Sichere E-Mail-Kommunikation ist wichtiger denn je

Der zunehmende Versand vertraulicher Dokumente via E-Mail statt per Post und die immer häufigeren Cyberattacken, die direkt auf E-Mail-Nutzerinnen und -Nutzer abzielen, machen die Verschlüsselung und elektronische Signierung des E-Mail-Verkehrs zu einem Muss – was jedoch längst nicht alle Unternehmen erkannt haben.

Man weiss es eigentlich: Cyberattacken nehmen tagtäglich zu, die Angriffe werden immer raffinierter, und eines der wichtigsten Einfallstore ist die E-Mail-Kommunikation. Cyberkriminelle arbeiten mit Methoden wie Phishing und Social Engineering, um die Echtheit von Inhalten und Absendern vorzutäuschen, die Empfänger zur Preisgabe vertraulicher Informationen zu verleiten und über infizierte Webseiten Schadcode ins Firmennetzwerk einzuschleusen.

E-Mail ungebrochen populär

Gleichzeitig hat E-Mail-Kommunikation trotz neuer Kommunikationsformen wie Instant Messaging und Kollaborationslösungen wie Teams, Zoom, Slack & Co. keineswegs an Bedeutung verloren – ganz im Gegenteil: Immer häufiger gelangen wichtige und vertrauliche Dokumente wie etwa Verträge, Offerten oder Rechnungen, die früher per Post verschickt wurden, per E-Mail an die Kunden und Geschäftspartner. Solche Dokumente enthalten oft personenspezifische Daten, die gemäss den neueren gesetzlichen Vorschriften wie der EU-DSGVO und künftig auch dem neuen Schweizer Datenschutzgesetz besonders sensibel sind und vor unbefugtem Zugriff geschützt werden müssen. Sonst drohen eventuell empfindliche Bussen, und die Reputation leidet.

Dennoch erfolgt die E-Mail-Kommunikation in vielen Unternehmen nach wie vor unverschlüsselt und unsigniert. So sind E-Mails mit einer offenen Postkarte vergleichbar, statt die Integrität und Authentizität eines eingeschriebenen Briefs zu bieten. Wer also sichergehen will, dass eine E-Mail unverfälscht ankommt und tatsächlich vom angegebenen Absender stammt, kommt um eine E-Mail-Sicherheitsplattform nicht herum, die Verschlüsselung und elektronische Signierung der Meldungen kombiniert und so einfach wie möglich in Betrieb zu nehmen und zu bedienen ist. Denn komplizierte Verschlüsselungslösungen mit schlechter Usability führen dazu, dass sie in der Praxis dann doch nicht genutzt werden.

Die ideale E-Mail-Security

Die gebotene Einfachheit einer E-Mail-Sicherheitslösung lässt sich am besten durch ein Secure E-Mail Gateway realisieren, das als zentrale Instanz für den gesamten E-Mail-Verkehr zwischen dem Firmennetzwerk und dem Internet fungiert und das manuell aufwändige Schlüssel- und Zertifikatsmanagement, das Voraussetzung für die Verschlüsselung und Signierung der Meldungen ist, möglichst vollständig automatisiert. Dabei sollten alle gängigen Standards unterstützt werden: OpenPGP, TLS, SSL sowie S/MIME für die Signatur der E-Mails. Ein solches Gateway kann entweder als Hardware- oder virtuelle Appliance oder aber im As-a-Service-Modell als Cloud-Dienst realisiert werden.

Ein zentrales Gateway ermöglicht darüber hinaus die sehr bequeme Domainverschlüsselung, die den Verkehr zwischen den Gateways der eigenen Firma und der unterschiedlichen Geschäftspartner ohne jedes Zutun der Absender und Empfänger vollautomatisch und ohne Software-Installation auf den Endgeräten verschlüsselt und signiert. Doch auch Empfänger, die nicht über eine eigene Verschlüsselungslösung verfügen, sollten in den Genuss authentischer und verschlüsselter Kommunikation kommen, für die nur ein E-Mail-Client und ein Browser benötigt werden. Die fortschrittlichsten E-Mail-Security-Lösungen verfügen über die dafür benötigte Technologie: Das Secure E-Mail Gateway generiert die erforderlichen Schlüssel ad hoc und schickt die verschlüsselte Meldung an den Empfänger, der sie mit einem separat über einen Kanal wie SMS übermittelten Passwort entschlüsseln und auch verschlüsselt beantworten kann.

DER AUTOR

Stefan Klein
Gründer und CEO, Seppmail
seppmail.ch

Den Beitrag finden Sie auch online
www.netzwoche.ch