Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2015

SICHERHEIT & DATENSCHUTZ

Verschlüsselung, Authentifizierung und Public-Key-Infrastruktur

Access Control:
Was Biometrie heute schon leisten kann

OpenPGP für Unternehmen:
Wie Open Encryption für Firmen funktioniert

E-Mail Security:
Welche Gefahren mit der Post kommen

Smart Grids & Industrie 4.0:
Wann kritische Infrastrukturen sicher sind

Vertrauensnetzwerke:
Wem wir unsere Schlüssel anvertrauen dürfen

Public-Key-Infrastruktur:
Welche Aufgaben eine PKI übernehmen muss

powered by: TeleTrusT Pioneers in IT security.

Nach innen und außen zuverlässig geschützt

Kombinierte Verschlüsselungsverfahren erfüllen sowohl Sicherheitsbedürfnisse als auch Compliance-Vorgaben

Dass E-Mail-Kommunikation nicht sicher ist, hat spätestens seit Snowdens NSA-Enthüllungen das öffentliche Bewusstsein erreicht. Daten werden im großen Stil kopiert und manipuliert, und niemand bemerkt es. Tatsächlichen Schutz gegen Cyberattacken kann nur eine umfassende PKI-basierte Verschlüsselung bieten.

E-Mails sind als Kommunikationsform längst nicht nur in der Mitte der Gesellschaft, sondern auch flächendeckend in der Wirtschaft angekommen. Ihre breite Verwendung in Unternehmen erklärt sich unter anderem aus ihrer Effizienz. Sie erlauben eine kostengünstige und standortunabhängige Kommunikation in Echtzeit, dokumentieren lückenlos den Kommunikationsverlauf und ermöglichen den einfachen Transport von Dateien ohne Medienbruch. Diese Vorteile möchten Unternehmen nicht missen, auch wenn es oft an der Sicherheit mangelt.

Echte Ende-zu-Ende-Verschlüsselung

Daher trifft der verantwortungsvolle Unternehmer Sicherheitsvorkehrungen, um nicht der Industrie- und Wirtschaftsspionage ausgeliefert zu sein und Firmeninterna zu schützen. Zusätzlich wird vom Gesetzgeber, etwa nach dem Bundesdatenschutzgesetz (BDSG), ein streng geregelter Umgang mit personenbezogenen Daten vorgeschrieben. Auch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wartet mit Compliance-Vorgaben auf, die eine Verschlüsselung nach dem Stand der Technik vorschreiben.

Eine Sicherheitsmaßnahme, die oft fälschlicherweise als vollwertiger Ersatz einer Ende-zu-Ende-Verschlüsselung (End-to-End Encryption oder E2EE) gewertet wird, ist die Verschlüsselung der Übertragungskanäle mittels Transport Layer Security (TLS). Damit ist der Einhaltung der Compliance-Regeln im ersten Schritt Genüge getan. Das Problem dabei: Auf den verschiedenen Stationen, die eine E-Mail durchläuft, wird nur der Weg von einem Server zum nächsten verschlüsselt. Den Server selbst passieren die E-Mails im Klartext. Auch im Postausgang und -eingang, den Anfangs- und Endpunkten der Verschlüsselungsstrecke, werden E-Mails unverschlüsselt abgelegt. Nur echtes End-to-End kann hier tatsächlich Sicherheit bieten.

Doch auch die Ende-zu-Ende-Verschlüsselung sollte abhängig vom Anwendungsfall differenziert betrachtet werden. Sie bedeutet die lückenlose Verschlüsselung vom Sendegerät bis zum Empfangsgerät. Die Nachrichten sind also nirgendwo im Klartext abgelegt, weder im Postausgang des Senders noch im Posteingang des Empfängers. Nur die Endnutzer verfügen letztlich über die notwendigen Schlüssel zum Ver- und Entschlüsseln. So lautet jedenfalls die Theorie.

Richtigerweise müsste End-to-End oft mit „Ende-zu-Weiß-nicht-genau“ übersetzt werden, da der Sender keine hundertprozentige Gewissheit darüber hat, dass sich der geheime Schlüssel wirklich nur im Besitz des adressierten Empfängers befindet. Verwendet dieser zum Beispiel ein Verschlüsselungs-Gateway, sieht man das den verwendeten Schlüsseln in der Regel nicht an. Vertrauen in die Unversehrtheit einer echten Ende-zu-Ende-Verschlüsselung kann es entsprechend nur geben, wenn sich beide Kommunikationspartner persönlich die verwendeten Zertifikate gegenseitig verifizieren und zusichern, dass es keine Kopie an anderer Stelle gibt.

