Analyse · 16. Mai 2026

← Zurück·Weiter →

Wenn niemand dazwischen ist

Die Verschlüsselung dessen, was über einen Server läuft, schützt den Inhalt. Keinen Server dazwischen zu haben, erübrigt die Frage. Beides ist nicht dasselbe.

Zwei Personen, ein Gespräch

Wenn zwei Personen in einem Raum von Angesicht zu Angesicht sprechen, muss niemand versprechen, dass er nichts gehört hat. Er hat nichts gehört, weil er nicht da war. Wenn zwei Personen ein Papier von Hand zu Hand weiterreichen, muss niemand dazwischen schwören, dass er es nicht gelesen hat. Es ist niemand dazwischen.

Die meisten Dinge im Alltag funktionieren so. Wir unterzeichnen keine Vertraulichkeitsvereinbarungen mit der Luft, die unsere Stimme überträgt, oder mit dem Papier, das wir halten. Die Privatsphäre des Gesprächs beruht nicht auf dem Versprechen eines Vermittlers, denn es gibt keinen Vermittler. Das ist eine der stärksten Formen von Privatsphäre: nicht weil sich etwas oder jemand gut verhält, sondern weil es dieses Etwas oder diesen Jemand gar nicht gibt.

Wenn das Gespräch in einen digitalen Kanal verlagert wird, ändert sich dies standardmäßig. Das übliche Modell ist folgendes: Zwei Personen verbinden sich mit einem Server, der Server empfängt die Nachricht, verschlüsselt sie oder speichert sie verschlüsselt und stellt sie dem Empfänger zu. Das Server ist dazwischen. Der Server kann ehrlich sein. Er kann auditiert sein. Er kann in einer günstigen Gerichtsbarkeit und unter einer strengen Datenschutzrichtlinie betrieben werden. All das kann wahr sein. Aber der Server ist dazwischen.

Der Unterschied zwischen Verschlüsseln und Nicht-Erheben (zweiter Teil)

In einem früheren Artikel derselben Serie haben wir dargelegt, dass die Verschlüsselung von Inhalten und das Nicht-Erheben von Metadaten nicht dasselbe sind. Es gibt einen weiteren Schritt, den man klar formulieren sollte: Verschlüsseln, was über einen Server läuft, und gar keinen Server zu haben, sind ebenfalls nicht dasselbe.

Das erste Modell — Server dazwischen, verschlüsselter Inhalt — schützt den Inhalt vor dem Betreiber des Servers, seinem Wartungspersonal, einem externen Angreifer, der das System kompromittiert. Und das ist wichtig. Aber es eliminiert den Server nicht. Der Server ist immer noch da. Er verarbeitet weiterhin Metadaten. Er ist weiterhin ein Punkt, der einen Gerichtsbeschluss, eine rechtliche Intervention, politischen Druck oder eine Sicherheitslücke erhalten kann. Er ist weiterhin ein Punkt, der Vertrauen in jemanden erfordert.

Das zweite Modell — kein Server zwischen den beiden Endpunkten — schützt den verschlüsselten Inhalt nicht besser: Wenn die Kryptografie solide ist, ist der Inhalt in beiden Fällen geschützt. Was sich ändert, ist nicht the Inhalt. Was sich ändert, ist, dass die Frage *„Was ist mit dem Server?“* gegenstandslos wird, weil es keinen Server gibt, nach dem man fragen könnte.

Vertrauen, Abwesenheit und der Unterschied zwischen beiden

Vertrauen kann gut investiert sein. Ehrliche Unternehmen existieren. Strenge Auditoren existieren. Nutzerfreundliche Gesetze existieren. Seriöse Dienste, die all das Genannte gewissenhaft erfüllen, existieren. Vertrauen ist, wenn es einem Betreiber geschenkt wird, der es verdient, keine schlechte Lösung.

Aber Vertrauen bleibt Vertrauen, egal wie solide es ist. Es ist eine soziale Lösung, keine technische. Ein Unternehmen kann den Besitzer wechseln. Eine Gerichtsbarkeit kann die Regierung wechseln. Morgen kann ein Gerichtsbeschluss eintreffen. Nächsten Monat kann eine neue Sicherheitslücke entdeckt werden. Nichts davon geschieht aus böser Absicht. Es geschieht, weil der Betreiber existiert, und alles Existierende ist den Unwägbarkeiten der Welt unterworfen.

Die Abwesenheit eines Betreibers ist diesen Unwägbarkeiten nicht unterworfen. Ein Gerichtsbeschluss kann keine Daten von einem Server verlangen, den es nicht gibt. Ein Angreifer kann keinen Server kompromittieren, den es nicht gibt. Eine Änderung der Unternehmensrichtlinien kann keine Daten betreffen, die das Unternehmen nie hatte. Der Schlüsselsatz ist einfach: Daten, die nicht existieren, können nicht verloren gehen.

Über das legitime Argument der Serverseite

Wer einen professionellen Messaging-Dienst mit Server dazwischen anbietet, führt meist drei vollkommen gültige Argumente an. Erstens, dass der Server notwendig ist, um die Zustellung zu garantieren, wenn der Empfänger offline ist. Zweitens, dass die Inhaltsverschlüsselung robust ist und der Betreiber sie daher nicht lesen kann. Drittens, dass der Dienst die europäische Gesetzgebung erfüllt und die Daten gesetzlich geschützt sind.

