INCIDENT-PLAYBOOK ACC-01

Passwort oder Zugangsdaten preisgegeben

Konto & Identität

Ein Passwort ist in fremde Hände geraten. Es wurde auf einer nachgebauten Seite eingetippt, am Telefon genannt, in einem Chat geteilt oder lag sichtbar für andere zugänglich. Ob damit schon jemand angemeldet ist, weißt du nicht.

- Passwort auf einer gefälschten Anmeldeseite eingegeben
- Zugangsdaten am Telefon weitergegeben
- Passwort per Chat oder Mail verschickt
- Notierte Zugangsdaten sind abhandengekommen

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort sofort ändern, von einem Gerät aus, das nicht Teil des Vorfalls ist.

02 In den Kontoeinstellungen alle aktiven Sitzungen abmelden. Sonst bleibt eine fremde Anmeldung trotz neuem Passwort bestehen.

03 Prüfen, wo dasselbe Passwort noch verwendet wird, und auch dort wechseln.

04 Melden, auch wenn du das Passwort bereits geändert hast. Die IT prüft, ob in der Zwischenzeit zugegriffen wurde.

05 Wenn möglich Multi-Faktor-Authentifizierung für das Konto aktivieren.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, zeitnah. Bei Konten mit Zahlungs- oder Personaldaten zusätzlich die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Nicht über das betroffene Konto selbst.

WAS BEREITHALTEN

- Um welches Konto und welchen Dienst es geht
- Wie und wann die Daten preisgegeben wurden
- Ob das Passwort bereits geändert wurde
- Wo dasselbe Passwort sonst noch im Einsatz war
- Ob das Konto Multi-Faktor-Authentifizierung hat

Nicht tun

HÄUFIGE FEHLER

- × Nur das Passwort ändern und die aktiven Sitzungen unangetastet lassen.
- × Eine leichte Abwandlung des alten Passworts wählen. Angreifer probieren genau diese Varianten durch.
- × Den Fall für erledigt halten, weil sich nichts Auffälliges zeigt. Zugänge werden oft erst Wochen später genutzt.
- × Aus Scham abwarten. Der Zeitvorsprung ist das Einzige, was in diesem Fall hilft.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Anmeldeprotokolle des Kontos auf fremde Zugriffe und ungewöhnliche Standorte.
- → Postfachregeln, Weiterleitungen und verknüpfte Anwendungen werden auf nachträgliche Änderungen kontrolliert.
- → Bei Konten mit Zugriff auf personenbezogene Daten folgt die Bewertung durch Datenschutz-Ansprechperson und Geschäftsführung.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Phishing-Link angeklickt (PHI-02) · Interne Kontakte siehe Incident-Kontaktblatt

Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.

Alle Playbooks, Kontaktblatt und Hintergründe online — kostenfrei und ohne Anmeldung.

wermescher.com/tools/it-notfallplan