Sensible Daten sicher per E-Mail versenden

E-Mails haben die Kommunikation in Unternehmen revolutioniert. Was früher als Brief versandt wurde, findet heute in der Regel elektronisch den Weg zum Empfänger. Immer mehr Unternehmen versenden E-Mails mit sensiblen, zu schützenden Informationen. Selbst Forschungsergebnisse, Konstruktionszeichnungen, Informationen über Mitarbeiter oder über die Geschäftslage gehen auf die elektronische Reise.

Sensible Daten verschlüsseln

Vom Absender bis zum Empfänger legen E-Mails via Internet einen langen Weg zurück. Die Inhalte werden dabei im Klartext versendet, sind offen und lesbar wie eine Postkarte, sofern keine Verschlüsselungsmechanismen eingesetzt werden. Das heißt: Jeder, auch Mitbewerber, könnten diese Nachrichten mitlesen oder auch verändern. Für Ihr Unternehmen kann das mit einem beträchtlichen wirtschaftlichen Schaden verbunden sein.

In der Regel lässt sich auch nicht feststellen, ob der Absender tatsächlich derjenige ist, für den er sich ausgibt.

Wenn Sie E-Mails geschäftlich einsetzen, sollten Sie für Ihr Unternehmen die erforderlichen Regeln nach dem BSI-Grundschutzkatalog erstellen und umsetzen.

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteiischer Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Netzwerk Elektronischer Geschäftsverkehr

www.ec-net.de

Praxistipps

Aus der Praxis für die Praxis

E-Mails sicher versenden

10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Netzwerk Elektronischer Geschäftsverkehr

TeleTrusT

TeleTrusT – Bundesverband IT-Sicherheit e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische“ rund um das Thema Informationssicherheit.

TeleTrusT ist mit mehr als 130 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.

TeleTrusT
Pioneers in IT security.

Impressum

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:
TeleTrusT – Bundesverband IT-Sicherheit e.V.,
Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:
Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:
Karl-Heinz Kottenhahn

Druck:
Buersche Druck- und Medien GmbH

Bildnachweis:
Danielle Bonardelle/Fotolia.com, Photosani/Fotolia.com, pressmaster/Fotolia.com

Stand: 12/2011

10 Tipps, die wirklich helfen

Wie können Sie Ihre E-Mails sicher versenden?

10 grundlegende Praxistipps helfen Ihnen, Ihre Kommunikation via E-Mail sicher zu gestalten.

Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema E-Mail-Sicherheit finden Sie unter www.ec-net.de und www.kmu-sicherheit.de.

Wenn Sie sensible Daten als E-Mail an Ihre Geschäftspartner versenden, sollten Sie diese verschlüsselt versenden.

Was müssen Sie tun, um E-Mails sicher zu versenden?

Wenn Sie E-Mails versenden wollen, so dass nur der gewünschte Empfänger in der Lage ist, diese zu lesen, müssen Sie diese verschlüsseln. Wollen Sie, dass der Empfänger überprüfen kann, ob die E-Mail manipuliert wurde und der angegebene Absender auch der tatsächliche Absender ist, sollten Sie diese „signiert“ versenden. Dann kann der Empfänger den Absender verifizieren. Beide Methoden – die Verschlüsselung und die elektronische Signatur – können Sie entweder einzeln oder kombiniert anwenden.

Verschlüsselung

Beim Verschlüsseln bleibt die E-Mail während des ganzen Übertragungsweges verschlüsselt, also unlesbar und wird erst vom Empfänger wieder entschlüsselt und damit lesbar gemacht. Dieser Schutz ist besonders bei der Übertragung sensibler und zu schützender Informationen, wie z.B. Übertragung von Angebots- oder Technologie-Daten, wichtig. Verschlüsselungsprogramme ermöglichen es Ihnen, entweder die gesamte Mail zu verschlüsseln oder nur Dokumente im Anhang.

Tipp 1: Sensible Daten identifizieren
Überlegen Sie sich gut, welche Daten besonders sensibel und schützenswert sind und nur für den Empfänger lesbar sein sollen.

