CNEXT SECURITY SERVICES · ÜBERGABEBERICHT · EINMALIG

Übergabebericht

KUNDE
Muster AG, Bern (erfunden)

FALL
BI-2026-017, Kontoübernahme in der Buchhaltung

DAUER
29. Oktober 2026, 16:41 bis 2. November 2026, 16:10

ERGEBNIS
Angreifer ausgesperrt, keine Datenabflüsse festgestellt

4	3	0	5
Tage mit Zugriff	Kunden informiert	Meldungen an Behörden nötig	Massnahmen für die nächsten Wochen

Wann Sie dieses Dokument erhalten: Innerhalb einer Woche nach Abschluss der Inspektion.

Zusammenfassung

Der Angreifer kam über eine gefälschte Anmeldeseite, die das Token der Buchhaltung abgriff und die Mehrfaktor-Prüfung umging. Er hatte vier Tage Zugriff auf ein Postfach, verschickte eine Zahlungsaufforderung und bereitete eine Rückkehr über eine Authenticator-App vor. Kein Kunde hat bezahlt. Personendaten sind nach unserer Prüfung nicht abgeflossen; eine Meldung an den EDÖB war nicht angezeigt, Muster AG fällt nicht unter die Meldepflicht für kritische Infrastrukturen.

Genutzte Lücken und geschlossene Türen

LÜCKE	WAS DER ANGREIFER TAT	GESCHLOSSEN DURCH
Token-Phishing	Anmeldung über gefälschte Seite, Token wiederverwendet	Anmeldung nur von konformen Geräten, kürzere Anmeldehäufigkeit
Anmeldemethode	Eigene Authenticator-App registriert	Registrierung neuer Methoden nur von vertrauenswürdigem Standort
Posteingangsregel	Antworten versteckt	Meldung bei neuer Regel, externe Weiterleitung gesperrt
Phishing-Mail	Link «Rechnung freigeben» an die Buchhaltung	Sichere Links und Anhänge für alle, Domäne gesperrt

Massnahmen für die nächsten Wochen

- Passkeys für Buchhaltung, Einkauf und Geschäftsleitung einführen, danach für alle; Zuständig: IT Muster AG mit CNEXT.
- Zahlungsfreigaben mit Vier-Augen-Prinzip ausserhalb der Mail, mit Rückruf bei neuer Bankverbindung; Zuständig: Finanzen.
- Anmelde- und Überwachungsprotokolle laufend in ein Speicherkonto leiten, damit die Spuren länger als 30 Tage reichen; Zuständig: CNEXT.
- Die Prüfliste dieser Inspektion monatlich gegen den Vormonat laufen lassen; Zuständig: CNEXT, falls die laufende Inspektion gebucht wird.
- Kurze Schulung für alle mit dem echten Beispiel dieser Mail; Zuständig: Muster AG mit Vorlage von CNEXT.

So geht es weiter

Dieser Bericht geht an Geschäftsleitung und IT-Leitung. Der Beweisordner bleibt bei Ihnen; wir löschen unsere Kopie nach der vereinbarten Frist.

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