Doppelt hält besser

Für den Großteil des internen und externen E-Mail-Verkehrs hat ein Unternehmen im Normalfall kein Interesse an einer durchgängigen Ende-zu-Ende-Verschlüsselung, bei der die geheimen persönlichen Schlüssel nur die jeweiligen Mitarbeiter besitzen. Diese Situation ist in etwa vergleichbar mit den Büroräumen am Firmensitz: Das Unternehmen gibt nicht jedem Mitarbeiter einen exklusiven Schlüssel für sein Büro. Es gibt so etwas wie ein Hausrecht inklusive der Nutzung von Zweit- bzw. Generalschlüsseln.

Genauso soll und muss ein Unternehmen schon aus Compliance-Gründen die Hoheit über die eigenen E-Mail-Daten besitzen. Ohne einen zentralen Zugriff auf den E-Mail-Verkehr ist auch der essenzielle Einsatz von Contentfiltern und Data-Loss-Prevention-Lösungen nicht möglich. Um nicht gänzlich die Kontrolle zu verlieren, müssen sonst flächendeckend Rollouts auf allen Clients organisiert und gepflegt werden.

Auch eine Archivierung ist ohne Nachschlüssel nicht sinnvoll, will man nicht die Archivzuführung ebenfalls dezentral auf den Clients realisieren. Entsprechend werden heute in der Regel in Unternehmen mithilfe von Public-Key-Infrastruktur-Anwendungen Kopien der geheimen Schlüssel der Mitarbeiter oder Generalschlüssel zentral und sicher verwaltet. Dazu gibt es verschiedene technische Ansätze, die im Allgemeinen als Key-Escrow-Verfahren bezeichnet werden.

Die genannten Problemfelder der Ende-zu-Ende-Verschlüsselung lassen sich durch eine einfache Veränderung des Blickwinkels auflösen. Am einen Ende der E-Mail-Verschlüsselung im geschäftlichen Bereich steht das Unternehmen an sich – also die juristische Person. Da die Mitarbeiter im Auftrag der Firma kommunizieren, ist der Sender beziehungsweise Empfänger grundsätzlich das Unternehmen. Deshalb kann die Grenze vom Internet zum Unternehmen als ein Endpunkt der sicheren externen Kommunikation angesehen werden. Zusätzlich sollten Unternehmen aber auch ihren internen Informationsaustausch mit

den eigenen Mitarbeitern wiederum End-to-End verschlüsseln. Dies könnte man dann gewissermaßen als Ende-zu-Ende-zu-Ende-Verschlüsselung bezeichnen.

Basis der Verschlüsselung ist die PKI

Eine wirksame E-Mail-Verschlüsselung basiert auf Public-Key-Infrastrukturen (PKIs). Dafür haben sich mit S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP zwei Standards etabliert. Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel (Zertifikate) und damit in den Vertrauensmodellen.

Der Enrollment-Prozess für X.509-Zertifikate, der für S/MIME eingesetzt wird, sieht vor, dass Schlüsselpaare beim Nutzer (im Unternehmen) generiert werden. Der private Schlüssel verbleibt dort, der öffentliche Schlüssel wird damit signiert und einer Certification Authority (CA) zur Zertifizierung übergeben. Die CA fügt dem öffentlichen Schlüssel ihre eigene Signatur hinzu und sendet den signierten öffentlichen Schlüssel zurück. Ab diesem Moment wird ein öffentlicher Schlüssel zum Zertifikat. Bei PGP signieren und zertifizieren sich die User ihre Schlüssel auf Basis persönlicher Kontakte gegenseitig und bilden damit ein Vertrauensnetzwerk (Web of Trust).

PKIs bauen darauf, dass Zertifikate breit gestreut werden, Dritte jedoch zu keinem Zeitpunkt Zugriff auf persönliche Schlüssel erhalten. Der Einsatz des Key-Escrow-Verfahrens innerhalb der Unternehmenskommunikation bleibt davon unberührt und sorgt für die Erfüllung von Compliance-Anforderungen, Zugriffsmöglichkeiten für zentrale Contentfilter, Data Loss Prevention (DLP) und Archivlösungen sowie die Datenhoheit des Unternehmens.

