

E-Mail-Verschlüsselung zwischen Realität und Anspruch



In diesem Beitrag:

- Die Folgen ungesicherter Mails
- Die wichtigsten Betrugstechniken
- Wie Mails sicher sind

Unverschlüsselt übermittelte E-Mails sind hinsichtlich unerlaubter Einsicht sowie Veränderung von Inhalt und Identität komplett ungeschützt.

Bankdaten

per Postkarte verschickt ...

Gesetzlichen Rahmenbedingungen sowie dem Schutz vertraulicher Inhalte zum Trotz: E-Mails werden mehrheitlich unverschlüsselt verschickt. Der Einsicht durch Unbefugte sowie der Veränderung von Inhalt und Identität durch Dritte sind folglich Tür und Tor geöffnet.

O bwohl die Verschlüsselung von E-Mails in zahlreichen Branchen zwingend notwendig ist – so etwa im Finanz- und Gesundheitswesen, bei Bund und Kantonen, bei Anwälten und Notaren –, wird das Gros der elektronischen Post noch immer ungesichert verschickt. Dies mit möglicherweise weitreichenden Folgen, ist es für Hacker doch vergleichsweise einfach, ungesicherte 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, Forschungsergebnisse oder technische Dokumente von Mitbewerbern einzusehen. Lückenlos und unbemerkt. Auch die unautorisierte Verbreitung vertraulicher Informationen wird dank unverschlüsselter Mails zum Kinderspiel. Möglich wird die beschriebene Problematik aufgrund der Tatsache, dass Mails über verschiedene Internet-Verbindungen geroutet werden und dass sogenannte Sniffer einfach in der Lage sind, den Mailverkehr mitzulesen.

Dreiste Organisationen machen daraus sogar ein Geschäft und bieten das Abfangen von Mails als Dienstleistung an.

Zahlreiche Betrugsmöglichkeiten

Eine weitere, stark verbreitete Problematik 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 und Know-how-intensiver präsentiert sich die dritte Problematik im Bereich der elektronischen Post: 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.

Infos zum Autor



Stefan Klein
ZOE-One GmbH



Grundsätzlich wäre es ein Einfaches, der beschriebenen Problematik Einhalt zu gebieten. So ermöglichen moderne Verschlüsselungs- und Signaturlösungen eine gesicherte Mail-Kommunikation. Trotzdem werden entsprechende Werkzeuge selten genutzt. Dies dürfte u. a. darin begründet sein, dass die Problematik unterschätzt oder schlicht gar nicht erkannt wird. So herrscht allenthalben die Meinung vor, der eigene Mailverkehr werde nicht «abgehört», da keine entsprechenden Anzeichen vorhanden sind. Und werden entsprechende kriminelle Machenschaften trotzdem erkannt, sind die Geschädigten darauf bedacht, diese totzuschweigen – wie dies etwa auch bei erfolgreichen E-Banking- und Phishing-Attacken geschieht. Entsprechende Präzedenzfälle fehlen folglich weitgehend. Kein Wunder, lässt eine Sensibilisierung für die Problematik auf sich warten und werden beispielsweise Patientendaten oder Projektunterlagen noch immer ungesichert übermittelt. Selbst Banken mit ihren hohen gesetzlichen Auflagen hinsichtlich Datenschutz und Bankgeheimnis – es dürfen beispielsweise keine vertraulichen Daten per Mail verschickt werden – übermitteln im Rahmen

ihrer täglichen Arbeit noch immer höchst brisante Daten per Mail – ungeschützt.

