Das Berufsgeheimnis im digitalen Zeitalter

Wenn die Kommunikation zwischen dem Fachmann und seinem Kunden über einen technisch unzureichenden Kanal erfolgt, wird das Geheimnis nicht am Tag des Lecks gebrochen. Es wurde schon viel früher gebrochen, im Moment der Wahl des Werkzeugs.

Ein Problem, das fast niemand sieht

Ein Anwalt erhält auf seinem Telefon ein vertrauliches Dokument von einem Kunden. Ein Arzt bespricht mit einem Kollegen eine sensible Diagnose. Ein Psychologe koordiniert mit einem Psychiater die Behandlung eines Patienten. Ein Steuerberater sendet die Daten einer zur Prüfung anstehenden Erklärung. Alle tun dies per Instant Messaging. Und fast niemand hält inne, um darüber nachzudenken, wo diese Nachrichten tatsächlich landen.

Die Antwort ist in den meisten Fällen dieselbe: auf einem Server, den der Fachmann nicht kontrolliert, in einem Land, dessen Gesetzgebung er nicht unbedingt kennt, verwaltet von einem Unternehmen, dessen Geschäftsmodell – in direkten wirtschaftlichen Begriffen – darin besteht, Daten anzuhäufen. Die Nachricht mag bei der Übertragung verschlüsselt sein. Aber sobald sie den Server erreicht, ist sie eine Kopie, die in der Infrastruktur eines Dritten gespeichert ist und den operativen, rechtlichen und kommerziellen Entscheidungen dieses Dritten unterliegt. Nicht denen des Fachmanns.

Was die Gesetzgebung sagt

Die europäische Datenschutz-Grundverordnung ist in ihrem Artikel 32 eindeutig: Wer personenbezogene Daten verarbeitet, muss "geeignete" technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Angemessenheit der Maßnahmen wird nicht daran gemessen, "was die App vorgibt zu tun", sondern am tatsächlichen Risiko. Wenn Kundendaten auf einem Server landen, dessen Gerichtsbarkeit kein dem Europäischen Wirtschaftsraum gleichwertiges Schutzniveau garantiert, übernimmt der Verantwortliche – also der Fachmann – ein Risiko, dessen er sich wahrscheinlich nicht ganz bewusst ist.

Und es ist nicht nur die DSGVO. Das Berufsgeheimnis, das spezifisch für Anwälte, Ärzte, Psychologen, Wirtschaftsprüfer, Journalisten und andere geregelt ist, verlangt, dass die Kommunikation mit dem Kunden vertraulich ist. Nicht "so vertraulich wie möglich". Vertraulich ohne Wenn und Aber. Wenn der technisch genutzte Kanal dies nicht garantieren kann, übernimmt der Fachmann ein Risiko, das die Standesregeln seines Berufs nicht erlauben.

Das Paradoxe ist, dass das Risiko unsichtbar ist. Niemand prüft das Messaging der Kanzlei. Niemand verlangt den Datenverarbeitungsvertrag des Chat-Anbieters. Das Risiko tritt erst zutage, wenn es zu spät ist: ein Leck, eine veröffentlichte Sicherheitslücke, ein auf einem anderen Kontinent ohne Benachrichtigung des Benutzers vollstreckter Gerichtsbeschluss.

Was ein Fachmann technisch benötigt

Was ein Berufsgeheimnisträger benötigt, ist aus Sicht der Anforderungen eigentlich überraschend einfach:

- Ein Kanal, auf dem Nachrichten direkt vom Gerät des Senders zum Gerät des Empfängers gehen, ohne einen Zwischenserver zu passieren, der Kopien speichert.
- Eine Infrastruktur, deren Gerichtsbarkeit und Richtlinien durch Konstruktion auf die DSGVO ausgerichtet sind, nicht durch Erklärung.
- Eine Möglichkeit, sich gegenüber dem Gesprächspartner zu identifizieren, ohne berufliche Kontakte (Kundennamen, Telefonnummern, Adressbuch) an Dritte übergeben zu müssen.
- Ein überprüfbares System – nicht basierend auf dem Wort des Anbieters –, um zu bestätigen, dass die Nachricht bei der richtigen Person angekommen ist.

