

VON DER DIGITALEN POSTKARTE ZUR VERSCHLÜSSELTEN NACHRICHT – E-MAILS UND ANHÄNGE SICHER VERSENDEN

Datenschutzbeauftragte und Sicherheitsbeauftragte erklären häufig, dass eine unverschlüsselte E-Mail ähnlich sicher sei wie eine Postkarte. Sprich, jeder, der die Karte in die Hände bekommt, kann den Inhalt lesen. Nun würde vermutlich kaum jemand auf die Idee kommen, seine Gehaltsdaten, Zugangsdaten oder vertrauliche Unternehmensdaten per Postkarte zu versenden.

Bei E-Mails ist das Risiko häufig nicht so offensichtlich und entsprechende Informationen werden somit per E-Mail versendet. Infolgedessen kommt es regelmäßig zu Datenschutz- und Sicherheitsvorfällen, z. B. wenn eine E-Mail mit den Gehaltsabrechnungen versehentlich nicht an die Steuerberaterin gesendet wird, sondern an eine Kundin oder Mitarbeiterin mit ähnlichem Namen oder ähnlicher E-Mail-Adresse.

Der Briefumschlag im Internet – die Transportverschlüsselung

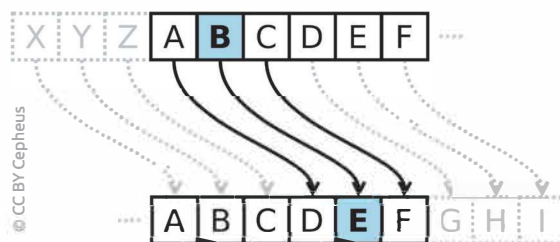
Wenn vertrauliche Daten auf dem Postweg versendet werden, wird die Nachricht einfach in einen Briefumschlag gepackt und losgeschickt. Sinnbildlich gibt es diesen Briefumschlag mit der Transportverschlüsselung (TLS/SSL) auch bei E-Mails. Im Gegensatz zum Brief, bei dem der Briefumschlag vom Anfang bis zum Ende verschlossen bleibt, wird dieser „digitale Briefumschlag“ auf dem Weg auch gewechselt. Kommt ein E-Mail-Programm zum Einsatz, wird die E-Mail im Regelfall auf dem Weg zwischen absendendem Computer und E-Mail-Server des Absenders erstmalig verschlüsselt. Auf dem E-Mail-Server des Absenders wird die E-Mail dann z. B. wieder verschlüsselt und im besten Fall verschlüsselt dem E-Mail-Server des Empfängers zugestellt, der die E-Mail dann im Klartext wieder zum Abruf bereithält. Der Vorteil der Transportverschlüsselung

ist, dass die Benutzer kaum etwas davon mitbekommen, da die beteiligten Server die Verschlüsselung untereinander regeln. Deshalb ist die Transportverschlüsselung selbst bei privaten Nutzern im Regelfall schon seit einiger Zeit üblich.

Der Nachteil ist, dass die Nachricht nur auf dem Transportweg verschlüsselt ist, wobei es selbst hier Ausnahmen geben kann. Beim Absender und Empfänger wird eine entsprechende Nachricht immer im Klartext angezeigt. Wobei der Empfänger auch versehentlich falsch gewählt sein kann.

Geheime Botschaften mit der Ende-zu-Ende-Verschlüsselung

Wollen Absender und Empfänger Nachrichten so austauschen, dass kein Dritter Kenntnis vom Inhalt bekommt, muss diese Nachricht durchgängig – von Ende zu Ende – verschlüsselt werden. Schon der römische Feldherr Gaius Julius Caesar soll seine militärische Korrespondenz verschlüsselt verschickt haben. Nach Überlieferungen nutzte er dafür eine Verschiebung des Alphabets um 3 Buchstaben, womit aus A der Buchstabe D wurde und aus dem Buchstaben B der Buchstabe E usw.



Einmal abgesehen davon, dass diese Art von Verschlüsselung heute ziemlich schnell geknackt wäre, bleibt das Problem, dass Absender und Empfänger sich auf ein gemeinsames Verfahren und mindestens einen gemeinsamen Schlüssel, in diesem Fall „Verschiebe um 3 Buchstaben“, einigen müssen. Zudem ergeben sich viele weitere >

- > Herausforderungen, z. B. die Übertragung des Schlüssels, die sichere Aufbewahrung des Schlüssels bei den Kommunikationspartnern und zumeist die Verwaltung vieler entsprechender Schlüssel, da häufig mit einer Vielzahl an Personen E-Mails ausgetauscht werden.

