Spies: Prism-Debatte und Vertraulichkeit der Anwaltskommunikation ZD-Aktuell 2013, 03668

Prism-Debatte und Vertraulichkeit der Anwaltskommunikation

Dr. Axel Spies ist Rechtsanwalt bei Bingham McCutchen in Washington DC und Mitherausgeber der Zeitschrift ZD.

Im Beck-Blog gab es eine lesenswerte Diskussion zum Thema NSA-Skandal und Vertraulichkeit der Anwaltskommunikation. Eine Grundfrage ist, ob die geltenden Wege der E-Mail-Kommunikation rechtlich ausreichend und gesichert sind. Anbei eine Zusammenfassung der weiterhin offenen Debatte.

Hintergrund

Die elektronische Kommunikation von Anwälten mit Mandanten mittels E-Mail gehört mittlerweile zum Alltag. Ob sich aber aus der anwaltlichen Schweigepflicht des § 43 a BRAO, § 2 BORA mit der strafrechtlichen Absicherung des § 203 StGB überhaupt eine Einschränkung für die elektronische Kommunikation mittels E-Mail ergibt, wird durchaus unterschiedlich beurteilt. Weder in der Rechtsprechung noch in der Literatur scheinen sich die Experten bislang für eine generelle Unzulässigkeit der unverschlüsselten elektronischen Kommunikation ausgesprochen zu haben. Eine Grundfrage ist: Reicht die mutmaßliche Einwilligung des Mandanten für eine unverschlüsselte Kommunikation aus?

Stellungnahmen

Ein Teilnehmer führte an, dass ein Anwalt seinen Mandanten die Kommunikation mit Verschlüsselung mittels der fortgeschrittenen Signatur zumindest anbieten solle – gerade im Lichte des *NSA*-Skandals. Diese sei nicht sonderlich schwierig zu installieren und (im Moment) hinreichend sicher. Eine ggf. auch nur konkludente Einwilligung des Mandanten sei bei E-Mails ohne Verschlüsselung nötig. Deshalb sieht der Teilnehmer im Hinblick auf neue Vorgaben keinen Handlungsbedarf.

Eine Verschlüsselung per qualifizierter Signatur (und Akkreditierung) sei hingegen ein „vollständiger Irrweg mit einer Insellösung, die plattformübergreifend schlicht nicht funktioniert." Nach dem Dafürhalten des Teilnehmers sei für sichere Kommunikation (sowohl mit Mandanten als auch mit Gerichten) eine fortgeschrittene Signatur (feS) ausreichend. Das gelte umso mehr, als man bei der qualifizierten elektronischen Signatur (qeS) nach dem deutschen SigG mit Akkreditierung „relativ staatsnah" sei, wenn man einer staatlichen Datensammlung zuvorkommen möchte. Wenn elektronischer Rechtsverkehr für Anwälte zwingend werden sollte, sollte man nach der Meinung dieses Teilnehmers mindestens mit zwei Rechnern als Anwalt arbeiten, von denen einer (der Arbeitsrechner)

dauerhaft nicht mit dem Internet verbunden ist.

Ein anderer Blog-Teilnehmer meint, dass sich aus den genannten Vorschriften keine Einschränkungen der mandatsbezogenen Kommunikation zwischen Anwalt und Mandant ergeben kann, wenn dieser seine Einwilligung erteilt habe, dass die Kommunikation via E-Mail abgewickelt wird. Insofern sieht dieser Teilnehmer auch die unverschlüsselte Antwort eines Mandanten auf eine E-Mail des Rechtsanwalts als Erklärung an, die Kommunikation zukünftig auf diesem Wege abwickeln zu wollen.

Da sich die E-Mail zum vorherrschenden Kommunikationsmittel auch für Anwälte entwickelt hat, lässt dies nach Ansicht des Teilnehmers auch den Schluss zu, dass, sofern der Mandant seine E-Mail-Adresse mitteilt, er auch auf diesem Wege mandatsbezogene Kommunikation betreiben will. In Anbetracht der neuesten Entwicklungen des Prism-Programms der *NSA* sei es allerdings wahrscheinlich, dass häufiger als bisher von Mandanten der Wunsch geäußert werde, eine sicherere Kommunikationsform als den gewöhnlichen E-Mail-Verkehr anzubieten.

