mMail: Sicherheit im Mailverkehr durch Verschlüsselung

WagnerTech UG, Turfstr. 18a, 81929 München, www.wagnertech.de

Nach dem Bekanntwerden der geheimdienstlichen Tätigkeiten im Internet ist es Allgemeingut geworden, dass sensible Firmendaten im ungeschützten Internet nichts zu suchen haben. Wie soll aber eine Firma im täglichen Betrieb für die nötige Sicherheit sorgen, ohne den freien Informationsaustausch in unnötiger Weise zu behindern? Dieser Artikel zeigt, wie mit entsprechenden Einstellungen im *mail transfer agent* (MTA) *postfix* für eine den Anforderungen eines Unternehmens graduelle Sicherheit realisiert werden kann.

Eine Sicherung des Mailverkehrs durch Verschlüsselung kann auf verschiedenen Ebenen erfolgen. Als sicherste Lösung gilt dabei die Ende-zu-Ende-Verschlüsselung über ein *public key*-Verfahren. Bei diesem Verfahren werden die *e-mails* mit dem öffentlichen Schlüssel des Empfängers[1] verschlüsselt. Nur der Empfänger der Mail kann die so verschlüsselte Mail mit seinem privaten Schlüssel wieder entschlüsseln. Dieses Verfahren hat folgende Nachteile:

- Alle Teilnehmer müssen die öffentlichen Schlüssel ihrer Kommunikationspartner auf ihrem Endgerät zur Verfügung haben.
- Ein Teilnehmer muss auf jedem seiner Endgeäte (PC, Laptop, Smartphone) seinen privaten Schlüssel zur Verfügung haben.
- Die Vervielfältigung des privaten Schlüssels ist eine potentielle Sicherheitslücke, wenn bei der Übertragung ungeeignete Methoden (z.B. Verschicken mit Mail, Clouddienste) verwendet werden.

Eine andere Form der Verschlüsselung ist die Transportverschlüsselung. Hier werden die Daten zwischen MTAs über das ssl-Protokoll verschlüsselt ausgetauscht. Dieses Verfahren hat folgende Nachteile:

- In den Mailfächern der Server liegen die Daten in unverschlüsselter Form vor.
- Ein Austausch über Transportverschlüsselung darf daher nur zu MTAs hin erfolgen, auf denen die (unverschlüsselten) Mails sicher liegen. Also nicht zu einem der großen Provider, auf die interessierte Stellen Zugriff haben.

mMail ist ein *postfix*-Zusatz, der folgenden Ansatz verfolgt:

- Der Mailverkehr innerhalb der Firma kann unverschlüsselt erfolgen.
- Für den Mailverkehr zu Partnerfirmen genügt eine Transportverschlüsselung.
- Mailverkehr zu einer Einzeladresse (z.B. Privatadresse eines Mitarbeiters) darf nur über eine Ende-zu-Ende Verschlüsselung erfolgen.
- Die Ver- und Entschlüsselung für das *public key*-Verfahren erfolgt dabei zentral auf dem Firmen-Mail-Server, damit der einzelne Mitarbeiter nicht mit der Schlüsselverwaltung zu tun hat.

mMail ist *open source* und kann über unsere Firma kostenlos bezogen werden. WagnerTech unterstützt Sie gerne bei Einrichtung und Betrieb der Software.

[1] Die grammatikalisch männliche Form umfasse sämtliche Geschlechtsausprägungen. Daher wird diese Form Formulierungen vorgezogen, die sich auf zwei Geschlechter beschränken. Bei allen anderen Ausdrücken wird in derselben Weise verfahren.