Analysen und Meinungen

Mit Sicherheit im Netz

WPin/StBin Dipl.-Kffr. Katrin Fischer, Steffen Heyde

Briefe sind out – E-Mails boomen. Die modernen Kommunikationsmittel, die unseren Alltag so sehr erleichtern, haben ihre Tücken beim Thema Vertraulichkeit. Dafür sollte jede Kanzlei Vorsorge treffen. Der Beitrag zeigt wesentliche Sicherheitsaspekte der Online-Datenkommunikation auf.

Verschwiegenheitspflicht

Der gesetzliche Abschlussprüfer ist nach § 323 Abs. 1 HGB zur Verschwiegenheit verpflichtet. Gleichzeitig ist die Verschwiegenheit in § 43 WPO explizit als Berufspflicht des Wirtschaftsprüfers ausgestaltet. Diese erstreckt sich nach § 50 WPO nicht nur auf den Berufsträger, sondern auch auf seine Gehilfen und Mitarbeiter, mithin also auf die gesamte Praxis. Diese allgemeine Berufspflicht wird in § 9 der Berufssatzung etwas näher erläutert. Danach haben Wirtschaftsprüfer dafür zu sorgen, dass „Tatsachen und Umstände, die ihnen bei ihrer Berufstätigkeit anvertraut oder bekannt werden“ Unbefugten unzugänglich bleiben. „Sie haben entsprechende Vorkehrungen zu treffen.“ Diese Pflichten bestehen auch nach Beendigung eines Auftragsverhältnisses fort.

Ein Wirtschaftsprüfer macht sich nach § 203 Abs. 1 Nr. 3 StGB wegen Verletzung von Privatgeheimnissen strafbar, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm als Wirtschaftsprüfer anvertraut oder sonst bekannt geworden ist. Eine Offenbarung in diesem Sinne ist auch durch Unterlassen möglich, denn der Berufsträger ist als Geheimhaltungsverpflichteter Beschützergarant. Deshalb dürfen unterlassene technische Schutzvorkehrungen nicht als unwesentliches Organisationsdefizit der Kanzlei abgetan werden.

Für die mündliche Kommunikation hat jeder Berufsträger seine Verschwiegenheitspflicht verinnerlicht. Aber was bedeutet dies für die elektronische Kommunikation? Obwohl die Papier-Post als Garant für Postgeheimnis und Datensicherheit einsteht, wird ihre Dienstleistung in der geschäftlichen Korrespondenz immer weniger genutzt. Neuerdings wird gemailt, per SMS oder Whats-App kommuniziert oder gleich im Internet per Skype miteinander gesprochen. Im Alltag einer Wirtschaftsprüfungskanzlei kommen in Verbindung mit modernen Kommunikationsmedien regelmäßig folgende typischen Verhaltensweisen vor:

- Recherche im Internet über Mandanten oder mit ihnen in Verbindung stehende Personen/Unternehmen
- Kommunikation via E-Mail
- Versand von Unterlagen per E-Mail oder als Upload über das Internet
- Bereitstellung von Unterlagen auf der eigenen Homepage für den Mandantenzugriff.

Spätestens seit dem NSA-Skandal der letzten Monate ist klar, dass die Nutzung des Internets eine erhebli-

che Gefahrenquelle für vertrauliche Daten darstellt, deren Schutz alles andere als eine Kleinigkeit ist.

Im Rahmen dieses kurzen Beitrags kann kaum eine vollständige Darlegung der technisch möglichen und berufsrechtlichen denkbaren Risiken und deren Präventionsmaßnahmen gelingen. Eines sollte jedoch jedem Berufsträger bewusst sein: Wer im Jahr 2014 nicht wenigstens allgemein verfügbare und gut beherrschbare Schutzsysteme standardmäßig im Kanzleialltag einsetzt, setzt sich dem Risiko der schwerwiegenden Berufspflichtverletzung und gegebenenfalls sogar einer strafbaren Handlung aus.

Zu derartigen Schutzsystemen gehören insbesondere die verschlüsselte E-Mail-Kommunikation und der Schutz von Dokumenten durch Verschlüsselung. Beide Verfahren setzen keine besonderen IT-Fähigkeiten mehr voraus, wohl aber eine entsprechende Kanzleiorganisation. Nachfolgend soll hierzu auf ausgewählte Aspekte eingegangen werden.

