INCIDENT-PLAYBOOK CLD-01

Verdacht auf kompromittiertes Cloud-Konto

Cloud & Zusammenarbeit

In einem Cloud-Dienst wie Microsoft 365 oder Google Workspace passieren Dinge, die niemand veranlasst hat. Anders als bei einem einzelnen Postfach hängen daran Dateien, Freigaben und verbundene Anwendungen des gesamten Unternehmens.

- Dateien in SharePoint oder Drive plötzlich geändert oder verschwunden
- Unbekannte App hat Zugriff auf das Konto erhalten
- Neue Freigabelinks für Ordner, die niemand erstellt hat
- Anmeldung aus einem Land ohne Standort des Unternehmens

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort von einem anderen, sauberen Gerät aus ändern und alle aktiven Sitzungen im Konto abmelden.

02 In den Kontoeinstellungen die verbundenen Apps und erteilten Berechtigungen ansehen und Auffälliges notieren.

03 Neu entstandene Freigabelinks und Zugriffsrechte notieren, bevor sie entfernt werden.

04 Die lokale Synchronisierung pausieren, damit Änderungen aus der Cloud nicht weiter auf die Geräte gespielt werden.

05 Unverzüglich melden. Cloud-Vorfälle betreffen fast nie nur ein Konto.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister mit Administrationsrechten für den Cloud-Dienst. Bei Administratorkonten zusätzlich die Geschäftsführung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über den betroffenen Cloud-Dienst, also weder per Mail noch per Chat darin.

WAS BEREITHALTEN

- Welcher Dienst und welches Konto betroffen sind
- Welche Auffälligkeit dir zuerst begegnet ist und wann
- Welche verbundenen Apps du gefunden hast
- Welche Ordner oder Dateien betroffen scheinen
- Ob das Konto Administrationsrechte hat

Nicht tun

HÄUFIGE FEHLER

- × Über den betroffenen Dienst selbst melden oder dort über den Vorfall chatten.
- × Verbundene Apps und Freigaben löschen, bevor sie festgehalten sind.
- × Dateien aus dem lokalen Ordner in die Cloud zurückspielen, um Änderungen zu reparieren.
- × Externe Empfänger von Freigabelinks eigenständig kontaktieren.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Administration prüft die Anmelde- und Aktivitätsprotokolle des Mandanten und grenzt ein, welche Konten betroffen sind.
- → Erteilte App-Berechtigungen werden entzogen, Freigaben zurückgenommen und Anmeldedaten samt Multi-Faktor-Authentifizierung neu aufgesetzt.
- → Anhand der Protokolle wird bewertet, ob Daten abgeflossen sind und ob daraus eine Meldepflicht folgt.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Verdacht auf Datenschutzverletzung (DAT-05) · Interne Kontakte siehe Incident-Kontaktblatt