INCIDENT-PLAYBOOK DAT-02

Daten versehentlich öffentlich freigegeben

Daten & Datenschutz

Eine Datei, ein Ordner oder ein Dokument ist über einen Link oder eine Freigabe für mehr Personen zugänglich als vorgesehen, im schlimmsten Fall für alle im Internet. Typisch sind Cloud-Links, die für jeden mit dem Link funktionieren, oder Freigaben, die nach einem Projekt nie zurückgenommen wurden.

- Cloud-Ordner per offenem Link für jeden zugänglich
- Tabelle mit Kundendaten öffentlich freigegeben
- Externe Freigabe nach Projektende nie entfernt
- Freigabe für das ganze Unternehmen statt für das Team

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Mit einem Screenshot festhalten, was freigegeben ist, für wen und seit wann, soweit erkennbar.

02 Danach die Freigabe einschränken, wenn du berechtigt bist, und den Zeitpunkt notieren. Gleichzeitig melden.

03 Die Datei oder den Ordner nicht löschen und nicht verschieben.

04 Notieren, welche Personengruppen und Datenarten betroffen sein könnten.

05 Sofort melden, auch wenn du nicht weißt, ob jemand zugegriffen hat.

Melden

SOFORT

WEN

Datenschutz-Ansprechperson und IT-Verantwortliche gemeinsam. Fehlt eine benannte Datenschutz-Ansprechperson, geht die Meldung an die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Den Freigabelink nicht in Chats oder Mails weiterverbreiten, nur den Speicherort nennen.

WAS BEREITHALTEN

- Welche Datei oder welcher Ordner betroffen ist
- Für wen die Freigabe galt und seit wann
- Welche Datenarten und wie viele Personen betroffen sind
- Ob die Freigabe bereits eingeschränkt wurde
- Wo der Link geteilt oder verschickt wurde

Nicht tun

HÄUFIGE FEHLER

- × Die Freigabe still zurücknehmen und den Fall damit für erledigt halten.
- × Datei oder Ordner löschen, um den Vorfall zu bereinigen.
- × Selbst nachforschen, wer den Link geöffnet hat, und dafür weitere Personen einbinden.
- × Den Link zur Prüfung an Kolleginnen und Kollegen schicken.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT wertet die Zugriffsprotokolle der Plattform aus und prüft, ob die Daten abgerufen wurden.
- → Die Datenschutz-Ansprechperson bewertet das Risiko. Ergibt sich eines, meldet das Unternehmen unverzüglich und möglichst binnen 72 Stunden an die Datenschutzbehörde (Art. 33 DSGVO).
- → Bestehende Freigaben im selben Bereich werden auf vergleichbare Fehler durchgesehen.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · 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