

Matthias Tauber

ist Leiter des Kompetenzzentrums Sicherheitslösungen bei Finanz Informatik Technologie Service (FI-TS) in München.

Managed Secure E-Mail Services

Effektiver Abwehrwall und Schutz für vertrauliche Nachrichten

E-Mail ersetzen im privaten wie geschäftlichen Umfeld immer mehr den klassischen Briefverkehr. Das stellt viele Unternehmen vor das Problem, auch vertrauliche Informationen über den elektronischen Postweg sicher zu versenden. Denn eine unverschlüsselte E-Mail ist so offen lesbar wie eine Postkarte. Abhilfe versprechen zahlreiche Produkte zur E-Mail-Verschlüsselung. Doch werden sie in der Praxis so gut wie nicht genutzt, da sie sehr schwer zu bedienen sind. Besonders hart trifft das Kreditinstitute und Finanzdienstleister. Denn diese Unternehmen haben besonders hohe Ansprüche an die Vertraulichkeit der mit ihren Kunden ausgetauschten Informationen. Ein Ausweg aus dem Dilemma sind „Managed Secure E-Mail Services“ eines erfahrenen IT-Dienstleisters. Denn diese Dienste vereinen Nutzerfreundlichkeit mit Sicherheit und schonen zudem das Investitionsbudget eines Kreditinstituts.

In vielen Banken nimmt die Geschäftskommunikation per E-Mail stetig zu. Das ist wenig verwunderlich, da die elektronische Art der Kommunikation schnell und unkompliziert ist. Deshalb wollen auch immer mehr Kunden auf diesem Weg mit ihrem Bankberater kommunizieren. Dabei stellt sich die Frage, ob die Vertraulichkeit der ausgetauschten Informationen beim Versand per E-Mail ebenso sichergestellt ist wie bei dem Versand eines Briefs im Umschlag. Doch klar ist, dass dem so nicht ist. Denn der Versand unverschlüsselter elektronischer Nachrichten durch das Internet gleicht einer Welt, in der es keine Briefumschläge gibt. Alle Dokumente sind offen und damit, theoretisch für alle lesbar, vom Absender zum Empfänger unterwegs.

Dieses Problem ist den meisten Absendern und Empfängern nicht bewusst. So schicken heute auch viele Bankberater persönliche, vertrauliche oder gar geheime Informationen völlig unverschlüsselt an ihre Kunden. Der an solche E-Mails oft automatisch angehängte Absatz über die Vertraulichkeit der enthaltenen Informationen wird Datendiebe jedoch kaum abschrecken.

Risiko „Elektronische Postkarte“

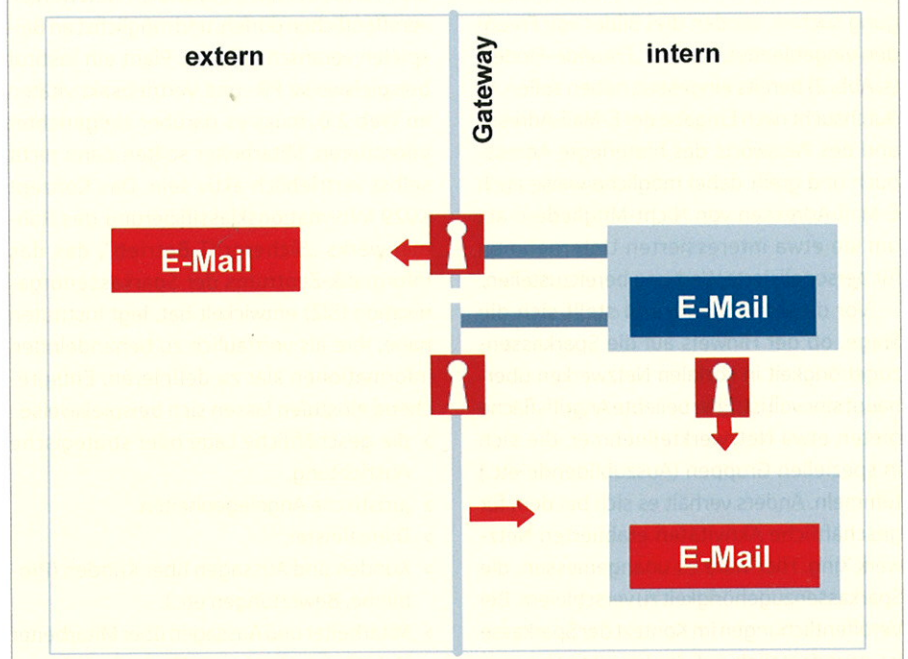
Es ist schwer zu beziffern, mit welcher Wahrscheinlichkeit eine E-Mail tatsächlich mitgelesen wird. Fakt ist jedoch, dass der Inhalt einer unverschlüsselten elektronischen Nachricht auf dem Weg zum Empfänger jedem offensteht, der sich Zugang zu dem Weg der Nachricht durch das Internet verschafft, ein dabei genutztes System kompromittiert oder sogar legal zum Abhören nutzt. Aufgrund

