INCIDENT-PLAYBOOK ACC-02

# MFA-Gerät verloren oder gewechselt

Konto & Identität

Das Gerät mit der Authenticator-App oder dem Sicherheitsschlüssel ist weg, defekt oder wurde getauscht. Anmeldungen, die einen zweiten Faktor verlangen, sind damit blockiert. Bei Verlust oder Diebstahl kommt hinzu, dass ein Fremder das Gerät in der Hand hält.

- Diensthandy verloren oder gestohlen
- Neues Handy ohne übertragene Authenticator-App
- Sicherheitsschlüssel nicht mehr auffindbar
- Gerät defekt und nicht mehr startfähig

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Bei Verlust oder Diebstahl sofort melden. Das ist ein Sicherheitsvorfall, keine reine Nutzerhilfe.

02 Ist das Gerät fremdverwaltet, die IT das Gerät sperren und die Fernlöschung auslösen lassen.

03 Beim geplanten Gerätewechsel die Übertragung durchführen, bevor das alte Gerät zurückgesetzt oder entsorgt wird.

04 Den zweiten Faktor für das alte Gerät in den Kontoeinstellungen entfernen lassen, sobald der neue eingerichtet ist.

05 Wiederherstellungscodes nicht auf demselben Gerät und nicht ungeschützt ablegen.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei Diebstahl zusätzlich die Geschäftsführung, bei Diensthandys auch wegen der enthaltenen Daten.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, wenn das Gerät verloren oder gestohlen wurde. Beim geplanten Wechsel über den normalen Meldeweg.

WAS BEREITHALTEN

- Um welches Gerät es geht und ob es dienstlich oder privat war
- Ob es verloren, gestohlen, defekt oder getauscht wurde
- Wann es zuletzt in deinem Besitz war
- Für welche Konten es als zweiter Faktor diente
- Ob das Gerät mit Code oder Biometrie gesperrt war

## Nicht tun

HÄUFIGE FEHLER

- × Das alte Gerät zurücksetzen oder entsorgen, bevor die hinterlegten Faktoren übertragen und entfernt sind.
- × Den Verlust als reines Ausstattungsthema behandeln und nur ein neues Gerät anfordern.
- × Wiederherstellungscodes im Postfach oder in einer Notiz-App auf demselben Gerät speichern.
- × Die Multi-Faktor-Authentifizierung vorübergehend abschalten, um weiterarbeiten zu können.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT entfernt die auf dem alten Gerät hinterlegten Faktoren aus allen betroffenen Konten.
- → Anmeldeprotokolle werden auf Zugriffe nach dem Verlustzeitpunkt geprüft.
- → Der neue zweite Faktor wird eingerichtet und neue Wiederherstellungscodes werden ausgegeben.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Privates Handy dienstlich genutzt (DEV-03) · 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