ELEKTRONISCHER SCHRIFTVERKEHR

# Einhaltung der anwaltlichen Schweigepflicht: Die sichersten Wege des E-Mail-Versands

von Christian A. Fischer, MBA (univ.), Augsburg

| E-Mail-Kommunikation und elektronische Akten haben mittlerweile in nahezu jede Anwaltskanzlei Einzug gehalten. Die Nutzung von Webmail-Diensten und Web- oder E-Mail-Hostern birgt viele Sicherheitsrisiken, die zur Verletzung der Schweigepflicht, mithin Strafbarkeit, führen können. Im Folgenden werden die Risiken des unverschlüsselten E-Mail-Verkehrs aufgezeigt und die passenden Lösungsansätze stichpunktartig geliefert. |

## 1. Tatsächliche und rechtliche Risiken

Das Risiko einer unerwünschten Dateneinsicht besteht auf dem Versandweg einer E-Mail an verschiedenen Stellen:

**Unverschlüsselte E-Mails bieten Sicherheitslücken auf dem Server, ...**

- Server des E-Mail-Providers: Die gängigen Protokolle zur Kommunikation mit dem Mail-Server (SMTP, POP, IMAP) stellen ein enormes Sicherheitsrisiko dar. Bei der Übertragung werden der Benutzername und das Passwort „im Klartext übermittelt" und können von Dritten abgefangen werden (Schmeh, Kryptografie, 2013, S. 671).

**... bei der Übertragung im Internet ...**

- Übertragung im Internet: E-Mails können abgefangen und gelesen werden. Das Abfangen ist mit durchschnittlichen Programmierkenntnissen einfach.

  Achtung | Bei verschlüsselter Übertragung ist zu beachten, dass nur die Übertragung gesichert ist, nicht aber die Speicherung der E-Mails am Endpunkt. Hier wird wieder im Klartext gespeichert (Schwenk, Sicherheit und Kryptografie im Internet, 2010, S. 118).

**... und auf den Rechnern in der Kanzlei**

- Kanzlei-Rechner: E-Mails können auf Kanzlei-Computern eingesehen werden, wenn im Netzwerk kein ausreichender Virenschutz vorhanden ist. Durch Öffnen einer E-Mail mit Schadsoftware können Programme ausgeführt werden, die dazu führen, dass Dritte Daten übermittelt bekommen oder gar Zugriff auf das interne Netzwerk der Kanzlei erhalten.

**Verletzung der Schweigepflicht gemäß § 203 StGB strafbar**

In § 203 Abs. 1 Nr. 3 StGB wird eine anwaltliche Verletzung der Schweigepflicht strafrechtlich mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe geahndet. Der Anwalt macht sich gemäß § 203 Abs. 1 Nr. 3 in Verbindung mit § 13 StGB einer Offenbarung durch Unterlassen strafbar, wenn er es pflichtwidrig unterlässt, die erforderlichen Sicherheitsmaßnahmen vorzunehmen und dadurch billigend in Kauf nimmt, dass Dritte Kenntnis von einer E-Mail nehmen können. Die herrschende Meinung geht davon aus, dass sich ein Rechtsanwalt, der zur Kommunikation mit Mandanten, Gegnern oder Gerichten das Kommunikationsmittel der unverschlüsselten E-Mail verwendet, gemäß § 203 StGB strafbar macht. Die Verwendung von verschlüsselten E-Mails für die Kanzleikommunikation wird daher dringend angeraten.

## 2. Lösungsmöglichkeiten für Ihre Kanzlei

Einige Lösungsmöglichkeiten verbessern die aufgezeigten Sicherheitsprobleme jedenfalls. Beachten Sie jedoch die verschiedenen Sicherheitsstufen.

### a) Verschlüsselung: einer der sichersten Wege zur Textsicherung

**Sicherheit durch die sogenannte „End-to-End"-Verschlüsselung**

Ziel einer Verschlüsselung ist eine sogenannte „End-to-End"-Verschlüsselung der E-Mail. Dies bedeutet, dass die Nachricht vom Versender verschlüsselt wird und erst vom Empfänger entschlüsselt werden kann. Sehr große Sicherheit bietet das sogenannte asymmetrische kryptografische Verfahren: Jeder Nutzer erzeugt lokal einen privaten und öffentlichen Schlüssel. Die Nachrichten werden vom Absender mit einem öffentlichen Schlüssel verschlüsselt. Der Empfänger kann diese E-Mail mit seinem privaten Schlüssel auf seinem Rechner wieder entschlüsseln.

**Metadaten bleiben aber weiterhin unverschlüsselt**

PRAXISHINWEIS | Es wird jedoch lediglich der Text einer E-Mail verschlüsselt. Die Metadaten, wie z.B. der Absender, Empfänger und Betreff, werden weiterhin unverschlüsselt im Internet übertragen. Eine Verschlüsselung der Metadaten ist aktuell noch nicht praktikabel möglich.

### b) Elektronische Signatur: sichert die Identifikation des Absenders

Die Identifikation des Absenders ist stets gewährleistet. Unterschieden werden folgende Unterarten, von denen die letzte am sichersten ist:

- Bei der einfachen elektronischen Signatur handelt es sich um ein Datum in elektronischer Form. Das Datum wird anderen Daten beigefügt und dient zur Authentifizierung.
- Fortgeschrittene elektronische Signaturen sind Signaturen, die nur dem Signaturschlüsselinhaber zugeordnet sind. So ist eine genaue Identifizierung möglich.
- Eine qualifizierte elektronische Signatur ist eine Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht. Sie ist daher ein mit einem privaten Signaturschlüssel erzeugtes Siegel. Es wird im Anschluss mit einem öffentlichen Schlüssel, dem Zertifikat einer Zertifizierungsstelle, versehen. Eine Verfälschung der enthaltenen Daten ist nahezu ausgeschlossen (Eckert, IT-Sicherheit, 2012, S. 402).