Schutz nach innen

Die beiden Verschlüsselungsmethoden S/MIME und PGP sind nicht miteinander kompatibel. Die Entscheidung im Unternehmen für einen Standard führt somit dazu, dass Verschlüsselung nur möglich ist, wenn der Kommunikationspartner genau denselben Standard nutzt. Im Unternehmensbereich hat sich S/MIME, in Kombination mit X.509-Zertifikaten, die durch Trustcenter oder im eigenen Unternehmen ausgestellt werden, vor der PGP-Verschlüsselung etabliert.

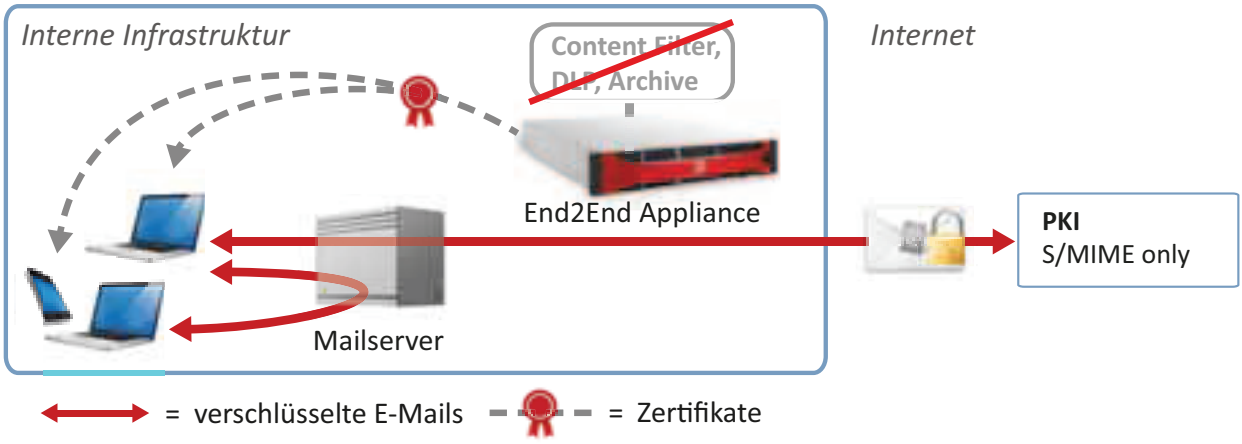
Wird PGP im Unternehmensumfeld genutzt, ist der Vertrauensaufbau in der Regel trotzdem hierarchisch. Anstelle einer breit angelegten Kreuz-Zertifizierung zwischen den einzelnen Mitarbeitern, gibt es einen zentralen Signer Key des Unternehmens, der analog einer CA im S/MIME-Umfeld alle PGP-Schlüssel der Mitarbeiter signiert. Damit wird allen anderen internen und externen Nutzern signalisiert, dass dieser Schlüssel nicht von irgendwem außerhalb des Unternehmens gefälscht wurde. Die Nutzung von PGP verlangt darüber hinaus eine Installation zusätzlicher Software auf den Clients. Denn der PGP-Standard wird anders als S/MIME von den heute im Unternehmensumfeld genutzten nativen E-Mail-Clients nicht generell unterstützt.

In der privaten E-Mail-Kommunikation ist – wenn überhaupt – die kostenfreie Verschlüsselung mit OpenPGP verbreitet. Auch kündigen große, im Privatkundenbereich relevante E-Mail-Provider, aktuell die Unterstützung von OpenPGP in ihren Web-Mail-Clients an. So ist davon auszugehen, dass insbesondere für Business-to-Customer-Szenarien (B2C) die Unterstützung von OpenPGP für Unternehmen in Zukunft wichtiger wird.

Sicherheit nach außen

Zum Verschlüsseln einer E-Mail wird bei PKI-basierten Methoden das Zertifikat (der öffentliche Schlüssel) des Empfängers benötigt. Die Nachricht kann nur vom Gegenstück des Zertifikats – nämlich dem privaten Schlüssel des Empfängers – entschlüsselt werden. Diese Zertifikate müssen vor der Verschlüsselung allerdings nicht nur gefunden, sondern auch validiert werden. In einer One-to-One-Situation lässt sich das als manueller Prozess durchführen. Die Kommunikationspartner tauschen die Fingerprints (Prüfsummen der Schlüssel) auf einem sicheren Kanal aus – oft bei persönlicher Begegnung oder durch den Upload auf eine Trustcenter-unabhängige Meta-Zertifikatssuchmaschine wie den Z1 Global TrustPoint – und bestätigen sie gegenseitig. Im geschäftlichen Einsatz, in dem gegebenenfalls eine große Anzahl Mitarbeiter und noch mehr externe Kommunikationspartner Zertifikate austauschen und bestätigen, verlängern und widerrufen, wäre das jedoch enorm aufwendig und langsam.

