



Sicherheit im Mailverkehr

E-Mail ist aus dem Alltag nicht mehr wegzudenken. Es bietet jedoch, ohne entsprechende technische Massnahmen, weder Vertraulichkeit noch Verbindlichkeit.

Ausgangslage

Der zunehmende Einsatz moderner Kommunikationsmittel im Geschäftsalltag sowie in unserer Gesellschaft hat dazu geführt, dass immer mehr Daten auf elektronischem Weg, insbesondere per E-Mail, SMS oder MMS, übermittelt werden. Die elektronische Post hat der Informationsgesellschaft bedeutende Impulse und Produktivitätsvorteile gebracht. Sie ist praktisch, schnell, und fast jeder ist damit erreichbar. Ob Verträge, Strategiepläne oder persönliche Dokumente: In Windeseile erhalten Kunden oder Geschäftspartner Informationen mit elektronischer Post. Die Datenübertragung per E-Mail erfolgt heute in

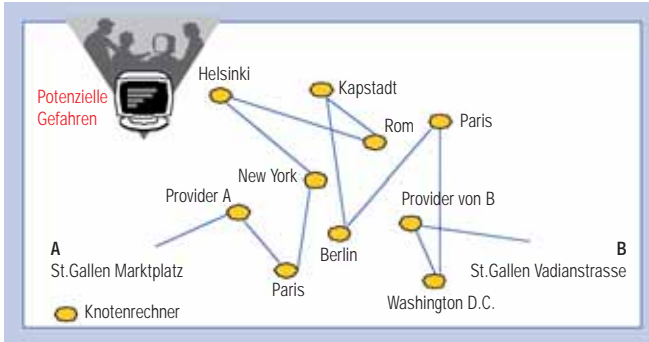
aller Regel im Klartext, das heisst, bildlich gesprochen werden elektronische Ansichtskarten versandt.

Risiken des E-Mail-Verkehrs

Ein wesentlicher Unterschied zwischen dem elektronischen Versand von Daten und dem herkömmlichen Versand per Post besteht darin, dass der Absender elektronischer Mitteilungen im Vorhinein nicht weiss, welchen Weg seine «Post» nehmen wird. Vermeintlich «lokal» und «nationaler» E-Mail-Verkehr wird sehr oft international abgewickelt, das heisst, ein E-Mail von einem Absender in St.Gallen (Marktplatz) an

einen Empfänger in St.Gallen (Vadianstrasse) kann durchaus über einen oder mehrere im Ausland (auch in Übersee) stehende Mailserver geleitet werden. Sodann können verschiedenste Transporteure (Provider) involviert sein. Die Provider sind aufgrund gesetzlicher Bestimmungen, die im europäischen Raum in etwa gleich sind, verpflichtet, den – auch bloss durchlaufenden – Mailverkehr während der Dauer von mindestens sechs Monaten zu spei-





Durchschnittlicher Weg einer E-Mail via Internet von Benutzer A zu Benutzer B

chern. Aus Kostengründen und weil technisch einfacher, werden nicht bloss die gesetzlich vorgeschriebenen sogenannten Header-Daten gespeichert, aus welchen hervorgeht, wer mit wem gemailt hat, sondern die vollständigen E-Mails samt Anhängen.

In technischer Hinsicht besteht die Möglichkeit, mit geringem Aufwand E-Mail-Verkehr (ausserhalb abgeschotteter Firmengrenzen) nach Informationen zu durchsuchen. Dass sich das Durchforsten des Mailverkehrs beziehungsweise des Internets für Kriminelle wirtschaftlich lohnen kann, haben die bekannt gewordenen Attacken auf Server, welche Kreditkarteninformationen enthielten, gezeigt. Aus dem Gesagten und der vorstehenden Grafik folgt, dass nicht geschützte Mails sowohl in Bezug auf den Absen-

der und den Inhalt verändert werden können, die Vertraulichkeit nicht gewahrt ist und zudem die Zustellung des Mails verhindert werden kann.

