



SEILBAHNEN

INTERNATIONAL

STUDIE
**SO BLEIBEN UNS DIE
GÄSTE ERHALTEN**

BOOMERANG HIRING
**SO GEWINNEN WIR
MITARBEITER ZURÜCK**

SKISERVICE
**SO ENTLASTEN ROBOTER
DAS PERSONAL**



MITARBEITERWECHSEL: TROTZ FLUKTUATION WISSEN SICHERN

Zugangsdaten von Social Media Accounts, Kontaktdaten „richtiger“ Ansprechpartner, „gute“ Einkaufskonditionen u.v.m. „verschwinden“ oft mit dafür zuständigen Mitarbeitern.

Es ist fatal, wenn bei Mitarbeiterwechseln unternehmenseigenes Wissen verschwindet, weil Systeme zur Verhinderung von Wissensverlust fehlen. Beispiele: Wenn die Facebook- oder Instagram-Zugangsdaten niemand im Unternehmen parat hat. Oder wenn auf Bewertungen, etwa bei Google, nicht reagiert werden kann, weil man keinen Zugriff auf unternehmenseigene Accounts hat. Kaum zu glauben, doch die beschriebenen Situationen – zwischen peinlich und unprofessionell angesiedelt – kommen regelmäßig vor.

Unprofessionell, nicht kriminell

Die Rede ist hier nicht von kriminellen Machenschaften, sondern von Mitarbeitern, die das Unternehmen verlassen, ohne dass sie von ihren Chefs mit Nachdruck dazu angehalten werden, entsprechende Daten und Informationen intern zu übergeben. Auch wenn man meinen würde, solche Übergaben wären Standard, ist dem nicht so. Ein anderes Problem lauert, wenn bei Übergabe von Informationen oder Zugangsdaten keine gründliche Prüfung dieser erfolgt, so lange die jeweilige Person noch im Dienst und greifbar ist. Durch unprofessionelles Verhalten aller Beteiligten entsteht ohne externes Zutun oder kriminelles Verhalten beträchtlicher Schaden. Es muss viel Zeit aufgewendet werden, um fehlende

Informationen wieder zu sammeln. Und die Außenwirkung entspricht nicht der eines professionellen Unternehmens. Ist man als Unternehmen nicht Herr/Frau von Zugangsdaten und unternehmensinternem Wissen, dann deutet das auf eine Firmenkultur mit geringem Professionalitätsgrad hin.

Strategischer Wissenserhalt

Gerade in unserer heutigen, meist schnelllebig-oberflächlichen Welt gilt es, von der Geschäftsführung ausgehend, in allen Unternehmensbereichen systematischen, strategischen Wissenserhalt zu kultivieren. Brachialer Zwang ist nicht die Lösung. Vielmehr geht es um gelebte Wissens-Sicherungsstrukturen, die geschaffen, gepflegt, überprüft und vor kriminellem Missbrauch gesichert werden. Es braucht – losgelöst von der Möglichkeit, dass ein Mitarbeiter das Unternehmen verlässt – geschützte Zugangsdaten- und Passwortlisten. Zudem benötigen Firmen einfache, verständliche Systeme, mit denen Arbeitsschritte bzw. Vorgangsweisen auch für nicht täglich damit arbeitende Kollegen greifbar werden. Und es braucht – als Teil der Arbeitsverträge – festgelegte Verpflichtungen zur vollständigen internen, persönlichen Übergabe aller Zugangsdaten, mit denen man arbeitet. Wer keine solche Vereinbarungen schließt,

darf sich nicht wundern, wenn es im Fall eines Ausscheidens von Mitarbeitern zu besagtem Wissensverlust kommt.

Check des Status quo

Erst einmal für das mögliche Problem „Wissensverlust“ sensibilisiert, sind es simple Bitten bzw. Fragen, die beruhigen oder entlarven. „Bitte um die vollständige Liste unserer Zugangsdaten zu Websites, Buchungstools, Social Media Accounts, Google, WeTransfer, Zoom, E-Mail-Zugangs- bzw. Einrichte-Daten und weitere Zugänge zu vorhandenen Systemen“, lautet eine davon. Gibt es die Liste, hat man sie elektronisch rasch zur Verfügung. Oder noch besser – man weiß, auf welchem „EDV-Pfad“ man die Liste findet. Hat man sie, lautet die nächste Frage: Ist sie passwortgeschützt? Und, wenn ja, wer kennt es? Ähnliche Fragen lassen sich stellen zu Lieferanten- bzw. Partneraufstellungen, zum E-Banking, Wartungspartnern und zu zahllosen weiteren Accounts, die man im Lauf der Zeit angelegt hat. Je nach „Ergebnis“ dieses Schnell-Checks ist entweder Gefahr in Verzug, nur einiger Optimierungsbedarf oder alles professionell gelöst. Darauf aufbauend gilt es, mit den Mitarbeitern alle Problembereiche, wo es zu Wissensverlust kommen könnte, mit klugen „Sicherheitsnetzen“ auszustatten.

Oliver Pichler