Bildquelle: iStock

Dossier
E-Mail-Sicherheit

IN KOOPERATION
MIT BOLL ENGINEERING

E-Mails sind gefährlich

mla. E-Mails können Schadsoftware enthalten und verbreiten, sie können schädigende Nachrichten verbreiten wie Spam, Hoaxes, Kettenbriefe, Belästigungen, Mobbing, «pump and dump» oder sie können der Unterstützung gezielter Attacken wie Information Gathering dienen. Und auch ihr Versand ist nicht sicher: Sie können auf Netzwerken und Mail Transfer Agents gelesen und/oder verändert werden, an nicht autorisierte Empfänger gehen, dem Datendiebstahl dienen und für unzählige andere kriminelle Handlungen missbraucht werden.

Dem gegenüber steht der geschäftliche E-Mail-Verkehr. E-Mail dient dem firmeninternen Informations- und Dokumentenaustausch, der Abwicklung von Geschäftsprozessen, der Kommunikation mit Partnern, Lieferanten und Kunden. Jede denkbare und undenkbare Information, und sei sie noch so sensibel, wird heutzutage als E-Mail verschickt. Kein Wunder, dass die CIOs dieser Welt nach tauglichen Lösungen verlangen, um den E-Mail-Verkehr sicher zu machen. Sicher vor äusseren und vor inneren Bedrohungen.

Die Anbieter von Lösungen für den sicheren E-Mail-Verkehr können diesen schützen durch clientbasierte, serverbasierte und die auf der Public-Key-Infrastruktur basierende E-Mail-Verschlüsselung und -Signatur oder durch die passwortbasierte E-Mail-Verschlüsselung. Die S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein weiterer Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein hybrides Kryptosystem.

Thomas Boll vom Security-Distributor Boll Engineering beleuchtet in seinem Fachartikel verschiedene Aspekte der E-Mail-Sicherheit und stellt auch die Seppmail-Appliance vor, die den Weg der sogenannten Push-E-Mail-Verschlüsselung geht. Eine «Zwei-Faktoren-Authentisierung» soll dabei für maximale Authentizität und Integrität im E-Mail-Verkehr sorgen.

Bildquelle: iStock

Secure E-Mail – notwendiger denn je

Der elektronische Versand vertraulicher Informationen ist einem grossen Wandel unterworfen. Es gilt, E-Mails umfassend zu schützen, die Authentizität des Senders zu garantieren und die Vertraulichkeit der Botschaft zu sichern.

Sowohl gesetzliche Rahmenbedingungen als auch die verstärkte Sensibilisierung für die Gefahren der elektronischen Datenübertragung führen dazu, dass Firmen ihre E-Mail-Kommunikation zunehmend schützen (müssen). Berufsgeheimnisträger wie Ärzte, Anwälte oder Finanzdienstleister beispielsweise sind von Gesetzes wegen zu einer gesicherten E-Mail-Kommunikation verpflichtet. Zudem sind Firmen gut Beraten, Daten und Informationen – und somit das Unternehmen – im Bereich der E-Mail-Kommunikation zu schützen. Auch die sichere E-Mail-Kommunikation mit Behörden ist ein wichtiger werdendes Thema und eine zentrale Komponente einer ganzheitlichen E-Government-Strategie.

Sorgt weltweit für Furore: Seppmail, die in der Schweiz entwickelte Lösung für den sicheren E-Mail-Verkehr (Verschlüsselung und digitale Signatur). Bildquelle: Seppmail

Mannigfaltige Gefahren

Bei der Übermittlung sensitiver, vertraulicher Daten via E-Mail gilt es, dafür zu sorgen, dass diese ausschliesslich durch die berechtigten Empfänger einsehbar sind und dass der Inhalt nicht verändert werden kann. Dies ist aus technologischer Sicht seit mehreren Jahren möglich. Trotzdem werden entsprechende Verschlüsselungs- und Signaturlösungen noch (zu) spärlich genutzt. Dies mit möglicherweise fatalen Folgen. So ist es für Hacker vergleichsweise einfach, ungesicherte E-Mails abzufangen beziehungsweise einzusehen, ohne dass der Absender oder der legitime Empfänger etwas davon merkt.

So bildet die elektronische Post beispielsweise im Bereich der Industrie- und Wirtschaftsspionage eine ausgezeichnete Plattform, um etwa Offerten, Kundenlisten, Forschungsresultate oder technische Dokumente von Mitbewerbern einzusehen. Ebenso problematisch ist das sogenannte «Mail Spoofing». Dabei werden Mails unter Vortäuschung falscher Absender verschickt, was der Verteilung von Malware, der Verlinkung auf verseuchte Websites oder dem Versand von Spam-Mails dient. Spoofing-Attacken benötigen weder tiefgreifende IT-Kenntnisse noch spezielle Tools. Vielmehr lassen sie sich einfach über Outlook (und andere Mail-Programme) ausführen. Etwas komplexer präsentiert sich die Veränderung von Mails. Verschaffen sich Hacker Zugriff auf einen Mail-Server, besteht für sie die Möglichkeit, Mails einzusehen und deren Inhalt vor der Weiterleitung zu modifizieren. Den Betrugsmöglichkeiten sind dabei kaum Grenzen gesetzt.

Der Autor

Thomas Boll,
Boll Engineering

Gesicherter Nachrichtenaustausch

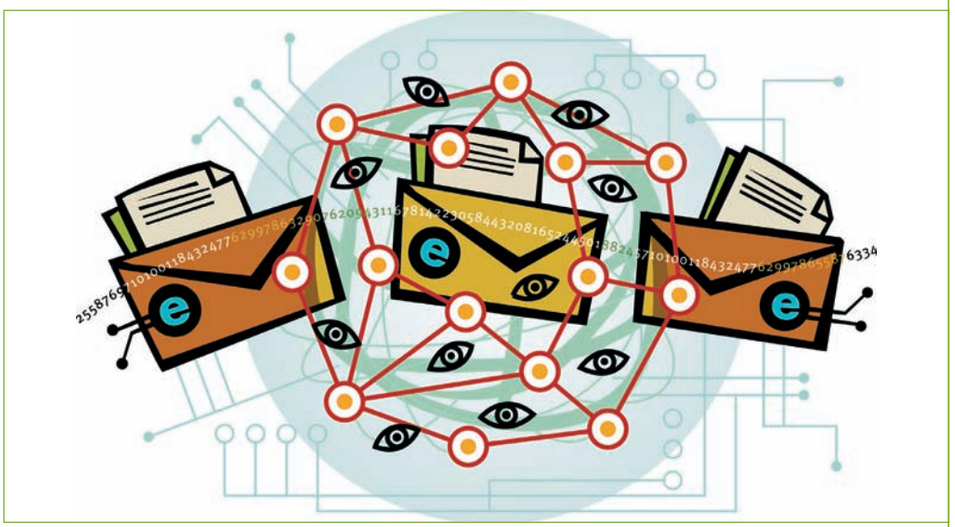
Allen Gefahren zum Trotz: Die Nutzung von Secure E-Mail ist vergleichsweise bescheiden. Ein Grund dafür dürfte sein, dass die Problematik unterschätzt wird. So herrscht vielerorts die Meinung vor, der eigene Mailverkehr werde nicht «abgehört» oder modifiziert, da keine entsprechenden Anzeichen vorhanden sind. Ferner gehen viele Nutzer davon aus, dass vorhandene Sicherheitsvorkehrungen wie UTM-Appliances oder Anti-Viren-Lösungen die E-Mail-Kommunikation sichern. Doch auf dem Weg von A nach B passieren E-Mails zahlreiche, für Absender und Empfänger unbekannte Server, womit jegliche Kontrolle darüber entfällt, wer wann welche Zugriffe auf die Nachricht hat. Ein weiterer Aspekt für die noch ungenügende Nutzung von Secure E-Mal dürfte in der zu komplexen Integration und Handhabung einiger Lösungen zu finden sein.

Unterschiedliche Lösungsansätze

Um der Sicherheitsproblematik bei der E-Mail-Kommunikation zu begegnen, stehen unterschiedliche Technologien zur Verfügung.

- **PGP und S/MIME**

PGP (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extension) sind userbasierte Technologien, bei denen jeder Benutzende ein eigenes Zertifikat benötigt, was deren Handhabung erschwert. Werden Zertifikate bzw. Schlüsselpaare jedoch in einer dedizierten E-Mail-Gateway-Appliance installiert, erfolgt die Ver- und Entschlüsselung der E-Mails zentral auf der Appliance. Der User wird vom Ver- bzw. Entschlüsselungsvorgang komplett entlastet. >



Nicht verschlüsselt übertragene E-Mails können durch Dritte einfach abgefangen, eingesehen und verändert werden. Bildquelle: iStock

Brisante und vertrauliche E-Mails werden häufig ungeschützt übermittelt. Bildquelle: photos.com

• **Secure Webmail**
Erfolgt die Kommunikation mittels Secure Webmail, erhält der Empfänger anstelle der E-Mail einen Link. Dieser führt ihn via Web zur verschlüsselten Nachricht. Diese grundsätzlich komfortable Lösung ist mit Sicherheitsrisiken verbunden. So lassen sich sogenannte Man-in-the-Middle-Attacken mit relativ einfachen Mitteln und Kenntnissen reiten. Dazu wird dem Empfänger anstelle des regulären Links ein «originalgetreues» Phishing-Mail zugestellt. Der darin enthaltene Link führt jedoch nicht direkt zur verschlüsselten Nachricht, sondern wird stattdessen über einen eigenen Server «umgeleitet».

Secure E-Mail aus der Cloud

Firmen und Institutionen gehen vermehrt dazu über, Teile ihrer IT an externe Partner auszulagern, um die jeweiligen Dienste als Service zu beziehen. Dank der offenen Seppmail-Architektur lassen sich Outsourcing-Strategien auch im Bereich Secure E-Mail umsetzen. Wird die Appliance bei einem externen Dienstleistungsanbieter installiert, stehen dem Kunden sämtliche Secure-E-Mail-Funktionen als Service zur Verfügung – unabhängig davon, ob der Mail-Server inhouse oder ebenfalls extern betrieben wird. Dadurch lassen sich Kosten sparen, und der Administrationsaufwand entfällt.

• **Verschlüsselung von PDF-Dateien**
Um Dokumente für Dritte unlesbar zu übertragen, lassen sich PDF-Dateien mittels Passwort schützen. Auch dieser Lösungsweg ist nicht unproblematisch. Einerseits können bei der PDF-Umwandlung Formatierungsfehler auftreten. Andererseits sind sie empfindlich gegenüber sogenannten Bruteforce-Attacken. Dabei werden alle möglichen Passwörter automatisch generiert und das passwortgeschützte PDF-Dokument in kürzester Zeit entschlüsselt.

• **«Push-E-Mail-Verschlüsselung»**
Bei dieser Mailverschlüsselungstechnologie werden E-Mails durch eine firmeneigene Secure-E-Mail-Plattform (Appliance) verschlüsselt und in einer HTML-Mail an den Empfänger geschickt. Öffnet dieser den entsprechenden Anhang, erfolgt eine automatische Übermittlung der verschlüsselten Nachricht an die Secure-E-Mail-Appliance. Alsdann wird der Empfänger aufgefordert, sich mittels Passwort zu identifizieren, wonach ihm die Nachricht in seiner gewohnten Mail-Umgebung angezeigt wird. Dieses von Seppmail entwickelte Verfahren hat mehrere Vorzüge. So maximiert die sogenannte «Zwei-Faktoren-Authentisierung» die Sicherheit (der Empfänger benötigt für den Zugriff auf die Daten sowohl die Nachricht selbst als auch ein Passwort) und trägt dazu bei, dass die Secure-E-Mail-Lösung revisionskonform ist und den aktuellen Compliance-Anforderungen (SOX, HIPAA, PCI, Basel II) entspricht. Ebenso bedeutsam: Die Empfänger verschlüsselter Nachrichten benötigen auf ihrem System keine spezifische Software bzw. Verschlüsselungslösung. Dies erlaubt einen sicheren Nachrichtenaustausch mit beliebigen Empfängern. Ferner ist es möglich, zuverlässige Lesebestätigungen auszustellen, was mit der Funktion «eingeschriebene E-Mails» bezeichnet werden kann.

• **Authentizität sichern**
Hat eine Nachricht den Empfänger ohne Einwirkung Dritter – und folglich unverändert – erreicht, und stammt die übermittelte E-Mail tatsächlich von der im Absender ausgewiesenen Person? Um dies garantieren und die Authentizität von Sender und Nachricht sicherzustellen zu können, müssen E-Mails digital signiert werden. Benötigt werden dazu sogenannte S/MIME-Zertifikate (Schlüssel). Diese benutzer- oder firmenspezifischen Zertifikate bestätigen einerseits die Echtheit des Absenders und garantieren andererseits, dass die Nachricht im Rahmen der Übertragung keine Änderungen erfahren hat. Werden Zertifikate verwendet, die von einem öffentlich akkreditierten Zertifikatsanbieter (offizielle CA) ausgestellt sind, wird ein Höchstmass an Vertrauenswürdigkeit erreicht. <

BOLL Engineering AG
Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60
info@boll.ch | www.boll.ch

«Irgendwann wird ein Grossteil der geschäftskritischen E-Mails verschlüsselt und digital signiert verschickt»

Avantec, Anbieterin von IT- und Informationssicherheitslösungen, ist seit Mai 2011 erster Schweizer Gold-Partner des Secure-E-Mail-Anbieters Seppmail. IT-Markt sprach mit CEO Lukas von Känel über die Beweggründe, sich in diesem Security-Teilmarkt stark zu machen.

Interview: Marc Landis

Lukas von Känel
ist CEO des IT-Security-Dienstleisters Avantec mit Sitzen in Zürich und Bern.

Avantec ist ein etablierter Anbieter von Secure-E-Mail-Lösungen und seit kurzem erster Seppmail-Gold-Partner in der Schweiz. Was sind die treibenden Kräfte hierfür?
Lukas von Känel: Wir nehmen für uns in Anspruch, unsere Kunden im Bereich der IT-Security mit einem ganzheitlichen Produkt- und Dienstleistungsangebot zu bedienen und so die Basis für eine nachhaltige Wertschöpfung zu schaffen. Dass Lösungen zur Gewährung einer sicheren E-Mail-Kommunikation in ein entsprechendes Gesamtangebot gehören, ist unbestritten.

Sind die Firmen bereit, in Secure E-Mail zu investieren?
Die Verschlüsselung und digitale Signatur von E-Mails hat einen direkten Einfluss auf Kundenprozesse. Vor diesem Hintergrund muss die Einbindung und Nutzung entsprechender Lösungen effizient und mit geringem Aufwand erfolgen. Im Gegensatz zu bisherigen Lösungen entsprechen Produkte neuerer Generation diesen Anforderungen, was deren Akzeptanz deutlich erhöht. Bemerkenswert ist auch, dass Initiativen wie die SuisseID zu einer vermehrten Auseinandersetzung mit Fragen rund um Zertifikate führen und daraus eine deutliche Sensibilisierung für die sichere Mail-Kommunikation resultiert. Letztlich führt auch die zunehmende Nutzung zu einer verstärkten Wahrnehmung und Akzeptanz. Kurz gesagt: Im Bereich E-Mail Security stellen wir ein klares Momentum fest.

In welchen Märkten sehen Sie das grösste Potenzial?
Grundsätzlich ist der gesicherte Mail-Verkehr immer dann ein Thema, wenn Geschäftsgeheimnisse vertraulich transportiert werden müssen – und dies ist in fast allen Branchen der Fall. Allerdings sind Unterschiede hinsichtlich «Need» und Sensibilisierung feststellbar. Die Finanz- und Versicherungsbranche beispielsweise ist aufgrund gesetzlicher Regularien verpflichtet, die E-Mail-Kommunikation zu sichern. In der Industrie wiederum gilt es, hauptsächlich Entwicklungs-Know-how zu schützen und Industriespionage zu verhindern. Wichtig ist dabei, die Kunden mit einer Secure-E-Mail-Lösung zu bedienen, die sich kostengünstig in die bestehende Kommunikationsinfrastruktur integrieren lässt und eine einfache Handhabung ermöglicht.

Welchen Mehrwert bieten Sie Ihren Kunden im Bereich Secure E-Mail?
Als Dienstleistungs- und Lösungsanbieter im ICT-Security-Bereich setzen wir generell auf eine ausgeprägte Engineering-Kompetenz sowie auf technologisch führende «Best of Breed»-Lösungen. Dank dieser konsequent umgesetzten Strategie werden wir von unseren Kunden oft als «GU» geschätzt und mit sämtlichen Aufgaben rund um die IT-Security betraut. So auch im Bereich E-Mail Security. Unseren Kunden bieten wir mit Seppmail eine mächtige und schlüsselfertige Secure-E-Mail-Gesamtlösung an, wobei wir für sämtliche Aufgabenbereiche – von der Planung über die Implementierung bis hin zu Wartung und Support – verantwortlich zeichnen.

Für die Verschlüsselung und digitale Signatur von E-Mails werden userspezifische Zertifikate benötigt. Ist dies ein aufwendiger Prozess?
Hier kommt eine zentrale Stärke der von uns eingesetzten Lösung Seppmail zum Tragen: Dank der innovativen Managed-PKI-Lösung (Public Key Infrastructure) ist das Zertifikatshandling elegant gelöst und die operativen Kosten für die Kunden markant reduziert. Ein wichtiger Grund, weshalb sich Secure E-Mail einer wachsenden Beliebtheit erfreut.

Welche Gründe haben dazu geführt, dass Sie bei Secure E-Mail auf Seppmail setzen?
Nebst den bereits erwähnten Aspekten erfolgte unsere Wahl namentlich aufgrund der technologischen Führerschaft von Seppmail. Diese führt zu einer bisher nicht erreichten Einfachheit hinsichtlich Implementierung und Nutzung. Zudem ist die Lösung skalierbar und auch als Cloud-Service verfügbar. <