dieser Problematik hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter anderem das „Mitlesen von E-Mails“ in seinen Gefährdungskatalog aufgenommen (G 5.77 Mitlesen von E-Mails). Banken sollten also die Gefährdungslage auf keinen Fall unterschätzen und ihre elektronischen Briefe vor dem Versand verschlüsseln. Denn nur so ist es möglich, die Vertraulichkeit der Informationen sicherzustellen und auch entsprechende Datenschutzanforderungen zu erfüllen.

Das Problem im praktischen Alltag ist, dass die meisten Verschlüsselungslösungen äußerst komplex und damit schwer handzuhaben sind. Die Akzeptanz eines Produkts im Geschäftsalltag steht und fällt jedoch mit dessen Bedienbarkeit. Daher verzichten viele Bankmitarbeiter nicht selten auf den Einsatz einer Verschlüsselungslösung, selbst dann, wenn sie ihnen zur Verfügung steht. Für ein Kreditinstitut bedeutet das einerseits, dass es weiterhin sensible Daten auf „elektronischen Postkarten“ versendet.

ABBILDUNG 1

Einsatz von Managed Secure E-Mail Services



Zudem erweist sich in diesen Fällen die zur Verfügung gestellte Technik als klassische Fehlinvestition, weil sie ja letztlich nicht genutzt wird.

Verschlüsselung als Service

Ein Lösungsansatz zur Behebung dieser Probleme wäre, die E-Mail-Verschlüsselung an einen professionellen Serviceanbieter auszulagern, der über seine Plattform dafür sorgen kann, dass vertrauliche elektronische Nachrichten für die Kunden vor Lauschangriffen geschützt sind. Dazu müssen weder der Bankberater noch dessen Kunde bei der Bedienbarkeit Kompromisse eingehen oder über besondere Fachkenntnisse verfügen.

Im einfachsten Fall läuft die Ver- und Entschlüsselung nämlich für beide Seiten überschaubar ab. Ein zusätzlicher Vorteil besteht darin, dass Kreditinstitute gemeinsam mit dem ausgewählten Dienstleister die entsprechenden Verschlüsselungsrichtlinien individuell regeln und dabei den Service sehr flexibel gestalten können. Ebenso wird dadurch die Einhaltung der Datenschutzrichtlinien sichergestellt.

Gateway-Dienst

Ein unkomplizierter, weil transparenter Ansatz bietet die Nutzung eines Verschlüsselungsservices auf Basis eines Gateway-Dienstes. Dabei fungiert das Gateway des Dienstleisters quasi als virtuelle Poststelle des entsprechenden Instituts. Hier kommen alle Briefe von Absendern aus dem Unternehmen an, werden entsprechend kuvertiert und anschließend sicher an die Empfänger weitergeleitet. Durch die Verschlüsselung auf dem Gateway schützt ein Managed Secure E-Mail Service den Inhalt der elektronischen Post vor unbefugten Zugriffen, sobald sie das sichere Netzwerk des eigenen Unternehmens verlassen.

Für den einzelnen Mitarbeiter ändert sich im Arbeitsablauf gar nichts. Sobald er ein bestimmtes Stichwort in den Betreff einer Nachricht setzt, die Vertraulichkeitsstufe einer Mail erhöht oder einen bestimmten Empfänger auswählt, verschlüsselt das Secure-E-Mail-Gateway automatisch die elektronische Nachricht und versendet sie sicher „verpackt“ über das unsichere Internet. Nutzt der Empfänger ebenfalls ein E-Mail-Gateway oder einen entsprechenden Service, wird die Botschaft entschlüsselt und ihm im eigenen Netzwerk im Klartext zur Verfügung gestellt.