Typische Risiken bei der Nutzung elektronischer Medien

Der IDW RS FAIT 2 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce) listete bereits im Jahr 2003 typische Probleme bei der elektronischen Kommunikation auf, die nahezu gleichlautend auch für die Kommunikation von WP-Praxen gelten können:

- Daten werden häufig unverschlüsselt oder unter Verwendung einer unsicheren Verschlüsselung übertragen (Verlust der Vertraulichkeit).
- Daten werden häufig ohne oder mit unzureichendem Schutz vor Verfälschung übertragen (Verlust der Integrität).
- Der Anschluss eines IT-Systems an das Internet birgt die Gefahr, Ziel von Angriffen zu werden, beispielsweise durch Viren, Trojaner oder Hacker (Verlust der Verfügbarkeit).
- Es existieren keine wirksamen Authentisierungsmechanismen zwischen den im Internet angeschlossenen Rechnern (Verlust der Authentizität).
- Beim Datentransfer können Hilfsprogramme (Java, Active-X) zu unautorisierten Zugriffen auf IT-Systeme führen (Verlust der Autorisierung).

Die Verwendung aktueller Virenschutzprogramme in allen elektronischen Bereichen (inklusive Mobiltelefone und Tablets) sollte für den Berufsträger selbstverständlich sein, so dass hierauf nicht weiter eingegangen wird.

Verschlüsselung von Dokumenten/Daten

Sensible Daten sollten zur Sicherstellung der erforderlichen Vertraulichkeit ausschließlich verschlüsselt versandt werden. Dabei sollten zunächst Regelungen getroffen werden, was genau die Kanzlei unter vertraulichen Daten versteht. Gleichzeitig sollten die Berufsträger ihre Mandanten aufgrund ihrer Vorbildfunktion anhalten, sensible Daten ebenfalls nur in verschlüsselter Weise (an den Wirtschaftsprüfer) zu versenden.

Die sichere Übertragung von Nachrichten kann mit Hilfe verschiedener Verfahren gewährleistet werden. Bei transportunabhängigen Verschlüsselungsverfahren (Ende-zu-Ende-Verfahren) können die Daten unabhängig vom Transportkanal (zum Beispiel E-Mail, USB-Stick, CD-Rom) nur von dem eigentlichen Empfänger entschlüsselt werden. Ein potentieller Angreifer kann die Kommunikation zwar abhören, aber die Nachricht nicht entschlüsseln. Daneben sind Transportverschlüsselungen möglich, bei denen Einzelnachrichten innerhalb eines verschlüsselten Transportkanals (sogenannter „Tunnel“) versendet werden. Ein potentieller Angreifer kann den Transport dadurch nicht abhören und die Daten nicht mitlesen. Derartige Tunnel werden beispielsweise beim SSL-basierten Online-Banking verwendet.

ZIP-Verschlüsselung oder PDF-Verschlüsselung

Für den einfachen und pragmatischen Austausch sensibler Daten bietet sich die Verwendung pass-

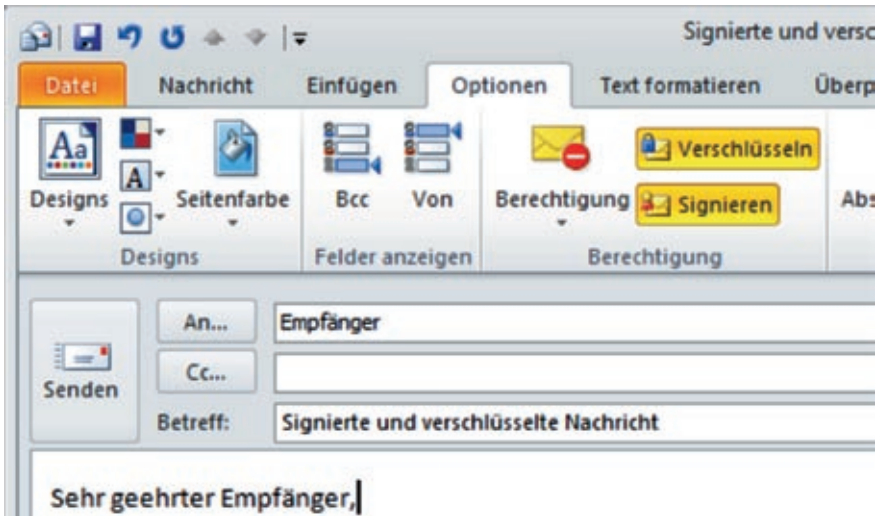

Abbildung 1: S/MIME-Nutzung bei Microsoft Outlook

WPin/StBin Dipl.-Kffr. Katrin Fischer, VISUS GmbH Wirtschaftsprüfungsgesellschaft, ist Mitglied des Beirates und Landespräsidentin der Wirtschaftsprüferkammer in Berlin.