**Qualifizierte Signatur: privater und öffentlicher Schlüssel**

### c) De-Mail: erschwert das Abfangen, bietet aber keine volle Sicherheit

**De-Mail setzt die EU-Dienstleistungsrichtlinie um**

Die De-Mail ist ein Ergebnis der deutschen Bundesregierung zur Umsetzung der EU-Dienstleistungsrichtlinie. Sie beruht generell auf der E-Mail-Technik, ist jedoch von ihr technisch getrennt. Die Dienstleistung wird von zertifizierten privaten Anbietern zur Verfügung gestellt. Durch eine sichere Authentifizierung der Teilnehmer bei der Registrierung wird sichergestellt, dass eine höchstmögliche Vertraulichkeit gewährleistet ist. Die De-Mails verlassen das Internet nicht und bleiben somit im De-Mail-System. Sehr sicher ist die Kommunikation per De-Mail aber nicht, da jeder mit Zugriff auf die Server des Providers die Möglichkeit besitzt, die Nachrichten abzufangen. Zwar stellt die De-Mail einen Zugewinn an Sicherheit gegenüber dem Versand einer normalen E-Mail dar, da ein Eindringen in das System und auf die Server nötig ist.

Bei einer echten „End-to-End-Verschlüsselung“ liegt die vorhandene Sicherheit jedoch bei Weitem höher. Auch, dass der Anbieter praktisch jede E-Mail entschlüsseln kann und staatliche Stellen einen Einblick in diese Kommunikation haben können, ist als bedenklich anzusehen.

**Verschlüsselung ist sicherer als De-Mail**

### d) E-Post-Brief: bietet Sicherheit nur im geschlossenem System

**Kommunikation nur für Kunden des E-Post-Briefs untereinander**

Der E-Post-Brief ist ein sogenannter Hybridpostdienst. Er wird von der Deutschen Post AG angeboten und soll einen besseren Datenschutz und mehr Authentizität als herkömmliche E-Mails gewährleisten. Mit dem elektronischen E-Post-Brief können nur Kunden des E-Post-Brief-Diensts miteinander kommunizieren, da es sich um ein geschlossenes System handelt. Der Absender und der Empfänger werden dadurch umfangreich authentifiziert. Dringen aber Dritte in das geschlossene System ein, stehen diesen sämtliche Schlüssel und Echtdaten zur Verfügung. Insgesamt ist der E-Post-Brief durch eine Portalverschlüsselung dennoch eine bessere Alternative zur herkömmlichen unverschlüsselten E-Mail (Heckmann, Seidl, Adäquates Sicherheitsniveau bei der elektronischen Kommunikation, 2012, S. 107).

**PRAXISHINWEIS |** Wenn Sie nicht den Weg über die Verschlüsselung von E-Mails gehen, sollten Sie immerhin für den Bereich der E-Mail-Nutzung eine umfassende Einwilligung Ihres Mandanten zur genutzten Kommunikationsart einholen. Das erhöht Ihre Rechtssicherheit jedoch auch nur eingeschränkt.

**FAZIT |** Es lässt sich abschließend festhalten, dass durch den Einsatz von Verschlüsselung und Signatur das Risiko, dass Mandatsgeheimnisse durch das Abfangen von E-Mails offenbart werden, erheblich verringert werden kann. Der verschlüsselte Inhalt kann ohne zugehörige Schlüssel nicht gelesen oder verfälscht werden. Lediglich die Metadaten, wie Absender, Betreff der E-Mail usw., bleiben erkennbar. Auch die Alternativen De-Mail und der E-Post-Brief bedeuten in der Kommunikation von Kanzleien einen Gewinn an Sicherheit, dürften jedoch in der Praxis aufgrund der geringen Verbreitung kaum handhabbar sein. Zudem besteht immer noch keine echte End-to-End-Verschlüsselung. Hier müssen immer noch die Anbieter die jeweiligen Schlüssel vorhalten, was wiederum ein Sicherheitsrisiko darstellt. Die Sicherheitswege sollten in folgender Reihenfolge gewählt werden: 1. Verschlüsselung von E-Mails 2. Einverständnis der Mandanten 3. Elektronische Signatur 4. De-Mail 5. E-Post-Brief. Jede Kanzlei muss für sich entscheiden, in welchem Verhältnis das Risiko einer Straftat nach § 203 StGB zur technischen Aufrüstung der Kanzleiausstattung (Verschlüsselung von E-Mails) steht.

**Verschlüsselung und Signatur verringern das Sicherheitsrisiko erheblich**

↘ WEITERFÜHRENDE HINWEISE

- AK 14, 127: Datenaustausch – im Büro mobil abhörsicher kommunizieren
- Bleich, Privatsache E-Mail, Nachrichten Verschlüsseln und signieren mit PGP, c't Magazin für Computer und Technik, 2013, 83
- Reuer, Die EU-Dienstleistungsrichtlinie, 2011, 8

ARCHIV
Ausgabe 8 | 2014
Seite 127