

Sichere Verbindung

Banken und Versicherungen als nächste Generation der Internet Provider



Zwei Drittel der Banken rechnen damit, dass das Internet als Vertriebsweg und als Instrument zur Kundenbindung weiter an Bedeutung zunimmt. 64 Prozent der Befragten planen daher entsprechende Investitionen. Das ergab eine Anfang 2008 von der Beratungsfirma Steria Mummert herausgegebene und von ibi research (Universität Regensburg) durchgeführte Umfrage zu aktuellen Trends im Bankgeschäft.

Diese Erwartungen decken sich mit den Trends im Verbraucherverhalten. Obwohl noch immer sechs von zehn Internetnutzern

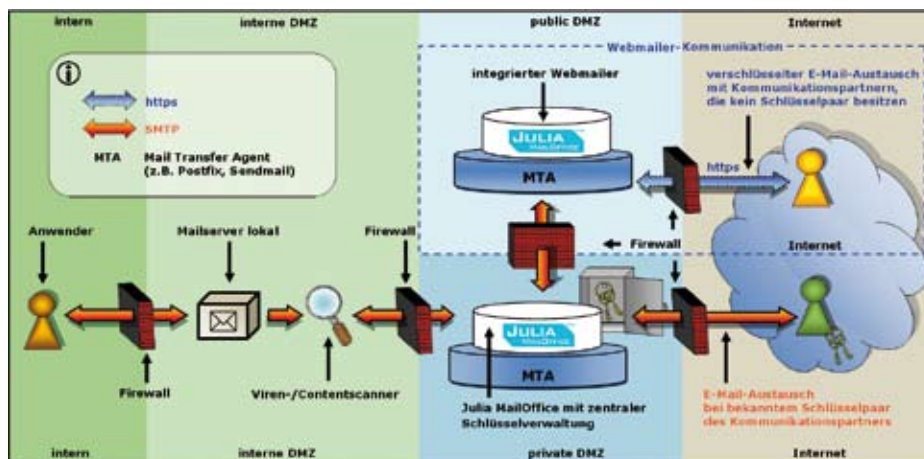
Sicherheitsbedenken haben, nimmt die Zahl der Onlinebanker Jahr für Jahr zu. Glaubt man dem Bundesverband deutscher Banken (www.bankenverband.de), nutzt bereits heute mehr als jeder zweite Kontoinhaber (55 Prozent) die Online-Dienstleistungen seines Geldinstituts. Gemessen an der Gesamtbevölkerung hat sich ihr Anteil in den letzten fünf Jahren von weniger als einem Viertel auf mehr als ein Drittel erhöht.

Doch die Online-Verbindung zum Kunden als Vertriebskanal für Banken und Versicherungen wirft auch Fragen auf. Während der Kunde die E-Mail als ein-

faches Kommunikationsinstrument begreift, können die Unternehmen diesen Weg häufig nicht ohne weiteres wählen. Fehlende oder mangelhafte E-Mail-Sicherheit ist dafür der Hauptgrund. Die größten Stolpersteine sind hinlänglich bekannt. Als „Phishing“ und „Whaling“ bekannte Online-Betrügereien sorgen immer wieder für Skandale und hohe Schäden. Möglich wird das, weil jeder Rechner im Unternehmen, der internetfähig ist, es erlaubt, E-Mails zu versenden und zu empfangen. Ohne Prüfmechanismen sind dem Betrug Tür und Tor geöffnet.

Dabei bietet gerade die E-Mail-Kommunikation viele Perspektiven für eine aktive Kundenbindung und die systematische Aufwertung des Internets als Vertriebskanal. Vor allem Banken und Versicherungen haben hier große Chancen. Sie können den ihnen zugestandenen Vertrauensvorschuss dazu nutzen, mit einem sicheren Internetservice in vielen anderen Lebensbereichen ihrer Kunden präsent zu sein. Der besondere Clou: Aufgrund der ohnehin notwendigen Identifizierungsprozesse bei der Einrichtung von Konten ist ein wichtiger Teil der notwendigen Voraussetzung für sicheren Online-Dialog bereits gegeben.

Instrumente, die für ein solches Angebot die notwendige sichere Infrastruktur bereitstellen, gibt es. Der Bund und seine Behörden beispielsweise setzen seit 2005 die Signatur- und Verschlüsselungssoftware Julia Mailoffice für den E-Mail-Verkehr ein. Als zentrales Krypto-Gateway verarbeitet die Software sämtliche ein- und ausgehenden E-Mails auf der Grundlage eines genau definierten Regelwerkes. Dabei erfüllt Julia im Wesentlichen folgende Funktionalitäten: Ver- und Entschlüsseln, Erstellen und Prüfen von Signaturen zur Sicherstellung der Authentizität der Nachrichten sowie ggf. auch das Erstellen bzw. Prüfen von Zeitstempeln. „Wer auf eine solide Signatur- und Verschlüsselungssoftware setzt, kann Phishing- oder Whaling-Angriffe auf sein Unternehmen nahezu ausschließen. Die Signatur stellt sicher, dass eine E-Mail einer bestimmten Person zugeordnet ist und nicht unbemerkt geändert wird. Dadurch wird die Identität des Signierenden und die Integrität der signierten Daten gewährleistet“, erläutert



Sabine Buchhalter, Deutsche Post Com, den Beitrag der Signatur zur E-Mail-Sicherheit. Der Nutzen für die Wirtschaft liegt auf der Hand. Der Faktor „Time to Market“, wird deutlich positiv beeinflusst. Die Fragen nach der „Kundenbindung“ werden in den Faktoren Tempo, Sicherheit und Problemlösung ebenfalls positiv beantwortet und schließlich dürfte auch der Faktor „Kosten“ im Sinne des Unternehmens gestaltbar sein.

