Privacy by Design in der anwaltlichen Praxis

Vermeidung von Lücken bei der Vertraulichkeit im Zeitalter des Internets

Die Vertraulichkeit kann in der anwaltlichen Praxis nie hoch genug gehalten werden. Daher muss es immer das Ziel sein, solche Technik einzusetzen, die von sich aus die Vertraulichkeit sicherstellt (Privacy by Design).

Bevor der Computer und insbesondere das Internet Einzug in die Kanzlei gehalten haben, war die anwaltliche Welt noch relativ einfach. Schriftsätze wurden mit der Post oder per Fax versandt, fernmündlich kommuniziert wurde ausschließlich über das Telefon. Die Wege, über die Daten die Kanzlei verlassen konnten, waren überschaubar und man konnte noch das Gefühl haben, die Vertraulichkeit sei unter Kontrolle. Das Internet hat diese Situation schlagartig verändert. Die neuen Kommunikationsmöglichkeiten und die Vernetzung der Kanzlei-Rechner haben viele Tore geöffnet, durch die Daten ungewollt und unkontrolliert nach draußen gelangen können. Die Herausforderung ist nunmehr, die IT-Infrastruktur in der Kanzlei so aufzusetzen, dass die eingesetzte Technik nicht nur „sicher", sondern vielmehr so „designed" ist, dass neben der Akte keine zusätzlichen, unnötigen Daten entstehen können, die ins Internet gelangen können und dort im Zweifel auch nicht mehr zu löschen sind.

Die Kommunikation mit der Mandantschaft per E-Mail ist nach wie vor problematisch. Auch vor „Snowden" war bekannt, dass die E-Mail nicht mehr Vertraulichkeit bietet als eine Postkarte. Die Situation verbessert sich im Hinblick auf die Vertraulichkeit auch dadurch nicht, dass der Mandant in diese unsichere Kommunikation einwilligt. Zwar kann man die E-Mails verschlüsselt übertragen, allerdings muss man sich immer im Klaren sein, dass der Betreff der Nachricht unverschlüsselt übertragen wird und weitere Meta-Daten des E-Mail-Verkehrs, insbesondere die Verbindungsdaten (wer kommuniziert mit wem, wann und wie oft) im Internet „abgegriffen" werden können.

Beteiligung von Dritten an der Datenverarbeitung birgt stets Gefahren

Der Kern des Problems ist, dass Dritte bei der Speicherung von Daten und der Kommunikation mit der Mandantschaft beteiligt werden. Die Kanzlei legt die Akte in eine Web-Akte und macht diese für die Mandantschaft verfügbar. Zwar wird die Akte dort verschlüsselt abgelegt, allerdings bedient man sich in der Regel eines Providers, also eines Dritten, der die Daten vorhält. Die Daten haben die Kanzlei also bereits verlassen. Der unberechtigte Zugriff auf die Daten ist möglicherweise aufgrund der Verschlüsselung heute nicht möglich, allerdings kann man nie sicher sein, dass die Verschlüsselung in 10 Jahren nicht doch „geknackt" wird. Dann würde man sich natürlich besser fühlen, wenn die Daten die Kanzlei nie verlassen hätten. Auch für die Kommunikation wäre es wünschenswert, wenn nicht der E-Mail-Provider und sonstige Akteure des Internets an der Kommunikation mit der Mandantschaft beteiligt wären, sondern der Mandant direkt mit der Kanzlei ohne Beteiligung eines Dritten kommuniziert.

Dezentrale Strukturen schaffen Verlässlichkeit

Nimmt man den Grundsatz „Privacy by Design" also ernst, so muss man sich stets auch die Frage stellen, ob nicht auf die Beteiligung von Dritten bei der Speicherung von Kanzlei-Daten und bei der Kommunikation verzichtet werden kann. Der Einsatz von Cloud-Lösungen ist zwar aus technischer und ökonomischer Sicht effizient, allerdings darf gesteigerte Effizienz nicht dazu führen, dass die Vertraulichkeit in irgendeiner Form geschwächt wird. Das Aufkommen der Blockchains zeigt, dass das Internet zunehmend auf dezentrale Strukturen setzt, bei denen die Verlässlichkeit höher wiegt als wirtschaftliche und technische Effizienz. In der anwaltlichen Praxis (auch von Klein-Kanzleien) können bestehende Hardware- und Softwarelösungen eingesetzt werden, sodass direkt oder über dezentrale (anonymisierte) Netzwerke kommuniziert werden kann, ohne dass ein Dritter die Möglichkeit hat, Daten abzugreifen. Die Nutzung von dezentralen E-Mail-Lösungen mit Ende-zu-Ende-Verschlüsselung (einschließlich der Metadaten) oder Video-Konferenz-Systemen mit Chat-Funktion (unabhängig von Skype und WhatsApp) zur Kommunikation mit der Mandantschaft ist mit der zunehmend verbesserten Breitband-Situation durch entsprechende Hardware- und Softwarelösungen möglich. Durch die derzeitigen Bandbreiten ist es ohne weiteres möglich, über Fernzugriff mit dem Laptop oder Handy auf die Daten in der Kanzlei zuzugreifen. In vielen Fällen dürften die Leistungen von Dritten gar nicht notwendig sein.

Mehr Vertraulichkeit durch Vermeiden von Spuren im Internet

Die Anbindung der Kanzlei an das Internet birgt im Hinblick auf die Vertraulichkeit noch weitere (lösbare) Herausforderungen, die auf den ersten Blick nicht so offensichtlich sind. Die Kanzlei bewegt sich im Internet und hinterlässt (wie jeder andere Benutzer auch) Spuren. Es werden im Rahmen der Mandatsbearbeitung Suchbegriffe bei Google eingegeben, in Urteilsdatenbanken recherchiert, ausländische Texte übersetzt, die Seite des „Gegners" angesurft und Screenshots erstellt. Bei all diesen Tätigkeiten hinterlässt die Kanzlei Spuren, die jedoch keinesfalls mit dem Mandanten in Verbindung gebracht werden dürfen. Auch hier sollten Hard- und Softwarelösungen eingesetzt werden, die solche Datenlecks möglichst schließen. Vor allem dem zunehmenden bedenklichen Einsatz von „Trackern", bei denen die Kanzlei-Rechner durch ein Fingerprinting-Verfahren ohne Rückgriff auf die IP-Adresse leicht wiedererkannt werden können, kann durch Hardware- und Software-Lösungen begegnet werden. Weder die am Internet angeschlossene Kaffeemaschine und schon gar nicht der Kanzlei-Drucker sollte ungefragt mit Dritten „sprechen" können. Was für die Kanzleimitarbeiter selbstverständlich ist, muss auch für Maschinen in der Kanzlei realisiert werden.

Hinweis zum Autor:

Dr. Christopher De Nicolò
ist Rechtsanwalt. Er ist Autor und Entwickler juristischer Apps und Mit-Gründer der Privacy-Box „Trutzbox".