Steffen Heyde ist Portfolio Manager bei secunet Security Networks AG

wortgeschützter PDF- oder ZIP-Container an. Programme wie Adobe Acrobat oder Tools wie Winzip, Winrar oder 7-Zip bieten seit Jahren Funktionen an, mit denen beliebige Dateien einfach per rechtem Mausklick mittels Passwort mit starken Algorithmen verschlüsselt werden können. Die so verschlüsselten Dateien können via E-Mail oder per USB-Stick einfach transportiert werden. Da sich die Container nahezu beliebig grafisch gestalten lassen, können sie der Kanzlei zusätzlich als wirksames Marketinginstrument dienen.

Das für die Verschlüsselung verwendete Passwort ist dem Kommunikationspartner auf einem sicheren zweiten Kanal (zum Beispiel Telefon, Post mit Rubbelfeld) mitzuteilen. Dabei bietet es sich an, für jeden Mandanten ein individuelles Passwort zu nutzen. Dies erfordert eine entsprechende Passwortverwaltung in der Kanzlei.

Selbstverständlich müssen die genutzten Passwörter dem jeweiligen Stand der Technik entsprechen und notfalls regelmäßig aktualisiert werden. Derzeit sollte ein sicheres Passwort mindestens neun Zeichen lang sein und den gesamten möglichen Zeichenraum ausnutzen (Ziffern, Groß- und Kleinbuchstaben, Sonderzeichen). Werden Dokumente so geschützt, sind auch über unsichere Kanäle die größten Risiken gebannt.

Sichere E-Mail-Kommunikation

Daneben ist eine Verschlüsselung der E-Mails möglich. Die gängigsten E-Mail-Systeme wie Microsoft Outlook, Lotus Notes oder Mozilla Thunderbird bieten die Verschlüsselung von E-Mails ohne weitere Zusatz-Software auf Basis des international anerkannten Sicherheitsprotokoll S/MIME (Secure/Multipurpose Internet Mail Extensions) an.

Allerdings sind für die Verwendung von S/MIME sogenannte Zertifikate erforderlich, die bei Trustcentern in verschiedenen Vertrauensstufen bezogen werden können und überschaubare jährliche Kosten verursachen. Um eine Nachricht bei S/MIME verschlüsseln zu können, benötigt der Sender das jeweils individuelle Zertifikat seines Kommunikationspartners, also des Mandanten. Vor der ersten Kommunikation mit einem Mandanten sind durch Austausch der Zertifikate beziehungsweise Schlüssel die technischen Voraussetzungen für eine

