E-Mail-Verschlüsselung für alle – mit allen

Die Erkenntnis, dass der Austausch von Informationen via E-Mail wirksam geschützt werden muss, setzt sich mehr und mehr durch. Neue Technologien, Architekturen und Services vereinfachen den Weg.

Ob Offerten, Kundendaten, Bestellungen oder Rechnungen – ob Vertragsentwürfe, Projektpläne, Entwicklungsunterlagen oder Forschungsresultate … vertrauliche Informationen jeglicher Art werden seit dem Siegeszug der elektronischen Kommunikation exzessiv – und oft bedenkenlos – verschickt. Allerdings besteht ein zunehmendes Bewusstsein dafür, dass sensitive Daten nicht schutzlos auf die Reise durchs Internet geschickt werden sollten. Neben der spürbar wachsenden Sensibilisierung für die gesicherte E-Mail-Kommunikation führen auch gesetzliche Rahmenbedingungen dazu, dass Firmen, Personen und Institutionen ihre elektronische Kommunikation vermehrt schützen. So sind beispielsweise Berufsgeheimnisträger wie Ärzte, Anwälte oder Finanzdienstleister vom Gesetzgeber verpflichtet, elektronisch übertragene Daten zu verschlüsseln. Eine weitere treibende Kraft ist die Forcierung und Umsetzung von E-Government-Strategien, die sich nur dann etablieren können, wenn ein gesicherter Informationsaustausch mit den Behörden garantiert ist.

Von der Awareness zur Umsetzung

Der umfassende Schutz der elektronischen Kommunikation ist eine vielschichtige Herausforderung. So gilt es einerseits, die Authentizität des Senders zu garantieren, und andererseits die Vertraulichkeit der Botschaft zu sichern. Zudem muss gewährleistet sein, dass die übertragene Nachricht ausschliesslich vom berechtigten Empfänger eingesehen werden kann und dass deren Inhalt sein Ziel unverändert erreicht. Diesen Anforderungen zu entsprechen ist zwar seit einigen Jahren möglich. Trotzdem werden entsprechende Verschlüsselungs- und Signaturlösungen nur selten genutzt. Dies dürfte nicht zuletzt darin begründet sein, dass die unterschiedlichen bestehenden Verschlüsselungsverfahren nicht kompatibel sind, teilweise nur limitierte Schutzfunktionen aufweisen und die Handhabung zu komplex ist.

Kommen für den gesicherten Nachrichtenaustausch Verschlüsselungstechnologien wie PGP (Pretty Good Privacy), S/MIME (Secure Multipurpose Internet Mail Extension) oder TLS (Transport Layer Security) zur Anwendung, benötigt jeder Benutzer eine dedizierte Software auf seinem PC sowie ein eigenes Zertifikat. Damit Nachrichten und deren Anhänge verschlüsselt übertragen werden können, müssen Sender und Empfänger zudem dieselbe Technologie einsetzen, was der verbreiteten Nutzung von Verschlüsselungstechnologien hinderlich ist. Diese Hürde zu umgehen vermögen sogenannte «Secure Webmail»-Lösungen. Sie benötigen auf dem Empfänger-PC keine spezifische Verschlüsselungssoftware. Stattdessen erhält der Empfänger anstelle einer verschlüsselt übertragenen E-Mail einen Link, der ihn via Web gesichert zur Nachricht führt. Allerdings ist diese grundsätzlich komfortable Lösung mit Vorsicht zu geniessen, da sie

BOLL Engineering AG

BOLL
IT Security Distribution

Jurastrasse 58 | 5430 Wettingen,
Tel. 056 437 60 60
info@boll.ch | www.boll.ch

sogenannte «Man in the Middle»-Attacke ermöglicht. Dabei erhält der Empfänger anstelle des regulären Links eine Phishing-Mail, deren Link nicht direkt, sondern über den Umweg eines Phishing-Servers zur gewünschten Nachricht führt. Eingaben des E-Mail-Empfängers (z. B. User-Name und Passwort) werden dadurch für die Hacker transparent. Ein weiterer erschwerender Faktor liegt darin, dass «Secure Webmail»-Lösungen die zu übertragenden E-Mails nicht tatsächlich ausliefern, sondern auf dem Mail-Server des Versenders speichern und den berechtigten Personen lediglich zur Ansicht zur Verfügung stellen. Dadurch ergeben sich – je nach Firmengrösse – enorme Datenmengen, die gespeichert, archiviert und verwaltet werden müssen, was erhebliche Kosten verursachen kann.

