INCIDENT-PLAYBOOK ACC-04

Unerwartete MFA-Anfragen

Konto & Identität

Auf dem Handy erscheint eine Bestätigungsanfrage für eine Anmeldung, die du nicht ausgelöst hast. Manchmal einmal, manchmal in Serie und mitten in der Nacht. Jede dieser Anfragen bedeutet, dass jemand dein Passwort bereits kennt.

- Push-Anfrage ohne eigene Anmeldung
- Mehrere Anfragen kurz hintereinander
- Anfrage nachts oder im Urlaub
- SMS-Code, den niemand angefordert hat

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Anfrage ablehnen. Niemals bestätigen, um die Serie zu beenden.

02 Passwort des betroffenen Kontos sofort ändern. Die Anfragen belegen, dass es bekannt ist.

03 Alle aktiven Sitzungen des Kontos abmelden.

04 Sofort melden, auch wenn du nichts bestätigt hast. Die IT braucht den Zeitpunkt der Versuche.

05 Hast du versehentlich bestätigt: telefonisch melden, das ist der dringende Fall.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei versehentlicher Bestätigung sofort telefonisch.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, bei bestätigter Anfrage telefonisch.

WAS BEREITHALTEN

- Für welches Konto die Anfragen kamen
- Wie viele Anfragen und zu welchen Uhrzeiten
- Ob eine Anfrage bestätigt wurde
- Ob das Passwort bereits geändert wurde
- Ob parallel Anrufe oder Nachrichten dazu kamen

Nicht tun

HÄUFIGE FEHLER

- × Eine Anfrage bestätigen, damit endlich Ruhe ist. Genau darauf zielt die Wiederholung.
- × Die Anfragen wegwischen und nichts weiter tun. Das Passwort bleibt in fremder Hand.
- × Einem Anrufer glauben, der sich als IT ausgibt und um Bestätigung der Anfrage bittet.
- × Bis zum nächsten Werktag warten, weil die Anfragen nachts kommen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Anmeldeprotokolle auf Herkunft und Zeitpunkt der Versuche und setzt die Anmeldedaten neu auf.
- → Der zweite Faktor wird bei Bedarf auf ein Verfahren mit Nummernabgleich oder Sicherheitsschlüssel umgestellt.
- → Ist eine Bestätigung erfolgt, werden Postfachregeln, Weiterleitungen und verknüpfte Anwendungen kontrolliert.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Verdächtiger Anruf (PHI-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