Disclaimer als Problemlösung

In der Praxis behelfen sich die Unternehmen oft mit dem Anbringen von sogenannten «Disclaimern» (Enthaftungserklärungen). Solche Erklärungen können allenfalls dazu dienen, das Unbehagen des Absenders beim Versand vertraulicher Informationen zu beruhigen und sich vor allfälligen strafrechtlichen Sanktionen zu schützen. Mit dem Anbringen von Disclaimern wird jedoch der Inhalt der elektronischen Post weder vertraulicher (immer noch Versand im Klartext) noch wird sichergestellt, dass Unbefugte keine Kenntnis vom Mailinhalt erhalten und diese Kenntnisse verwenden.

Absicherung des E-Mail-Verkehrs mit technischen Mitteln

Die dargelegten Sicherheitsrisiken führen zur Erkenntnis, dass schützenswerte Informationen durch einen vom Absender bis zum Empfänger durchgehenden, vom Zugriff von unbefugten Personen geschützten Prozess abgesichert werden sollten. Zur schützenswerten Kommunikation zählen etwa die Vorbereitung und Abwicklung eines Rechtsgeschäftes (zum Beispiel Unternehmenskauf beziehungsweise Verkauf), der Austausch von Geschäftsgeheimnissen, die Übermittlung von Finanzinformationen oder kursrelevanten Informationen sowie von Personaldaten wie zum Beispiel Lohndaten an Versicherungsgesellschaften. Dabei gibt es keinen Unterschied zwischen einzelnen Berufsgeheimnisträgern und Unternehmen.

Der Mailverkehr kann im Wesentlichen mit zwei Vorgehensweisen sicherer ausgestaltet

werden. Einerseits können sogenannte digitale Signaturen zum Signieren/Verschlüsseln von Mails verwendet werden. Andererseits besteht die Möglichkeit, den Mailverkehr über eine sogenannte Secure E-Mail-Plattform abzuwickeln.

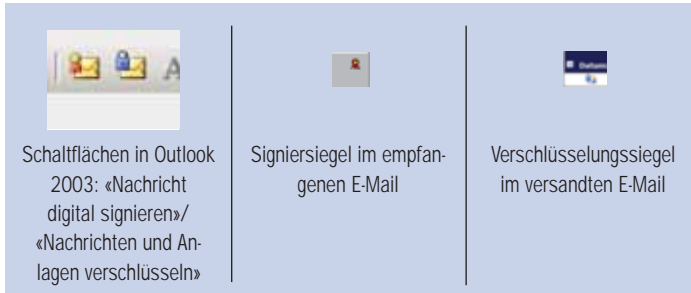
Signieren/Verschlüsseln von E-Mails mit digitalen Signaturen (auf Stufe Benutzer) Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder der Identität des Absenders. Elektronische Signaturen werden wie Identitätskarten oder Reisepässe von vertrauenswürdigen Dritten verwaltet und ausgegeben, den sogenannten Anbieterinnen von Zertifizierungsdiensten (in der Schweiz derzeit: Swisscom Solutions AG, SwissSign AG [Schweizerische Post], QuoVadis Trustlink Schweiz AG). Dabei ist der Identifikationsprozess zur Erlangung der digitalen Signatur mit demjenigen zur Ausstellung einer Identitätskarte vergleichbar beziehungsweise gleich. Die rechtlichen Grundlagen zur Ausstellung von digitalen Signaturen (elektronische Identitäten) enthält das Bundesgesetz über die elektronische Signatur (ZertES). Zertifikate nach Art. 2 ZertES erfüllen (fortgeschrittene elektronische Signaturen) folgende Anforderungen (mehr zum Thema digitale Signaturen unter www.quovadis.ch oder www.swissign.ch/index_de.html):

1. Sie sind ausschliesslich der Inhaberin oder dem Inhaber zugeordnet.
2. Sie ermöglichen die Identifizierung der Inhaberin oder des Inhabers.
3. Sie werden mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.
4. Sie werden mit den Daten, auf die sie sich beziehen, so



Disclaimer

Wir machen Sie darauf aufmerksam, dass der E-Mail-Verkehr grundsätzlich nicht sicher ist. Die Integrität und Vertraulichkeit der Informationen, die über ein E-Mail versendet werden, sind zu keiner Zeit gewährleistet. Wir lehnen daher jegliche Haftung für Schäden ab, die aus der Verwendung des E-Mail-Verkehrs entstehen können. Die in diesem E-Mail enthaltenen Informationen sind für den exklusiven Gebrauch durch den Empfänger bestimmt und möglicherweise vertraulich. Alle Personen, die dieses E-Mail erhalten, aber nicht Empfänger oder Mitarbeiter des Empfängers sind, werden informiert, dass die Benutzung sowie die Veröffentlichung, Reproduktion oder das Weiterleiten dieser Information untersagt ist. Wenn Sie dieses E-Mail aufgrund eines Fehlers erhalten haben, bitten wir Sie, uns dies per Mail oder telefonisch so schnell wie möglich mitzuteilen und das Mail zu löschen. Herzlichen Dank.



verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Mit einem fortgeschrittenen elektronischen Zertifikat können E-Mails signiert (funktioniert auch, wenn der Empfänger über kein Zertifikat verfügt) und/oder auch verschlüsselt (sofern auch der Empfänger über ein Zertifikat verfügt) werden. Zum Signieren beziehungsweise Verschlüsseln ist im Mailprogramm die eine oder andere oder es sind beide Schaltflächen anzuklicken.

Die Vorteile der Verwendung von fortgeschrittenen digitalen Zertifikaten bestehen darin, dass das E-Mail samt Inhalt «End-to-End» verschlüsselt ist, das heisst der Mailinhalt (inklusive Anhänge) auf dem gesamten Transportweg vom Absender bis zum Empfänger von Dritten nicht eingesehen werden kann. Sowohl in der Mailbox des Absenders als auch in derjenigen des Empfängers bleibt das E-Mail verschlüsselt «liegen» und kann nur dann geöffnet werden, wenn der persönliche USB-Token im PC eingesteckt ist und der Benutzer den PIN-Code des USB-Token eingibt. Der Nachteil der Mailverschlüsselung mit digitalen Signaturen besteht darin, dass sowohl der Absender als auch der Empfänger über digitale Signaturen verfügen müssen.

Signieren/Verschlüsseln von E-Mails mit digitalen Signaturen (auf Stufe Unternehmen) Wird in einem Unternehmen der Mailverkehr, wie vorstehend dargelegt worden ist, «End-to-End» verschlüsselt, besteht die Problematik darin, dass

im Falle der Abwesenheit/des Austritts eines Mitarbeiters der unternehmensrelevante Mailverkehr nur dann im Klartext reproduziert beziehungsweise lesbar gemacht werden kann, wenn das Unternehmen über die digitale Signatur, das heisst den USB-Token und den PIN-Code des entsprechenden Mitarbeiters, verfügt. Zur Optimierung der Abläufe sollte deshalb in einem Unternehmen der Verschlüsselungs- beziehungsweise Entschlüsselungsprozess nicht individuell auf Stufe des einzelnen Mitarbeiters, sondern zentral auf Stufe des Mailservers erfolgen. Auf dem Markt sind diverse Lösungen verfügbar, welche diese Funktionalität aufweisen (zum Beispiel SEPPmail, Totemto, PGP Universal Gateway E-Mail, usw.). Dabei ist zu berücksichtigen, dass beim Einsatz einer solchen Lösung (gilt auch für die im vorstehenden Kapitel dargestellte End-to-End-Verschlüsselung) die sogenannte Beziehungsvertraulichkeit nicht gewahrt ist, das heisst, wohl ist der Mailinhalt samt Anhängen verschlüsselt, nicht jedoch die Absender- beziehungs-

weise Empfängeradresse. Diesem Umstand ist besonders dann Beachtung zu schenken, wenn die Geschäftsbeziehung als solche nicht offengelegt werden soll oder darf (zum Beispiel Mailverkehr von Banken mit Kunden).

