Leitfaden
Eigene Infrastruktur

Unabhängig davon, ob Sie einen eigenen Server betreiben oder ob Ihre gesamte Infrastruktur von Ihrem IT-Partner für Sie gehosted und betreut wird: Gewisse Geräte befinden sich nach wie vor bei Ihnen. Was es zu beachten gibt, können Sie diesem Leitfaden entnehmen.

1. Unverschlüsselte Festplatten

Falls Sie Notebooks im Einsatz haben und Daten lokal auf diesen Geräten speichern, ist es empfehlenswert, die Festplatten zu verschlüsseln, um die sensible Daten zu schützen und zu vermeiden, dass sie in fremde Hände gelangen, beispielsweise bei Verlust oder Diebstahl der Hardware. Zur Entschlüsselung der Festplatte wird ein Passwort benötigt. Falls Sie keine sensiblen Daten lokal auf ihrem Notebook oder Büro-PC speichern, sondern diese ausschliesslich bei Ihrem IT-Anbieter oder in der Cloud speichern, ist keine Verschlüsselung notwendig. Sollten Sie aber Dateien lokal speichern, ist eine Festplattenverschlüsselung angezeigt.

Falls Sie eine eigene Serverinfrastruktur betreiben, empfehlen wir Ihnen, diese von eine Sicherheitsspezialisten überprüfen zu lassen.

☞ **Checkliste:**

- □ Prüfen Sie mit Ihrem IT-Partner, ob Sie Daten lokal auf Ihrem PC oder Notebook speichern. Beauftragen Sie ihn gegebenenfalls mit der Verschlüsselung der Harddisk.

2. Bildschirmschoner / PC sperren

Computer und Monitore sollten, wenn sie unbeaufsichtigt sind, mit einem Bildschirmschoner gesperrt werden. Positionieren Sie ausserdem Ihren Bildschirm so, dass niemand die Daten sehen kann.

☞ **Checkliste:**

- □ Aktivieren Sie den Bildschirmschoner manuell, sobald Sie Ihren Arbeitsplatz verlassen.
- □ Stellen Sie den Bildschirmschoner bei allen Mitarbeitenden auf Aktivierung nach Ablauf von 5 Minuten ein.

3. Monitor mit Sichtschutz

Sobald Dritte freien Blick auf Monitore haben, sind die Daten nicht mehr ausreichend geschützt (Visual Hacking). Dies kann bei der Verwendung von Notebooks im öffentlichen Verkehr der Fall sein, aber auch, wenn Bildschirme etwa durch Fensterfronten, Glastüren oder in gemeinsam genutzten Büros mit Publikumsverkehr einsehbar sind. Durch das Umpositionieren von Bildschirmen und die Verwendung von Sichtschutzfolien können die Daten angemessen geschützt werden.

☞ **Checkliste:**

- □ Überprüfen der Einsehbarkeit Ihrer Bildschirme durch Fenster usw. und allenfalls neu positionieren.
- □ Notebooks und Tablets mit Sichtschutzfolien ausstatten.

4. 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 Prozent 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 ersetzt werden müssen.

5. Verschlüsseltes WLAN / Gäste-WLAN

Offene WLAN-Netze sind durch Angriffe von Hackern besonders stark gefährdet. Um interne Geschäftsdaten zu schützen ist es notwendig, mit einer privaten virtuellen Netzwerkverbindung (VPN) zu arbeiten. Denn selbst wenn es einem Hacker gelingt die Verbindung abzufangen, werden die Daten hochverschlüsselt bleiben. Mit einem Gäste-WLAN können Unternehmen den Kunden-Zugang zum Internet gewähren, ohne dass die Sicherheit des Heimnetzes verletzt wird. Da die beiden Netzwerke voneinander getrennt sind, fängt die Firewall des Routers Viren ab, mit denen Geräte der Kunden infiziert sein könnten.

Arbeiten Sie im Homeoffice, achten Sie darauf, dass Sie Ihr WLAN mit einem starken Passwort schützen.

☞ Checkliste:

- □ Öffentliche WLAN-Netze meiden / WLAN deaktivieren, sobald es nicht mehr benötigt wird.
- □ Im öffentlichen WLAN-Netz mit einer privaten virtuellen Netzwerkverbindung (VPN) arbeiten.
- □ Separates, getrenntes Gäste-WLAN einrichten. Fragen Sie dazu Ihren IT-Partner.
- □ Im Homeoffice WLAN mit starkem Passwort schützen.

6. Nutzung von fremden USB-Sticks und Datenträgern

Bei der Nutzung von fremden USB-Sticks ist Vorsicht geboten, denn einer der ältesten Tricks von Hackern ist es, sich durch einen mit Mal- oder Spyware infiziertem USB-Stick Zugang zum Firmennetzwerk zu verschaffen. Hersteller bieten USB-Schlösser an, mit denen die USB-Eingänge an PC´s und Notebooks verriegelt werden können. Dabei handelt es sich um kleine Vorrichtungen, die in die USB Eingänge gesteckt werden können. Möglich ist auch, die USB Eingänge direkt durch die Software zu deaktivieren.

☞ Checkliste:

- □ Unbeaufsichtigte PC´s, zum Beispiel in Sitzungszimmern, mit USB-Schlössern sichern.

7. Unterwegs mit dem Notebook / Laptop

Auf Reisen gelangen vertrauliche Daten häufig in die Hände von Unberechtigten. Um dies möglichst zu vermeiden, sollten folgende Vorsichtsmassnahmen beachtet werden:

- Geräte niemals unbeaufsichtigt lassen.
- Sichtschutzfolie verwenden.

- Nicht mit ungesicherten WLAN-Netz online gehen.
- Vor der Reise ins Ausland über die Datenschutz-Risiken und Gepflogenheiten des Ziellandes informieren.
- Im Hotelzimmer niemals den Laptop / Notebook offen liegen lassen, sondern den Safe benutzen.
- Nur so wenige Daten wie möglich auf möglichst «leerem» Notebook / Laptop mitnehmen.
- Daten auf Harddisk verschlüsseln.