Praxistipps Datenschutz 03 2017

Sichere Übermittlung von E-Mails ist möglich

Zusammenfassung: Wenn E-Mails sicher übermittelt werden sollen, müssen sie verschlüsselt sein. Das geht entweder mit einem Programm zur Verschlüsselung wie GNU PGP oder per Grundeinstellung auf dem Server. In diesem Fall muss der empfangende Server allerdings auch mitspielen. Ist das gewährleistet, kann aus Outlook heraus eine Mail verschlüsselt transportiert werden. Sind die sendenden und empfangenden Server jedoch nicht richtig konfiguriert, kann die sichere Übertragung unterwegs leicht durchbrochen werden.

Der Praxisfall: In der Datenschutzunterweisung fragen Beschäftigte, ob sie Rechnungen per Mail versenden dürfen. Immerhin seien auf den Rechnungen die Bankdaten des Unternehmens aufgeführt. Die Informationspflicht des Unternehmens bedeute aber, wie gerade in der Unterweisung gelernt, dass eine Meldung an die Aufsichtsbehörde erfolgen müsse, wenn diese Daten Dritten zur Kenntnis gelangt sein könnten. Da eine Übermittlung in einer unverschlüsselten Mail aber offen wie eine Postkarte sei, müsste das Unternehmen für eine Verschlüsselung des Mailverkehrs sorgen. Da gebe es doch die TLS-Verschlüsselung. Die Teilnehmer an der Unterweisung möchten nun wissen, ob diese Verschlüsselung im Unternehmen verwendet wird und man daher Mails sicher versenden könne. Viele Datenschutzbeauftragte werden jetzt auf dem falschen Fuß erwischt worden sein.

Rechnungen werden häufig per Mail verschickt: Seit die Finanzverwaltung akzeptiert, dass Rechnungen als PDF erstellt und gesendet werden, werden diese immer häufiger per Mailanhang versendet. Dass dabei geprüft werden muss, wie sicher die Übermittlung per Mail ist, ist eigentlich selbstverständlich. Dies gehört zu den Prüfaufgaben der Datenschutzbeauftragten.

Vertraulichkeit oft Fehlanzeige: In vielen Mails kann von einer vertraulichen Übermittlung nicht die Rede sein. Zum einen kann ein Empfänger nie sicher sein, ob nicht der Absender noch einen weiteren Empfänger in „bcc“ eingegeben hat. Zum anderen können Mails auf ihrem Weg vom Absender zum Empfänger unterwegs ausgelesen und kopiert werden. Ob sie inhaltlich verändert wurden, lässt sich eigentlich im so genannten Header einer E-Mail erkennen. Da jedoch bei unverschlüsselten Mails auch der Header verändert werden könnte, ist diese Information nicht zuverlässig.

Wege der Mails im Internet: Auf ihrem Weg vom Absender zum Empfänger durchläuft die E-Mail einige Kontenpunkte. Diese liegen oft außerhalb der Europäischen Union. Können schon hier unter anderem Geheimdienste Mailinhalte auswerten, so ist davon erst recht in Drittstaaten auszugehen. So kann nicht davon ausgegangen werden, dass Vertraulichkeit gegeben ist.

Wer könnte Interesse an Mails haben? Ein berechtigtes Interesse können Geheimdienste haben, wenn es in der Mail Inhalte gibt, die im Zusammenhang mit einer begangenen oder geplanten Straftat stehen, die die öffentliche oder staatliche Sicherheit gefährden kann. Ausländische Geheimdienste gehen in der Interpretation dieser Gefährdungen aber so weit, dass auch alle Unterlagen, die im Zusammenhang mit technischen Entwicklungen stehen, daraufhin zu prüfen sind, ob damit solche Straftaten begangen werden könnten. Entsprechend erhalten verlässliche Partner diese Unterlagen zur Prüfung. Was sie damit machen, entzieht sich der Kontrolle des versendenden Unternehmens. Wirtschaftsspionage ist somit Tür und Tor geöffnet.