Trügerische Sicherheit

Ein wichtiger Grund für die bescheidene Nutzung der E-Mail-Verschlüsselung dürfte die falsche Sicherheit sein, in der sich viele Nutzer wägen. Denn installierte Sicherheitsmassnahmen wie leistungsfähige Firewalls (UTM-Appliances) oder Anti-Viren- und Anti-Spam-Lösungen führen zur irrtümlichen Annahme, die elektronische Kommunikation sei gesichert. Dies ist etwa bei SSL-verschlüsselten Web-Applikationen wie E-Banking auch tatsächlich der Fall. Nicht jedoch bei der E-Mail-Kommunikation, bei der die elektronische Post zwar von einem gesicherten zu einem anderen gesicherten Arbeitsplatz übermittelt wird, auf diesem Weg jedoch zahlreiche, für Absender und Empfänger unbekannt Server beziehungsweise Internet Service Provider (ISPs) passiert. Eine ebenso zentrale Einflussgrösse für den seltenen Einsatz der Mail-Verschlüsselung dürfte die teilweise zu komplexe Integration und Handhabung entsprechender Lösungen sein. Dies ist namentlich dann der Fall, wenn auf der Empfängerseite ebenfalls eine entsprechende Applikation, ein Plug-in oder ein Zertifikat installiert werden muss.

Nicht alle Lösungen sind sicher

Um der beschriebenen Problematik zu begegnen, stehen unterschiedliche Lösungsansätze und Technologien zur Verfügung.

• PGP und S/MIME

Die Technologien PGP (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extension) gelten als «Verschlüsselungs-Pioniere». Sie sind User-basiert; das heisst, dass jeder Benutzende ein eigenes Zertifikat benötigt, was deren Handhabung stark verkompliziert. Die beiden Standards sind deshalb im täglichen Mail-Leben kaum anzutreffen. Werden PGP und S/MIME allerdings in einer Mail-Gateway-Appliance wie z. B. SEPPmail installiert, erfolgt die Ver- und Entschlüsselung der Mails zentral auf der Appliance. Der User wird vom Ver- bzw. Entschlüsselungsvorgang völlig entlastet, womit die Akzeptanz der E-Mail-Verschlüsselung steigt.

• Secure Webmail

Dank der einfachen Implementierung handelt es sich bei Secure Webmail um die wohl am stärksten verbreitete Lösung. Dabei erhält der Empfänger anstelle der E-Mail selbst einen Link, der ihn via Web zur verschlüsselten Nachricht führt. Dieser an sich komfortable Lösungsweg ist jedoch mit hohen Sicherheitsrisiken verbunden. So lassen sich beim «sicheren Webmail» sogenannte «Man in the middle»-Attacken mit relativ bescheidenen Mitteln und Kennt-

VORAUSSETZUNG für sichere Mail-Korrespondenz

Für eine sichere elektronische Korrespondenz sind die folgenden Kriterien zu gewähren:

- Vertraulichkeit (Confidentiality) des Inhaltes sowie der Kommunikationsbeziehung
- Unverfälschtheit (Integrity)
- Verantwortlichkeit (Accountability)
- Rechtsverbindlichkeit (Binding Force)

EVALUATIONSKRITERIEN

Im Rahmen der Evaluation einer Verschlüsselungslösung sollten u. a. die folgenden Kriterien berücksichtigt werden:

- Automatische Verschlüsselung und Entschlüsselung im gewohnten E-Mail-Client (idealerweise ohne zusätzliche Plug-ins)
- Unterstützung von Verschlüsselungsstandards wie OpenPGP, S/MIME und TLS
- Geeignete Lösung zur sicheren Kommunikation mit beliebigen Empfängern (wie z. B. SEPPmail)
- Lösung benötigt auf der Empfängerseite keine Software zur Entschlüsselung der Mails
- Einfach zu installierende Lösung, vorzugsweise Hardware-Appliance
- Automatischer Versand des Passworts (z. B. per SMS)
- Zentrale User- und Schlüsselverwaltung
- Hochverfügbarkeit
- Integrierter Viren-, Spam- und Phishing-Schutz
- Domain-Verschlüsselung (benötigt für eine Domain bzw. Firma lediglich ein gemeinsames Zertifikat)
- Geringer administrativer Aufwand
- Gesamtkosten der Lösung (Gestehungspreis, Update- und Wartungskosten)



E-Mail-Verschlüsselung zwischen Realität und Anspruch



Die in der Schweiz entwickelte Appliance SEPPmail ermöglicht eine komfortable Push-E-Mail-Verschlüsselung.