Denn auch wenn der IT-Aufwand als Internet Provider deutlich steigt, sinkt zugleich die Notwendigkeit aufwändiger Spam-Filter und lassen sich Workflow-Systeme einrichten, mit denen die Prozesskosten reduziert werden können. Dies umso mehr, als sich zudem die Chance eröffnet, mit zertifizierten elektronischen Unterschriften auch Verträge rechtsverbindlich zu schließen, sie elektronisch zu übermitteln und ggf. sogar zu archi-

vieren. Sind die privaten Kunden über eine sichere E-Mail-Infrastruktur angebunden, gibt es schlussendlich auch für die unternehmerischen Kommunikationspartner keinen Grund mehr, E-Mails als rechtsverbindliche Dialoginstrumente zu verweigern. Ob privat oder geschäftlich, die E-Mail hat dann Einzug in die Geschäftswelt gehalten und erfüllt die Vorgaben zur elektronischen Datenhaltung, wie es der Gesetzgeber verlangt.

„Der Imageschaden ist immens“

Thomas Carstens, ICC Solutions, über sichere E-Mail-Verschlüsselung



„Da nach deutschem Recht die Verantwortung für sichere Geschäfte bei den Unternehmen liegt, wächst mit der Zahl der Einzelkunden auch das Risiko, Opfer von Online-Kriminellen zu werden. Der Imageschaden, den eine solche Attacke gerade bei Banken und Versicherern nach sich ziehen würde, ist immens.“

Thomas Carstens, Geschäftsführer ICC Solutions

Wie schätzen Sie das Problembewusstsein der deutschen Wirtschaft in punkto IT- und E-Mail-Sicherheit ein?

Carstens: IT- und E-Mail-Sicherheit stehen in vielen Unternehmen in Deutschland bereits auf der Tagesordnung. In den vergangenen Jahren hatten jedoch zunächst IT-Systeme Priorität, die unmittelbar zum Unternehmenserfolg beitrugen. Dabei haben die Unternehmen gelernt, funktionale und bezahlbare IT-Strukturen aufzubauen und zugleich damit gekämpft, den Anwendern die Welt der IT näher zu bringen. Sicherheitsthemen wurden erst später relevant. Und das birgt Probleme. Denn da der Fokus Sicherheit erst im Anschluss auf die bestehenden Systeme gerichtet wurde, ist er zum Teil nur sehr schwer nachträglich zu integrieren.

Welche Schäden können Unternehmen durch ungesicherte Online-Kommunikation entstehen?

Carstens: Stellen Sie sich vor, was passieren kann, wenn Sie vertrauliche Informationen per Postkarte und mit Bleistift geschrieben auf den Weg bringen. Genau das tun Sie, wenn Sie E-Mails ungesichert durch das WorldWideWeb schicken. Nicht signierte, nicht verschlüsselte E-Mails sind eine Einladung, gelesen und sogar gefälscht zu werden. Eine ungesicherte E-Mail ist manipulierbar und nicht vertrauenswürdig. Image- und Haftungsschäden sind die daraus resultierenden Risiken, die bis zur Geschäftsaufgabe reichen können.

Inwiefern sind insbesondere Banken und Versicherungen davon betroffen?

Carstens: Alle Unternehmen, die mit vertraulichen Kundendaten zu tun haben, sind von dem Thema betroffen. Steuerberater und Ärzte ebenso wie Banken und Versicherungen. Doch weil hier finanzielle Daten übermit-

telt werden, sind sie ganz besonders von Angriffen aus dem Netz bedroht. Da nach deutschem Recht die Verantwortung für sichere Geschäfte bei den Unternehmen liegt, wächst mit der Zahl der Einzelkunden auch das Risiko, Opfer von Online-Kriminellen zu werden. Der Imageschaden, den eine solche Attacke gerade bei Banken und Versicherern nach sich ziehen würde, ist immens. Schließlich basiert gerade ihr Geschäft auf Sicherheit und Vertrauen.

Wie kann die Problemlösung aussehen?

Carstens: E-Mail Kommunikation ist aus unserem Leben nicht mehr wegzudenken. Ein guter Weg für Unternehmen, diesen Kommunikationsweg sicherer zu machen, könnte sein, die Kunden in die eigenen, gut gesicherten Systeme einzubinden. Vor allem Banken und Versicherungen haben hier einen Vorteil, da die Identität ihrer Kunden bereits nachgewiesen ist und eine Überprüfung der User-Identität weniger aufwändig ausfällt. Zudem braucht jedes Unternehmen Regeln für die E-Mail Kommunikation. Faktisch unterwirft sich jedes Unternehmen, das seinen Mitarbeitern E-Maildienste zur Verfügung stellt, dem Telekommunikationsgesetz, mit allen daraus resultierenden Pflichten. Die obligatorische Ausstattung der Mails mit einer Signatur eines Trust Centers kann SPAM oder Phishing ausschließen und sollte daher der normale Standard sein.