Von der vermeintlichen zur tatsächlichen Sicherheit

Mängel dieser Art umgehen Systeme, die auf der Push-PDF-Technologie basieren. Sie verschlüsseln PDF-Dokumente automatisch und übertragen sie passwortgeschützt. Dadurch sind die Dokumente für Dritte nicht einsehbar. Doch auch dieses für die Empfänger grundsätzlich bequeme Verfahren ist nicht unproblematisch. So entstehen bei der PDF-Umwandlung häufig Formatierungsfehler. Wichtiger noch: Signaturen werden durch die Umwandlung unwiderruflich zerstört, wodurch die Authentizität des Senders nicht mehr verifizierbar ist. Erschwerend kommt hinzu, dass sich das Push-PDF-Verfahren durch Brute-Force-Attacken vergleichsweise einfach aushebeln lässt. Dabei werden alle möglichen Passwörter automatisch generiert, wodurch sich passwortgeschützte PDF-Dokumente in kurzer Zeit durch Unbefugte entschlüsseln lassen.

Diesen Nachteilen zu begegnen vermögen sogenannte Secure-E-Mail-Appliances. Dabei verschlüsselt eine im Firmennetz installierte Secure-E-Mail-Plattform die E-Mail-Nachrichten und sendet diese als HTML-Mail an den gewünschten Adressaten. Will der Empfänger den verschlüsselten Anhang öffnen, wird dieser automatisch an die Secure-E-Mail-Appliance übermittelt. Danach wird der Empfänger aufgefordert, sich mit seinen persönlichen Zugangsdaten zu identifizieren. Ist dies erfolgreich abgeschlossen, wird ihm die Nachricht in seiner gewohnten Mail-Umgebung angezeigt. Bei diesem Verfahren benötigt der Empfänger für den geschützten Zugriff auf die übermittelten Daten die Nachricht selbst sowie ein persönliches Passwort, was als «Zwei-Faktoren-Authentisierung» bezeichnet wird. Dank der dadurch gewonnenen hohen Sicherheit sind Secure-E-Mail-Lösungen wie die in der Schweiz entwickelte SEPPmail-Appliance revisionskonform und entsprechen Compliance-Anforderungen wie SOX, HIPAA, PCI und Basel II.

Hybride E-Mail-Verschlüsselung

Von Bedeutung ist, dass Secure-E-Mail-Lösungen auf der Empfängerseite keine spezifische Software beziehungsweise Verschlüsselungstechnologien erfordern. Sie sind vielmehr in der Lage, weltweit mit jedem beliebigen Teilnehmer (Empfänger) verschlüsselt zu kommunizieren. Zudem bieten sie die Möglichkeit, Lesebestätigungen auszustellen, was mit «eingeschriebene E-Mail» bezeichnet werden kann.

HIN, Health Info Net, ermöglicht den Plattformteilnehmenden (rund 13 000 Hausärzte, über 230 Institutionen wie Spitäler und Labors sowie weitere Akteure des schweizerischen Gesundheitswesens) einen sicheren und datenschutzkonformen Datenaustausch. Bildquelle: iStockphoto

Hat der Empfänger auf seinem Rechner bereits eine der bestehenden Verschlüsselungstechnologien installiert (z. B. PGP, S/MIME, TLS), wird die Kommunikation noch einfacher. Dies aufgrund der Tatsache, dass Secure-E-Mail-Appliances alle gängigen Verschlüsselungsverfahren unterstützen und folglich eine direkte Übermittlung verschlüsselter Nachrichten ermöglichen. Allerdings: Bei dieser mit «User-based» bezeichneten Technologie benötigt jeder Anwender ein eigenes Zertifikat, was die Handhabung erschwert. Werden die Zertifikate (Schlüsselpaare) jedoch in einer dedizierten Secure-E-Mail-Appliance installiert, erfolgt die Ver- und Entschlüsselung der Nachricht auf der Plattform selbst – komplett automatisch, ohne jegliches Zutun der User.

Dieses von SEPPmail mit «Domain-Verschlüsselung» beziehungsweise «Managed Domain Encryption» (MDE) bezeichnete Verfahren bildet die komfortabelste Form, Secure E-Mail umzusetzen. So kann jede installierte SEPPmail-Appliance ohne Austausch von Schlüsseln an diesem Verbund teilnehmen. Ebenso lassen sich – wie zuvor erwähnt – Domain-Keys anderer Hersteller (z. B. S/MIME oder PGP) einbinden.

