E-Mail-Verschlüsselung

Ungeschützte E-Mails sind unsicherer als eine Postkarte

E-Mails werden mehrheitlich unverschlüsselt verschickt, obwohl sie auf ihrem Weg durchs Internet von vielen Augen eingesehen werden können. Dies mit möglicherweise weitreichenden Folgen; ist es für Hacker doch vergleichsweise einfach, ungesicherte E-Mails abzufangen beziehungsweise einzusehen, ohne dass der Absender oder der legitime Empfänger etwas davon merkt.

Stefan Klein

Obwohl die Verschlüsselung von E-Mails in zahlreichen Branchen zwingend notwendig ist – etwa im Finanz- und Gesundheitswesen, bei Bund und Kantonen, bei Anwälten und Notaren –, wird das Gros der elektronischen Post noch immer ungesichert verschickt.

Unsicherer als eine Postkarte

Doch es ist für Hacker vergleichsweise einfach, ungesicherte E-Mails abzufangen beziehungsweise einzusehen, ohne dass der Absender oder der legitime Empfänger etwas davon merkt. Ebenso problematisch ist das so genannte «Mail Spoofing». Dabei werden E-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 tief greifende IT-Kenntnisse noch spezielle Tools. Vielmehr lassen sie sich einfach über Outlook (und andere Mail-Programme) ausführen. Etwas komplexer präsentiert sich die dritte Problematik im Bereich der elektronischen Post: die Veränderung von E-Mails. Verschaffen sich Hacker Zugriff auf einen Mail-Server, besteht für sie die Möglichkeit, E-Mails einzusehen und deren Inhalt vor der Weiterleitung zu modifizieren. Den Betrugsmöglichkeiten sind dabei kaum Grenzen gesetzt.

Grundsätzlich wäre es einfach möglich, der beschriebenen Problematik Einhalt zu gebieten. Trotzdem werden entsprechende Verschlüsselungs- und Signaturlösungen selten genutzt. Dies dürfte unter anderem 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» oder modifiziert, da keine entsprechenden Anzeichen vorhanden seien. Und werden entsprechende kriminelle Machenschaften trotzdem erkannt, sind die Geschädigten darauf bedacht, diese totzuschweigen.

«Wir haben kein Problem»

Ein wichtiger Grund für die bescheidene Nutzung der E-Mail-Verschlüsselung dürfte

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

ferner 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 falschen Annahme, die elektronische Kommunikation sei gesichert. Dies ist jedoch nicht der Fall. So wird die elektronische Post zwar von einem gesicherten zu einem andern gesicherten Arbeitsplatz übermittelt, passiert auf diesem Weg jedoch zahlreiche, für Absender und Empfänger unbekannte Server. Dadurch entfällt jede Kontrolle darüber, wer Zugriff auf die E-Mails hat.

Ebenso wichtig für den seltenen Einsatz der E-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.

Unterschiedliche Lösungen

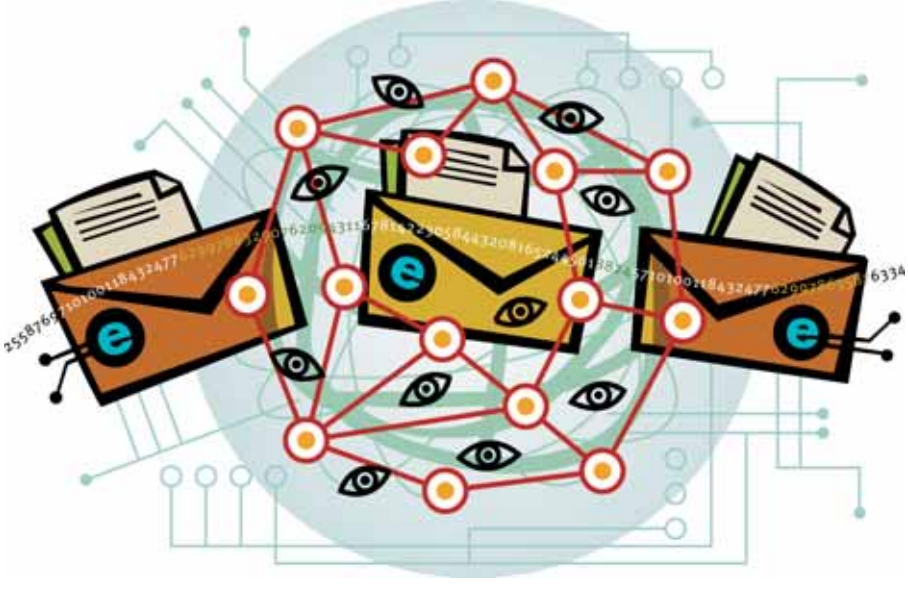
Um der beschriebenen Problematik zu begegnen, stehen unterschiedliche Lösungsansätze und Technologien zur Verfügung.

PGP und S/MIME

Die Technologien PGP (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extension) gelten als «Verschlüsselungspioniere». 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 Leben kaum anzutreffen. Werden PGP und S/MIME allerdings in einer Mail-Gateway-Appliance wie zum Beispiel 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 er-



Unverschlüsselt übermittelten E-Mail können durch Dritte abgefangen und eingesehen werden, ohne dass Sender und Empfänger etwas davon merken.