Umfassender E-Mail Schutz

Ist der Adressat einer verschlüsselten Mail nicht auf deren Empfang vorbereitet, könnten Nutzer lokal installierter Lösungen allerdings Schwierigkeiten haben, die Sendung zu entschlüsseln. Dieses Problem lässt sich allerdings durch die Nutzung eines Managed Secure E-Mail Services lösen. Denn in diesem Fall agiert das Gateway wie ein Absender-Postfach in der virtuellen Poststelle. Es speichert die verschlüsselte Nachricht zunächst ab und informiert anschließend den Empfänger in einer unverschlüsselten E-Mail darüber, dass eine vertrauliche Nachricht für ihn vorliegt. Anschließend hat der Empfänger die Wahl, auf welche Art er die Nachricht empfangen möchte. Eine Möglichkeit bildet der Aufruf einer verschlüsselten Webseite, um die eingegangene Mail dort anschließend sicher zu lesen. Alternativ kann das Gateway den Inhalt aber auch in ein passwortgeschütztes, verschlüsseltes PDF-Dokument einbetten und dieses dann dem Empfänger zustellen. Über das Passwort ist die Vertraulichkeit des Inhalts weiterhin gewährleistet. Der Empfänger kann alternativ auch seinen öffentlichen Schlüssel per E-Mail an das Gateway schicken, mit dem dann die Nachricht verschlüsselt und zugestellt werden kann. Der Empfänger schickt in dieser Variante sozusagen seinen eigenen Umschlag an die virtuelle Postzentrale, in dem dann die vertrauliche Nachricht verpackt und zugestellt wird.

Ein Managed Secure E-Mail Service ist zudem nicht auf die Kommunikation zwischen Bank und Kunde beschränkt. Es lässt sich, je nach Sicherheitsbedürfnis, auch intern einsetzen, um beispielsweise die Kommunikation zwischen Vorständen vor einem unbefugten Zugriff zu schützen. Wichtig ist

bei der Auswahl, dass sich der Service auch in bestehende E-Mail-Systeme nahtlos integrieren lässt.

Fazit

In der Finanzbranche ist heute die Auslagerung von Services, die nicht das eigentliche Kerngeschäft betreffen, fast schon obligatorisch. Auch die Nutzung von verschlüsselten, sicheren E-Mail bietet sich für eine solche Auslagerung an. Denn so müssen sich Kreditinstitute nicht unnötig mit komplexen Technikthemen befassen und können sich umso intensiver auf das eigentliche Tagesgeschäft konzentrieren. Zudem gewährleisten sie auf diesem Wege, dass ihre Mitarbeiter den Kommunikationskanal „E-Mail“ tatsächlich sicher nutzen und dabei auch datenschutzrechtliche Vorgaben konsequent einhalten.

Vor der Auslagerung der Verschlüsselung der elektronischen Kommunikation sollten Unternehmen jedoch darauf achten, dass alle für den sicheren Mail-Versand notwendigen Komponenten beim Serviceanbieter jederzeit verfügbar und dort auch selbst sicher sind. Denn wer einen eigenen Schlüsselservers betreibt, der weiß, dass dieser mindestens genauso gut abgesichert werden muss, wie die Schlüssel und die Geheimcodes zu einem privaten Safe, in dem wiederum wichtige Passwörter aufbewahrt werden. Auch deshalb ist es für fachfremde Unternehmen oftmals besser, den Betrieb einer sicheren E-Mail-Infrastruktur einem Spezialisten zu überlassen, der das Know-how und langjährige Erfahrung in diesem Bereich mitbringt. ◀

INFOBOX

Vorteile von Managed Secure E-Mail Services

- > Sicherer E-Mail-Verkehr innerhalb und außerhalb des Unternehmens
- > Funktioniert mit jedem Empfänger
- > Funktioniert mit jedem E-Mail-Server
- > FI-TS bietet eine kostengünstige Ergänzung zu anderen Produkten im Bereich der E-Mail-Kommunikation
- > Kein aufwendiger Betrieb einer eigenen Public-Key-Infrastruktur
- > Keine extra Software auf den Arbeitsplätzen
- > Kein langwieriger Lernprozess bei den Anwendern
- > Optional auch in eigene E-Mail-Systeme integrierbar