Es ist keine anspruchsvolle Liste. Es ist eigentlich das, was in der vor-digitalen Berufskommunikation als selbstverständlich vorausgesetzt wurde. Ein Einschreiben erfüllte all diese Kriterien. Ein Telefonanruf von der Kanzleizentrale zu der des Kunden ebenfalls. Das Merkwürdige ist nicht, dass diese Garantien heute gefordert werden: Das Merkwürdige ist, dass sie beim Übergang zum digitalen Kanal verloren gegangen sind, ohne dass es jemand bemerkt hat.

Der Unterschied zwischen Verschlüsseln und Nicht-Speichern

Es gibt eine nützliche Metapher. Eine Nachricht zu verschlüsseln und auf einem Server zu speichern, entspricht dem Legen eines Dokuments in einen Safe und dem Hinterlassen des Safes im Haus eines Unbekannten. Der Safe ist gut. Das Dokument kann im Prinzip nicht gelesen werden. Aber das Dokument *befindet sich weiterhin im Haus eines anderen*. Und dieser andere kann einen Gerichtsbeschluss erhalten, einen Cyberangriff erleiden, seine Servicebedingungen ändern, von einem anderen Unternehmen mit einer anderen Ethik gekauft werden oder morgen verschwinden.

Die strukturelle Alternative – nicht verfahrenstechnisch, nicht durch Vertrauen – besteht darin, dass das Dokument die Kanzlei nie verlässt. Dass es direkt vom Schreibtisch des Fachmanns zum Schreibtisch des Kunden reist, ohne jeglichen Vermittler. Das ist es, was die Punkt-zu-Punkt-Kommunikation zwischen Geräten technisch tut: Sie eliminiert den Vermittler. Nicht, dass der Vermittler böse wäre. Es ist nur so, dass der Vermittler für den Fall des Berufsgeheimnisses *unnötig* ist. Und Unnötiges muss in jedem System, das sicher sein will, aus Prinzip eliminiert werden.

Die Frage der Verantwortung

Letztlich ist die Frage, die jeder Berufsgeheimnisträger mit einem klaren Ja beantworten können sollte, folgende:

> Wenn morgen ein Gespräch mit einem meiner Kunden durchsickert und ein Gericht oder eine Berufskammer mich fragt, wie ich die Vertraulichkeit verwalte, kann ich dann technisch nachweisen, dass der von mir genutzte Kanal keine Kopien in der Infrastruktur Dritter speichert? Kann ich nachweisen, dass die Daten die Geräte der beiden an der Konversation beteiligten Personen nie verlassen haben? Kann ich, ohne mich auf das Wort eines Unternehmens von einem anderen Kontinent zu verlassen, nachweisen, dass die Vertraulichkeit durch die Architektur und nicht durch ein Versprechen garantiert war?

Wenn die Antwort nein lautet, ist das Problem nicht das Werkzeug im Konkreten. Das Problem ist, dass an ein Werkzeug eine Verantwortung delegiert wurde, für deren Unterstützung das Werkzeug nicht konzipiert war. Es ist, als würde man vertrauliche Akten in einen transparenten Umschlag stecken und darauf vertrauen, dass der Postbote nicht hineinschaut.

Das Werkzeug, das ein Fachmann wählt, um mit seinen Kunden zu kommunizieren, sagt viel darüber aus, wie er deren Vertrauen schätzt. Es gibt Werkzeuge, die so konzipiert sind, dass dieses Vertrauen nicht von Versprechen

abhängt, sondern von der Architektur. Und es gibt Werkzeuge, die das nicht sind. Den Unterschied zu kennen, ist Teil der Arbeit.

Zitierter Rechtsrahmen

- Verordnung (EU) 2016/679 (DSGVO), insbesondere Art. 5, 25 (Datenschutz durch Technikgestaltung) und 32 (Sicherheit der Verarbeitung).
- Bundesrechtsanwaltsordnung (BRAO) § 43a Abs. 2 (Berufliche Schweigepflicht).
- Strafgesetzbuch (StGB) § 203 (Verletzung von Privatgeheimnissen).
- Musterberufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä) § 9 (Schweigepflicht).

← ZurückVerschlüsseln bedeutet nicht privat sein: Was Metadaten über Sie aussagenWeiter →DSGVO und professionelles Messaging: Warum die meisten unwissentlich dagegen verstoßen

Aktuelle Lektüre

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 b0d25b06427e3efc4aa40ccd90f2a7a91806040e3203a164419d5143adc0479c

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.