Soll man E-Mails verschlüsseln?

E-Mails sind aus dem geschäftlichen Alltag nicht mehr wegzudenken. Aber den wenigsten Nutzern ist bewusst, wie einfach zugänglich unverschlüsselte Nachrichten für Dritte sind. Wer vertrauliche Daten oder besonders schützenswerte Personendaten handhabt, muss Vorsicht walten lassen.

Boris Blaser

Steigen wir mit einem Beispiel ein: Ein Mitarbeiter im Team von Garagist Peter Huber fällt krankheitshalber für ein paar Wochen aus. Die Abrechnung über das Krankentaggeld, die er von der Versicherung erhält, schickt Huber an seinen Treuhänder weiter, der die Lohnabrechnungen erstellt. Gleichzeitig verlangt Huber vom betroffenen Mitarbeiter, der immer noch krankgeschrieben ist, ein aktuelles Arztzeugnis für den laufenden Monat. All das wird schnell und bequem per E-Mail abgewickelt. Warum das zum Problem werden kann? Weil sich E-Mails bezüglich Vertraulichkeit auf der Stufe von Postkarten bewegen.

Unverschlüsselte E-Mails sind etwa so vertraulich wie Postkarten. Wer will, kann mitlesen. stock.adobe.com/German

Jeder kann mitlesen

Unverschlüsselte E-Mails kann unterwegs jeder mitlesen, der das will. Das Risiko ist umso grösser, als E-Mails nicht immer direkt vom Versender zum Empfänger gelangen. Vielmehr kann es sein, dass sie durch zahlreiche Server und sogar Länder geleitet werden. Kurz: Man sollte – als Unternehmen wie als Privatperson – reiflich überlegen, bevor man vertrauliche Angaben per E-Mail übermittelt. Spezielle Vorsicht ist geboten, wenn «besonders schützenswerte Personendaten» im Spiel sind. Als solche gelten neben Gesundheitsdaten wie sie im obigen Beispiel vorkommen auch Angaben zu Religion, strafrechtlicher Verfolgung, Gewerkschaftszugehörigkeit, sexueller Orientierung oder biometrische Daten. Wenn solche Daten oder andere vertrauliche Daten per E-Mail an externe Empfänger verschickt werden, müssen sie speziell geschützt werden. In Grossunternehmen, die sich mit viel Aufwand für die Anforderungen der Datenschutzgesetzgebung fit gemacht haben, gehört die verschlüsselte Übermittlung von vertraulichen Daten und schützenswerten Personendaten heute zum Standard. Das zeigt sich übrigens auch im Beispiel von Garagist Peter Huber: Die Abrechnung über das Krankentaggeld hat ihm seine Versicherung via das hauseigene «Secure Mail» zugestellt; für den Zugriff darauf hat er von der Versicherung ein entsprechendes Passwort erhalten. Im Gegensatz zu grösseren Firmen machen sich kleinere Betriebe weniger Gedanken darüber, welche Risiken sie mit dem Austausch von unverschlüsselten E-Mails potenziell eingehen.

Boris Blaser ist Vorstandsmitglied des Schweiz. Treuhänderverbands TREUHAND|SUISSE, Sektion Zürich

Nachricht oder Anhang sichern

Wenn Sie als Gewerbebetrieb Ihre Risiken und den geeigneten Lösungsansatz ausloten möchten, folgender freundschaftlicher Tipp: Technisch gesehen ist E-Mail-Verschlüsselung etwas umständlich zu bewerkstelligen; idealerweise wenden Sie sich mit diesem Anliegen an Ihren IT-Partner. Mit ihm können Sie auch die Frage besprechen, welche Stufe der Verschlüsselung und welche Methode für Ihre Bedürfnisse passend sind. Als Alternative oder Übergangslösung kann man in Erwägung ziehen, zumindest vertrauliche Mail-Anhänge auf sicherem Weg zu übermitteln. Im einleitenden Beispiel wären dies die Abrechnung über das Krankentaggeld oder das Arztzeugnis. Solche Dokumente kann man auf einem sicheren und allgemein zugänglichen Portal für Datentransfer speichern (Upload) und dem Empfänger direkt aus diesem Portal heraus – also gesichert – einen Link mit einem Passwort zum Herunterladen (Download) schicken. Theoretisch kann man auch das Dokument selber, beispielsweise eine PDF-Datei, mit einem Passwort schützen, aber dieser Schutz gilt als nicht besonders sicher.

Die Risiken?

Die E-Mail-Verschlüsselung minimiert das Risiko, dass Personendaten und andere sensitive Informationen an unbefugte Dritte gelangen. Unternehmen sind gut beraten, wenn sie prüfen, welche Daten sie per E-Mail versenden. Handelt es sich um besonders schützenswerte Daten, sollten sie sich mit dem Thema Verschlüsselung beschäftigen. Denn wenn es zu einer Verletzung der Datensicherheit kommt und die Daten in falsche Hände geraten (z. B. durch einen Hackerangriff), können die Folgen für das Unternehmen beziehungsweise den Verantwortlichen und die Betroffenen sehr weitreichend sein. Wenn das Risiko für die betroffenen Personen als erheblich einzustufen ist, muss der Vorfall zudem ohne Verzögerung dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden.