Sichere E-Mails sind Pflicht

Der Versand von vertraulichen Informationen via E-Mail ist mit grossen Gefahren verbunden. Secure E-Mail ist darum längst keine Option mehr, sondern ein Muss.

Von Jürg Hefel

Die Informationsspionage ist ein grosses Ding. Gemäss dem deutschen Verfassungsschutz steht die Industrie- und Wirtschaftsspionage nach Hackerangriffen und Viren auf dem dritten Platz der Gefährdungen für Organisationen und Unternehmen. In einem «Handelsblatt»-Interview von Januar 2014 bezifferte Hans-Georg Maassen, Präsident des Bundesamts für Verfassungsschutz, den jährlichen Schaden, welcher der deutschen Wirtschaft durch Spionage entsteht, auf rund 50 Milliarden Euro. Detaillierte Zahlen für die Schweiz liegen zwar nicht vor, dürften sich aber prozentual zur Wirtschaftsleistung in einem vergleichbaren Rahmen bewegen.

Eine im Zusammenhang mit der Informationsspionage oft vernachlässigte Schwachstelle ist die E-Mail-Kommunikation. Werden sensitive und vertrauliche Informationen ungesichert via E-Mail verschickt, ist es für Hacker ein Leichtes, diese unbemerkt abzufangen beziehungsweise einzusehen. So erhalten Staaten und Mitbewerber Zugriff auf Offerten, Kundenlisten, Forschungsresultate, technische Dokumentationen und so weiter. Problematisch ist auch die unbemerkte Veränderung von Nachrichten. Verschaffen sich Hacker Zugriff auf einen E-Mail-Server, haben sie die Möglichkeit, Inhalte so zu modifizieren, dass Schaden entsteht.

Die Kernproblematik dieser Gefahren ist, dass diese mehrheitlich unterschätzt und in der täglichen Praxis nicht erkannt werden. So besteht vielerorts die Meinung, der eigene E-Mail-Verkehr werde nicht kompromittiert, da keine entsprechenden Anzeichen vorliegen. Ferner gehen viele Nutzer davon aus, dass Sicherheitsvorkehrungen wie UTM-Appliances oder Anti-Viren-Lösungen die E-Mail-Kommunikation sichern. Doch dem ist nicht so. Auf ihrem Weg von A nach B passieren E-Mails zahlreiche unbekannte Server. Somit entfällt jegliche Kontrolle darüber, wer wann welche Zugriffe auf die Nachricht hat. Angesichts dieser Tatsachen ist es bemerkenswert, dass Firmen in der Regel bereit sind, grosse Summen in den Schutz des Firmennetzes nach aussen (Gateway-Schutz) zu investieren, kritische Daten, die das Unternehmen verlassen, aber ungeschützt auf Reisen schicken.

IN KÜRZE

- Nicht verschlüsselt übertragene E-Mails können durch Dritte abgefangen, eingesehen und verändert werden.
- Ein sicherer E-Mail-Verkehr lässt sich auf Basis unterschiedlicher Technologien umsetzen.
- Benötigt wird neben einer Verschlüsselung eine Signatur auf Basis eines persönlichen Benutzerzertifikats.

Sensitive Daten wirksam schützen

Die zunehmenden Gefahren im Bereich der elektronischen Kommunikation sollten staatliche Stellen, Firmen und Institutionen dazu veranlassen, ihre E-Mail-Kommunikation umfassend zu schützen. Dazu sind zwei sich ergänzende Vorkehrungen notwendig. Einerseits die Verschlüsselung der übertragenen Nachrichten, welche sicherstellt, dass diese nicht durch Unbefugte einsehbar sind. Andererseits braucht es eine Signatur der Nachricht auf Basis eines persönlichen Benutzerzertifikats. Damit wird zum einen die Unveränderlichkeit der übermittelten Daten garantiert, zum anderen die Echtheit des Absenders bestätigt.

