



Dipl.-Kfm. Axel Schmitt
stellv. Vorsitzender EDV-Arbeitskreis

E-Mail Versand - aber sicher?

Wie sicher sind Smartphones und ähnliche Geräte und wie leicht lassen sich passwortgeschützte Zugänge öffnen? Mit dieser Frage haben sich Veranstaltungen des hessischen Steuerberaterverbandes und der Steuerberaterkammer im laufenden Jahr beschäftigt.

Ein ähnlich gelagertes Problem stellt sich beim E-Mailversand sensibler Informationen und Daten.

E-Mail als Kommunikationsweg hat im Praxisalltag vieler Kanzleien das „alte Fax“ abgelöst. Der Austausch erfolgt in vielen Fällen jedoch offen, d.h. für jeden - auch unberechtigte Dritte - lesbar. Nun muss nicht jede Nachricht geschützt werden und absolute Sicherheit kann es nicht geben. Aber wenn sensible Daten die Kanzlei verlassen, verpflichtet das Berufsrecht diese gegen unberechtigten Zugriff zu sichern.

Wie können solche Schutzmaßnahmen umgesetzt werden?

In unserer Kanzlei erfolgt die Lösung wie folgt:

Als Standardsoftware für die elektronische Kommunikation setzen wir MS Outlook ein. Da wir Datevanwender sind, nutzen wir daneben das Datev-Sicherheitspaket und jeder Mitarbeiter setzt an seinem Arbeitsplatz eine Datev-Smartcard mit klassischem Kartenleser ein. Die Smartcard des Mitarbeiters ist mit seinen persönlichen Daten unter Vorlage einer Personalausweiskopie personalisiert. Spiegelbildlich erfolgte die Installation bei ausgewählten Mandanten, mit denen sensible Daten per Mail ausgetauscht werden.

Der Mandant sendet zu Beginn einmalig eine Testmail an unseren Mitarbeiter und verwendet bei gleicher Vorgehensweise wie sonst per Mausklick den Button „Mail signieren“. Damit erhält die ausgehende Mail eine Signatur, bei der der öffentliche Teil des Schlüssels an die Mail gekoppelt wird.

Unser Mitarbeiter als Empfänger dieser Mail kann nun diesen öffentlichen Teil des Schlüssels zu den Adressdaten des Mandanten anfügen und hält damit den notwendigen Teil zur Verschlüsselung vor. Wenn nun sensible Daten an den Mandanten gesendet werden sollen, wählt der Mitarbeiter beim Versand per Mausklick „Mail verschlüsseln“. Die Mail an den Adressaten wird chiffriert und ist damit für Dritte nicht mehr lesbar. Nur der Mandant kann die Mail lesen, da nur er den Code zur Dechiffrierung kennt.

Zusammenfassend kann man festhalten, dass bei dieser Vorgehensweise der Sender den öffentlichen Schlüsselteil des Empfängers vorab kennen muss. Er hängt diesen Teil an die zu versendende Mail, macht sie so für Dritte unlesbar und nur der Empfänger kann mit seinem privaten Schlüsselteil die Mail wieder lesbar machen.

Zu bedenken ist dabei, dass nicht alle Mandanten für diese Vorgehensweise zu begeistern sind. Ein Hilfsargument kann jedoch sein, dass die Verschlüsselung selbstverständlich nicht

nur zum Steuerberater sondern auch zu jedem Kunden und Lieferanten des Mandanten eingesetzt werden kann.
Sicherlich werden dieses Verfahren ohnehin eher Mandanten mit einer Akzeptanz für digitale Kommunikation einsetzen.

Neben dem vorgenannten Verfahren gibt es zahlreiche andere Möglichkeiten einer Vielzahl von Anbietern. Wer im Kollegenkreis auf den am Anfang angesprochenen Veranstaltungen gesehen hat, wie schnell Passwörter „geknackt“ sind und wie leicht Smartphones „auspioniert“ werden können, sollte unbedingt an einen sicheren E-Mailversand denken.

Für den Fall, dass der Artikel Ihr Interesse geweckt hat, freuen wir uns auf Ihre Anregungen und Kontaktaufnahme. Sie erreichen uns über www.steuerberaterverband-hessen.de unter der Rubrik Verband / EDV Arbeitskreis.