

VORFALLART 04 · ERKENNEN & MELDEN

Kompromittierte Zugangsdaten & Konten

Wenn ein Passwort in falsche Hände gerät oder ein Konto fremde Aktivität zeigt.

Was ist das?

Zugangsdaten sind kompromittiert, wenn ein Passwort auf einer falschen Seite eingegeben, abgephisht, mehrfach wiederverwendet oder aus einem Datenleck bekannt wurde – oder wenn ein Konto fremde Aktivität zeigt.

Ein gekapertes Konto wird schnell zum Ausgangspunkt für Phishing im Namen des Betriebs oder für Zahlungsbetrug.

Was kann im Betrieb passieren?

- Fremdzugriff auf Postfach, Cloud oder Kundenkonten
- Versand von Phishing oder Betrug im Namen des Betriebs
- Abfluss personenbezogener oder vertraulicher Daten
- Ausgangspunkt für BEC und weitere Kontoübernahmen

Woran erkennst du es?

- Unerwartete Logins oder Anmeldungen aus fremden Orten
- MFA-Anfragen ohne eigenen Anlass
- Neue Weiterleitungen oder Regeln im Postfach
- Gesperstes Konto oder Hinweise von Kontakten auf seltsame Nachrichten

Sofort richtig reagieren

Der Handlungsrahmen aus der Fortbildung – Schritt für Schritt:

1	Trennen	Kein pauschales Kabelziehen. Von einem freigegebenen, sauberen Gerät die IT erreichen und die Kontosperre veranlassen. Ein Passwortwechsel allein ist keine Freigabe.
2	Festhalten	Betroffenes Konto, Uhrzeit und beobachtete Aktivität notieren. Keine Beweise löschen – z. B. fremde Postfachregeln erst dokumentieren.
3	Melden	IT sofort. Sind personenbezogene Daten betroffen, zusätzlich den Datenschutzkontakt informieren.
4	Bewahren	Konto erst nach Prüfung durch die IT wieder nutzen. MFA einrichten oder erneuern und verknüpfte Konten prüfen.

Merksatz

Passwort ändern reicht nicht – Konto sichern lassen und fremde Regeln und Weiterleitungen entfernen.



Das ist erst der erste Schritt

In der Fortbildung „Geprüfter Betrieblicher Cyber-Ersthelfer“ (290 €, 2× 100 Min live & digital) übst du genau diesen Ablauf für jede typische Vorfallart – mit Checklisten, Mailvorlagen, Urkunde & Badge. Empfehlung: zwei Ersthelfer je Betrieb. Anmeldung & Termine: info@secumetrix.de

Grenzen dieses Whitepapers: Es vermittelt allgemeines Wissen und ersetzt keine Rechtsberatung, keine technische Einzelfallprüfung und keine Versicherungszusage. Die Bewertung eines konkreten Vorfalls, die verbindliche rechtliche Einordnung und die Entscheidung über Versicherungsschutz erfordern die Prüfung des Einzelfalls. Führe nur Maßnahmen aus, für die du im Betrieb beauftragt und eingewiesen bist.