Innerhalb einer Domäne sollten Mails sicher sein: Werden Mail innerhalb einer Domäne (bzw. innerhalb der Reichweite eines Servers) versendet, geschieht dies in einem eigens geschützten Bereich des Internet. Somit ist hier schon deutlich mehr Schutz für sensible Informationen gegeben als beim offenen Versand einer E-Mail nach extern über das Internet, zumindest solange nicht davon ausgegangen werden muss, dass die Mails innerhalb einer Domäne systematisch oder stichprobenartig verdeckt oder offen ausgewertet werden, was rechtlich unzulässig, technisch aber möglich ist.

Rechtliche Einordnung: Ob die Mail unterwegs tatsächlich kopiert und gelesen wird, ist aber aus rechtlicher Sicht unerheblich. Es genügt schon die Möglichkeit, dass dies geschehen kann. Von Vertraulichkeit kann daher keine Rede sein. Lediglich Inhalte, die auch veröffentlicht werden dürfen, dürfen offen per Mail verschickt werden. Darüber sind sich die wenigsten Beschäftigten im Klaren.

Risiko unverschlüsseltes Mailen: Das offene, also unverschlüsselte Versenden einer E-Mail mit schützenswerten Inhalten ist somit ein ernstzunehmendes Sicherheitsrisiko für jedes Unternehmen. Gleiches gilt natürlich

auch für Anhänge, die der Mail unverschlüsselt angehängt werden.

Mails verschlüsseln mit PGP: Für die Verschlüsselung von Mails gibt es mehrere Systeme. Sicher, aber nicht ganz einfach zu handhaben, ist GNU PGP. Hier müssen vor der verschlüsselten Kommunikation Schlüsselpaare gebildet werden. Zwar können nach der einmaligen Einrichtung von Mailkonto zu Mailkonto ohne weitere Einschränkung Mails ausgetauscht werden, ohne dass Dritte diese sehen können. Das entspricht aber nicht der Lebenspraxis beim Mailen. Denn die Verschlüsselung gilt auch Mailempfängern gegenüber, die in die Zeilen cc oder bcc eingetragen werden. Diese könnten dann nur die verschlüsselte Nachricht sehen, was regelmäßig zu Nachfragen führt.

Mails verschlüsseln mit Dienstleistern: Es gibt auch Dienstleister, die dieses Hindernis ausgeräumt haben. Dabei wird der Mailverkehr über deren Server abgewickelt. Die Mailübermittlung geschieht komplett über verschlüsselte Wege über den Dienstleister. Vorteil ist, dass sich die Anwender selbst nicht um den als umständlich empfundenen Schlüsselaustausch kümmern müssen. Dafür wird die Dienstleistung in der Cloud erbracht, was bei manchen Unternehmen Vorbehalte auslösen dürfte.

Mails verschlüsseln mit STARTTLS: Server sind von den Grundeinstellungen her häufig mit einer Verschlüsselungsfunktion ausgestattet, die eine verschlüsselte Übertragung der Nachrichten über das Internet erlaubt, zumindest von Server zu Server. Allerdings setzt das voraus, dass entsprechende Einstellungen vorgenommen wurden. Dieses Verfahren kombiniert zwei wichtige Grundprinzipien des Datenschutzes, nämlich Vertraulichkeit und Integrität.

So geht weitgehend sichere Mailübermittlung: Bevor eine E-Mail versendet wird, legen die an der Kommunikation beteiligten Mailserver einen Standard für die Übertragung der Nachricht fest. Erst dann wird die E-Mail verschickt. Je nach Konfiguration holen die Mailserver die Information ein, ob von der Gegenseite eine Transportverschlüsselung (Transport Layer Security, kurz TLS) unterstützt wird. Dann wird die E-Mail mit der bestmöglichen Verschlüsselung abgeschickt. Dies funktioniert jedoch nur, wenn beide Mailserver STARTTLS zur Verschlüsselung unterstützen. Um die Integrität sicherzustellen, ist darüber hinaus noch Perfect Forward Secrecy einzusetzen. Damit kann verhindert werden, dass die per TLS verschlüsselte Übertragung der E-Mail nicht nachträglich entschlüsselt werden kann.

