Leitfaden
E-Mail und Datenübermittlung

Ein besonderes Augenmerk sollte – neben dem Schutz der Daten auf Ihren Systemen – auf die elektronische Übermittlung von Daten und Informationen gelegt werden: Die Angriffsfläche auf dem Transportweg ist besonders gross. E-Mails und andere Übermittlungsdienste werden häufig benutzt, um in ein System eindringen zu können.

1. E-Mail Passwörter

Ein sicheres E-Mail-Passwort ist das A und O, um sich vor Hackern zu schützen. Nach wie vor gehören Passwörter wie «123456», «qwertz» und «hallo» zu den beliebtesten, obwohl allgemein bekannt ist, dass sichere 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.
- Falls möglich beim Login eine Zwei-Faktor-Authentifizierung nutzen.

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.

2. E-Mail-Verschlüsselung

Die E-Mail-Verschlüsselung ist ein wichtiges Thema im Bereich der Datensicherheit, besonders bei personenbezogenen Daten sowie vertrauliche Firmen- und Kundendaten. Beim Senden von vertraulichen Informationen bietet die Verschlüsselung zwischen den Endgeräten von Absender und Empfänger erhöhte Sicherheit. Es ist empfehlenswert, unternehmensübergreifend eine einheitliche E-Mail-Verschlüsselung umzusetzen.

☞ Checkliste:

- □ Festlegen, für welche E-Mails Verschlüsselungen verwendet werden sollen.
- □ Firmeninterner Leitfaden für Mitarbeitende bezüglich der E-Mail-Verschlüsselung.
- □ Unter Umständen einen externen IT-Dienstleister konsultieren, der sich um die E-Mail-Verschlüsselung kümmert.

3. Gefälschte E-Mails / Phishing

Beim Phishing handelt es sich um eine Angriffsmethode, bei der mit falschen E-Mails / Webseiten versucht wird, an Login- und Bankdaten zu gelangen. Es handelt sich um eine Betrugsform, bei der Personen verleitet werden, ihre Sicherheitsdaten, wie beispielsweise die Anmelde-ID oder das Passwort freizugeben durch täuschend echt aussehende Inhalte von seriösen Unternehmen oder Institutionen. Am häufigsten wird mit beliebten Dienstanbietern gephisht; in der Schweiz sind oft die Unternehmen Migros, SBB, Swisscom, UBS und die Post betroffen.

Erkennungsmerkmale von Phishing:

- Sprachliche Mängel
- Daten werden verlangt.
- Anhänge und Links
- Versprechungen, die zu gut sind, um wahr zu sein.

☞ Checkliste:

- □ Schulungen für Mitarbeitende, um sie für IT-Sicherheit zu sensibilisieren.
- □ Posteingang sauber und übersichtlich behalten: Je weniger E-Mails darin enthalten sind, desto eher behält man den Überblick.
- □ Sparsame Datenfreigabe: Je weniger Informationen man online freigibt, desto weniger Chancen haben Phisher.
- □ Phishing melden: Sobald man eine Phishing-Nachricht erhält, die Nachricht melden und den Absender blockieren.
- □ Passwortmanager: Für jeden Dienst ein anderes Passwort verwenden, so können die anderen Konten gerettet werden, falls ein Konto durch eine Phishing-Attacke gehackt wird.
- □ Jedes E-Mail, auch wenn von bekannten Absendern, sehr kritisch hinterfragen und bei Bedarf beim Absender nochmals nachfragen. Im Zweifelsfall lieber löschen und nicht auf Links klicken.
- □

4. Viren / Malware im Anhang

Seit mehreren Jahren gehören E-Mails zu den wichtigsten Kommunikationsmitteln. Leider werden die meisten Computerviren auch über E-Mail-Anhänge verbreitet, daher ist beim Öffnen von E-Mail-Attachments Vorsicht geboten.

☞ Checkliste:

- □ Virenschutz: Antivirenschutzprogramme, welche bereits im Betriebssystem von Windows (Defender) und macOS (XProtect) enthalten sind, besitzen meist eine relativ hohe Qualität und bieten einen hohen Schutz gegenüber schädlichen Eindringlingen.
- □ Dokumente mit den folgenden Datei-Endungen sind risikobehafteter als andere:
  - **Textdateien doc/.docx/.xls/xlsx/.ppt/.pptx:** Office-Dokumente in E-Mail-Anhängen können Makroviren enthalten, daher sollten sie nur geöffnet werden, wenn die Identität des Absenders bekannt ist.
  - **Bilddateien jpg.:** Diese Endung kann als Deckmantel für Programm-Dateien genutzt werden, deshalb ist es wichtig, dass das E-Mail-Programm die Dateiendung anzeigt.
  - **Komprimierte Dateien *zip/rar*:** Bei komprimierten Dateien können Viren beim Entpacken aktiv werden, daher sollte auch hier der Absender bekannt sein.
  - **PDF-**Dateien sind zwar meist harmlos, können aber auch Computerviren enthalten. Es ist also auch bei diesem relativ sicheren Dateityp wichtig, dass Sie den Absender verifizieren.

5. Sichere Datenübermittlung / Filesharing

Grössere Dateien und grössere Datenmengen können nicht mittels E-Mail verschickt werden. Statt USB-Sticks werden heute hauptsächlich Filesharing-Dienste genutzt. Je nach Art der Daten, die Sie übertragen möchten, eignet sich nicht jeder Filesharing-Anbieter. Übermitteln Sie Personendaten, ist zu beachten, in welchen Ländern die Server des Anbieters stehen.
Zum sicheren Teilen von Daten empfehlen wir Schweizer Anbieter, wie z.B. die Secure File-Transferlösung von SecureSafe, einem Partner von TREUHAND|SUISSE, oder den Large File Transfer (LFT) von IncaMail der Schweizerischen Post. Der Large File Transfer (LFT) von IncaMail kann auch im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV, SR 172.021.2), in Zivil- und Strafprozessen und in Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV, SR 272.1) genutzt werden.