Leitfaden
Externe Infrastruktur (IT-Partner und Cloud-Anbieter)

Viele Treuhandunternehmen arbeiten mit einem externen IT-Anbieter zusammen, der das Netzwerk betreut, die Software installiert und auch für die Sicherheit dieser Infrastruktur zuständig ist. Auch wenn Ihre IT Systeme von einem externen Unternehmen betrieben werden oder Sie alle Daten in der Cloud speichern, gibt es trotzdem einige Sicherheitsmassnahmen und Regeln zu beachten. Diese werden im folgenden Leitfaden genauer beschrieben.

1. Accounts / Online-Konten

Bei einem Passwort für alle Online-Konten haben Hacker ein leichtes Spiel. Aus Sicherheitsgründen sollten Sie für jeden Account ein anderes Passwort verwenden. Teilen Sie Ihre Online-Konten möglichst nicht mit anderen Personen. Jeder Mitarbeitende sollte ein eigenes Konto haben, damit nachvollzogen werden kann, wer wie aktiv war.

2. Passwörter

Nach wie vor gehören Passwörter wie «123456», «qwertz» und «hallo» zu den beliebtesten, obwohl allgemein bekannt ist, dass sicherere Passwörter verwendet werden sollten. Aktuell wird empfohlen, Passwörter wie folgt zu erstellen:

- Mindestens zehn Zeichen: Diese Passwortlänge ist erforderlich für mittelgrosse Sicherheit.
- Sie enthalten Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen, aber keine Umlaute.
- Sie enthalten keine Wortfolgen, die in einem Wörterbuch stehen.
- Für jedes Konto wird ein eigenes Passwort verwendet. Sollte ein Passwort geknackt werden, sind die anderen Konten geschützt.
- Zusätzlich zum Passwortschutz ist eine **Zwei-Faktor-Authentifizierung** zu empfehlen.

Da sich kaum jemand solche Passwörter merken kann, wird die Verwendung eines **Passwort-Managers** empfohlen. Dabei handelt es sich um eine App oder einen Online-Dienst, der alle Ihre Passwörter verschlüsselt und Passwort-geschützt speichert. Dieses Passwort ist das einzige, dass Sie sich merken müssen. Für die Zugangsdaten zu den einzelnen Konten können Sie mit dem eingebauten Generator sichere, schwer erratbare Zeichenkombinationen erzeugen und für jeden Zugang ein separates Passwort festlegen. Optional ist bei vielen Passwort-Managern eine Zwei-Faktor-Authentifizierung möglich, was für zusätzlichen Schutz sorgt.

Ein Partner von TREUHAND|SUISSE, **SecureSafe**, bietet einen solchen Passwort-Manager an und Mitglieder erhalten 10 Rabatt Rabatt: https://www.securesafe.com/de/treuhand-suisse

☞ Checkliste:

- □ Einführen eines Passwort-Managers in Ihrem Unternehmen.
- □ Den Mitarbeitenden eine Frist setzen, bis zu der alle Passwörter durch sichere Passwörter ersetzt werden müssen.

3. Datenverschlüsselung

Die meisten Cloud-Anbieter bieten eine Verschlüsselung der Daten an. Auch bei der Übertragung der Daten von Ihrem Computer auf den Cloudserver werden in der Regel Verschlüsselungsverfahren eingesetzt. Da Sie aber keine Sicherheit haben, dass Dritte nicht doch auf die Daten auf dem Cloudserver zugreifen können, ist es ratsam, die vertraulichen Unternehmensdaten zusätzlich mit eigenem Verschlüsselungsverfahren bereits vor dem Hochladen zu sichern.

Es gibt verschiedene Verschlüsselungslösungen, die auf dem Endgerät installiert und anschliessend mit dem gewählten Speicherdienst verknüpft werden.

Ein verbreitetes Tool für die Verschlüsselung ist https://www.boxcryptor.com/de/.

☞ **Checkliste:**

- □ Cloud-Anbieter mit Verschlüsselungsverfahren auswählen.
- □ Tool für die Verschlüsselung von sensitiven Daten einführen.