Alle drei Argumente sind wahr. Keines ändert das Wesen der Sache. Es stimmt, dass ein Server das Speichern von Nachrichten zur zeitversetzten Zustellung ermöglicht; es stimmt aber auch, dass zeitversetzte Zustellung anders gelöst werden kann, nämlich über Protokolle zur direkten Kommunikation zwischen Geräten, die seit Jahrzehnten verfeinert wurden und heute einsatzbereit sind. Es stimmt, dass die Verschlüsselung von Inhalten bei der Übertragung bei seriösen Diensten robust ist. Und es stimmt, dass die europäische Gesetzgebung Nutzer besser schützt als in vielen anderen Regionen.

Die Frage ist nicht, ob Dienste mit Server dazwischen legal sind, oder ob sie sicher sind, oder ob sie den Inhalt schützen. Sie können es sein, sie sind legal und meist sicher. Die Frage ist, dass ein Server dazwischen eine architektonische Entscheidung ist, keine technische Notwendigkeit. Und jede Entscheidung hat Konsequenzen. Eine Architektur mit Server dazwischen erzeugt zwangsläufig einen Akteur, dem man vertrauen muss. Eine Architektur ohne Server dazwischen nicht.

Was das Gesetz sagt und what die Architektur tut

Die DSGVO schreibt kein bestimmtes Architekturmodell vor. Sie verlangt Ergebnisse: Datenminimierung, Zweckbindung, Schutz durch Technikgestaltung und durch datenschutzfreundliche voreinstellungen, Nachweisbarkeit der Einhaltung. Ein Dienst mit Server dazwischen kann all diese Anforderungen erfüllen. Ein Dienst ohne Server dazwischen erfüllt mehrere davon bereits durch seine Konstruktion, nicht erst durch eine Erklärung. Absolute Minimierung — nichts zu erheben, was nicht zwingend für die Zustellung der Nachricht erforderlich ist — ist trivial, wenn kein Server existiert, der etwas erheben könnte.

Für alltägliche, nicht sensible Nutzungen ist eine Server-Architektur vollkommen vernünftig, und das Vertrauen in einen seriösen Betreiber eine gültige Lösung. Für andere Nutzungen — solche, die einem geregelten Berufsgeheimnis unterliegen, die deontologische Verantwortung mit sich bringen, die besonders sensible Informationen betreffen — ist das Fehlen eines Vertrauenspunktes kein Luxus, sondern ein struktureller Vorteil.

Für den professionellen Leser

Die Fragen, die man sich angesichts eines professionellen Kommunikationsdienstes stellen sollte und die bereits aus früheren Artikeln dieser Serie bekannt sind, werden um eine einzige architektonische Frage ergänzt:

1. Wird der Inhalt bei der Übertragung verschlüsselt? (Wahrscheinlich ja.)
2. Werden Metadaten darüber erzeugt und gespeichert, mit wem ich wann spreche? (Wahrscheinlich ja.)
3. Gibt es auf dem Weg zwischen meinem Gerät und dem des Empfängers einen Server?
4. Wenn ja: Wer betreibt ihn, in welcher Gerichtsbarkeit, und was müsste geschehen, damit er Daten über mich herausgibt?
5. Wenn nein: Die vorangegangenen Fragen sind gegenstandslos.

Der Unterschied zwischen beiden Kategorien ist nicht graduell, sondern fundamental. Wenn es an der Zeit ist, dies einem Mandanten, einem Patienten oder einem Kollegen zu erklären, ist die ehrlichste Formulierung auch die einfachste: Bei der einen ist jemand dazwischen; bei der anderen nicht.

Dieser Artikel schließt den ersten Zyklus der Cuadernos Lacre ab. Nach Verschlüsselung, Metadaten und Berufsgeheimnis vervollständigen wir das architektonische Bild: Den Inhalt zu verschlüsseln und keinen Server dazwischen zu haben, sind zwei verschiedene Dinge. Beides kann legal sein; nur eines eliminiert den Vertrauenspunkt.

Quellen und weiterführende Literatur

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Grundlagentext des Prinzips, nach dem die Garantien eines Systems an den Endpunkten implementiert werden sollten, nicht im dazwischenliegenden Kanal.
- Verordnung (EU) 2016/679, Art. 25 — Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
- Verordnung (EU) 2016/679, Art. 5.1.c — Grundsatz der Datenminimierung.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitel über Architekturen, die die Datenerhebung durch ihre Konstruktion minimieren.

← ZurückDSGVO und professionelles Messaging: Warum die meisten unwissentlich dagegen verstoßenWeiter →CUADERNOS_LIST_SCHREMS_TITLE

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 daaf8625b6176b8a0c56b2087696b12193b25774bd5b7d8b45c3767742f8a4cf

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

Präferenz des hellen/dunklen Designs erforderliche Minimum an JavaScript. Keine Tracker, kein Profiling, keine Datenweitergabe. Wenn Sie uns folgen möchten: RSS.