Secure E-Mail innerhalb des Benutzernetzwerks

Eine interessante Integrationsform für die automatische Verschlüsselung von E-Mails bilden Lösungen für sogenannte «Closed Groups». Ziel dabei ist es, den Informationsaustausch unter den Mitgliedern beziehungsweise Plattformteilnehmern automatisch und umfänglich zu sichern – und gegebenenfalls auch Personen und Firmen ausserhalb des Verbunds in die Secure-E-Mail-Umgebung einzubinden. Ein ▸

Dank der von SEPPmail angewandten «Zwei-Faktoren-Authentisierung» – der Empfänger benötigt für den Zugriff auf die Daten die Nachricht selbst sowie ein Passwort – und der vollständigen Auslieferung der E-Mail an den Kunden, wird die E-Mail-Kommunikation revisionskonform. Sie entspricht zudem Compliance-Anforderungen wie SOX, HIPAA, PCI und Basel II. Bildquelle: SEPPmail

diesbezüglich ideales Beispiel bildet das Gesundheitsnetzwerk HIN, Health Info Net AG. Die HIN-Plattform verbindet heute 13 000 Einzelabonnenten (rund 80 Prozent der Hausärzte) mit über 230 Institutionen (Spitäler, Labors etc.) sowie weitere Akteure des schweizerischen Gesundheitswesens.

HIN ermöglicht den Plattformteilnehmenden einen sicheren und datenschutzkonformen Datenaustausch. Basis dazu bildet der sogenannte HIN Mail Gateway 2.0, der auf der «Secure E-Mail»-Technologie von SEPPmail basiert und den Anschluss institutioneller E-Mail-Infrastrukturen an die HIN-Plattform erlaubt. Damit werden Anwenderinnen und Anwender in den Institutionen in die Lage versetzt, E-Mails mit sämtlichen HIN-Plattform-Teilnehmenden sicher und komfortabel auszutauschen.

Nun lanciert SEPPmail zusammen mit HIN eine komfortable Lösung zur integralen Einbindung von SEPPmail-Kunden. Diese erhalten die Möglichkeit, ihre E-Mail-Kommunikation mit HIN-Teilnehmern automatisch zu verschlüsseln. Die Anbindung an die HIN-Plattform ist für bestehende SEPPmail-Kunden einfach und komfortabel. Benötigt werden dazu lediglich ein sogenannter HIN-Konnektor, der sich auf der SEPPmail-Appliance aktivieren lässt, sowie ein Nutzungsvertrag mit HIN, der die Konnektionskosten (Nutzungsgebühren) regelt. Sind diese Voraussetzungen erfüllt, ist es allen SEPPmail-Kunden möglich, vertrauliche Nachrichten gesichert zu übertragen beziehungsweise den gesamten E-Mail-Verkehr automatisch zu verschlüsseln und digital zu signieren.

E-Mail-Verschlüsselung «in der Wolke»

Um Kosten zu sparen und den Administrationsaufwand zu minimieren gehen Firmen vermehrt dazu über, Teile ihrer IT an externe Partner auszulagern und die jeweiligen Dienste als Service zu beziehen. Heute stehen auch im Bereich Secure E-Mail leistungsfähige Cloud-Services zur Verfügung. Diese ermöglichen, ohne Aufbau und Betrieb einer eigenen Infrastruktur und folglich ohne Investitionskosten, «Secure E-Mail» umzusetzen. Demnach lassen sich vertrauliche Informationen weltweit an jeden gewünschten Empfänger verschlüsselt und digital signiert versenden – unabhängig von deren bestehender Hardware- und Softwareinfrastruktur und unabhängig davon, ob der Mail-Server inhouse oder ebenfalls extern betrieben wird.

Digitalisierung von Businessprozessen

Angesichts der Tatsache, dass mit «Secure E-Mail» einfache, komfortable und sichere E-Mail-Verschlüsselungslösungen vorhanden sind, erhält die Digitalisierung von Businessprozessen einen markanten Auftrieb – denn durch die Portierung bestehender Geschäftsprozesse auf Secure E-Mail lassen sich markante Kosteneinsparungen erwirken. Wird die Secure-E-Mail-Lösung beispielsweise in eine ERP-Lösung integriert, können Dokumente wie Offerten, Rechnungen und Lieferscheine sowie jegliche Art vertraulicher Informationen auf elektronischem Weg verschickt werden. Aufwendungen für den Postversand, für Kuverts und Handling entfallen komplett. Besonders anschaulich lässt sich dies im Bereich Banking illustrieren. Führt man sich die atemberaubende Zahl verschickter Kontoauszüge, Quartalsabrechnungen oder Steuerbescheinigungen vor Augen, wird klar, dass Secure E-Mail ein millionenschweres Einsparpotenzial offeriert. Nebst Finanzinstituten zählen auch grössere Firmen jeder anderen Branche zu den Gewinnern. Werden beispielsweise die monatlichen Lohnabrechnungen via Secure E-Mail verschickt, lassen sich sofort markante Kosteneinsparungen realisieren. Secure E-Mail kann selbst für Firmen interessant sein, die ihre Lohnabrechnungen via firmeninterne elektronische Plattform zur Verfügung stellen. Dies namentlich dank der höheren Sicherheit und Vertraulichkeit, die dadurch gewonnen wird. ■