4. Daten im Ausland

Unternehmen müssen bei Datenübermittlungen ins Ausland die gesetzlichen Vorlagen erfüllen. Wenn Personendaten ins Ausland übermittelt beziehungsweise dort gespeichert werden, müssen sie vor dem Zugriff ausländischer Behörden geschützt werden. In der Regel können Daten bei Anbietern, die ihren Hauptsitz in der Europäischen Union (EU) haben, ohne Probleme abgespeichert werden. Bei der Datenverarbeitung ausserhalb Europas muss überprüft werden, ob die Staaten ein angemessenes Datenschutzniveau aufweisen. Unter folgendem Link finden Sie eine Staatenliste, die gemäss Eidgenössischem Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) angemessenen Datenschutz bieten:

https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

Werden die Daten vor der Übertragung an den Cloud-Anbieter verschlüsselt und verfügt dieser nicht über den zur Entschlüsselung erforderlichen Schlüssel, ist gemäss Schweizerischem Anwaltsverband die Nutzung von Cloud-Diensten straf- und datenschutzrechtlich unbedenklich.

☞ **Checkliste:**

- □ Falls Sie Cloud-Dienste nutzen und Personendaten speichern, prüfen Sie, ob ein angemessener Datenschutz garantiert wird.

5. Back-up

Das Speichern von relevanten Daten ist für Unternehmen von grosser Bedeutung, denn ein Datenverlust kann gravierende Folgen für das Image und den wirtschaftlichen Erfolg eines Unternehmens haben. Lokale Back-ups und Cloud-Back-ups bieten Abhilfe. Folgende Punkte sind bei einem Back-up zu beachten:

- IT-Abteilung sollte das Cloud-Back-up regelmässig auf dessen Funktionalität überprüfen, damit die Datenwiederherstellung im Notfall problemlos durchführbar ist.
- Testen Sie periodisch die Back-up-Leistungen Ihres IT Partners. Löschen Sie eine Testdatei und bitten Sie Ihren IT-Partner, diese wiederherzustellen.

☞ **Checkliste:**

- □ Notieren Sie sich in Ihrer Agenda mindestens zweimal pro Jahr einen Test Ihres Back-up.

6. Cloudbasierte Dienste

Bei cloudbasierten Diensten werden teilweise vertrauliche Daten an externe Cloudanbieter ausgelagert. Deshalb ist bei der Auswahl von Cloudanbietern auf deren Seriösität zu achten.

☞ **Checkliste:**

- □ Zertifikate und Testate durch Dritte: Erfüllt der Cloud-Anbieter die nötigen Sicherheitsvorschriften?
- □ Transparente Kommunikation des Cloud-Anbieters: Zustellung von Informationen, was mit den Unternehmensdaten passiert, wo sie abgespeichert werden und wie sie vor Fremdzugriffen geschützt werden.

- □ Nachfragen, was bei einem Cyber-Angriff auf den Cloudanbieter passiert (Back-up der Cloud, Ausfallzeiten etc.)
- □ Datenverschlüsselung: Der Cloud-Anbieter ergreift Massnahmen zur sicheren Übermittlung und Speicherung der Daten.

7. Sicheres Login / Authentifizierung

Egal ob in sozialen Netzwerken, beim Cloud-Anbieter oder bei geschäftlichen Online-Dienstanbietern: Wer im Internet unterwegs ist, nutzt heute ganz alltäglich zahlreiche Logins. In Deutschland benutzt ein Mensch im Durchschnitt über 78 Online-Konten. Standardmässig sind die meisten Benutzerkonten im Netz mit einer Kombination aus Benutzernamen und Passwort geschützt. Folgende Regeln sind für ein sicheres Login zu beachten:

- Für jedes Konto ein eigenes Passwort verwenden (Passwort-Manager).
- Verwenden Sie «starke» Passwörter.
- Halten Sie Ihr Login geheim.
- Aktivieren Sie die Benachrichtigungsfunktion über ungewöhnliche Anmeldungen bei Ihrem Account.

Wenn möglich sollte eine Zwei-Faktoren-Authentifizierung verwendet werden. Unterdessen bieten nicht nur Banken, sondern viele andere Online-Dienstleister diese Authentifizierungsmöglichkeit an. Sie dient dazu, die Identität des Nutzers zu überprüfen. Der zweite Faktor erfolgt meist durch den Einsatz von mobilen Geräten: Es werden Codes per Push-Benachrichtigung zu den Smartphones gesendet, ein QR-Code muss auf dem Bildschirm gescannt werden oder eine App zeigt einen Code an.

☞ Checkliste:

- □ Überprüfen Sie Ihre Logins hinsichtlich der erwähnten Regeln.
- □ Aktivieren Sie, falls vorhanden, die Zwei-Faktoren-Authentifizierung.