Verschiedene Technologien im Vergleich

	«Secure Webmail»	PDF-Verschlüsselung	Selbstextrahierendes Archiv	Spezieller Client	Push-Mail
Keine Speicherung ausgehender E-Mails	x	✓	✓	✓	✓
Phishing-Resistent	x	✓	✓	✓	✓
Resistent gegenüber Brute-force-Attacken	✓	x	x	✓	✓
Unterstützung von «eingeschriebenen E-Mails»	✓	x	x	x	✓
Keine Installation bei Empfänger notwendig	✓	✓	✓	x	✓
Auf den gängigen Plattformen lesbar	✓	✓	x	x	✓
Zwei-Faktoren-Authentisierung	x	x	x	✓	✓

Das Push-Mail-Verfahren ermöglicht als einzige Technologie eine einfache und dennoch sichere Kommunikation mit beliebigen Empfängern.

hält der Empfänger anstelle der E-Mail 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» so genannte «Man in the middle»-Attacken mit relativ bescheidenen Mitteln und Kenntnissen 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» E-Mail. Der darin beinhaltete 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 – exakt auf den Teil der Information, den die Kommunkationspartner eigentlich als «vertraulich» deklariert haben.

Verschlüsselung von PDF-Dateien

Im Bestreben, Dokumente für Dritte unlesbar zu übermitteln, werden auch 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. Dieser Lösungsweg ist nicht unproblematisch. So entstehen bei der PDF-Umwandlung nicht selten Formatierungsprobleme. Zudem wird die Signatur des Absenders zerstört und die Lesbarkeit der Dokumente ist abhängig von dem auf der Empfängerseite installierten PDF-Reader. Noch stärker ins Gewicht fallen so genannte Brute-force-Attacken, bei denen alle möglichen Passwörter automatisch generiert und geprüft werden. Demnach ist es somit möglich, passwortgeschützte PDF-Dateien abzufangen und zu entschlüsseln.

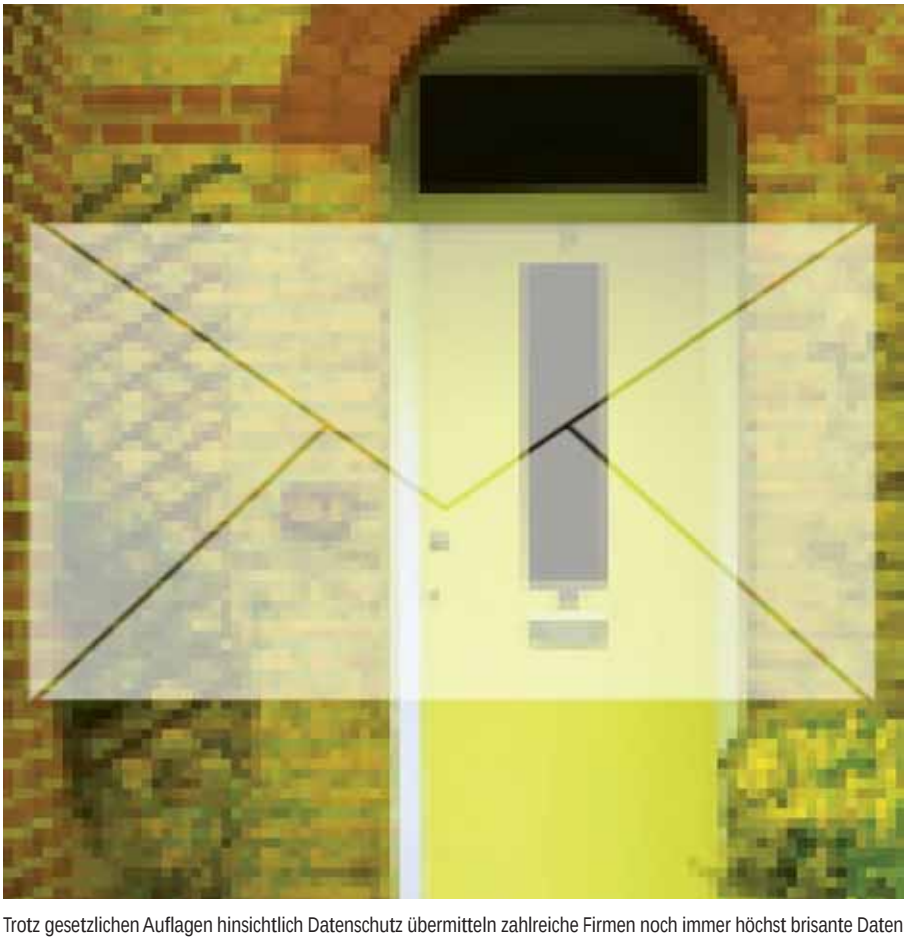
Push-E-Mail-Verschlüsselung

Bei dieser Mailverschlüsselungstechnologie werden die E-Mails 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

Kriterien bei der Evaluation

Im Rahmen der Evaluation einer Verschlüsselungslösung sollten unter anderem die folgenden Kriterien berücksichtigt werden:

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



Trotz gesetzlichen Auflagen hinsichtlich Datenschutz übermitteln zahlreiche Firmen noch immer höchst brisante Daten per Mail – ungeschützt.

Gesetzliche Grundlagen

Die Anforderungen an die sichere elektronische Korrespondenz sind vielfältig. So regelt etwa das auf den 1. Januar 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 unter anderem relevant bei der Aufbewahrung von Geschäftsdokumenten, bei der E-Mail-Verschlüsselung (Datengeheimnis), bei Data Warehousing, Data Mining usw. Weitere Informationen über die rechtlichen Grundlagen stehen über folgende Links zur Verfügung:

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

der korrekten Zugriffsdaten wird ihm die Mail in entschlüsselter Form in seinem Browser präsentiert. Die Push-E-Mail-Verschlüsselung gilt dank einer so genannten «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 verunmöglicht. 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.

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. ■

Fragen

Stefan Klein
???
ZOE-One GmbH
Pilatusstrasse 4, 6036 Dierikon
Tel. 041 455 40 50
info@zoe-one.com
www.zoe-one.com