Ein weiterer Blog-Teilnehmer hält es für grundsätzlich fraglich, ob man sensible Daten durch Verschlüsselung des E-Mail-Verkehrs vor dem Zugriff durch US-Behörden schützen kann. U. U. gehe man sogar das Risiko ein, dass der E-Mail-Verkehr gerade auf Grund der Verschlüsselung archiviert werde. Zwei vom britischen *Guardian* veröffentlichte Dokumente, auf denen auch die Unterschrift von US-Attorney General *Eric Holder* zu finden sei, zeigen nach Ansicht des Teilnehmers, unter welchen Voraussetzungen die *NSA* auch US-Bürger überwachen darf. Dabei scheint man auch daran anzuknüpfen, ob eine Nachricht verschlüsselt ist oder nicht. Zwar bezogen sich die Dokumente auf die Überwachung von US-Bürgern – so dieser Teilnehmer, allerdings deute der zitierte Bericht darauf hin, dass verschlüsselte Nachrichten für die *NSA* „besonders interessant" seien. Deshalb meint der Teilnehmer, dass eine dortige Archivierung der E-Mail in der Hoffnung, die Nachricht später entschlüsseln zu können, weitaus wahrscheinlicher sei als bei einer nicht verschlüsselten Nachricht.

Fazit

Die im Blog nur angestoßene Diskussion zeigt, dass aus Anwaltssicht kein großes Bedürfnis besteht, die E-Mail-Kommunikation mit Mandanten zu verschlüsseln. Das verwundert nicht, denn Verschlüsselungssysteme sind aufwändig und nicht ganz billig. Aus Mandantensicht könnte dies anders sein: Bei großen Anwaltskanzleien wird schon jetzt immer häufiger bei der Erteilung von wichtigen Mandaten ein Audit gefordert, dass die Verfahrensdaten, gespeicherte Dokumente und die elektronischen Kommunikationswege sicher sind. Im einen oder anderen Fall wird es durchaus vorkommen, dass der Mandant bittet, die Dokumente nur in seinem Heimatland zu speichern oder die Kommunikation zu verschlüsseln. Das Problem geht allerdings über den E-Mail-Verkehr hinaus, da auch Telefongespräche abgehört und gespeichert werden können – gerade wenn wie bei VoIP

Informationswege über das Internet gewählt werden. Auch an die wachsenden Mobilitätsanforderungen des Anwalts und die Kommunikation via WLAN und Mobilfunk und die Verwundbarkeit dieser Kommunikationswege ist zu denken.

Ein denkbarer, einfacher Weg ist die von E-Mail-Providern oftmals kostenlos angebotene Möglichkeit zu nutzen, den E-Mail-Versand mittels Transportverschlüsselung, z. B. TLS, abzusichern. Besonders verwundbar ist jede Anwaltskommunikation, die extern, z. B. beim Provider oder in der „Cloud", abgespeichert wird. Deswegen sollte sich der Rechtsberater vorab informieren, welche Speicherungsmöglichkeiten bestehen und wie diese abgesichert sind. Entscheidende Kriterien für die Nutzung von Verschlüsselungstechniken sollten das technische Verständnis des Mandanten für die involvierten Risiken sowie das Sicherheitsbedürfnis des Mandanten sein (vgl. die neuesten Empfehlungen der *Rechtsanwaltskammern Hamm* und *Düsseldorf* zur Anwaltskommunikation). Ein allgemeines Gebot zur Verschlüsselung mittels Signatur gibt es derzeit nicht. Gerade in Fällen eines besonderen Sicherheitsbedürfnisses sollte der Anwalt eine ausdrückliche Erklärung des Mandanten einholen, die zu Beweiszwecken durchaus schriftlich festgehalten werden sollte.

Weiterführende Links

Vgl. zu Prism auch *Spies,* ZD-Aktuell 2013, 03608; ZD-Aktuell 2013, 03659 und ZD-Aktuell 2013, 03652.