30 Inspektion beginnt; 10:15 Protokolle exportiert; 10:20 Sitzungen widerrufen.

So geht es weiter

Die Sofortmassnahmen aus dem Protokoll sind umgesetzt. Bitte informieren Sie die drei Kunden heute mit der Vorlage im Beweisordner; der Übergabebericht folgt am Mittwoch.

Alle Namen, Systeme und Zahlen in diesem Dokument sind erfunden. Ihr Bericht enthält Ihre Umgebung am Tag der Prüfung.