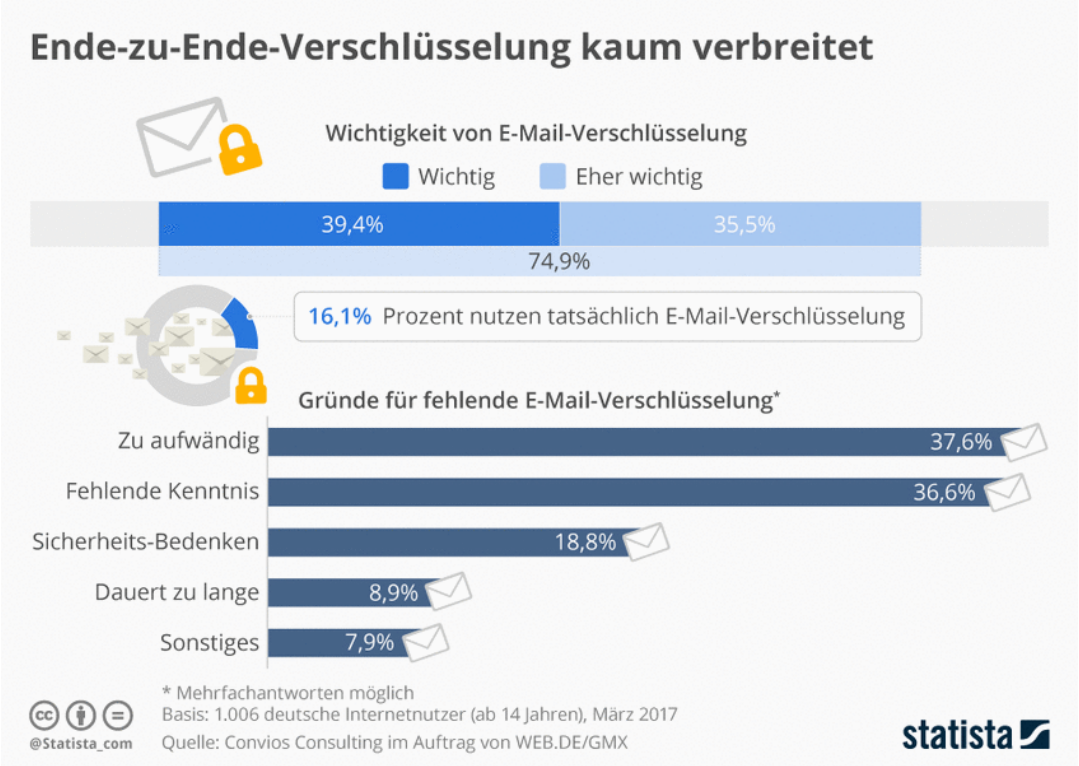
Mit diesen Tipps gelingt die E-Mail-Verschlüsselung

Aufgrund des immer noch geringen Einsatzes von E-Mail-Verschlüsselung haben wir einige hilfreiche Tipps zur Umsetzung für Sie zusammengefasst.

E-Mail-Verschlüsselung ist schon lange ein Thema und war in den letzten Jahren auch bei uns bspw. im Hinblick auf S/MIME immer wieder im Fokus. Gerade im Zuge großer Hackerangriffe oder E-Mail-Affären, wie der von Hillary Clinton im US-Wahlkampf, wird das Thema wieder populär. Die E-Mail-Verschlüsselung ist in der heutigen Zeit nicht mehr aufwendig, dennoch nutzen immer noch sehr wenige den Service. Den meisten ist zwar bekannt, dass es dadurch zu Problemen und Vertrauensverlusten kommen kann, die Umsetzung von Maßnahmen in dieser Richtung ist laut einer aktuellen Studie jedoch mangelhaft. Gerade im Zuge der neuen Datenschutzgrundverordnung (DSGVO) ist das Thema wieder hoch brisant, ein Fehlen kann zu hohen Strafen führen. Auch im Hinblick auf die immer noch steigende Bedeutung der E-Mail-Kommunikation lohnt sich ein Blick auf die Sicherheit.