Tipp 2: Passende Verschlüsselung wählen
Programme, mit denen Sie nur Mail-Anhänge verschlüsseln wollen, sind relativ einfach zu bedienen. Programme, die die gesamte E-Mail verschlüsseln und auch signieren, sind in der Anwendung komplexer. Lassen Sie die Programme ggf. von einem externen Fachmann einrichten.

Digitale Signatur

Wenn Sie sichergehen wollen, dass der angegebene Absender der Nachricht auch mit dem tatsächlichen Absender identisch ist und die Inhalte der E-Mail „unterwegs“ nicht manipuliert wurden, hilft eine so

genannte „Digitale Signatur“. Sie hat eine ähnliche Funktion wie die Unterschrift unter einem Papierdokument und zeigt Ihrem Kommunikationspartner, dass die E-Mail wirklich von Ihnen geschrieben und der Inhalt nicht von Dritten verändert wurde.

Tipp 3: Beratung bei der Auswahl
Für die Signatur werden zwei digitale Schlüssel benötigt. Der eine ist geheim und verbleibt bei Ihnen, der andere wird veröffentlicht bzw. in einem öffentlichen Verzeichnis hinterlegt. Lassen Sie sich bei der Auswahl der Signatur und der Vorgehensweise unbedingt beraten.

Tipp 4: Zugangsdaten sicher aufbewahren
Stellen Sie sicher, dass digitale Schlüssel und Zugangsdaten (z.B. Passworte) sachgerecht erstellt und aufbewahrt werden.

Tipp 5: E-Mail-Software einstellen
Wählen Sie ggf. die Einstellungen Ihrer E-Mail-Software so, dass ein Empfänger auf jeden Fall den Nachrichtentext lesen kann, auch wenn er Ihre Signatur nicht überprüfen kann.

Gibt es auch Lösungen, die sicher und einfach zu bedienen sind?

Verschlüsselungs- und Signatur-Verfahren sind oft komplex und umständlich zu bedienen. Viele Nutzer haben damit Probleme, deshalb sollte man eine Lösung verwenden, die einfach zu bedienen ist. Es gibt Verfahren, die Sie z.B. über Ihren Browser bedienen können. Bei diesen brauchen Sie keine weiteren Installationen von Hard- oder Software auf Ihrem Rechner vornehmen.

Tipp 6: Auf leichte Bedienbarkeit achten
Achten Sie unbedingt auf eine leichte Bedienbarkeit von Verschlüsselungs- und Signatur-Systemen. Lassen Sie sich hierbei beraten.

Tipp 7: De-Mail-Service
In Deutschland wird der Mail-Dienst über den Browser als De-Mail angeboten. Die E-Mails werden dabei verschlüsselt versendet. Voraussetzung ist, dass die Teilnehmer sich vorher registrieren lassen.

Tipp 8: Mitarbeiter schulen
Die beste Technik nützt nichts, wenn die Mitarbeiter über den richtigen Umgang mit sensiblen E-Mails nicht richtig informiert sind. Schulen Sie Ihre Mitarbeiter im Umgang mit Verschlüsselung und Signaturen.

Was muss ich sonst noch grundsätzlich beachten?

Verschlüsselung und Signierung Ihrer E-Mails setzen einen „sauberen“ Computer voraus. Auf Ihrem Rechner darf sich keine schädliche Software (z.B. Viren, Trojaner) befinden. Mittels Schadsoftware können Ihre Passwörter kopiert, die Sicherheitssoftware ausgeschaltet und sogar Ihr gesamter Rechner kontrolliert werden. In diesem Fall nützt Ihnen auch die beste Verschlüsselungssoftware nichts.

Tipp 9: Installieren von Schutzsoftware
Installieren Sie Schutzsoftware mit Viren- und Spyware-Erkennung und einer Firewall. Halten Sie diese, wie auch Ihr Betriebssystem und den Internetbrowser, immer auf dem neuesten Stand.

Tipp 10: Gesonderte Konten einrichten
Richten Sie gesonderte Benutzerkonten an Ihrem PC ein und benutzen Sie das Administrator-Konto nur, wenn es absolut notwendig ist. Denn bei der Verwendung von Administratorrechten können Schadprogramme größtmöglichen Schaden anrichten.