Verschlüsseln bedeutet nicht privat sein: Was Metadaten über Sie aussagen

Verschlüsselter Inhalt und sichtbare Metadaten sind zwei verschiedene Dinge. Wenn ein Dienst von "Ende-zu-Ende-Verschlüsselung" spricht, erzählt er nur die halbe Geschichte.

Das Schloss, das nicht alles schützt

Ein Großteil der heutigen Messaging-Dienste wirbt mit Ende-zu-Ende-Verschlüsselung. Und das stimmt: Der Inhalt der Nachrichten wird verschlüsselt übertragen, sodass niemand auf dem Weg – nicht einmal der Dienstanbieter – den Text lesen kann, während er übertragen wird. Bis dahin ist die Aussage exakt.

Das Problem ist, dass der Inhalt nur ein Teil der Geschichte ist. Auch wenn niemand lesen kann, was Sie sagen, weiß der Dienst andere Dinge mit höchster Präzision: mit wem Sie sprechen, zu welcher Zeit, wie oft, von welchem ungefähren Standort aus, auf welchem Gerät, wie viele Nachrichten Sie senden und wie viele Sie empfangen, wie viele Dateien Sie teilen. All dies nennt man Metadaten. Und Metadaten sagen in vielen Fällen fast so viel aus wie die Nachricht selbst.

Was Metadaten offenbaren

Man muss keine Nachricht lesen, um viele Dinge zu wissen. Wenn eine Person sechs Monate lang jeden Dienstagmorgen um neun Uhr einen Onkologen anruft oder ihm schreibt, muss man das Gespräch nicht mithören, um zu ahnen, was vor sich geht. Wenn zwei Personen hundert Nachrichten am Tag austauschen und plötzlich damit aufhören, muss man keine einzige lesen, um zu verstehen, was passiert ist. Wenn ein Steuerberater in der Nacht vor einem Quartalsabschluss zwanzig Nachrichten hintereinander von demselben Kunden erhält, spricht das Muster für sich selbst.

Metadaten offenbaren Verhaltensmuster: wer mit wem in Beziehung steht, welche Zeitpläne jede Person hat, wann sie wach ist, wann sie schläft, wann sie reist, welche Kunden am aktivsten sind, welche beruflichen Beziehungen am intensivsten sind. Ein Server, der Metadaten sammelt, kann ein detailliertes Profil des persönlichen und beruflichen Lebens eines jeden Benutzers erstellen, ohne jemals ein einziges Wort von dem gelesen zu haben, was er schreibt.

Es gibt ein historisches Beispiel, das dies mit Härte illustriert. Der ehemalige Direktor der NSA, Michael Hayden, formulierte es 2014 ohne Umschweife: *"We kill people based on metadata"*. Die Aussage bezog sich auf US-Militäroperationen gegen Ziele, die ausschließlich anhand ihrer Kommunikationsmuster identifiziert wurden. Keine einzige gelesene Nachricht. Nur der Kontaktgraph und die Zeitpläne.

Dass ein Dienst Metadaten sammelt, bedeutet nicht zwangsläufig, dass er sie gegen seine Benutzer verwenden wird. Es bedeutet, dass er die Fähigkeit dazu hat, und dass ein Dritter mit Zugriff auf diese Daten – durch Gerichtsbeschluss, durch eine Sicherheitslücke oder durch Verkauf an Dritte, falls die Servicebedingungen dies zulassen – diese ebenfalls hat.

Der Zugriff auf das Adressbuch

Ein weiterer Vektor, der fast unbemerkt bleibt: die Kontaktliste. Ein Großteil der Messaging-Dienste bittet bei der Registrierung um Zugriff auf das Adressbuch des Telefons. Sie laden alle Nummern auf ihren Server hoch, um anzuzeigen, wer den Dienst noch nutzt. Von diesem Moment an hat das Unternehmen eine vollständige Karte der Beziehungen des Benutzers, auch wenn dieser noch nie eine einzige Nachricht an jemanden geschrieben hat.

