INCIDENT-PLAYBOOK ACC-03

Verdacht auf Kontoübernahme

Konto & Identität

Es gibt Anzeichen, dass jemand anderes Zugriff auf ein dienstliches Konto hat. Typisch sind Anmeldungen zu ungewöhnlichen Zeiten, Nachrichten, die du nie geschrieben hast, oder Einstellungen, die sich von selbst geändert haben.

- Anmeldung aus einem fremden Land gemeldet
- Gesendete Mails, die du nicht geschrieben hast
- Neue Weiterleitungsregel im Postfach
- Passwort funktioniert plötzlich nicht mehr

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort sofort ändern, von einem anderen, sauberen Gerät aus. Funktioniert das nicht mehr, direkt zur Meldung übergehen.

02 In den Kontoeinstellungen alle aktiven Sitzungen abmelden, damit fremde Zugriffe unterbrochen werden.

03 Postfachregeln und Weiterleitungen prüfen und auffällige Einträge notieren, bevor du sie entfernst.

04 Prüfen, ob dasselbe Passwort noch anderswo im Einsatz ist, und diese Konten ebenfalls ändern.

05 Sofort melden, auch wenn du den Zugriff schon unterbrochen hast.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei Konten mit Zahlungsfreigabe zusätzlich die Geschäftsführung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über das betroffene Konto, weil Angreifer dort mitlesen können.

WAS BEREITHALTEN

- Um welches Konto und welchen Dienst es geht
- Woran du den fremden Zugriff bemerkt hast
- Seit wann die Auffälligkeiten bestehen
- Welche Weiterleitungen oder Regeln du gefunden hast
- Ob das Passwort auch für andere Dienste genutzt wurde

Nicht tun

HÄUFIGE FEHLER

- × Über das verdächtige Konto selbst melden oder dort über den Vorfall schreiben.
- × Gefundene Weiterleitungsregeln löschen, ohne sie vorher festzuhalten. Sie sind ein wichtiger Hinweis auf das Vorgehen.
- × Abwarten, ob sich das Problem von selbst erledigt.
- × Kundinnen und Kunden auf eigene Faust warnen, bevor das Vorgehen abgestimmt ist.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT sperrt das Konto vorübergehend, setzt die Anmeldedaten neu auf und richtet die Multi-Faktor-Authentifizierung neu ein.
- → Anhand der Anmeldeprotokolle wird geprüft, welche Daten eingesehen und welche Nachrichten versendet wurden.
- → Sind personenbezogene Daten oder Zahlungsvorgänge betroffen, folgt die Bewertung durch Datenschutz-Ansprechperson und Geschäftsführung.

Verweise: Incident-Kontaktblatt (PDF) · Cloud-Konto kompromittiert (CLD-01) · Verdacht auf Datenschutzverletzung (DAT-05) · 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