CNEXT SECURITY SERVICES · MASSNAHMENPROTOKOLL · EINMALIG

Protokoll der Sofortmassnahmen

KUNDE
Muster AG, Bern (erfunden)

FALL
BI-2026-017

FREIGABE DURCH
IT-Leitung Muster AG, telefonisch 10:18

STAND
Montag, 2. November 2026, 16:30

9	2	1	0
Massnahmen	Konten zurückgesetzt	Regel entfernt	offene Massnahmen

Wann Sie dieses Dokument erhalten: Laufend während der Inspektion, abgeschlossen mit dem Spurenbericht.

Zusammenfassung

Jede Massnahme wurde nach der Beweissicherung ausgeführt und mit einem Nachweis abgeschlossen: einem Protokolleintrag, einem Screenshot oder einem erneuten Export, der zeigt, dass die Spur weg ist. Die Reihenfolge folgt der Prüfliste: zuerst die Sitzungen, dann die Hintertüren, dann die Regeln für alle.

Massnahmen

ZEIT	MASSNAHME	KONTO	NACHWEIS
10:20	Alle Sitzungen und Aktualisierungstokens widerrufen	buchhaltung@	Protokoll 11
10:24	Posteingangsregel «.» entfernt, RSS-Feeds-Ordner geprüft, 14 Antworten zurück in den Posteingang	buchhaltung@	Export 02b
10:31	Authenticator-App auf unbekanntem Gerät gelöscht, Passwort zurückgesetzt, neue Methode mit der Mitarbeiterin am Telefon registriert	buchhaltung@	Protokoll 12
10:40	Sitzungen widerrufen, Passwort zurückgesetzt (gleiche Anmeldeseite, keine weitere Spur)	einkauf@	Protokoll 13
11:05	Gefälschte Anmeldeseite in Defender for Office 365 als Phishing gemeldet, Domäne gesperrt, Mail bei allen Empfängern entfernt	alle	Protokoll 14
11:30	Riskanter Benutzer in Entra ID Protection bestätigt und geschlossen	buchhaltung@	Screenshot 15
13:10	Richtlinie für bedingten Zugriff: Anmeldung nur von konformen Geräten, Anmeldehäufigkeit für Buchhaltung und Geschäftsleitung verkürzt	alle	Export 16

ZEIT	MASSNAHME	KONTO	NACHWEIS
14:00	Externe Weiterleitung für alle Postfächer per Transportregel gesperrt, Meldung bei neuer Posteingangsregel eingerichtet	alle	Export 17
16:10	Erneuter Export der Anmeldungen seit 10:20: keine Anmeldung ausserhalb der Schweiz	alle	Export 18

Beweisordner

- 18 Exporte und Screenshots, jeder mit Zeitstempel und SHA-256-Prüfsumme im Verzeichnis, abgelegt in einer SharePoint-Bibliothek mit Zugriff nur für Geschäftsleitung, IT-Leitung und CNEXT.
- Die Anmelde- und Überwachungsprotokolle der letzten 30 Tage sind vollständig exportiert; Audit (Standard) deckt 180 Tage, wir haben den ganzen Zeitraum gesichert.

So geht es weiter

Keine Massnahme ist offen. Die drei Massnahmen für alle Konten bleiben bestehen; der Übergabebericht nennt, was in den nächsten Wochen dazukommt.

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