Abbildung 2: → www.wpk.de/link/mag021406/

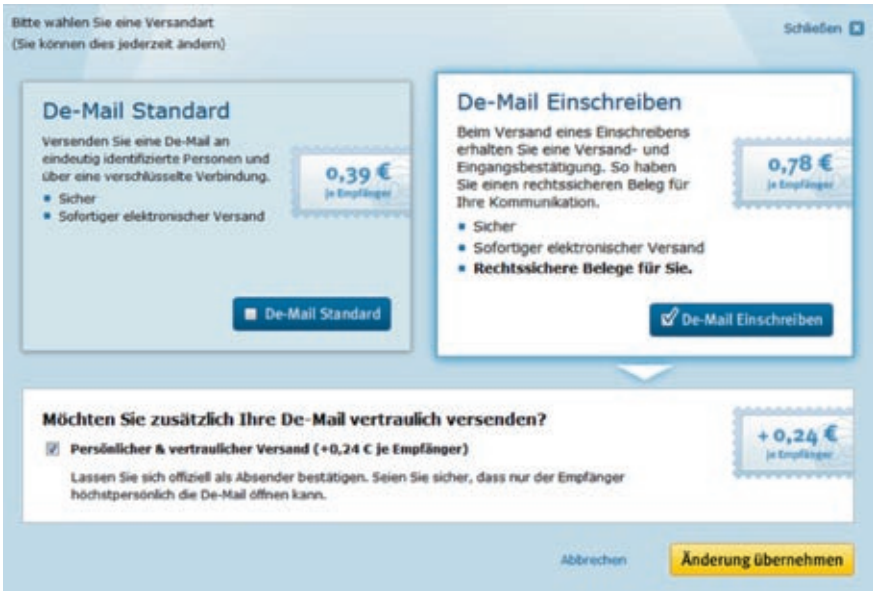

Abbildung 3: Auswahl Versandoptionen bei web.de

verschlüsselte Kommunikation zu schaffen. Die so ausgetauschten Schlüssel müssen in der Kanzlei verwaltet und aktuell gehalten werden. Und genau hier liegt die Achillesferse des Systems, denn die Koordinierung dieser Vielzahl an Zertifikaten ist nach den bisherigen Erfahrungen sehr aufwendig. Immer wieder treten auch reale technische Schwierigkeiten bei der Verbindung unterschiedlicher Kommunikationswelten verschiedener Unternehmen auf.

Es bleibt festzuzahlten, dass die hohen organisatorischen Anforderungen an die Verwaltung der Verschlüsselungsinfrastruktur die E-Mail-Verschlüsselung zu einem überraschend aufwendigen Verfahren machen.

De-Mail

Seit 2011 existiert in Deutschland das sogenannte De-Mail-Gesetz, auf dessen Grundlage privatwirtschaftlich agierende Diensteanbieter ein Kommunikationsnetz auf Basis erweiterter E-Mail-Standards etabliert haben, welches den Versand elektronischer Nachrichten in verschlüsselter, geschützter und auch hinsichtlich der Zustellsicherheit nachweisbarer Form gewährleistet. Aufgrund spezialgesetzlicher Haftungsnormen übernehmen die Provider die gesamten Haftungsrisiken hinsichtlich Identität des Empfängers, Vertraulichkeit der Daten und Integrität der Übermittlung. De-Mail gilt unter anderem als sicherer Zugangsweg für den elektronischen Rechtsverkehr mit der Justiz.

Das eigens geschaffene De-Mail-Gesetz regelt die Mindestanforderungen an den sicheren elektronischen Nachrichtenaustausch. De-Mail wird daher nur von Providern angeboten, die beim Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditiert sind; hierzu zählen derzeit T-Systems, T-Online, Web.de, GMX und Mentana-Claimsoft.

Für die Nutzung von De-Mail müssen alle Kommunikationspartner (Absender und Empfänger) einen De-Mail-Account und eine De-Mail-Adresse (zum Beispiel hans.meyer@unternehmen.de-mail.de) besitzen. Damit ist jeder Kontoinhaber eindeutig identifiziert – dies gilt sowohl für Behörden und Unternehmen als auch für natürliche Personen. Bisher haben bereits etliche Tausend Unternehmen ein De-Mail-Konto.

Der Absender kann für einzelne De-Mails das gewünschte Authentisierungsniveau definieren. Neben der obligatorischen Transportverschlüsselung, die auch zwischen den De-Mail-Providern verpflichtend ist, kann zusätzlich eine Ende-zu-Ende-Verschlüsselung zum Beispiel mittels S/MIME oder ZIP-Verschlüsselung für Sonderfälle genutzt werden. Der Versender kann bei seinem Provider analog dem postalischen Einschreibe-Verfahren Nachweise über Versand und den Eingang einer De-Mail beim Empfänger anfordern.

Im Gegensatz zur einfachen Mail fallen beim Versand einer De-Mail Kosten in Form eines E-Porto an, die aber deutlich unterhalb des Briefportos liegen. Zieht man in Betracht, dass die Provider den Berufsträger von den kommunikationsbedingten Haftungsrisiken freistellen, ist das E-Porto mit Sicherheit jeden Cent wert.

Fazit

In Anbetracht der eingangs dargestellten Risiken und des stetigen Ausbaus der elektronischen Kommunikation sollte die Nutzung der jeweils aktuellen Schutzinstrumente für jeden Berufsträger obligatorisch sein. Hierzu gehört neben einer Verschlüsselung auf Dateiebene auch die Möglichkeit, per De-Mail erreichbar zu sein. Rechtsanwälte haben die Einrichtung eines besonderen elektronischen Anwaltspostfachs (beispielsweise in Form eines De-Mail-Postfachs) übrigens ab 2016 verpflichtend für ihre Berufsträger geregelt.