Wegen des komplexen Schlüssel- und Zertifikatsmanagements hat sich die seit Jahrzehnten verfügbare PKI-basierte Verschlüsselung direkt am Client bisher nicht in der Breite durchsetzen können. Während Privatanwender wahrscheinlich die Mühe scheuen oder wegen fehlendem Sicherheitsbewusstsein auf diese Technologie ganz verzichten, setzen Unternehmen und Organisationen eher auf zentrale Lösungsansätze, sogenannte Secure E-Mail Gateways, um die aufwendige PKI-basierte Verschlüsselung nicht an den vielen internen Clients implementieren zu müssen.



Quelle: Burkhard Wiegel

Bei Personal End-to-End haben Contentfilter ebenso wenig Zugriff auf die E-Mail wie der Gateway-Administrator (Abb. 1).

Gateways automatisieren das interne und externe Schlüssel- und Zertifikatsmanagement und bedienen sich zur Zertifikatssuche und -validierung weitestgehend spezieller Zertifikatsserverkomponenten. Dabei wird Server-basiert – und somit zentral und transparent für die Nutzer – der sicherheitssensible E-Mail-Verkehr gemäß den eingestellten Regelwerken (Policies) geschützt. Compliance Enforcement, eine hohe Nutzer-Akzeptanz sowie der Verzicht auf Client-Installationen sind die Vorteile, die einen Gateway-Einsatz attraktiv machen. Auf diese Weise können Keys sowohl mit X.509-Zertifikaten als auch mit OpenPGP verschlüsselt werden. Falls für externe Kommunikationspartner keine Zertifikate verfügbar sind, verwendet das Gateway alternative Verschlüsselungsmethoden.

Alternativen für Empfänger ohne PKI-Zertifikate

Für zertifikatslose Empfänger gibt es üblicherweise passwortbasierte Verschlüsselungsverfahren. Dabei wird zunächst die Nachricht in einem Puffer zwischengelagert (Spooling) und der Empfänger über die beabsichtigte Zustellung einer vertraulichen E-Mail informiert. Er muss sich dann authentifizieren und erhält die Nachricht beispielsweise als passwortverschlüsselten PDF-, HTML- oder ZIP-Container im E-Mail-Anhang zugestellt. Eine ebenfalls verbreitete Variante der passwortbasierten Verschlüsselung ist die Bereitstellung eines on-the-fly erstellten HTTPS-gesicherten Webmailers. De-Mail-Anbindungen, TLS-Unterstützung und VPN (Virtual Private Network) sind ebenso auf einigen Gateways verfügbar. So können Unternehmen ohne Verzögerung mit jedermann verschlüsselt kommunizieren.

Eine kontrovers diskutierte Option ist die Ad-hoc-Ausstellung von X.509-Zertifikaten für externe Kommunikationspartner. Auch diese Möglichkeit wird manchmal verfolgt, wenn man mit zertifikatslosen Empfängern verschlüsselt kommunizieren will. Der Sender agiert in diesem Fall selbst als CA und stellt on-the-fly Zertifikate und private Schlüssel für externe Nutzer aus. Auf diese Weise erhält der Empfänger in kurzem zeitlichen Abstand die verschlüsselte Nachricht, den privaten Schlüssel und das Zertifikat.

Damit ergeben sich allerdings einige Probleme, da grundsätzliche PKI-Funktionsweisen umgangen werden. Es stellen sich nicht nur heikle Sicherheitsfragen, weil ein Dritter – hier der Ersteller – Kenntnis der privaten Schlüssel der externen Nutzer hat. Es käme auch zu einer inflationären Zertifikatsvermehrung, würde sich dieser Ansatz in der Breite durchsetzen. Denn üblicherweise besitzt ein PKI-Teilnehmer nur ein Zertifikat beziehungsweise eine sehr geringe Anzahl von Zertifikaten, die er allen seinen Kommunikationspartnern zentral verfügbar macht – in etwa vergleichbar mit seiner Telefonnummer. Im Gegensatz dazu bekäme beim eben beschriebenen Ansatz jeder einzelne Mitarbeiter gegebenenfalls von Hunderten seiner Kommunikationspartner wieder jeweils ein separates Zertifikat ausgestellt. Man stelle sich dann nur einmal die vertrackte Situation vor, wenn dieser Nutzer den Arbeitgeber wechselt und damit auch eine andere E-Mail-Adresse erhält.

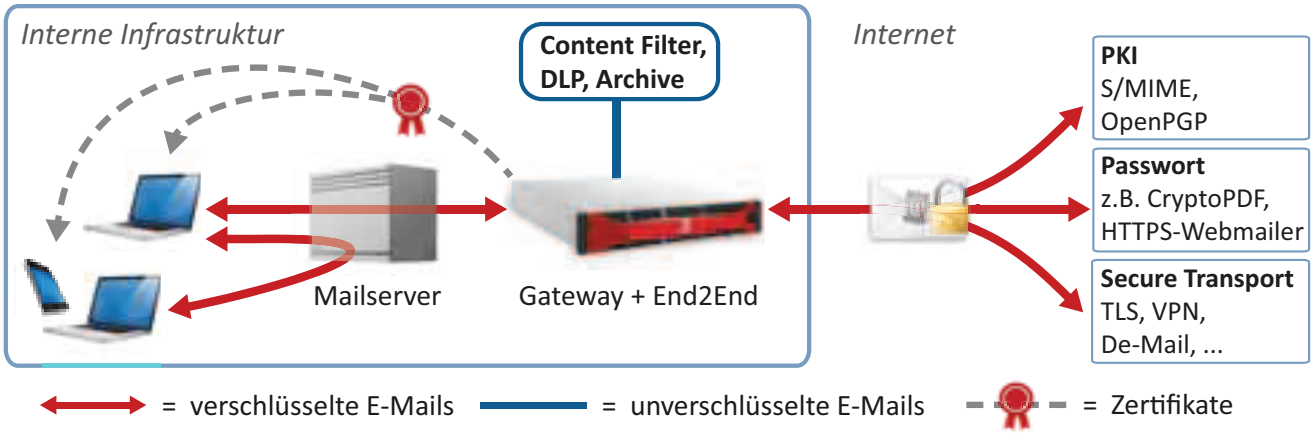
Grenzen der Gateway-Sicherheit

Ein Secure E-Mail Gateway bildet zwar eine zentrale Schnittstelle zum Internet, die von und nach außen ent- bzw. verschlüsselt. Innerhalb des Firmennetzwerkes werden die Nachrichten jedoch unverschlüsselt transportiert. Mit dem Gateway-Ansatz allein nutzen Unternehmen demnach keine klassische Ende-zu-Ende-Verschlüsselung. Für den Schutz gegen Geheimdienstprogramme und Wirtschaftsspionage im Internet ist dies dennoch eine sichere und bewährte Methode. Sie wird seit Jahren erfolgreich von Unternehmen, Behörden und Institutionen eingesetzt. Gleichwohl gibt es Anwendungen, bei denen echtes End-to-End notwendig ist.

Das betrifft beispielsweise die Kommunikation über mobile Endgeräte. Per Notebook, Tablet oder Smartphone ausgetauschte E-Mails werden über WLAN oder Mobilfunknetze im Klartext übertragen. Jede Verschlüsselung über die Transportstrecke Internet ist wirkungslos, wenn ein Angreifer mit etwas IT-Know-how und geringem technischen Equipment über WLAN oder Mobilfunknetze Nachrichten im Klartext abfangen kann. Eine fehlende interne Verschlüsselung erlaubt es außerdem jedem Administrator des Unternehmens mit Zugang zum E-Mail-Server, Inhalte unverschlüsselt auszulesen.