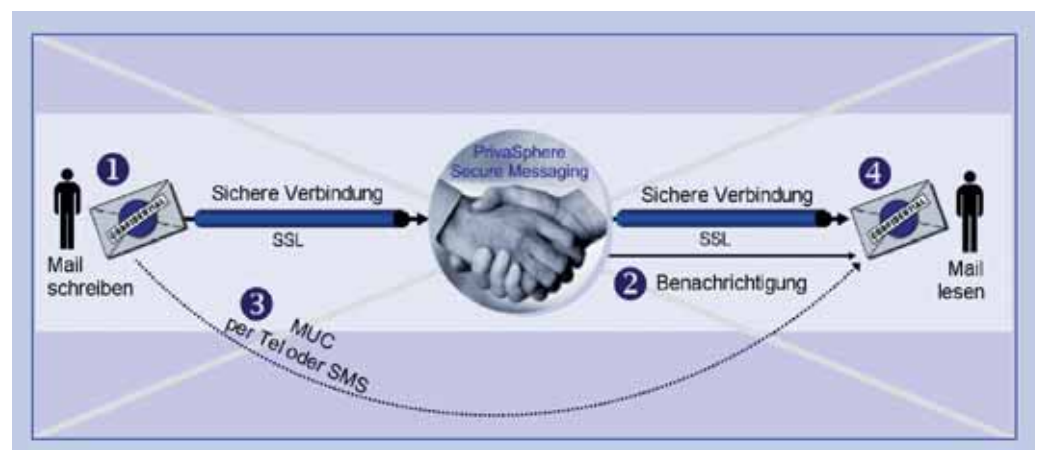
Verwendung einer firmenübergreifenden Secure-E-Mail-Plattform

Wer ohne Verwendung von digitalen Signaturen vertraulich E-Mails versenden möchte, dem steht die Nutzung einer Secure E-Mail-Plattform zur Verfügung. Dies funktioniert wie folgt (mehr zu diesem Thema unter: www.privaspHERE.com):

Der Absender verfasst seine E-Mail in seinem Mailprogramm oder online über eine sichere Verbindung auf der Secure-E-Mail-Plattform (1). Der Empfänger einer sicheren E-Mail wird mit einem normalen E-Mail (im Klartext) von der Secure-E-Mail-Plattform darüber informiert, dass für ihn auf der Plattform eine vertrauliche Meldung zum Abholen bereit liegt (2). Beim erstmaligen Kontakt mit einem Empfänger über die Secure-E-Mail-Plattform wird dem Empfänger vom Sender der Meldung ein einmaliger Zugangs-Code (MUC = Message Unlock Code) übermittelt (3). Aus Sicherheitsgründen sollte der MUC dem Empfänger auf einem anderen Kanal als über E-Mail mitgeteilt werden (zum Beispiel persönlich, per Telefon



lic. iur. HSG
Adrian Rufener
Rechtsanwalt
St. Gallen



THEMA

oder per SMS). Dieser MUC ermöglicht es dem Empfänger, auf die bereitliegende vertrauliche Meldung zuzugreifen und er holt seine vertraulichen Meldungen inklusive angehängten Dokumenten ab (4). Bei weiteren Kontakten mit einem bei der Secure-E-Mail-Plattform registrierten Kunden entfällt die Verwendung eines MUC.

Dank flexibler Integrationsmöglichkeiten kann der Mailversand in der Praxis benutzerfreundlich umgesetzt werden. Der Absender verfasst seine E-Mail in seinem Mailprogramm und wählt mittels Schaltflächen die gewünschte Übertragungsart an («Signieren» = E-Mail mit einer digitalen Signatur versehen; «Vertraulich» = Mailzustellung via Secure-E-Mail-Plattform; «Eingeschrieben» = Mailzustellung via Secure-E-Mail-Plattform, elektronisch eingeschrieben).



Ferner stellt die Secure-E-Mail-Plattform weitere Dienste zur Verfügung. So ist es möglich, elektronisch, eingeschriebene E-Mails (analog: Einschreibebrief) zuzustellen oder auf der eigenen Homepage einen Link auf ein sicheres Webformular zur Verfügung zu stellen (vgl. www.privaspHERE.com; vertrauenswürdige, Schweizer Firma mit Geschäftsdomizil in Zürich).



Wie verhält sich Ihr Anwalt?

Die Mitglieder des St.Gallischen Anwaltsverbandes sind sich der dargestellten Problematik bewusst und deshalb bemüht, ihren Kunden sichere Kommunikationslösungen per E-Mail anzubieten. Ende März 2007 haben sich die st.gallischen Anwälte und Anwältinnen an einer verbandsinternen Tagung über die Lösungsmöglichkeiten eines sicheren Mailverkehrs informiert. Die Umsetzung der einen oder anderen Secure-E-Mail-Lösung wird sowohl auf Seiten der Kunden als auch der Anwälte Zeit in Anspruch nehmen. Nehmen Sie mit Ihrem Anwalt Kontakt auf und klären Sie ab, wie Sie mit ihm sicher per E-Mail kommunizieren können. ■