Datenschutzkonferenz

Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand

Die Datenschutzkonferenz erarbeitet derzeit Empfehlungen zur datenschutzkonformen E-Mail-Kommunikation. Daher stehen die folgenden Ausführungen unter dem Vorbehalt späterer Anpassungen an die Empfehlungen.

Wie ist die Datenschutz-Grundverordnung (DS-GVO) in Bezug auf den unverschlüsselten Versand von E-Mails zu interpretieren?

E-Mails enthalten zusätzlich zu den Inhaltsdaten (d.h. dem Text der Mail und etwaigen Anhängen) auch Metadaten wie Absender und Empfänger, das Datum und den Betreff.

Sowohl Inhalts- als auch Metadaten können personenbezogene Daten beinhalten. Daher sind bei der datenschutzrechtlichen Beurteilung beide Datenarten zu berücksichtigen.

Bei der Übermittlung von E-Mails ist grundsätzlich zwischen einer Verschlüsselung auf Inhaltsebene und einer Verschlüsselung auf Transportebene zu unterscheiden.

Inhaltsebene

Für die Verschlüsselung des Textes einer E-Mail sowie von Anhängen kommen in erster Linie die Standards S/MIME und OpenPGP infrage. Beide Standards unterstützen darüber hinaus digitale Signaturen, um Manipulationen auf dem Übertragungsweg entdecken zu können.

Mit S/MIME und OpenPGP ist eine Ende-zu-Ende-Verschlüsselung möglich, d.h. die Nachricht wird auf dem System des Absenders verschlüsselt und auf dem System des Empfängers entschlüsselt und liegt auf dem Übertragungsweg niemals im Klartext vor.

Die Metadaten werden von der Inhaltsverschlüsselung jedoch nicht erfasst, sie liegen auf den an der Übertragung beteiligten Servern im Klartext vor.

Transportebene

Bei einer Verschlüsselung auf Transportebene werden sowohl Meta- als auch Inhaltsdaten auf der Verbindung zwischen Mail-Client und Server bzw. zwischen verschiedenen Mail-Servern verschlüsselt. Dadurch ist sichergestellt, dass die E-Mail während des Transports über unsichere Netze wie dem Internet von Dritten nicht mitgelesen werden kann. Auf den beteiligten Mail-Servern liegt die E-Mail jedoch im Klartext vor.

In Nordrhein-Westfalen sind bei der Wahl der technischen und organisatorischen Maßnahmen folgende Positionen zugrunde zu legen:

- Die Kommunikation per E-Mail bedarf mindestens der Transport-Verschlüsselung, wie sie von den namhaften europäischen Providern standardmäßig angeboten wird.
- Die Transportverschlüsselung sollte entsprechend der Technischen Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport“ implementiert sein. In Abhängigkeit vom Schutzbedarf der versendeten Daten und dem Risiko können Abweichungen von der Richtlinie statthaft sein.
- Es ist zu berücksichtigen, dass bei einer Transportverschlüsselung die E-Mails auf den E-Mail-Servern im Klartext vorliegen und grundsätzlich einsehbar sind. Bei besonders schützenswerten Daten (z.B. Kontobewegungsdaten, Finanzierungsdaten, Daten zum Gesundheitszustand, Mandantendaten von Rechtsanwälten und Steuerberatern, Beschäftigtendaten) ist eine alleinige Transportverschlüsselung möglicherweise nicht ausreichend. Zusätzliche technische und organisatorische Maßnahmen, wie z. B. eine Ende-zu-Ende-Verschlüsselung können geboten sein. Sollte dies nicht gewährleistet werden können, sind ggf. alternative Übertragungswege denkbar: Hierzu zählen der elektronische Austausch über eine gesicherte Verbindung (Web-Portal des Verantwortlichen mit Zugangsbeschränkungen) oder die klassische postalische Zusendung.
- Der Betreff der E-Mail sollte keine personenbezogenen Daten enthalten.

Helga Block, Landesbeauftrage für Datenschutz und Informationsfreiheit Nordrhein-Westfalen