Für einen Berufsgeheimnisträger – Anwalt, Arzt, Psychologe, Berater – enthält dieses Adressbuch Kunden. Wenn das Adressbuch auf einen Server von Drittanbietern hochgeladen wurde, befinden sich die Namen der Kunden in einer Infrastruktur, deren Gerichtsbarkeit und Richtlinien der Fachmann nicht kontrolliert. Das Berufsgeheimnis wird nicht erst an dem Tag gebrochen, an dem jemand ein Gespräch durchsickern lässt: Es wurde schon viel früher gebrochen, im Moment der Zustimmung zum Upload.

Der Unterschied zwischen Verschlüsseln und Nicht-Sammeln

Verschlüsseln bedeutet, den Inhalt zu schützen. Privat sein bedeutet, nicht zu sammeln, was nicht benötigt wird. Das sind verschiedene Dinge, und der Unterschied ist operativ entscheidend. Ein Dienst kann alle Nachrichten perfekt verschlüsseln und gleichzeitig fast alles über seine Benutzer über Metadaten wissen. Beides ist vollkommen kompatibel. Tatsächlich ist es das dominierende Geschäftsmodell in der Branche.

Die richtige Frage zur Bewertung der tatsächlichen Privatsphäre eines Dienstes lautet nicht *"Verschlüsselt er den Inhalt?"*. Diese Frage wird seit Jahren als beantwortet vorausgesetzt. Die richtige Frage lautet: *"Welche Metadaten werden erzeugt und wo werden sie gespeichert?"*. Und vor allem: *"Welche Metadaten muss er nicht erzeugen?"*.

Eine Architektur, die Metadaten durch Design minimiert – nicht durch Versprechen, nicht durch interne Richtlinien – ist strukturell privater als eine Architektur, die sie sammelt und verschlüsselt. Denn Daten, die nicht existieren, können weder durchsickern noch verkauft noch an einen Gerichtsbeschluss übergeben oder bei einer Sicherheitslücke verloren gehen.

Für den professionellen Leser

Wenn Ihre berufliche Tätigkeit Berufsgeheimnis, Vertraulichkeit oder einfach Respekt vor den Informationen Dritter beinhaltet, lohnt es sich, die Fragen in dieser Reihenfolge zu stellen:

1. Verschlüsselt die Anwendung, die ich zur Kommunikation verwende, den Inhalt? (Wahrscheinlich ja.)
2. Verschlüsselt sie die Metadaten? (Wahrscheinlich nein.)
3. Erzeugt sie Metadaten, die sie zum Funktionieren *nicht benötigt*? (Fast sicher ja.)
4. Wo sind diese Metadaten gespeichert und unter welcher Gerichtsbarkeit? (Wahrscheinlich außerhalb des Europäischen Wirtschaftsraums.)
5. Weiß mein Kunde oder Patient, dass seine Daten dort sind?

Die letzte Frage ist die unangenehme. Denn die ehrliche Antwort lautet in den meisten Fällen: nein.

Dieser Artikel ist der erste in einer Reihe über die tatsächliche Funktionsweise professioneller Kommunikationstools. Nächste Ausgaben werden die DSGVO-Konformität beim Messaging und das Konzept des Berufsgeheimnisses im digitalen Zeitalter behandeln.

Quellen und weiterführende Literatur

- Hayden, M. – Erklärung an der Johns Hopkins University, 2014 ("We kill people based on metadata"). Öffentliche Transkripte verfügbar.
- DSGVO (EU-Verordnung 2016/679), Art. 4 und 5 – Definition personenbezogener Daten und Grundsätze der Verarbeitung (Metadaten sind personenbezogene Daten).
- EDSB und EDSA – Stellungnahmen zur Verarbeitung von Verkehrsdaten und Metadaten in der elektronischen Kommunikation (ePrivacy-Richtlinie).

← ZurückEine kurze Geschichte des SiegellacksWeiter →Das Berufsgeheimnis im digitalen Zeitalter

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 c7bf0e7210f3ea4093cfd8a9b84812a5a0066dc266bf02b7843c582541f9dbcd

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