INCIDENT-PLAYBOOK SUP-04

Repository versehentlich veröffentlicht

Lieferanten & Softwareentwicklung

Ein internes Code-Repository war oder ist öffentlich einsehbar, etwa nach einer geänderten Sichtbarkeit, durch einen öffentlichen Fork oder eine Kopie auf einer privaten Plattform. Damit können Quellcode, Konfiguration und darin enthaltene Zugangsdaten für Unbefugte sichtbar sein.

- Sichtbarkeit eines Repositorys auf öffentlich gestellt
- Interner Code in ein privates Konto kopiert
- Öffentlicher Fork eines internen Projekts
- Hinweis von außen auf auffindbaren Firmencode

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Wenn du berechtigt bist, die Sichtbarkeit sofort auf privat stellen und den Zeitpunkt notieren. Gleichzeitig melden, nicht stillschweigend.

02 Festhalten, seit wann das Repository öffentlich war, soweit das erkennbar ist.

03 Alle Zugangsdaten und Schlüssel, die im Repository oder seiner Historie stehen, als bekannt behandeln.

04 Nichts aus der Historie löschen und keine Commits umschreiben, bevor die IT den Stand gesichert hat.

05 Sofort melden, auch wenn das Repository nur kurz öffentlich war.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die Leitung der Softwareentwicklung. Bei personenbezogenen Daten oder Kundencode zusätzlich Datenschutz-Ansprechperson und Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Repository und Plattform genau benennen.

WAS BEREITHALTEN

- Welches Repository auf welcher Plattform betroffen ist
- Seit wann und wie lange es öffentlich war
- Ob es Zugangsdaten, Schlüssel oder Konfiguration enthält
- Ob personenbezogene Daten oder Kundencode enthalten sind
- Ob Forks oder Kopien entstanden sind

Nicht tun

HÄUFIGE FEHLER

- × Das Repository still wieder auf privat stellen und den Fall für erledigt halten.
- × Die Historie bereinigen, bevor die enthaltenen Schlüssel gewechselt sind.
- × Personen, die einen Fork erstellt haben, eigenständig anschreiben.
- × Das Repository löschen, um die Spuren zu beseitigen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT wechselt alle Zugangsdaten und Schlüssel, die im Repository oder seiner Historie enthalten waren.
- → Die Protokolle der Plattform werden auf Zugriffe, Klone und Forks während der öffentlichen Phase geprüft.
- → Sind personenbezogene Daten betroffen, folgt die Bewertung nach Art. 33 DSGVO durch die Datenschutz-Ansprechperson.
- → Die Geschäftsführung entscheidet, ob Kunden oder Partner zu informieren sind, deren Code oder Daten betroffen waren.

Verweise: Incident-Kontaktblatt (PDF) · Zugangsdaten oder Secrets veröffentlicht (SUP-03) · Daten versehentlich öffentlich freigegeben (DAT-02) · 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