GESETZLICHE GRUNDLAGEN

Die Anforderungen an die sichere elektronische Korrespondenz sind vielfältig. So regelt etwa das auf den 1.1.2008 stark revidierte Datenschutzgesetz (Bundesgesetz über den Datenschutz, DSG) die Beschaffung und Bearbeitung von Personendaten durch Private und Bundesorgane. Dabei soll der missbräuchliche Umgang mit Personendaten bekämpft werden. Das Gesetz ist u. a. relevant bei der Aufbewahrung von Geschäftsdokumenten, bei der E-Mail-Verschlüsselung (Datengeheimnis), bei Data Warehousing, Data Mining etc.



Webtips:

www.yourlaw.ch/itlaw/it_gesetze.asp
www.weblaw.ch/de/

WIE E-MAILS AUFZUBEWAHREN SIND

[Art. 9 GeBüV; Geschäftsbücherverordnung]

Zur Aufbewahrung von Unterlagen sind zulässig:

- unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger;
- veränderbare Informationsträger, wenn:
 - technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z. B. digitale Signaturverfahren)
 - der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z. B. durch «Zeitstempel»)
 - die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden
 - die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log files) ebenfalls aufbewahrt werden.

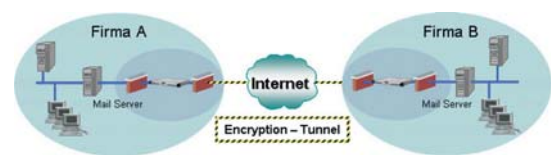
Informationsträger gelten als veränderbar, wenn die auf ihnen gespeicherten Informationen geändert oder gelöscht werden können, ohne dass die Änderung oder Löschung auf dem Datenträger nachweisbar ist (wie Magnetbänder, magnetische oder magnetooptische Disketten, Fest- oder Wechselplatten, Solid-state-Speicher).

Quelle: Adrian Rufener, Rufener & Partner

nissen bewerkstelligen. Dabei wird dem Empfänger anstelle des regulären Links ein Phishing-Mail zugeschickt. Diese Mail sieht auf den ersten Blick exakt gleich aus wie eine «richtige» Mail. Der darin beihaltete Link zur verschlüsselten E-Mail jedoch führt den Empfänger nicht direkt auf die Website des Secure Webmails. Stattdessen wird er über einen eigenen, präparierten Server «geschlauft». Dadurch kann sich der Hacker Zugang zum Account des Empfängers verschaffen und erhält Zugriff auf dessen Kommunikation – perfiderweise exakt auf den Teil der Information, den die Kommunikationspartner als «vertraulich» deklariert haben.

Der «Faktor Mensch» führt folglich dazu, dass eine technologisch an und für sich sichere Lösung de facto weniger sicher ist als die «normale», unverschlüsselte Kommunikation. Diese Problematik bleibt auch dann bestehen, wenn zusätzliche Sicherheitskomponenten wie OTP-Passworte eingesetzt werden.

Eine weitere Alternative sind Lösungsansätze, die die Installation eines – meist proprietären – Clients beim Empfänger verlangen. Dass dies in Anbetracht der unterschiedlichen Kundenumgebungen nicht immer ganz unproblematisch ist, liegt auf der Hand.



Durch den Einsatz von sogenannten Domain-Zertifikaten können ganze E-Mail-Domänen einfach und mit geringem Verwaltungsaufwand sicher per E-Mail kommunizieren.

