INCIDENT-PLAYBOOK SUP-03

Zugangsdaten oder Secrets veröffentlicht

Lieferanten & Softwareentwicklung

Ein Passwort, ein API-Schlüssel, ein Token oder ein privater Schlüssel ist an einer Stelle gelandet, die andere einsehen können. Typisch sind ein Commit im Repository, ein Ticket, ein Chatverlauf oder eine Konfigurationsdatei in einem geteilten Ordner.

- API-Schlüssel versehentlich ins Repository committet
- Zugangsdaten in einem Ticket oder Chat gepostet
- Konfigurationsdatei mit Passwörtern geteilt
- Warnung eines Dienstes über einen gefundenen Schlüssel

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Den Schlüssel oder das Passwort sofort widerrufen oder wechseln, wenn du dazu berechtigt bist. Das Löschen der Fundstelle allein reicht nicht.

02 Ohne Berechtigung sofort die Person erreichen, die den Schlüssel sperren kann. Bis dahin hat das Vorrang vor allem anderen.

03 Fundstelle, Zeitpunkt der Veröffentlichung und betroffenen Dienst notieren.

04 Den Commit oder Beitrag nicht eigenmächtig aus der Historie entfernen, bevor die IT den Stand gesichert hat.

05 Melden, auch wenn der Schlüssel bereits gewechselt ist.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die Verantwortlichen für den betroffenen Dienst. Bei Zugang zu Kunden- oder Produktivsystemen zusätzlich die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Den Schlüssel selbst nicht in die Meldung kopieren, nur Fundstelle und Dienst nennen.

WAS BEREITHALTEN

- Welcher Schlüssel für welchen Dienst betroffen ist
- Wo und seit wann er sichtbar war
- Wer die Fundstelle einsehen konnte
- Ob der Schlüssel bereits widerrufen oder gewechselt ist
- Welche Rechte der Schlüssel hatte

Nicht tun

HÄUFIGE FEHLER

- × Nur den Commit löschen oder die Historie umschreiben und den Schlüssel weiter verwenden.
- × Den Schlüssel per Mail oder Chat weitergeben, um den Fall zu erklären.
- × Abwarten, weil die Fundstelle nur intern sichtbar ist. Auch intern erreicht sie mehr Personen als nötig.
- × Den neuen Schlüssel wieder an derselben Stelle ablegen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Protokolle des Dienstes auf Zugriffe mit dem Schlüssel seit dem Zeitpunkt der Veröffentlichung.
- → Abhängige Systeme werden auf den neuen Schlüssel umgestellt, der alte bleibt dauerhaft gesperrt.
- → Die Fundstelle wird bereinigt. Secrets werden künftig in einem dafür vorgesehenen Tresor verwaltet.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen, ob ein erheblicher Cybersicherheitsvorfall vorliegt, der nach § 34 zu melden ist.

Verweise: Incident-Kontaktblatt (PDF) · Repository versehentlich veröffentlicht (SUP-04) · Passwort oder Zugangsdaten preisgegeben (ACC-01) · Verdacht auf kompromittiertes Cloud-Konto (CLD-01) · 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