Deshalb gilt es, eine vertrauliche Kommunikation im Unternehmen – das heißt vom Gateway zum einzelnen Mitarbeiter und für den E-Mail-Austausch der Mitarbeiter untereinander – herzustellen. VPNs schützen beispielsweise generell vor Gefahren von außen, bieten aber ähnlich wie TLS nur Verschlüsselung auf Transportebene. Investitionen in Mobile-Device-Management-Systeme (MDM) können dafür sehr lohnend sein. Hierbei ist jedoch eher die Umgebung als Container geschützt und nicht zwingend die einzelne Nachricht. Im MDM-Bereich dominieren zudem Hersteller der „Five-Eyes-Staaten“ den Markt. Wer geheimdienstsicher verschlüsseln möchte, strenge eigene Ansprüche oder branchenspezifische Vorgaben zu erfüllen hat, sollte immer das

Quelle: Burkhard Wiegel



Organizational End-to-End gewährleistet eine sichere Kommunikation von und nach außen und sorgt für die notwendige Flexibilität (Abb. 2).

Ziel haben, die Nachrichten und Anhänge selbst zu verschlüsseln und nicht nur ihre Transportwege und Aufbewahrungsorte.

Leider ist nicht davon auszugehen, dass irgendeines der vielen neuen Start-ups in der Verschlüsselungsbranche die Situation in nächster Zeit revolutionieren wird. Deren Ansätze zielen zwar überwiegend auf mobile Endgeräte ab, wenden sich aber vor allem an Einzelanwender und erst in einem zweiten Schritt an Unternehmen. Oft werden dabei die unterschiedlichen Bedürfnisse nicht ausreichend berücksichtigt. Diese Angebote sehen zumeist vor, dass sich Sender und Empfänger bereits kennen und sich gemeinsam auf die Notwendigkeit einer sicheren Kommunikation verständigt haben. In der Regel müssen beide dann auch die gleiche Software installieren und bleiben auf das Endgerät angewiesen, auf dem die Software installiert ist. Eine spontane, effiziente und sichere Kommunikation lässt sich so nicht umsetzen. Zum Teil ist eine sichere Kommunikation auch nur auf bestimmten Betriebssystemen möglich. Derartige Einschränkungen machen den Einsatz für Unternehmen wenig attraktiv.

Personal und Organizational End-to-End

Es bleibt festzuhalten, dass sowohl intern als auch extern verschlüsselt werden sollte. Wenn diese Verschlüsselung in zwei verschiedenen Modi zur Verfügung steht, ist sie in der Tat auch auf breiter Basis unternehmenstauglich.

Im ersten Modus wird die E-Mail komplett durchgängig vom Sender bis zum Empfänger verschlüsselt. Das kann im Einzelfall auf persönlicher Ebene durchaus gerechtfertigt sein und wird deshalb als Personal End-to-End bezeichnet. Dies entspricht der klassischen Form der Ende-zu-Ende-Verschlüsselung. Personal End-to-End dient vor allem der Kommunikation zwischen einzelnen Usern im Hochsicherheitsbereich. Contentfilter und andere Applikationen haben hier keinen Zugriff auf die E-Mail-Inhalte. Ebenso wenig kann der Gateway-Administrator die Nachrichten auslesen oder manipulieren (Abbildung 1).

Für den Einsatz auf breiter Front hingegen eignet sich ein anderer Modus der E-Mail-Übertragung. Hier wird die E-Mail zwischen den Teilstrecken am Gateway umverschlüsselt und der Zugriff für Contentfilter, Virenschutzprogramme u. Ä. gewährt. Das ist ganz im Sinne der einsetzenden Organisation und wird deshalb als Organizational End-to-End betitelt. Im firmeneigenen Netzwerk setzt Organizational End-to-End auf S/MIME. Eine gekapselte, rein interne Public-Key-Infrastruktur dient dem sicheren Nachrichtentransport auf unternehmensinternen Strecken, einschließlich der Verschlüsselung von Nachrichten der Mitarbeiter untereinander. Am Gateway wird die Verschlüsselung unterbrochen und berechtigten Systemen innerhalb der Organisation der Zugriff gewährt. Da die Umverschlüsselung direkt innerhalb des Firmennetzwerkes stattfindet, bleibt ein hohes Sicherheitsniveau gewährleistet. Auf dem E-Mail-Server werden die Nachrichten in verschlüsseltem Zustand abgelegt und sind auf diese Art auch für Administratoren nicht auslesbar.

Von S/MIME, PGP bis zum passwortverschlüsselten PDF oder zum SecureChannel (u. a. TLS oder De-Mail) ist dann eine Abstimmung auf die Infrastruktur des Empfängers möglich. Mit diesem Konzept wird eine sichere Kommunikation von und nach außerhalb gewährleistet und gleichzeitig für die notwendige Flexibilität gesorgt (Abbildung 2).

