CHECKLISTE FÜR GESCHÄFTSFÜHRUNG UND PERSONALABTEILUNG

Wenn jemand das Unternehmen verlässt

Was am letzten Arbeitstag in Microsoft 365 passieren sollte, in welcher Reihenfolge, und welche Zugänge auch Wochen später noch offen sind.

Nexus.365 — powered by farpoint Solution UG (haftungsbeschränkt) farpoint.tech

Das Problem mit dem letzten Arbeitstag

> **Der Schreibtisch ist am Freitag leer. Das Konto ist es oft Monate später noch nicht.**

In den meisten Unternehmen ist das Onboarding neuer Mitarbeitender gut geregelt. Es gibt eine Liste, jemand ist zuständig, und am ersten Tag funktioniert alles. Beim Austritt fehlt dieselbe Sorgfalt: Das Konto wird irgendwann deaktiviert, meist wenn es jemandem auffällt.

Das ist aus drei Gründen heikel. Erstens bleibt der Zugriff auf Mails und Dateien bestehen, auch nach dem letzten Arbeitstag. Zweitens zahlen Sie für die Lizenz weiter. Drittens ist genau das die Frage, die im Fragebogen der Cyber-Versicherung steht.

Teil 1 — Am letzten Arbeitstag

- [ ] **Anmeldesitzungen beenden.** Ein deaktiviertes Konto sperrt niemanden aus, der bereits angemeldet ist. Aktive Sitzungen laufen weiter, auf dem Telefon oft tagelang. Sperren und Abmelden sind zwei getrennte Schritte.
- [ ] **Passwort ändern und Konto sperren.** In dieser Reihenfolge, nicht umgekehrt.
- [ ] **Zweiten Sicherheitsschritt zurücksetzen.** Sonst bleibt das private Telefon der ausgeschiedenen Person als Bestätigungsgerät hinterlegt.
- [ ] **Firmendaten vom Gerät entfernen.** Bei verwalteten Geräten aus der Ferne möglich. Bei privaten Geräten nur, wenn Firmendaten vorher getrennt abgelegt wurden.
- [ ] **Weiterleitungen und Stellvertreterregeln im Postfach prüfen.** Eine automatische Weiterleitung auf eine private Adresse überlebt die Kontosperrung und fällt sonst niemandem auf.

Teil 2 — In der ersten Woche danach

- [ ] **Postfach umwandeln und Vertretung einrichten.** Mails sollen jemanden erreichen, nicht ins Leere laufen.
- [ ] **Lizenz entziehen.** Das ist der Punkt, an dem laufende Kosten enden. Vorher prüfen, ob Daten gesichert sind, denn mit der Lizenz läuft eine Frist.
- [ ] **Dateien übergeben.** Der persönliche Ablagebereich gehört niemandem sonst. Ohne aktive Übergabe sind die Inhalte nach Ablauf der Frist weg.
- [ ] **Mitgliedschaften in Teams und Gruppen beenden.** Eine Gruppenmitgliedschaft überlebt die Kontosperrung und fällt bei einer Reaktivierung sofort wieder an.
- [ ] **Geteilte Links prüfen.** Von der ausgeschiedenen Person erzeugte Freigaben funktionieren weiter, auch wenn das Konto gesperrt ist.

Teil 3 — Was fast immer vergessen wird

- ☐ **Zugänge außerhalb von Microsoft 365.** Der Onlineshop, das Buchhaltungsprogramm, der Social-Media-Zugang, das Portal des Steuerberaters. Diese Konten hängen selten am zentralen Login.
- ☐ **Gemeinsam genutzte Passwörter.** Jedes Passwort, das die Person kannte und das mehrere nutzen, gehört geändert. Ohne Passwortverwaltung weiß meist niemand, welche das sind.
- ☐ **Persönlich erteilte App-Freigaben.** Verbindungen zu Drittanbieter-Diensten, die über das Konto autorisiert wurden.
- ☐ **Telefonnummer in Notfalllisten und Weiterleitungen.**
- ☐ **Schlüssel für verschlüsselte Geräte.** Wenn das Gerät weitergegeben wird und der Wiederherstellungsschlüssel nur beim Vorbesitzer lag, ist es Elektroschrott.

Wer macht was

Schritt	Verantwortlich	Wann
Austritt melden	Personalabteilung oder Geschäftsführung	sobald bekannt, nicht am letzten Tag
Zugriff entziehen	IT oder Dienstleister	letzter Arbeitstag, nach Dienstschluss
Vertretung und Übergabe	Führungskraft der Abteilung	erste Woche
Lizenz und Daten	IT oder Dienstleister	erste Woche
Fremdsysteme	jeweiliger Fachbereich	erste Woche

Der eine Schritt, der den Unterschied macht

Melden Sie den Austritt, sobald er feststeht, nicht am letzten Arbeitstag. Alles andere auf dieser Liste lässt sich vorbereiten. Was nicht vorbereitet ist, wird zwischen Tür und Angel erledigt, und dort entstehen die Lücken, die später im Fragebogen der Versicherung stehen.

Eine unangenehme Kontrollfrage

Nehmen Sie die letzte Person, die Ihr Unternehmen verlassen hat. Könnten Sie heute, ohne nachzufragen, sagen: Hat dieses Konto noch Zugriff auf Mails? Läuft noch eine Lizenz? Existiert noch eine Weiterleitung? Ist das Gerät zurück und gelöscht?

Wenn die Antwort auf eine dieser Fragen „weiß nicht“ lautet, ist das kein Vorwurf. Es ist der übliche Zustand in Unternehmen ohne festen Ablauf. Es ist aber auch ein guter Grund, diesen Ablauf einmal aufzuschreiben.

Wie es weitergeht.
Dieses Dokument beschreibt einen möglichen Weg, keine Vorschrift. Wenn Sie wissen möchten, wo Ihr Microsoft 365 heute steht, ist die Bestandsaufnahme der nächste Schritt: Nexus.365 Security Scan, 7 Tage, fester Preis, Bericht in Klartext.

farpoint Solution UG (haftungsbeschränkt) · Welfenstrasse 110, 81541 München
info@farpoint.tech · farpoint.tech

Microsoft 365 wie Strom aus der Steckdose. Laufende Produktivität, automatisierte Security.