• PDF-«Verschlüsselung»

Im Bestreben, Dokumente für Dritte unlesbar zu übermitteln, werden auch immer wieder passwortgeschützte PDF-Dateien thematisiert. Dazu wird eine Mail in ein PDF-Dokument umgewandelt, das sich durch den Empfänger erst nach der richtigen Eingabe des notwendigen Passworts lesen lässt. Diese grundsätzlich komfortable Lösung ist mit mehreren Unzulänglichkeiten behaftet. So entstehen bei der PDF-Umwandlung nicht selten Formatierungsprobleme (namentlich bei Anhängen), die Signatur des Absenders wird zerstört und die Lesbarkeit der Dokumente ist in Abhängigkeit der auf der Empfängerseite installierten PDF-Reader. Noch stärker ins Gewicht fallen sogenannte Brute-force-Attacken, bei denen alle möglichen Passwörter automatisch generiert und geprüft werden. Demnach ist es möglich, passwortgeschützte PDF-Dateien abzufangen und zu entschlüsseln. Die für die Attacke notwendigen Tools kann sich der Angreifer aus dem Internet herunterladen. Die Suche nach den Begriffen «PDF password



E-Mail-Verschlüsselung

recovery» findet eine ganze Reihe von Anbietern entsprechender Programme.

• Push-Mail-Verschlüsselung

Bei der Push-Mail-Verschlüsselung werden die Mails – ganz im Gegensatz zur Lösungsvariante Secure Webmail – durch eine firmeneigene Secure-Mail-Plattform (Appliance) verschlüsselt an den Empfänger verschickt. Zudem erhält der Empfänger ein persönliches Passwort, das beispielsweise per SMS übermittelt wird. Will nun der Empfänger die verschlüsselte Nachricht lesen, wird diese automatisch an die Secure Mail Appliance des Versenders zurückgeschickt. Nach Eingabe der korrekten Zugriffsdaten wird ihm die Mail in entschlüsselter Form in seinem Browser präsentiert. Die Push-E-Mail-Verschlüsselung (die Plattform SEPPmail bietet dazu eine einfache, patentierte Lösung) gilt dank einer sogenannten «Zwei-Faktoren-Authentisierung» als sicherste Verschlüsselungstechnologie. So wird nicht nur das Passwort, sondern auch die Originalnachricht selbst benötigt, um die Mail lesen zu können. Phishing-Attacken werden dadurch nutzlos. Darüber hinaus benötigen Push-E-Mail-Verschlüsselungslösungen auf der Empfängerseite keine spezifischen Programme, Plug-ins oder Zertifikate. Folglich unterstützen sie den Versand verschlüsselter E-Mails an jeden gewünschten Empfänger.

Angesichts der Tatsache, dass die verschlüsselten Mails nicht auf dem Gateway des Versenders, sondern bei den jeweiligen Empfängern gespeichert werden, ist der Speicherplatzbedarf der Secure Mail Appliances höchst bescheiden.

Ein Zertifikat für alle

Dank Push-E-Mail-Verschlüsselungslösungen sind die Sicherheitslücken früherer Lösungen komplett eliminiert und die Umsetzung einer sicheren (und trotzdem) komfortablen E-Mail-Kommunikation Realität. Unterstützt die gewählte Plattform gar eine sogenannte «Domain-Verschlüsselung», wird für alle Mitarbeitenden beziehungsweise für alle ab einer bestimmten Domain verschickten Mails lediglich ein gemeinsames Zertifikat benötigt, was deren Handhabung weiter vereinfacht. Bei der Lösung SEPPmail ist diese Domainverschlüsselung komplett automatisiert (mehr als 200 mit SEPPmail ausgerüstete Schweizer Domänen kommunizieren bereits verschlüsselt untereinander). Appliance-basierte Secure-Mail-Lösungen sind bereits ab rund 2000 Franken erhältlich. Somit sind nicht nur grosse Unternehmen, sondern auch Kleinstbetriebe, Gemeindeverwaltungen, Anwaltskanzleien und Ärzte in der Lage, sensible Daten gesichert zu übermitteln. Beinhaltet die Lösung gar Funktionen wie elektronische Signatur, Anti-Spam und Anti-Virus, sind der sicheren elektronischen Kommunikation kaum Grenzen gesetzt. □