Nebst sicherheitsbezogenen Aspekten sorgen zahlreiche weitere Gründe für den Einsatz einer Secure-E-Mail-Plattform. Dazu gehören beispielsweise Compliance-Richtlinien. So sind Berufsgeheimnisträger wie Ärzte, Anwälte oder Finanzdienstleister von Gesetzes wegen zu einer gesicherten E-Mail-Kommunikation verpflichtet. Genauso gilt das für Firmen, die Vorgaben wie SOX, HIPAA, Basel-III oder PCI erfüllen müssen. Werden die Richtlinien nicht eingehalten, kann das Management im Schadenfall zur Rechenschaft gezogen werden. Auch E-Government beziehungsweise die sichere E-Mail-Kommunikation unter und mit Behörden ist ein zunehmend wichtigerer Anwendungsbereich.

Ein weiterer Grund für den Einsatz von E-Mail-Verschlüsselungslösungen sind Kosteneinsparungen, die sich durch die Digitalisierung von Geschäftsprozessen ergeben. Anwendungen wie papierlose Lohnabrechnungen oder die elektronische Übermittlung von Laborberichten im Gesundheitswesen sind ohne verschlüsselte Datenübertragung nicht denkbar. Ein weiterer Treiber ist der Imagefaktor. So erwarten auf Sicherheit setzende Kunden von ihren Lieferanten und Partnern, dass die E-Mail-Kommunikation verschlüsselt erfolgt. Zudem wird das Signieren von E-Mails als Qualitätsmerkmal im Umgang mit (Kunden-)Daten gewertet.

Technologien und Möglichkeiten

Secure E-Mail lässt sich auf Basis unterschiedlicher Technologien umsetzen. Nachfolgend ein paar Beispiele:

PGP und S/MIME: Bei PGP (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extension) handelt es sich um Nutzerbasierte Technologien, wobei jeder Teilnehmer für die verschlüsselte Kommunikation ein eigenes Zertifikat benötigt. Dabei setzt S/MIME auf hierarchische Zertifikate, die durch eine akkreditierte Zertifizierungsstelle (Certificate Authority, CA) ausgestellt werden. PGP hingegen basiert auf einem nicht hierarchischen Modell und setzt auf ein Netz des Vertrauens anderer PGP-Teilnehmer. Die Vertrauenswürdigkeit muss ein Empfänger einer E-Mail somit selbst einschätzen und damit auch, ob das Zertifikat tatsächlich dem Absender gehört. Damit sich nicht jeder einzelne Benutzer um die Verschlüsselung kümmern muss, existieren am Markt dedizierte Secure-E-Mail-Appliances mit integrierten Zertifikaten beziehungsweise Schlüsselpaaren. Diese übernehmen den gesamten Ver- und Entschlüsselungsprozess der jeweiligen E-Mail.

TLS: Bei TLS handelt es sich um eine gesicherte Punkt-zu-Punkt-Verbindung, die lediglich auf einer Leitungsverschlüsselung basiert. TLS ist mit einem hohen Verwaltungsaufwand behaftet und eignet sich primär für Verbin-

dungen zwischen internem Mail-Server und Gateway.

Secure Webmail mit Zwischenspeicherung: Erfolgt die E-Mail-Kommunikation via ein sicheres Webmail-System mit Zwischenspeicherung, erhält der Nachrichten-Empfänger anstelle der eigentlichen E-Mail einen Link, der ihn via Web zur verschlüsselten Nachricht führt. Diese Lösung ist mit beachtlichen Sicherheitsrisiken verbunden. So lassen sich «Man in the Middle»-Attacken mit relativ bescheidenen Mitteln realisieren. Dabei erhält der Empfänger anstelle des regulären Links eine echt wirkende Phishing-Mail zugestellt, deren Link nicht zur verschlüsselten Nachricht, sondern zu einem korrumpierten Server führt.

Verschlüsselte PDF-Dateien: Ein weiterer unsicherer Weg ist der Versand passwortgeschützter PDF-Dateien. Der vermeintliche Schutz lässt sich einfach mittels Brute-Force-Attacken aushebeln. Dabei werden alle möglichen Passwörter automatisch generiert und das passwortgeschützte PDF-Dokument in kürzester Zeit entschlüsselt. Zu beachten ist ferner, dass das generierte Passwort nicht veränderbar ist und dadurch bei Verlust nicht neu erstellt werden kann (Passwort-Reset).

