

Wie Sie vertrauliche E-Mails sicher zustellen

E-Mails sind eine feine Sache. Sie sind bequem, sparen Zeit, sind schnell, unabhängig und preisgünstig. Derzeit werden weltweit rund 30 Milliarden dieser elektronischen Nachrichten pro Tag verschickt. Ungefähr die Hälfte ist geschäftlicher Natur. Das ist die gute Nachricht.

Die schlechte: Technisch gesehen sind E-Mails nichts weiter als virtuelle Postkarten. Und ebenso wie die Postkarte auf dem Weg vom Absender zum Empfänger „offen“ ist, kann auch die E-Mail ohne größere Probleme abgefangen, gelesen und manipuliert werden.

Als Empfänger einer geschäftlichen E-Mail muss man sich deshalb folgende Fragen stellen:

- **Authentizität der E-Mail:** Ist die E-Mail authentisch, stammt sie wirklich von diesem Absender oder wurde die Absenderadresse gefälscht?
- **Vertraulichkeit der E-Mail:** Wurde die Vertraulichkeit gewahrt oder ist die E-Mail noch von anderen Personen gelesen worden, die dazu kein Recht haben?
- **Integrität der E-Mail:** Ist die E-Mail auf dem Transportweg abgefangen und verändert worden?

Eine verlässliche Antwort auf diese Fragen ist für viele Unternehmen existenziell wichtig. Denn die gesetzlichen Bestimmungen zum Datenschutz gelten selbstverständlich auch für Informationen, die in Form von E-Mails übertragen werden. Wer gegen diese Vorschriften verstößt, dem drohen neben einem wirtschaftlichen Schaden auch ein großer Imageverlust sowie Geld- oder sogar Gefängnisstrafen.

E-Mail-Sicherheit: Für immer mehr Unternehmen ein großes Thema

Das Thema E-Mail-Sicherheit ist deshalb für immer mehr Unternehmen, unabhängig von der Branche, ein großes Thema. Besonders wichtig ist es allerdings für Firmen, die einer Informationspflicht unterliegen, wie z. B. Banken, Versicherungen, Finanzdienstleister oder Unternehmen aus dem Healthcare-Bereich. Um dieser Pflicht

nachzukommen, versenden die meisten dieser Unternehmen sensible Inhalte wie Kontoauszüge, Rechnungen oder persönliche Gesundheitsinformationen bisher häufig mit der Post. Das verursacht allerdings immense Portokosten und einen hohen Verwaltungsaufwand, wenn die eingegangenen Daten manuell erfasst werden müssen. Ein Versand per E-Mail würde die Kosten deutlich reduzieren.

In anderen Branchen – besonders bei Telekommunikationsunternehmen und Internet Providern – erfreuen sich Rechnungen, die im PDF-Format per E-Mail versandt werden, großer Beliebtheit. Rechtlich gesehen bewegt sich diese Praxis allerdings in einer Grauzone, denn einer Manipulation dieser E-Mails ist, wie oben dargestellt, Tür und Tor geöffnet.

Zwei gängige Lösungen für die Signierung und Verschlüsselung von E-Mails

Was können Unternehmen tun, um ihre E-Mails manipulations- und damit rechtssicher zu machen? Sie müssen die E-Mails mit einem privaten Schlüssel signieren und anschließend verschlüsselt versenden. Dafür gibt es zwei Möglichkeiten: eine dezentrale Lösung (das sogenannte clientbasierte Verfahren) und eine zentrale Lösung (das sogenannte Gateway-Verfahren).

Die dezentrale, clientbasierte Lösung

Bei diesem Verfahren erfolgen E-Mail-Signierung und -Verschlüsselung direkt auf dem Desktop des Mitarbeiters. Das ist jedoch mit einem hohen technischen, organisatorischen und finanziellen Aufwand verbunden, der vor allem aus der zeitintensiven Administration und den häufig notwendigen Anwenderschulungen resultiert.

Wenn ein Mitarbeiter aus dem Unternehmen ausscheidet oder neu eingestellt wird, müssen Zertifikate widerrufen bzw. neu erteilt werden. Außerdem muss jeder Empfänger einer verschlüsselten E-Mail über denselben Schlüssel verfügen, um die E-Mail öffnen zu können, sodass der Schlüssel mit jedem neuen Geschäftspartner ausgetauscht werden muss.

Was jedoch am gravierendsten ist: Es bleibt jedem einzelnen Mitarbeiter überlassen, ob er eine E-Mail verschlüsselt oder nicht. Eine zentrale, unternehmensweite Security

Policy, die die Verschlüsselung bestimmter Inhalte vorschreibt, kann zwar definiert, aber nicht technisch durchgesetzt werden.

