INCIDENT-PLAYBOOK DEV-03

Privates Gerät für Firmendaten verwendet

Geräte & Datenträger

Unternehmensdaten sind auf einem privaten Gerät oder in einem privaten Konto gelandet. Manchmal bewusst, weil es schneller ging. Oft unbemerkt, weil eine Synchronisierung im Hintergrund lief.

- Firmendokument am eigenen Laptop bearbeitet
- Dienstliche Mail ans private Postfach weitergeleitet
- Foto von Unterlagen am privaten Handy
- Firmendaten in privatem Cloud-Speicher abgelegt

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts löschen. Was jetzt verschwindet, fehlt später bei der Frage, welche Daten überhaupt betroffen waren.

02 Keine weiteren Kopien anlegen, nichts weiterleiten, nicht weiterbearbeiten.

03 Automatische Synchronisierung pausieren, wenn eine läuft: Cloud-Backup, Fotomediathek, Messenger-Sicherung.

04 Kurz notieren, welche Daten es sind, wann sie auf das Gerät kamen und über welchen Weg.

05 Den Vorgang melden, auch wenn nichts Schlimmes passiert ist. Die Bewertung übernimmt die IT.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die direkte Führungskraft. Bei personenbezogenen Daten zusätzlich die Datenschutz-Ansprechperson.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, im Zweifel telefonisch. Für die Meldung ein dienstliches Gerät verwenden.

WAS BEREITHALTEN

- Um welches private Gerät oder Konto es geht
- Welche Daten betroffen sind und ungefähr wie viele
- Seit wann die Daten dort liegen
- Ob personenbezogene Daten dabei sind
- Ob weitere Personen Zugriff auf das Gerät haben

Nicht tun

HÄUFIGE FEHLER

- × Die Daten eigenmächtig löschen, bevor der Vorgang aufgenommen ist.
- × Den Vorgang verschweigen, weil er unangenehm ist. Eine späte Meldung kostet immer mehr als eine unangenehme.
- × Zur Bereinigung weitere Kopien auf andere private Geräte oder Konten ziehen.
- × Screenshots der Daten an Kolleginnen und Kollegen schicken, um die Lage zu erklären.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT klärt den Umfang, prüft eine nachweisbare Löschung und entscheidet, ob das Gerät bereinigt werden muss.
- → Bei personenbezogenen Daten bewertet die Datenschutz-Ansprechperson, ob eine meldepflichtige Datenschutzverletzung vorliegt.
- → Gibt es einen echten fachlichen Bedarf, richtet die IT einen freigegebenen Weg ein: sicherer Zugriff oder ein verwaltetes Gerät.

Verweise: Incident-Kontaktblatt (PDF) · 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