Push-E-Mail-Verschlüsselung: Bei dieser E-Mail-Verschlüsselungstechnologie handelt es sich um ein Verfahren mit einer Zwei-Faktor-Authentisierung. Dabei werden E-Mails durch eine (firmeneigene) Secure-E-Mail-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. Ist dies erfolgt, wird die Nachricht angezeigt. Idealerweise setzen Firmen bei der Nutzung der Push-E-Mail-Verschlüsselung auf eine revisionskonforme Secure-E-Mail-Plattform, die Compliance-Anforderungen entspricht und empfängerseitig keine spezifische Software voraussetzt. Dieses Verfahren wurde von der Schweizer Firma Seppmail patentiert und kommt heute auch bei Incamail sowie bei HIN, einer Lösung für sichere E-Mails im Schweizer Healthcare-Bereich, zum Einsatz.

Push-E-Mail aus der Cloud: Um von der Push-E-Mail-Verschlüsselung zu profitieren, ist nicht zwingend die Anschaffung einer Appliance notwendig. Alternativ können Kunden auf Cloud-Lösungen zurückgreifen, auch aus der Schweiz.

Die E-Mail-Kommunikation ist eine oft vernachlässigte Sicherheitslücke in IT-Systemen.

Managed-Domain-Verschlüsselung: Besonders bequem präsentiert sich die E-Mail-Verschlüsselung zwischen dedizierten Domains. Ein mit Managed Domain Encryption (MDE) bezeichnetes Verfahren sorgt für eine automatische und transparente E-Mail-Verschlüsselung zwischen Secure-E-Mail-Appliances – ohne Zutun der User.

Authentizität mit Zertifikaten aus der Schweiz

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 sicherzustellen, müssen E-Mails neben der Verschlüsselung wie erwähnt auch 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, sofern die Nachricht mit dem Zertifikat signiert wurde.

Auf der Liste der gemäss Bundesgesetz über die elektronische Signatur (ZertES) anerkannten Anbieter von Zertifizierungsdiensten findet man vier Unternehmen beziehungsweise Institutionen: Quovadis Trustlink, Swisscom, Swisssign sowie das Bundesamt für Informatik und Telekommunikation (BIT). Bei der Wahl eines Anbieters sollte darauf geachtet werden, dass es sich um ein unabhängiges Unternehmen handelt. Ein solches ist beispielsweise Swisssign, eine Tochtergesellschaft der Schweizerischen Post. Swisssign, der grösste SSL-Zertifikatsanbieter Zentraleuropas überhaupt, entwickelt seine CA-Software ausschliesslich in der Schweiz und vertraut einzig und allein auf die eigene Root-CA – dies im Gegensatz zu vielen anderen Zertifikatsanbietern, deren ursprüngliche Herausgeber wiederum auf amerikanischen Root-CAs basieren und dem Paragraph 702 des «Foreign Intelligence Surveillance Act» (FISA) unterliegen. Dieser befugt die NSA, die Kommunikation ausländischer Bürger ohne Genehmigung abzuhören, sofern sie nicht auf amerikanischem Territorium sind. Dabei können Dienstanbieter «zur unverzüglichen Bereitstellung aller erforderlichen Informationen, Anlagen oder Hilfen an die Regierung für den Erwerb ausländischer Geheimdienstinformationen angehalten» und folglich gezwungen werden, kryptographische Schlüssel (SSL) offenzulegen.

Durch die Offenlegung der Aktivitäten der amerikanischen Geheimdienste hat das Thema E-Mail-Verschlüsselung deutlich an Aktualität gewonnen – und die Nachfrage nach Secure-E-Mail-Lösungen ist in den letzten Monaten deutlich gestiegen. Es ist ein Gebot der Stunde, E-Mails umfassend zu schützen, die Authentizität des Absenders zu garantieren und die Unverfälschtheit der Botschaft zu sichern.

Jürg Hefel ist Product Manager bei Boll Engineering für die E-Mail-Verschlüsselungslösungen von Seppmail.