Öffentlicher und privater Schlüssel

Um das Problem des Schlüsselaustauschs zu beheben und auch die Verwaltung der Schlüssel zu vereinfachen, kann das sogenannte Public-Key-Verschlüsselungsverfahren zum Einsatz kommen. Hierbei erzeugt jeder Kommunikationspartner einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird, ganz dem Namen entsprechend, öffentlich zugänglich gespeichert. Möchte nun jemand eine E-Mail an diesen Empfänger schicken, verschlüsselt er diese Nachricht mit dem öffentlichen Schlüssel des Empfängers. Nur dieser kann dann die Nachricht mit seinem privaten Schlüssel wieder entschlüsseln.

In der analogen Welt entspricht dies in etwa dem Briefkasten, in dem jeder einen Brief einwerfen kann, aber nur der hierzu Berechtigte den Schlüssel zum Öffnen des Briefkastens hat.

Obwohl beispielsweise mit OpenPGP sogar eine kostenfreie Lösung für die Ende-zu-Ende-Verschlüsselung von E-Mails zur Verfügung steht, werden bis heute kaum entsprechend verschlüsselte E-Mails ausgetauscht.

Der Mittelweg: zumindest Anhänge absichern

Durch die große Anzahl an E-Mails geschehen auch häufig Pannen. Da die Transportverschlüsselung die E-Mails nur auf dem Transportweg verschlüsselt und die Ende-zu-Ende-Verschlüsselung sich bislang noch nicht durchsetzen konnte, gilt es, die Sicherheit so gut wie möglich zu erhöhen. Eine Möglichkeit besteht darin, den Empfängern sensible Daten über einen verschlüsselten Anhang zukommen zu lassen. Wenn möglich, erhält der Empfänger noch

nicht einmal diesen Anhang per E-Mail, sondern lediglich einen Link auf die Datei in einem abgesicherten Online-Speicher. Der Zugriff auf die Datei sollte zudem mit einem Kennwort geschützt werden.

Mit wenigen Klicks Anhänge kostenfrei verschlüsseln

Neben professionellen Lösungen gibt es auch Tools für den gelegentlichen Bedarf im Unternehmen bzw. für private Zwecke, um Anhänge zu verschlüsseln. Ein kostenfreies und einfach zu bedienendes Tool ist 7-Zip. Der ursprüngliche Zweck des Programms ist es, Dateien zu komprimieren, also kleiner zu machen. Optional bietet das Tool aber auch die Möglichkeit, den Anhang zu verschlüsseln.

Nach der Installation reichen ein einfacher Rechtsklick auf die zu verschlüsselnde Datei (Bild 1, Punkt 1) und die Auswahl 7-Zip (Bild 1, Punkt 2) sowie „Zu einem Archiv hinzufügen ...“ (Bild 1, Punkt 3).

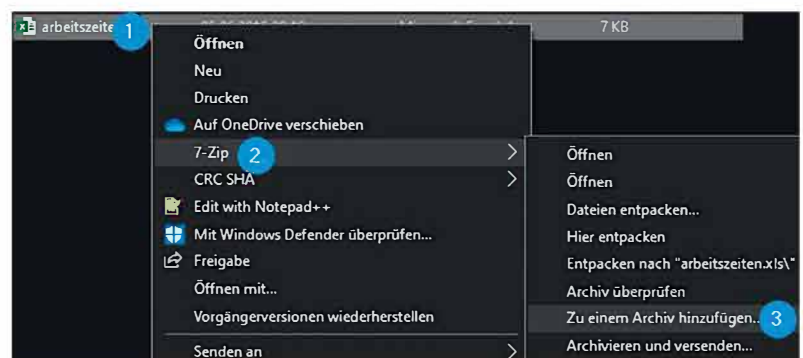


Bild 1: Datei mit wenigen Klicks verschlüsseln

Da das ZipCrypto-Verfahren wohl einfacher zu knacken ist, sollte im Anschluss das Verfahren „AES-256“ ausgewählt und ein möglichst langes, komplexes Passwort eingegeben werden. Danach kann der Anhang dann für den Empfänger bereitgestellt oder via E-Mail an diesen gesendet werden.

Ohne die Eingabe eines Passworts kann der Empfänger lediglich den Inhalt der Archiv-Datei einsehen. Zum Öffnen der Dateien ist dann das im Vorfeld festgelegte Passwort erforderlich. Das erforderliche Passwort sollte möglichst über einen anderen Weg, z. B. per Anruf, SMS etc., dem Empfänger der Datei übermittelt werden.