

Special Innovation

Sichere Unternehmensdaten

Das Verschicken von E-Mails im Internet ist alles andere als sicher. Security-Lösungen, die einen verschlüsselten Austausch von Informationen über elektronische Kommunikationswege gewährleisten, sorgen dafür, dass heikle Unternehmensdaten unterwegs nicht gelesen oder gar verändert werden können. Und das mit Garantie.

Sonja Gerstl

Auch wenn viele von uns es nicht wirklich wahrhaben wollen: Das Sicherheitsniveau einer über das Internet versendeten E-Mail entspricht in etwa jenem einer mit Bleistift geschriebenen Postkarte.

1. Es gibt keine Garantie, wer sie erhält. 2. Sie kann während der Übermittlung gelesen werden. 3. Sie kann unbemerkt verändert werden.

Was für private Nutzer dieser Art des Kommunikationsaustauschs im Falle einer Manipulation bereits äußerst unangenehme Folgen hat, kann für Unternehmen mitunter enorme geschäftliche Nachteile mit sich bringen oder sie im schlimmsten Fall die Existenz kosten.

Sicheres Business

GME, also Group Mail Encryption, verschlüsselt und signiert E-Mails und steigert so ganz wesentlich die Sicherheit des Mail-Verkehrs. Eingesetzt wird sie zum Beispiel schon in der Raiffeisen Gruppe. Patrick Höbart, Security-Verantwortlicher von Raiffeisen Informatik: „Die Verschlüsselung bietet die Möglichkeit, vertrauliche E-Mails sicher über das Internet zu versenden, und ist somit Basis für sichere Business-Kommunikation.“

Die Verschlüsselung einer E-Mail ist denkbar einfach, sprich: benutzerfreundlich. Der Versender wählt durch Anklicken einer Checkbox in seinem Mail-Programm aus, dass die



Vielen Usern ist nicht bewusst, dass eine E-Mail, sobald sie ihren Weg übers Internet antritt, nicht selbstverständlich beim Empfänger landet. Hinzu kommt, dass diese unterwegs auch gelesen oder inhaltlich verändert werden kann. Foto: Photos.com

Nachricht verschlüsselt und signiert werden soll. Der Rest geschieht automatisch im Hintergrund des Programms. Das bedeutet, die E-Mail gelangt zum sogenannten Secure Mail Gateway, wo die eigentliche Verschlüsselung letztendlich erfolgt.

Die Verschlüsselung wird dabei durch den Einsatz von X.509-Zertifikaten gewährleistet. „Die E-Mail-Verschlüsselungslösung der RZB benötigt keine zusätz-

liche Software-Installation“, erklärt Höbart. „Unternehmen, die bereits ein System besitzen, das Zertifikate unterstützt, können direkt miteinander kommunizieren. Ist das nicht der Fall, wird eine Secure Mailbox zum Austausch vertraulicher Daten zur Verfügung gestellt.“

Einfache Handhabung

Für den Empfänger der verschlüsselten E-Mails ergeben sich – abhängig davon, ob er

ein entsprechendes Zertifikat besitzt oder nicht – zwei Szenarien: Besitzt er ein Zertifikat, wird die Nachricht direkt in seine Inbox zugestellt. Die Entschlüsselung erfolgt am Mailserver beziehungsweise Client des Empfängers. Besitzt der Empfänger kein Zertifikat, kann er die Nachricht von der Secure Mail Box abholen. Diese erfüllt die Aufgabe eines sicheren Postfachs. Der Empfänger erhält eine Mail, dass eine verschlü-

selte Nachricht vorliegt, und verbindet sich mit der Secure Mail Box. Nach erfolgreicher Identifizierung kann er seine Mails lesen und bearbeiten.

Raiffeisen selbst erledigt seinen internen Mailverkehr übrigens nicht über das Internet, sondern über ein eigenes Konzernnetzwerk. Aus sicherheitstechnischen Gründen kommt aber auch intern eine Verschlüsselung zum Einsatz.

www.raiffeiseninformatik.at

1999 | 2009

10 Jahre **economyaustria.at**BMW^a

Das Special Innovation wird von der Plattform **economyaustria** finanziert. Die inhaltliche Verantwortung liegt bei **economy**. Redaktion: Ernst Brandstetter