Vertraulichkeit kann dennoch verletzt sein: Allerdings kann eine Transportverschlüsselung durch STARTTLS eine Ende-zu-Ende Verschlüsselung (z. B. mit PGP) nicht ersetzen. Sie ist vielmehr als zusätzlicher Baustein zur Erhöhung der Kommunikationssicherheit zu sehen ist. Das liegt daran, dass die E-Mail vor der Übermittlung den Weg vom System des Absenders zum Server und beim Empfänger vom Server zu dessen System zurücklegen muss. Auf diesem Weg können Mail ausgelesen werden. Außerdem kann auf den Systemen von Sender und Empfänger ein Keylogger installiert sein, der ein lückenloses Mitlesen aller erstellten Nachrichten (und noch viel mehr) ermöglicht. Gegen solche Angriffe helfen selbst Ende-zu-Ende-Verschlüsselung und Hochsicherheits-Passwörter nicht mehr.

Geringer Aufwand für mehr Sicherheit: Unternehmen die diese Maßnahmen zur Erhöhung der Sicherheit ihrer Mailserver umsetzen wollen, haben damit einen sehr geringen Aufwand. Es ist damit zumeist damit getan, die Konfiguration der Mailserver an den Stand der Technik anzupassen. Falls noch nicht vorhanden, müssen noch zusätzlich entsprechende TLS-Zertifikate von einer vertrauenswürdigen Stelle erworben werden. Dafür, dass dann eine weitaus höhere Sicherheit bei der Kommunikation per E-Mail erlangt werden kann, lohnt sich der Aufwand allemal. Umso verwunderlicher war das Ergebnis einer vom Bayerischen Landesamt für Datenschutz vor nicht allzu langer Zeit vorgenommenen Überprüfung von 2.336 bayerischen Unternehmen, ob dort die hier geschilderte Verschlüsselungstechnik vorhanden ist. Mehr als ein Drittel der überprüften Unternehmen hatte diese einfach herbeizuführende Sicherheitsmaßnahme leider nicht eingestellt.

Besonders ärgerlich: Diese Unternehmen torpedieren damit auch die Sicherheit derer, die sich eigentlich richtig verhalten. Wie oben dargestellt, müssen sendender und empfangender Server über diese Technik verfügen, einer alleine reicht nicht aus. Und je nach Konfiguration erfährt der Absender nicht einmal, dass seien eigentlich verschlüsselte Mail beim Empfänger gar nicht verschlüsselt angekommen ist, weil dort diese einfachen Sicherheitsmaßnahmen nicht vorgenommen wurden. Warum das nicht getan wurde, ist oft nicht nachvollziehbar; es sei denn, man wollte der Geschäfts- oder Behördenleitung unterstellen, dass sie nicht möchte, dass die Beschäftigten auf sicheren Wegen per Mail kommunizieren können, sprich, verschlüsselte Mails senden und empfangen können.

Aufgaben für Datenschutzbeauftragte:

1. Zusammen mit der IT prüfen, ob die eigenen Mailserver mit STARTTLS und TLS sowie Perfect Forward Secrecy einsetzen.
2. Sollte dies nicht der Fall sein, müssen die Gründe geklärt werden.
3. Prüfen, welche der wichtigsten Kommunikationspartner ihre Server entsprechend konfiguriert haben.
4. Prüfen, wie Mailversender möglichst vor dem Mailversand feststellen können, ob die Verschlüsselung eingeschaltet ist.
5. Verschlüsselten Mailversand als Thema der Datenschutzrichtlinien des Unternehmens aufnehmen
6. In den Datenschutzunterweisungen auf die Verschlüsselung hinweisen, vor allem, wie erkannt werden kann, dass die Mail nicht verschlüsselt beim Empfänger ankommen wird

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de