E-Mail-Sicherheit

E-Mail-Kommunikation, die nicht gesichert abläuft, ist vergleichbar mit dem Austausch von Postkarten. Jeder Knoten im Internet, der zur Auslieferung einer ungesicherten E-Mail verwendet wird (und davon gibt es viele), kann den Inhalt der E-Mail lesen. Zwar sollten diese Knoten – Server oder Router – so programmiert sein, dass die E-Mail einfach weiter geleitet wird, aber es ist i.d.R. wenig über die Besitzer, die Sicherheit und damit die Vertrauenswürdigkeit dieser Server und Router bekannt. So können diese gehackt worden sein oder Hintertüren enthalten, sodass automatisch alle E-Mails auch an Dritte (Kriminelle oder Geheimdienste) gelangen.

Ein weiteres Problem von ungesicherten E-Mails ist, dass der Empfänger nicht weiß, von wem die E-Mail wirklich kommt. Dass der Absender angela.merkel@bund.de lautet, bedeutet nicht, dass die E-Mail von Frau Merkel kommt. Für diese Angriffe ist es nicht einmal erforderlich, Zugriff auf die zuvor erwähnen Knoten zu haben. Angriffe dieser Art werden bei Social Engineering-Angriffen verwendet; die verbreitetste Form ist das Phishing: E-Mails, die beispielsweise vorgeben, von Amazon zu kommen und dem Nutzer Zugangsdaten entlocken.

Da heutzutage fast die komplette Kommunikation im privaten und Unternehmenskontext elektronisch abläuft, ist der Einsatz von sicherer E-Mail-Kommunikation längst überfällig. Was heißt aber sichere E-Mail-Kommunikation? Es gibt zwei Modelle, die sich hinsichtlich ihrer Sicherheit und Benutzbarkeit unterscheiden: Im benutzbareren Modell wird eine sichere Kommunikation zwischen den verschiedenen Komponenten (Endgeräten und E-Mail-Servern) zugesichert und i.d.R. mittels TLS realisiert. Hier wird sichergestellt, dass die Knoten zwischen diesen Komponenten die E-Mails nicht mehr lesen können (die E-Mail-Server können dies allerdings nach wie vor). Wird eine E-Mail an einen E-Mail-Server außerhalb dieses Systems geschickt, ist für Empfänger und Sender nicht klar, ob diese Zusicherung noch gilt. Dieses Modell wird oft innerhalb von Unternehmen und Behörden verwendet. Im privaten Kontext werben die Betreiber von „E-Mail made in Germany" mit diesem Modell. Ein Schutz der Authentizität ist in diesem Modell nicht fest verankert, wird aber teilweise angeboten, wenn eine Nachricht über die E-Mail-Server selbst verschickt wird. Da die E-Mail Kommunikation hier nur innerhalb des Systems (und das auch nur unter der Annahme der Vertrauenswürdigkeit der Anbieter) gesichert ist, ist dieser Ansatz einfach zu verwenden, weil der Schutz automatisch erfolgt und der Empfänger lediglich auf die Authentizität des Absenders achten muss.

Das zweite Modell ist die klassische Ende-zu-Ende-Absicherung der Kommunikation. Weil hier nur die Geräte von Empfänger und Sender auf die Inhalte der E-Mail zugreifen können, müssen sich beide Kommunikationspartner eine entsprechende Software auf ihren Geräten installieren und jeder sich kryptographische Schlüssel generieren. Die Schlüssel werden verwendet, um die E-Mail zu verschlüsseln und zu signieren. Wie sicher der Empfänger sein kann, dass die Nachricht wirklich von dem Sender ist, hängt von verschiedenen Faktoren ab. Zwar kennt dieses Modell keine Systemgrenzen (wie das erste), jedoch sind derzeit viele Lösungen noch nicht miteinander kompatibel. Die schlechte Benutzbarkeit der verschiedenen Lösungen wurde in der Vergangenheit oft kritisiert. Anders als im ersten Modell kann hier die Sicherheitstechnik allerdings nicht im Hintergrund „aufgeschaltet" werden. Die Bedienbarkeit selbst ist aber nicht der einzige Grund, warum die Ende-zu-Ende-Absicherung der E-Mail-Kommunikation kaum verbreitet ist. Andere Gründe sind die fehlende Awareness, das mangelnde Verständnis für die verschiedenen Schlüssel und die fehlende Interoperabilität. Hinsichtlich der Sicherheit müssen die Kommunikationspartner nun nicht mehr den E-Mail-Servern vertrauen, sondern der Software, die sie auf ihren Geräten einsetzen.

In diesem Schwerpunktheft gehen die Autoren auf verschiedene Aspekte der sicheren E-Mail-Kommunikation ein.

Melanie Volkamer