Warum IT ins Mitarbeiter-Offboarding gehört?

Wenn ein Mitarbeiter ein Unternehmen verlässt, denken die meisten zuerst an Kündigung, Zeugnis und Schlüsselrückgabe. Die IT-Seite wird dabei häufig vergessen – mit teils erheblichen Folgen für Sicherheit, Kosten und Datenschutz.

Sicherheitsrisiken durch offene Zugänge

Jedes aktive Konto eines ausgeschiedenen Mitarbeiters ist ein potenzielles Einfallstor. E-Mail-Postfächer, Microsoft 365-Lizenzen, VPN-Zugänge, Cloud-Dienste und Systempasswörter bleiben ohne IT-Einbindung oft wochenlang – manchmal dauerhaft – aktiv. Ein ehemaliger Mitarbeiter, der (bewusst oder unbewusst) weiterhin Zugriff hat, kann Daten einsehen, kopieren oder löschen. Laut einer Studie von Beyond Identity (2022) hatten **83% der befragten Unternehmen** nach Mitarbeiterabgängen noch aktive Zugänge im System. Auch unbeabsichtigte Szenarien sind gefährlich: Konten ohne aktiven Nutzer werden häufig von Angreifern für unbemerkte Zugriffe missbraucht, da dort niemand mehr die Aktivität prüft.

Datenschutz und DSGVO-Pflichten

Nach DSGVO sind Unternehmen verpflichtet, personenbezogene Daten nur so lange zu verarbeiten, wie ein legitimer Zweck besteht. Das betrifft auch die Zugriffsrechte ausgeschiedener Mitarbeiter: Aktive Konten eines Ex-Mitarbeiters verstoßen gegen das Prinzip der Datensparsamkeit und können bei einer Datenschutzprüfung zum Problem werden. Hinzu kommt: Unternehmen haften für Datenpannen, die über solche offenen Zugänge entstehen – auch wenn der Mitarbeiter das Unternehmen längst verlassen hat.

Lizenz- und Kostenoptimierung

Microsoft 365, Adobe, Antivirensoftware und viele andere Dienste werden **pro Benutzer und Monat** abgerechnet. Wird ein ausgeschiedener Mitarbeiter nicht aus der Lizenz entfernt, zahlen Sie

für ein Konto, das niemand mehr nutzt – oft unbemerkt über Monate oder Jahre. Die IT-seitige Kontobereinigung ist damit nicht nur ein Sicherheits-, sondern auch ein direktes Einsparungsthema.

Datensicherung und Wissenserhalt

Vor der Deaktivierung eines Kontos muss geprüft werden, welche Daten, E-Mails, Dateien oder Freigaben der Mitarbeiter hinterlässt – und wer zukünftig darauf zugreifen muss. Ohne geordnetes IT-Offboarding gehen Projektdaten, Kundenkommunikation oder geteilte Dokumente verloren oder sind nicht mehr zugänglich. Ein strukturierter Übergabeprozess sichert das betriebliche Wissen.

Was wir im Offboarding übernehmen

Damit nichts übersehen wird, kümmern wir uns beim Ausscheiden eines Mitarbeiters um folgende Punkte:

- **Sofortige Deaktivierung** aller Konten (Microsoft 365, E-Mail, VPN, Cloud-Dienste)
- **Weiterleitung oder Archivierung** des E-Mail-Postfachs
- **Entzug von Geräte- und Systemzugriffen** (Laptop, Mobilgerät, Server)
- **Entfernung aus Gruppen, Freigaben und Shared Mailboxes**
- **Lizenzbereinigung** zur Kosteneinsparung
- **Datensicherung** relevanter Nutzerinhalte vor der Löschung
- **Passwortänderung** für gemeinsam genutzte Accounts

Unsere Bitte an Sie

Bitte informieren Sie uns **so früh wie möglich** – idealerweise vor dem letzten Arbeitstag – wenn ein Mitarbeiter das Unternehmen verlässt. Ein kurzer Hinweis per E-Mail oder Ticket genügt. Je früher wir Bescheid wissen, desto reibungsloser, sicherer und kostengünstiger läuft der Prozess ab.

> “ Offboarding | PC-SPEZIALIST Wiki

Version #2
Erstellt: 2026-06-05 06:43:09 UTC von Frank Böttger
Zuletzt aktualisiert: 2026-06-05 06:46:17 UTC von Frank Böttger