Inhalts- und Transportverschlüsselung

Auch wenn die Verschlüsselung von E-Mails heute relativ einfach umsetzbar ist, sollte man einige Dinge beachten. Die Computerwoche hat dazu Anfang des Jahres einige Tipps vorgestellt, auf die im Folgenden näher eingegangen werden soll. Demnach können oft schon die einfachen Standards, wie SSL/TLS oder S/MIME bzw. (Open)PGP einen guten Schutz bieten. Bei SSL bzw. TLS handelt es sich um Transportverschlüsselungen. Hier werden die übertragenen Daten auf verschiedenen Übermittlungsabschnitten verschlüsselt, auf den einzelnen Servern sind sie jedoch in Klartext gespeichert – das stellt ein potenzielles Risiko dar. Bei S/MIME oder PGP werden die Inhalte der Mail verschlüsselt, die Metadaten bleiben hingegen unverschlüsselt und somit im Grunde lesbar – also z. B. der Absender, der Empfänger oder der Betreff der Nachricht. Am sichersten ist die Verwendung einer Kombination aus Transport- und Inhaltsverschlüsselung. Damit werden die Risiken der jeweiligen Verschlüsselungslösung minimiert. Leider ist die Ende-zu-Ende-Verschlüsselung noch immer kaum verbreitet:



Quelle: Statista

Anpassung an Bedürfnisse und individuelle Begebenheiten

Die Auswahl an Lösungen ist natürlich groß. Abgesehen von den eigenen Bedürfnissen, an die das System angepasst werden sollte, ist es ratsam, auf ein möglichst unabhängiges System zu setzen. Dabei sollte man nicht nur die Kommunikation gegenüber Dritten im Blick haben, sondern auch den E-Mail-Verkehr im eigenen Unternehmen schützen. Dies ist in der Regel ebenfalls einfach über Standards im jeweiligen E-Mail-Client durchführbar. Neben der internen Kommunikation gibt es weitere Fälle, bei denen der erste Gedanke nicht unbedingt der Sicherheit gilt – denn auch viele Apps nutzen beispielsweise diesen Weg der Kommunikation. Werden größere Anhänge angefügt, sollte auch hier beachtet werden, dass diese in die Verschlüsselungslösung integriert sind. Zudem ist darauf zu achten, dass die großen Anhänge die Mailserver nicht überlasten.

Mobile Endgeräte und weitere Sicherheitsvorkehrungen

Da die Nutzung mobiler Endgeräte weiter steigt, ist es ratsam, auch hier auf E-Mail-Verschlüsselung zu achten. Besonders Unternehmen, deren Mitarbeiter mit Firmen-Handys ausgestattet sind, stehen hier in der Pflicht, sofern sie keine bösen Überraschungen erleben wollen. Am Ende bleibt natürlich als wichtigstes Kriterium die Anwenderfreundlichkeit für die Nutzer. Eine wirklich gute und sichere Lösung nützt wenig, wenn sie von den Personen nicht einfach und selbsterklärend verwendet werden kann. Verschlüsselung ist aber nicht alles. Zusätzlichen Schutz bietet weitere Sicherheitssoftware, wie bspw. ein Virenscanner. Auch die Archivierung der Mails spielt eine wichtige Rolle. Um die elektronischen Nachrichten später wieder zu finden, sollte das Archivsystem auf die E-Mail-Inhalte im Klartext zugreifen können.

Das sollten Sie in Bezug auf E-Mail-Verschlüsselung beachten:

- Standards verwenden: am besten eine Kombination aus Transport- und Inhaltsverschlüsselung, also z.B. SSL kombiniert mit S/MIME
- auch die interne und mobile E-Mail-Kommunikation verschlüsseln
- weitere Sicherheitssoftware installieren (z.B. Virenscanner)
- Nutzerfreundlichkeit und Archivierung im Auge behalten

E-Mail-Verschlüsselung ist kein Hexenwerk: Mit den richtigen Tipps kann man schnell einen grundsätzlichen Schutz für seine elektronische Kommunikation schaffen. Was in diesem Bereich noch fehlt ist das Problembewusstsein: Ein Leck in der E-Mail-Kommunikation kann einem Unternehmen großen Schaden zufügen, wenn beispielsweise geheime Dokumente an die Öffentlichkeit gelangen. Deshalb sollte man sich nicht nur bei externer Kommunikation absichern, sondern auch intern die vorhandenen Möglichkeiten nutzen. In der heutigen Zeit empfiehlt es sich zudem, ein besonderes Augenmerk auf die Verschlüsselung der Kommunikation bei mobilen Endgeräten zu legen.