Auch das Viren- und Contentscannen wird bei der clientbasierten Lösung auf den Desktop jedes einzelnen Mitarbeiters verlagert. IT-Experten haben jedoch immer wieder darauf hingewiesen, dass das Scannen der E-Mails auf einem zentralen Server eine weitaus bessere Lösung ist, als jedem einzelnen Mitarbeiter die Verantwortung dafür zu übertragen.

Das Gateway-Verfahren setzt sich durch

Aufgrund der massiven Nachteile der dezentralen, clientbasierten Lösung setzt sich das Gateway-Verfahren zunehmend durch. Beim Gateway-Verfahren werden die Signierung und die Prüfung der Signatur von E-Mails sowie die Verschlüsselung und die Entschlüsselung von einem zentralen Vermittlungsserver (dem Gateway) ausgeführt – und nicht mehr von den einzelnen PCs der Mitarbeiter.

Der große Vorteil dieser Lösung ist, dass die Anwender ihre E-Mails absenden und empfangen können, ohne sich um die Signierung und die Verschlüsselung zu kümmern. Die Regeln für die Verschlüsselung können zentral definiert werden, sodass keine Gefahr besteht, dass die Mitarbeiter sie vergessen oder ignorieren. Der Aufwand für die Implementierung des Systems ist wesentlich geringer und die Mitarbeiterschulungen entfallen komplett. Auch die Viren- und Spamprüfung wird bei der Gateway-Lösung automatisch zentral und nicht mehr auf den einzelnen Rechnern der Mitarbeiter vorgenommen.

Die Implementierung des Gateways ist technisch und organisatorisch anspruchsvoll

Im günstigsten Fall läuft das Gateway unbemerkt und diskret im Hintergrund. Die Mitarbeiter bemerken gar nicht, dass ihre E-Mails signiert und verschlüsselt werden. Um dies zu erreichen, muss das Gateway allerdings perfekt in die bestehende IT-Infrastruktur des Unternehmens integriert werden – eine große Hürde für die meisten IT-Abteilungen der Unternehmen. Denn die Implementierung eines Gateways ist weitaus anspruchsvoller und komplexer als die Installation einer Software.

Die technische Herausforderung besteht darin, das Gateway in die bestehenden und funktionierenden E-Mail-Infrastrukturen einzufügen, ohne den laufenden E-Mail-Verkehr zu gefährden. Der kritische Punkt sind dabei die oft unterschiedlichen E-Mail-Systeme und die verschiedenen Sicherheitsebenen der E-Mail-Prüfung (Spam, Contentfilter, Virenschancen). Auch beim Zusammenspiel von Betriebssystem, Datenbank und Gateway stoßen Administratoren ohne spezielle Kenntnisse häufig an ihre Grenzen.

Während die technischen Anforderungen schnell sichtbar werden und so in den Mittelpunkt rücken, wird der organisatorischen Einbindung des Gateways dagegen meist zu wenig Aufmerksamkeit geschenkt. Um einen hohen Automatisierungsgrad des Gateways zu erreichen, muss es an die bestehenden E-Mail-Prozesse des Unternehmens angepasst werden, die hierfür zu analysieren und auf das Gateway zu übertragen sind. Über folgende Aspekte ist dabei zu entscheiden:

- die Art des Verfahrens
- die Art der automatisierten Registrierung
- das Design des Webmailsystems
- die Einbindung der vorhandenen Administration
- Prozesse im Fehlerfall
- die eventuelle Einbindung eines Helpdesks
- Umsetzung und Pflege zentraler Security Policies
- Design und Inhalt der vom Gateway an die Mitarbeiter und an die externen Kommunikationspartner versandten Informations-E-Mails

Um auf diese technisch und organisatorisch anspruchsvollen Herausforderungen die optimale Antwort zu finden, empfiehlt es sich, einen Dienstleister hinzuzuziehen, der den gesamten Implementierungsprozess von der Auswahl der passenden Gateway-Lösung bis hin zur Installation des Systems entweder beratend begleitet oder selbst durchführt.



Der Verfasser

Ulf Lorenzen ist Projektleiter bei der Vater Unternehmensgruppe. Er hat viele Projekte zur Implementierung eines Gateways für den sicheren E-Mail-Versand begleitet – unter anderem bei der HSH Nordbank, wo die Vater Unternehmensgruppe sowohl technische als auch organisatorische Unterstützung leistete.

Kontakt

Vater Unternehmensgruppe
Liebigstraße 26
24145 Kiel
Telefon 0431 20084 200
www.vater-gruppe.de