Bordmittel reichen aus, optionale Plug-ins bieten noch mehr

Nachdem die technischen Herausforderungen betrachtet wurden, darf nicht vernachlässigt werden, auch für eine fehlerfreie Anwendung zu sorgen. Ende-zu-Ende-Verschlüsselung bindet den User mit ein. Abhängig von der Wahl der Clients und eventueller Plug-ins kann der Nutzer Verschlüsselungsaktionen einsehen oder muss sie sogar eigenverantwortlich auslösen.

Da Standard-E-Mail-Clients eigentlich generell S/MIME unterstützen, ist eine Umsetzung mit Bordmitteln, das heißt die Nutzung der nativen Clients, im End-to-End-Szenario problemlos möglich. Ein unternehmensweiter Rollout von Client-Installationen ist daher in der Regel nicht zwingend notwendig. LDAP- (Lightweight Directory Access Protocol) und Active-Sync-Proxies sorgen für den Informationsfluss, der zur Zertifikatsbeschaffung und -validierung benötigt wird. Beim ausschließlichen Einsatz von Bordmitteln trägt allerdings der Endnutzer eine große Verantwortung. Er muss die Verschlüsselung explizit ansteuern und daher entsprechend sensibilisiert und geschult werden. Ein Compliance Enforcement (die Durchsetzung der Unternehmensrichtlinien und -vorgaben) ist beim Einsatz nativer E-Mail-Clients aber nicht möglich.

Sehr viel komfortabler und mit weiteren Mehrwerten angereichert wird die Nutzung von E-Mail-Clients mittels entsprechender Plug-ins. Diese sind gewöhnlich für alle gängigen Client-Programme verfügbar. Sie übersetzen dem User nicht nur die eigentlichen Verschlüsselungsaktionen in einen einfachen Button-Klick, sondern sorgen auch für eine hohe Transparenz beim Zertifikatsmanagement. Verschiedene Verschlüsselungsfunktionen können durch die Abfrage zentraler Policies gesteuert werden. Dadurch wird dann auch ein Compliance Enforcement gewährleistet. Dem User stehen darüber hinaus optional weitere sicherheitserhöhende Aktionen zur Verfügung.

Mithilfe von Plug-ins lassen sich sowohl der gesamte E-Mail-Verkehr wie auch die Einstellungen jedes einzelnen Nutzers sehr einfach über mehrere Endgeräte synchronisieren. Zusätzlich wird Key Escrow – in diesem Fall der zusätzliche, mit einem Escrow Key verschlüsselte Versand – an eine unternehmenszentrale Stelle unterstützt. Das bietet besonders bei Verschlüsselung im Personal-End-to-End-Modus dem Unternehmer die Option, im Notfall an die firmeneigenen Daten zu gelangen. Das Konzept einer kombinierten Verschlüsselung im Organizational und Personal End-to-End-Modus bedient also alle unternehmerischen Anforderungen bei einem Höchstmaß an Sicherheit, Effizienz und Usability.

Fazit

Public-Key-Infrastrukturen bilden ein solides Fundament für den Schutz der E-Mail-Kommunikation im unternehmerischen Bereich. Einzelne Komponenten und unterschiedliche Methoden lassen sich dabei flexibel und anwendungsorientiert kombinieren. Für alle Organisationen, Firmen, Behörden und Institutionen, die nicht ausschließlich kabelgebunden kommunizieren und keine Geheimnisse vor ihren internen Administratoren haben, stellt eine Verschlüsselung per Organizational End-to-End, punktuell ergänzt mit Personal End-to-End, ein universell einsetzbares Lösungskonzept für den sicheren Austausch von schützenswerten Informationen dar.

Unabhängig von der jeweiligen Infrastruktur auf der Empfängerseite und der dort eingesetzten Verschlüsselungstechnik können auf diese Weise Nachrichten in jedem Fall ad hoc verschlüsselt zugestellt werden. Im E-Mail-Verkehr innerhalb des Unternehmens funktioniert das am besten über eine Verschlüsselung per S/MIME. Der Informationsfluss nach außen hin lässt sich zum überwiegenden Teil über ein Secure E-Mail Gateway abwickeln – und das spricht dann im Idealfall alle Sprachen der sicheren E-Mail-Kommunikation.

Dr. Burkhard Wiegel
Geschäftsführer Zertificon Solutions GmbH